Лілія Десятнюк *– викладачка кафедри медичної і біологічної фізики та інформатики Національного медичного університету імені О. О. Богомольця, м. Київ, Україна.*

Коло наукових інтересів: *впровадження інноваційних педагогічних методик, цифровізації освіти, вдосконалення української освітньої системи та забезпечення її відповідності європейським стандартам.*

Liliia_31@nmu.ua

https://orcid.org/0000-0002-5170-7378

УДК 378.6.147:004.056

https://doi.org/10.32405/2411-1317-2026-3-113-124

Подано до редакції: 19.05.2026
Прийнято після рецензування: 09.06.2026
Затверджено до друку: 20.08.2026
Опубліковано: 30.09.2026

КІБЕРБЕЗПЕКА В МЕДИЧНІЙ ОСВІТІ: РЕТРОСПЕКТИВНИЙ АНАЛІЗ ТА ПЕДАГОГІЧНІ ЗАСАДИ ФОРМУВАННЯ КОМПЕТЕНТНОСТІ МАЙБУТНІХ МЕДИЧНИХ ФАХІВЦІВ

Анотація. У статті представлено результати ретроспективного аналізу розвитку кібербезпеки в медичній освіті як складової цифрової трансформації системи охорони здоров'я. Простежено еволюцію підходів до захисту медичних даних – від забезпечення фізичної конфіденційності паперових архівів до функціонування сучасних цифрових екосистем, що охоплюють електронні медичні картки, телемедичні платформи, хмарні сервіси, Internet of Medical Things (IoMT), системи штучного інтелекту та інтегровані eHealth-середовища.

У дослідженні здійснено аналіз ключових міжнародних регуляторних моделей і стандартів кіберзахисту (HIPAA, NIST, GDPR, NIS, EHDS), які визначають сучасну парадигму проактивного управління цифровими ризиками в галузі охорони здоров'я. Проаналізовано сучасні кіберзагрози, зокрема ransomware-атаки, соціальну інженерію, DDoS-атаки, витоки конфіденційної інформації та вразливості IoMT-пристроїв, що безпосередньо впливають на якість медичної допомоги та функціонування медичних установ. Висвітлено специфіку українського контексту розвитку eHealth-системи в умовах гібридної війни та цілеспрямованих кібератак на критичну медичну інфраструктуру.

Особливу увагу приділено освітньому виміру проблеми. Доведено, що зростання цифровізації медичної практики актуалізує необхідність інтеграції кібербезпеки як міждисциплінарної складової професійної підготовки майбутніх медичних фахівців. Обґрунтовано, що сучасний медичний працівник повинен володіти не лише клінічними знаннями, а й компетентностями у сфері кібергігієни, безпечної роботи з електронними медичними системами, захисту персональних даних пацієнтів, розпізнавання цифрових загроз та дотримання етико-правових норм функціонування цифрової медицини.

Визначено педагогічні засади формування компетентності з кіберзахисту, серед яких: компетентнісний, контекстний, міждисциплінарний та ризик-орієнтований підходи; інтеграція клінічного й цифрового мислення; використання кейс-методів, симуляційних сценаріїв та практикоорієнтованого навчання. Наголошено на необхідності переходу від фрагментарного інформування про кіберзагрози до системного формування поведінкових моделей безпечної професійної діяльності у цифровому середовищі.

© Десятнюк Л.

Проаналізовано історико-генезисні бар'єри формування компетентності з кібербезпеки у майбутніх медичних працівників, серед яких: розрив між темпами цифровізації медичної практики та змістом освітніх програм; інституційна маргіналізація кіберзахисту в медичній освіті; домінування традиційного клінічного мислення над ризик-орієнтованим цифровим підходом; асинхронність розвитку нормативно-правового регулювання та освітніх змін; недостатня інтеграція міжнародних стандартів кібербезпеки в систему професійної підготовки; відсутність цілісної педагогічної моделі навчання кіберзахисту майбутніх медичних фахівців. Обґрунтовано необхідність модернізації змісту медичної освіти відповідно до сучасних викликів цифрової медицини та кіберрезилієнтності системи охорони здоров'я.

Ключові слова: кібербезпека; медична освіта; професійна підготовка; компетентність з кібербезпеки; цифрова трансформація; захист медичних даних.

Вступ. Актуальність дослідження зумовлена не лише стрімкою цифровізацією системи охорони здоров'я, а й необхідністю переосмислення освітньої підготовки майбутніх медичних фахівців в умовах зростання кіберзагроз. Сучасна медицина функціонує в цифровому середовищі, де електронні медичні картки, хмарні сервіси, телемедицина, системи штучного інтелекту та Internet of Medical Things (IoMT) стали невід'ємною складовою професійної діяльності лікаря. Водночас активне впровадження цифрових технологій супроводжується збільшенням кількості ransomware-атак, випадків соціальної інженерії, витоків персональних даних та атак на медичну інфраструктуру, що створює ризики не лише для інформаційної безпеки, а й для життя та здоров'я пацієнтів.

За таких умов кібербезпека перестає бути суто технічною проблемою IT-фахівців і набуває виразного освітнього та професійного виміру. Значна частина кіберінцидентів у сфері охорони здоров'я пов'язана саме з людським фактором: недостатнім рівнем цифрової грамотності, порушенням правил кібергігієни, невмінням розпізнавати цифрові загрози та безпечно працювати з медичними інформаційними системами. Це актуалізує потребу у формуванні компетентності з кіберзахисту як обов'язкової складової професійної підготовки майбутніх медичних працівників.

