ВІСНИК науки та освіти
ISSN 2786-6165 (ONLINE) № 5(47) 2026
Bulletin of Science and Education

УДК: 377.091.3:004.056:004.77

https://doi.org/10.52058/2786-6165-2026-5(47)-2519-2537

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

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

КІБЕРБЕЗПЕКА ЯК СКЛАДНИК ЦИФРОВОЇ КОМПЕТЕНТНОСТІ ЗДОБУВАЧІВ ПРОФЕСІЙНОЇ ОСВІТИ В УМОВАХ ЗМІШАНОГО НАВЧАННЯ

Анотація. У статті обґрунтовано актуальність розгляду кібербезпеки як невід'ємного складника цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання. Акцентовано, що цифровізація освітнього процесу, активне використання електронних платформ, онлайн-сервісів, хмарних технологій, мережевих ресурсів і засобів дистанційної комунікації посилюють потребу у формуванні в здобувачів не лише технічних умінь роботи з цифровими інструментами, а й навичок безпечної, критичної та відповідальної поведінки в цифровому середовищі. Розкрито теоретичні підходи до визначення кібербезпеки як комплексної характеристики цифрової компетентності, що охоплює знання про кіберзагрози, уміння захищати персональні дані, здатність критично оцінювати цифровий контент, дотримуватися правил цифрової етики, академічної доброчесності та кібергігієни. Визначено основні кіберзагрози, з якими стикаються здобувачі професійної освіти під час використання цифрових освітніх платформ і мережевих ресурсів, зокрема фішингові атаки, несанкціонований доступ до облікових записів, шкідливе програмне забезпечення, порушення конфіденційності персональних даних, кібербулінг, недостовірний цифровий контент, небезпечне використання хмарних сервісів і ризики, пов'язані з генеративним штучним інтелектом. Охарактеризовано можливості змішаного навчання для розвитку практичних умінь здобувачів щодо налаштування приватності, створення надійних паролів, перевірки джерел інформації, безпечної онлайн-комунікації та відповідального використання інформаційних технологій у навчальній і майбутній професійній діяльності. Узагальнено методичні підходи до інтеграції

елементів кібербезпеки в освітній процес закладів професійної освіти, серед яких виокремлено кейс-метод, проблемне навчання, симуляційні вправи, адаптивні цифрові середовища, міждисциплінарні завдання та практичні тренінги з кібергігієни. Запропоновано практичні рекомендації щодо формування кібербезпечної поведінки здобувачів професійної освіти.

Ключові слова: кібербезпека, цифрова компетентність, здобувачі професійної освіти, змішане навчання, цифрове освітнє середовище, кібергігієна, персональні дані, цифрова безпека, онлайн-сервіси, інформаційні технології.

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

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

CYBERSECURITY AS A COMPONENT OF DIGITAL COMPETENCE OF VOCATIONAL EDUCATION STUDENTS IN BLENDED LEARNING ENVIRONMENTS

The article confirms the need to include cybersecurity as part of the digital competences of the students of vocational education in blended learning. It is underlined that the digitalisation of the educational process, the active use of learning management systems, online services, cloud technologies, network resources and tools for distance communication places a new demand on developing both students' technical skills in using the digital tools and their ability to act safely, critically and responsibly in the digital environment. The study reveals theoretical approaches to defining cybersecurity as a complex component of digital competence, which includes knowledge of cyber threats, skills in protecting personal data, the ability to critically evaluate digital content, and readiness to follow the principles of digital ethics, academic integrity and cyber hygiene. The key cyber risks for vocational education students in the context of digital learning platforms, online services and resources on the network are outlined. These comprise malware, unauthorised access to accounts, phishing, breach of confidentiality of personal data, cyberbullying, digital content reliability and risks posed by the use of generative artificial intelligence. The article reflects the potential of blended learning in developing practical skills of students in the field of privacy settings, safe management of personal passwords, recognition of

suspicious links and messages, verification of information sources, safe communication in the Internet and responsible use of information technologies in learning and future work tasks. The methodology approaches of introducing cybersecurity components into the teaching of vocational education institutions educational process are presented, such as: case-based learning, problem-based learning, simulation tasks, adaptive digital environments, interdisciplinary assignments and practical training in cyber hygiene. It is suggested that cybersecurity should not be presented as a separate topic, but should be part of a whole professional training aimed at equipping students with the skills needed to function safely in digital environments in learning and work. Practical suggestions for creating cyber secure behavior of vocational education students in blended learning are offered.

Keywords: cybersecurity, digital competence, vocational education students, blended learning, digital educational environment, cyber hygiene, personal data, digital safety, online services, information technologies.

Постановка проблеми.

Цифрова трансформація професійної освіти зумовила активне впровадження змішаного навчання, електронних освітніх платформ, онлайн-сервісів, хмарних технологій і мережевих ресурсів у підготовку здобувачів. Такі зміни розширюють можливості доступу до навчального контенту, індивідуалізації освітньої траєкторії, організації самостійної роботи та формування практичних умінь, необхідних для майбутньої професійної діяльності. Водночас інтенсивне використання цифрового середовища посилює ризики, пов’язані з кіберзагрозами, порушенням конфіденційності персональних даних, фішинговими атаками, недостовірним цифровим контентом, кібербулінгом, несанкціонованим доступом до облікових записів і небезпечним використанням інформаційних технологій. У цих умовах цифрова компетентність здобувачів професійної освіти не може обмежуватися лише технічними навичками роботи з цифровими інструментами, а має включати здатність до безпечної, критичної, етичної та відповідальної поведінки в онлайн-середовищі. Саме тому актуалізується проблема теоретичного обґрунтування кібербезпеки як складника цифрової компетентності здобувачів професійної освіти та визначення методичних підходів до формування кібербезпечної поведінки в умовах змішаного навчання.

