



УДК 004.738.5:37.018.43:159.9

[https://doi.org/10.52058/2786-5274-2026-5\(57\)-3571-3586](https://doi.org/10.52058/2786-5274-2026-5(57)-3571-3586)

Лунченко Надія Вікторівна кандидат психологічних наук, завідувачка лабораторії прикладної психології освіти, Український науково-методичний центр практичної психології і соціальної роботи, м. Київ, <https://orcid.org/0000-0002-4926-7115>.

Шкредов Ігор Володимирович магістр психології, випускник кафедри педагогіки і психології управління соціальними системами імені академіка І. А. Зязюна, Навчально-науковий інститут соціально-гуманітарних технологій, Національний технічний університет «Харківський політехнічний інститут», м. Харків, <https://orcid.org/0009-0006-0593-5173>.

Новіцька Інеса Василівна кандидат педагогічних наук, доцент, завідувач відділу аспірантури та докторантури, доцент кафедри професійно-педагогічної спеціальної освіти, андрагогіки та управління, Навчально-науковий інститут педагогіки, Житомирський державний університет імені Івана Франка, м. Житомир, <https://orcid.org/0000-0003-0780-0580>.

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ СТУДЕНТІВ У ХМАРНО-ОРІЄНТОВАНОМУ ОСВІТНЬОМУ СЕРЕДОВИЩІ

Анотація. Актуальність дослідження зумовлена інтенсивною цифровізацією освітнього процесу та поширенням хмарно-орієнтованих середовищ, що супроводжується зростанням не лише кібернетичних, а й інформаційно-психологічних ризиків для студентів. У цих умовах традиційні підходи до безпеки виявляються обмеженими, оскільки не враховують взаємодію технологічних, поведінкових і психоемоційних чинників.

Мета дослідження полягає у розробленні та теоретичному обґрунтуванні концептуальної моделі забезпечення інформаційно-психологічної безпеки студентів у хмарно-орієнтованому освітньому середовищі на основі інтеграції технологічних і психолого-педагогічних підходів.

Методи дослідження включають системний аналіз, узагальнення, порівняння та структурно-функціональний підхід до дослідження характеристик цифрового освітнього середовища, факторів ризику та механізмів забезпечення безпеки.

У результаті дослідження розкрито сутність та структурні компоненти інформаційно-психологічної безпеки студентів, систематизовано фактори ризику та загрози у хмарно-орієнтованих освітніх середовищах, узагальнено





наукові підходи до забезпечення безпеки в умовах цифровізації освіти. Виявлено основні наукові та практичні проблеми, зокрема концептуальну невизначеність феномену, розрив між технічними та психолого-педагогічними підходами, перевантаженість інформаційного середовища та неузгодженість цифрових практик. Доведено, що ключові ризики формуються у взаємодії інформаційних потоків і поведінкових сценаріїв користувачів.

У висновках обґрунтовано, що підвищення рівня інформаційно-психологічної безпеки досягається через узгодження технологічних, організаційних і поведінкових параметрів освітнього середовища. Запропонована модель забезпечує перехід від фрагментарних заходів до процесно інтегрованого управління безпекою.

Перспективи подальших досліджень пов'язані з розробленням методів кількісної оцінки інформаційно-психологічної безпеки, створенням інструментів її моніторингу в режимі реального часу та емпіричною перевіркою ефективності моделі в різних типах освітніх середовищ.

Ключові слова: хмарно-орієнтоване середовище, цифрове освітнє середовище, кіберзагрози, когнітивне навантаження, психоемоційна стійкість, цифрова взаємодія, інформаційні ризики, інформаційно-психологічна безпека..

Nadiia Lunchenko PhD in Psychology, Head of the Laboratory of Applied Psychology of Education, Ukrainian Scientific and Methodological Center of Applied Psychology and Social Work, Kyiv, <https://orcid.org/0000-0002-4926-7115>.

Igor Shkredov Master's degree in Psychology, Department of Pedagogy and Psychology of Management of Social Systems of Academician I. A. Zyazyun, Educational and Scientific Institute of Social and Humanitarian Technologies, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, <https://orcid.org/0009-0006-0593-5173>.

Inesa Novitska PhD in Pedagogy, Associate Professor, Head of the Postgraduate and Doctoral Studies Department, Associate Professor of the Department of Vocational and Pedagogical Special Education, Andragogy and Management, Educational and Research Institute of Pedagogics, Zhytomyr Ivan Franko State University, Zhytomyr, <https://orcid.org/0000-0003-0780-0580>.

CONCEPTUAL MODEL FOR ENSURING INFORMATION AND PSYCHOLOGICAL SECURITY OF STUDENTS IN A CLOUD-ORIENTED EDUCATIONAL ENVIRONMENT

Abstract. The relevance of the study is determined by the intensive digitalization of the educational process and the widespread adoption of cloud-oriented learning environments, which are accompanied by the growth of not only cyber threats but also





information and psychological risks for students. Under these conditions, traditional security approaches prove to be limited, as they do not take into account the interaction of technological, behavioral, and psycho-emotional factors.

The purpose of the study is to develop and theoretically substantiate a conceptual model for ensuring the information and psychological security of students in a cloud-oriented educational environment based on the integration of technological and psycho-pedagogical approaches.

The research methods include system analysis, generalization, comparison, and a structural-functional approach to studying the characteristics of the digital educational environment, risk factors, and security mechanisms.

