УДК 378.61.004.8
DOI https://doi.org/10.32782/eddiscourses/2025-4-13

ФОРМУВАННЯ КІБЕРГРАМОТНОСТІ ЯК ПЕРЕДУМОВА КОМПЕТЕНТНОСТІ З КІБЕРБЕЗПЕКИ МАЙБУТНІХ ЛІКАРІВ

Стучинська Наталія Василівна,
доктор педагогічних наук, професор, завідувачк кафедри медичної і біологічної фізики та інформатики,
Національний медичний університет імені О.О. Богомольця
ORCID: 0000-0002-5583-899X

Матвієнко Микола Миколайович,
аспірант кафедри медичної і біологічної фізики та інформатики,
Національний медичний університет імені О.О. Богомольця
ORCID: 0009-0004-5888-2584

Стаття присвячена формуванню кіберграмотності майбутніх лікарів як основи їхньої компетентності з кібербезпеки в умовах цифрової трансформації медицини. Обґрунтовано актуальність цілеспрямованого ознайомлення майбутніх лікарів з основними типами кіберзагроз у медичній сфері: malware/ransomware-атаки, що блокують доступ до електронних медичних записів; атаки відмови в обслуговуванні (DoS/DDoS), які паралізують роботу медичних інформаційних систем; фішинг і соціальна інженерія, орієнтовані на медичний персонал; витоки медичних даних (data breaches), що загрожують конфіденційності пацієнтів; атаки на медичні пристрої та Інтернет медичних речей (IoMT), що створюють пряму загрозу життю пацієнтів. Показано, що ці загрози безпосередньо впливають на безпеку пацієнтів, якість медичної допомоги, репутацію медичних установ, а в умовах війни набувають значення загроз національній безпеці. Представлено результати емпіричного дослідження, проведеного на базі Національного медичного університету імені О. О. Богомольця (n=127 студентів першого курсу медичного та стоматологічного факультетів), спрямованого на діагностику вихідного рівня обізнаності щодо специфічних кіберзагроз у медичній галузі. Встановлено, що лише 11,8% студентів були обізнані про конкретні типи медичних кіберзагроз і могли їх пояснити, при цьому найнижчим був рівень обізнаності щодо атак на IoMT (6,3%) та інсайдерських загроз (9,4%). З'ясовано, як ці загрози, що безпосередньо впливають на якість медичної допомоги, детермінують специфіку та вимоги до підготовки майбутніх лікарів, зумовлюючи необхідність формування в них обізнаності й компетентності у сфері захисту цифрових даних. Кібербезпеку майбутнього лікаря запропоновано розглядати як інтегральне утворення, що поєднує когнітивний, діяльнісний та ціннісно-етичний компоненти цифрової компетентності та забезпечує здатність свідомо і безпечно використовувати у професійній діяльності увесь спектр необхідних цифрових технологій. Обґрунтовано доцільність інтеграції обізнаності з кібербезпеки в кейс-орієнтоване та симуляційне навчання, роль яких зростає у процесі підготовки здобувачів вищої медичної освіти. Зроблено висновок про те, що системне ознайомлення з основними кіберзагрозами створює когнітивну основу кіберграмотності та мотиваційне підґрунтя для подальшого поглибленого вивчення методів і засобів кібербезпеки в професійній медичній діяльності, а також сприяє формуванню культури цифрової відповідальності майбутніх лікарів.

Ключові слова: кібербезпека, кіберграмотність, медична освіта, вибіркові дисципліни, магістри медицини, компетентнісний підхід, цифрова компетентність, майбутні лікарі, кіберзагрози, обізнаність, медичні інформаційні системи, цифрова етика, фішинг, витоки даних, інсайдерські інциденти, Інтернет медичних речей (IoMT), ransomware, DDoS-атаки.

Stuchynska Natalia, Matvienko Mykola. Formation of cyberliteracy as a prerequisite for cybersecurity competence of future doctors

The article addresses the development of cyber literacy among future physicians as a foundation of their cybersecurity competence within the context of the digital transformation of healthcare. The urgency of targeted familiarization of medical students with key types of cyber threats in the medical domain is substantiated, including: malware/ransomware attacks that block access to electronic medical records; denial-of-service attacks (DoS/DDoS) that paralyze medical information systems; phishing and social engineering targeting healthcare personnel; data breaches that jeopardize patient confidentiality; attacks on medical devices and the Internet of Medical Things (IoMT), which pose direct risks to patient safety. It is demonstrated that these threats directly affect patient security, quality of medical services, and the reputation of healthcare institutions, and under wartime conditions may escalate into national security threats. The article presents

results of an empirical study conducted at Bogomolets National Medical University (n = 127 first-year students of medical and dental faculties), aimed at diagnosing baseline awareness of specific cyber threats in healthcare. It was found that only 11.8% of students were aware of concrete types of cyber threats and could explain them, with the lowest awareness observed regarding IoMT-related attacks (6.3%) and insider threats (9.4%). The study reveals how such threats, directly affecting the quality of medical care, shape specific requirements for medical training, necessitating the development of awareness and competence in digital data protection. Cybersecurity of a future physician is conceptualized as an integral formation combining cognitive, operational, ethical-value components of digital competence and provides the ability to consciously and safely use the full range of necessary digital technologies in professional activities.

The article substantiates the integration of cybersecurity content into case-based and simulation-based learning in medical education. It is concluded that systematic introduction to core cyber threats provides the motivational and cognitive groundwork for further in-depth study of cybersecurity tools and practices in professional medical activity, and fosters a culture of digital responsibility among future physicians.

