Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 9.

DOI: http://doi.org/10.32702/2307-2105.2025.9.29

УДК 005.334:378:004.738.5

Д. М. Загірняк,

д. е. н., професор, завідувач кафедри обліку і фінансів,

Кременчуцький національний університет імені Михайла Остроградського

ORCID ID: https://orcid.org/0000-0002-7009-8635

І. В. Ховрак,

аспірант,

Кременчуцький національний університет імені Михайла Остроградського

ORCID ID: https://orcid.org/0000-0001-6211-6437

АДАПТИВНИЙ РИЗИК-МЕНЕДЖМЕНТ У СТРАТЕГІЧНОМУ РОЗВИТКУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОГО СЕРЕДОВИЩА ЗАКЛАДІВ ВИЩОЇ ОСВІТИ

D. Zagirniak,

Doctor of Economic Sciences, Professor, Head of the Department of Accounting and Finance, Kremenchuk Mykhailo Ostrohradskyi National University

I. Khovrak,

Postgraduate student, Kremenchuk Mykhailo Ostrohradskyi National University

ADAPTIVE RISK MANAGEMENT IN THE STRATEGIC DEVELOPMENT OF THE INFORMATION AND COMMUNICATION ENVIRONMENT OF HIGHER EDUCATION INSTITUTIONS

У статті запропоновано концепцію адаптивного ризик-менеджменту для стратегічного розвитку інформаційно-комунікаційного середовища закладів вищої освіти в умовах тривалої невизначеності та воєнних загроз. На відміну від фрагментарних підходів, зосереджених на окремих аспектах кібербезпеки або безперервності надання послуг, запропонований підхід інтегрує врядування ризиками та засади сталого управління в замкнений управлінський цикл «відчувати, інтерпретувати, вирішувати, діяти, навчатися». Методичну основу формують багатокритеріальне оцінювання, сценарне та стрес-моделювання, моніторинг випереджувальних сигналів і принципи прийняття рішень за умов глибокої невизначеності. Результати дослідження включають: таксономію зовнішніх і внутрішніх ризиків ІК-середовища ЗВО; узгоджену систему KRI/KPI стійкості; п'ятимодульну архітектуру аналітико-керуючої системи (реєстр ризиків; оцінювання; раннє попередження; адаптивне планування та реагування; моніторинг і навчання). В статті також надано набір адаптивних механізмів, релевантних українським ЗВО у воєнний час. Наукова новизна полягає у формалізації інтегрованої системи управління ІК-ризиками, що поєднує ризик-менеджмент і сталий менеджмент та забезпечує адаптивне реагування на пролонговану нестабільність. Запропонована поетапна модель впровадження забезпечує швидкий запуск пілоту, подальше масштабування та регулярний аудит ефективності, що безпосередньо підвищує безперервність і якість сервісів ЗВО.

This article substantiates a conceptual model of adaptive risk management in the strategic development of the information and communication environment of higher education institutions under conditions of protracted uncertainty and wartime challenges. Unlike fragmented approaches that typically emphasise narrow aspects of cybersecurity or the continuity of services, the proposed model integrates risk governance with the principles of sustainability and institutional resilience within a closed managerial cycle comprising the following stages: sense, interpret, decide, act, learn. The methodological framework draws on multi-criteria assessment, scenario and stress analysis, the monitoring of leading

indicators through key risk indicators (KRIs), as well as robust decision-making techniques designed for contexts of deep uncertainty. The research results include: the development of a taxonomy of external and internal IC-environment risks for higher education institutions; the construction of a coherent system of resilience-oriented KRIs and key performance indicators (KPIs); the design of a five-module architecture for an integrated analytics and control system consisting of a risk register, comprehensive assessment tools, an early warning module, adaptive planning and response mechanisms, and a monitoring and learning module. In addition, the study identifies a set of adaptive mechanisms that are particularly relevant to Ukrainian higher education institutions operating during wartime. These mechanisms involve managed service degradation, the use of offline packages, multi-channel notification systems, autonomous power supply, structured management of «bring your own device» practices, regular emergency drills, geo-redundancy of critical resources, and inter-university mutual support arrangements. The originality of the research lies in the formalisation of an integrated IC-risk management system that combines the logic of risk management with the principles of sustainable management while enabling adaptive responses to persistent instability. The practical significance is demonstrated through a phased implementation pathway consisting of pilot introduction, further scaling, and independent auditing, which collectively ensure measurable improvements in service continuity, reliability, and overall quality within the information and communication environment of higher education institutions. This provides a scientifically grounded and practically relevant foundation for the long-term strengthening of institutional resilience in higher education at both the national and international levels.

Ключові слова: *ризик-менеджмент; інформаційно-комунікаційне середовище; заклади вищої освіти; інституційна резилієнтність; стале управління; KRI; KPI; адаптивність.*

Keywords: *risk management; information and communication environment; higher education institutions; institutional resilience; sustainability management; key risk indicators (KRI); key performance indicators (KPI); adaptability.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Сучасні заклади вищої освіти (ЗВО) все більшою мірою залежать від інформаційно-комунікаційного середовища (ІК-середовища) для реалізації освітніх програм, наукових досліджень, трансферу технологій, управління даними та процесами, взаємодії з партнерами та виконання «третьої місії». При цьому, ІК-середовище поєднує навчальні платформи, репозитарії та сховища даних, хмарні ресурси, управлінські інформаційні системи, засоби комунікації, а також сервіси підтримки здобувачів і персоналу. Варто наголосити, що в контексті цифрової трансформації саме ІК-середовище здатне забезпечити масштабованість освітніх форматів та наукових процесів, мобільність учасників, прозорість управлінських процедур, відкритість наукових результатів та включеність ЗВО у світовий простір вищої освіти.

Водночас портфель ризиків істотно розширився й виходить за межі вузько зрозумілої кібербезпеки [18]. Йдеться про пошкодження критичної інфраструктури, загрози захисту даних, залежність від безперебійної роботи хмарних провайдерів, платформ та зовнішніх підрядників, регуляторні та репутаційні ризики, а також відсутність культури безпеки. У воєнних реаліях України ці ризики посилюються фізичними руйнуваннями інфраструктури, блекаутами, міграцією здобувачів і персоналу, кібератаками, а також високою невизначеністю планування. Наслідки проявляються у перериванні навчання та досліджень, затримках виконання проектів і трансферу технологій, стратах даних і зниженні довіри стейкхолдерів. Дослідження демонструють зростання вразливості ЗВО до комплексних ризиків та обґрунтовують потребу в системних підходах до їх мінімізації [31]. Отже, забезпечення безперервності та безпеки ІК-середовища має розглядатися як один із пріоритетів першого порядку для ЗВО.