Особливої актуальності проблема набуває в системі медичної освіти України, де зміст професійної підготовки часто не відповідає сучасним викликам цифрової трансформації медицини. Традиційна модель навчання орієнтована переважно на формування клінічних знань і практичних навичок, тоді як питання кібербезпеки залишаються фрагментарними або взагалі винесеними за межі професійної підготовки. Як наслідок, виникає суперечність між високим рівнем цифровізації медичної практики та недостатньою готовністю майбутніх фахівців до безпечної роботи у цифровому середовищі.

Отже, актуальність статті визначається потребою в науковому осмисленні еволюції кібербезпеки в медицині та обґрунтуванні педагогічних засад формування компетентності з кіберзахисту в майбутніх медичних фахівців. Це вимагає модернізації змісту медичної освіти, впровадження міждисциплінарних підходів до навчання та розроблення цілісної педагогічної моделі формування кіберкомпетентності як невід'ємної складової професійної діяльності сучасного лікаря.

Постановка проблеми. Фундамент сучасної системи цифрового захисту держави закладено в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. У законодавчому полі України кібербезпека трактується як комплексна характеристика захищеності ключових інтересів особи, суспільства та держави в цифровому середовищі, що охоплює не лише технічні, а й організаційні та правові аспекти протидії загрозам. Законодавець визначає пріоритетом створення безпечного комунікативного середовища, яке здатне оперативно ідентифікувати, запобігати та нейтралізувати як реальні, так і потенційні виклики національним інтересам.

У сучасну епоху тотальної цифровізації кібербезпека в медицині трансформувалася з вузькотехнічного сервісу у фундаментальний елемент виживання пацієнта та забезпечен-

ня національної стійкості. Проте стрімкий розвиток цифрових екосистем (ЕМК, IoMT, ШІ) виявив критичну проблему: технологічний прогрес значно випереджає темпи адаптації медичної освіти. Сьогодні цифрова стійкість медичної установи – це не лише ІТ-завдання, а насамперед результат професійної відповідальності медичного персоналу, де кожна помилка, спричинена низькою цифровою грамотністю, може коштувати життя.

Освітній вимір проблеми загострюється через «парадокс медицини»: необхідність миттєвого доступу до даних конфліктує з вимогами безпеки. Це призводить до того, що медичні працівники часто ігнорують протоколи захисту заради зручності, створюючи умови для реалізації 95% порушень, зумовлених людським фактором. Така статистика підкреслює, що проблема повязана насамперед не з відсутністю технічних засобів, а з недостатньою сформованістю кіберкомпетентності як невід'ємної частини професійної культури сучасного лікаря.

На теперішньому етапі спостерігається низка суперечностей, які потребують педагогічного розв'язання:

– Інституційний розрив: зміст освітніх програм медичних закладів вищої освіти (ЗВО) часто не відповідає реальним викликам цифровізації, залишаючи питання кіберзахисту на периферії підготовки.
– Когнітивний дисонанс: у навчальному процесі домінує традиційне клінічне мислення, тоді як сучасні умови вимагають ризик-орієнтованого цифрового мислення, де безпека даних сприймається як частина безпеки пацієнта.
– Методичний дефіцит: відсутність системної педагогічної моделі формування кібергігієни призводить до того, що студенти сприймають цифрові загрози як абстрактні, а не персоналізовані професійні ризики.

Особливої актуальності це набуває в умовах війни в Україні, де медична інфраструктура стала ціллю для wiper-атак, що мають на меті не просто викрадення, а повне знищення клінічних даних. У цих екстремальних умовах здатність медичного фахівця дотримуватися правил кібербезпеки стає фактором національної резилієнтності.

Отже, існує нагальна потреба в ретроспективному аналізі розвитку кіберзагроз та переосмисленні педагогічних засад підготовки майбутніх фахівців. Розв'язання проблеми вимагає переходу від фрагментарного інформування до створення цілісної методики формування компетентності з кіберзахисту, яка б інтегрувала клінічні, технічні та етико-правові аспекти цифрової медицини.

Аналіз останніх досліджень і публікацій. Актуальні дослідження з кібербезпеки в галузі охорони здоров'я демонструють поступове зміщення акценту від технічних аспектів до освітніх, поведінкових і системних компонентів. У роботі В. Т. Аргай та ін. (Argaw S. T. et al., 2020) обґрунтовано комплексний підхід до кібербезпеки медичних закладів, ідентифіковано ключові вразливості інфраструктури та запропоновано напрями зниження ризиків, зокрема через підвищення стійкості медичних інформаційних систем. У дослідженні А. Т. Аланазі (Alanazi, 2023), присвяченому аналізу сприйняття кіберзагроз клініцистами, встановлено, що недостатній рівень практичних знань персоналу є критичним фактором ризику для безпеки даних пацієнтів. У систематичному огляді авторського колективу на чолі з Дж. К. де Ганьє (De Gagne et al., 2023) розкрито концепцію кіберетики в медичній освіті та підкреслено необхідність формування етичної відповідальності при роботі з цифровими даними. Вітчизняні дослідники Н. В. Стучинська та М. М. Матвієнко (2025) визначають кіберграмотність як основу формування професійної компетентності майбутніх лікарів і в роботі щодо методичних аспектів підготовки магістрів пропонують інтеграцію кібербезпеки в освітні програми. І. І. Кучеренко та ін. (2025) емпірично доводять недостатній рівень обізнаності студентів медичних ЗВО щодо кібербезпеки, що свідчить про наявність освітнього розриву. У дослідженні Н. В. Стучинської, Ю. В. Паламарчука та В. О. Ніжегородцева (2024) обґрунтовано необхідність включення кібербезпеки до підготовки стоматологів у контексті цифровізації