Key words: cybersecurity, cyber literacy, medical education, elective disciplines, masters of medicine, competency-based approach, digital competence, future physicians, cyber threats, awareness, medical information systems, digital ethics, phishing, data breaches, insider incidents, Internet of Medical Things (IoMT), ransomware, DDoS attacks.

Обґрунтування актуальності проблеми. В умовах сучасного світу кібербезпека є глобальною проблемою, адже цифрові технології постійно стають об'єктом кіберзагроз, а медична сфера – однією з найчутливіших до втручання у дані та порушення інформаційної безпеки. Цифровізація охорони здоров'я, впровадження медичних інформаційних систем (МІС), електронних медичних карток, телемедичних сервісів, систем дистанційного моніторингу пацієнтів та пристроїв Інтернету медичних речей (Internet of Medical Things, IoMT) створюють нові можливості для підвищення якості медичної допомоги, але водночас породжують нові канали вразливості. Неналежний рівень готовності до протидії кібератакам може призвести до безпосередньої загрози життю й здоров'ю пацієнтів та зриву лікувальних процесів. Ситуація, пов'язана з кіберзагрозами в медицині, загострилася під час пандемії COVID-19, коли відбулося стрімке розгортання телемедичних платформ, систем дистанційного моніторингу та мобільних додатків для взаємодії «лікар–пацієнт». Безпрецедентний перехід до віддаленого надання медичної допомоги відкрив нові точки доступу для кібератак, зробивши критично важливими питання захисту каналів зв'язку, автентифікації користувачів, збереження конфіденційності та цілісності даних. У цьому контексті важливими чинниками стала цифрова стійкість медичних установ, захист персональних та медичних даних, а також здатність медичних працівників швидко реагувати на потенційні кіберризики. Тому для здобувачів ступеня магістра медицини особливо актуальною є готовність працювати в умовах постійно зростаючих цифрових загроз, вміти своєчасно їх ідентифікувати та приймати обґрунтовані рішення щодо захисту даних пацієнтів і безперервності надання медичної допомоги. Показово, що аналогічні виклики проявляються і в освітньому середовищі, де цифровізація процесів навчання формує подібні вразливості. Відтак проблема кібербезпеки загострилася після масового переходу університетів на дистанційне й змішане навчання. Широке використання віртуальних систем управління навчанням, хмарних сховищ, відеоконференцій породило нові ризики: фішингові атаки на акаунти викладачів і студентів, несанкціонований доступ до навчальних платформ, порушення конфіденційності навчальних даних.

Варто зазначити, що державна політика у сфері кібербезпеки формувалася поступово й передувала воєнним викликам сьогодення, задаючи нормативну основу, на яку спирається наразі безпекова практика воєнного часу. Держава відповідає на ці виклики ухваленням стратегічних документів: «Стратегії кібербезпеки України» (2016, оновлена редакція 2021 р.), «Доктрини інформаційної безпеки України» (2017), «Плану реалізації Стратегії кібербезпеки України» (2022), Закону України «Про захист інформації в інформаційно-комунікаційних системах», а також Закону України від 27 березня 2025 року щодо захисту інформації та кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури (реєстр. № 11290) [1–6]. Сектор охорони здоров'я наразі розглядається як елемент критичної національної інфраструктури, який, відповідно, стає мішенню цілеспрямованих кібератак в умовах воєнного часу. Чутлива інформація про стан здоров'я військовослужбовців, маршрути медичної евакуації, структура медичної логістики, дані електронної системи охорони здоров'я (ЕСОЗ) набувають стратегічного значення.

На міжнародному рівні кібербезпека закріплена як стратегічний пріоритет розвитку цифрового суспільства (Конвенція Ради Європи про кіберзлочинність, Політична програма «Цифрове десятиліття» ЄС, Декларація про цифрові права і принципи тощо). У цих документах наголошено

на необхідності підготовки фахівців, які здатні діяти відповідально в умовах кіберризиків. Отже, актуальність дослідження проблеми кібербезпеки в медичній освіті зумовлена:

– зростанням кількості та складності кібератак на медичну інфраструктуру;

– посиленням нормативних вимог до захисту інформації;

– воєнним контекстом і статусом охорони здоров'я як критичної інфраструктури;

– недостатнім рівнем готовності здобувачів вищої медичної освіти до роботи в умовах цифрових загроз.

Аналіз останніх досліджень та публікацій. Оскільки кібербезпека в медицині виступає інтегральною характеристикою професійної діяльності лікаря, що містить захист даних, цифрову етику та протидію загрозам, ключового значення набуває належна підготовка майбутніх лікарів, спрямована на розвиток їхньої цифрової обізнаності та компетентності у сфері кібербезпеки. Це узгоджується з положеннями Європейської рамки цифрової компетентності DigComp 2.2 [6], у якій компонент «Безпека» охоплює захист пристроїв, персональних даних, а також відповідальність за цифрові дії в інтегрованому інформаційному середовищі. Для охорони здоров'я це особливо важливо, оскільки цифровізація медичних процесів (від ведення медичних записів до використання систем підтримки клінічних рішень) робить очевидною вразливість інформаційної інфраструктури.

