УДК 378.61.004.8
DOI https://doi.org/10.32782/NPU-VOU.2025.4(99).08

Микола МАТВІЄНКО
аспірант кафедри медичної і біологічної фізики та інформатики
Національний медичний університет імені О.О. Богомольця
https://orcid.org/0009-0004-5888-2584

МЕТОДИЧНИЙ АСПЕКТ ФОРМУВАННЯ КОМПЕТЕНТНОСТІ З КІБЕРБЕЗПЕКИ МАГІСТРІВ МЕДИЦИНИ

У статті обґрунтовано один із методичних аспектів формування компетентності з кібербезпеки магістрів медицини у процесі їхньої фахової підготовки. Актуальність дослідження зумовлена зростанням ролі цифрових технологій у системі охорони здоров'я, широким використанням електронних медичних записів, інформаційних систем і дистанційних сервісів, що підвищує ризики порушення конфіденційності та цілісності медичних даних. У цих умовах майбутній лікар має володіти не лише загальними цифровими навичками, а й професійно орієнтованою компетентністю з кібербезпеки. Окреслено дидактичні можливості тематичного блоку для структурування змісту навчання, забезпечення професійної спрямованості завдань і формування стійких практичних умінь кібергігієни. Показано, що використання кейсів, ситуаційних і практико-орієнтованих завдань у межах тематичного блоку сприяє підвищенню відповідальності майбутніх лікарів за безпеку медичної інформації. Наукова новизна статті полягає в обґрунтуванні тематичного блоку як ефективної форми організації навчання для реалізації окремого методичного аспекту формування компетентності з кібербезпеки магістрів медицини.

Ключові слова: компетентність із кібербезпеки, медична освіта, магістри медицини, методичні аспекти, тематичний блок, кейс-метод, цифрові ризики, електронні медичні системи, кібергігієна, студентоцентрований підхід.

Mykola MATVIIENKO

METHODICAL ASPECT OF FORMING CYBERSECURITY COMPETENCE IN MEDICAL MASTER'S STUDENTS

The article substantiates one of the methodical aspects of forming cybersecurity competence in medical master's students during their professional training. The relevance of the study is determined by the growing role of digital technologies in the healthcare system, the widespread use of electronic medical records, information systems, and remote services, which increases the risks of breaching the confidentiality and integrity of medical data. In this context, future doctors must possess not only general digital skills but also professionally oriented cybersecurity competence. The didactic potential of a thematic module is outlined for structuring the learning content, ensuring the professional focus of tasks, and developing sustainable practical skills in cyber hygiene. It is demonstrated that using case studies, situational, and practice-oriented tasks within the thematic module contributes to enhancing future doctors' responsibility for the security of medical information. The scientific novelty of the article lies in substantiating the thematic module as an effective form of organizing learning to implement a specific methodical aspect of forming cybersecurity competence in medical master's students.

Key words: cybersecurity competence, medical education, medical master's students, methodical aspects, thematic module, case method, digital risks, electronic medical systems, cyber hygiene, student-centered approach.

ISSN: 2078-1016

Обґрунтування актуальності проблеми. Цифрова трансформація охорони здоров'я зумовлює суттєві зміни у професійній діяльності лікаря, пов'язані з використанням електронних медичних записів, клінічних інформаційних систем, телемедичних сервісів та цифрових платформ взаємодії з пацієнтами. За цих умов зростає значущість компетентності з кібербезпеки як складника професійної готовності майбутніх лікарів до роботи в цифровому середовищі. Недотримання базових принципів цифрової безпеки, помилки в організації доступу до медичних систем або необізнаність щодо типових цифрових ризиків можуть призводити не лише до витоків конфіденційної інформації, а й до порушення безперервності надання медичної допомоги та загроз для безпеки пацієнтів. Актуальність проблеми посилюється в умовах воєнного часу, коли система охорони здоров'я функціонує як елемент критичної інфраструктури, а медичні інформаційні ресурси набувають стратегічного значення. Водночас цифровізація освітнього процесу у закладах вищої медичної освіти створює додаткові виклики, пов'язані з безпечним використанням навчальних платформ, хмарних сервісів та електронних ресурсів. Це зумовлює необхідність цілеспрямованого формування у здобувачів вищої медичної освіти не лише знань про кіберзагрози, а й практичних умінь безпечної цифрової поведінки та відповідального ставлення до обробки медичних даних.

