УДК 351:37(477)
DOI https://doi.org/10.32782/tnv-pub.2025.2.5

КІБЕРБЕЗПЕКА В УКРАЇНСЬКИХ ЗАКЛАДАХ ОСВІТИ: ОСНОВНІ ПРОБЛЕМИ ТА ШЛЯХИ РОЗВ'ЯЗАННЯ

Дей Г. А. *– аспірант кафедри публічного управління і проектного менеджменту*
ДЗВО «Університет менеджменту освіти»
ORCID: 0009-0009-5358-3047

Актуалізація питання кібербезпеки в українських закладах освіти зумовлена різким зростанням цифрової залежності навчального процесу та одночасним збільшенням кількості кіберінцидентів у цій сфері. Освітні установи дедалі частіше стають об'єктами кібератак через слабкі механізми захисту персональних даних і недостатню підготовку учасників освітнього процесу. Метою дослідження є висвітлення основних проблем кібербезпеки в закладах освіти України та пошук ефективних шляхів їх розв'язання. У роботі використано метод системного аналізу для виявлення взаємозв'язків між технологічними, організаційними і кадровими чинниками вразливості; метод контент-аналізу – для оцінки поточного стану кібербезпеки на основі сучасних публікацій і нормативних джерел; метод класифікації – для впорядкування основних типів кіберзагроз; метод проблемно-цільового аналізу – для виокремлення ключових бар'єрів упровадження заходів безпеки; метод індуктивного узагальнення – для формулювання практичних напрямів розв'язання виявлених проблем. В процесі дослідження здійснена класифікація видів кіберзлочинів в освітньому середовищі, де акцентовано не лише на технічних, а й на соціотехнічних загрозах. Друге завдання передбачало виявлення основних бар'єрів упровадження кібербезпеки: визначено шість напрямів проблем, включно з інституційною неготовністю, кадровим дефіцитом, нестачею фінансування, низькою цифровою культурою, технічною вразливістю та фрагментарністю політик безпеки. Третє завдання полягало у формулюванні стратегічних шляхів розв'язання, серед яких: впровадження інтегрованих політик реагування на інциденти, модернізація технічної інфраструктури, розвиток цифрової компетентності персоналу, інституціоналізація культури кібергігієни. Дослідження підтвердило, що для реального підвищення рівня кібербезпеки закладам освіти необхідно не лише модернізувати інфраструктуру, а й змінити управлінські підходи, підвищити цифрову культуру всіх учасників освітнього процесу й сформувати стійку практику реагування на кіберзагрози.

Ключові слова: *інформаційна безпека, учасники освітнього процесу, кіберзлочини, освітні заклади, кібергігієна, виток даних, фішинг, програми-вимагачі.*

Dei H. A. Cybersecurity in Ukrainian educational institutions: main problems and ways to solutions

The actualization of the issue of cybersecurity in Ukrainian educational institutions is due to the sharp increase in the digital dependence of the educational process and the simultaneous increase in the number of cyber incidents in this area. Educational institutions are increasingly becoming objects of cyberattacks due to weak mechanisms for protecting personal data and insufficient training of participants in the educational process. The purpose of the study is to highlight the main problems of cybersecurity in Ukrainian educational institutions and find effective ways to solve them. The work uses the system analysis method to identify relationships between technological, organizational and personnel vulnerability factors; the content analysis method – to assess the current state of cybersecurity based on modern publications and regulatory sources; the classification method – to organize the main types of cyber threats; the problem-target analysis method – to identify key barriers to the implementation of security measures; the inductive generalization method – to formulate practical directions for solving the identified problems. The research has classified the types of cybercrimes in the educational environment, focusing not only on technical but also on socio-technical threats. The second task involved identifying the main barriers to implementing cybersecurity: six areas of problems were identified, including institutional unpreparedness, staff shortage, lack of funding, low digital culture, technical vulnerability, and fragmentation of security policies. The third task was to formulate strategic solutions, including: implementing integrated incident response policies, modernizing technical infrastructure, developing digital competence of personnel, and institutionalizing a culture of cyber hygiene. The study confirmed that to truly improve cybersecurity, educational institutions need not only to modernize infrastructure, but also to change management approaches, improve

the digital culture of all participants in the educational process, and form a sustainable practice of responding to cyber threats.

