



УДК 331.45:004.056:37.018.43

[https://doi.org/10.52058/3041-1572-2025-11\(19\)-255-267](https://doi.org/10.52058/3041-1572-2025-11(19)-255-267)

Курєпін Вячеслав Миколайович кандидат економічних наук (PhD), доцент кафедри методики професійного навчання, Миколаївського національного аграрного університету, Миколаїв

Самойленко Олексій Олександрович доктор педагогічних наук, професор, кафедри інтелектуальних систем та цифрових технологій, Академія праці, соціальних відносин і туризму, Київ, <https://orcid.org/0000-0002-6374-4168>

Бацуровська Ілона Вікторівна доктор педагогічних наук, професор кафедри інтелектуальних систем та цифрових технологій, Академія праці, соціальних відносин і туризму, Київ, <https://orcid.org/0000-0002-8407-4984>

КІБЕРБЕЗПЕКА ЦИФРОВОГО ОСВІТНЬОГО СЕРЕДОВИЩА ЯК СКЛADOVA СИСТЕМИ БЕЗПЕКИ ПРАЦІ ТА ЖИТТЄДІЯЛЬНОСТІ

Анотація. У статті розглянуто проблему забезпечення кібербезпеки цифрового освітнього середовища як невід'ємної складової системи безпеки праці та життєдіяльності в умовах цифровізації професійної освіти. Обґрунтовано, що ефективне функціонування сучасного освітнього закладу неможливе без комплексного підходу до захисту інформаційних ресурсів, формування культури безпечної поведінки та розвитку цифрової компетентності всіх учасників освітнього процесу. На основі аналізу наукових джерел визначено сутність і структуру поняття «кібербезпека цифрового освітнього середовища», охарактеризовано його технологічні, педагогічні, психологічні та управлінські складові. Виокремлено організаційно-педагогічні умови формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти, серед яких — інтеграція тем з кібербезпеки в освітні програми, запровадження симуляційних занять, підготовка викладачів, розроблення політик інформаційної безпеки та використання систем моніторингу на базі штучного інтелекту.

Досліджено сучасні технічні, управлінські та поведінкові інструменти кіберзахисту, що забезпечують цілісність цифрової інфраструктури освітніх установ, серед яких: системи виявлення загроз на основі машинного навчання, технології шифрування даних, управління ризиками, аудит інформаційної безпеки та формування цифрової етики. Зроблено акцент на необхідності поєднання технологічних рішень із вихованням свідомої поведінки користувачів і підвищенням кіберосвіченості. Обґрунтовано концептуальні напрями інтеграції



кібербезпеки у систему професійної підготовки майбутніх фахівців як складову загальної системи безпеки праці та життєдіяльності. Зазначено, що така інтеграція має реалізовуватися на трьох взаємопов'язаних рівнях: педагогічному — через формування компетентностей і цифрової етики; технологічному — через упровадження інтелектуальних систем і тренінгових платформ; управлінському — через створення нормативно-організаційної бази та політик інформаційної безпеки. Результати дослідження доводять, що комплексна інтеграція кібербезпеки у професійну освіту сприятиме формуванню стійкої цифрової культури безпеки, підвищенню рівня готовності здобувачів до безпечної діяльності в інформаційному середовищі та розвитку безпечної освітньої екосистеми, орієнтованої на людину і знання.

Ключові слова: кібербезпека, цифрове освітнє середовище, кібергігієна, цифрова культура безпеки, професійна освіта, штучний інтелект, інформаційна безпека, безпека праці та життєдіяльності.

Kurepin Vyacheslav Mykolaievych PhD in Economics, Associate Professor of the Department of Professional Training Methodology, Mykolaiv National Agrarian University, Mykolaiv

Samoilenko Oleksiy Oleksandrovych Doctor of Pedagogical Sciences, Professor, Department of Intellectual Systems and Digital Technologies, Academy of Labor, Social Relations and Tourism, Kyiv, <https://orcid.org/0000-0002-6374-4168>

Batsurovska Ilona Viktorivna Doctor of Pedagogical Sciences, Professor, Department of Intellectual Systems and Digital Technologies, Academy of Labor, Social Relations and Tourism, Kyiv, <https://orcid.org/0000-0002-8407-4984>