Аналіз останніх досліджень і публікацій.

Проблема формування цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання активно розглядається в сучасному науково-педагогічному дискурсі, оскільки цифровізація освіти

змінює зміст, методи, засоби та організаційні форми професійної підготовки. В. Любарець, Г. Кашина, Я. Качан, С. Брезецький, А. Островершенко акцентують увагу на необхідності адаптації професійного розвитку до цифрової трансформації ринку праці, що передбачає оновлення цифрових умінь, здатність до роботи з новими технологіями та готовність до безперервного професійного самовдосконалення [1]. В. Ковальчук розглядає цифровізацію фахової підготовки в закладах професійної освіти як один із ключових викликів сучасної освітньої практики, пов'язаний із необхідністю модернізації змісту навчання, цифрової інфраструктури та педагогічних підходів [11]. У працях Л. Карташової та А. Квятковської обґрунтовано значення змішаного навчання для підготовки майбутніх фахівців, зокрема наголошено на поєднанні аудиторної та дистанційної взаємодії, використанні цифрових платформ, електронних ресурсів і самостійної роботи здобувачів як чинників підвищення якості професійної підготовки [7; 8]. І. Бацуровська, Г. Кашина, О. Макієвський підкреслюють важливість методологічно обґрунтованої розробки дидактичних матеріалів для професійної освіти, що є особливо значущим в умовах інтеграції цифрових інструментів у навчальний процес [5].

Окремий напрям наукових досліджень пов'язаний із формуванням кібербезпекових умінь і створенням безпечного цифрового освітнього середовища. Т. Волошанівська розглядає підвищення якості підготовки фахівців з кібербезпеки в умовах цифрової трансформації освіти, акцентуючи увагу на потребі оновлення змісту навчання, розвитку практичних навичок і готовності здобувачів до роботи в умовах сучасних цифрових ризиків [6]. М. Козир аналізує безпечне освітнє середовище як відповідь на нові виклики, зокрема ті, що виникають унаслідок активного використання онлайн-сервісів, мережевої комунікації та цифрових ресурсів [9]. Зарубіжні дослідники П. Седа, Я. Викопал, В. Швабенський, П. Челеда обґрунтовують ефективність практико-орієнтованого та адаптивного навчання для формування навичок кібербезпеки, зокрема через інтерактивні середовища, тренувальні завдання й моделювання реальних кіберситуацій [3; 4]. К. Патель, Й.-З. Лін, Г. Раул, Б. П.-Дж. Ших, М. В. Редондо, Б. С. Латібарі, Дж. Пачеко, С. Салехі, П. Сатам розкривають потенціал генеративного штучного інтелекту, OCR-технологій і мультимодальних мовних моделей у навчанні кібербезпеки, що відкриває нові можливості для індивідуалізації освітнього процесу та розвитку практичних умінь здобувачів [2]. Водночас аналіз наукових праць засвідчує, що питання кібербезпеки як складника цифрової компетентності саме здобувачів професійної освіти в умовах змішаного навчання потребує подальшого

системного осмислення, зокрема щодо визначення кіберзагроз, методичних підходів до інтеграції елементів кібербезпеки в освітній процес і формування кібербезпечної поведінки здобувачів.

Мета статті – теоретично обґрунтувати кібербезпеку як складник цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання, визначити основні кіберзагрози цифрового освітнього середовища та розкрити методичні підходи до формування кібербезпечної поведінки здобувачів у процесі використання цифрових освітніх платформ, онлайн-сервісів і мережевих ресурсів.

Виклад основного матеріалу.

Аналіз теоретичних підходів до визначення кібербезпеки як складника цифрової компетентності здобувачів професійної освіти дає підстави стверджувати, що це поняття доцільно розглядати не лише як сукупність технічних знань про захист інформації, а як інтегровану характеристику особистості здобувача, яка охоплює знання, практичні навички, ціннісні орієнтації та відповідальну поведінку в цифровому середовищі. У контексті професійної освіти кібербезпека набуває особливого значення, оскільки здобувачі активно використовують цифрові платформи, хмарні сервіси, електронні освітні ресурси, системи дистанційної взаємодії та професійно орієнтоване програмне забезпечення.

Саме тому цифрова компетентність не може обмежуватися лише здатністю працювати з інформаційними технологіями, а має включати усвідомлення ризиків, пов’язаних із захистом персональних даних, безпекою комунікації, критичним оцінюванням цифрового контенту та дотриманням етичних норм онлайн-взаємодії [1; 11].

Перший теоретичний підхід можна визначити як *компетентнісний*. У його межах кібербезпека розглядається як структурний компонент цифрової компетентності, що поєднує когнітивний, операційний і поведінковий аспекти.

Когнітивний аспект передбачає знання про типові кіберзагрози, способи захисту даних, принципи безпечної автентифікації, правила роботи з електронними ресурсами. Операційний аспект пов’язаний із практичними вміннями використовувати паролі, налаштовувати приватність, розпізнавати фішингові повідомлення, перевіряти достовірність джерел, безпечно працювати з файлами та програмами. Поведінковий аспект охоплює відповідальне ставлення до власної цифрової активності, дотримання академічної доброчесності, цифрової етики та правил кібергігієни. Такий підхід узгоджується з позицією В. Любарець, Г. Кашиної, Я. Качана, С. Брезецького, А. Островершенка, які акцентують увагу на необхідності адаптації професійного розвитку до цифрової трансформації ринку праці [1].