Key words: *information security, participants in the educational process, cybercrime, educational institutions, cyber hygiene, data leakage, phishing, ransomware.*

Постановка проблеми. Сьогодні інформація в будь-яких її проявах є найважливішою складовою розвитку людського суспільства. Вона супроводжує людину у всіх сферах її життя – економіці, політиці, промисловій і гуманітарній сферах. А, отже, система освіти не є винятком. Будь-який сучасний вітчизняний заклад освіти щодня отримує величезний потік інформації як ззовні, так і по внутрішніх каналах. І така інформація буває кардинально різною. Проте, у той же час існує такий масив інформації, який має залишатися конфіденційним, і бути доступним лише невеликому колу вищого керівництва такої організації. Тому заклади освіти мають здійснювати контроль за своєю інформаційною безпекою з метою забезпечення своєї освітньої й господарської діяльності. У світлі зазначеного вище, постає питання кібербезпеки закладів освіти, адже вони дедалі частіше стають мішенню для хакерських атак, витоків даних, онлайн-шантажу та кібербулінгу.

Слід також зазначити, що проблема кібербезпеки закладів освіти гостро постає не лише в Україні, але й у всьому світі. Так, у 2023 році уряд Великої Британії провів опитування щодо порушень кібербезпеки в освітніх установах. Було виявлено, що заклади вищої освіти більш схильні до кібервзломів і атак, ніж загальноосвітні заклади. Вони також схильні до більш різноманітного спектру типів атак, включно з підміною, вірусами або іншими шкідливими програмами, а також атаками типу «відмова в обслуговуванні» [1]. Схоже дослідження провів журнал Infosecurity Magazine – з 2018 року до середини вересня 2023 року кіберінциденти порушили понад 6,7 мільйона персональних записів, що призвело до втрат від простою в розмірі понад 53 мільярди доларів США. Тільки у США 386 інцидентів із програмами-вимагачами призвели до втрат від простою в розмірі 35,1 мільярда доларів США [2].

Отже, проблема дослідження полягає у тому, що в українських закладах освіти досі відсутній цілісний, зрозумілий і практичний підхід до кібербезпеки: не існує системного навчання, нормативної підтримки, оновленої інфраструктури й, головне, культури безпечної поведінки у цифровому середовищі. Тож ці аспекти потребують більш ґрунтовного аналізу і пошуку ефективних рішень.

Аналіз останніх досліджень і публікацій. Сьогодні тематика кібербезпеки в сфері освіти активно розглядається сучасними українськими і зарубіжними дослідниками. Так, у статті С. Доценко досліджено питання кібербезпеки учасників освітнього процесу під час дистанційного навчання. Представлено поради Міжнародного союзу електрозв'язку для навчальних закладів з метою підвищення безпеки в онлайн-середовищі [3]. Інші автори О. Карабін і М. Шуль розглядали теоретичні засади інформатизації освіти, розглянуто способи формування цифрової компетентності, окреслено актуальні напрями освітньої діяльності здобувачів освіти та їх адаптацію до умов інформаційного суспільства [4]. У дослідженні Л. Арсеновича здійснено аналіз вітчизняного і зарубіжного досвіду з питань формування цифрової компетентності і ефективного впровадження інформаційних технологій у навчальний процес [5]. Авторки Н. Бєляєва, О. Зацерковна та М. Ребрина у своїй роботі висвітили ключові аспекти формування безпечного й підтримувального освітнього середовища, яке забезпечує рівні умови для навчання та особистісного зростання кожного здобувача освіти [6].

Цікаве дослідження цієї проблеми було проведено зарубіжними науковцями I. Wada та ін., ними було здійснено аналіз керованих моделей штучного інтелекту, навчених на відкритих наборах даних із кібербезпеки, з метою отримання емпіричного уявлення про потенціал штучного інтелекту у підвищенні ефективності виявлення кіберзагроз і реагування на інциденти [7]. У статті M. Nkambule, J.J. Vuuren та L. Leenen розглядалось питання кібербезпеки африканських закладів освіти. Для цього автори застосували модифікований загальний морфологічний аналіз (MGMA) для виокремлення головних елементів адаптивної структури кібербезпеки з урахуванням специфіки африканської системи вищої освіти [8]. Інші науковці S. Watini, G. Davies та N. Andersen розглядали актуальні проблеми кібербезпеки в освітніх інформаційних системах і цифрових навчальних платформах, з акцентом на захисті конфіденційної інформації та забезпеченні приватності користувачів [9]. У дослідженні A. Kakembo аналізується ландшафт кіберзагроз, важливість захисту конфіденційних даних та правові норми, що регулюють конфіденційність інформації [10].