Існуючі дослідження та практики протидії ризикам ІК-середовища ЗВО часто є фрагментованими, зокрема, сфокусованими на кібербезпеці та технічних засобах захисту чи дбаючими про забезпечення безперервності навчального процесу. Такий підхід не враховує взаємозалежності різних типів ризиків і необхідність балансування між стратегічними цілями

(безпека, доступність та якість). Водночас, досвід українських ЗВО під час війни демонструє необхідність оперативно впроваджувати такі нетипові заходи як резервні канали зв'язку, автономні джерела живлення та релокацію серверів задля підтримки роботи цифрових сервісів [11]. Тому традиційних планів реагування на надзвичайні ситуації недостатньо, необхідною є проактивна та адаптивна система ризик-менеджменту, яка здатний гнучко реагувати на зміни обставин та об'єднає моніторинг ризиків, їх оцінку, раннє попередження та адаптивне планування дій.

Дослідження доводять, що ризик-менеджмент здатний стати запорукою організаційної стійкості, адже ЗВО з комплексними системами управління ризиками краще пережили кризу COVID-19, мінімізувавши перерви у власній діяльності [27]. Дослідники підкреслюють необхідність інтеграції управління ризиками у стратегію ЗВО, щоб забезпечити стійкість та сталість ІК-середовища. Відтак постає науково-практична задача формування системи адаптивного ризик-менеджменту ІК-середовища ЗВО, здатної функціонувати за умов тривалої невизначеності та воєнних загроз. Саме тому стаття пропонує концептуальне обґрунтування, методичний інструментарій і управлінську логіку застосування даного адаптивного підходу.

Аналіз останніх досліджень і публікацій. Теорія та практика управління ризиками в просторі вищої освіти розвиваються на перетині інформаційної безпеки, менеджменту організацій, сталого розвитку та управління в умовах невизначеності. У дослідженнях також з'являється концепція освітньої резилієнтності, що відображає здатність ЗВО і здобувачів вищої освіти адаптуватися до сучасних потрясінь [4; 27; 29]. Ризик-менеджмент визначено як ключовий компонент цієї резилієнтності, оскільки дозволяє ідентифікувати та пом'якшувати фактори дестабілізації навчання. При цьому впровадження культури ризик-менеджменту та підвищення цифрової грамотності здобувачів освіти здатні підсилити їхню стійкість до стресів, а також сприяють кращим навчальним результатам [27]. Це узгоджується з результатами дослідження процесів забезпечення академічної безперервності та розвитку резилієнтності ЗВО на основі розвитку можливості передбачення, подолання труднощів та адаптації [29], а

також здатності діяти на основі отриманого досвіду [4]. Відповідно, дослідження підтверджують як здатність ЗВО справлятися з неочікуваними викликами, так і наявність потенціалу резилієнтності ЗВО [4]. Варто також додати, що висновки галузевих оглядів EDUCAUSE [12] також наголошують на пріоритеті цілісного ризик-планування та адаптивних стратегій для стійкості ЗВО. Таким чином, інтеграція ризик-менеджменту в стратегію розвитку ЗВО розглядається як необхідна передумова їхньої життєздатності у довгостроковій перспективі.

Відповідно до Міжнародної ради з врядування ризиками та О. Ренна [15; 26], управління ризиками передбачає участь вищого керівництва, багатостороннє залучення стейкхолдерів і системне розуміння ризиків, що поєднує наукові, економічні, соціокультурні та комунікаційні виміри. Для ЗВО перехід до управління ризиками означає відмову від розрізнених локальних практик на користь адаптивного управління ризиками на рівні закладу, яке надає керівництву цілісний огляд взаємопов'язаних загроз і сприяє прийняттю узгоджених стратегій мінімізації ризиків [6; 31]. В українському контексті потреба в такому підході посилюється множинністю викликів воєнного часу. Водночас, міжнародні дослідження наголошують, що вища освіта відіграє ключову роль у відновленні конфліктно уражених суспільств [22], а українські кейси демонструють успішну інституційну адаптацію до тривалої нестабільності та збереження безперервності освітніх послуг [11].

Управління ризиками за умов тривалої невизначеності потребує рішень, адаптивних до широкого діапазону можливих майбутніх станів, а не спираються виключно на найімовірніший сценарій. Саме цю логіку втілює підхід «robust decision-making», що поєднує експлоративне моделювання, виявлення вразливостей стратегій та ітераційний цикл адаптації на основі аналізу [20; 21]. Це дозволяє ранжувати альтернативи з огляду на стабільність ключових показників в умовах варіативності сценаріїв, а також цілеспрямовано враховувати тривалу невизначеність, при якій параметри системи, їхні ймовірності та взаємозв'язки не є відомими чи узгодженими між стейкхолдерами. Зазначений підхід надзвичайно релевантний для

українських ЗВО у період повномасштабної війни, де варіативними є тривалість і частота блекаутів, інтенсивність кібератак, стабільність постачальників та регуляторні зміни. Застосування такого підходу дозволяє зберігати мінімально прийнятний рівень результативності для більшості правдоподібних сценаріїв.

Важливий напрям сучасної практики ризик-менеджменту є також раннє виявлення ризиків на основі ключових індикаторів ризику (KRI) [16]. На відміну від ключових показників ефективності (KPI), що фіксують досягнення цілей постфактум, KRI виконують роль випереджувальних сигналів про зростання вразливості системи та дозволяють ініціювати превентивні дії. Така концепція раннього попередження апробована емпірично й для простору вищої освіти, зокрема, ЗВО застосовують ранні сигнали для прогнозування відрахувань та академічних ризиків [3; 5; 10]. Це підтверджує можливості застосування KRI-моніторингу для ІК-середовища ЗВО. При цьому, типовими KRI можуть бути зростання частоти дрібних інцидентів, зростання середньої тривалості відновлення роботи сервісів або аномалії навантаження систем, що є ранніми сигналами ймовірного наближення системних збоїв й дозволяють запускати заздалегідь визначені превентивні сценарії реагування. Відповідно, це дає змогу оперативно коригувати ймовірності настання подій у міру надходження нових даних та підтримувати адаптивну систему раннього попередження.