As a result of the study, the essence and structural components of students' information and psychological security have been examined, and the risk factors and threats inherent in cloud-oriented educational environments have been systematized. Scientific approaches to ensuring security under conditions of educational digitalization have been generalized. The main scientific and practical problems have been identified, including conceptual ambiguity of the phenomenon, the gap between technological and psycho-pedagogical approaches, information overload, and inconsistency of digital practices. It has been demonstrated that key risks arise from the interaction between information flows and users' behavioral patterns.

The conclusions substantiate that improving the level of information and psychological security is achieved through the alignment of technological, organizational, and behavioral parameters of the educational environment. The proposed model ensures a transition from fragmented measures to process-integrated security management.

Prospects for further research are associated with the development of methods for quantitative assessment of information and psychological security, the creation of real-time monitoring tools, and empirical validation of the proposed model in various types of educational environments.

Keywords: cloud-oriented environment, digital learning environment, cyber threats, cognitive load, psycho-emotional resilience, online interaction, information risks, information and psychological security.

Постановка проблеми. Стрімка цифровізація вищої освіти, що супроводжується широким впровадженням хмарно-орієнтованих освітніх середовищ, суттєво трансформує умови навчальної діяльності, водночас загострюючи проблему забезпечення інформаційно-психологічної безпеки студентів.

Інтеграція цифрових сервісів, платформ спільної роботи та віддаленого доступу до навчальних ресурсів підвищує відкритість і мобільність освітнього процесу, проте формує нові ризики, пов'язані не лише з технічним захистом даних, а й з впливом інформаційного середовища на когнітивні, емоційні та поведінкові характеристики здобувачів освіти. У цих умовах відбувається поєднання кіберзагроз, інформаційного перевантаження, маніпулятивного контенту та психологічної вразливості, що особливо посилюється в контексті

соціальної нестабільності та війни Росії проти України. Проблема набуває міждисциплінарного характеру, оскільки її вирішення потребує узгодження підходів інформаційної безпеки, психології, педагогіки та управління освітніми системами, що наразі реалізується фрагментарно. Існуючі дослідження переважно зосереджені або на технічних аспектах захисту інформації, або на окремих психологічних ефектах цифрового середовища, що ускладнює формування цілісних моделей безпеки, здатних врахувати взаємозв'язок технологічних і психосоціальних факторів.

У практичній площині це проявляється у відсутності інтегрованих механізмів управління ризиками в хмарно-орієнтованих освітніх середовищах, недостатній адаптації освітніх платформ до принципів безпечної взаємодії та обмеженій готовності викладачів і студентів до протидії інформаційно-психологічним впливам.

Так, актуалізується науково-прикладне завдання розроблення концептуальних засад забезпечення інформаційно-психологічної безпеки студентів, що передбачає інтеграцію технологічних, організаційних і психолого-педагогічних рішень у межах єдиної моделі, орієнтованої на мінімізацію ризиків цифрового середовища та підтримку стійкості особистості в умовах інформаційної турбулентності.

Аналіз останніх досліджень і публікацій. Огляд сучасних досліджень засвідчує, що проблематика забезпечення інформаційно-психологічної безпеки студентів у хмарно-орієнтованому освітньому середовищі формується на перетині педагогіки, інформаційно-комунікаційних технологій (ІКТ) та психології безпеки, що зумовлює її комплексний і міждисциплінарний характер. І. Книш та Ю. Панфілов обґрунтовують доцільність інтеграції ІКТ у безпечне освітнє середовище як інструменту формування ціннісного ставлення до здоров'я учасників освітнього процесу, акцентуючи на превентивному потенціалі цифрових інструментів [1]. І. Чичкань та співавтори розвивають ці положення, визначаючи освітнє середовище як простір формування культури безпечної поведінки у кіберпросторі, де ключову роль відіграють компетентнісні та поведінкові аспекти цифрової безпеки [2]. Р. Моцик та співавтори розглядають хмарні сервіси як основу створення ефективного цифрового освітнього середовища, підкреслюючи їх значення для організації доступу до ресурсів і взаємодії, що опосередковано впливає на рівень інформаційної безпеки [3]. Л. Калмикова та співавтори уточнюють роль хмарних технологій у вищій освіті, інтерпретуючи їх не лише як інновацію, а як системоутворювальний фактор трансформації освітнього простору [4].

Б. Шевчук акцентує увагу на проектуванні віртуальних освітніх середовищ, де питання безпеки інтегруються на етапі архітектурного моделювання освітнього процесу [5], тоді як О. Гавриленко підкреслює значення інформаційно-цифрових інструментів як засобів підвищення ефективності навчальної діяльності, що формує передумови для безпечної цифрової взаємодії [6].



Подальший розвиток досліджуваної проблематики простежується у працях, присвячених хмарно-орієнтованим середовищам та їх функціонуванню. О. Глазунова (O. Glazunova) та співавтори обґрунтовують модель гібридного хмарного освітнього середовища для організації командної роботи студентів, акцентуючи на необхідності узгодження технологічних і педагогічних компонентів [7]. Т. Вакалюк (T. Vakaliuk) та співавтори розширюють цей підхід, розглядаючи концепцію «зелених» інформаційних технологій (Green Information Technology, Green IT) як основу формування сталого хмарно-орієнтованого середовища, що передбачає баланс між технологічною ефективністю та безпекою [8]. Г. Варіна (H. Varina) та співавтори доводять, що використання хмарних технологій у змішаному навчанні сприяє розвитку професійної стійкості майбутніх фахівців, що має безпосередній зв'язок із їх психологічною безпекою в цифровому середовищі [9]. О. Бондарчук (O. Bondarchuk) та співавтори досліджують інструменти моніторингу психологічної складової діяльності викладачів за допомогою сервісу Google Forms, що дозволяє екстраполювати отримані результати на оцінювання психологічного стану учасників освітнього процесу [10]. К. Билинська (K. Bilynska) та співавтори акцентують увагу на ролі інтерактивного мультимедійного контенту у підвищенні якості навчання, що водночас актуалізує питання інформаційно-психологічного впливу на студентів [11].