Попри наявність нормативних вимог щодо захисту інформації та активний розвиток цифрових технологій, проблема формування компетентності з кібербезпеки магістрів медицини не набула системного методичного опрацювання, що актуалізує потребу в розкритті механізмів реалізації відповідної методики в освітньому процесі. Здебільшого питання цифрової безпеки інтегруються у навчальні курси фрагментарно або подаються переважно в інформаційному форматі, без чітко вибудуваної логіки поєднання теорії, практики та самоконтролю. Це актуалізує потребу в розробленні та описі таких методичних підходів, які дозволяють реалізувати формування компетентності з кібербезпеки як цілісний і керований освітній процес.

Аналіз останніх досліджень та публікацій. У сучасному науковому дискурсі питання підготовки майбутніх лікарів до роботи в цифровому середовищі дедалі частіше розглядаються крізь призму кібербезпеки як професійно значущої компетентності, безпосередньо пов'язаної із захистом медичних даних, безперервністю клінічних процесів та безпекою пацієнтів. Методологічним підґрунтям для осмислення безпекового виміру професійної діяльності лікаря слугують, зокрема, положення європейської рамки цифрової компетентності DigComp, у якій безпека виокремлюється як самостійний домен і охоплює захист даних, цифрову відповідальність та етичні аспекти роботи з інформацією [14]. У медичній освіті цей домен набуває прикладного характеру, оскільки стосується роботи з електронними медичними записами, медичними інформаційними системами та підключеними цифровими пристроями.

Зарубіжні дослідники акцентують увагу на тому, що формування кібербезпекової компетентності майбутніх лікарів не може обмежуватися ознайомленням із загальними відомостями про цифрові загрози. Науковці наголошують на необхідності практико-орієнтованого навчання, яке дає змогу відпрацьовувати безпечні моделі професійної поведінки в умовах, наближених до реальної клінічної практики [15; 18]. У цьому контексті ефективними визнаються кейс-метод, симуляційні та problem-based підходи, що дозволяють інтегрувати знання про кіберзагрози, практичні дії та відповідальне прийняття рішень у цифровому медичному середовищі [17]. В окремих працях доведено, що high-fidelity симуляції, спрямовані на моделювання кіберінцидентів у медичних системах, сприяють формуванню професійної пильності лікарів і готовності враховувати кіберінциденти як фактор ризику у клінічній діяльності [16].

У вітчизняному науковому дискурсі проблематика кібербезпеки в медичній освіті представлена значно менш системно

порівняно із зарубіжними дослідженнями. Водночас аналіз законодавства України та нормативно-правових документів засвідчує усвідомлення на державному рівні необхідності врегулювання питань кібербезпеки в процесі використання цифрових медичних ресурсів, зокрема електронних медичних записів, телемедичних сервісів і медичних інформаційних систем [2; 3; 4; 5; 10].

У сучасних вітчизняних наукових публікаціях наголошується, що навчання основ кібербезпеки та кібергігієни є критично важливою освітньою компонентою підготовки майбутніх медичних працівників усіх спеціальностей, оскільки забезпечує захист медичних даних, конфіденційність інформації про пацієнтів і безперервність надання медичних послуг [9]. Практичну доцільність такого підходу підтверджують результати досліджень, у яких обґрунтовано ефективність упровадження спеціалізованих курсів з основ медіаграмотності та кібербезпеки в медичній освіті як засобу формування навичок безпечного й відповідального використання цифрових технологій у професійній діяльності лікаря [6].

Окрему увагу українські науковці приділяють ролі людського чинника у виникненні кіберінцидентів у сфері охорони здоров'я, підкреслюючи, що значна частина порушень інформаційної безпеки зумовлена недостатнім рівнем цифрової обізнаності та невмінням медичних працівників дотримуватися базових правил кібергігієни [8]. Це, своєю чергою, актуалізує освітню значущість формування відповідальної цифрової поведінки майбутніх лікарів у процесі професійної підготовки.

