

КІБЕРБЕЗПЕКА У ЦИФРОВИХ ФІНАНСОВИХ СИСТЕМАХ ЗАКЛАДІВ ВИЩОЇ ОСВІТИ: РИЗИКИ ТА ЗАСОБИ ЗАХИСТУ

Вербовський Ігор

кандидат педагогічних наук, доцент

Кафедра професійно-педагогічної,

спеціальної освіти, андрагогіки та управління

Житомирський державний університет імені Івана Франка

здобувач вищої освіти магістерського рівня

спеціальності 072 Фінанси, банківська справа та страхування

Поліський національний університет, Україна

У сучасних умовах цифровізації освітнього простору питання забезпечення кібербезпеки у фінансових системах закладів вищої освіти набуває особливої актуальності. Зростання обсягів обробки та зберігання конфіденційної

інформації, використання електронних платіжних систем, а також впровадження дистанційних освітніх платформ підвищують ризики кібератак, витоку персональних та фінансових даних студентів і співробітників. Недостатній рівень захищеності цифрової інфраструктури закладів освіти може призвести до фінансових втрат, порушення освітнього процесу та втрати довіри до інституцій. Враховуючи зростаючу складність кіберзагроз та обмеженість ресурсів закладів освіти, формування ефективної системи кібербезпеки є необхідною умовою стабільного функціонування та розвитку цифрових фінансових систем у сфері вищої освіти.

Проблематика кібербезпеки у фінансових системах закладів вищої освіти досліджується як українськими, так і зарубіжними науковцями. Серед вітчизняних дослідників варто відзначити роботи Калекіної С. та Лісовської Ю., які аналізують особливості кіберзахисту фінансових установ [2, 3]. Значний внесок у дослідження ризиків цифровізації та механізмів кібербезпеки зробили Азьмук Н., Апалькова В., Волосович С., Циганова С., а також іноземні вчені – Forcadell F. J., Eisenbach T. M., Kovner A., Lee M. J., які розглядають питання захисту даних та управління кіберризиками у фінансових системах [6]. Окрему увагу приділяють питанням цифрової грамотності та формування культури кібербезпеки в освітньому середовищі. Незважаючи на значний науковий доробок, питання інтеграції сучасних засобів захисту у цифрових фінансових системах вимагає подальшого дослідження з урахуванням новітніх загроз та специфіки освітніх установ.

Особливу увагу слід приділяти людському фактору, оскільки необізнаність користувачів щодо основ кібергігієни сприяє успішності атак. За даними досліджень, більшість інцидентів у сфері вищої освіти пов'язані саме з помилками користувачів або нехтуванням правилами безпеки [5]. Відтак, важливою складовою захисту є проведення регулярних навчань та підвищення обізнаності студентів і персоналу щодо сучасних кіберзагроз.

Управління кібербезпекою у фінансових системах закладів вищої освіти передбачає впровадження багаторівневих технічних та організаційних заходів. Згідно з рекомендаціями Universities UK, ефективна система кіберзахисту повинна базуватися на чотирьох основних компонентах: управлінні (governance), забезпеченні (assurance), технологіях (technology) та культурі безпеки (culture). Зокрема, до базових технічних засобів захисту належать використання сучасних антивірусних програм, шифрування даних, двофакторна автентифікація, регулярне оновлення програмного забезпечення та моніторинг мережевої активності [6].

Важливим аспектом є розробка політик доступу до фінансової інформації, ідентифікація користувачів та контроль за діями в інформаційних системах. Для цього рекомендується впроваджувати системи управління ідентифікацією та доступом (IAM), а також вести журнали аудиту для виявлення аномальної активності. Окрему увагу слід приділяти захисту особистих пристроїв, які підключаються до мережі закладу, оскільки вони можуть стати джерелом проникнення шкідливого програмного забезпечення

У таблиці 1 наведено основні типи кіберзагроз для фінансових систем закладів вищої освіти та відповідні засоби захисту.

