

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

внутрішню мережу безпечною, у Zero Trust є відкидання «безумовної» довіри і перевірки кожного підключення користувача або пристрою перед наданням будь-якого доступу на вимогу. Основний принцип полягає в наданні користувачу, пристрою або процесу тільки той рівень доступу, що необхідний для роботи. Наприклад, новому працівнику дають доступ тільки до потрібних файлів на час виконання роботи, а після завершення такої, права доступу автоматично прибирають. Така поведінка дозволяє зменшити можливість атаки і сильно ускладнює рух атакуючого в мережі.

Для великих компаній або закладів вищої освіти гарним рішенням є мікросегментація, коли мережа поділена на дрібні, зазвичай ізольовані сегменти або різні підмережі для різних факультетів чи служб, з власними правилами доступу та об'ємами даних. Відтак жоден студент чи співробітник одного відділу не отримає доступу до ресурсів іншого, якщо це не передбачено вимогами. Для мікросегментації часто використовується технологія контейнеризації, але нажаль навіть такий варіант не позбавлений певних недоліків. Звісно можна додати багатофакторну автентифікацію, додасть кілька додаткових етапів перевірки особи перед входом у систему, наприклад за допомогою одноразового паролю чи апаратного токена, або ж використовувати превентивні заходи, акті як постійний моніторинг та адаптивні політики. В такому випадку налаштована система контролю безперервно аналізує поведінку користувачів, процесів і пристроїв, та за необхідності фіксує місце, час та інша параметри, що можуть свідчити про аномальне відхилення і призводить до додаткової перевірки або блокування на певний час. Завдяки таким превентивним механізмам більшість атак виявляються майже миттєво, а політики доступу можна швидко коригувати в залежності від вимог.

Незважаючи на те, що концепція Zero Trust досі розвивається, станом на сьогодні вже є приклади застосування такої концепції в освітніх установах. В інженерному коледжі Університету Південної Кароліни (США) побудовано ізольоване науково-дослідне середовище (Carolina Enclave for Secure Research) для проєктів оборонного департаменту США. Для захисту даних було обрано саме Zero Trust-платформу Zscaler Zero Trust Exchange. Зазначено, що ця платформа фільтрує контент, щоб запобігти виведенню надчутливих даних, працює поза межами звичайної інфраструктури та підтримує віддалених користувачів [3]. Таким чином, навіть проникнення на локальний сервер чи в локальну мережу не дає зловмиснику доступу до наукових даних без додаткової автентифікації. В Україні мало публічних кейсів, проте, досвід світових провідних закладів вищої освіти демонструє ефективність підходу для освітнього середовища України.

Список використаних джерел

1. Про кібербезпеку в Україні - KPMG Ukraine [Електронний ресурс] – Режим доступу: <https://kpmg.com/ua/uk/home/media/press-releases/2023/08/pro-kiberbezpeku-v-ukrayini.html>- Назва з екрану
2. CERT-UA минулого року опрацювала 4315 кіберінцидентів [Електронний ресурс] – Режим доступу: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv> - Назва з екрану
3. Marshall Hollis, University of South Carolina Case Study [Електронний ресурс] – Режим доступу: <https://www.zscaler.com/customers/university-south-carolina> - Назва з екрану

Науковий керівник: Миронцов М.Л., д.ф.-м.н. старший науковий співробітник