Разом із тим аналіз вітчизняних досліджень засвідчує, що більшість наукових праць зосереджена переважно на проблемах цифрової та ІТ-компетентності магістрів медицини в межах інформатичних дисциплін, а також на впровадженні цифрових технологій у навчальний процес закладів вищої медичної освіти. У такому контексті кібербезпека здебільшого розглядається як супутній складник цифрової грамотності без її виокремлення як самостійного об'єкта методичного проєктування та цілеспрямованого педагогічного впливу.

Узагальнення результатів наукових праць дозволяє дійти висновку, що, попри наявність ґрунтовних теоретичних підходів і прикладних напрацювань у сфері цифрової компетентності [7; 11], проблема методичної організації навчання з кібербезпеки в медичній освіті залишається недостатньо конкретизованою. Зокрема, бракує досліджень, у яких було б детально описано функціонування методики формування компетентності з кібербезпеки через чітко структуровану навчальну одиницю, що інтегрує мотиваційний, когнітивний і діяльнісний компоненти та відповідає специфіці професійної діяльності майбутнього лікаря.

Така логіка зумовлює перехід від фрагментарного тематичного викладу до використання структурованої дидактичної одиниці, здатної відтворювати цілісний фрагмент професійної діяльності лікаря в цифровому середовищі. У межах даного дослідження такою одиницею обрано тематичний блок, який розглядається як інструмент реалізації методики формування компетентності з кібербезпеки магістрів медицини, оскільки він дозволяє послідовно поєднати актуалізацію проблеми, практичну діяльність і аналіз типових помилок. Така логіка зумовила розроблення методики, що ґрунтується на використанні тематичних блоків як базових дидактичних одиниць, здатних функціонувати як у структурі навчального курсу, так і як самодостатні елементи освітнього процесу, реалізовані в конкретних професійно орієнтованих ситуаціях.

Мета статті полягає в розкритті механізму реалізації методики формування компетентності з кібербезпеки магістрів медицини на прикладі одного тематичного блоку як базової дидактичної одиниці.

Досягнення поставленої мети передбачає опис структури тематичного блоку, логіки його побудови та функціонування в освітньому процесі, а також обґрунтування його дидактичного потенціалу як інструменту реалізації методики формування кібербезпекової компетентності майбутніх лікарів у професійно орієнтованих ситуаціях.

ISSN: 2078-1016

Завдання дослідження

Відповідно до мети у статті поставлено такі завдання:

– проаналізувати підходи до формування кібербезпекової компетентності майбутніх лікарів у контексті сучасної медичної освіти;

– обґрунтувати доцільність використання тематичного блоку як структурної одиниці реалізації методики формування компетентності з кібербезпеки;

– розкрити послідовність етапів тематичного блоку та їхнє функціональне призначення в навчальному процесі;

– продемонструвати інтеграцію теоретичних положень і практичних дій у межах тематичного блоку на прикладі професійно орієнтованої ситуації.

Методи дослідження

У процесі дослідження використано комплекс теоретичних методів, адекватних меті статті та її теоретико-методичному характеру. Зокрема, *аналіз і синтез* застосовувалися для опрацювання вітчизняних і зарубіжних наукових праць із проблем формування компетентності з кібербезпеки в медичній освіті, а також для узагальнення підходів до організації практико-орієнтованого навчання майбутніх лікарів.

Порівняння та узагальнення дали змогу зіставити існуючі підходи до навчання кібербезпеки в медичній освіті та виявити їхні спільні риси й обмеження з погляду методичної реалізації. *Структурно-функціональний аналіз* використовувався для визначення логіки побудови тематичного блоку як дидактичної одиниці та окреслення функцій його окремих елементів у формуванні мотиваційного, пізнавального та практично-діяльнісного складників кібербезпекової компетентності магістрів медицини.

Елементи *педагогічного моделювання* застосовано для опису функціонування методики формування компетентності з кібербезпеки на прикладі одного тематичного блоку, що реалізується в конкретній професійно орієнтованій ситуації.

Стаття має *теоретико-методичний характер* і спрямована на концептуальне осмислення механізмів реалізації методики формування компетентності з кібербезпеки майбутніх лікарів, що передує її подальшій емпіричній перевірці.