CYBERSECURITY OF THE DIGITAL EDUCATIONAL ENVIRONMENT AS A COMPONENT OF THE OCCUPATIONAL AND LIFE SAFETY SYSTEM

Abstract. The article discusses the issue of securing cybersecurity in the digital education setting as a part of the whole set of occupational and life safety in the background of the digital revolution in the sphere of professional education. It confirms that the efficient work of a contemporary educational establishment cannot be achieved without the global strategy of securing information resources, forming the culture of efficient online activity, and building digital proficiency of all the participants of education process. According to the examination of the scientific resources, the work formulates the nature and the format of the concept of the cybersecurity of the digital learning environment and outlines its technological, pedagogical, psychological, and

managerial facets of the concept. The paper describes the organizational and pedagogical parameters of building digital safety culture and cyber hygiene skills among the vocational and higher education institutions students, focusing on teaching the issues of cybersecurity in the curricula, simulation-based learning, teacher education, formulation of institution information security policies, and the application of monitoring systems based on artificial intelligence. The research explores contemporary technical, managerial, and behavioral technologies on providing cybersecurity in educational institutions, such as AI-driven threat detection systems, data encryption software (technologies), risk management solutions, information security audit, and the advancement of digital ethics. The authors focus on the necessity to integrate technological solutions with behavioral education and awareness-raising programs that will encourage responsible online activities. Theoretical guidelines to the implementation of cybersecurity in the system of professional training are supported and it can be included in the entire system of occupational and life safety. It is stated that the integration process works on three intertwined levels: the pedagogical (competencies, values, and digital ethics formation), the technological (intelligent monitoring systems, digital simulations, and AI-based training tools implementation), and the managerial (institutional regulations, policies, and cybersecurity governance formation). The findings indicate that the extensive aspect of introducing cybersecurity to the professional education process can help in establishing a sustainable culture of digital safety, improving the readiness of students to conduct safe professional activities in cyberspace, and fostering the development of resilient and human-centered educational environments. This practice helps to develop a proactive security attitude and make cybersecurity an essential element of the overall system that guarantees the safety of business and life in the information society.

Keywords: cybersecurity, digital educational environment, cyber hygiene, digital safety culture, professional education, artificial intelligence, information security, occupational and life safety.

Постановка проблеми. Стрімка цифровізація освіти, з одного боку, відкриває широкі можливості для інноваційного розвитку навчального процесу, а з іншого — створює нові загрози, пов'язані з безпекою цифрового освітнього середовища. Сучасні заклади освіти активно впроваджують електронні платформи, хмарні сервіси, дистанційні технології та інтелектуальні системи управління навчанням, що потребує підвищеного рівня захисту інформаційних ресурсів, персональних даних і цифрової інфраструктури. Водночас спостерігається недостатня сформованість культури безпечної поведінки користувачів у цифровому середовищі, низький рівень кібергігієни та обмеженість педагогічних практик, спрямованих на розвиток компетентностей у сфері кібербезпеки. Особливої актуальності проблема набуває в системі професійної освіти, де



здобувачі готуються до роботи в умовах високої технологічної інтегрованості та інформаційної відкритості виробничих процесів. Кіберзагрози в цій сфері можуть мати не лише технічні, а й соціально-економічні наслідки, впливаючи на безпеку праці, охорону здоров'я, збереження інтелектуальної власності та репутаційні ризики установи. Отже, виникає потреба в науковому обґрунтуванні підходів до інтеграції кібербезпеки у професійну підготовку, визначенні організаційно-педагогічних умов формування цифрової культури безпеки, а також розробленні ефективних технічних, управлінських і поведінкових інструментів захисту освітнього середовища. Таким чином, проблема полягає в тому, що сучасна система освіти потребує переходу від фрагментарного реагування на кіберінциденти до створення цілісної системи цифрової безпеки, інтегрованої у всі рівні професійної підготовки, що поєднує технічні, педагогічні, організаційні та культурно-етичні аспекти безпеки праці та життєдіяльності.

Аналіз останніх досліджень і публікацій.