медицини. О. М. Литвинов (2024) розглядає кібербезпеку як фактор ефективності ЗВО, підкреслюючи її вплив на стабільність освітнього середовища. І. І. Парфьонова (2024) аналізує розвиток кібербезпеки в системі eHealth України. Таким чином, сучасні дослідження підтверджують, що кібербезпека в охороні здоров'я трансформується в міждисциплінарну сферу, де ключову роль відіграють не лише технології, а й підготовка медичних фахівців та організаційні механізми управління безпекою.

Метою дослідження є комплексне висвітлення результатів ретроспективного аналізу розвитку кібербезпеки в галузі охорони здоров'я та обґрунтування педагогічних засад формування компетентності з кіберзахисту у майбутніх медичних фахівців в умовах цифровізації медицини.

У дослідженні використано **комплекс теоретичних методів**, що забезпечили системне осмислення розвитку компетентності кібербезпеки в медичній освіті:

– Аналіз і синтез – застосовано для опрацювання наукових джерел у галузях кібербезпеки, медичної інформатики, охорони здоров'я та цифровізації медицини; дали змогу узагальнити підходи до визначення сутності кібербезпеки, еволюції загроз і механізмів захисту медичних інформаційних систем.
– Порівняльний аналіз – використано для зіставлення міжнародного та вітчизняного досвіду забезпечення кібербезпеки в системах охорони здоров'я, зокрема в контексті впровадження електронних медичних систем, нормативно-правового регулювання та підготовки медичних фахівців.

Результати та обговорення. Шлях галузі охорони здоров'я до цифрової безпеки – це еволюція від фізичного захисту паперових архівів 1920-х років до створення інтелектуальних систем протидії кібервійнам. Стійкий зв'язок між медициною та кібернетикою будо закріплено ще в 1958 р. зі створенням Міжнародного товариства кібернетичної медицини. У табл. 1 представлено етапи еволюції медичного ІТ-середовища за матеріалами Центру координації кібербезпеки сектору охорони здоров'я (США).

Таблиця 1. **Етапи еволюції ІТ-середовища в галузі охорони здоров'я**

Період, роки	Ключові технології	Виклики безпеки
1920–1930-ті	Паперові записи, Blue Cross, Закон про соцзабезпечення (1935)	Фізична конфіденційність, безпека архівів за часів Великої депресії
1940–1950-ті	Фундаментальні принципи МРТ, діаліз, кардіостимулятори	Заснування Міжнародного товариства кібернетичної медицини (1958)
1960–1970-ті	Hospital Information Systems (HIS), концепція пакетної комутації (Д. Дейвіс, 1965)	Поява мейнфреймів, перші спроби мережевого обміну даними
1980–1990-ті	Клінічні інформаційні системи, перші ЕМК, прийняття в 1996 р. Акта про мобільність та підзвітність медичного страхування (Health Insurance Portability and Accountability Act, HIPAA)	Атака Джозефа Поппа (1989) – перша ransomware-атака на конференції Всесвітньої організації охорони здоровя
2000-ні – сьогодення	Хмари, IoMT, ШІ, eHealth. Атака Anonymous на Boston Children's Hospital (2014)	WannaCry (2017), Conti/Ryuk (2019–2021), кібервійна проти України

Міжнародні стандарти та регуляторні моделі трансформували роль кібербезпеки з реактивної («ліквідація наслідків витоку») на проактивну («забезпечення стійкості»):

– Американські моделі (HIPAA, Національний інститут стандартів і технологій США (National Institute of Standards and Technology. NIST)): HIPAA (діє з 1996 р.) встановлюють жорсткі вимоги до захисту медичних даних пацієнта. Ключовою особливістю моделі є вимога до закладів охорони здоров'я підтвердити наявність стійкої архітектури до того як стався кіберінцидент, а не просто констатувати факт зламу. Правило безпеки HIPAA передбачає багаторівневу систему захисту, що поєднує управлінські, інфраструктурні та технологічні механізми забезпечення конфіденційності, цілісності й доступності медичних даних пацієнта. Модель NIST орієнтована на ризики структури закладу охорони здоров'я і побудована навколо шести функцій – ідентифікація, захист, виявлення, реагування, відновлення та управління.
– Європейські моделі (NIS, GDPR, EHDS). Відмінності Директиви ЄС про безпеку мережевих та інформаційних систем (Network and Information Security, NIS) і Загального регламенту про захист даних (General Data Protection Regulation, GDPR) полягають як у сфері застосування (використання NIS спрямовано на мережі, інформаційні системи та загальну кібербезпеку, а GDPR зосереджений на захисті персональних даних та застосовується до будь-якої організації), так і у вимогах та штрафів за їх недотримання. Відповідно до NIS, організації повинні впроваджувати надійні заходи кібербезпеки та повідомляти про будь-які значні інциденти кібербезпеки протягом 24 годин. Регламент GDPR наголошує на отриманні явної згоди користувачів перед обробкою їхніх даних та вимагає, щоб про порушення даних повідомлялося органам влади протягом 72 годин. Штрафи за недотримання вимог NIS можуть сягати 10 млн євро або 2% світового обороту компанії, а GDPR – сягають 20 млн євро або 4% світового річного доходу компанії.

