

В цілому, цифрові інструменти взаємного оцінювання можуть бути корисним засобом для покращення навчального процесу, розвитку навичок самооцінки та сприяння співпраці між студентами.

Список використаних джерел

1. Boud D., Cohen R. & Sampson J. (1999): Peer Learning and Assessment, *Assessment & Evaluation in Higher Education*, 24:4, 413-426. <http://dx.doi.org/10.1080/0260293990240405>.
2. Артющина М.В., Артющин Г.М., Саркісова О.Ю. (2025). Особистісна рефлексивність як психологічний чинник запровадження технології рефлексивного контролю в освіті дорослих. *Наукові перспективи*. № 1 (55). 1626-1642. DOI: [https://doi.org/10.52058/2708-7530-2025-1\(55\)-1626-1642](https://doi.org/10.52058/2708-7530-2025-1(55)-1626-1642).
3. Артющина М.В., Саркісова О.Ю. (2024). Технологія пірінгового навчання в умовах цифрової трансформації вищої освіти в Україні. *Вісник Національного авіаційного університету. Серія: Педагогіка. Психологія*. Т. 1. № 24. 9-19. DOI: <https://doi.org/10.18372/2411-264X.24.19194>.
4. *Модернізація освіти в цифровому вимірі: монографія* (2021) / за наук. ред. Н. Морзе, О. Буйницької. Київ : Київ. ун-т ім. Б. Грінченка. 300.
5. Романов Л. А. Забезпечення рефлексивного контролю навчання студентів (2013). *Гуманітарний вісник ДВНЗ «Переяслав-Хмельницький державний педагогічний університет імені Григорія Сковороди»*. Вип. 31 (49). 523-529.

Вдовіна О.О.,

к. соц. ком., доц.,

Національний університет оборони України

КІБЕРБЕЗПЕКА В СИСТЕМІ ВИЩОЇ ОСВІТИ: ЗАБЕЗПЕЧЕННЯ ЯКОСТІ В УМОВАХ ЦИФРОВИХ ЗАГРОЗ

Упродовж останнього десятиліття система вищої освіти України дедалі активніше інтегрується в цифровий простір. Від електронного документообігу до віртуальних середовищ навчання — майже всі ключові процеси закладів вищої освіти (далі - ЗВО) частково або повністю переходять у цифрову площину.

Така трансформація відкриває широкі можливості для гнучкості, доступності та модернізації освітніх послуг. Водночас, вона суттєво змінює карту ризиків, з якими стикаються університети. Кібератаки, витоки персональних даних, підміна результатів навчання, блокування платформ дистанційного доступу — все це вже не гіпотетичні сценарії, а реальні виклики, які вимагають системної реакції. У цьому контексті питання кібербезпеки більше не може розглядатись як суто технічна або ІТ-проблема. Йдеться про базову умову підтримки якості вищої освіти, її безперервності, доброчесності та довіри. Саме тому сьогодні постає потреба в науковому осмисленні кібербезпеки як складової стратегічного управління якістю в цифровому освітньому середовищі. Це, у свою чергу, вимагає міждисциплінарного підходу і комплексного аналізу на перетині освітології, інформаційної безпеки та менеджменту ризиків.

Проблема кібербезпеки в системі вищої освіти не зводиться до захисту інфраструктури чи запобігання інцидентам — вона зачіпає саму сутність освітнього процесу, його цілісність і довіру до результатів. Тому необхідно осмислити низку ключових понять: цифрову безпеку освіти як захист не лише інфраструктури, а й освітнього змісту, процедур оцінювання, персональних даних; кіберстійкість ЗВО як здатність забезпечувати безперервність освітніх і управлінських функцій в умовах інцидентів; інституційну кіберграмотність як нову норму професійної культури освітян, керівників і здобувачів освіти. Такий концептуальний підхід дозволяє сформувати цілісне уявлення про кібербезпеку не як про технічну опцію, а як про невід’ємну складову системного забезпечення якості вищої освіти.

Розуміння кібербезпеки як ключової передумови якісного функціонування ЗВО в цифрову добу потребує не лише теоретичного осмислення, а й чіткого уявлення про ті загрози, з якими університети стикаються на практиці. Після виявлення критичних понять, що формують бачення цифрової безпеки освітнього середовища, необхідно перейти до конкретизації характеру ризиків, їх типології та механізмів впливу на освітні процеси. Сьогодні університети функціонують у мінливому цифровому середовищі, де атаки на інфраструктуру освітніх платформ, втручання в бази даних студентських досягнень,

компрометація облікових записів працівників та студентів, маніпуляції в системах оцінювання й реєстрації навчальних результатів — не поодинокі інциденти, а системна загроза, що вимагає глибокого аналітичного реагування.