Отже, незважаючи на достатньо велику та ґрунтовну кількість досліджень стосовно кібербезпеки в освіті, недостатньо вивченим залишається питання, які гальмують розвиток кібербезпеки закладів освіти, які і потребують подальших розвідок.

Метою дослідження є висвітлення основних проблем кібербезпеки в закладах освіти і пошуку ефективних шляхів їх розв'язання. Відповідно до поставленої мети дослідницькі завдання зведено, до наступних:

1. Класифікувати види кіберзлочинів в системі освіті.
2. Визначити основні проблеми, які гальмують впровадження кібербезпеки в заклади освіти.
3. Сформувати напрями розв'язання проблем кібербезпеки в закладах освіти.

Виклад основного матеріалу. Сучасні науковці [8-10] вважають, що інформаційна безпека в освіті включає три складові: конфіденційність – захист конфіденційної інформації учнів, студентів і викладачів від несанкціонованого доступу; цілісність – захист точності й повноти інформації і програмного забезпечення освітнього процесу; доступність – забезпечення доступності інформації для пізнавального процесу, а також основних інформаційних, бібліотечних і інших послуг для користувача.

Разом із розширенням цифрового освітнього середовища, питання забезпечення цих принципів (конфіденційності, цілісності й доступності інформаційних ресурсів) набуває дедалі суперечливішого характеру.

З одного боку, базові принципи інформаційної безпеки чітко артикульовані в сучасних дослідженнях, з іншого – практика їх застосування в українських закладах освіти демонструє значні диспропорції. Висновки на кшталт тих, що містяться у звіті «ENISA Threat Landscape 2024» [11], що освітні установи стають дедалі привабливішими цілями для кіберзлочинців через наявність великих обсягів персональних даних і обмежені ресурси для забезпечення належного рівня захисту. Цей факт дозволяє висунути обґрунтовану гіпотезу, що освітні заклади сприймаються зловмисниками як «м'яка ціль» – з огляду на поєднання слабких технічних бар'єрів і наявності великих обсягів персональних даних. Отже, можемо зробити висновок, що специфічне поєднання зростаючої цифрової залежності, фрагментованості захисних систем і нестачі кваліфікованих кадрів закономірно призводить до зростання частоти атак на освітній сектор.

З метою розуміння того, чому саме освітні заклади так часто стають об'єктами кібератак, варто відійти від суто технічних понять. Адже цифрові загрози – це не тільки про шкідливе програмне забезпечення чи невидимих хакерів. Один необачно відкритий лист, випадковий клік на сумнівне посилання – і система вже вразлива. Адміністрація надсилає повідомлення, викладачі готують матеріали, студенти працюють з онлайн-курсами, батьки перевіряють оцінки – і всі ці дії відбуваються через цифрові платформи. І кожна з цих точок взаємодії може бути використана зловмисниками.

У контексті наведених фактів постає необхідність більш системного бачення того, які саме типи кіберзагроз є найбільш релевантними для сфери освіти. Наявні дані дають підстави припустити, що загрози мають різну природу та цільову спрямованість, що вимагає їх чіткої класифікації. З цією метою доцільно структурувати основні види кіберзлочинів, характерних для освітніх установ (табл. 1).

Отже, аналіз наведених типів кіберзлочинів дозволяє констатувати, що проблема кібербезпеки в освітньому середовищі не зводиться до технічних ризиків у вузькому сенсі. Набагато істотнішою є інституційна нездатність передбачати