Регламент EHDS (European Health Data Space) має на меті створення спільної системи для використання та обміну електронними даними про здоров'я пацієнтів в ЄС. Він розширює доступ осіб до особистих електронних даних про здоров'я та контроль над ними, а також дозволяє повторно використовувати певні дані в суспільних інтересах – для підтримки політики та науково-дослідних цілей. Модель EHDS сприяє створенню середовища даних, орієнтованого на здоров'я, яке підтримує єдиний ринок цифрових послуг та продуктів охорони здоров'я. Крім того, регламент встановлює гармонізовану правову й технічну основу для систем електронних медичних карток, сприяючи взаємодії, інноваціям та безперебійному функціонуванню внутрішнього ринку.

Розглянуті моделі диктують нову парадигму: кібербезпека – це не видатки, а інвестиція в довіру пацієнта та операційну безперервність. Запровадження чітких стандартів кібербезпеки зумовлено зростаючою кількістю кіберінцидентів. Особливе значення мала подія 2014 р. – DDoS-атака групи Anonymous на дитячу лікарню Бостона (США), яка ознаменувала перехід від простого застосування шкідливого програмного забезпечення до ідеологічно вмотивованого «хактивізму», що цілить у критичну інфраструктуру.

У березні 2022 р. Координаційний центр з питань кібербезпеки сектору охорони здоров'я при Міністерстві охорони здоров'я і соціальних служб США (HHS) представив звіт «Кібербезпека сектору охорони здоров'я: ретроспектива 2021 року та погляд у 2022 рік». 2021 р. став точкою детермінації, коли атаки на цифрову інфраструктуру закладів охорони здоров'я не лише кількісно зросли (на 45%), а і якісно ускладнилися. Аналіз кіберінцидентів продемонстрував такі ключові тенденції:

– *Масштабність компрометації даних:* протягом 2021 р. зафіксовано понад 700 масштабних інцидентів, у результаті яких було скомпрометовано конфіденційну інформацію 45,7 млн. пацієнтів. Це найвищий показник вразливості сектору за останнє десятиліття.
– *Деструктивний вплив «ransomware»:* Використання програм-вимагачів перейшло з площини фінансового шантажу в площину загрози життю. Через блокування систем понад 70% медичних установ зазнали затримок у госпіталізації та наданні екстреної допомоги.
– *Державне регулювання та контрзаходи:* У відповідь на агресивну тактику зловмисників країни ЄС (зокрема Франція) ініціювали масштабні освітні проєкти для персоналу лікарень. Важливим правовим аспектом залишається законодавча заборона для державних медустанов на виплату будь-яких викупів кіберзлочинцям.
– *Технологічна еволюція зловмисників:* згідно з даними Trend Micro, хакери почали використовувати мову програмування Rust для створення кросплатформеного коду (зокрема в сімействі Agenda). Це дає змогу шкідливому програмному забезпеченню бути однаково ефективним як у середовищі Windows, так і в Linux, що критично для сучасних eHealth-систем.

Окрему увагу варто приділити звіту Міністерства охорони здоров'я США (HHS) за березень 2022 р., де медичну галузь визначено як одну з найбільш пріоритетних цілей для атак, що приймає 6% загального обсягу кіберінцидентів у країні (рис. 1).

Рис. 1. **Розподіл частки кібератак за галузями у США за 2022 р.**

Україна сьогодні стала «тестовим середовищем» для випробування медичної кіберрезилієнтності в умовах гібридної та повномасштабної війни. Розвиток системи eHealth (з 2016 р.) допоміг швидко цифровізувати галузь, але російське повномасштабне вторгнення висунуло екстремальні вимоги до цього захисту.

Розглянемо специфіку українського контексту.

1. Гібридна війна та «whispergate». У січні 2022 р. медична інфраструктура зазнала атак шкідливого програмного забезпечення (ПЗ) «whispergate». Важливо розуміти: це не традиційний ransomware, а wiper – ПЗ, розроблене для безповоротного знищення даних з метою спричинити хаос у системі охорони здоров'я.
2. Законодавча адаптація. Держава продемонструвала безпрецедентну швидкість змін, інтегруючи стандарти NIST та GDPR-орієнтовані локальні акти для захисту даних в умовах воєнного стану.
3. Кадровий дефіцит. В умовах мобілізації та міграції фахівців, Україна впроваджує автоматизовані системи захисту, що мінімізують потребу в ручному управлінні. Міністерство цифрової трансформації України стало рушієм цифрової трансформації публічного сектору України та популяризації електронних сервісів серед населення. Під час повномасштабної війни воно координує проєкти кіберзахисту, інформаційного спротиву та розвитку цифрової дипломатії, зберігаючи стабільність державних ІТ-систем і сервісів. Відомство відіграє ключову роль у створенні «держави у смартфоні» та впровадженні сервісу «Дія».