Дослідження з управління ризиками у вищій освіті все частіше пов’язують ризик-менеджмент зі сталим менеджментом і реалізацією Цілей сталого розвитку. Для ЗВО це означає враховувати не лише короткострокові загрози, а й довготривалі соціальні, екологічні та операційні ризики, що впливають на місію, репутацію ЗВО та довіру стейкхолдерів. Саме тому відбувається поєднання ризик-менеджменту з політиками сталості ЗВО. При цьому цифрова трансформація підтримує «зелені» операції та інклюзивність, а системи показників і процедур управління забезпечують проактивне врахування екологічних, соціальних і операційних ризиків [1; 7; 30]. Акцент зміщується від реактивного відновлення після кризи до проактивного підвищення стійкості ЗВО на основі здатності навчатися на пережитих

загрозах, дієвих практик управління й участі стейкхолдерів, а також інституційній резилієнтності [23; 28]. У контексті війни та післявоєнного відновлення України це набуває особливої ваги. Дослідження підтверджують, що ЗВО можуть стати каталізатором відновлення держави за умови, що вони будуть достатньо життєздатними та стійкими [17; 25; 32]. Відповідно, адаптивний ризик-менеджмент у стратегічному розвитку ІК-середовища ЗВО має ґрунтуватися як на найкращих практиках управління ризиками, так і на засадах сталого менеджменту та розвитку потенціалу резилієнтності. Отже, аналіз останніх досліджень та публікацій вказує на потребу в новій концепції управління ризиками для ЗВО.

Формулювання цілей статті (постановка завдання). Мета дослідження полягає в обґрунтуванні концептуальної моделі адаптивного ризик-менеджменту для стратегічного розвитку ІК-середовища ЗВО в умовах тривалої нестабільності, що інтегрує управління ризиками та стале управління. Дослідження має комплексний, міждисциплінарний характер і спирається на рецензовані публікації з управління ризиками, кібербезпеки, резилієнтності та безперервності освіти, доповнені аналітичними звітами, кейсами та чинними нормативами. Така тріангуляція джерел забезпечила емпіричну верифікацію результатів дослідження та дозволила точно врахувати контекст функціонування українських ЗВО.

Виклад основного матеріалу дослідження. Проведене дослідження дозволило сформувати таксономія ризиків ІК-середовища ЗВО. Вона включає дві основні категорії зовнішніх та внутрішніх ризиків, які поділяються на низку підкатегорій (таблиця 1). Такий підхід відображає як тенденції кіберзагроз, так і управлінські й технологічні прогалини ЗВО. Важливо додати, що наявні в Україні воєнні загрози та енергетична нестабільність призводять до виділення частини ризиків ІК-середовища у площину фізичної інфраструктури (живлення, зв’язок, релокація серверів та даних, альтернативні канали). Важливо підкреслити, що ризики різних підкатегорій можуть проявлятися одночасно та взаємно посилювати один одного. Тому адаптивний ризик-менеджмент має враховувати можливість

комбінованих сценаріїв та передбачати заходи, здатні охоплювати декілька різних ризиків одразу.

Таблиця 1. Таксономія ризиків ІК-середовища ЗВО

Категорія	Підкатегорія	Опис: сутність і типові прояви у ЗВО
Зовнішні	Кіберзагрози: цілеспрямовані	Програми-вимагачі, атаки відмови в обслуговуванні, цільовий фішинг на поштові скриньки ЗВО, платформи дистанційного навчання, системи єдиного входу та наукові репозитарії; переривання доступу та компрометація даних.
	Кіберзагрози: масові	Масові фішингові розсилки, експлуатація відомих вразливостей у сервісах, «перебір» паролів, поширення шкідливого програмного забезпечення; вплив на великі групи користувачів.
	Ризики ланцюга постачання	Компрометація або відмова хмарних провайдерів, сервісів відеоконференцій, освітніх платформ чи інтегрованих онлайн-послуг; непрямі витоки та простої через інциденти у партнерів.
	Збої критичної інфраструктури (електроживлення, мережі)	Відключення електроенергії, перебої інтернет-зв’язку/маршрутизації, відмови вузлів дата-центру або каналів провайдерів; зриви занять, наукових заходів та процесів оцінювання, втрата активних сеансів.
	Геополітичні та воєнні загрози (фізична безпека)	Руйнування будівель, необхідність евакуації, ризики для серверних та комунікаційних ліній; потреба в релокації ІТ-ресурсів, автономному живленні та альтернативних каналах зв’язку.
	Регуляторні та комплаєнс-ризики	Невиконання вимог захисту персональних даних і кіберстійкості, порушення порядку повідомлення про інциденти; штрафи, судові претензії, обмеження фінансування.
	Репутаційні ризики	Негативний медійний резонанс від витоків або тривалих збоїв (особливо під час вступної кампанії й акредитацій); зниження довіри абітурієнтів, партнерів і донорів.
	Кліматичні та природні загрози	Повені, спека, шторми, інші екстремальні явища, що викликають відмови обладнання, перебої в живленні чи охолодженні серверних; потреба в територіально рознесеному резервуванні та локальних енергоефективних рішеннях.
Внутрішні ризики	Управління даними та конфіденційність	Неповна інвентаризація даних, слабка сегментація, недостатнє шифрування та резервне копіювання, помилки у налаштуванні доступів; ризик витоків персональних і дослідницьких даних.
	Людський фактор і культура безпеки	Низька цифрова гігієна, нехтування політиками, помилки персоналу й здобувачів (відкриття шкідливих файлів, передавання паролів); потреба в системному навчанні.

Продовження таблиці 1.

Категорія	Підкатегорія	Опис: сутність і типові прояви у ЗВО
	Ідентифікація та керування доступом	Надмірні повноваження, відсутність регулярних переглядів доступів і своєчасного відкликання прав, слабкі налаштування систем єдиного входу та служб керування ідентичностями.
	Архітектурні та технологічні ризики	Застарілі системи, нерегулярне керування оновленнями, різні платформ без належних інтеграцій, брак журналів подій та телеметрії для контролю безпеки.
	Операційна надійність інформаційно-комп'ютерних технологій	Відсутність або нетестованість планів безперервності діяльності та відновлення після збоїв, нерегулярні резервні копії, завищений цільовий час відновлення; тривалі простої освітнього, наукового та управлінського процесів.
	Недосконалість управління ризиками	Розпорошеність відповідальності, відсутність єдиного реєстру ризиків і регулярних оглядів індикаторів; слабка участь керівних органів у прийнятті рішень щодо ризиків.
	Етичні та академічні ризики даних і досліджень	Академічна доброчесність, коректне використання інструментів штучного інтелекту, дотримання принципів відкритої науки та належної анонімізації даних.
	Безпека на місцях та доступність у воєнний час	Наявність укриттів і «пунктів незламності», автономні джерела живлення, резервні канали зв'язку, релокація серверів; узгодження з розкладом і процедурами безпеки.