Другий підхід можна охарактеризувати як *практико-орієнтований*. Він виходить із того, що кібербезпека формується не стільки через засвоєння теоретичних положень, скільки через виконання практичних завдань, моделювання реальних ситуацій, розв'язання кейсів і тренувальні дії в цифровому середовищі. У цьому контексті важливого значення набувають адаптивні освітні середовища, симуляційні платформи, інтерактивні вправи та завдання, що дають змогу здобувачам професійної освіти відпрацьовувати навички реагування на кіберризики. П. Седа, Я. Викопал, В. Швабенський, П. Челеда підкреслюють значення практичної підготовки у сфері кібербезпеки, зокрема через адаптивне навчання, яке дає змогу індивідуалізувати траєкторію формування відповідних умінь [3]. Близьку позицію простежуємо і в дослідженні Я. Викопала, П. Седи, В. Швабенського, П. Челеди, де обґрунтовано потенціал «розумного» середовища для адаптивного розвитку навичок кібербезпеки [4].

Третій підхід доцільно визначити як *цифрово-педагогічний*. Його сутність полягає в тому, що кібербезпека розглядається як невід'ємна частина організації цифрового та змішаного навчання. В умовах змішаного формату освітній процес відбувається одночасно в аудиторному та онлайн-середовищі, тому здобувач має бути здатним безпечно взаємодіяти з електронними курсами, цифровими платформами, онлайн-комунікацією, спільними документами, відеоконференціями та навчальними застосунками. Л. Карташова та А. Квятковська наголошують, що змішане навчання потребує спеціальної методики підготовки майбутніх фахівців, оскільки воно змінює способи комунікації, організації самостійної роботи й оцінювання результатів навчання [7]. У цьому контексті кібербезпека постає не допоміжним елементом, а обов'язковою умовою якісного й безпечного функціонування цифрового освітнього середовища.

Четвертий підхід можна окреслити як *безпеково-середовищний*. У його межах кібербезпека трактується як складова ширшого поняття безпечного освітнього середовища. Йдеться не лише про технічний захист інформації, а й про створення таких умов навчання, за яких здобувачі почуваються захищеними від інформаційних маніпуляцій, кібербулінгу, шахрайства, несанкціонованого використання персональних даних і шкідливого цифрового контенту.

М. Козир розглядає безпечне освітнє середовище як відповідь на нові виклики сучасної освіти, що особливо актуально в умовах активного використання цифрових технологій [9].

Для професійної освіти цей підхід є важливим тому, що здобувачі мають не лише знати правила цифрової безпеки, а й навчитися застосовувати їх у професійно значущих ситуаціях.

П’ятий підхід можна визначити як *технологічно-інноваційний*. Він пов’язаний із використанням сучасних цифрових інструментів, зокрема штучного інтелекту, мультимодальних систем, автоматизованого аналізу даних, OCR-технологій та інтелектуальних навчальних середовищ для формування кібербезпекових умінь. К. Патель, Й.-З. Лін, Г. Раул, Б. П.-Дж. Ших, М. В. Редондо, Б. С. Латібарі, Дж. Пачеко, С. Салехі, П. Сатам акцентують увагу на можливостях генеративного штучного інтелекту та мультимодальних мовних моделей у навчанні кібербезпеки [2]. Такий підхід є перспективним, оскільки дає змогу створювати інтерактивні навчальні сценарії, автоматизовано аналізувати типові помилки здобувачів, індивідуалізувати навчальні завдання та підвищувати рівень залученості до вивчення питань кібербезпеки.

Водночас важливо враховувати, що технологічні інновації не можуть замінити педагогічно обґрунтованої методики. І. Бацуровська, Г. Кашина, О. Макієвський підкреслюють значення методологічно виваженої розробки дидактичних матеріалів для професійної освіти, що передбачає поєднання змістової, методичної та практичної складових навчання [5]. У контексті формування кібербезпеки це означає, що навчальні матеріали мають не лише інформувати здобувачів про загрози, а й формувати здатність діяти в проблемних цифрових ситуаціях, приймати безпечні рішення, оцінювати ризики та усвідомлювати наслідки власної онлайн-поведінки.

Окремої уваги потребує *професійно-орієнтований підхід*. Він передбачає розгляд кібербезпеки відповідно до майбутньої професійної діяльності здобувачів. Для різних спеціальностей зміст кібербезпекової підготовки може мати різні акценти: для ІТ-напрямів — це захист інформаційних систем, програмування, мережеві технології; для економічних спеціальностей — безпечна робота з фінансовими даними; для технічних професій — захист цифрового обладнання, автоматизованих систем і виробничих платформ. Т. Волошанівська зазначає, що підвищення якості підготовки фахівців із кібербезпеки в умовах цифрової трансформації освіти потребує оновлення змісту, методів і технологій навчання [6]. Отже, кібербезпека як складник цифрової компетентності має формуватися не абстрактно, а з урахуванням професійного профілю здобувача.

З позицій інформатичної підготовки кібербезпека пов’язана також із розумінням алгоритмічних принципів, логіки роботи програм, основ програмування та цифрової обробки інформації. І. Лопатинська, О. Сиротенко, В. Ладиженко розглядають алгоритмізацію та програмування як важливу основу інформатичної підготовки, що сприяє розвитку логічного мислення й розумінню принципів функціонування цифрових систем [10]. Для формування кібербезпеки це має важливе значення, оскільки здобувач,

який розуміє базові принципи роботи цифрових інструментів, краще усвідомлює потенційні ризики, пов'язані з програмним забезпеченням, файлами, мережевими підключеннями та обробкою даних.