Викладене актуалізує проблему формування компетентності з кіберзахисту в майбутніх медичних працівників, зокрема й магістрів стоматології. Цей процес має складну історико-генезисну зумовленість, яка відображає еволюцію як стоматологічної практики, так і інформаційних технологій у системі охорони здоров'я. На початкових етапах розвитку медицини та стоматології захист даних обмежувався фізичною конфіденційністю паперових архівів, етичними нормами лікарської таємниці та інституційною відповідальністю медичного закладу. У цих умовах питання кіберзахисту як окремої професійної компетентності не актуалізувалося, а підготовка стоматологів орієнтувалася суто на клінічні навички та біомедичні знання.

Результати аналізу наукових джерел також допомогли виокремити низку історико-генезисних проблем формування компетентності з кіберзахисту у майбутніх медичних працівників. Поява перших інформаційних систем та впровадження електронних медичних карток започаткували нову фазу в розвитку професійної діяльності стоматолога, в якій зберігання, обробка та передавання медичних даних набули цифрової форми. Проте освітні програми з підготовки здобувачів вищої освіти спеціальності «Стоматологія» тривалий час не враховували ці зміни, зберігаючи біомедичну та техніко-мануальну домінанту підготовки. Це зумовило першу історико-генезисну проблему – розрив між цифровізацією стоматологічної практики і змістом професійної освіти, у межах якої питання захисту даних залишалися поза фокусом системної підготовки.

Подальший розвиток телемедицини, хмарних сервісів, цифрової рентгенології, CAD/CAM-технологій у протезуванні, систем управління стоматологічною клінікою та інтеграція стоматології в загальнонаціональні eHealth-платформи суттєво підвищили рівень кіберризиків. Стоматолог став не лише користувачем медичного обладнання, а й активним суб'єктом цифрового середовища, який щоденно працює з персональними даними пацієнтів, фінансовою інформацією, цифровими зображеннями та віддаленими сервісами. Водночас освітні стандарти і далі трактувати інформаційну безпеку як технічну або суто ІТ-проблему, що сформувало другу історико-генезисну проблему – інституційну маргіналізацію кіберзахисту в професійній підготовці стоматологів.

Третя проблема має соціально-професійний характер і пов'язана з домінуванням клінічного мислення над ризик-орієнтованим цифровим мисленням. У традиційній стоматологічній освіті безпека асоціюється переважно з інфекційним контролем, асептикою, радіацій-

ним захистом та клінічними протоколами, тоді як кіберзагрози сприймаються як абстрактні, малоймовірні або такі, що не впливають безпосередньо на клінічний результат. Це спричинило недооцінку людського фактора як ключового вектора кібератак і відсутність у здобувачів вищої освіти сформованих навичок кібергігієни, безпечної автентифікації, роботи з електронними медичними картками та захисту цифрових носіїв інформації.

Четверта історико-генезисна проблема зумовлена асинхронністю розвитку нормативно-правового поля й освітніх практик. Попри появу міжнародних стандартів захисту персональних даних (HIPAA, GDPR) і національних регуляторних актів у сфері eHealth, ці вимоги не було своєчасно інкорпоровано в освітні програми підготовки магістрів стоматології. У результаті майбутні фахівці отримують фрагментарні уявлення про правові аспекти захисту даних пацієнтів і не усвідомлюють власної юридичної відповідальності за порушення режиму конфіденційності в цифровому середовищі.

Нарешті, сучасний етап розвитку стоматології в умовах гібридних кіберзагроз, масового поширення ransomware-атак і зростання ролі IoMT (Internet of Medical Things) актуалізує п'яту історико-генезисну проблему – відсутність цілісної педагогічної моделі формування компетентності з кіберзахисту в майбутніх магістрів стоматології. Освітній процес і надалі орієнтований переважно на засвоєння знань, а не на формування практичних поведінкових патернів безпечної роботи з цифровими технологіями в реальних клінічних умовах.

Формування компетентності майбутніх медичних фахівців (зокрема у сфері кібербезпеки та цифрової гігієни) базується на поєднанні класичних дидактичних принципів і новітніх методологічних підходів. Це «фундамент», який визначає загальну стратегію навчання:

- Компетентнісний підхід: Зміщує акцент із накопичення знань на здатність практично діяти в нестандартних ситуаціях тобто орієнтація не на знання (умовно говорячи, що таке вірус), а на здатність діяти (як захистити дані пацієнта).
- Контекстний підхід: Навчання відбувається в умовах, максимального наближених до майбутньої професійної діяльності (наприклад, робота в інтерфейсі медичної інформаційної системи), а також через розв'язання реальних професійних ситуацій (кейсів) стоматолога.
- Міждисциплінарний підхід: Інтеграція медичних знань із технічними аспектами захисту даних та юридичними нормами (GDPR, HIPAA).
- Ризик-орієнтований підхід: Формування здатності прогнозувати загрози й оцінювати наслідки цифрових інцидентів для здоров'я пацієнта тобто формування мислення, спрямованого на випередження загроз.

Отже, історико-генезисний аналіз засвідчує, що проблеми формування компетентності з кіберзахисту в майбутніх магістрів стоматології мають системний характер і зумовлені розривом між темпами цифровізації стоматологічної практики та еволюцією освітніх стандартів, недооцінкою людського фактора, інституційною маргіналізацією кібербезпеки і відсутністю інтегрованої педагогічної концепції. Це обґрунтовує необхідність цілеспрямованої модернізації змісту професійної підготовки стоматологів і розроблення методики формування їхньої компетентності з кіберзахисту як складової професійної та етичної відповідальності в умовах цифрової медицини.