Важливим напрямом міжнародних досліджень є аналіз ризиків, пов'язаних із підключеним медичним обладнанням та технологіями IoMT. Огляди систематизують типові загрози, що виникають при взаємодії мережевих медичних пристроїв: від компрометації каналів передачі даних до потенційного втручання у параметри роботи обладнання та несанкціонованого доступу до масивів медичних даних. У контексті навчання студентів-медиків це означає потребу у формуванні в них практичних навичок безпечного використання медичних пристроїв, розпізнавання ознак їх компрометації та розуміння взаємозв'язку між IT-захистом і клінічною безпекою пацієнта [7-9].

Дослідження з кібербезпеки в лікарнях показують, що провідну роль у забезпеченні захисту відіграє людський чинник. Вони доводять, що навіть за наявності розвиненої технічної інфраструктури вразливості зумовлені помилками персоналу, недостатньою обізнаністю та відсутністю культури безпечної цифрової поведінки [10]. Своєю чергою існує також акцент на організаційних аспектах кібербезпеки: політики доступу, розподіл відповідальності [11]. Аналогічні висновки можуть бути екстрапольовані і на підготовку майбутніх лікарів: саме формування у студентів стійких практик цифрової обережності, критичного мислення та відповідальної поведінки в інформаційному середовищі стає ключовим чинником запобігання кіберзагрозам у майбутній професійній практиці.

В українському дослідницькому полі проблема цифрової компетентності та кібербезпеки в медичній освіті розглядається переважно в контексті загальної цифровізації навчального процесу. Л. В. Батюк аналізує цифрову компетентність студентів медичних закладів освіти при вивченні дисципліни «Інформатизація у сфері громадського здоров'я», наголошуючи на необхідності цілеспрямованого формування цифрових навичок у межах професійної підготовки, однак без виокремлення безпекового аспекту роботи в цифровому середовищі [12]. Дослідження, присвячені розвитку електронної системи охорони здоров'я та її кіберзахисту в Україні, демонструють зростання уваги до роботи з електронними медичними записами, eHealth-системами та цифровими платформами взаємодії «лікар–пацієнт», при цьому звертаючи увагу на потенційні ризики для захисту медичних даних [13].

Важливим складником національного дискурсу є праці, що стосуються формування цифрової компетентності майбутніх лікарів, в структурі якої цифрова безпека постає як ключовий компонент професійної готовності до роботи з медичними даними. Так, Н. В. Стучинська у дослідженнях, проведених на базі Національного медичного університету імені О. О. Богомольця, розглядає формування цифрової компетентності майбутніх стоматологів [14] та окреслює роль вибіркових дисциплін у підвищенні рівня цифрової компетентності майбутніх лікарів [15]. П. В. Микитенко [16] пропонує підходи до діагностики рівнів IT-компетентності студентів-медиків у процесі вивчення медичної інформатики, що створює емпіричну основу для подальшої побудови моделей цифрової компетентності. Ці дослідження демонструють практичні підходи до інтеграції цифрових технологій у професійну підготовку та підтверджують необхідність поетапного ускладнення змісту цифрових умінь, поступового переходу від базової цифрової грамотності до спеціалізованої компетентності у сфері кіберзахисту клінічних даних і взаємодії з медичними інформаційними системами.

Особливе місце у сформованій науковій традиції посідають напрацювання В. Г. Терентюка [17] у якого наголошено на ролі цифрової обізнаності медичного персоналу у забезпеченні стабільності функціонування цифрових медичних систем, профілактиці кіберінцидентів та формуванні довіри до цифрової медицини. Актуальною є в цьому сенсі є інформація, подана в Звіті за грантовим проєктом (2023–2024) «Роль та значення розвитку цифрових компетентностей працівників охорони здоров'я **…**». Цей проєкт стосується створення/оновлення освітніх програм для медичних і фармацевтичних навчальних закладів із урахуванням цифрових викликів [18].

Утім попри значну кількість праць про цифровізацію медицини, питання системної підготовки майбутніх лікарів до роботи в умовах кіберризиків залишається недостатньо розробленим і потребує спеціального теоретичного та методичного обґрунтування.

Мета дослідження полягає в розкритті змісту кібербезпеки як складника цифрової компетентності майбутніх лікарів, систематизації основних типів кіберзагроз у медичній сфері та обґрунтуванні методичних орієнтирів щодо інтеграції змісту кібербезпеки в медичну освіту.

Методи дослідження. У дослідженні використано комплекс теоретичних методів:

– **аналіз і синтез** – для вивчення наукових праць, міжнародних і національних нормативних документів із проблем цифрової компетентності, кібербезпеки, цифровізації медицини;

– **порівняння й узагальнення** – для зіставлення зарубіжних і вітчизняних моделей інтеграції кібербезпеки в освіту медичних працівників, виявлення спільних і відмінних рис;

– **структурно-функціональний аналіз** – для виділення основних типів кіберзагроз у медичному середовищі та визначення їхнього зв'язку з компонентами професійної компетентності лікаря;

– **елементи моделювання** – для окреслення можливих напрямів кейс-орієнтованого навчання основам кібербезпеки в медичній освіті.

Стаття має теоретико-аналітичний характер і є етапом концептуального осмислення проблеми, що передує розробленню та емпіричній перевірці конкретних методик.

Виклад основного матеріалу дослідження. Сучасна кібербезпека в медичній освіті має багатовимірний зміст, що включає: **знання** про цифрові загрози, архітектуру медичних інформаційних систем, вимоги законодавства, принципи захисту даних; **уміння** використовувати цифрові інструменти та медичні інформаційні системи з дотриманням принципів кібергігієни, виявляти ознаки атак, діяти відповідно до протоколів реагування; **ціннісні орієнтації** відповідального використання цифрових технологій, дотримання етичних норм і прав пацієнтів щодо конфіденційності й недоторканності інформації.