Водночас окремі дослідження зосереджуються на прикладних аспектах функціонування цифрового освітнього середовища та управління освітнім процесом. М. Шерман (M. Sherman) та співавтори розробляють електронні системи дистанційного оцінювання знань у хмарному середовищі, підкреслюючи необхідність забезпечення надійності та захищеності даних [12]. М. Джаялакшмі (M. Jayalakshmi) та В. Гоматі (V. Gomathi) пропонують підходи до моніторингу стану користувачів на основі інтеграції відеоаналізу та сенсорних даних у хмарних системах, що відкриває можливості для відстеження психофізіологічних показників [13]. Ю. Крилова-Грек (Y. Krylova-Grek) та М. Шишкіна (M. Shyshkina) аналізують розвиток онлайн-навчання у закладах вищої освіти України, виокремлюючи виклики, пов'язані з цифровою безпекою та психологічною адаптацією студентів [14]. К. Мішра (K. Mishra) та С. Пандей (S. Pandey) узагальнюють потенціал інтеграції хмарних та інтернет-речей технологій (Cloud-Internet of Things technologies, Cloud-IoT) у концепції Society 5.0, де освітні середовища розглядаються як частина ширших кіберфізичних систем, що потребують комплексного забезпечення безпеки [15].

Попри наявні дослідження, залишається невирішеним питання цілісного розуміння інформаційно-психологічної безпеки як системного явища, оскільки наукові підходи зосереджуються переважно на окремих її аспектах – технічному або психолого-педагогічному. Така фрагментарність посилюється складністю емпіричного фіксування взаємозв'язку між параметрами цифрового середовища та станом студентів, що зумовлює розрив між теоретичними уявленнями і реальними практиками організації навчання.

Невирішеність цих аспектів обмежує можливість побудови ефективних рішень, оскільки ризики виникають саме на рівні їх взаємодії. Саме тому дослідження спрямоване на подолання цієї роз'єднаності через формування узгодженого бачення проблеми та обґрунтування підходу, який дозволяє інтегрувати різноманітні елементи освітнього середовища у логіку безпечного функціонування.

Мета і завдання статті. Мета статті полягає у розробленні концептуальної моделі забезпечення інформаційно-психологічної безпеки студентів у хмарно-орієнтованому освітньому середовищі на основі інтеграції технологічних і психолого-педагогічних підходів.

Завдання статті:

1. Розкрити сутність інформаційно-психологічної безпеки та систематизувати ризики хмарно-орієнтованого освітнього середовища.
2. Узагальнити підходи та виявити ключові проблеми її забезпечення.
3. Обґрунтувати концептуальну модель забезпечення інформаційно-психологічної безпеки студентів.

Виклад основного матеріалу. Інформаційно-психологічна безпека студентів у цифровому освітньому середовищі розглядається як інтегральна характеристика, що відображає здатність освітньої системи та особистості забезпечувати захищеність інформаційних процесів і психічної сфери від деструктивних впливів, зберігаючи стабільність когнітивного функціонування, емоційної регуляції та поведінкових реакцій у процесі навчання. У хмарно-орієнтованих середовищах така безпека формується на перетині технологічних рішень, організаційних практик і психолого-педагогічних механізмів, що зумовлює її багаторівневу структуру та потребує узгодженого управління всіма складовими (табл. 1).

Таблиця 1

Структурні компоненти інформаційно-психологічної безпеки студентів у цифровому освітньому середовищі

Компонент	Змістова характеристика	Практичне значення
Інформаційний	Захист даних, контроль доступу, фільтрація контенту	Запобігання витоку інформації та впливу деструктивного контенту
Когнітивний	Регулювання інформаційного навантаження, забезпечення зрозумілості матеріалів	Підтримка ефективного сприйняття та обробки інформації
Емоційно-психологічний	Мінімізація стресових впливів, підтримка психологічного комфорту	Зниження рівня тривожності та емоційного виснаження



Компонент	Змістова характеристика	Практичне значення
Поведінковий	Формування безпечних моделей онлайн-взаємодії	Запобігання ризикованій цифровій поведінці
Організаційно-педагогічний	Регламентация цифрової взаємодії, впровадження безпечних освітніх практик	Підвищення керованості та стабільності освітнього процесу

Джерело: сформовано авторами на основі [1, с. 110; 2, с. 360; 5; 10; 11, р. 190; 14, р. 168].

Ці компоненти у хмарно-орієнтованому освітньому середовищі мають системний характер і визначаються їхньою взаємною обумовленістю у реальних освітніх практиках. Інформаційний компонент забезпечується через поєднання технічних і регламентних рішень – зокрема, диференційоване надання прав доступу до навчальних матеріалів і сервісів дозволяє обмежити несанкціоноване поширення даних та мінімізувати вплив неконтрольованого інформаційного контенту [14, р. 167].

При цьому ефективність таких заходів залежить від когнітивного компоненту, оскільки надмірно складні або перевантажені інтерфейси знижують здатність студентів орієнтуватися в освітньому середовищі, що підвищує ризик помилкових дій і інформаційної дезорганізації.