Кібербезпека в медичній галузі за останнє століття пройшла шлях від елементарного фізичного захисту паперових архівів до складних цифрових екосистем, у яких безпека даних стала критичною умовою безперервності лікування та безпеки пацієнтів. Сьогодні медичні дані є одним із найцінніших активів цифрової економіки, що зумовлює зростання кількості цілеспрямованих атак на заклади охорони здоров'я та трансформацію кіберзагроз у пряму за-

грозу життю людини. Історичний і порівняльний аналіз міжнародних регуляторних моделей США та ЄС засвідчує формування нової парадигми, в якій кібербезпека розглядається не як допоміжна ІТ-функція чи фінансові витрати, а як стратегічна інвестиція в довіру пацієнтів, операційну стійкість і національну безпеку.

Висновки та перспективи подальших розвідок. Ретроспективний аналіз еволюції кібербезпеки в галузі охорони здоров'я засвідчив трансформацію підходів до захисту даних. Встановлено, що кібербезпека перестала бути допоміжною ІТ-функцією і перетворилася на критичний фактор безпеки пацієнтів та забезпечення безперервності лікувального процесу. Визначено ключові педагогічні проблеми, що перешкоджають ефективному формуванню кіберкомпетентності майбутніх медичних фахівців. Основними з них є:

– історично зумовлений розрив між темпами цифровізації медицини та змістом освітніх програм;
– домінування традиційного клінічного мислення над цифровим ризик-орієнтованим підходом;
– відсутність цілісної педагогічної моделі навчання кіберзахисту.

Обґрунтовано теоретико-методологічні засади формування компетентності з кібербезпеки, що базуються на поєднанні компетентнісного, контекстного, міждисциплінарного та ризик-орієнтованого підходів. Це передбачає зміщення фокуса навчання з теоретичного засвоєння знань про цифрові загрози на формування практичних навичок безпечної професійної діяльності в реальних клінічних умовах.

Концептуалізовано роль людського фактора як ключового вектора кіберзагроз у медицині. Оскільки понад 95% порушень безпеки спричинено діями персоналу, системне навчання кібергігієни та формування професійної етики в цифровому середовищі є безальтернативним шляхом підвищення кіберрезилієнтності всієї системи охорони здоров'я.

Перспективи подальших досліджень полягають у розробленні та апробації конкретної методики формування компетентності з кіберзахисту для здобувачів вищої освіти спеціальності «Стоматологія», з урахуанням специфіки роботи з цифровими CAD/CAM-системами та персональними даними у приватній практиці.

Використані джерела

Бєліков, О. Б. (2025). Цифровізація стоматологічної освіти: виклики та перспективи формування професійної компетентності. *Вісник науки та освіти*, (4), 112–125. https://doi.org/10.52058/2786-6165-2025-9(39)-961-972

Верховна Рада України. (2021). *Стратегія кібербезпеки України*. https://zakon.rada.gov.ua/laws/show/447/2021

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

Кучеренко, І. І., Микитенко, П. В., Терентюк, В. Г., Ніжегородцев В. О. (2025). Стан обізнаності щодо кібербезпеки серед здобувачів вищої освіти НМУ імені О.О. Богомольця. *Медицина та фармація: освітні дискурси,* (4), 54–60. https://doi.org/ 10.32782/eddiscourses/2025-4-9

Литвинов, О., Ковальчук, І., & Грищенко, М. (2024). Кібербезпека як фактор ефективності закладів вищої освіти. *Пропілеї права та безпеки,* (5), 15–23. https://doi.org/10.32620/ pls.2024.5.02

Матвієнко, М. М. (2025). Методичний аспект формування компетентності з кібербезпеки магістрів медицини. *Вища освіта України,* 4(99), 62–69. https://doi.org/10.32782/NPU-VOU.2025.4(99).08

Національний координаційний центр кібербезпеки. (2022). *Cyber digest: Огляд подій в сфері кібербезпеки, грудень 2022*. https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20digest_December_2022.pdf

Стучинська, Н. В., & Матвієнко, М. М. (2025). Формування кіберграмотності як передумова компетентності з кібербезпеки майбутніх лікарів. *Медицина та фармація: освітні дискурси*, (4), 76–84. https://doi.org/10.32782/eddiscourses/2025-4-13

Стучинська, Н. В., Паламарчук, Ю. В., & Ніжегородцев, В. О. (2024). Кібербезпека як необхідна складова в підготовці майбутніх стоматологів. *Наукові записки: Педагогічні науки, 158*, 133–144. https://doi.org/10.31392/NZ-udu-158.2024.14

Adnan, M., Kutafina, E., & Beyan, O. (2024). Cybersecurity frameworks in healthcare data: Short literature review. *Studies in Health Technology and Informatics*, (306). https://doi.org/10.3233/SHTI240403

Alanazi, A. T. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. *Cureus,* 15(10), e47026. https://doi.org/10.7759/cureus.47026

Al-Qarni, A. U. (2023). Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications,* 14(5). https://doi.org/10.14569/IJACSA.2023.0140513

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eyers, D., & Martin, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making,* (20), 146. https://doi.org/10.1186/s12911-020-01161-7

