Набуття досвіду прийняття управлінських рішень на основі даних із використанням хмарних технологій передбачає формування здатності збирати, зберігати, обробляти та аналізувати інформацію за допомогою цифрових інструментів, а також інтерпретувати отримані результати для обґрунтування ефективних управлінських рішень. Використання хмарних сервісів забезпечує доступ до актуальних даних у режимі реального часу, сприяє розвитку аналітичного мислення, підвищує точність прогнозування та ефективність управлінської діяльності в умовах цифрового середовища [1].

Підвищення рівня автономності та відповідальності здобувачів освіти засобами хмарних технологій передбачає створення умов для самостійного планування, організації та контролю власної діяльності у цифровому освітньому середовищі. Використання хмарних сервісів забезпечує постійний доступ до навчальних матеріалів, інструментів самооцінювання та моніторингу результатів, що сприяє розвитку саморегуляції, відповідального ставлення до виконання завдань і здатності приймати самостійні рішення у процесі навчання.

Ефективність використання хмарних технологій у формуванні управлінської компетентності залежить від педагогічних умов, зокрема: інтеграції цифрових інструментів у зміст дисциплін, використання проєктного та проблемно-орієнтованого навчання, створення цифрового освітнього середовища, а також підготовленості викладачів до використання відповідних технологій.

Отже, хмарні технології є дієвим інструментом формування управлінської компетентності у здобувачів вищої освіти, оскільки сприяють розвитку ключових управлінських умінь і забезпечують адаптацію майбутніх фахівців до умов цифрового суспільства.

Список використаних джелел

1. Листопад О. А., Листопад Н. Л. Хмарні технології як інструмент цифрової трансформації управління закладом вищої і фахової передвищої освіти. Збірник тез IX Всеукраїнської науково-практичної конференції *Нові інформаційні технології управління бізнесом*. Київ: Спілка автоматизаторів бізнесу, 2026. С. 158–162.

2. Мардарова І. К., Гуданич Н. М. Хмарні платформи як засіб підвищення ефективності освітнього менеджменту. Збірник тез IX Всеукраїнської науково-практичної конференції *Нові інформаційні технології управління бізнесом*. Київ: Спілка автоматизаторів бізнесу, 2026. С. 174–178.

INQUIRY-BASED LEARNING У ФОРМУВАННІ КУЛЬТУРИ КІБЕРБЕЗПЕКИ: ЦИФРОВА СТІЙКІСТЬ В УМОВАХ ВОЄННОГО СТАНУ

Іваницький Роман Іванович
кандидат технічних наук, асистент кафедри інформатики та методики її навчання
Тернопільський національний педагогічний університет імені Володимира Гнатюка
romik_iv@ukr.net
Ковальчук Ольга Ярославівна
доктор юридичних наук, кандидат фізико-математичних наук, доцент кафедри теорії права та конституціоналізму
Західноукраїнський національний університет
olhakov@gmail.com

Повномасштабна війна рф проти України докорінно змінила вимоги до підготовки фахівців у всіх сферах, передусім у технічній та юридичній. Поряд із традиційними компетентностями у студентів формується запит на практичне

розуміння кіберзагроз, спроможність критично оцінювати інформаційне середовище та діяти в умовах цифрової нестабільності. Водночас академічне навчання кібербезпеці в багатьох вітчизняних закладах вищої освіти досі залишається переважно теоретичним і слабко пов'язаним із реальним досвідом гібридної війни, в яку втягнуто Україну.

Проблема полягає не у відсутності навчального контенту з кібербезпеки, а у розриві між декларативними знаннями та операційною готовністю студентів. Майбутні фахівці у сферах інформаційних технологій (ІТ) та права здатні описати принципи захисту інформаційних систем, однак вони демонструють низьку спроможність реагувати на реальні інциденти (фішингові атаки, маніпулятивні OSINT-кампанії, витоки персональних даних), які стали буденністю воєнного часу. Цей розрив є педагогічною, а не лише технічною проблемою. Для студентів-правників він набуває додаткового виміру: недостатня цифрова грамотність безпосередньо впливає на якість майбутньої професійної діяльності у сфері кіберправа, захисту персональних даних та розслідування кіберзлочинів.

У відповідь на цей виклик ми пропонуємо модель «активної цифрової стійкості», що реалізується через три такі педагогічні принципи:

1. Контекстуалізація загроз. Навчальний матеріал будується на верифікованих кейсах кіберінцидентів воєнного часу: атаки на держреєстри, дезінформаційні кампанії у Telegram-каналах, злом критичної інфраструктури. При цьому для студентів ІТ-спеціальностей акцент робиться на технічному аналізі векторів атак, тоді як для майбутніх правників – на правових наслідках інцидентів, механізмах відповідальності та доказовій базі у кіберсправах. Такий диференційований підхід дозволяє зберегти єдину навчальну канву, адаптувати навчальну програму до фахового профілю студента [2].