Таблиця 1

Види кіберзлочинів в закладах освіти

№	Вид кіберзлочину	Опис	Можливі наслідки
1	Фішинг і соціальна інженерія	Маніпуляції для отримання конфіденційної інформації через електронні листи або інші засоби обману.	Викрадення логінів, паролів, персональних даних, фінансові втрати, шахрайство.
2	Програми-вимагачі (Ransomware)	Вірусні програми, які блокують доступ до даних або системи та вимагають викуп за відновлення.	Втрата або шифрування важливих даних, фінансові втрати, зупинка навчального процесу.
3	Атаки типу «відмова в обслуговуванні» (DDoS)	Перенавантаження серверів або систем з метою їх блокування шляхом масованих запитів.	Зупинка роботи освітніх платформ, неможливість доступу до навчальних ресурсів, шкода репутації.
4	Крадіжка особистих і академічних даних	Незаконний доступ до персональних даних студентів, викладачів або академічних результатів.	Втрата персональної інформації, порушення академічної доброчесності, шахрайство, репутаційні втрати.
5	Кібербулінг та онлайн-харассмент	Переслідування або знущання через інтернет або соціальні медіа.	Психологічні травми, зниження успішності, соціальна ізоляція учнів і студентів.
6	Неправомірний контент і його поширення	Поширення забороненого контенту, такого як порнографія, насильство, екстремізм тощо.	Порушення законодавства, шкода репутації навчальних закладів, юридичні наслідки.

Джерело: власна розробка автора.

комбіновані атаки, що поєднують технічні й психологічні методи впливу. Особливо тривожним є те, що значна частина загроз – фішинг, крадіжка даних, поширення неправомірного контенту – безпосередньо експлуатує вразливості самих користувачів, а не недоліки систем безпеки як такі.

Варто наголосити, що учні й студенти часто ігнорують базові правила безпеки. Саме тому питання цифрової обізнаності, усвідомленої поведінки в мережі й інформаційної культури стає таким же важливим, як і наявність сучасного антивірусу.

В наступній табл. 2 автором представлено узагальнення реальних типів кіберзлочинів, з якими може зіткнутись будь-яка освітня установа, а також можливі наслідки та практичні шляхи їх подолання.

Аналіз наведених у таблиці 2 проблем свідчить: уразливість українських закладів освіти в контексті кібербезпеки формується не лише через брак фінансування або технологічну застарілість, як зазвичай вважають. Структурна вада полягає у відсутності взаємопов'язаного підходу, де інституційна готовність, кадрова спроможність і технічні засоби мали би діяти як єдиний механізм, але фактично розвиваються окремо, фрагментарно і без взаємної підтримки. Особливо гострим питанням виглядає прихований лаг між формальним наявністю стратегії та її реальним застосуванням у середовищі закладів освіти: нормативні документи створюються, але не проникають у практичну середу функціонування установ. Так само проблема кадрового дефіциту не обмежується нестачею ІТ-фахівців як таких; йдеться, радше, про відсутність профільних компетенцій навіть серед наявного персоналу, що унеможливлює розбудову внутрішніх систем швидкого реагування.

Таблиця 2

Основні проблеми впровадження кібербезпеки в заклади освіти України

№	Напрями проблем	Ідентифікація проблеми	Стратегічні наслідки та ризики
1	2	3	4
1	Інституційна неготовність	Відсутність формалізованих політик реагування на кіберінциденти – у проєкті Стратегії кібербезпеки України (2021–2025 роки) зазначено, що реалізація попередньої стратегії була ускладнена відсутністю цілісного бачення розвитку спроможностей основних суб'єктів національної системи кібербезпеки та недостатнім залученням освітніх установ до поширення кіберграмотності [12].	Підвищена вразливість до складних атак; обмежена здатність до швидкого реагування та відновлення після інцидентів.
2	Дефіцит кваліфікованих кадрів	Відсутність штатних ІТ-фахівців у закладах освіти; обмежене залучення зовнішніх експертів.	Зниження ефективності впровадження заходів кібербезпеки; підвищений ризик помилок через недостатню експертизу.

Продовження таблиці 2

1	2	3	4
3	Недостатнє фінансування	Обмежені бюджети на оновлення інфраструктури та впровадження сучасних засобів захисту.	Неможливість впровадження необхідних заходів безпеки; підвищений ризик успішних атак.
4	Низький рівень цифрової культури	Недостатній рівень обізнаності щодо кіберзагроз серед персоналу і студентів; обмежене проведення тренінгів та навчань.	Підвищена ймовірність успішних фішингових атак і інших соціотехнічних методів впливу.
5	Технічна вразливість інфраструктури	Використання застарілого програмного забезпечення; відсутність регулярного оновлення систем безпеки.	Підвищений ризик експлуатації відомих вразливостей; можливість компрометації систем.
6	Відсутність системного підходу	Фрагментованість заходів кібербезпеки; відсутність інтегрованої стратегії захисту.	Неможливість ефективного управління ризиками; підвищена ймовірність неузгоджених дій при інцидентах.