Таблиця 1. Основні типи кіберзагроз для фінансових систем закладів вищої освіти та відповідні засоби захисту

Тип кіберзагрози	Опис загрози	Засоби захисту
Фішинг	Викрадення облікових даних через підроблені листи	Навчання, фільтри електронної пошти
Програми-вимагачі	Блокування даних із вимогою викупу	Резервне копіювання, антивірус
Несанкціонований доступ	Злом облікових записів, отримання фінансової інформації	Двофакторна автентифікація, IAM
Інсайдерські загрози	Дії співробітників або студентів з доступом до системи	Контроль доступу, аудит дій
Атаки на інфраструктуру	DDoS-атаки, виведення з ладу фінансових платформ	Захисні шлюзи, моніторинг мережі

Законодавчі вимоги до кібербезпеки у сфері освіти також передбачають впровадження стандартів захисту даних, зокрема відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» та міжнародних норм, таких як GDPR для захисту персональних даних [1, 4]. Дотримання цих вимог є обов'язковим для уникнення юридичних та фінансових санкцій.

Зарубіжний досвід свідчить про ефективність впровадження багаторівневого захисту (defence in depth), що поєднує технічні, організаційні та освітні заходи. Наприклад, у Великій Британії університети активно впроваджують сертифікацію Cyber Essentials, що дозволяє підвищити рівень базового захисту та продемонструвати відповідність сучасним вимогам кібербезпеки. В Україні також спостерігається тенденція до інтеграції західних практик у систему управління кіберризиками у вищій освіті [6].

Таким чином, забезпечення кібербезпеки у цифрових фінансових системах закладів вищої освіти є багатогранним завданням, що вимагає поєднання сучасних технологій, ефективного управління ризиками, постійного навчання користувачів та дотримання законодавчих вимог.

Забезпечення кібербезпеки у цифрових фінансових системах закладів вищої освіти є ключовим чинником їх ефективного функціонування та розвитку. Комплексний підхід до управління кіберризиками, що включає технічні, організаційні та освітні заходи, дозволяє мінімізувати ймовірність виникнення інцидентів, пов'язаних із витоком або знищенням фінансової інформації. Впровадження сучасних технологій захисту, регулярне оновлення програмного забезпечення, контроль доступу та підвищення обізнаності користувачів сприяють формуванню стійкої системи кібербезпеки. Досвід зарубіжних країн підтверджує ефективність багаторівневих систем захисту, які доцільно адаптувати до українських реалій. Подальші дослідження у цій сфері мають бути спрямовані на розробку інноваційних рішень для протидії новим типам кіберзагроз, а також на вдосконалення нормативно-правового забезпечення кібербезпеки у сфері вищої освіти.

Список використаних джерел

1. Гелеш А. В., Матійців Б. О. Актуальні питання кібербезпеки у професійній освіті: методи захисту інформації. Академічні візії. 2025. Випуск 42. С. 1-5. DOI: <https://doi.org/10.5281/zenodo.15376086>
2. Калекіна С. С. Загрози кібербезпеці банківських установ при впровадженні банківських інновацій та шляхи їх усунення. Теоретичні та практичні аспекти формування економічної системи в умовах нестабільності збірник тез наукових робіт. 2020. С. 78-82
3. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посіб. Київ, 2019. 272 с.
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
5. Савченко В., Маклюк О. Кібербезпека як фактор ефективності функціонування закладів вищої освіти. Економіка та суспільство. 2024. № 60. DOI: <https://doi.org/10.32782/2524-0072/2024-60-24>
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. Cyber security and universities: managing the risk [Електронний ресурс]. 2023. URL: [https://www.universitiesuk.ac.uk/sites/default/files/uploads/UUKi%20reports/279%20FINAL%20-%20Cyber%20Security%20and%20Universities%20\(002\).pdf](https://www.universitiesuk.ac.uk/sites/default/files/uploads/UUKi%20reports/279%20FINAL%20-%20Cyber%20Security%20and%20Universities%20(002).pdf)