2. Симуляційне навчання під тиском, що поєднує використання CTF-змагань (Capture the Flag) і рольових сценаріїв, де студент діє в умовах обмеженого часу та неповної інформації [1]. Для студентів-правників рольові сценарії моделюють реальні ситуації: допит постраждалих від кібератаки, складання процесуальних документів за матеріалами цифрового розслідування, юридична кваліфікація інциденту в режимі реального часу.

Показовим прикладом такого підходу є симуляція фішингової атаки: студент ІТ-спеціальності аналізує її технічну складову (підроблені заголовки електронного листа, фіктивний домен, механізм перенаправлення), тоді як студент-правник працює з тим самим кейсом у правовому вимірі: кваліфікує діяння за відповідними статтями КК України, визначає склад цифрових доказів та процесуальний порядок їх фіксації [3]. Таке паралельне опрацювання одного інциденту наочно демонструє нерозривність технічних та правових складових у протидії кіберзагрозам.

3. Рефлексивне портфоліо цифрового інциденту. Студент документує та аналізує реальні випадки зіткнення з кіберзагрозами у власному цифровому житті. Для правників цей інструмент розширюється до аналізу публічних судових справ у сфері кіберзлочинності, що формує зв'язок між особистим досвідом і майбутньою професійною практикою.

Теоретичним підґрунтям моделі слугує концепція inquiry-based learning (IBL) – навчання через дослідницький пошук [4]. Студент не отримує готові алгоритми захисту, а самостійно досліджує механізми атаки, формулює гіпотези щодо вразливостей і перевіряє їх у симуляційному середовищі. IBL формує навичку прийняття рішень в умовах невизначеності. Це саме та компетентність,

якої потребують як ІТ-фахівець, так і юристи під час реального інциденту, коли часу на обдумування немає, а ціна помилки висока. Підхід POGIL (Process-Oriented Guided Inquiry Learning), апробований у технічних дисциплінах, довів ефективність у паралельному розвитку технічних і аналітичних навичок [5]. IBL однаково продуктивний для обох цільових груп: ІТ-студент і студент-правник проходять спільний дослідницький цикл (спостереження, гіпотеза, перевірка, рефлексія). Відрізняються тільки інструментарій і перспектива аналізу. Поєднання IBL із дослідженням реальних кіберінцидентів воєнного часу створює навчальне середовище, у якому критичне мислення й фахова компетентність розвиваються як єдина, нерозривна якість.

Окремим складником моделі є навчання студентів критичному ставленню до інструментів штучного інтелекту як потенційного вектора атак. Генеративні моделі активно використовуються для створення дипфейків, автоматизованих фішингових листів та синтетичної дезінформації. З цими явищами ІТ-фахівець стикатиметься як розробник або системний адміністратор, а юрист – як учасник розслідування або судового процесу, де такі матеріали фігурують як докази чи інструменти маніпуляції. Відповідна компетентність стає критично важливою як для одних, так і для інших [1].

Навчання кібербезпеці в умовах активного збройного конфлікту не може залишатися академічною дисципліною у класичному розумінні. Воєнний стан перетворює цифрову стійкість і здатність до швидкого прийняття ефективних рішень з питань національної безпеки, а університет – на один із ключових інститутів їх формування. Міждисциплінарне поєднання ІТ та права у контексті кібербезпеки є не методичним експериментом, а відповіддю на реальну потребу: ефективна протидія кіберзагрозам вимагає одночасно технічної спроможності та правової рамки для її застосування. Концепція активної цифрової стійкості на засадах IBL пропонує педагогічну відповідь на цей виклик, переводячи підготовку фахівця з площини знань у площину дії.

Список використаних джерел

1. Василенко В., Гринкевич Г., Кузнєцов І. Роль змагань capture-the-flag (ctf) у дослідженнях та навчанні з кібербезпеки: аналіз машини “Editorial”. *Кібербезпека: освіта, наука, техніка*. 2022. № 4(28). С. 137–149. URL: https://doi.org/10.28925/2663-4023.2025.28.762. (дата звернення 03.03.2026).

2. Ковальчук О. Я., Іваницький Р. І. Впровадження проблемно-орієнтованого навчання при вивченні дисципліни «Логіка» студентами юридичних спеціальностей. Матеріали V Міжнародної науково-практичної інтернет-конференції «Сучасні інформаційні технології та інноваційні методики навчання: досвід, тенденції, перспективи» (м. Тернопіль, 30 квітня, 2020). Тернопіль : ТНПУ ім. В. Гнатюка, 2020. С. 26–28.

3. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III. *Законодавство України*. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (дата звернення 07.03.2026).

4. Sam R. Systematic review of inquiry-based learning: assessing impact and best practices in education. *F1000Research*. 2024. Vol. 13:1045. URL: https://f1000research.com/articles/13-1045/v1. (дата звернення 13.02.2026).

5. He Y., He W., Xu L., Tian X., Yuan X., Yang L., Ellis J. T. Guided Inquiry Collaborative Learning (GICL) for Online Teaching in Cybersecurity: Challenges and Recommendations. *Computer and Information Science and Engineering (CISSE).* 2022. Vol. 9. No. 1. URL: https://cisse.info/journal/index.php/cisse/article/view/143. (дата звернення 01.03.2026).