Узагальнюючи різні теоретичні підходи, можна стверджувати, що кібербезпека як складник цифрової компетентності здобувачів професійної освіти є багатовимірним педагогічним феноменом. Вона поєднує знання про цифрові ризики, практичні навички захисту інформації, здатність до критичного мислення, культуру безпечної онлайн-комунікації, відповідальне використання цифрових ресурсів і готовність діяти в умовах постійної технологічної трансформації. У системі професійної освіти кібербезпека має формуватися цілеспрямовано, через поєднання теоретичного навчання, практичних завдань, адаптивних цифрових середовищ, професійно орієнтованих кейсів і методично обґрунтованих дидактичних матеріалів [4; 5; 8]. Саме такий комплексний підхід дає змогу розглядати кібербезпеку не як окрему тему, а як необхідний компонент цифрової компетентності сучасного здобувача професійної освіти.

Формування цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання має комплексний характер, оскільки поєднує аудиторну взаємодію, самостійну роботу в цифровому середовищі, використання електронних освітніх ресурсів, онлайн-комунікацію та виконання практико-орієнтованих завдань. У такому форматі здобувач не лише опановує цифрові інструменти, а й навчається відповідально застосовувати їх у професійній діяльності, організовувати власну навчальну траєкторію, критично оцінювати інформацію, дотримуватися правил кібербезпеки та ефективно взаємодіяти з викладачем і одногрупниками в онлайн- та офлайн-середовищах. Змішане навчання створює умови для гнучкого поєднання теоретичної підготовки з практичними діями, що особливо важливо для професійної освіти, орієнтованої на формування прикладних умінь і готовності до роботи в цифровізованому ринку праці [1; 7; 11].

Особливості формування цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання узагальнено в таблиці 1.

Таблиця 1.

Особливості формування цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання

Особливість	**Змістова характеристика**	**Практичне значення для здобувачів професійної освіти**
Поєднання аудиторного та онлайн-навчання	Здобувачі працюють як у традиційному освітньому середовищі, так і на цифрових платформах, використовуючи електронні курси, відеоматеріали, тести, форуми, хмарні сервіси.	Забезпечує гнучкість навчання, розвиває вміння самостійно організовувати роботу та відповідально використовувати цифрові ресурси [7].
Практико-орієнтований характер навчання	Цифрова компетентність формується через виконання професійно спрямованих завдань, кейсів, проєктів, симуляцій і тренувальних вправ.	Дає змогу застосовувати цифрові інструменти не формально, а відповідно до реальних професійних ситуацій [5].
Розвиток самостійності здобувачів	Змішане навчання передбачає значну частку самостійної роботи з електронними матеріалами, цифровими бібліотеками, навчальними платформами та інтерактивними ресурсами.	Формує навички самоорганізації, планування навчальної діяльності, відповідальності за результат і вміння працювати з інформацією.
Формування інформаційної культури	Здобувачі навчаються знаходити, аналізувати, перевіряти, структурувати та використовувати цифрову інформацію.	Сприяє розвитку критичного мислення, уміння відрізняти достовірні джерела від маніпулятивного або недостовірного контенту.
Інтеграція кібербезпекових навичок	У процесі роботи з цифровими платформами здобувачі засвоюють правила захисту персональних даних, безпечної онлайн-комунікації, використання паролів, перевірки файлів і посилань.	Забезпечує формування відповідальної та безпечної поведінки в цифровому освітньому й професійному середовищі [6; 9].
Індивідуалізація навчальної траєкторії	Цифрові платформи дають змогу адаптувати темп, складність і послідовність виконання завдань відповідно до рівня підготовки здобувача.	Підвищує ефективність навчання, дає змогу враховувати індивідуальні освітні потреби та рівень сформованості цифрових умінь [3; 4].

Особливість	Змістова характеристика	Практичне значення для здобувачів професійної освіти
Розвиток комунікативної цифрової взаємодії	Здобувачі використовують електронну пошту, месенджери, відеоконференції, форуми, спільні документи та навчальні платформи для взаємодії з викладачами й одногрупниками.	Формує культуру цифрового спілкування, навички командної роботи, дотримання етичних норм онлайн-комунікації.
Використання інноваційних цифрових інструментів	У змішаному навчанні можуть застосовуватися адаптивні системи, мультимедійні ресурси, інтерактивні завдання, елементи штучного інтелекту та автоматизованого оцінювання.	Сприяє підвищенню мотивації, активізації пізнавальної діяльності та наближенню освітнього процесу до сучасних технологічних умов [2; 4].
Посилення ролі викладача як тьютора й фасилітатора	Викладач не лише передає знання, а й координує цифрову діяльність здобувачів, консультує, супроводжує індивідуальні траєкторії, допомагає оцінювати цифрові ризики.	Забезпечує педагогічний супровід формування цифрової компетентності та запобігає формальному використанню цифрових технологій [5; 8].
Орієнтація на потреби цифрового ринку праці	Зміст цифрової підготовки має відповідати вимогам сучасних професій, у яких цифрові інструменти, автоматизовані системи й онлайн-сервіси стають необхідними для виконання трудових функцій.	Підвищує конкурентоспроможність випускників і їхню готовність до професійної діяльності в умовах цифрової трансформації [1; 11].