Джерело: складено автором на основі джерел [2; 7-9; 11-13; 18; 19; 24; 25].

Наведена в таблиці 1 таксономія ризиків дозволяє сформувати робочий реєстр ризиків для ЗВО. Так, для кожної підкатегорії фіксуються: відповідальний (власник ризику); джерело та типова подія; ймовірність і масштаб впливу; реалізовані контрольні заходи та позаплановані вдосконалення; KRI і KPI; цільові орієнтири часу/обсягу відновлення; пов'язані плани безперервності діяльності та плани відновлення після збоїв; пріоритет за критичністю. З урахуванням воєнних умов варто окремо маркувати ризики, що потребують автономного електроживлення, резервних каналів зв'язку та географічного резервування даних і сервісів. Важливо одразу відповідні позиції інтегрувати у навчально-тренувальні сценарії й календар перевірок. Такий спосіб побудови реєстру узгоджується з логікою ISO/IEC 27005 (ідентифікація, аналіз, оцінювання, оброблення, моніторинг)

та рамкою NIST CSF 2.0, а також відповідає рекомендаціям професійних спільнот щодо інституційної резилієнтності у просторі вищої освіти [12; 13; 24]. Для подальшого переходу від описової діагностики ризиків до керованої стійкості ЗВО, пропонуємо двокомпонентну систему індикаторів: KRI як випереджувальні сигнали зростання уразливості та KPI як підсумкові метрики результативності реалізованих заходів (таблиця 2 та 3).

Таблиця 2. Ключові індикатори ризику для ІК-середовища ЗВО

Назва	Опис
Середній час виявлення інциденту	Середній інтервал від фактичного початку інциденту до його фіксації засобами моніторингу; зростання часу означає наявність сліпих зон у виявленні.
Частота дрібних інцидентів за період	Кількість некритичних, але повторюваних збоїв (короткотривалі обмеження доступу, помилки ідентифікації, відмови модулів), що часто передують збоям більшої тривалості.
Частка облікових записів без багатофакторної ідентифікації	Відсоток активних користувачів та адміністраторів без багатофакторної ідентифікації; порогові значення задаються політикою доступу.
Затримка встановлення критичних оновлень	Середній час між виходом критичного оновлення та його встановленням на відповідні системи; перевищення порогів вказує на вразливість системи.
Частка критичних сервісів без актуальних і протестованих планів відновлення	Відсоток визначених як критичні сервісів, що не мають чинних та перевірених планів безперервності діяльності та відновлення після збоїв; випереджувальний ризик затяжних простоїв.
Аномалії навантаження мереж та платформ	Частота та тривалість перевищення порогів пропускної здатності або нехарактерних піків трафіку; індикатор загрози майбутніх відмов.
«Свіжість» резервних копій	Частка резервних копій, що не відповідають цільовій точці відновлення; перевищення порога означає ризик втрати даних.
Частота повідомлень користувачів про фішинг, частка успішних симуляцій	Кількість валідних повідомлень про підозрілі листи та відсоток «провалів» у симульованих фішингових кампаніях.
Порушення зобов’язань постачальників зовнішніх критичних сервісів	Кількість та тривалість інцидентів у провайдерів; випереджає ризик повторних або ескалованих збоїв.
Запас автономного електроживлення та час до вичерпання	Оціночний час роботи критичних вузлів від автономних джерел за типових навантажень.
Частка сервісів без географічного резервування	Відсоток ключових систем без територіально рознесеного дублювання; підвищує вразливість до локальних катастроф та обстрілів.

Джерело: складено автором на основі джерел [12; 16; 14; 18; 33].

Таблиця 3. Ключові показники ефективності для ІК-середовища ЗВО

Назва	Опис
Середній час відновлення після інциденту	Середній інтервал від початку збою до повного відновлення сервісу; базова метрика результативності реагування.
Частка занять, проведених за розкладом у періоди надзвичайних подій	Відсоток навчальних активностей, що відбулися попри блекаути, тривоги та інші інциденти (за місяць, семестр).
Частка критичних сервісів із актуальними та протестованими планами відновлення	Відсоток критичних сервісів із актуальними планами відновлення, що пройшли навчально-тренувальні перевірки за останні 12 міс.
Досягнення цілей під час реальних інцидентів	Частка інцидентів, у яких втрати даних чи час простою були в межах установлених цілей.
Частка систем із увімкненою багатофакторною ідентифікацією	Відсоток сервісів і користувачів, для яких багатофакторною ідентифікацією є обов'язковою та активною.
Середній час закриття критичних уразливостей	Середній інтервал між виявленням і виправленням уразливостей високої (критичної) ваги.
Доступність навчальних платформ і ключових е-сервісів	Частка часу доступності платформ, електронної пошти, е-журналів, репозитаріїв (щомісячно, квартально).
Частка сервісів з географічним резервуванням	Відсоток критичних систем, дубльованих в іншій локації чи регіоні; щорічна перевірка працездатності.
Питома частка підтверджених інцидентів із витоком персональних даних	Кількість підтверджених інцидентів за рік відносно обсягу оброблюваних персональних даних; має прагнути до нуля.
Частка підрозділів, що пройшли навчально-тренувальні сценарії	Відсоток підрозділів, що за рік пройшли симуляційні сценарії реагування; відображає інституціалізацію практик.
Середній час до відновлення занять	Середній інтервал від початку збою до повернення до проведення занять за адаптованим розкладом.

Джерело: складено автором на основі джерел [12; 14; 18; 24].

Запропонована система індикаторів дозволяє поєднати попереджувальне спостереження стану ІК-середовища ЗВО (KRI) та оцінювання досягнутої стійкості (KPI) у єдину управлінську логіку. KRI працюють як радар (зафіксовані порогові значення автоматично ініціюють превентивні дії). KPI, своєю чергою, відображають результат (наскільки швидко й повно університет відновлює сервіси та зберігає безперервність

діяльності ЗВО). Такий підхід відповідає сучасним науковим уявленням про метрики та рекомендаціям профільних інституцій для вищої освіти.