Когнітивний компонент у практиці реалізується через структурування навчальних матеріалів, поетапне подання інформації та обмеження паралельних інформаційних потоків, що дозволяє підтримувати стабільний рівень концентрації та зменшувати ефекти перевантаження. У свою чергу, емоційно-психологічний компонент проявляється у здатності освітнього середовища знижувати напруження, яке виникає внаслідок інтенсивної цифрової взаємодії – наприклад, за рахунок прогнозованості навчальних сценаріїв, чітких часових меж активностей і наявності каналів оперативного зворотного зв'язку [10]. Це особливо актуально в умовах підвищеної соціальної нестабільності, коли цифрове середовище фактично виконує компенсаторну функцію підтримки психологічної рівноваги студентів.

Поведінковий компонент забезпечує трансформацію індивідуальних моделей взаємодії у безпечні практики використання цифрових ресурсів – від дотримання академічної доброчесності до критичного відбору інформації, що прямо впливає на зниження вразливості до маніпулятивних впливів. Його реалізація неможлива без організаційно-педагогічного компонента, який задає нормативні та методичні рамки функціонування системи, інтегруючи технічні можливості платформи з педагогічними цілями [2, с. 365]. У практичному вимірі це означає, що навіть за наявності сучасних технологічних інструментів рівень інформаційно-психологічної безпеки визначається якістю їх педагогічного впровадження – зокрема, узгодженістю навчального контенту, режимів взаємодії

та вимог до діяльності студентів, що забезпечує не лише захист, а й стійкість освітнього процесу в умовах цифрової трансформації.

Систематизація факторів ризику та загроз у хмарно-орієнтованих освітніх середовищах потребує врахування специфіки їх функціонування, що поєднує відкритість цифрових платформ, розподіленість інформаційних ресурсів і високу інтенсивність онлайн-взаємодії. У таких умовах ризику формуються не лише внаслідок технічних вразливостей, а й через особливості поведінки користувачів, характер інформаційних потоків та організаційні недоліки управління освітнім процесом. Важливою є диференціація загроз за їх природою та механізмами впливу, що дозволяє визначити критичні зони вразливості та обґрунтувати напрями їх мінімізації в межах єдиної системи безпеки (табл. 2).

Таблиця 2

Фактори ризику та загрози у хмарно-орієнтованих освітніх середовищах

Тип загрози	Джерело виникнення	Характер впливу	Потенційні наслідки
Кібернетичні	Несанкціонований доступ, шкідливе ПЗ, фішингові атаки	Порушення конфіденційності та цілісності даних	Витік персональної інформації, компрометація акаунтів
Інформаційно-контентні	Ненадійні джерела, маніпулятивний або деструктивний контент	Викривлення інформаційного сприйняття	Формування хибних уявлень, зниження якості навчання
Когнітивні	Надлишкові інформаційні потоки, складність інтерфейсів	Перевантаження уваги та пам'яті	Зниження концентрації, підвищення кількості помилок
Психоемоційні	Тривала онлайн-взаємодія, соціальна ізоляція, стресові фактори	Дестабілізація емоційного стану	Виснаження, тривожність, зниження мотивації
Організаційні	Недосконалі регламенти, відсутність чітких правил використання платформ	Порушення узгодженості освітніх процесів	Зниження керованості, конфлікти, інформаційний хаос

Джерело: сформовано авторами на основі [2, с. 364; 4, с. 103; 8; 12, р. 296; 13, р. 3702; 14, р. 169; 15].

У практиці функціонування хмарно-орієнтованих освітніх середовищ ризику проявляються як динамічні ситуації, у яких технічні, інформаційні та



психологічні чинники переплітаються і взаємно підсилюються. Типовим є сценарій, коли порушення доступу до акаунта через елементарну помилку користувача не обмежується лише технічним інцидентом – воно призводить до втрати навчальних матеріалів, збою комунікації з викладачем і, як наслідок, формує стан невизначеності та зниження навчальної впевненості [2, с. 364]. У таких випадках ризик набуває не лише інформаційного, а й виразного психологічного виміру.

Інша група ризиків актуалізується в процесі роботи з навчальним контентом, коли відкритість цифрового середовища фактично перекладає частину функцій експертизи на самого студента. Зіткнення з альтернативними інтерпретаціями, спрощеними поясненнями або відверто маніпулятивними матеріалами змінює траєкторію засвоєння знань, причому ці відхилення не завжди очевидні ні для викладача, ні для самого здобувача освіти [15]. У результаті виникає ситуація прихованого викривлення навчального результату, що не фіксується стандартними інструментами контролю.

Водночас інтенсивність цифрової взаємодії формує специфічний режим когнітивного навантаження, у якому навчальна діяльність розгортається через постійне перемикання між різними інформаційними каналами. Така розпорошеність не завжди усвідомлюється як проблема, однак поступово знижує здатність до глибокого аналізу і підвищує залежність від поверхневих стратегій опрацювання матеріалу. Саме на цьому тлі загострюються психоемоційні реакції – зростає напруження в періоди пікового навантаження, з'являється відчуття втрати контролю над навчальним процесом, навіть за формальної доступності всіх ресурсів.

Вирішальним у цьому контексті виявляється не стільки наявність окремих захисних інструментів, скільки логіка організації самого середовища. Там, де відсутня узгодженість у використанні платформ, каналів комунікації та форматів подання матеріалу, ризики накопичуються і переходять у системний стан. Натомість практики, що передбачають чітке структурування інформаційних потоків, обмеження надлишкових каналів взаємодії та узгодженість вимог до навчальної діяльності, демонструють іншу динаміку – зниження частоти інцидентів і стабілізацію психоемоційного стану студентів [8]. У такому підході безпека постає не як реакція на окремі загрози, а як властивість добре організованого освітнього середовища.