Виклад основного матеріалу. Методика формування компетентності з кібербезпеки магістрів медицини ґрунтується на поєднанні теоретичних положень і практичних дій, орієнтованих на типові професійні ситуації цифрової медичної практики. У межах запропонованого підходу реалізація методики здійснюється через *тематичний блок*, який розглядається як логічно завершена навчальна одиниця, спрямована на формування конкретних умінь і моделей безпечної професійної поведінки в цифровому середовищі.

Звернення саме до тематичного блоку зумовлене його дидактичним потенціалом: він дозволяє інтегрувати зміст кібербезпеки у навчальний процес без перевантаження теоретичними узагальненнями та водночас забезпечує практичну спрямованість навчання. Тематичний блок поєднує опис професійно значущої проблемної ситуації, аналіз цифрових ризиків, виконання практичних завдань і засоби контролю правильності дій, що відповідає вимогам студентоцентрованого та компетентнісного підходів.

Функціонування методики формування компетентності з кібербезпеки магістрів медицини пропонуємо проілюструвати на прикладі тематичного блоку «Аутентифікація та контроль доступу», спрямованого на формування в майбутніх лікарів умінь безпечної роботи з електронними медичними системами. Актуальність цього блоку зумовлена широким використанням електронних медичних записів, лабораторних інформаційних систем і дистанційного доступу до медичних даних, що підвищує ризики несанкціонованого втручання в інформаційні ресурси.

Про недостатній рівень сформованості відповідних знань і вмінь у студентів-медиків свідчать результати зарубіжних емпіричних досліджень. Зокрема, дослідження, проведене в Індії, виявило обмежене розуміння студентами базових механізмів кіберзахисту, зокрема принципів багатофакторної автентифікації та захисту

персональних даних, що є критично важливими для безпечної роботи з медичними інформаційними системами [19]. Це підтверджує необхідність цілеспрямованого методичного впливу в процесі професійної підготовки майбутніх лікарів.

Зміст тематичного блоку вибудувано навколо типової професійної ситуації, пов'язаної з доступом лікаря до електронної медичної системи в умовах внутрішньої або віддаленої взаємодії. У межах навчальної роботи студенти опановують принципи створення надійних облікових даних, використання багатофакторної автентифікації, розподілу прав доступу та фіксації змін у системі. Паралельно здійснюється аналіз типових помилок, які найчастіше призводять до компрометації облікових записів і витоку медичної інформації.

Практична реалізація змісту блоку забезпечується через навчальний кейс «Фейковий сайт лікарні», що моделює ситуацію фішингової атаки. Робота з кейсом передбачає виявлення ознак шахрайського ресурсу, оцінювання потенційних ризиків для пацієнтів і медичного персоналу та вироблення обґрунтованого алгоритму дій у разі підозри на компрометацію доступу. Такий формат навчання узгоджується з положеннями педагогічних досліджень, у яких кейс-метод розглядається як ефективний засіб формування фахових компетентностей і перенесення теоретичних знань у практичну площину [1; 12; 13].

Для закріплення результатів навчання застосовуються чек-листи цифрової безпеки, що виконують функцію інструменту самоконтролю та дозволяють студентам систематизувати власні дії під час роботи з медичними інформаційними системами. На основі чек-листів здобувачі формують персоналізовані алгоритми безпечної поведінки, адаптовані до конкретних професійних ситуацій.

Отже, використання тематичного блоку дозволяє конкретизувати методичний аспект формування компетентності з кібербезпеки магістрів медицини та забезпечити прикладний характер навчання без розширення методики до рівня цілісної системи. Тематичний блок «Аутентифікація та контроль доступу» демонструє можливості реалізації методики формування компетентності з кібербезпеки магістрів медицини через поєднання проблемно орієнтованого змісту, навчальних кейсів і засобів самоконтролю, забезпечуючи прикладний характер навчання та готовність майбутніх лікарів до безпечної професійної діяльності в цифровому середовищі.

Висновки. У статті розкрито особливості реалізації методики формування компетентності з кібербезпеки магістрів медицини на прикладі одного тематичного блоку, що дозволило продемонструвати її прикладний і студентоцентрований характер. Показано, що використання тематичного блоку як базової навчальної одиниці забезпечує інтеграцію теоретичних знань і практичних дій у межах професійно орієнтованих ситуацій цифрової медичної практики.