Carello, M. P., et al. (2023). A systematization of cybersecurity regulations, standards and guidelines for the healthcare sector. *arXiv*. https://doi.org/10.48550/arXiv.2304.14955

De Gagne, J. C., Cho, E., Randall, P. S., Woodward, A., Park, H. K., & Yamane, S. S. (2023). Exploration of cyberethics in health professions education: A scoping review. *International Journal of Environmental Research and Public Health,* 20(22), 7048. https://doi.org/10.3390/ijerph20227048

European Commission. (n.d.). European health data space (EHDS). https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en

IITD. (2022). Технічний аналіз шкідливого завантажувача WhisperGate, націленого на українські організації. https://iitd.ua/tehnichnij-analiz-shkidlivogo-zavantazhuvacha-whispergate-naczilenogo-na-ukrayinski-organizacziyi/

Khatun, M. A., et al. (2024). Machine learning for healthcare IoT security: A review and risk mitigation. In *EEE Access*, vol. 11, pp. 145869-145896. https://doi.org/10.1109/ACCESS.2023.3346320

Kruse, C. S., et al. (2018). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Maturitas*. https://doi.org/10.1016/j.maturitas.2018.04.008

Parfonova, I., & Zinchenko, O. (2024). Cybersecurity enhancement in the field of eHealth system development in Ukraine. *Medical Perspectives,* 29(4), 247–256. https://doi.org/10.26641/2307-0404.2024.4.319402

Rocket.Chat. (2024). *EU NIS directive vs GDPR: Three key differences and why compliance matters*. https://www.rocket.chat/blog/eu-nis-directive

TechTarget. (2022). *HC3 outlines history of healthcare cybersecurity from 1980s to now*. https://www.techtarget.com/healthtechsecurity/news/366594895/HC3-Outlines-History-of-Healthcare-Cybersecurity-From-1980s-to-Now

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, (4). https://doi.org/10.3389/fdgth.2022.862221

References

Adnan, M., Kutafina, E., & Beyan, O. (2024). Cybersecurity frameworks in healthcare data: Short literature review. *Studies in Health Technology and Informatics*. https://doi.org/10.3233/SHTI240403 (in English).

Alanazi, A. T. (2023). Clinicians' perspectives on healthcare cybersecurity and cyber threats. *Cureus,* 15(10), e47026. https://doi.org/10.7759/cureus.47026 (in English).

Al-Qarni, A. U. (2023). Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. *International Journal of Advanced Computer Science and Applications,* 14(5). https://doi.org/10.14569/IJACSA.2023.0140513 (in English).

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J. M., O'Leary, C., Eyers, D., & Martin, A. (2020). Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, (20), 146. https://doi.org/10.1186/s12911-020-01161-7 (in English).

Belikov, O. B. (2025). Digitalization of dental education: Challenges and prospects for the formation of professional competence. *Perspectives and Innovations in Science (Pedagogy Series)*, (4), 112–125. https:// perspectives.pp.ua/index.php/vno/article/view/29799 (in Ukrainian).

Verkhovna Rada of Ukraine. (2021). *Ukraine's Cybersecurity Strategy*. https://zakon.rada.gov.ua/ laws/show/447/2021 (in Ukrainian).

Carello, M. P., et al. (2023). A systematization of cybersecurity regulations, standards and guidelines for the healthcare sector. *arXiv*. https://doi.org/10.48550/arXiv.2304.14955 (in English).

De Gagne, J. C., Cho, E., Randall, P. S., Woodward, A., Park, H. K., & Yamane, S. S. (2023). Exploration of cyberethics in health professions education: A scoping review. *International Journal of Environmental Research and Public Health,* 20(22), 7048. https://doi.org/10.3390/ijerph20227048 (in English).

European Commission. (n. d.). *European health data space (EHDS).* https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space-regulation-ehds_en (in English).

IITD. (2022). *Tekhnichnyi analiz shkidlyvoho zavantazhuvacha WhisperGate, natsilenoho na ukrainski orhanizatsii*. https://iitd.ua/tehnichnij-analiz-shkidlivogo-zavantazhuvacha-whispergate-naczilenogo-na-ukrayinski-organizacziyi/ (in Ukrainian).

Khatun, M. A., et al. (2024). Machine learning for healthcare IoT security: A review and risk mitigation. In *EEE Access*, vol. 11, pp. 145869-145896. https://doi.org/10.1109/ACCESS.2023.3346320 (in English).

Koval, B. F., Koval, L. D., & Poida, S. A. (2023). Teaching future doctors the basics of media literacy and cybersecurity. *Perspectives and Innovations in Science (Pedagogy Series, Psychology Series, Medicine Series),* 8(26), 171–183. https://doi.org/10.52058/2786-4952-2023-8–183 (in Ukrainian).

Kruse, C. S., et al. (2018). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Maturitas*. https://doi.org/10.1016/j.maturitas.2018.04.008 (in English).

Kucherenko, I. I., Mykytenko, P. V., Terentiuk, V. H., & Nizhehorodtsev, V. O. (2025). Stan obiznanosti shchodo kiberbezpeky sered zdobuvachiv vyshchoi osvity NMU imeni O. O. Bohomoltsia [The state of cybersecurity awareness among students at Bogomolets National Medical University]. *Medytsyna ta farmatsiia: osvitni dyskursy*, (4), 54–60. https://doi.org/ 10.32782/eddiscourses/2025-4-9 (in Ukrainian).