Джерело: власна розробка автора.

На цьому тлі цифрова культура виглядає скоріше як риторичне поняття, ніж реальний інструмент запобігання загрозам. Системна ж фрагментарність заходів остаточно перетворює заклади освіти на мішень для атак з непередбачуваними довгостроковими наслідками, починаючи від втрати репутації й закінчуючи паралічем освітнього процесу на локальному або навіть регіональному рівні.

Отже, системна вразливість освітніх установ, виявлена у процесі аналізу, свідчить: розв'язання проблем кібербезпеки потребує не стільки фрагментарних заходів, скільки цілісної перебудови управлінських, технічних і культурних основ функціонування закладів освіти.

Відповідно, наступним кроком є визначення ключових напрямів стратегічного реагування, що здатні забезпечити реальне підвищення стійкості освітнього середовища до кіберзагроз.

Необхідну увагу слід приділяти безпеці особистості того, хто навчається, зокрема перешкоджати витоку інформації, що стосуються питань вступу, передавання та оброблення навчальної та особистої інформації тощо.

Крім серйозних технічних робіт необхідно організувати якісні організаційні заходи щодо захисту інформації. Це передбачає складання регламентів про роботу з локальною мережею, Інтернетом, кожною інформаційною системою безпеки тощо. При цьому в регламентах необхідно описувати порядок дій, конкретні заборони і відповідальних посадових осіб установи, які відповідають за його інформаційну безпеку. На сьогоднішній день українське законодавство не містить прямої вимоги для освітніх закладів щодо обов'язкової розробки і впровадження регламенту реагування на кіберінциденти. Закон України «Про основні засади забезпечення кібербезпеки України» [13] та нещодавній Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів…» 27.03.2025 року [14] встановлюють обов'язки в цій сфері переважно для органів державної влади, об'єктів критичної інформаційної

інфраструктури і власників державних інформаційних ресурсів. Проте в умовах цифровізації освітнього процесу, гібридних форм навчання й зростання кіберзагроз, наявність такого документа перетворюється з формальної ініціативи на практичну необхідність для збереження безперервності освітнього процесу.

Серйозно підійти до питання забезпечення надійного захисту цифрових систем, що використовуються закладами освіти. Якщо великим школам і університетам під силу виділити достатні бюджети для закупівлі корпоративного програмного забезпечення і для найму фахівців з кібербезпеки, то невеликі заклади освіти часто не можуть собі цього дозволити. Як результат, вони нерідко приходять до використання захисного програмного забезпечення, призначеного для домашніх користувачів. Однак це не найкращий вибір: такі продукти не розраховані на централізоване адміністрування, тому їхнє встановлення на шкільні та університетські комп'ютери, а особливо подальше управління захистом, можуть перетворитися на велику проблему.

Правильним розв'язанням завдання для невеликих закладів освіти може стати використання захисних продуктів, розроблених для малого та середнього бізнесу. З одного боку, таке захисне програмне забезпечення пропонує всі найважливіші функції, які необхідні для базової безпеки: надійний захист від шифрувальників-здирників та інших шкідливих програм; автоматичне резервне копіювання; захист облікових записів за допомогою менеджера паролів; перевірку на наявність вразливостей і багато іншого. З іншого боку, рішення легко розгорнути на комп'ютерах, і воно працює за принципом «встановив і забув» – для налаштування та управління не потрібен виділений IT-фахівець.

Для посилення кібербезпеки в закладах освіти рекомендується проводити для працівників тренінги, які підвищують їхню обізнаність про кіберзагрози.

Red Teaming. Подібно до протипожежних навчань, які є нормою в будь-якій установі, дуже важливо періодично проводити інсценування реальної кібератаки у звичайні навчальні години.