Обґрунтовано, що тематичний блок дозволяє цілеспрямовано формувати уміння безпечної роботи з електронними медичними системами, сприяє усвідомленню цифрових ризиків та розвитку відповідальної поведінки майбутніх лікарів у цифровому середовищі. Практична спрямованість блоку, реалізована через навчальний кейс, тестові завдання та чек-листи цифрової безпеки, створює умови для перенесення навчального досвіду в реальні професійні ситуації.

Застосування чек-листів і персоналізованих алгоритмів дій сприяє розвитку навичок самоконтролю та прийняття обґрунтованих рішень у сфері кібербезпеки, що є критично важливим для сучасної медичної практики. Результати аналізу функціонування тематичного блоку підтверджують доцільність використання блокового підходу як інструменту реалізації методики формування компетентності з кібербезпеки магістрів медицини.

Перспективи подальших досліджень пов'язані з апробацією запропонованої методики в освітньому процесі закладів вищої медичної освіти та аналізом її ефективності під час використання інших тематичних блоків у різних професійно орієнтованих контекстах.

ISSN: 2078-1016

ЛІТЕРАТУРА

1. **Арлачов, К. В., & Рудась, В. Г.** (2024). Методичні засади використання кейс-технологій при викладанні економічних дисциплін. *Проблеми інженерно-педагогічної освіти*, *83*, 212–223. https://doi.org/10.26565/2074-8922-2024-83-18

2. Доктрина інформаційної безпеки України : затв. Указом Президента України від 25.02.2017 р. № 47/2017.

3. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (зі змінами).

4. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI (зі змінами).

5. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 р. № 11290

6. **Коваль, Б. Ф., Коваль, Л. Д., & Пойда, С. А**. (2023). Навчання майбутніх лікарів основам медіаграмотності та кібербезпеки. *Перспективи та інновації науки. Серія «Педагогіка», Серія «Психологія», Серія «Медицина»*, *8(26)*, 171–183. https://doi.org/10.52058/2786-4952-2023-8(26)-171-183

7. **Микитенко, П. В.** (2018). Діагностика рівнів ІТ-компетентності іноземних студентів у процесі вивчення медичної інформатики. *Комп'ютер у школі та сім'ї*, *8*, 3–10. https://doi.org/10.33407/itlt.v75i1.3569

8. **Пойда, С., & Якименко, О.** (2022). Формування та розвиток цифрової компетентності медичного працівника в період пандемії SARS COVID-19. *Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування»*, *2*(2022). https://doi.org/10.32782/2786-5681-2022-2.07

9. **Сілкова, О. В., Макаренко, О. В., Макаренко, В. І., & Хміль, О. В.** (2025). Впровадження нової освітньої компоненти «кібербезпека, кібергігієна» у медичну освіту – вимога сьогодення. *Перспективи та інновації науки*, *1(47)*, 1089–1099. https://doi.org/10.52058/2786-4952-2025-1(47)-1089-1098

10. Стратегія кібербезпеки України : затв. Указом Президента України від 26.08.2021 р. № 447/2021.

11. **Стучинська, Н. В., & Матвієнко, М. М.** (2023). Роль вибіркових дисциплін у формуванні цифрової компетентності майбутніх лікарів. *Педагогіка формування творчої особистості у вищій і загальноосвітній школах*, *88*, 138–145. https://doi.org/10.32840/1992-5786.2023.88.25

12. **Федів, В. І., Олар, О. І., Бірюкова, Т. В., Микитюк, О. Ю., & Кульчинський, В. В.** (2021). Використання кейс-методу під час вивчення дисципліни «Медична та біологічна фізика». *Вісник Університету імені Альфреда Нобеля. Серія «Педагогіка і психологія»*, *1*, 269–278. https://doi.org/10.32342/2522-4115-2021-1-21-31

13. **Шкатуляк, Н. М., Усов, В. В., & Павловський, В. В.** (2025). Інтегровані кейс-уроки – інноваційна технологія навчання. *Наукові записки. Серія «Педагогічні науки»*, *217*, 78–83. https://doi.org/10.36550/2415-7988-2025-1-217-78-83