Litvinov, O., Kovalchuk, I., & Gryshchenko, M. (2024). Cybersecurity as a factor in the effectiveness of higher education institutions. *Propylaea of Law and Security*, (5), 15–23. https://doi.org/10.32620/pls.2024.5.02 (in Ukrainian).

Matvienko, M. M. (2025). Methodological aspects of developing cybersecurity competencies among medical master's students. *Higher Education in Ukraine*, 4(99), 62–69. https://doi.org/10.32782/NPUVOU.2025.4(99).08 (in Ukrainian).

National Cybersecurity Coordination Center. (2022). Cyber digest: Overview of cybersecurity events, December 2022. https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/%D0%9D%D0%9A%D0%A6%D0%9A-1/Cyber%20digest_December_2022.pdf (in Ukrainian).

Parfonova, I., & Zinchenko, O. (2024). Cybersecurity enhancement in the field of eHealth system development in Ukraine. *Medical Perspectives, 29*(4), 247–256. https://doi.org/10.26641/2307-0404.2024.4.319402 (in English).

Rocket.Chat. (2024). *EU NIS directive vs GDPR: Three key differences and why compliance*ю matters. https://www.rocket.chat/blog/eu-nis-directive (in English).

Stuchynska, N. V., & Matvienko, M. M. (2025). Developing digital literacy as a prerequisite for cybersecurity competence among future physicians. *Medicine and Pharmacy: Educational Discourses*, (4), 76–84. https://doi.org/10.32782/eddiscourses/2025-4-13 (in Ukrainian).

Stuchynska, N. V., Palamarchuk, Y. V., & Nizhegorodtsev, V. O. (2024). Cybersecurity as an essential component in the training of future dentists. *Scientific Notes: Pedagogical Sciences*, (158), 133–144. https://doi. org/10.31392/NZ-udu-158.2024.14 (in Ukrainian).

TechTarget. (2022). *HC3 outlines history of healthcare cybersecurity from 1980s to now*. https://www.techtarget.com/healthtechsecurity/news/366594895/HC3-Outlines-History-of-Healthcare-Cybersecurity-From-1980s-to-Now (in English).

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). *Frontiers in Digital Health*, (4). https://doi.org/10.3389/fdgth. 2022.862221 (in English).

Liliia Desiatniuk, *teacher, Department of Medical and Biological Physics and Computer Science, Bogomolets National Medical University, Kyiv, Ukraine.*
Research interests: *the implementation of innovative teaching methods, the digitization of education, the improvement of the Ukrainian education system, and ensuring its compliance with European standards.*

CYBERSECURITY IN MEDICAL EDUCATION: A RETROSPECTIVE ANALYSIS AND PEDAGOGICAL PRINCIPLES FOR DEVELOPING THE COMPETENCIES OF FUTURE MEDICAL PROFESSIONALS

Abstract. This article presents the results of a retrospective analysis of the development of cybersecurity in medical education as a component of the digital transformation of the healthcare system. It traces the evolution of approaches to protecting medical data—from ensuring the physical confidentiality of paper archives to the functioning of modern digital ecosystems encompassing electronic health records, telemedicine platforms, cloud services, the Internet of Medical Things (IoMT), artificial intelligence systems, and integrated eHealth environments.

The study analyzes key international regulatory models and cybersecurity standards (HIPAA, NIST, GDPR, NIS, EHDS) that define the current paradigm of proactive digital risk management in the healthcare sector. It examines contemporary cyber threats, including ransomware attacks, social engineering, DDoS attacks, leaks of confidential information, and vulnerabilities in IoMT devices, which directly impact the quality of medical care and the functioning of healthcare facilities. The paper highlights the specifics of the Ukrainian context of eHealth system development amid a hybrid war and targeted cyberattacks on critical medical infrastructure.

Particular attention is paid to the educational dimension of the problem. It is demonstrated that the growing digitalization of medical practice underscores the need to integrate cybersecurity as an interdisciplinary component of the professional training of future healthcare professionals. It is argued that a modern healthcare professional must possess not only clinical knowledge but also competencies in the areas of cyber hygiene, secure operation of electronic medical systems, protection of patients' personal data, recognition of digital threats, and adherence to the ethical and legal norms governing the practice of digital medicine.

The pedagogical foundations for developing cybersecurity competencies have been identified, including: competency-based, contextual, interdisciplinary, and risk-oriented approaches; the integration of clinical and digital thinking; and the use of case studies, simulation scenarios, and practice-oriented learning. The need to transition from fragmented information about cyber threats to the systematic development of behavioral models for safe professional practice in the digital environment is emphasized.

The historical and genesis-related barriers to the development of cybersecurity competence among future healthcare professionals are analyzed, including: the gap between the pace of digitalization in medical practice and the content of educational programs; the institutional marginalization of cybersecurity in medical education; the dominance of traditional clinical thinking over a risk-oriented digital approach; the asynchrony between the development of regulatory frameworks and educational reforms; insufficient integration of international cybersecurity standards into the professional training system; and the absence of a comprehensive pedagogical model for teaching cybersecurity to future medical professionals. The necessity of modernizing the content of medical education in accordance with the contemporary challenges of digital medicine and the cyber resilience of the healthcare system is substantiated.

Keywords: cybersecurity; medical education; professional training; cybersecurity competence; digital transformation; protection of medical data.