Для чіткості подальшого викладу матеріалу вважаємо за необхідне надати авторське розуміння двох базових понять, які становлять концептуальну основу дослідження.

Кібербезпека – це стан захищеності цифрового середовища, за якого дані та процеси залишаються цілісними, конфіденційними і доступними, а дія кіберзагроз – передбаченою та контрольованою. Таке визначення акцентує не на технічних заходах захисту як таких, а на результативному стані системи, що дозволяє в контексті медичної освіти говорити про кібербезпеку як про інтегральну характеристику професійної діяльності лікаря, а не суто про ІТ-компетенцію.

Кіберграмотність – це здатність діяти компетентно й відповідально в цифровому середовищі, розпізнаючи ризики, обираючи безпечні рішення та критично оцінюючи інформаційні впливи. На відміну від вужчого терміна «цифрова грамотність», який часто редукується до технічних навичок користування, кіберграмотність включає ціннісно-рефлексивний вимір, критично важливий для майбутніх лікарів, які працюватимуть із чутливими даними про здоров'я та життя пацієнтів.

Відтак, кібербезпеку майбутнього лікаря будемо розглядати як інтегральне утворення, що поєднує когнітивний, діяльнісний та ціннісно-етичний компоненти цифрової компетентності та забезпечує здатність свідомо і безпечно використовувати у професійній діяльності увесь спектр необхідних цифрових технологій.

Ці терміни не претендують на статус універсальних, проте вони визначають ключові концепти дослідження. Саме в такому значенні поняття *кібербезпека* та *кіберграмотність* використовуються в подальшому тексті статті.

Із позицій педагогічної теорії кібербезпека як компонент цифрової компетентності є показником сформованості критичного мислення, цифрової етики та професійної відповідальності [19]. Отже, вона відображає здатність майбутнього лікаря не лише оперувати клінічними даними, а й усвідомлювати наслідки їх неналежного захисту – від індивідуальних ризиків для пацієнта до загроз національній безпеці в умовах війни.

Важливим елементом формування цієї компетентності є розуміння конкретних типів кібер-

загроз. Найбільш поширеними для медичного середовища є атаки типу **malware/ransomware**, унаслідок яких дані медичних інформаційних систем шифруються, а за їх розблокування вимагається викуп. Такі інциденти унеможливлюють доступ до електронних медичних записів, результатів досліджень, планів лікування, що прямо впливає на безпеку пацієнтів. Стратегіями захисту є регулярне оновлення систем, використання сучасних антивірусних рішень, політики резервного копіювання, сегментація мереж. Для майбутніх лікарів надзвичайно важливо розуміти, що навіть тимчасова недоступність даних не є абстрактною «технічною проблемою», а може означати затримку в постановці діагнозу, призначенні терапії, проведенні операції. Оскільки симуляційні технології використовуються під час підготовки майбутніх лікарів [24], з освітньої точки зору доречним є використання кейс-симуляцій атак ransomware, під час яких студенти відпрацьовують дії медичного персоналу в умовах недоступності електронних систем (перехід на резервні протоколи, пріоритизація відновлення критичних баз даних, комунікація з пацієнтами).

Не менш значущими є атаки **відмови в обслуговуванні (DDoS)**, які спричиняють перевантаження серверів та мережевої інфраструктури. У медичній сфері такі атаки можуть блокувати системи електронної реєстрації, телемедичні сервіси й доступ до електронних архівів. Для підготовки майбутніх лікарів важливо моделювати ситуації, коли цифрові сервіси недоступні, а команда повинна оперативно переходити на резервні канали зв'язку, мінімізуючи ризики для пацієнтів.

Окрему категорію становлять атаки, засновані на **соціальній інженерії**, зокрема фішинг. Вони орієнтовані не на технічні вразливості системи, а на людські слабкості: довірливість, поспіх, недостатню обізнаність. Фішингові атаки базуються на обмані користувача через листи, SMS, повідомлення в месенджерах, підроблені сторінки входу. Для медичних установ типовим є маскування під офіційні повідомлення: «адміністратор системи», «постачальник ПЗ», «колега з лікарні» тощо. Відкриття шкідливого вкладення або введення пароля на фальшивому сайті може стати стартом для зараження мережі, запуску ransomware, витоку даних. Дослідження [10] демонструє, що подібні інциденти часто пов'язані з відсутністю системного навчання персоналу. Тому в освітньому процесі необхідні не лише тренінги з розпізнавання фішингових повідомлень, аналізу заголовків листів, перевірки доменів і безпечної роботи з вкладеннями, але й упровадження навчально-методичного супроводу: чітких алгоритмів реагування, чек-листів цифрової безпеки, симуляційних сценаріїв атак та систематичного моніторингу сформованості компетентності з кібергігієни у студентів.

Витоки даних (data breaches) є особливо чутливими через специфіку медичної інформації. Вони означають несанкціонований доступ до медичної інформації, який може бути зумовлений як зовнішніми зломами, так і помилками або недобросовісними діями персоналу. Електронні медичні записи містять не тільки ідентифікаційні дані, а й чутливу клінічну інформацію, що робить їх надзвичайно привабливими для кіберзлочинців. За даними галузевої аналітики HIPAA Journal [20], у США кількість скомпрометованих записів пацієнтів упродовж останніх років досягала рекордних показників, що свідчить про масштаб проблеми. Наслідки витоків виходять за межі фінансових збитків: можливі також шахрайські операції зі страховками, шантаж, дискримінація, психологічний тиск, а у воєнних умовах – створення загроз для військовослужбовців і членів їхніх родин. У навчанні студентів-медиків доцільно використовувати кейси інцидентів витоку даних, у яких відпрацьовується аналіз причин (слабкі паролі, надмірні права доступу, відсутність шифрування, недотримання процедур), визначення масштабу компрометації, планування заходів реагування та попередження повторних випадків.

