

УДК 378.6.147:004.056](477.411)

DOI <https://doi.org/10.32782/eddiscourses/2025-4-9>

СТАН ОБІЗНАНОСТІ ЩОДО КІБЕРБЕЗПЕКИ СЕРЕД ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ НМУ ІМЕНІ О.О. БОГОМОЛЬЦЯ

Кучеренко Інна Іванівна,

PhD педагогічних наук, доцент, доцент кафедри медичної і біологічної фізики та інформатики,

Національний медичний університет імені О.О. Богомольця

ORCID: 0000-0002-0734-6544

Микитенко Павло Васильович,

доктор педагогічних наук, доцент,

доцент кафедри медичної і біологічної фізики та інформатики,

Національний медичний університет імені О.О. Богомольця

ORCID: 0000-0003-1188-4334

Терентюк Вадим Георгійович,

кандидат медичних наук, доцент,

доцент кафедри менеджменту охорони здоров'я,

Національний медичний університет імені О.О. Богомольця

ORCID: 0000-0002-7046-4922

Ніжегородцев Владислав Олександрович,

кандидат педагогічних наук, доцент, доцент кафедри

комп'ютерних та інформаційних технологій і систем,

Державний податковий університет

ORCID: 0000-0001-9434-0564

У статті здійснено комплексний аналіз рівня обізнаності з основ кібербезпеки здобувачів вищої освіти НМУ імені О.О. Богомольця в умовах активної цифровізації освітнього процесу та медичної сфери.

За результатами анкетування здобувачів першого (бакалаврського) та другого (магістерського) рівнів вищої освіти визначено рівень їхніх знань, практичних навичок та готовності протидіяти найпоширенішим кіберзагрозам. Можна констатувати, що хоча більшість респондентів усвідомлюють базову важливість кібербезпеки для майбутньої професійної діяльності, проте значна частина здобувачів вищої освіти мають фрагментарні або поверхові знання ключових понять – фішингу, конфіденційності медичних даних, принципів управління паролями та правил безпечної поведінки онлайн, а практичні навички часто залишаються недостатньо сформованими.

Особливу увагу привертає низький рівень знань щодо методів захисту конфіденційної інформації пацієнтів, що є критично важливим для майбутніх медичних працівників. Під час опитування респондентів встановлено основні проблеми з якими стикались здобувачі вищої освіти в контексті кіберзахисту, а саме: недостатня регулярність оновлення паролів, нерівномірне використання антивірусних засобів та обмежену здатність розпізнання шкідливих повідомлень. Незважаючи на це, майже 80% опитаних визнали високу важливість кібербезпеки у майбутній професійній роботі, а понад 70% висловлюють готовність підвищувати свій рівень цифрової грамотності.

На основі результатів здійсненого дослідження можна констатувати потребу у впровадженні цілеспрямованих освітніх програм, тренінгів та інтеграції елементів цифрової безпеки в існуючі навчальні дисципліни. Підвищення рівня кіберграмотності здобувачів вищої освіти сприятиме не лише захисту персональних даних, а й загальній цифровій стійкості медичної галузі, яка все активніше використовує інформаційні системи, телемедицину та онлайн-сервіси.

Ключові слова: кібербезпека, кібергігієна, цифрова компетентність, цифрова грамотність, цифрові загрози, фішинг.

Kucherenko Inna, Mykytenko Pavlo, Terentiuk Vadym, Nizhehorodtsev Vladyslav. State of cybersecurity awareness among higher education students of Bogomolets National Medical University

The article presents a comprehensive analysis of the level of cybersecurity awareness among higher education students of Bogomolets National Medical University in the context of active digitalization of the educational process and the medical sector.

Based on a survey of students pursuing the first (bachelor's) and second (master's) levels of higher education, the level of their knowledge, practical skills, and readiness to counter the most common cyber threats was assessed. The findings indicate that although most respondents recognize the fundamental importance of cybersecurity for their future professional activities, a significant proportion of students possess fragmented or superficial knowledge of key concepts – such as phishing, medical data confidentiality, password management principles, and safe online behavior – while their practical skills often remain insufficiently developed.