Формування цифрової компетентності здобувачів професійної освіти в умовах змішаного навчання ґрунтується на поєднанні технологічної, інформаційної, комунікативної, безпекової та професійно-практичної складових. Його особливість полягає в тому, що здобувачі не лише засвоюють цифрові інструменти, а й навчаються застосовувати їх у реальних або наближених до професійної діяльності ситуаціях. Змішане навчання забезпечує гнучкість освітнього процесу, розширює можливості індивідуалізації, активізує самостійну роботу та водночас потребує

системного педагогічного супроводу. Саме тому цифрова компетентність у професійній освіті має формуватися як цілісна здатність здобувача безпечно, критично, відповідально й продуктивно діяти в цифровому освітньому та професійному середовищі.

Використання цифрових освітніх платформ, онлайн-сервісів і мережевих ресурсів у професійній освіті розширює доступ здобувачів до навчальних матеріалів, інтерактивних завдань, відеокомунікації, хмарних документів і професійно орієнтованих цифрових інструментів. Водночас така активна цифрова взаємодія підвищує вразливість здобувачів до кіберзагроз, пов'язаних із несанкціонованим доступом до персональних даних, фішинговими атаками, шкідливим програмним забезпеченням, маніпулятивним контентом, порушенням конфіденційності та небезпечною онлайн-комунікацією. У контексті змішаного навчання ці загрози набувають особливого значення, оскільки здобувачі значну частину освітньої діяльності виконують самостійно в цифровому середовищі, використовуючи особисті пристрої, відкриті мережі, електронну пошту, месенджери, системи управління навчанням і зовнішні онлайн-сервіси [6; 7; 9].

Основні кіберзагрози, з якими стикаються здобувачі професійної освіти під час використання цифрових освітніх платформ, онлайн-сервісів і мережевих ресурсів, систематизовано в таблиці 2.

Таблиця 2.

Основні кіберзагрози для здобувачів професійної освіти в цифровому освітньому середовищі

Кіберзагроза	**Змістова характеристика**	**Потенційні наслідки для здобувачів професійної освіти**	**Шляхи мінімізації ризиків**
Фішингові атаки	Надсилання підроблених повідомлень, посилань або форм входу, які імітують офіційні освітні платформи, електронну пошту закладу освіти чи сервіси дистанційного навчання.	Втрата доступу до облікових записів, викрадення паролів, персональних даних, навчальних матеріалів або результатів оцінювання.	Перевірка адрес сайтів, використання двофакторної автентифікації, критичне ставлення до підозрілих листів і посилань [6; 9].

Кіберзагроза	Змістова характеристика	Потенційні наслідки для здобувачів професійної освіти	Шляхи мінімізації ризиків
Несанкціонований доступ до облікових записів	Отримання сторонніми особами доступу до особистого кабінету здобувача, електронної пошти, хмарного сховища або навчальної платформи.	Зміна чи видалення навчальних матеріалів, порушення конфіденційності, використання акаунта для шахрайських дій.	Створення складних паролів, регулярна їх зміна, заборона передавання логінів і паролів іншим особам.
Шкідливе програмне забезпечення	Потрапляння вірусів, троянів, шпигунських програм або програм-вимагачів через завантаження файлів, перехід за небезпечними посиланнями чи використання неперевірених ресурсів.	Пошкодження пристроїв, втрата навчальних файлів, блокування доступу до даних, викрадення особистої інформації.	Використання антивірусного захисту, оновлення програмного забезпечення, завантаження матеріалів лише з перевірених джерел [10].
Використання незахищених мереж	Підключення до відкритих Wi-Fi мереж у громадських місцях під час роботи з освітніми платформами, електронною поштою або хмарними сервісами.	Перехоплення даних, доступ сторонніх осіб до логінів, паролів, навчальних матеріалів і персональної інформації.	Уникнення авторизації в освітніх сервісах через відкриті мережі, використання захищених підключень і надійних пристроїв.
Порушення конфіденційності персональних даних	Небезпечне зберігання, передавання або публікація персональної інформації здобувачів у цифровому середовищі.	Розголошення особистих даних, шахрайське використання інформації, психологічний дискомфорт, ризик цифрового переслідування.	Обмеження доступу до персональних даних, налаштування приватності, уважне ставлення до того, які дані публікуються онлайн [9].

Кіберзагроза	Змістова характеристика	Потенційні наслідки для здобувачів професійної освіти	Шляхи мінімізації ризиків
Кібербулінг і небезпечна онлайн-комунікація	Агресивна, принизлива або маніпулятивна взаємодія в чатах, форумах, месенджерах, коментарях чи під час відео-конференцій.	Зниження мотивації до навчання, емоційне напруження, порушення безпечного освітнього середовища.	Дотримання правил цифрової етики, модерація онлайн-взаємодії, своєчасне повідомлення викладача або адміністрації про порушення [9].
Недостовірний або маніпулятивний цифровий контент	Використання неперевірених сайтів, фейкових матеріалів, псевдонавчальних ресурсів, дезінформації або викривлених даних.	Формування хибних знань, помилки у виконанні завдань, зниження якості професійної підготовки.	Розвиток критичного мислення, перевірка джерел, зіставлення інформації з офіційними освітніми матеріалами [1; 5].
Небезпечне використання хмарних сервісів	Збереження навчальних документів, проєктів, презентацій або персональних файлів у хмарних сховищах без належних налаштувань доступу.	Випадкове або навмисне розголошення матеріалів, втрата контролю над документами, порушення академічної доброчесності.	Налаштування рівнів доступу, обмеження прав редагування, регулярна перевірка спільного доступу до файлів.
Ризики використання генеративного штучного інтелекту	Використання ШІ-сервісів для створення текстів, відповідей, коду чи навчальних матеріалів без критичної перевірки результатів.	Отримання помилкової інформації, формальне виконання завдань, порушення академічної доброчесності, залежність від автоматизованих відповідей.	Критичний аналіз результатів ШІ, перевірка фактів, дотримання правил академічної доброчесності й педагогічно обґрунтоване використання ШІ [2].