14. **Carretero, S., Vuorikari, R., & Punie, Y.** (2022). DigComp 2.2: The Digital Competence Framework for citizens. Update phase 1: The conceptual reference model. Publications Office of the European Union. https://doi.org/10.2760/115376

15. **Coventry, L., & Branley, D.** (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

16. **Dameff, C., Pfeffer, M. A., & Longhurst, C. A.** (2019). Cybersecurity implications for hospital quality. *Health Services Research*, *54*(5), 969–970. https://doi.org/10.1111/1475-6773.13202

17. **Elendu, C., Amaechi, D. C., Okatta, A. U., Amaechi, E. C., Elendu, T. C., Ezeh, C. P., & Elendu, I. D.** (2024). The impact of simulation-based training in medical education: A review. *Medicine*, *103*(27), e38813. https://doi.org/10.1097/MD.0000000000038813

18. **Jalali, M. S., & Kaiser, J. P.** (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5), e10059. https://doi.org/10.2196/10059

19. **Rathod, P. I., & Potdar, A. B.** (2019). Study of awareness of cyber-security among medical students. *Indian Journal of Forensic Medicine & Toxicology*, *13*(1), 196–198. https://doi.org/10.5958/0973-9130.2019.00040.9

REFERENCES

1. **Arlachov, K. V., & Rudas, V. H.** (2024). Metodychni zasady vykorystannia keis-tekhnolohii pry vykladanni ekonomichnykh dystsyplin [Methodological principles of using case technologies in teaching economic disciplines]. Problemy inzhenerno-pedahohichnoi osvity – Problems of Engineering and Pedagogical Education, 83, 212–223. https://doi.org/10.26565/2074-8922-2024-83-18 [in Ukrainian].

2. Doktryna informatsiinoi bezpeky Ukrainy [Doctrine of Information Security of Ukraine]. (2017). Approved by the Decree of the President of Ukraine dated February 25, 2017, No. 47/2017 [in Ukrainian].

3. Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh" [Law of Ukraine "On Protection of Information in Information and Telecommunication Systems"]. (1994). No. 80/94-VR dated July 5, 1994 (as amended) [in Ukrainian].

4. Zakon Ukrainy "Pro zakhyst personalnykh danykh" [Law of Ukraine "On Personal Data Protection"]. (2010). No. 2297-VI dated June 1, 2010 (as amended) [in Ukrainian].

5. Zakon Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv ta obiektiv krytychnoi informatsiinoi infrastruktury [Law of Ukraine on Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure Objects]. (2025). No. 11290 dated March 27, 2025 [in Ukrainian].

6. **Koval, B. F., Koval, L. D., & Poida, S. A.** (2023). Navchannia maibutnikh likariv osnovam mediahramotnosti ta kiberbezpeky [Teaching future doctors the basics of media literacy and cybersecurity]. Perspektyvy ta innovatsii nauky (Seriia "Pedahohika", Seriia "Psykholohiia", Seriia "Medytsyna") – Perspectives and Innovations of Science (Series "Pedagogy", Series "Psychology", Series "Medicine"), 8(26), 171–183. https://doi.org/10.52058/2786-4952-2023-8(26)-171-183 [in Ukrainian].

7. **Mykytenko, P. V.** (2018). Diahnostyka rivniv IT-kompetentnosti inozemnykh studentiv u protsesi vyvchennia medychnoi informatyky [Diagnostics of IT competence levels of foreign students in the process of studying medical informatics]. Kompiuter u shkoli ta simi – Computer at School and Family, 8, 3–10 https://doi.org/10.33407/itlt.v75i1.3569. [in Ukrainian].

8. **Poida, S., & Yakymenko, O.** (2022). Formuvannia ta rozvytok tsyfrovoi kompetentnosti medychnoho pratsivnyka v period pandemii SARS COVID-19 [Formation and development of digital competence of a medical worker during the SARS COVID-19 pandemic]. Naukovyi visnyk Vinnytskoi akademii bezperervnoi osvity. Seriia "Ekolohiia. Publichne upravlinnia ta administruvannia" – Scientific Bulletin of Vinnytsia Academy of Continuing Education. Series "Ecology. Public Management and Administration", 2(2022). https://doi.org/10.32782/2786-5681-2022-2.07 [in Ukrainian].