Інсайдерські загрози пов'язані з діями співробітників або підрядників, які мають легальний доступ до інформаційних систем. Це можуть бути як навмисні зловживання, так і ненавмисні порушення (використання слабких паролів, передача доступів стороннім, зберігання службової інформації на особистих пристроях). В одному дослідженні [21] звертається увага на те, що інформаційна безпека в охороні здоров'я значною мірою залежить від того, наскільки чітко в організації визначено політики доступу, розподілено відповідальність і налагоджено внутрішній контроль. З педагогічної точки зору важливо сформувати в майбутніх лікарів розуміння, що кожний працівник є суб'єктом кібербезпеки, а не «пасивним користувачем системи». Це передбачає дотримання принципу мінімально необхідних повноважень, усвідомлене ставлення до обробки даних, недопущення несанкціонованого копіювання інформації.

Нарешті, однією з найбільш небезпечних форм кібератак є втручання у медичні пристрої та техно-

логії **Internet of Medical Things (IoMT)**, що поєднує інформаційну й клінічну безпеку. Атаки на медичні пристрої та IoMT (так звані MEDJACK) можуть призвести як до витоку даних, так і до безпосередньої загрози життю пацієнтів. Martin, S., & Harrison, V. (2023) [22] у своєму дослідженні показали вразливість імплантованих медичних пристроїв до несанкціонованого доступу, а Khaled, A. (2022) розглядає таксономію ризиків для Інтернету медичних речей, підкреслюючи складність захисту розподілених медичних мереж. Відомі випадки, коли через вразливості в налаштуваннях мережі зловмисники отримували доступ до медичних пристроїв і могли теоретично змінювати параметри інфузійних помп, порушувати роботу апаратів діагностики, використовувати обладнання як «точку входу» для подальшого поширення шкідливого програмного забезпечення. Для майбутніх лікарів необхідно розуміти, що безпека медичного обладнання – не суто технічна проблема, а складник клінічної безпеки. Тому в освітніх програмах необхідно акцентувати увагу на дотриманні протоколів безпечної експлуатації обладнання, значенні своєчасних оновлень програмного забезпечення, контролі підозрілих збоїв у роботі пристроїв.

Описані типи атак (ransomware, DDoS, фішинг, витоки даних, інсайдерські інциденти, MEDJACK) можуть виступати основою для навчальних кейсів, побудованих на реалістичних сценаріях. Студенти мають не просто читати теоретичні описи, а розв'язувати практичні ситуації, пропонувати алгоритми дій, оцінювати клінічні, організаційні та етичні наслідки. Окремий акцент варто зробити на симуляціях інцидентів: наприклад, раптова недоступність електронної системи, підозрілі листи, виявлення факту витоку даних чи компрометації медичного пристрою. Такі завдання сприяють розвитку не лише знань, а й операційного мислення, стресостійкості, навичок командної взаємодії між медичним і IT-персоналом.

Навчання кібербезпеки має включати розгляд норм українського законодавства («Про захист персональних даних», «Про захист інформації в інформаційно-комунікаційних системах», спеціальних актів щодо ЕСОЗ), міжнародних стандартів (GDPR, рекомендації ВООЗ), а також етичних засад роботи з вразливими групами пацієнтів. Важливо, щоб студенти розуміли не лише «як» технічно забезпечується захист, а й «чому» це є моральним і правовим обов'язком лікаря.

Поза формальними курсами важливо підтримувати в студентів сталий інтерес до теми кібербезпеки: проводити короткі тренінги, інформаційні кампанії, залучати до участі у профільних заходах, аналізувати актуальні кіберінциденти в медичній сфері. Це сприяє перетворенню знань на стійкі поведінкові патерни – уважність до паролів, обережність із листами та вкладеннями, дотримання протоколів доступу до медичних інформаційних систем.

Для верифікації гіпотези про необхідність цілеспрямованого ознайомлення студентів-медиків з основними типами кіберзагроз перед початком систематичного вивчення теми кібербезпеки було проведено емпіричне анкетування на базі Національного медичного університету імені О. О. Богомольця.

В анкетуванні взяли участь 127 студентів першого курсу спеціальності «Медицина» у рамках вивчення дисципліни «Медична інформатика» (2024–2025 навчальний рік). Анкета містила 12 питань, серед яких ключовими були: «Чи знаєте ви, що таке ransomware-атаки на медичні установи?», «Чи чули ви про фішингові атаки, спрямовані на медичний персонал?», «Чи знайомі ви з поняттям Internet of Medical Things (IoMT) та загрозами, пов'язаними з ним?», «Чи розумієте ви, що таке інсайдерські загрози в контексті медичних даних?», «Чи можете ви навести приклади витоків медичних даних в Україні або світі?».

Результати анкетування виявили критично низький рівень обізнаності студентів першого курсу щодо специфічних кіберзагроз у медичній галузі (рис. 1).