Кіберзагроза	Змістова характеристика	Потенційні наслідки для здобувачів професійної освіти	Шляхи мінімізації ризиків
Низький рівень цифрової гігієни	Недостатнє розуміння правил безпечної роботи з паролями, файлами, посиланнями, пристроями, програмами та онлайн-сервісами.	Підвищення загальної вразливості здобувача до більшості кіберзагроз, зниження безпеки навчальної та професійної діяльності.	Систематичне формування навичок кібергігієни, проведення практичних занять, тренінгів і ситуаційних вправ [3; 4; 6].
Порушення академічної доброчесності в цифровому середовищі	Несанкціоноване копіювання матеріалів, використання чужих робіт, передавання доступу до акаунтів, виконання завдань сторонніми особами або сервісами.	Зниження якості навчання, формування неправильної професійної поведінки, втрата довіри до результатів оцінювання.	Формування відповідальності, прозорі правила використання цифрових ресурсів, застосування практико-орієнтованих завдань і педагогічний супровід [5; 8].
Технічна вразливість особистих пристроїв	Використання застарілих операційних систем, неліцензійного програмного забезпечення, незахищених смартфонів, ноутбуків або планшетів.	Витік даних, зараження пристроїв, неможливість безпечно працювати з освітніми платформами та професійними програмами.	Регулярне оновлення програм, використання ліцензійного або перевіреного програмного забезпечення, резервне копіювання даних.

Так, основні кіберзагрози, з якими стикаються здобувачі професійної освіти в умовах використання цифрових освітніх платформ, онлайн-сервісів і мережевих ресурсів, пов’язані не лише з технічними ризиками, а й з інформаційною, комунікативною, етичною та поведінковою складовими цифрової діяльності. Найбільш поширеними серед них є фішингові атаки,

несанкціонований доступ до облікових записів, шкідливе програмне забезпечення, порушення конфіденційності персональних даних, кібербулінг, маніпулятивний контент, небезпечне використання хмарних сервісів і ризики, пов'язані з генеративним штучним інтелектом. Для професійної освіти особливо важливо не лише інформувати здобувачів про ці загрози, а й системно формувати в них навички кібергігієни, критичного мислення, безпечної онлайн-комунікації та відповідального використання цифрових інструментів. Саме тому кібербезпека має розглядатися як обов'язковий складник цифрової компетентності здобувачів професійної освіти та як необхідна умова якісного змішаного навчання.

Змішане навчання створює широкі можливості для розвитку практичних умінь здобувачів професійної освіти щодо захисту персональних даних, критичного оцінювання цифрового контенту та відповідального використання інформаційних технологій, оскільки поєднує безпосередню педагогічну взаємодію з самостійною роботою в онлайн-середовищі. В аудиторному форматі викладач може пояснювати базові принципи кібергігієни, демонструвати алгоритми безпечної роботи з цифровими ресурсами, аналізувати типові помилки здобувачів, тоді як онлайн-компонент дає змогу закріпити ці знання через практичні завдання: налаштування приватності, створення надійних паролів, розпізнавання фішингових повідомлень, перевірку джерел інформації, роботу з хмарними сервісами та навчальними платформами. У цьому контексті змішане навчання є ефективним середовищем для формування не лише технічних умінь, а й цифрової відповідальності, оскільки здобувачі навчаються самостійно приймати рішення в реальних або змодельованих кіберситуаціях [3; 4; 7].

Методичні підходи до інтеграції елементів кібербезпеки в освітній процес закладів професійної освіти мають ґрунтуватися на міждисциплінарності, практичній спрямованості, системності та поступовому ускладненні навчальних завдань. Кібербезпека не повинна розглядатися лише як окрема тема в межах інформатики чи цифрових технологій, оскільки в умовах змішаного навчання вона безпосередньо пов'язана з усіма видами освітньої діяльності здобувачів: роботою на електронних платформах, використанням хмарних сервісів, обміном файлами, онлайн-комунікацією, підготовкою проєктів, виконанням тестових завдань і застосуванням професійно орієнтованого програмного забезпечення. Саме тому доцільно впроваджувати елементи кібербезпеки не лише в окремі навчальні модулі, а й у зміст професійно орієнтованих дисциплін, де здобувачі працюють із цифровими інструментами, електронними документами, базами даних, професійними платформами, комунікаційними

сервісами та інформаційними ресурсами. Такий підхід дає змогу формувати в здобувачів не фрагментарні знання про цифрові загрози, а цілісну готовність до безпечної, відповідальної й критичної поведінки в освітньому та майбутньому професійному середовищі.