Узагальнення наукових підходів до забезпечення безпеки в умовах цифровізації освітнього процесу свідчить про поступовий перехід від вузько технократичного розуміння захисту до інтегративних моделей, у межах яких безпека розглядається як властивість освітньої системи, що формується на стику технологій, педагогічного дизайну та психологічної підтримки. Сучасні дослідження акцентують увагу на необхідності поєднання превентивних і адаптивних механізмів, орієнтованих не лише на мінімізацію ризиків, а й на формування стійкості користувачів до деструктивних впливів цифрового

середовища. У цьому контексті особливого значення набувають підходи, що враховують поведінкові та когнітивні аспекти взаємодії з інформаційними системами, а також організаційні принципи побудови освітнього середовища (табл. 3).

Таблиця 3

Наукові підходи до забезпечення безпеки
в умовах цифровізації освітнього процесу

Підхід	Теоретична основа	Механізми реалізації	Очікуваний ефект
Технологічно-орієнтований	Концепції кібербезпеки та захисту інформації	Шифрування, автентифікація, контроль доступу, моніторинг активності	Зниження технічних вразливостей і захист даних
Психолого-педагогічний	Теорії когнітивного навантаження та психологічної стійкості	Адаптивний дизайн навчання, підтримка емоційного стану, розвиток критичного мислення	Підвищення стійкості до інформаційних впливів
Поведінковий	Моделі цифрової поведінки та інформаційної культури	Формування навичок безпечної взаємодії, цифрова грамотність	Зменшення ризикованих дій користувачів
Організаційно-управлінський	Системний підхід до управління освітніми процесами	Регламентація процедур, стандартизація використання платформ	Підвищення узгодженості та керованості середовища
Інтегративний	Синтез міждисциплінарних підходів	Поєднання технологічних, педагогічних і організаційних рішень	Комплексне забезпечення безпеки та стійкості системи

Джерело: сформовано авторами на основі [1, с. 111; 2, с. 365; 3, с. 160; 10; 11, р. 192; 12, р. 300; 15].



Різні підходи до забезпечення безпеки проявляються через конкретні управлінські та педагогічні рішення, які або стабілізують середовище, або, навпаки, створюють додаткові точки напруження. Показовою є ситуація впровадження нової хмарної платформи для навчання: технічно вона може бути захищеною, однак за відсутності продуманого сценарію використання виникає розрив між можливостями системи та фактичними діями студентів [11, р. 192]. Наприклад, дублювання матеріалів у різних сервісах або паралельне використання кількох каналів комунікації призводить не до підвищення доступності, а до втрати орієнтації в навчальному процесі, що підвищує когнітивне навантаження і провокує помилки навіть у базових діях.

Інша характерна ситуація пов'язана з роботою з навчальним контентом. Коли викладачі орієнтуються лише на технологічні можливості платформи і не коригують логіку подання матеріалу, студенти змушені самотійно вибудувати зв'язки між фрагментами інформації. У таких умовах безпека набуває неочевидного виміру – формально середовище функціонує коректно, але фактично зростає ризик викривленого засвоєння знань і втрати контролю над навчальною діяльністю [12, р. 300]. Натомість практика чіткої структуризації курсу, обмеження надлишкових інформаційних каналів і синхронізації завдань із функціоналом платформи демонструє інший ефект – знижується кількість помилок, стабілізується темп роботи і зменшується напруження, пов'язане з невизначеністю.

Не менш показовим є вплив поведінкових факторів, які часто залишаються поза увагою при технічному проектуванні середовища. Навіть за наявності інструкцій студенти адаптують їх до власних практик – наприклад, обмінюються матеріалами через неформальні канали або зберігають дані поза офіційною системою. У таких випадках реальна конфігурація середовища відрізняється від запроєктованої, що створює приховані вразливості. Там, де ці практики враховуються – через уніфікацію каналів взаємодії, інтеграцію сервісів і чітке розмежування функцій – середовище стає більш передбачуваним і стійким.

Отже, у сучасних умовах ключовим виявляється не стільки вибір окремого підходу, скільки здатність узгодити технологічні рішення з реальною логікою навчальної діяльності. Саме в цій точці формується практична ефективність безпеки – коли інструменти, правила і поведінкові сценарії не суперечать один одному, а працюють як єдина система, що знижує ймовірність збоїв і забезпечує стабільність освітнього процесу.

Забезпечення інформаційно-психологічної безпеки студентів у хмарно-орієнтованому освітньому середовищі ускладнюється низкою взаємопов'язаних наукових і практичних проблем, що не зводяться до окремих технічних або педагогічних рішень. На концептуальному рівні зберігається невизначеність змісту цього феномену та відсутність узгоджених критеріїв його оцінювання, що обмежує можливість побудови цілісних моделей і порівняння результатів досліджень.



Дослідницьке поле залишається фрагментованим – технічні аспекти захисту розглядаються відокремлено від психологічних наслідків взаємодії з цифровим середовищем, унаслідок чого втрачається розуміння їх системної взаємодії [3, с. 160].

Методичною проблемою є розрив між характеристиками середовища і їх впливом на стан студента – наявні інструменти фіксують або технічні інциденти, або психоемоційні показники, але не дозволяють пояснити їх взаємозв'язок. У практиці це посилюється динамічністю хмарних платформ, де зміни функціоналу випереджають адаптацію освітніх підходів. Водночас спостерігається перевантаженість середовища інструментами та каналами комунікації, що створює когнітивну дезорганізацію і підвищує ймовірність помилок у навчальній діяльності [10].