Звичайно, жоден із запропонованих заходів не може миттєво вирішити усі проблеми. Але разом вони утворюють міцну основу, з якої можна почати. Це не про одномоментне рішення – це про формування цілісного підходу, де технічний захист, грамотна організація роботи, чітке регламентування дій і підвищення обізнаності всіх учасників освітнього процесу працюють як єдина система.

Висновки. Отже, підсумовуючи дослідження, можна сказати, що кібербезпека в освіті – це вкрай важливе питання, яке потребує суттєвої уваги. Проаналізувавши основні проблеми, можна зробити висновок, що закладам освіти необхідно регулярно оновлювати системи захисту від кібератак. Важливим фактором залишається обізнаність викладачів та їх недостатня цифрова грамотність. Адже недотримання техніки безпеки з використання цифрових технологій – це потенційна загроза, яку не в змозі зупинити жодний антивірус. Слід зауважити, що розв'язати ці проблеми цілком реально. Частину рішень можна впровадити вже зараз. По-перше – це регулярне навчання персоналу, оновлення техніки, прості правила цифрової гігієни для учнів і студентів. Частина заходів потребує більше часу – розробка політик, створення єдиної стратегії на рівні закладу або навіть країни, регламенти реагування.

Цифрове середовище змінюється швидко, і освітні заклади мають змінюватися разом з ним. Інакше заклади освіти ризикують втратити не лише дані, а й довіру – учнів, батьків, суспільства загалом. Тож головним завданням для закладів освіти залишається: зробити кібербезпеку частиною культури свого освітнього закладу, це має бути не тимчасовим проєктом, а щоденною практикою.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. UK Government. Cyber security breaches survey 2023: education institutions annex. 2023. URL: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex (дата звернення: 11.04.2025).

2. Mascellino A. Exploitation accounts for 29% of education sector attacks. *Infosecurity Magazine*. 2023. URL: https://www.infosecurity-magazine.com/news/exploitation-29-education-sector/ (дата звернення: 11.04.2025).

3. Доценко С. О. Кібербезпека учасників освітнього процесу в умовах дистанційного навчання. *Психолого-педагогічні проблеми вищої і середньої освіти в умовах сучасних викликів: теорія і практика : матеріали VII Міжнародної науково-практичної конференції*, 16–18 березня 2023 р. Харків, 2023. С. 207–209. URL: https://dspace.hnpu.edu.ua/handle/123456789/11649 (дата звернення: 11.04.2025).

4. Карабін О.Й., Шуль М.В. Формування цифрових компетентностей здобувачів освіти в контексті нової української школи. *Інноваційна педагогіка.* 2020. №29(1). С. 140-144. DOI: https://doi.org/10.32843/2663-6085/2020/29-1.28.

5. Арсенович Л.А. Інструментарій підвищення рівня цифрової компетентності фахівців із кібербезпеки в освітньому процесі. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка».* 2022. № 3(15). С. 93–109. DOI: https://doi.org/10.28925/2663-4023.2022.15.93109

6. Бєляєва Н., Зацерковна О., Ребрина М. Проєктування безпечного освітнього середовища в умовах реформування нової української школи. *Грааль науки*. 2023. № 30. С. 288–292. DOI: http://dx.doi.org/10.36074/grail-of-science.04.08.2023.046

7. Wada I., Izibili G.O., Babayemi T., Abdulkareem A. AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews.* 2025. №25(3). P. 2233-2245. DOI: http://dx.doi.org/10.30574/wjarr.2025.25.3.0989

8. Nkambule M., Vuurenj J. J., Leenen L. Creating a cybersecurity culture framework in higher education. *Proceedings of the 20th International Conference on Cyber Warfare and Security.* 2025. №20(1). P. 304–312. DOI: https://doi.org/10.34190/iccws.20.1.3268

9. Watini, S., Davies, G., Andersen, N. Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. *International Transactions on Education Technology*. 2024. № 3(1). P. 26–35. DOI: http://dx.doi.org/10.33050/itee.v3i1.665

10. Kakembo A. Cybersecurity in Educational Institutions: Management Strategies. *Eurasian Experiment Journal of Humanities and Social Sciences.* 2025. № 6(2). P. 51–56.

11. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024: July 2023 to June 2024. 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 11.04.2025).

12. Рада національної безпеки і оборони України. Проєкт. Стратегії кібербезпеки України (2021–2025 роки). 2021. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 11.04.2025).