Ефективними методичними засобами інтеграції кібербезпеки є кейс-метод, проблемне навчання, симуляційні вправи, проєктні завдання, аналіз реальних цифрових ризиків, адаптивне навчання та використання інтерактивних освітніх середовищ, що дають змогу моделювати ситуації, наближені до професійної діяльності [4; 5; 6]. Наприклад, здобувачі можуть аналізувати фішингові повідомлення, оцінювати надійність паролів, визначати ризики відкритого доступу до хмарних документів, перевіряти достовірність онлайн-джерел, розробляти правила безпечної цифрової комунікації або створювати пам'ятки з кібергігієни для навчальної групи. Важливо, щоб такі завдання не мали формального характеру, а були пов'язані з конкретними практичними ситуаціями: захистом навчального акаунта, безпечною передачею файлів, налаштуванням приватності, дотриманням академічної доброчесності, критичним використанням цифрового контенту та відповідальним застосуванням інструментів штучного інтелекту [2; 9]. У цьому контексті викладач виконує роль не лише джерела знань, а й фасилітатора цифрово безпечної поведінки, який спрямовує здобувачів на усвідомлення наслідків власних дій у цифровому середовищі, формує навички самоконтролю, відповідальності та здатності приймати обґрунтовані рішення в умовах потенційних кіберризиків.

Практичні рекомендації щодо формування кібербезпечної поведінки здобувачів професійної освіти в умовах змішаного навчання мають передбачати системне поєднання інформаційної, технічної, етичної та педагогічної складових. Передусім необхідно розробити чіткі правила цифрової поведінки для роботи з освітніми платформами, електронною поштою, месенджерами, відеоконференціями та хмарними сервісами; регулярно проводити короткі тренінги з кібергігієни; включати до навчальних завдань ситуації з виявлення фішингу, перевірки достовірності інформації, захисту персональних даних і безпечного використання цифрових ресурсів. Доцільно також застосовувати чек-листи безпечної роботи в онлайн-середовищі, інструкції щодо налаштування приватності, практичні пам'ятки з використання паролів і двофакторної автентифікації, а також рефлексивні завдання, у яких здобувачі аналізують власну цифрову поведінку. Отже, кібербезпечна поведінка має формуватися не епізодично, а як постійна складова цифрової компетентності здобувача, що забезпечує його готовність до безпечної навчальної, професійної та соціальної взаємодії в цифровому середовищі.

Висновки.

Отже, кібербезпека в умовах змішаного навчання є невід'ємним складником цифрової компетентності здобувачів професійної освіти, оскільки забезпечує їхню здатність безпечно, критично й відповідально діяти в цифровому освітньому та професійному середовищі. У статті обґрунтовано, що формування кібербезпечної поведінки має здійснюватися на основі комплексного поєднання теоретичних знань, практичних умінь, цифрової етики, критичного мислення та навичок захисту персональних даних. Визначено, що основними кіберзагрозами для здобувачів є фішингові атаки, несанкціонований доступ до облікових записів, шкідливе програмне забезпечення, порушення конфіденційності, небезпечна онлайн-комунікація, недостовірний цифровий контент і ризики неусвідомленого використання сучасних інформаційних технологій. Доведено, що змішане навчання створює сприятливі умови для розвитку цифрової компетентності завдяки поєднанню аудиторної взаємодії, самостійної онлайн-роботи, практико-орієнтованих завдань, кейсів, симуляцій і педагогічного супроводу. Перспективним напрямом є системна інтеграція елементів кібербезпеки в освітній процес закладів професійної освіти через міждисциплінарні завдання, тренінги з кібергігієни, адаптивні цифрові середовища та чіткі правила безпечної цифрової поведінки, що сприятиме підготовці здобувачів до ефективної й безпечної професійної діяльності в умовах цифрової трансформації.

Література:

1. Liubarets V., Kashyna G., Kachan Y., Brezetskyi S., Ostrovershenko A. Adapting professional development to the digital transformation of today's job market // Multidisciplinary Science Journal. 2024. Vol. 6. https://doi.org/10.31893/multiscience.2024ss0713

2. Patel K., Lin Y.-Z., Raul G., Shih B.P.-J., Redondo M.W., Latibari B.S., Pacheco J., Salehi S., Satam P. Integrating Generative AI into Cybersecurity Education: A Study of OCR and Multimodal LLM-assisted Instruction : article / K. Patel, Y.-Z. Lin, G. Raul, B.P.-J. Shih, M.W. Redondo, B.S. Latibari, J. Pacheco, S. Salehi, P. Satam. 2025. 9 p.

3. Seda P., Vykopal J., Švábenský V., Čeleda P. Reinforcing Cybersecurity Hands-on Training With Adaptive Learning : article / P. Seda, J. Vykopal, V. Švábenský, P. Čeleda. 2022. 6 p.

4. Vykopal J., Seda P., Švábenský V., Čeleda P. Smart Environment for Adaptive Learning of Cybersecurity Skills : article / J. Vykopal, P. Seda, V. Švábenský, P. Čeleda. – IEEE Transactions on Learning Technologies. 2023. Vol. 16, No. 3. P. 443–456. DOI: 10.1109/TLT.2022.3216345.

5. Бацуровська І. В., Кашина Г. С., Макієвський О. І. Методологічні підходи до розробки дидактичних матеріалів для професійної освіти: Від теорії до практики // Moderní aspekty vědy: XLVIII. Díl mezinárodní kolektivní monografie. Česká republika: Mezinárodní Ekonomický Institut s.r.o., 2024. С. 172–191.

6. Волошанівська Т.В. Підвищення якості підготовки фахівців з кібербезпеки в умовах цифрової трансформації освіти // Педагогічні науки. 2023. № 7. С. 88-94.