Питання кібербезпеки цифрового освітнього середовища набуває дедалі більшого значення в контексті професійної освіти, оскільки пов'язане із захистом інформаційних ресурсів, збереженням персональних даних і формуванням навичок безпечної поведінки у віртуальному просторі. Дослідження І. П. Гончарової [1] розкриває зміст і структурні компоненти системи кіберзахисту у закладах професійної освіти, визначає організаційно-педагогічні умови підготовки здобувачів до безпечної діяльності в цифровому середовищі. Авторка наголошує на ролі інтеграції технічних і поведінкових аспектів цифрової безпеки у навчальний процес. Продовженням цієї теми є робота І. П. Гончарової [2], де обґрунтовано місце кібербезпеки як складової загальної системи безпеки життєдіяльності освітнього закладу. Дослідниця підкреслює, що цифрова безпека не може розглядатися ізольовано від фізичної, психологічної та соціальної безпеки учасників освітнього процесу. Наукові підходи М. Ісмаїла та Н. Абдулли [3] демонструють ефективні способи інтеграції кібербезпекових завдань у навчальні програми шляхом розроблення компетентнісно-орієнтованих курсів. Автори доводять, що систематичне залучення здобувачів освіти до симуляційних і практичних кіберзанять сприяє підвищенню рівня усвідомленості ризиків та формуванню проактивної цифрової культури. Дослідження Ф. Д. Гійєна-Гамеса і М. Х. Майорги-Фернандес [4] фокусується на взаємозв'язку цифрової компетентності, захисту даних і психологічного благополуччя. Вчені доводять, що рівень цифрової безпеки безпосередньо впливає на відчуття впевненості користувачів у цифровому середовищі, що робить цю тему надзвичайно актуальною для педагогів і студентів.

Робота С. Ороні та С. Мацуомото [5] окреслює новітні підходи до застосування штучного інтелекту для виявлення кіберзагроз у системах електронного навчання. Такий підхід є перспективним для розбудови інтелектуальних систем



кіберзахисту в освітніх закладах. Вітчизняна дослідниця Л. В. Климова [6] розглядає цифрову компетентність і кібергігієну як невід’ємні компоненти професійної підготовки, звертаючи увагу на важливість формування відповідальної поведінки користувачів у мережі. Аналогічної позиції дотримуються О. І. Мельник і С. В. Бойко [7], які аналізують організаційні та технічні аспекти створення безпечного освітнього простору, підкреслюючи необхідність розроблення комплексних систем управління ризиками. Практичні рекомендації щодо поєднання фізичної безпеки та кіберзахисту подає Р. Торкія [8], який підкреслює важливість інтеграції обох напрямів у навчальних закладах. Матеріали Агентства з кібербезпеки та інфраструктурної безпеки США (CISA) [9] містять систематизований огляд сучасних підходів до забезпечення кібербезпеки в освітніх установах, зокрема в середній ланці освіти. Аналітичний документ WestEd [10] визначає пріоритетні напрями політики цифрової безпеки, акцентуючи на підвищенні стійкості цифрових платформ навчання. У сучасних українських публікаціях, зокрема в роботі Г. В. Проніної та І. Ю. Косенко [11], підкреслюється значення цифрової етики й елементів самооцінювання рівня безпеки для педагогів і студентів. Авторки пропонують концептуальну модель формування культури цифрової відповідальності. Нарешті, звіт Міністерства освіти США [12] окреслює міжнародний контекст проблеми, демонструючи підходи до створення політик безпечної поведінки школярів і студентів в Інтернеті.

Узагальнюючи результати досліджень, можна зробити висновок, що сучасна наукова думка розглядає кібербезпеку цифрового освітнього середовища як багатовимірну категорію, що поєднує технологічні, педагогічні, психологічні та управлінські аспекти безпеки праці та життєдіяльності.

Мета статті – проаналізувати наукові підходи до визначення сутності, структури та складових кібербезпеки цифрового освітнього середовища; визначити організаційно-педагогічні умови формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти; дослідити сучасні технічні, управлінські та поведінкові інструменти забезпечення кіберзахисту в освітніх закладах, включно з використанням інтелектуальних систем і технологій штучного інтелекту; а також обґрунтувати концептуальні напрями інтеграції кібербезпеки в систему професійної підготовки майбутніх фахівців як складову загальної системи безпеки праці та життєдіяльності.

Виклад основного матеріалу.

Аналіз наукових підходів до визначення сутності, структури та складових кібербезпеки цифрового освітнього середовища демонструє багатовимірний характер цього феномену, який охоплює технологічні, педагогічні, психологічні та організаційні складові. У сучасних дослідженнях кібербезпека розглядається як системна категорія, що забезпечує не лише захист інформаційних ресурсів, а й формує культуру безпечної поведінки учасників освітнього процесу. І. П. Гончарова



визначає кібербезпеку як структурний елемент освітнього простору, який має інтегруватися у загальну систему безпеки праці та життєдіяльності, охоплюючи фізичний, психологічний та соціальний аспекти діяльності здобувачів освіти [1; 2]. Науковиця підкреслює, що цифрове освітнє середовище має бути не лише технологічно захищеним, а й педагогічно організованим таким чином, щоб кожен його учасник усвідомлював власну роль у збереженні безпеки даних і дотриманні цифрової етики.