9. **Silkova, O. V., Makarenko, O. V., Makarenko, V. I., & Khmil, O. V.** (2025). Vprovadzhennia novoi osvitnoi komponenty "kiberbezpeka, kiberhihiiena" u medychnu osvitu – vymoha sohodennia [Implementation of a new educational component "cybersecurity, cyber hygiene" in medical education – a requirement of today]. Perspektyvy ta innovatsii nauky – Per-

spectives and Innovations of Science, 1(47), 1089–1099. https://doi.org/10.52058/2786-4952-2025-1(47)-1089-1098 [in Ukrainian].

10. Stratehiia kiberbezpeky Ukrainy [Cybersecurity Strategy of Ukraine]. (2021). Approved by the Decree of the President of Ukraine dated August 26, 2021, No. 447/2021 [in Ukrainian].

11. **Stuchynska, N. V., & Matviienko, M. M.** (2023). Rol vybirkovykh dystsyplin u formuvanni tsyfrovoi kompetentnosti maibutnikh likariv [The role of elective disciplines in the formation of digital competence of future doctors]. Pedahohika formuvannia tvorchoi osobystosti u vyshchii i zahalnoosvitnii shkolakh – Pedagogy of Creative Personality Formation in Higher and Secondary Schools, 88, 138–145. https://doi.org/10.32840/1992-5786.2023.88.25 [in Ukrainian].

12. **Fediv, V. I., Olar, O. I., Biriukova, T. V., Mykytiuk, O. Yu., & Kulchynskyi, V. V.** (2021). Vykorystannia keis-metodu pid chas vyvchennia dystsypliny "Medychna ta biolohichna fizyka" [Using the case method in studying the discipline "Medical and Biological Physics"]. Visnyk Universytetu imeni Alfreda Nobelia. Seriia: Pedahohika i psykholohiia – Bulletin of Alfred Nobel University. Series: Pedagogy and Psychology, 1, 269–278. https://doi.org/10.32342/2522-4115-2021-1-21-31 [in Ukrainian].

13. **Shkatuliak, N. M., Usov, V. V., & Pavlovskyi, V. V.** (2025). Intehrovani keis-uroky – innovatsiina tekhnolohiia navchannia [Integrated case lessons – an innovative learning technology]. Naukovi zapysky. Seriia: Pedahohichni nauky – Scientific Notes. Series: Pedagogical Sciences, 217, 78–83. https://doi.org/10.36550/2415-7988-2025-1-217-78-83 [in Ukrainian].

14. **Carretero, S., Vuorikari, R., & Punie, Y.** (2022). DigComp 2.2: The Digital Competence Framework for citizens. Update phase 1: The conceptual reference model. Publications Office of the European Union. https://doi.org/10.2760/115376 [in English].

15. **Coventry, L., & Branley, D.** (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008 [in English].

16. **Dameff, C., Pfeffer, M. A., & Longhurst, C. A.** (2019). Cybersecurity implications for hospital quality. Health Services Research, 54(5), 969–970. https://doi.org/10.1111/1475-6773.13202 [in English].

17. **Elendu, C., Amaechi, D. C., Okatta, A. U., Amaechi, E. C., Elendu, T. C., Ezeh, C. P., & Elendu, I. D.** (2024). The impact of simulation-based training in medical education: A review. Medicine, 103(27), e38813. https://doi.org/10.1097/MD.0000000000038813 [in English].

18. **Jalali, M. S., & Kaiser, J. P.** (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. Journal of Medical Internet Research, 20(5), e10059. https://doi.org/10.2196/10059 [in English].

19. **Rathod, P. I., & Potdar, A. B.** (2019). Study of awareness of cyber-security among medical students. Indian Journal of Forensic Medicine & Toxicology, 13(1), 196–198. https://doi.org/10.5958/0973-9130.2019.00040.9 [in English].

Дата першого надходження статті до видання: 01.12.2025
Дата прийняття статті до друку після рецензування: 26.12.2025
Дата публікації (оприлюднення) статті: 30.12.2025