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради*, 2017, № 45, С. 403.

14. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-IX#Text (дата звернення: 11.04.2025).

REFERENCES:

1. UK Government. (2023). Cyber security breaches survey 2023: education institutions annex. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023-education-institutions-annex

2. Mascellino, A. (2023). Exploitation accounts for 29% of education sector attacks. *Infosecurity Magazine*. Retrieved from https://www.infosecurity-magazine.com/news/exploitation-29-education-sector/

3. Dotsenko, S.O. (2023). Kiberbezpeka uchasnykiv osvitnoho protsesu v umovakh dystantsiynoho navchannia [Cybersecurity of participants in the educational process under distance learning conditions]. *Psykholoho-pedahohichni problemy vyshchoi i serednoi osvity v umovakh suchasnykh vyklykiv: teoriia i praktyka: materialy VII Mizhnarodnoi naukovo-praktychnoi konferentsii* (16–18 March 2023, Kharkiv) (pp. 207–209). Retrieved from https://dspace.hnpu.edu.ua/handle/123456789/11649 [in Ukrainian].

4. Karabin, O.Y., Shul, M.V. (2020). Formuvannia tsyfrovykh kompetentnostei zdobuvachiv osvity v konteksti novoi ukrainskoi shkoly [Formation of digital competencies of education seekers in the context of the New Ukrainian School]. *Innovatsiina pedahohika, 29*(1), 140–144. https://doi.org/10.32843/2663-6085/2020/29-1.28 [in Ukrainian].

5. Arsenovych, L.A. (2022). Instrumentarii pidvyshchennia rivnia tsyfrovoi kompetentnosti fakhivtsiv iz kiberbezpeky v osvitnomu protsesi [Tools for enhancing the digital competence of cybersecurity specialists in the educational process]. *Kiberbezpeka: osvita, nauka, tekhnika, 3*(15), 93–109. https://doi.org/10.28925/2663-4023.2022.15.93109 [in Ukrainian].

6. Bieliaeva, N., Zatserkovna, O., Rebryna, M. (2023). Proiektuvannia bezpechnoho osvitnoho seredovyshcha v umovakh reformuvannia novoi ukrainskoi shkoly [Designing a safe educational environment under the reform of the New Ukrainian School]. *Hraal nauky, 30*, 288–292. http://dx.doi.org/10.36074/grail-of-science.04.08.2023.046 [in Ukrainian].

7. Wada, I., Izibili, G.O., Babayemi, T., Abdulkareem, A. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews, 25*(3), 2233–2245. http://dx.doi.org/10.30574/wjarr.2025.25.3.0989

8. Nkambule, M., Vuuren, J.J., Leenen, L. (2025). *Creating a cybersecurity culture framework in higher education*. *Proceedings of the 20th International Conference on Cyber Warfare and Security, 20*(1), 304-312. https://doi.org/10.34190/iccws.20.1.3268

9. Watini, S., Davies, G., Andersen, N. (2024). Cybersecurity in learning systems: Data protection and privacy in educational information systems and digital learning environments. *International Transactions on Education Technology, 3*(1), 26–35. http://dx.doi.org/10.33050/itee.v3i1.665

10. Kakembo, A. (2025). Cybersecurity in educational institutions: Management strategies. *Eurasian Experiment Journal of Humanities and Social Sciences, 6*(2), 51–56.

11. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024: July 2023 to June 2024. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

12. Rada Natsionalnoi Bezpeky i Oborony Ukrainy. (2021). *Proiekt Stratehii kiberbezpeky Ukrainy (2021–2025 roky) [Draft Cybersecurity Strategy of Ukraine (2021–2025)]*. Retrieved from https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf [in Ukrainian].

13. Verkhovna Rada Ukrainy. (2017). Zakon Ukrainy vid 05.10.2017 № 2163-VIII Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [Law of Ukraine № 2163-VIII On the basic principles of cybersecurity in Ukraine]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

14. Verkhovna Rada Ukrainy. (2025). Zakon Ukrainy vid 27.03.2025 № 4336-IX Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv [Law of Ukraine № 4336-IX On amendments to laws regarding information and cybersecurity protection of public information resources]. Retrieved from https://zakon.rada.gov.ua/laws/show/4336-IX#Text [in Ukrainian].