Суттєвим залишається розрив між регламентованими правилами та фактичними практиками користувачів – неформальні канали обміну інформацією і зберігання даних формують приховані вразливості, які не враховуються в офіційних моделях безпеки.

Додатковим обмеженням є недостатня інтеграція питань безпечної взаємодії у зміст навчання та обмежена готовність викладачів до системного використання цифрових інструментів з урахуванням їх психологічного впливу.

У цих умовах психоемоційна стійкість студентів, особливо в контексті війни Росії проти України, стає критичним, але недостатньо керованим параметром, що вимагає переходу від декларативних підходів до комплексних рішень, здатних узгоджувати технологічні, організаційні та поведінкові аспекти безпеки.

Розроблена концептуальна модель забезпечення інформаційно-психологічної безпеки студентів у хмарно-орієнтованому освітньому середовищі розглядається як інтегрована система узгоджених дій, спрямованих на одночасне управління інформаційними потоками, поведінковими практиками та психоемоційним станом учасників освітнього процесу. Її актуальність зумовлена тим, що існуючі підходи, як правило, або фокусуються на технічному захисті, або обмежуються педагогічними рекомендаціями, не враховуючи їх взаємодію в реальних умовах цифрового навчання.

Запропонована модель відрізняється тим, що будується на принципі процесної узгодженості – безпека формується не як набір окремих заходів, а як послідовність взаємопов'язаних етапів, інтегрованих у логіку освітнього процесу. Її основу становить поєднання системного підходу, концепцій адаптивного управління та урахування поведінкових патернів користувачів, що дозволяє враховувати динамічність середовища та змінність умов навчання. Модель являє собою покрокову організаційну схему, у межах якої кожен етап виконує функцію виявлення, узгодження та корекції параметрів безпеки з орієнтацією на стабільність навчальної діяльності (рис. 1).



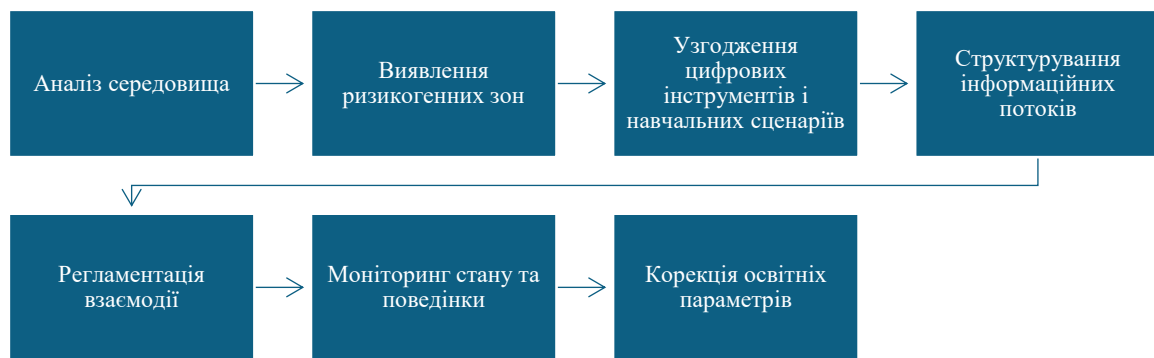


Рис. 1. Модель забезпечення інформаційно-психологічної безпеки студентів у хмарно-орієнтованому освітньому середовищі

Джерело: власна розробка автора

Практична реалізація моделі в сучасних умовах передбачає її інтеграцію у повсякденну організацію навчального процесу без додаткового ускладнення для користувачів. На початковому етапі відбувається оцінювання конфігурації освітнього середовища – кількості платформ, каналів комунікації та типів навчальних матеріалів, що дозволяє виявити перевантажені або неузгоджені елементи. Далі здійснюється узгодження інструментів із логікою курсу, що передбачає обмеження дублювання ресурсів і визначення чітких каналів взаємодії.

Структурування інформаційних потоків забезпечує передбачуваність навчальної діяльності – студент отримує матеріал у впорядкованому вигляді, що знижує когнітивне напруження. Регламентація взаємодії формує сталі правила роботи з цифровим середовищем, що мінімізує поведінкові відхилення і неформальні практики.

Моніторинг дозволяє фіксувати зміни в активності та стані студентів, що дає змогу своєчасно реагувати на ознаки перевантаження або дезорганізації навчальної діяльності. Завершальний етап корекції забезпечує адаптацію параметрів середовища – зміну обсягу матеріалу, форматів взаємодії або розподілу навантаження відповідно до отриманих даних. У результаті модель функціонує як замкнений цикл, що підтримує баланс між технологічними можливостями та психолого-педагогічними умовами навчання, знижує ймовірність виникнення критичних ситуацій і підвищує стійкість освітнього процесу в умовах цифрової нестабільності.

Висновки. У результаті дослідження встановлено, що інформаційно-психологічна безпека студентів у хмарно-орієнтованому освітньому середовищі формується як інтегральна властивість, що виникає внаслідок узгодженості технологічних рішень, організації освітнього процесу та поведінкових практик користувачів. Доведено, що її забезпечення не може обмежуватися технічним захистом, оскільки ключові ризики формуються у взаємодії інформаційних потоків і психоемоційного реагування студентів.

Встановлено, що основні проблеми пов'язані з концептуальною невизначеністю феномену, відсутністю інструментів, які дозволяють пов'язати параметри цифрового середовища зі станом студента, а також із розбалансованістю практичної організації навчання – перевантаженістю середовища, фрагментацією взаємодії та розривом між регламентами і реальними поведінковими сценаріями.