Врахування сучасних рамок та стандартів [12-14; 24] дозволило розробити архітектуру з п’яти взаємопов’язаних модулів, які реалізують повний цикл «відчувати, інтерпретувати, вирішувати, діяти, навчатися» в контексті ІК-середовища ЗВО. Така концептуальна модель дозволяє об’єднати раннє попередження, оцінювання та планування реагування, а також системне навчання на інцидентах із урахуванням українських реалій війни, ризиків ланцюгів постачання і фізичної безпеки інфраструктури (таблиця 4).

Наведена архітектура операціоналізує запропонований підхід до ризик-менеджменту ІК-середовища ЗВО, зокрема діє від єдиного реєстру та динамічного оцінювання до раннього попередження, адаптивного планування й циклу навчання на інцидентах. Вона встановлює чіткі ролі, потоки даних та точки управлінського контролю, забезпечує вимірюваність рішень завдяки KRI/KPI, а також регулярну верифікацію планів безперервності та відновлення. Такий підхід дає змогу не лише швидше реагувати на ризики, а й поступово підвищувати інституційну резилієнтність ЗВО. Здійснена систематизація наявного досвіду українських ЗВО та наукових досліджень дозволила виділити основні адаптивні механізми реагування у воєнний час. Вони дозволяють перетворити аналітику на дії, підвищуючи інституційну резилієнтність:

1) Кероване погіршення функціональності, при якому критичні освітні, наукові та адміністративні сервіси підтримують спрощені режими замість повної зупинки: резервний «легкий» портал, локальні копії навчальних матеріалів у внутрішній мережі, пріоритизація трафіку для базових сервісів, розподілене резервування та переїзд частини сервісів у хмару під час активних бойових дій.

Таблиця 4. Концептуальна архітектура адаптивного ризик-менеджменту для ІК-середовища ЗВО

Модуль	Призначення	Типові вхідні дані	Вихідні дані
Реєстр ризиків	Класифікація ризиків за таксономією: фіксація відповідальних, зв'язок із планами безперервності діяльності та відновлення після збоїв, прив'язка KRI/KPI.	Опис сценаріїв, історія інцидентів, політики, договори з постачальниками, результати аудитів.	Аналітичні звіти та панелі моніторингу, канали обміну даними з модулями оцінювання та планування.
Оцінювання ризиків	Динамічні оцінки та пріоритизація: формування матриці «ймовірність та вплив» ризику, сценарний та стрес-аналіз, «теплові карти» ризиків, оновлення оцінок за поточними даними моніторингу.	Експертні оцінки, статистика інцидентів, KRI, результати тестувань і навчань.	Рейтинги та пріоритети ризиків, карти ризиків, рекомендації для планування.
Раннє попередження	Своєчасне виявлення відхилень і формування попереджувальних сигналів: моніторинг доступності сервісів, аналіз журналів подій, порогові значення та правила, багаторівневі сповіщення.	KRI, журнали систем безпеки, дані про рівні узгоджених послуг з постачальниками, зовнішні попередження.	Сигнали та ризики з пріоритетами, завдання для реагування, повідомлення відповідальним.
Адаптивне планування та реагування	Прийняття та виконання рішень у змінному середовищі: каталог типових сценаріїв і планів дій, вибір альтернатив за принципами стійкого прийняття рішень в умовах невизначеності, автоматизовані дії, інтеграція з розкладом і сповіщеннями.	Сигнали з раннього попередження, пріоритети та рейтинги ризиків, стан інфраструктури, доступність ресурсів.	Команди на виконання, оновлення розкладу, багатоканальні повідомлення для користувачів.
Моніторинг і навчання (цикл удосконалення)	Замкнений цикл «виконали, оцінили, поліпшили»: контроль виконання рішень, післяінцидентний аналіз, планування й облік навчань та симуляцій, коригування політик і планів.	Показники KPI, відгуки користувачів, уроки з інцидентів.	Оновлені плани й регламенти, графік навчань, звіти для керівництва.

Джерело: складено автором на основі джерел [8; 11-14; 18; 20; 24].

2) Для фаз блекаутів і нестабільного зв’язку готуються офлайн-пакети на носіях та у локальних сховищах з альтернативними місцями доступу (укриття/«пункти незламності» з автономним живленням та локальним Wi-Fi).

3) Багатоканальні оповіщення про критичні зміни з підтвердженням доставки, що дублюються електронною поштою, мобільними застосунками та месенджерами. Це дозволяє знизити ризик непоінформованості здобувачів, персоналу та партнерів.

4) Автономне енергозабезпечення критично важливої ІК-інфраструктури завдяки створенню мікромереж в межах кампусу, наприклад із застосуванням сонячних панелей з накопичувачами та керуванням навантаженнями. Також здійснюється забезпечення безперебійного живлення для мережевого та серверного обладнання.

5) Контрольовані ризики та підтримка використання власних пристроїв за умов розосередженості здобувачів та персоналу завдяки багатофакторній ідентифікації, сегментації доступу, керування мобільними пристроями, а також навчання користувачів.

6) Регулярні навчальні тренування та післяінцидентний детальний аналіз як частина циклу удосконалення системи адаптивного ризик-менеджменту для ІК-середовища ЗВО.

7) Узгодження з стратегічною резилієнтністю ЗВО, де акцент робиться на гнучких процесах, резервуванні критичних функцій і використанні даних для прийняття рішень. Для сучасних українських ЗВО це означає прозоре балансування між безпекою, доступністю та якістю. Опорою виступають перевірені практики та кейси ЗВО, а також міжнародні стандарти.

8) Територіально рознесене резервування даних і критичних сервісів завдяки інфраструктурі зовнішніх партнерів, а також угоди взаємної підтримки з іншими ЗВО. Це сприяє тимчасовому хостингу навчальних платформ і репозиторіїв, спільному використанню лабораторій та обладнання, отриманню доступу до каналів зв’язку тощо. У сукупності ці

механізми зменшують ризик, зменшують кількість «вузьких місць» пропускної спроможності й підвищують масштабованість безперервності поза межами локального периметра ЗВО.