7. Карташова Л. М., Квятковська А. О. Змішане навчання: методика підготовки майбутніх фахівців з телекомунікацій : стаття / Л. М. Карташова, А. О. Квятковська // Вісник післядипломної освіти. 2024. Вип. 27(56). С. 55–69. DOI: https://doi.org /10.58442/2218-7650-2024-27(56)-55-69

8. Карташова Л. М., Квятковська А. О. Модель змішаного навчання майбутніх фахівців з телекомунікацій як засіб підвищення рівня професійної підготовки : стаття / Л. М. Карташова, А. О. Квятковська // Педагогіка формування творчої особистості у вищій і загальноосвітній школах. 2023. № 89. С. 99–103. DOI: https://doi.org/ 10.32782/1992-5786.2023.89.19.

9. Козир М.В. Безпечне освітнє середовище: нові виклики та сучасні рішення / М.В. Козир // Вісник Київського університету імені Бориса Грінченка. 2025. Вип. 1. С. 55-62.

10. Лопатинська І.В., Сиротенко О.В., Ладиженко В.П. Інформатика. Основи алгоритмізації і програмування мовою Python : підручник. Київ : КНУ імені Тараса Шевченка, 2022. 320 с.

11. Ковальчук, В.І. Проблеми цифровізації фахової підготовки в закладах професійної освіти // Актуальні проблеми технологічної і професійної освіти: матеріали ІІ Міжнародної науково-практичної конференції (14 травня 2020 р.). Глухів: ГНПУ ім. О. Довженка, 2020. С. 40–43.

References:

1. Liubarets, V., Kashyna, G., Kachan, Y., Brezetskyi, S., & Ostrovershenko, A. (2024). Adapting professional development to the digital transformation of today's job market. Multidisciplinary Science Journal, 6. https://doi.org/10.31893/multiscience.2024ss0713

2. Patel, K., Lin, Y.-Z., Raul, G., Shih, B. P.-J., Redondo, M. W., Latibari, B. S., Pacheco, J., Salehi, S., & Satam, P. (2025). Integrating Generative AI into Cybersecurity Education: A Study of OCR and Multimodal LLM-assisted Instruction. arXiv preprint arXiv:2509.02998.

3. Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2022). Reinforcing Cybersecurity Hands-on Training With Adaptive Learning. arXiv preprint arXiv:2201.01574.

4. Vykopal, J., Seda, P., Švábenský, V., & Čeleda, P. (2023). Smart environment for adaptive learning of cybersecurity skills. IEEE Transactions on Learning Technologies, 16(3), 443–456. https://doi.org/10.1109/TLT.2022.3216345

5. Batsurovska, I. V., Kashyna, H. S., & Makiievskyi, O. I. (2024). Metodolohichni pidkhody do rozrobky dydaktychnykh materialiv dlia profesiinoi osvity: vid teorii do praktyky [Methodological approaches to developing didactic materials for professional education: From theory to practice]. In Moderní aspekty vědy: Volume XLVIII. International collective monograph (pp. 172–191). Česká republika: Mezinárodní Ekonomický Institut s.r.o. [in Ukrainian].

6. Voloshanivska, T. V. (2023). Pidvyshchennia yakosti pidhotovky fakhivtsiv z kiberbezpeky v umovakh tsyfrovoi transformatsii osvity [Improving the quality of cybersecurity specialists' training in conditions of digital transformation of education]. Pedahohichni nauky – Pedagogical Sciences, 7, 88–94 [in Ukrainian].

7. Kartashova, L. M., & Kviatkovska, A. O. (2024). Zmishane navchannia: metodyka pidhotovky maibutnikh fakhivtsiv z telekomunikatsii [Blended learning: Methodology of

training future telecommunications specialists]. Visnyk pisliadyplomnoi osvity – Bulletin of Postgraduate Education, 27(56), 55–69. https://doi.org/10.58442/2218-7650-2024-27(56)-55-69 [in Ukrainian].

8. Kartashova, L. M., & Kviatkovska, A. O. (2023). Model zmishanoho navchannia maibutnikh fakhivtsiv z telekomunikatsii yak zasib pidvyshchennia rivnia profesiinoi pidhotovky [Model of blended learning of future telecommunications specialists as a means to enhance professional training quality]. Pedahohika formuvannia tvorchoi osobystosti u vyshchii i zahalnoosvitnii shkolakh – Pedagogy of the Formation of a Creative Personality in Higher and General Education Schools, 89, 99–103. https://doi.org/10.32782/1992-5786.2023.89.19 [in Ukrainian].

9. Kozyr, M. V. (2025). Bezpechne osvitnie seredovyshche: novi vyklyky ta suchasni rishennia [Safe educational environment: New challenges and modern solutions]. Visnyk Kyivskoho universytetu imeni Borysa Hrinchenka – Bulletin of Borys Grinchenko Kyiv University, 1, 55–62 [in Ukrainian].

10. Lopatynska, I. V., Syrotenko, O. V., & Ladyzhenko, V. P. (2022). Informatyka. Osnovy alhorytmizatsii i prohramuvannia movoiu Python [Informatics. Basics of algorithmization and programming in Python]. Kyiv, Ukraine: KNU imeni Tarasa Shevchenka [in Ukrainian].

11. Kovalchuk, V. I. (2020). Problemy tsyfrovizatsii fakhovoi pidhotovky v zakladakh profesiinoi osvity [Problems of digitalization of vocational training in professional education institutions]. In Aktualni problemy tekhnolohichnoi i profesiinoi osvity – Current issues of technological and vocational education: Proceedings of the II International Scientific and Practical Conference (May 14, 2020) (pp. 40–43). Hlukhiv, Ukraine: HNPU im. O. Dovzhenka [in Ukrainian].

Дата першого надходження статті до видання: 11.05.2026
Дата прийняття статті до друку після рецензування: 25.05.2026