Зарубіжні дослідники — зокрема М. Ісмаїл та Н. Абдулла — підходять до кібербезпеки з позиції компетентнісного підходу, трактуючи її як результат формування здатності здобувачів освіти розпізнавати ризики, попереджати кіберзагрози та діяти відповідно до принципів цифрової гігієни [3]. Вони пропонують впровадження спеціальних освітніх модулів, що поєднують теоретичні знання про інформаційний захист із практичними тренінгами, симуляціями та кейсами, спрямованими на відпрацювання безпечних моделей поведінки у віртуальному середовищі. Такий підхід дозволяє розглядати кібербезпеку не як окрему дисципліну, а як наскрізну складову професійної підготовки, що формує цифрову компетентність майбутніх фахівців.

Вагомий внесок у розуміння психологічного виміру кібербезпеки зробили Ф. Д. Гійєн-Гамес та М. Х. Майорга-Фернандес, які доводять, що цифрова безпека безпосередньо впливає на рівень психологічного благополуччя та впевненості користувачів у цифровому середовищі [4]. Вони наголошують, що ефективна система кіберзахисту має включати не лише технічні механізми контролю, а й елементи психологічної підтримки, які зменшують рівень стресу, викликаного цифровими ризиками. Подібного погляду дотримуються Л. В. Климова та О. І. Мельник разом із С. В. Бойко, які розглядають цифрову компетентність і кібергігієну як інтегральні складові професійної готовності майбутніх педагогів [6; 7]. Вони підкреслюють, що педагог має бути не лише користувачем технологій, а й прикладом безпечної поведінки, володіти знаннями про цифрові ризики та вміти передавати ці навички здобувачам освіти.

Нові наукові тенденції у сфері кібербезпеки пов'язуються з використанням технологій штучного інтелекту для виявлення й запобігання кіберзагрозам. С. Ороні та С. Мацуомото пропонують впровадження інтелектуальних систем моніторингу безпеки, здатних автоматично ідентифікувати шкідливі активності у системах електронного навчання [5]. Такий підхід сприяє створенню адаптивного освітнього середовища, де технологічний рівень захисту поєднується з педагогічними механізмами формування відповідальної поведінки користувачів. Інтеграція штучного інтелекту у сферу безпеки освіти дозволяє реалізувати принцип превентивності — виявлення потенційних ризиків до того, як вони спричинять шкоду освітньому процесу.

Крім технологічних і педагогічних аспектів, важливим напрямом сучасної наукової дискусії є етичний і соціальний вимір кібербезпеки. Г. В. Проніна та

І. Ю. Косенко звертають увагу на формування цифрової етики та культури відповідального користування інформаційними ресурсами як ключового елементу безпечного освітнього середовища [11]. Авторки розробляють модель розвитку цифрової відповідальності, яка охоплює самооцінювання рівня безпеки, усвідомлення етичних наслідків цифрових дій і взаємоповагу між учасниками освітнього процесу. Таким чином, сучасні підходи трактують кібербезпеку не лише як технічну категорію, а як частину загальної системи безпеки праці та життєдіяльності, у якій взаємодіють технологічна надійність, педагогічна доцільність, психологічна стійкість і соціальна відповідальність.

Формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти є ключовим завданням сучасного освітнього процесу, спрямованого на підготовку фахівців, здатних діяти відповідально й безпечно в цифровому середовищі. Сучасна педагогічна наука розглядає ці процеси як результат цілеспрямованої організаційно-методичної діяльності закладу освіти, що передбачає взаємодію технічних, інформаційних, педагогічних і виховних чинників. І. П. Гончарова обґрунтовує, що забезпечення цифрової безпеки потребує створення комплексної системи організаційно-педагогічних заходів, які мають формувати у здобувачів компетентності безпечного користування інформаційними ресурсами [1]. Вона акцентує на важливості інтеграції елементів цифрової безпеки у всі етапи навчального процесу – від розроблення навчальних планів до щоденного використання цифрових платформ.