Висновки та перспективи подальших розвідок у даному напрямі. Проведене дослідження обґрунтовує концептуальну модель адаптивного ризик-менеджменту для стратегічного розвитку ІК-середовища ЗВО в умовах тривалої нестабільності, що здатна охопити весь портфель зовнішніх та внутрішніх ризиків ІК-середовища, відповідати циклу «відчувати, інтерпретувати, вирішувати, діяти, навчатися», підтримувати прийняття рішень в умовах невизначеності, а також забезпечувати сталість і резилієнтність ЗВО у воєнних та післявоєнних реаліях.

Практична значущість полягає у відтворюваному інструментарії для керівництва ЗВО, що забезпечує прозоре балансування між безпекою, доступністю та академічною якістю, знижує залежність від окремих постачальників і зменшує ризики через географічне резервування й угоди взаємодопомоги між ЗВО. Для державної політики й регуляторів модель пропонує вимірювану основу для настанов щодо безперервності та кіберстійкості у секторі вищої освіти.

Подальші дослідження доцільно спрямувати на економіко-управлінський аналіз інвестицій у стійкість, оцінку людського фактору (культура безпеки, поведінкові патерни, підтримка добробуту спільноти), сумісність із національними та європейськими регуляторними вимогами, а також можливості інтеграції з академічними інформаційними системами. Узгодження цих напрямів забезпечить масштабованість та довгострокову життєздатність запропонованого підходу, а також підтримає післявоєнне відновлення та розвиток вищої освіти України.

Література

1. Amorós Molina Á., Helldén D., Alfvén T., Niemi M., Leander K., Nordenstedt H., Rehn C., Ndejjo R., Wanyenze R., Biermann O. Integrating the

United Nations sustainable development goals into higher education globally: a scoping review. *Global Health Action*. 2023. 16(1). 2190649. DOI: https://doi.org/10.1080/16549716.2023.2190649

2. Armas R., Taherdoost H. Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm. *Information*. 2025. 16(5). 336. DOI: https://doi.org/10.3390/info16050336

3. Bañeres D., Rodríguez-González M.E., Guerrero-Roldán A.E., Cortadas P. An early warning system to identify and intervene online dropout learners. *International Journal of Educational Technology in Higher Education*. 2023. 20. 3. DOI: https://doi.org/10.1186/s41239-022-00371-5

4. Bartusevičienė I., Pazaver A., Kitada M. Building a resilient university: Ensuring academic continuity – transition from face-to-face to online in the COVID-19 pandemic. *WMU Journal of Maritime Affairs*. 2021. 20. 151–172. DOI: https://doi.org/10.1007/s13437-021-00239-x

5. Çirak C. R., Akilli H., Ekinci Y. Development of an early warning system for higher education institutions by predicting first-year student academic performance. *Higher Education Quarterly*. 2024. 78(4). e12539. DOI: https://doi.org/10.1111/hequ.12539

6. Clark C., Cluver M., Fishman T., Kunkel D. 2025 Higher Education Trends. *Deloitte Insights*. 07.04.2025. URL: https://www.deloitte.com/us/en/insights/industry/public-sector/2025-us-higher-education-trends.html (Accessed 09 Aug 2025).

7. Dawodu A., Dai H., Zou T., Zhou H., Lian W., Oladejo J., Osebor F. Campus sustainability research: indicators and dimensions to consider for the design and assessment of a sustainable campus. *Heliyon*. 2022. 8(12). e11864. DOI: https://doi.org/10.1016/j.heliyon.2022.e11864

8. European Union Agency for Cybersecurity. ENISA Threat Landscape 2023 (ETL 2023). URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf (Accessed 09 Aug 2025).

9. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 … (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (Accessed 09 Aug 2025).

10. Flanagan B., Majumdar R., Ogata H. Early-warning prediction of student performance and engagement in open book assessment by reading behavior analysis. *International Journal of Educational Technology in Higher Education*. 2022. 19. 41. DOI: https://doi.org/10.1186/s41239-022-00348-4

11. Greshta V., Shylo S., Korolkov V., Kulykovskyi R., Kapliienko O. Universities in times of war: Challenges and solutions for ensuring the educational process. *Problems and Perspectives in Management*. 2023. 21(2-si). 80–86. DOI: https://doi.org/10.21511/ppm.21(2-si).2023.10

12. Hoit M., Milhans J., Trubitt L. 2025 EDUCAUSE Top 10 #6: Institutional Resilience. 2024. URL: https://er.educause.edu/articles/2024/10/2025-educause-top-10-6-institutional-resilience (Accessed 09 Aug 2025).

13. International Organization for Standardization. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks. 2022. URL: https://www.iso.org/standard/80585.html (Accessed 09 Aug 2025).

14. International Organization for Standardization. ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles of incident management. 2023. URL: https://www.iso.org/standard/78973.html (Accessed 09 Aug 2025).

15. International Risk Governance Council (IRGC). White Paper on Risk Governance: Toward an Integrative Framework (reprinted version). 2006. URL: https://irgc.org/wp-content/uploads/2018/09/IRGC_WP_No_1_Risk_Governance__reprinted_version_3.pdf (Accessed 09 Aug 2025).

16. Ionescu Ș., Dumitrescu G., Ioanăș C., Delcea C. Mapping the landscape of key performance and key risk indicators in business: A comprehensive

bibliometric analysis. *Risks*. 2024. 12(8). 125. DOI: https://doi.org/10.3390/risks12080125

17. Kaźmierczak M., Jastrzębska E., Khovrak I. University Social Responsibility in Poland: The Review of Codes of Ethics, USR Strategies, and Reports. *Engineering Management in Production and Services*. 2025. 17(1). 66–79. DOI: https://doi.org/10.2478/emj-2025-0006

18. Khovrak I. Information and communication technologies in ensuring digital security in higher education institutions: policies, strategies, and international experience. *Studies in a Changing Business Environment*. 2025. 21–31. Vilnius: Lietuvos ekonomikos dėstytojų asociacija. URL: https://leda.lt/images/documents/Studijos_kintancioje_verslo_aplinkoje_2025.pdf (Accessed 09 Aug 2025).

19. Lallie H. S., Thompson A., Titis E., Stephens P. Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers*. 2025. 14(2). 49. DOI: https://doi.org/10.3390/computers14020049

20. Lempert R. J., Popper S. W., Bankes S. C. Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis. Santa Monica, CA: RAND Corporation, 2003. URL: https://www.rand.org/pubs/monograph_reports/MR1626.html (Accessed 09 Aug 2025).