Запропонована модель забезпечує перехід до процесно узгодженого управління безпекою через структурування інформаційних потоків, уніфікацію цифрової взаємодії та адаптивну корекцію освітніх параметрів, що дозволяє знизити ризики і підвищити стабільність навчальної діяльності.

Перспективи подальших досліджень пов'язані з розробленням методів кількісної оцінки безпеки, інструментів її моніторингу в реальному часі та емпіричною перевіркою ефективності моделі в різних освітніх середовищах.

Література:

1. Книш І., Панфілов Ю. Впровадження практик інформаційно-комунікаційних технологій у безпечне освітнє середовище для формування ціннісного ставлення до здоров'я учасників освітнього процесу. *Теорія і практика управління соціальними системами*. 2025. № 1. С. 109–122. DOI: <https://doi.org/10.20998/2078-7782.2025.1.09>.
2. Чичкань І. В., Спасітелєва С. О., Жданова Ю. Д. Освітнє середовище для формування культури безпекового поведіння у кіберпросторі при підготовці фахівців з економіки та управління. *Інформаційні технології і засоби навчання*. 2021. Т. 84, № 4. С. 354–375. DOI: <https://doi.org/10.33407/itlt.v84i4.3646>.
3. Моцик Р., Коломієць Н., Ящук О. Використання хмарних сервісів у створенні ефективного цифрового освітнього середовища. *Педагогічна освіта: теорія і практика*. 2025. № 38. С. 157–170. DOI: <https://doi.org/10.32626/2309-9763.2025-38-157-170>.
4. Калмикова Л., Харченко Н., Мисан І. Хмарні технології у вищій освіті: новація чи інновація? *Педагогічні інновації: ідеї, реалії, перспективи*. 2021. Вип. 2, № 27. С. 99–111. DOI: [https://doi.org/10.32405/2413-4139-2021-2\(27\)-99-111](https://doi.org/10.32405/2413-4139-2021-2(27)-99-111).
5. Шевчук Б. В. Проектування та впровадження віртуального освітнього середовища інформатичної підготовки майбутніх педагогів професійного навчання. *Педагогічна Академія: наукові записки*. 2024. № 13. DOI: <https://doi.org/10.5281/zenodo.14557241>.
6. Гавриленко О. Інформатично-цифрові інструменти та хмарні технології як інноваційні засоби навчальної діяльності вчителя математики. *Освіта. Інноватика. Практика*. 2023. Т. 11, № 10. С. 132–140. DOI: <https://doi.org/10.31110/2616-650X-vol11i10-020>.
7. Glazunova O. G., Voloshyna T. V., Korolchuk V. I. Hybrid cloud-oriented learning environment for IT student project teamwork. *Information Technologies and Learning Tools*. 2020. Vol. 77, № 3. P. 114–128. DOI: <https://doi.org/10.33407/itlt.v77i3.3210>.
8. Vakaliuk T., Antoniuk D., Morozov A., Medvedieva M., Medvediev M. Green IT as a tool for design cloud-oriented sustainable learning environment of a higher education institution. 2020. *arXiv preprint*. arXiv.2012.07744. DOI: <https://doi.org/10.48550/arXiv.2012.07744>.
9. Varina H. B., Osadcha K. P., Shevchenko S. V., Voloshyna V. V. Developing professional stability of future socionomic specialists using cloud technologies in blended learning. *CEUR Workshop Proceedings*. 2023. Vol. 3482. P. 148–168. URL: <https://ceur-ws.org/Vol-3482/paper255.pdf> (дата звернення: 18.04.2026).
10. Bondarchuk O., Balakhtar V., Balakhtar K. Monitoring of the quality of the psychological component of teachers' activity of higher education institutions based on Google Forms. *E3S Web of Conferences*. 2020. Vol. 166. Article 10024. DOI: <https://doi.org/10.1051/e3sconf/202016610024>.



11. Bilynska K., Markova O., Chornobryva N., Kuznietsov Y., Mingli W. The power of digitalization in education: Improving learning with interactive multimedia content. *Amazonia Investiga*. 2024. Vol. 13, № 76. P. 188–201. DOI: <https://doi.org/10.34069/AI/2024.76.04.15>.
12. Sherman M. I., Samchynska Y. B., Kobets V. M. Development of an electronic system for remote assessment of students' knowledge in cloud-based learning environment. *CTE Workshop Proceedings*. 2022. Vol. 9. P. 290–305. DOI: <https://doi.org/10.55056/cte.121>.
13. Jayalakshmi M., Gomathi V. Pervasive health monitoring through video-based activity information integrated with sensor-cloud oriented context-aware decision support system. *Multimedia Tools and Applications*. 2020. Vol. 79, № 5. P. 3699–3712. DOI: <https://doi.org/10.1007/s11042-018-6716-8>.
14. Krylova-Grek Y., Shyshkina M. P. Online learning at higher education institutions in Ukraine: achievements, challenges, and horizons. *Information Technologies and Learning Tools*. 2021. Vol. 85, № 5. P. 163–174. DOI: <https://doi.org/10.33407/itlt.v85i5.4660>.
15. Mishra K. N., Pandey S. C. *Cloud-IoT Technologies in Society 5.0*. Cham: Springer, 2023. 340 p. DOI: <https://doi.org/10.1007/978-3-031-28711-4>.