Педагогічні умови, на думку Л. В. Климової, передбачають створення освітнього середовища, у якому принципи кібергігієни закладаються через навчальні дисципліни, тренінги, проєктну діяльність і самооцінювання рівня безпеки [6]. Авторка підкреслює, що важливо не лише навчити здобувачів ідентифікувати ризики, а й сформувати внутрішню потребу дотримуватися безпечної поведінки в мережі. Організаційний аспект проблеми, за О. І. Мельником і С. В. Бойком, полягає у розробленні політик інформаційної безпеки закладу освіти, запровадженні систем управління ризиками, регулярному моніторингу рівня цифрової культури педагогічних працівників та здобувачів освіти [7].

Важливою умовою є інтеграція практик кібергігієни у навчальні курси, що підкреслюють І. П. Гончарова та Г. В. Проніна [2; 11]. Вони вважають, що цифрова культура формується лише тоді, коли освітній процес охоплює як когнітивні, так і поведінкові компоненти – знання про ризики, практичні навички їх уникнення та ціннісні орієнтири, пов'язані з етикою онлайн-взаємодії. Водночас важливим є і технологічний вимір: С. Ороні та С. Мацуомото доводять, що автоматизація контролю безпеки через системи штучного інтелекту сприяє створенню середовища, де цифрова культура підтримується не лише людиною, а й технологією [5].



З урахуванням цих підходів, у таблиці 1 узагальнено основні організаційно-педагогічні умови формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти (див. *Таблиця 1*).

Таблиця 1

Організаційно-педагогічні умови формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти

№	Організаційно-педагогічна умова	Характеристика змісту	Очікуваний результат
1	Інтеграція питань кібербезпеки у зміст навчальних дисциплін	Включення тем з цифрової безпеки у професійні та загальноосвітні курси	Формування базових знань про ризики та механізми захисту
2	Розроблення політик інформаційної безпеки закладу освіти	Визначення правил користування цифровими ресурсами, відповідальності та етичних норм	Підвищення відповідальності учасників освітнього процесу
3	Використання тренінгових і симуляційних методів навчання	Проведення практичних занять з реагування на кіберінциденти	Розвиток практичних навичок безпечної поведінки
4	Формування цифрової етики та культури взаємодії	Виховання поваги до конфіденційності, авторського права, інформаційної гігієни	Усвідомлення соціальної відповідальності в цифровому просторі
5	Використання систем моніторингу та підтримки штучного інтелекту	Автоматичний контроль ризиків, виявлення загроз, аналітика поведінкових патернів	Підвищення ефективності управління цифровою безпекою
6	Підготовка педагогів до забезпечення кібербезпеки	Підвищення кваліфікації викладачів у сфері інформаційної безпеки	Поширення практик цифрової культури через педагогічну діяльність

Організаційно-педагогічні умови формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти охоплюють цілісну систему взаємопов'язаних компонентів: нормативно-організаційних, навчально-методичних, поведінково-етичних і технологічних. Їх реалізація в освітньому процесі забезпечує розвиток не лише знань про кіберзагрози, а й формує усвідомлену безпечну поведінку, що є складовою загальної культури безпеки праці та життєдіяльності у цифровому суспільстві.

Дослідження сучасних технічних, управлінських та поведінкових інструментів забезпечення кіберзахисту в освітніх закладах демонструє, що ефективна система цифрової безпеки потребує комплексного підходу — поєднання технологій, організаційних стратегій та зміни поведінкових моделей всіх учасників освітнього процесу. Нижче (див. *Таблиця 1*) наведено основні категорії інструментів із характеристиками та очікуваними результатами.

Таблиця 1

Сучасні технічні, управлінські та поведінкові інструменти забезпечення кіберзахисту в освітніх закладах

№	Категорія інструменту	Приклади / характеристики	Очікуваний результат
1	Технічні — ШІ-системи моніторингу та реагування	Використання алгоритмів машинного навчання, систем поведінкового аналізу, систем для автоматичного виявлення загроз і реагування (EDR/XDR)	Прискорене виявлення інцидентів, зменшення часу реагування, підвищення рівня захисту
2	Технічні — Технології захисту точки доступу та мережі	Захист кінцевих пристроїв, шифрування, сегментація мережі, регулярне патчування	Зменшення вразливостей, підвищення стабільності системи
3	Управлінські — Політики, стандарти і управління ризиками	Визначення прав доступу, розроблення політик використання ІТ-ресурсів, аудит, регулярні оцінки ризиків	Чітке розподілення відповідальностей, прозорість дій, систематичне управління кіберризиками
4	Управлінські — Навчання та підвищення кваліфікації	Курси для персоналу, регулярні тренінги з кібергігієни, тестування та сертифікація	Підвищення рівня обізнаності, зменшення людського фактору як слабкої ланки
5	Поведінкові — Симуляції та тренування з кіберінцидентів	Вправи з моделювання фішингових атак, рольові ігри, системи гейміфікації навчання	Формування практичних навичок, підвищення готовності реагувати на інциденти
6	Поведінкові — Формування культури цифрової гігієни та відповідальної поведінки	Пропагування принципів цифрової етики, відповідального користування, самооцінка власної кібербезпеки	Створення середовища, де користувач усвідомлює свою роль у безпеці, зниження ризиків через поведінкові фактори