Як видно з рисунку, лише від 6,3% до 24,4% студентів могли пояснити сутність конкретних типів кіберзагроз у медичній галузі. Найменшою була обізнаність щодо атак на IoMT (6,3%) та інсайдерських загроз (9,4%). Водночас понад третину студентів (37,0–61,4%) взагалі не були знайомі з відповідними термінами. Додаткове питання «Чи можете ви навести приклад реального інциденту порушення кібербезпеки в медичній установі?» виявило, що лише 7 студентів (5,5%) змогли згадати конкретні випадки, причому всі вони посилалися на загальні новини про «злом лікарень», без розуміння специфіки атаки. На питання «Чи вважаєте ви, що кібербезпека буде важливою для вашої майбутньої професії лікаря?» 89,8% студентів відповіли ствердно, проте в обґрунтуваннях переважали загальні формулювання на кшталт «це важливо в сучасному світі», «треба захищати дані», без конкретизації медичного контексту. Це свідчить про наявність абстрактного розуміння важливості теми за від-

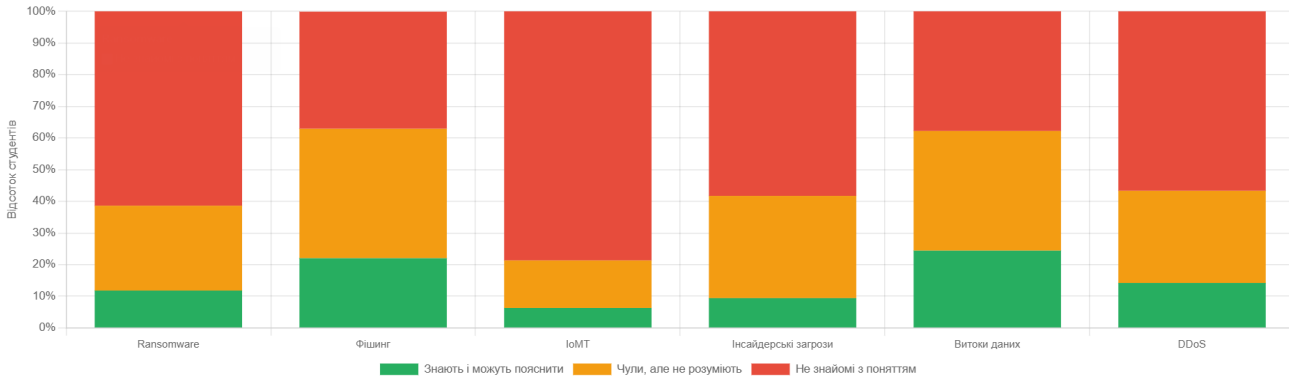

Рис. 1. Рівень обізнаності щодо специфічних кіберзагроз у медицині

сутності предметних знань. Результати анкетування вказують на критичну прогалину в базовій цифровій освіті майбутніх лікарів: студенти першого курсу, які є цифровими аборигенами (digital natives), мають високий рівень володіння цифровими інструментами в побутовому контексті, але майже не обізнані зі специфічними ризиками використання таких інструментів у професійній медичній діяльності. Це підтверджує тезу про те, що загальна цифрова грамотність не еквівалентна професійній цифровій компетентності, а кібербезпека в медицині потребує особливої підготовки з урахуванням галузевої специфіки.

Висновки. Кібербезпека в умовах цифрової трансформації охорони здоров'я є базовою умовою гарантування безпеки пацієнтів, конфіденційності медичних даних і стійкості функціонування медичних установ. Для України, яка переживає повномасштабну війну, ця проблема має додатковий вимір як елемент захисту критичної інфраструктури та національної безпеки. Аналіз міжнародних і вітчизняних досліджень показує, що, попри швидкий розвиток цифрової медицини та наявність значного масиву робіт із цифрової компетентності, питання системного формування компетентності з кібербезпеки майбутніх лікарів залишаються недостатньо розробленими. Безпековий компонент часто розглядається фрагментарно, без чіткої дидактичної моделі. Систематизовано основні типи кіберзагроз, релевантних для медичної сфери (malware/ransomware, DDoS-атаки, фішинг, витоки даних, інсайдерські загрози, атаки на медичні пристрої та IoMT) і показано, що вони мають безпосередній вплив на клінічну практику, репутацію лікаря, довіру пацієнтів, а в окремих випадках – на обороноздатність держави. Компетентність з кібербезпеки майбутнього лікаря доцільно розглядати як інтегральне утворення, що поєднує когнітивний, діяльнісний та ціннісно-етичний компоненти цифрової компетентності й забезпечує готовність до безпечної взаємодії з цифровими медичними системами. Вона є невід'ємним складником цифрової компетентності й має формуватися цілеспрямовано в процесі професійної підготовки.

Встановлено, що вихідний рівень обізнаності студентів першого курсу щодо специфічних кіберзагроз у медичній галузі є критично низьким: лише 11,8% студентів могли правильно ідентифікувати всі основні типи загроз.

Обґрунтовано інтеграцію змісту кібербезпеки в медичну освіту через кейс-орієнтований та симуляційний підходи, поєднання технічного, правового й етичного компонентів, формування культури кібергігієни. Реалізація цих орієнтирів створює передумови для побудови ефективної системи навчання основам кібербезпеки майбутніх лікарів. Перспективними напрямами подальших досліджень є: розроблення та емпірична перевірка конкретних навчальних моделей (наприклад, тематично-блокової моделі з використанням кейс-методу), створення діагностичного інструментарію для оцінки рівня сформованості компетентності з кібербезпеки у студентів медичних університетів, а також розроблення галузевих стандартів компетентності в кібербезпеці для різних категорій медичних працівників.