Серед найпоширеніших загроз, що безпосередньо впливають на якість освітнього процесу, варто виокремити фішингові атаки на корпоративну пошту працівників, злам акаунтів у системах управління навчанням (LMS), поширення шкідливого програмного забезпечення через внутрішні сервіси, а також цілеспрямовані інсайдерські дії — несанкціонована зміна оцінок, викрадення інтелектуальної власності, копіювання захищених освітніх матеріалів. Як слушно зазначають дослідники, «ключовими факторами ефективного протистояння кіберзагрозам є рівень підготовки, компетентність і відповідальність учасників освітнього процесу» [1], що безпосередньо співвідноситься з поняттям інституційної кіберграмотності як одного з опорних елементів забезпечення якості. Науковці та фахівці з кібербезпеки наголошують на тому, що нині «Проблема захисту інформації від різних загроз: — несанкціонований доступ – 2%; — укорінення вірусів – 3%; — технічні відмови апаратури мережі – 20%; — цілеспрямовані дії персоналу – 20%; — помилки персоналу (недостатній рівень кваліфікації) – 55%» [2]. Їхня типологізація є відправною точкою для формування відповідної системи протидії. На цьому етапі постає потреба в структурованому управлінні ризиками та посиленні кіберстійкості університету як складової його академічної надійності.

У цьому контексті важливо усвідомити, що рівень кіберзахищеності прямо впливає на здатність ЗВО гарантувати якість освітніх послуг. Стійкий доступ до електронних платформ, достовірність даних про результати навчання, захист персональної інформації — це не просто технічні параметри, а ключові ознаки якості вищої освіти. Порушення цих елементів підриває систему оцінювання, дискредитує академічну доброчесність і може спричинити правові конфлікти. Згідно зі ст. 16 Закону України «Про освіту» [3], якість освітньої діяльності передбачає дотримання академічної доброчесності, прозорість процедур оцінювання, захист прав усіх учасників освітнього процесу — усі ці компоненти

вразливі в умовах слабкої цифрової безпеки. Кібератака, що призводить до втрати навчальних даних або несанкціонованих змін, має наслідки як для репутації закладу, так і для його легітимності. Тому кібербезпека повинна розглядатися не як допоміжна функція, а як структуроутворюючий чинник якості освіти.

Оцінка рівня цифрового захисту ЗВО в Україні засвідчує значну нерівномірність. Деякі університети вже реалізують політики інформаційної безпеки — впроваджують автентифікацію доступу до освітніх сервісів, проводять резервне копіювання, здійснюють аудит доступів, інформують персонал про правила кібергігієни. Проте більшість ЗВО не мають регламентованих внутрішніх документів, штатних фахівців із кібербезпеки, а також практикують ризиковані підходи до комунікації, використовуючи публічні мережі або неавторизовані платформи. Фахівці у сфері кібербезпеки стверджують, що саме освітні установи входять до переліку найбільш атакованих категорій. Така вразливість пояснюється відсутністю уніфікованих стандартів захисту та слабким інтегруванням кібербезпеки в управлінську модель. В окремих випадках її розглядають як технічне питання, що належить до сфери IT-відділу, а не як стратегічний напрям розвитку. Проте сьогодні виникає об'єктивна необхідність визнання інформаційної безпеки частиною системи забезпечення якості та інституційної відповідальності.

Побудова кіберстійкого університету вимагає розгортання цілісної політики, що поєднує оцінювання ризиків, управління інцидентами, навчання персоналу, аудит інформаційної безпеки, а також лідерську відповідальність керівництва. Важливою умовою є впровадження міжнародних стандартів ISO/IEC 27001 [4] або NIST [5], адаптованих до потреб вищої освіти. Ці моделі дають змогу системно управляти ризиками, підвищувати довіру до результатів діяльності закладу та забезпечувати сталість його функціонування в умовах зростаючих цифрових загроз.

Реалізація таких підходів вимагає нормативної, організаційної та освітньої інтеграції. Зокрема, доцільно розробити внутрішні документи, що регламентують інформаційну безпеку, ввести обов'язкові тренінги для всіх учасників освітнього процесу, передбачити регулярний аудит систем безпеки. Інституційний рівень

відповідальності має бути підкріплений керівними рішеннями та участю академічної спільноти у формуванні безпечного цифрового простору. Впровадження міжнародних стандартів сприятиме не лише відповідності університетів глобальним практикам, а й підвищенню якості освітніх послуг. Саме системне поєднання технічних рішень, управлінських стратегій і педагогічної відповідальності створює передумови для формування надійного освітнього середовища.

Забезпечення якості вищої освіти в умовах цифрових загроз неможливе без цілісної системи кібербезпеки, інтегрованої в управлінські, нормативні та освітні процеси. Формування культури цифрової безпеки, підвищення обізнаності всіх учасників освітнього процесу та впровадження міжнародних стандартів управління інформаційною безпекою є передумовами стійкого розвитку університетів. Тільки скоординований підхід дозволить гарантувати довіру до освітніх результатів і зберегти академічну доброчесність у цифрову добу.

Список використаних джерел

1. Литвинов, О., Філіпенко, Н., Лукашевич, С., & Палкова, К. (2024). Кібербезпека як фактор ефективності закладів вищої освіти. *Пропілеї права та безпеки*, (5), 15–23. <https://doi.org/10.32620/pls.2024.5.02>.
2. Бурячок, А. І., & Бурячок, В. А. (2020). Технологія забезпечення інформаційної і кібербезпеки в закладах вищої освіти України. *ResearchGate*. <https://www.researchgate.net/publication/342579531>.
3. Верховна Рада України. (2017). Закон України «Про освіту» № 2145-VIII від 05.09.2017 р. Вилучено з: <https://surl.li/lkovul>.
4. International Organization for Standardization. (2013). *ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements*. Geneva: ISO. Retrieved from <https://www.iso.org/standard/54534.html>.
5. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity, version 1.1*. Gaithersburg, MD: NIST. Retrieved from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.