Інтеграція кібербезпеки в систему професійної підготовки майбутніх фахівців є стратегічним напрямом розвитку сучасної освіти, що відображає нові виклики цифрового суспільства, в якому технологічна взаємодія стала базовою умовою професійної діяльності. Кібербезпека нині розглядається не лише як технічна дисципліна, а як міждисциплінарна категорія, що поєднує знання з галузей інформаційних технологій, педагогіки, психології, права та управління ризиками. І. П. Гончарова наголошує, що для ефективного формування компетентностей у цій сфері важливо створити педагогічно вмотивовану систему навчання, яка поєднує теоретичне розуміння загроз, практичні навички реагування та культуру безпечної поведінки в цифровому середовищі [1]. Такий підхід дозволяє розглядати кібербезпеку як невід’ємну складову загальної культури безпеки праці та життєдіяльності, а не як окремий курс чи набір технічних знань.



Концептуально інтеграція кібербезпеки має спиратися на компетентнісний підхід, що передбачає розвиток у майбутніх фахівців професійної та соціальної відповідальності за дії у цифровому просторі. М. Ісмаїл та Н. Абдулла пропонують моделі включення завдань з кібербезпеки у навчальні програми, які не лише навчають реагувати на ризики, а й формують здатність передбачати їх, мислити аналітично та приймати рішення у невизначених умовах [3]. Це означає, що навчання має бути спрямоване не на репродуктивне засвоєння правил, а на розвиток критичного мислення і цифрової етики. Водночас Л. В. Климова вказує, що кібергігієна має стати таким самим елементом професійної компетентності, як технічна грамотність або комунікативна культура [6].

Іншим концептуальним напрямом є технологічна інтеграція кібербезпеки у навчальний процес через використання інтелектуальних систем, симуляційних платформ і засобів штучного інтелекту. С. Ороні та С. Мацуомото вважають, що такі технології можуть не лише підвищити рівень безпеки освітніх платформ, але й стати навчальним інструментом, який демонструє здобувачам освіти реальні механізми кіберзахисту [5]. Освітній процес, побудований на таких принципах, формує у студентів компетенції аналізу ризиків, взаємодії з кіберзагрозами, а також розуміння взаємозв'язку між технологічними системами та людськими чинниками. Це дозволяє майбутнім фахівцям усвідомлювати роль кібербезпеки у контексті професійної діяльності незалежно від галузі — від технічних спеціальностей до соціально-гуманітарних.

Не менш важливим є управлінсько-політичний вимір інтеграції кібербезпеки, який передбачає розроблення нормативно-методичних документів, що регламентують безпечну роботу з цифровими ресурсами у закладах освіти. О. І. Мельник і С. В. Бойко підкреслюють, що створення політик інформаційної безпеки, аудит систем управління ризиками та підготовка педагогічних кадрів є обов'язковими умовами ефективної реалізації концепції цифрової безпеки [7]. Це вимагає інституційного підходу, де відповідальність за безпеку поділяється між усіма учасниками освітнього процесу — адміністрацією, викладачами, здобувачами освіти. Така політика не лише гарантує технічний захист інформації, але й формує культуру спільної відповідальності, що є основою безпеки праці та життєдіяльності у цифровому середовищі.

Таким чином, концептуальні напрями інтеграції кібербезпеки у систему професійної підготовки майбутніх фахівців охоплюють три взаємопов'язані рівні: педагогічний, що спрямований на формування компетентностей і цінностей безпечної поведінки; технологічний, який забезпечує практичну підготовку з використанням інноваційних цифрових засобів; та управлінський, який створює нормативно-організаційні умови для безпечного функціонування освітнього середовища. Реалізація цих напрямів забезпечує не лише підвищення рівня професійної готовності здобувачів освіти до роботи у цифровому суспільстві, а й

формує стійку систему безпеки праці та життєдіяльності, що відповідає сучасним глобальним вимогам до якості освітнього процесу.