References:

1. Knysh, I., & Panfilov, Yu. (2025). Vprovadzhennia praktyk informatiino-komunikatsiinykh tekhnolohii u bezpechne osvितnie seredovyshche dlia formuvannia tsinnisnoho stavlennia do zdorovia uchasnykiv osvितnoho protsesu [Implementation of ICT practices in a safe educational environment for forming a value-based attitude to health of participants in the educational process]. *Teoriia i praktyka upravlinnia sotsialnyimi systemamy – Theory and Practice of Social Systems Management*, (1), 109–122. DOI: <https://doi.org/10.20998/2078-7782.2025.1.09>.
2. Chychkan, I. V., Spasitelieva, S. O., & Zhdanova, Yu. D. (2021). Osvitnie seredovyshche dlia formuvannia kultury bezpekovogo povedinky u kiberprostorii pry pidhotovtsi fakhivtsiv z ekonomiky ta upravlinnia [Educational environment for forming a culture of safe behavior in cyberspace in training specialists in economics and management]. *Informatsiini tekhnolohii i zasoby navchannia – Information Technologies and Learning Tools*, 84(4), 354–375. DOI: <https://doi.org/10.33407/itlt.v84i4.3646>.
3. Motsyk, R., Kolomiets, N., & Yashchuk, O. (2025). Vykorystannia khmarnykh servisiv u stvorenni efektyvnoho tsyfrovoho osvितnoho seredovyshcha [Use of cloud services in creating an effective digital educational environment]. *Pedahohichna osvita: teoriia i praktyka – Pedagogical Education: Theory and Practice*, (38), 157–170. DOI: <https://doi.org/10.32626/2309-9763.2025-38-157-170>.
4. Kalmykova, L., Kharchenko, N., & Mysan, I. (2021). Khmarni tekhnolohii u vyshchii osviti: novatsiia chy innovatsiia? [Cloud technologies in higher education: novelty or innovation?]. *Pedahohichni innovatsii: idei, realii, perspektyvy – Pedagogical Innovations: Ideas, Realities, Prospects*, 2(27), 99–111. DOI: [https://doi.org/10.32405/2413-4139-2021-2\(27\)-99-111](https://doi.org/10.32405/2413-4139-2021-2(27)-99-111).
5. Shevchuk, B. V. (2024). Proektuvannia ta vprovadzhennia virtualnoho osvितnoho seredovyshcha informatychnoi pidhotovky maibutnikh pedahohiv profesiinoho navchannia [Design and implementation of a virtual educational environment for training future vocational education teachers]. *Pedahohichna Akademiia: naukovy zapysky – Pedagogical Academy: Scientific Notes*, (13). DOI: <https://doi.org/10.5281/zenodo.14557241>.
6. Havrylenko, O. (2023). Informatychno-tsyfrovi instrumenty ta khmarni tekhnolohii yak innovatsiini zasoby navchalnoi diialnosti vchytelia matematyky [Digital tools and cloud technologies as innovative means of mathematics teacher's educational activity]. *Osvita. Innovatyka. Praktyka – Education. Innovation. Practice*, 11(10), 132–140. DOI: <https://doi.org/10.31110/2616-650X-vol11i10-020>.



7. Glazunova, O. G., Voloshyna, T. V., & Korolchuk, V. I. (2020). Hybrid cloud-oriented learning environment for IT student project teamwork. *Information Technologies and Learning Tools*, 77(3), 114–128. DOI: <https://doi.org/10.33407/itlt.v77i3.3210>.
8. Vakaliuk, T., Antoniuk, D., Morozov, A., Medvedieva, M., & Medvediev, M. (2020). Green IT as a tool for design cloud-oriented sustainable learning environment of a higher education institution. *arXiv preprint*, arXiv:2012.07744. DOI: <https://doi.org/10.48550/arXiv.2012.07744>.
9. Varina, H. B., Osadcha, K. P., Shevchenko, S. V., & Voloshyna, V. V. (2023). Developing professional stability of future socioeconomic specialists using cloud technologies in blended learning. *CEUR Workshop Proceedings*, 3482, 148–168. Retrieved from <https://ceur-ws.org/Vol-3482/paper255.pdf>.
10. Bondarchuk, O., Balakhtar, V., & Balakhtar, K. (2020). Monitoring of the quality of the psychological component of teachers' activity of higher education institutions based on Google Forms. *E3S Web of Conferences*, 166, 10024. DOI: <https://doi.org/10.1051/e3sconf/202016610024>.
11. Bilynska, K., Markova, O., Chornobryva, N., Kuznietsov, Y., & Mingli, W. (2024). The power of digitalization in education: Improving learning with interactive multimedia content. *Amazonia Investiga*, 13(76), 188–201. DOI: <https://doi.org/10.34069/AI/2024.76.04.15>.
12. Sherman, M. I., Samchynska, Y. B., & Kobets, V. M. (2022). Development of an electronic system for remote assessment of students' knowledge in cloud-based learning environment. *CTE Workshop Proceedings*, 9, 290–305. DOI: <https://doi.org/10.55056/cte.121>.
13. Jayalakshmi, M., & Gomathi, V. (2020). Pervasive health monitoring through video-based activity information integrated with sensor-cloud oriented context-aware decision support system. *Multimedia Tools and Applications*, 79(5), 3699–3712. DOI: <https://doi.org/10.1007/s11042-018-6716-8>.
14. Krylova-Grek, Y., & Shyshkina, M. P. (2021). Online learning at higher education institutions in Ukraine: achievements, challenges, and horizons. *Information Technologies and Learning Tools*, 85(5), 163–174. DOI: <https://doi.org/10.33407/itlt.v85i5.4660>.
15. Mishra, K. N., & Pandey, S. C. (2023). *Cloud-IoT Technologies in Society 5.0*. Cham: Springer. DOI: <https://doi.org/10.1007/978-3-031-28711-4>.

Дата першого надходження статті до видання: 21.04.2026

Дата прийняття статті до друку після рецензування: 05.05.2026

