

Вербовський І.А. Кібербезпека фінансових операцій закладів вищої освіти в умовах тотальної цифровізації. *Матеріали XII Міжнародної науково-практичної Інтернет-конференції*, 24 квітня 2025 р. Полтава : Національний університет імені Юрія Кондратюка, 2025. С. 180-183.

Вербовський Ігор Андрійович

кандидат педагогічних наук, доцент, доцент кафедри професійно-педагогічної, спеціальної освіти, андрагогіки та управління, начальник навчального відділу

Житомирського державного університету імені Івана Франка

КІБЕРБЕЗПЕКА ФІНАНСОВИХ ОПЕРАЦІЙ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ В УМОВАХ ТОТАЛЬНОЇ ЦИФРОВІЗАЦІЇ

Тотальна цифровізація освітніх процесів, зокрема фінансових операцій, суттєво підвищує ефективність управління ресурсами закладів вищої освіти. Однак паралельно зростають ризики кіберзагроз, пов'язані з витоком конфіденційних даних, фінансовими шахрайствами та атаками на інфраструктуру.

Дослідження кібербезпеки у фінансовому секторі активно розвиваються. Так, Н. Ситник та І. Половчак. аналізують вплив цифровізації на фінансову безпеку банків, акцентуючи увагу на необхідності гнучких механізмів захисту даних [6]. С. Козанчин виділяє специфіку кібербезпеки страхових компаній, зокрема важливість нормативно-правової бази [4]. У контексті закладу вищої освіти А. Мазаракі, Н. Новікова та Ю. Сонько підкреслюють роль цифрових компетенцій, але недостатньо висвітлюють аспекти фінансових ризиків. Н. Пасько та О. В'юненко в своїх працях досліджують вразливості електронних систем навчання, що має прямий зв'язок із захистом фінансових транзакцій [7].

Аналіз наукових праць свідчить про значний прогрес у дослідженні окремих аспектів кібербезпеки фінансових інституцій. Однак фрагментарність підходів, обмежена увага до специфіки закладів вищої освіти та недостатнє врахування системних взаємозв'язків між цифровізацією освітніх процесів і фінансовими ризиками обумовлюють низку структурних проблем.

На сьогоднішній день заклади вищої освіти стикаються з унікальними викликами: обробка масивів персональних даних студентів і співробітників, проведення онлайн-платежів за навчання, управління грантовими коштами та інтеграція з державними фінансовими системами. Це створює численні точки вразливості, зокрема ризик фішингових атак на бухгалтерські служби, маніпуляцій з електронними рахунками або навіть блокування доступу до систем через DDoS-атаки. Як зазначають дослідження, понад 60% кібератак на освітні установи мають фінансову мотивацію, що підкреслює критичність адаптації банківських механізмів захисту до академічного середовища [3, 6].

Ефективне протидіяння цим загрозам вимагає інтеграції технологічних, організаційних та нормативних рішень. Технологічно доречним є впровадження багатофакторної аутентифікації для доступу до фінансових систем, шифрування транзакцій за стандартами PCI DSS та використання штучного інтелекту для виявлення аномалій у фінансових потоках [1, 2]. Наприклад, досвід банківського сектору демонструє ефективність машинного навчання у виявленні підозрілих операцій у реальному часі, що може бути адаптовано для моніторингу бюджетних розподілів або стипендіальних виплат [6].

Організаційний аспект передбачає створення окремих підрозділів кібербезпеки в структурі закладів, які займатимуться регулярним аудитом систем, оновленням протоколів захисту та навчанням персоналу. Сьогодні більшість успішних кібератак на освітні установи пов'язані з людським фактором, зокрема недостатньою обізнаністю співробітників щодо соціальної інженерії [2, 8]. Тому впровадження обов'язкових тренінгів з кіберграмотності, аналогічно до вимог НБУ для банківських працівників, має стати ключовим елементом стратегії [6].

Нормативна складова потребує синхронізації з державними ініціативами. Наприклад, запровадження обов'язкових стандартів кібербезпеки для закладів вищої освіти, аналогічних до «Положення про захист інформації та кіберзахист учасниками платіжного ринку» НБУ, могло б уніфікувати вимоги до шифрування даних, резервного копіювання та протоколів реагування на інциденти. Важливим кроком є також інтеграція фінансових систем університетів із державними платформами кіберзахисту, що дозволить оперативно обмінюватися даними про нові загрози та координувати зусилля.

Таким чином, забезпечення кібербезпеки фінансових операцій у закладах вищої освіти потребує системного підходу, що поєднує технологічні інновації, організаційні зміни та гармонізацію нормативної бази. Досвід фінансового сектору, зокрема банківської галузі, слугує важливим орієнтиром, але потребує адаптації з урахуванням специфіки академічного середовища. Подолання фрагментарності в підходах та інтеграція зусиль усіх стейкхолдерів – від адміністрації закладів до державних органів – є запорукою стійкості фінансових систем освіти в умовах тотальної цифровізації.

Література:

1. Белов А. О. Система захисту банківських онлайн транзакцій: квал. роб. ... маг. : 125 / Державний торговельно-економічний університет. Київ. 2023.
2. Дмитренко Т. Л., Терещенко Г. М. Підвищення рівня освіти у сфері кібербезпеки, фінансової та цифрової грамотності як чинник зниження ризиків на крипторинку. Освітня аналітика України. 2023. Вип. 1. С. 38-50. URL: http://nbuv.gov.ua/UJRN/educanalukr_2023_1_4
3. Дорош О. В., Василенко В. Ю. Особливості забезпечення цифрової безпеки під час реалізації освітнього процесу в закладах освіти. Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса. 2023. Випуск 15. Том 2. С. 190-193. URL: <https://jvestnik-sss.donnu.edu.ua/article/view/14712>
4. Козачин С. М. Кібербезпека фінансових установ України: квал. роб. ... маг. : 072 / Львівський національний університет імені Івана Франка. Львів. 2022. 74 с.
5. Мазаракі А., Новікова Н., Сонько Ю. 2020. Цифрові детермінанти трендів підготовки фахівців. Вісник Київського національного торговельно-економічного університету. 2020. № 2 С. 5–20. DOI: [https://doi.org/10.31617/visnik.knute.2020\(130\)01](https://doi.org/10.31617/visnik.knute.2020(130)01).
6. Ситник Н., Половчак І. Цифровізація та кібербезпека у забезпеченні фінансової безпеки банків в умовах війни. Галицький економічний вісник. 2024. Том 89. № 4. С. 70-81. DOI: https://doi.org/10.33108/galicianvisnyk_tntu2024.04.070
7. Pasko N., Viunenko O. Modeling Human-Machine Interaction in Information Processing and Management Systems. European Science, 2023. Vol. sge17-02, pp. 6–52. DOI: <https://doi.org/10.30890/2709-2313.2023-17-02-027>

8. Why the Education Sector Needs to Prioritize Cybersecurity.
GlobalSign Blog. URL: <https://www.globalsign.com/en/blog/why-education-sector-needs-prioritize-cybersecurity>