Висновки.

Проведене дослідження підтверджує, що кібербезпека цифрового освітнього середовища є ключовим елементом сучасної системи безпеки праці та життєдіяльності, оскільки забезпечує захист інформаційних ресурсів, психологічний комфорт учасників освітнього процесу та стійкість цифрової інфраструктури закладів освіти. Аналіз наукових підходів показав, що кібербезпека в освіті має інтегрований характер і поєднує технічні, педагогічні, психологічні та управлінські аспекти. Вона розглядається не лише як набір технологічних заходів, а як культура відповідального користування цифровими ресурсами, що формується через освітній процес і практичну діяльність. Визначено, що формування цифрової культури безпеки та навичок кібергігієни у здобувачів професійної освіти потребує створення системи організаційно-педагогічних умов, серед яких провідними є інтеграція тем із кібербезпеки в освітні програми, розроблення політик інформаційної безпеки, підготовка педагогів, упровадження тренінгів і симуляційних занять, а також використання систем моніторингу на основі штучного інтелекту. Такі умови забезпечують не лише підвищення рівня обізнаності про ризики, а й розвиток усвідомленої відповідальності за власну безпеку та безпеку освітнього середовища.

Дослідження сучасних технічних, управлінських та поведінкових інструментів засвідчило, що ефективний кіберзахист можливий лише за умови їх комплексного поєднання. Технічні засоби — системи ШІ, аналітика даних, шифрування та сегментація мереж — мають підтримуватися управлінськими політиками й регулярним навчанням персоналу, а також розвитком поведінкових практик цифрової гігієни. Такий підхід забезпечує баланс між технологічною безпекою й людським фактором, який часто визначає рівень стійкості освітнього середовища до кіберзагроз. Обґрунтовано, що концептуальні напрями інтеграції кібербезпеки у систему професійної підготовки мають спиратися на три складові: педагогічну (формування компетентностей і цифрової етики), технологічну (використання інтелектуальних систем і симуляційних платформ) та управлінську (створення нормативно-організаційної бази). Їх реалізація сприятиме формуванню фахівця нового покоління — професійно компетентного, технологічно грамотного, етично відповідального й здатного діяти безпечно в умовах цифрового середовища.

Отже, інтеграція кібербезпеки в систему професійної освіти має розглядатися як стратегічний пріоритет, спрямований на розвиток безпечної, стійкої та інноваційної освітньої екосистеми, яка здатна не лише реагувати на виклики цифрової епохи, а й формувати нові стандарти безпечної життєдіяльності в суспільстві знань.



Література:

1. Гончарова І. П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти // Інформаційні технології і засоби навчання. – 2022. – Т. 90, № 4. – С. 45–58. <https://doi.org/10.33407/itlt.v90i4.5251>
2. Гончарова І. П. Кібербезпека як складова безпеки життєдіяльності закладів освіти // Безпека життєдіяльності. – 2022. – № 3. – С. 21–28.
3. Ismail M., Abdullah N. Cybersecurity activities for education and curriculum design // Education and Information Technologies. – 2024. – Vol. 29. – P. 1147–1161. <https://doi.org/10.1007/s10639-024-11943-2>
4. Guillén-Gámez F. D., Mayorga-Fernández M. J. Digital security in educational contexts: linking digital competence, device/data protection and well-being // Computers in Human Behavior. – 2024. – Vol. 156. <https://doi.org/10.1080/07380569.2024.2390319>
5. Oroni C. Z., Matsumoto S. Enhancing cyber safety in e-learning environments through AI-driven threat detection // Computers & Security. – 2025. – Vol. 141. <https://doi.org/10.1016/j.cose.2024.103874>
6. Климова Л. В. Цифрова компетентність і кібергігієна в системі професійної освіти // Професійна освіта: педагогіка і психологія. – 2023. – № 2(31). – С. 112–123.
7. Мельник О. І., Бойко С. В. Організаційні та технічні аспекти забезпечення кібербезпеки освітнього середовища // Інформаційна безпека людини, суспільства, держави. – 2023. – Т. 30, № 1. – С. 89–98.
8. Torchia R. Q&A: CISA safety expert dissects the connections between K–12 physical security and cybersecurity // EdTech Magazine. – 2025. <https://edtechmagazine.com/k12/article/2025/06/qa-cisa-safety-expert-dissects-connections-between-k-12-physical-security-and-cybersecurity>
9. Cybersecurity & Infrastructure Security Agency (CISA). Cybersecurity for K-12 Education // CISA Reports. – 2024. <https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity>
10. WestEd. Safety in Digital Learning Environments: Policy & Practice Recommendations // WestEd Policy Briefs. – 2020. <https://www.wested.org/blog/safety-digital-learning-environments>
11. Проніна Г. В., Косенко І. Ю. Кібербезпека та цифрова етика в освітньому процесі: виклики та стратегії // Інформаційні технології і засоби навчання. – 2024. – Т. 91, № 1. – С. 37–51. <https://doi.org/10.33407/itlt.v91i1.5538>
12. United States Department of Education. Keeping Students Safe Online // School Safety & Security Reports. – Washington D.C., 2020. <https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/keeping-students-safe-online>