21. Lempert R. J. Robust Decision Making (RDM). In: Marchau V., Walker W., Bloemen P., Popper S. (eds) *Decision Making under Deep Uncertainty*. Cham: Springer, 2019. DOI: https://doi.org/10.1007/978-3-030-05252-2_2

22. Milton S., Barakat S. Higher education as the catalyst of recovery in conflict-affected societies. *Globalisation, Societies and Education*. 2016. 14(3). 403–421. DOI: https://doi.org/10.1080/14767724.2015.1127749

23. Morris P., Park C., Auld E. Covid and the future of education: global agencies 'building back better'. *Compare: A Journal of Comparative and International Education*. 2022. 52(5). 691–711. DOI: https://doi.org/10.1080/03057925.2022.2066886

24. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 (Cybersecurity White Paper 29). 26.02.2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (Accessed 09 Aug 2025).

25. Protsyk H. Higher Education Amid the War: A Resilience Test for Ukraine's Integration into the European Higher Education Area. In: Rabinovych M., Pintsch A. (eds) *Ukraine's Thorny Path to the EU*. Cham: Palgrave Macmillan, 2025. DOI: https://doi.org/10.1007/978-3-031-69154-6_12

26. Renn O. Risk Governance: From Knowledge to Regulatory Action. In: Glückler J., Herrigel G., Handke M. (eds) *Knowledge for Governance. Knowledge and Space*, vol. 15. Cham: Springer, 2020. DOI: https://doi.org/10.1007/978-3-030-47150-7_5

27. Setyadi A., Pawirosumarto S., Damaris A. Enhancing Sustainable Learning Through Risk Management and Digital Literacy: The Role of Modern Learning Environments. *Preprint* (March 2025). DOI: https://doi.org/10.2139/ssrn.5189966

28. Shah R., Flemming J., Chinnery J., Heaner G. Building back better? The role of education sector responses in strengthening or eroding societal resilience during the COVID-19 pandemic. *Frontiers in Education*. 2024. 9. 1089422. DOI: https://doi.org/10.3389/feduc.2024.1089422

29. Shaya N., Abukhait R., Madani R., Khattak M.N. Organizational Resilience of Higher Education Institutions: An Empirical Study during Covid-19 Pandemic. *Higher Education Policy*. 2023. 36. 529–555. DOI: https://doi.org/10.1057/s41307-022-00272-2

30. Trevisan L. V., Eustachio J. H. P. P., Dias B. G., Filho W.L., Pedrozo E.Á. Digital transformation towards sustainability in higher education: state-of-the-art and future research insights. *Environment, Development and Sustainability*. 2024. 26. C. 2789–2810. DOI: https://doi.org/10.1007/s10668-022-02874-7

31. Vitters C., Braunsdorf J., Lord J., Mathew R. Significant risks facing higher education: Getting to the roots of risk. *Deloitte Insights*. 2024. URL:

https://www.deloitte.com/us/en/insights/industry/articles-on-higher-education/top-risks-in-higher-education.html (Accessed 09 Aug 2025).

32. World Bank. Education: Impact of the war in Ukraine. Brief. 2022. URL: https://documents1.worldbank.org/curated/en/099945306202211104/pdf/P1775870809f1d04d0844c0e7042abf0eb5.pdf (Accessed 09 Aug 2025).

33. Xu J., Cheung C., Manu P., Ejohwomu O. Safety leading indicators in construction: A systematic review. *Safety Science*. 2021. 139. 105250. DOI: https://doi.org/10.1016/j.ssci.2021.105250

References

1. Amorós Molina, Á., Helldén, D., Alfvén, T., Niemi, M., Leander, K., Nordenstedt, H., Rehn, C., Ndejjo, R., Wanyenze, R. and Biermann, O. (2023), "Integrating the United Nations sustainable development goals into higher education globally: a scoping review", *Global Health Action*, vol. 16, no. 1, 2190649. https://doi.org/10.1080/16549716.2023.2190649

2. Armas, R. and Taherdoost, H. (2025), "Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm", *Information*, vol. 16, no. 5, 336. https://doi.org/10.3390/info16050336

3. Bañeres, D., Rodríguez-González, M.E., Guerrero-Roldán, AE. and Cortadas, P. (2023), "An early warning system to identify and intervene online dropout learners", *International Journal of Educational Technology in Higher Education*, vol. 20, 3. https://doi.org/10.1186/s41239-022-00371-5

4. Bartusevičienė, I., Pazaver, A. and Kitada, M. (2021), "Building a resilient university: Ensuring academic continuity – transition from face-to-face to online in the COVID-19 pandemic", *WMU Journal of Maritime Affairs*, vol. 20, pp. 151-172. https://doi.org/10.1007/s13437-021-00239-x

5. Çirak, C. R., Akilli, H. and Ekinci, Y. (2024), "Development of an early warning system for higher education institutions by predicting first-year student

academic performance", *Higher Education Quarterly*, vol. 78, no. 4, e12539. https://doi.org/10.1111/hequ.12539

6. Clark, C., Cluver, M., Fishman, T. and Kunkel, D. (2025), "2025 Higher Education Trends", *Deloitte Insights*, available at: https://www.deloitte.com/us/en/insights/industry/public-sector/2025-us-higher-education-trends.html (Accessed 09 Aug 2025).

7. Dawodu, A., Dai, H., Zou, T., Zhou, H., Lian, W., Oladejo, J. and Osebor, F. (2022), "Campus sustainability research: indicators and dimensions to consider for the design and assessment of a sustainable campus", *Heliyon*, vol. 8, no. 12, e11864. https://doi.org/10.1016/j.heliyon.2022.e11864

8. European Union Agency for Cybersecurity (2023), "ENISA Threat Landscape 2023", available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf (Accessed 09 Aug 2025).

9. European Union (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 … (General Data Protection Regulation)", *Official Journal of the European Union*, L 119, pp. 1-88, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (Accessed 09 Aug 2025).