Список літератури:

1. Стратегія кібербезпеки України (затв. Указом Президента України від 26.08.2021 р. № 447/2021). URL: https://www.president.gov.ua/documents/4472021-40013
2. Доктрина інформаційної безпеки України (затв. Указом Президента України від 25.02.2017 р. № 47/2017). URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text

3. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. № 80/94-ВР (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
4. 4. Закон України «Про захист персональних даних» від 01.06.2010 р. № 2297-VI (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
5. Закон України від 27.03.2025 р. № 11290 щодо захисту інформації та кіберзахисту державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.
6. Carretero S., Vuorikari R., Punie, Y. *DigComp 2.2: The Digital Competence Framework for citizens. Update phase 1: The conceptual reference model*. Publications Office of the European Union. 2022.
7. Selvaraj S., Sundaravaradhan S. Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Applied Sciences*, 2020. 2, 1–8.
8. Sardi A., Rizzi A., Sorano E., Giussani A. The role of data breaches in healthcare sector: A systematic literature review. *Health Policy and Technology*, 2020. 9(4), 100–117.
9. Alsubaei F., Abuhussein A., Shikfa A., Shiva S. Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment. *IEEE Access*, 2019. 7, 170–188.
10. Jalali M. S., Kaiser J. P. Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, 2018. 20(5), e10059.
11. Aksoy C. Building a Cyber Security Culture for Resilient Organizations Against Cyber Attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 2024. 7(1), 96–110.
12. Батюк Л. В. Цифрова компетентність студентів медичних закладів освіти при вивченні дисципліни «Інформатизація у сфері громадського здоров'я». *Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: методологія, теорія, досвід, проблеми*, 2022. (62), 22–27.
13. Парфьонова І., Зінченко О. Cybersecurity enhancement in the field of eHealth system development in Ukraine. *Медична перспектива*, 2024. 29(2), 37–45.
14. Стучинська Н. В., Паламарчук Ю. В. Формування цифрової компетентності майбутніх стоматологів. *Медицина та фармація: освітні дискурси*, 2024. (2), 43–48.
15. Стучинська Н. В., Матвієнко М. М. Роль вибіркових дисциплін у формуванні цифрової компетентності майбутніх лікарів. *Педагогіка формування творчої особистості у вищій і загальноосвітній школах*, 2023. (88), 138–145.
16. Микитенко П. В. 2018. Діагностика рівнів ІТ-компетентності іноземних студентів у процесі вивчення медичної інформатики. *Комп'ютер у школі та сім'ї*, 2023. (8), 3–10.
17. Терентюк В. Г., Кучеренко І. І., Матукова-Ярига Д. Г. Роль та значення розвитку цифрових компетентностей працівників охорони здоров'я, здобувачів медичної та фармацевтичної освіти та науково-педагогічних працівників закладів вищої медичної освіти в умовах цифровізації та цифрової трансформації охорони здоров'я. *Медицина та фармація: освітні дискурси*, 2024. (3).
18. Національний медичний університет імені О. О. Богомольця. (2024). Реалізація грантового проєкту USAID "Підтримка реформи охорони здоров'я": матеріали з оприлюднення результатів грантової програми. URL: https://nmuofficial.com/grantova-diyalnist/realizatsiya-grantovogo-proektu-usaid-pidtrymka-reformy-ohorony-zdorov-ya/materialy-z-oprylyudnennya-rezultativ-grantovoyi-programy
19. Петренко Л. Цифрова безпека в структурі цифрової компетентності майбутнього викладача педагогічного закладу вищої освіти: змістовий компонент. *Освіта дорослих: теорія, досвід, перспективи*, 2023. 23(1), 98–109.
20. HIPAA Journal. (2023). *Healthcare Data Breach Statistics*. URL: https://www.hipaajournal.com/healthcare-data-breach-statistics/
21. Information security management in the operations of healthcare entities. (2024). *Scientific Papers of Silesian University of Technology. Organization and Management Series*, 192, Article 11.
22. Martin S., Harrison V. Cybersecurity vulnerabilities in integrated medical devices and their risks to patient safety. *Cybersecurity Vulnerabilities in Integrated Medical Devices and Their Risks to Patient Safety.* 2023.
23. Khaled A. Internet of medical things (IoMT): Overview, taxonomies, and classifications. *Journal of Computer and Communications*, 2022. 10(8), 64–89.
24. Кучин Ю. Л., Канюра О. А., Мельник В. С., Стучинська Н. В., Микитенко П. В. Симуляційні технології у системі підготовки майбутніх лікарів в умовах Covid-19. *Науковий часопис НПУ імені М.П. Драгоманова. Серія 5. Педагогічні науки: реалії та перспективи: Збірник наукових праць. Київ: Видавничий дім «Гельветика».* 2022. Вип. 86. С. 132–142.