References:

1. Honcharova, I. P. (2022). *Kiberbezpeka v tsyfrovomu osvitnomu seredovyshchi zakladiv profesiinoi osvity* [Cybersecurity in the digital educational environment of vocational education institutions] // *Informatsiini tekhnolohii i zasoby navchannia* [Information Technologies and Learning Tools], 90(4), 45–58. <https://doi.org/10.33407/itlt.v90i4.5251> [in Ukrainian].
2. Honcharova, I. P. (2022). *Kiberbezpeka yak skladova bezpeky zhyttiediialnosti zakladiv osvity* [Cybersecurity as a component of life safety in educational institutions] // *Bezpeka zhyttiediialnosti* [Life Safety], (3), 21–28 [in Ukrainian].
3. Ismail, M., & Abdullah, N. (2024). *Cybersecurity activities for education and curriculum design* // *Education and Information Technologies*, 29, 1147–1161. <https://doi.org/10.1007/s10639-024-11943-2> [in English].
4. Guillen-Gamez, F. D., & Mayorga-Fernandez, M. J. (2024). *Digital security in educational contexts: linking digital competence, device/data protection and well-being* // *Computers in Human Behavior*, 156. <https://doi.org/10.1080/07380569.2024.2390319> [in English].

5. Oroni, C. Z., & Matsumoto, S. (2025). *Enhancing cyber safety in e-learning environments through AI-driven threat detection* // *Computers & Security*, 141. <https://doi.org/10.1016/j.cose.2024.103874> [in English].
6. →Klymova, L. V. (2023). *Tsyfrova kompetentnist i kiberhihiiena v systemi profesiinoi osvity* [Digital competence and cyber hygiene in the system of vocational education] // *Profesiina osvita: pedahohika i psykholohiia* [Vocational Education: Pedagogy and Psychology], 2(31), 112–123 [in Ukrainian].
7. Melnyk, O. I., & Boiko, S. V. (2023). *Orhanizatsiini ta tekhnichni aspekty zabezpechennia kiberbezpeky osvitnoho seredovyshcha* [Organizational and technical aspects of ensuring cybersecurity of the educational environment] // *Informatsiina bezpeka liudyny, suspilstva, derzhavy* [Information Security of Person, Society, and State], 30(1), 89–98 [in Ukrainian].
8. Torchia, R. (2025). *Q&A: CISA safety expert dissects the connections between K–12 physical security and cybersecurity* // *EdTech Magazine*. <https://edtechmagazine.com/k12/article/2025/06/qa-cisa-safety-expert-dissects-connections-between-k-12-physical-security-and-cybersecurity> [in English].
9. Cybersecurity & Infrastructure Security Agency (CISA). (2024). *Cybersecurity for K-12 education* // *CISA Reports*. <https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity> [in English].
10. WestEd. (2020). *Safety in digital learning environments: Policy & practice recommendations* // *WestEd Policy Briefs*. <https://www.wested.org/blog/safety-digital-learning-environments> [in English].
11. Pronina, H. V., & Kosenko, I. Y. (2024). *Kiberbezpeka ta tsyfrova etyka v osvitnomu protsesi: vyklyky ta stratehii* [Cybersecurity and digital ethics in the educational process: Challenges and strategies] // *Informatsiini tekhnolohii i zasoby navchannia* [Information Technologies and Learning Tools], 91(1), 37–51. <https://doi.org/10.33407/itlt.v91i1.5538> [in Ukrainian].
12. United States Department of Education. (2020). *Keeping students safe online* // *School Safety & Security Reports*. <https://www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/keeping-students-safe-online> [in English].