10. Flanagan, B., Majumdar, R. and Ogata, H. (2022), "Early-warning prediction of student performance and engagement in open book assessment by reading behavior analysis", *International Journal of Educational Technology in Higher Education*, vol. 19, 41. https://doi.org/10.1186/s41239-022-00348-4

11. Greshta, V., Shylo, S., Korolkov, V., Kulykovskyi, R. and Kapliienko, O. (2023), "Universities in times of war: Challenges and solutions for ensuring the educational process", *Problems and Perspectives in Management*, vol. 21, no. 2-si, pp. 80-86. https://doi.org/10.21511/ppm.21(2-si).2023.10

12. Hoit, M., Milhans, J. and Trubitt, L. (2024), "2025 EDUCAUSE Top 10 #6: Institutional Resilience", available at: https://er.educause.edu/articles/2024/10/2025-educause-top-10-6-institutional-resilience?utm_source=chatgpt.com (Accessed 09 Aug 2025).

13. International Organization for Standardization (2022), “ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks”, available at: https://www.iso.org/standard/80585.html (Accessed 09 Aug 2025).

14. International Organization for Standardization (2023), “ISO/IEC 27035-1:2023 Information technology. Information security incident management. Part 1: Principles of incident management”, available at: https://www.iso.org/standard/78973.html (Accessed 09 Aug 2025).

15. International Risk Governance Council (2006), “White Paper on Risk Governance: Toward an Integrative Framework (reprinted version)”, available at: https://irgc.org/wp-content/uploads/2018/09/IRGC_WP_No_1_Risk_Governance__reprinted_version_3.pdf (Accessed 09 Aug 2025).

16. Ionescu, Ș., Dumitrescu, G., Ioanăș, C. and Delcea, C. (2024), “Mapping the landscape of key performance and key risk indicators in business: A comprehensive bibliometric analysis”, *Risks*, vol. 12, no. 8, 125. https://doi.org/10.3390/risks12080125

17. Kaźmierczak, M., Jastrzębska, E. and Khovrak, I. (2025), “University Social Responsibility in Poland: The Review of Codes of Ethics, USR Strategies, and Reports”, *Engineering Management in Production and Services*, vol. 17, no. 1, pp. 66-79. https://doi.org/10.2478/emj-2025-0006

18. Khovrak, I. (2025), “Information and communication technologies in ensuring digital security in higher education institutions: policies, strategies, and international experience”, *Studies in a Changing Business Environment*, available at: https://leda.lt/images/documents/Studijos_kintancioje_verslo_aplinkoje_2025.pdf (Accessed 09 Aug 2025).

19. Lallie, H.S., Thompson, A., Titis, E. and Stephens, P. (2025), “Analysing cyber attacks and cyber security vulnerabilities in the university sector”, *Computers*, vol. 14, no. 2, 49. https://doi.org/10.3390/computers14020049

20. Lempert, R.J., Popper, S.W. and Bankes, S.C. (2003), “Shaping the next one hundred years: New methods for quantitative, long-term policy analysis”, *RAND Corporation*, available at: https://www.rand.org/pubs/monograph_reports/MR1626.html (Accessed 09 Aug 2025).

21. Lempert, R.J. (2019), “Robust Decision Making (RDM)”, *Decision Making under Deep Uncertainty*, Springer, Cham. https://doi.org/10.1007/978-3-030-05252-2_2

22. Milton, S. and Barakat, S. (2016), “Higher education as the catalyst of recovery in conflict-affected societies”, *Globalisation, Societies and Education*, vol. 14, no. 3, pp. 403-421, available at: https://www.tandfonline.com/doi/abs/10.1080/14767724.2015.1127749 (Accessed 09 Aug 2025).

23. Morris, P., Park, C. and Auld, E. (2022), “Covid and the future of education: global agencies ‘building back better’”, *Compare: A Journal of Comparative and International Education*, vol. 52, no. 5, pp. 691-711. https://doi.org/10.1080/03057925.2022.2066886

24. National Institute of Standards and Technology (2024), “The NIST Cybersecurity Framework (CSF) 2.0 (Cybersecurity White Paper 29)”, available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (Accessed 09 Aug 2025).

25. Protsyk, H. (2025), “Higher Education Amid the War: A Resilience Test for Ukraine’s Integration into the European Higher Education Area”, *Ukraine’s Thorny Path to the EU*, Palgrave Studies in European Union Politics. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-69154-6_12

26. Renn, O. (2020), “Risk Governance: From Knowledge to Regulatory Action”, *Knowledge for Governance. Knowledge and Space*, vol 15. Springer, Cham. https://doi.org/10.1007/978-3-030-47150-7_5

27. Setyadi, A., Pawirosumarto, S. and Damaris, A. (2025), “Enhancing Sustainable Learning Through Risk Management and Digital Literacy: The Role of Modern Learning Environments”, *Preprint*. https://doi.org/10.2139/ssrn.5189966

28. Shah, R., Flemming, J., Chinnery, J. and Heaner, G. (2024), “Building back better? The role of education sector responses in strengthening or eroding societal resilience during the COVID-19 pandemic”, *Frontiers in Education*, vol. 9, 1089422. https://doi.org/10.3389/feduc.2024.1089422

29. Shaya, N., Abukhait, R., Madani, R. and Khattak, M.N. (2023), “Organizational Resilience of Higher Education Institutions: An Empirical Study during Covid-19 Pandemic”, *Higher Education Polic*, vol. 36, pp. 529-555. https://doi.org/10.1057/s41307-022-00272-2

30. Trevisan, L.V., Eustachio, J.H.P.P., Dias, B.G., Filho, W.L. and Pedrozo, E.Á. (2024), “Digital transformation towards sustainability in higher education: state-of-the-art and future research insights”, *Environment, Development and Sustainability*, vol. 26, 2789-2810. https://doi.org/10.1007/s10668-022-02874-7

31. Vitters, C. Braunsdorf, J. Lord, J. and Mathew, R. (2024), “Significant risks facing higher education: Getting to the roots of risk”, *Deloitte Insights*, available at: https://www.deloitte.com/us/en/insights/industry/articles-on-higher-education/top-risks-in-higher-education.html (Accessed 09 Aug 2025).

32. World Bank (2022), “Education: Impact of the war in Ukraine”, Brief, available at: https://documents1.worldbank.org/curated/en/099945306202211104/pdf/P1775870809f1d04d0844c0e7042abf0eb5.pdf (Accessed 09 Aug 2025).

33. Xu, J. Cheung, C. Manu, P. and Ejohwomu, O. (2021), “Safety leading indicators in construction: A systematic review”, *Safety Science*, vol. 139, 105250. https://doi.org/10.1016/j.ssci.2021.105250

Стаття надійшла до редакції 12.09.2025 р.