References:

1. Stratehiia kiberbezpeky Ukrainy [Cybersecurity Strategy of Ukraine] (2021). Approved by the Decree of the President of Ukraine dated 26.08.2021 No. 447/2021. Retrieved from: https://www.president.gov.ua/documents/4472021-40013
2. Doktryna informatsiinoi bezpeky Ukrainy [Doctrine of Information Security of Ukraine] (2017). Approved by the Decree of the President of Ukraine dated 25.02.2017 No. 47/2017. Retrieved from: https://zakon.rada.gov.ua/laws/show/47/2017#Text
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 05.07.1994 (as amended). Retrieved from: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
4. Zakon Ukrainy «Pro zakhyst personalnykh danykh» [Law of Ukraine «On Personal Data Protection»] (2010). No. 2297-VI dated 01.06.2010 (as amended). Retrieved from: https://zakon.rada.gov.ua/laws/show/2297-17#Text

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 27.03.2025.
6. 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.
7. Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: A systematic review. *SN Applied Sciences*, 2, 1–8.
8. Sardi, A., Rizzi, A., Sorano, E., & Giussani, A. (2020). The role of data breaches in healthcare sector: A systematic literature review. *Health Policy and Technology*, 9(4), 100–117.
9. Alsubaei, F., Abuhussein, A., Shikfa, A., & Shiva, S. (2019). Security and privacy in the Internet of Medical Things: Taxonomy and risk assessment. *IEEE Access*, 7, 170–188.
10. Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in hospitals: A systematic, organizational perspective. *Journal of Medical Internet Research*, 20(5), e10059.
11. Aksoy, C. (2024). Building a Cyber Security Culture for Resilient Organizations Against Cyber Attacks. *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi*, 7(1), 96–110.
12. Batiuk, L. V. (2022). Tsyfrova kompetentnist studentiv medychnykh zakladiv osvity pry vyvchenni dystsypliny «Informatyzatsiia u sferi hromadskoho zdorovia» [Digital competence of students of medical educational institutions in the study of the discipline «Informatization in the field of public health*»]. Suchasni informatsiini tekhnolohii ta innovatsiini metodyky navchannia u pidhotovtsi fakhivtsiv: metodolohiia, teoriia, dosvid, problemy*, (62), 22–27.
13. Parfonova, I., & Zinchenko, O. (2024). Cybersecurity enhancement in the field of eHealth system development in Ukraine. *Medychna perspektyva*, 29(2), 37–45.
14. Stuchynska, N. V., & Palamarchuk, Yu. V. (2024). Formuvannia tsyfrovoi kompetentnosti maibutnikh stomatolohiv [Formation of digital competence of future dentists]. *Medytsyna ta farmatsiia: osvitni dyskursy*, (2), 43–48.
15. 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*, (88), 138–145.
16. 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*, (8), 3–10.
17. Terentiuk, V. H., Kucherenko, I. I., & Matukova-Yaryha, D. H. (2024). Rol ta znachennia rozvytku tsyfrovykh kompetentnostei pratsivnykiv okhorony zdorovia, zdobuvachiv medychnoi ta farmatsevtychnoi osvity ta naukovo-pedahohichnykh pratsivnykiv zakladiv vyshchoi medychnoi osvity v umovakh tsyfrovizatsii ta tsyfrovoi transformatsii okhorony zdorovia [The role and significance of the development of digital competencies of healthcare workers, medical and pharmaceutical education students and scientific and pedagogical workers of higher medical education institutions in the conditions of digitalization and digital transformation of healthcare]. *Medytsyna ta farmatsiia: osvitni dyskursy*, (3).
18. Natsionalnyi medychnyi universytet imeni O. O. Bohomoltsia [Bogomolets National Medical University]. (2024). Realizatsiia hrantovoho proiektu USAID «Pidtrymka reformy okhorony zdorovia»: materialy z opryliudnennia rezultativ hrantovoi prohramy [Implementation of the USAID grant project «Support for Healthcare Reform»: materials on the disclosure of the results of the grant program]. Retrieved from: https://nmuofficial.com/grantova-diyalnist/realizatsiya-grantovogo-proektu-usaid-pidtrymka-reformy-ohorony-zdorov-ya/materialy-z-oprylyudnennya-rezultativ-grantovoyi-programy
19. Petrenko, L. (2023). Tsyfrova bezpeka v strukturi tsyfrovoi kompetentnosti maibutnoho vykladacha pedahohichnoho zakladu vyshchoi osvity: zmistovyi komponent [Digital security in the structure of digital competence of the future teacher of a pedagogical institution of higher education: content component]. *Osvita doroslykh: teoriia, dosvid, perspektyvy,* 23(1), 98–109.
20. HIPAA Journal. (2023). Healthcare Data Breach Statistics. Retrieved from: https://www.hipaajournal.com/healthcare-data-breach-statistics/
21. Information security management in the operations of healthcare entities. (2024). Scientific Papers of Silesian University of Technology. Organization and Management Series, 192, Article 11.
22. Martin, S., & Harrison, V. (2023). Cybersecurity vulnerabilities in integrated medical devices and their risks to patient safety. Cybersecurity Vulnerabilities in Integrated Medical Devices and Their Risks to Patient Safety.
23. Khaled, A. (2022). Internet of medical things (IoMT): Overview, taxonomies, and classifications. *Journal of Computer and Communications*, 10(8), 64–89.
24. Kuchyn Y. L., Kaniura O. A., Melnyk V. S., Stuchynska N. V., Mykytenko P. V. (2022). Symuliatsiini tekhnolohii u systemi pidhotovky maibutnikh likariv v umovakh Covid-19 [Simulation technologies in the system of training future doctors in the conditions of Covid-19]. *Naukovyi chasopys NPU imeni M.P. Drahomanova. Seriia 5. Pedahohichni nauky: realii ta perspektyvy: Zbirnyk naukovykh prats*. Kyiv: Helvetica Publishing House. Vol. 86. P. 132–142.

Дата надходження статті: 20.10.2025
Дата прийняття статті: 03.11.2025
Опубліковано: 17.11.2025