Particular attention is drawn to the low level of understanding of methods for protecting patients' confidential information, which is critically important for future healthcare professionals. The survey revealed several key challenges faced by students in the context of cyber protection, including insufficient frequency of password updates, inconsistent use of antivirus tools, and limited ability to identify malicious messages. Nevertheless, nearly 80% of respondents acknowledged the high importance of cybersecurity in their future professional work, and more than 70% expressed their willingness to improve their level of digital literacy.

Based on the research results, the authors highlight the need for implementing targeted educational programs, training sessions, and integrating digital security components into existing academic disciplines. Enhancing the cybersecurity literacy of higher education students will contribute not only to protecting personal data but also to strengthening the overall digital resilience of the medical sector, which increasingly relies on information systems, telemedicine, and online services.

Key words: cybersecurity, cyber hygiene, digital competence, digital literacy, digital threats, phishing.

Постановка проблеми. Стрімкий розвиток цифрових технологій призводить до трансформації суспільства, формує відкритий кіберпростір, який розширює можливості громадян, сприяє прозорій діяльності органів влади, підвищує ефективність управління та створює умови для розвитку інновацій. Водночас цифровізація породжує нові загрози національній та міжнародній безпеці. Зростає кількість цілеспрямованих кібератак, випадків незаконного збору та використання персональних даних, фінансових махінацій, шахрайства і транснаціональної кіберзлочинності. Агресія рф та зміни у безпековому середовищі України обумовлюють потребу у формуванні національної системи кібербезпеки як складової системи національної безпеки.

Цифровізація освітнього процесу, зростання кількості онлайн-сервісів та активне використання електронних ресурсів у закладах вищої освіти зумовлюють необхідність підвищення рівня кібербезпеки серед студентської молоді. У медичній сфері ця потреба набуває особливої актуальності, оскільки майбутні фахівці галузі охорони здоров'я працюватимуть з конфіденційною інформацією пацієнтів, електронними медичними системами та цифровими інструментами, від безпеки яких залежить якість надання медичної допомоги. Здобувачі вищої освіти НМУ імені О.О. Богомольця активно залучені до цифрового середовища – використовуючи навчальні платформи, електронні журнали, хмарні сервіси та комунікаційні інструменти, що підвищує ризики кіберінцидентів у разі недостатнього рівня знань та навичок.

Проблематика кібергігієни та цифрової грамотності здобувачів вищої освіти є однією з ключових у сучасному інформаційному суспільстві. Незважаючи на широке поширення цифрових технологій, багато користувачів залишаються вразливими до таких загроз, як фішингові атаки, крадіжка даних, несанкціонований доступ чи маніпуляція інформацією. Це свідчить про необхідність системного вивчення поточного стану обізнаності молоді щодо кібербезпеки, виявлення прогалин та формування рекомендацій для підвищення цифрової стійкості у медичній освіті.

Таким чином, дослідження рівня обізнаності здобувачів вищої освіти НМУ імені О.О. Богомольця щодо кібербезпеки є важливим кроком до формування безпечного освітнього середовища, розвитку відповідальної цифрової поведінки та забезпечення готовності майбутніх медичних працівників до ефективної роботи в умовах цифрової трансформації системи охорони здоров'я.

Аналіз джерел. Галузь охорони здоров'я значною мірою залежить від технологій та інформаційного цифрового середовища, яке інтегровано з іншими секторами економіки, зокрема фінансовим та державним регулюванням. Це свідчить про необхідність про те, що галузь охорони здоров'я в короткий термін повинна пройти ті етапи розвитку інформаційної безпеки, які фінансовий сектор та державні установи проходили протягом останніх п'яти десятиліть [6].

Метою Стратегії кібербезпеки України є забезпечення безпечного функціонування кіберпростору в інтересах особи, суспільства і держави шляхом [16; 10]: створення національної системи

кібербезпеки; посилення спроможностей сектору безпеки й оборони для протидії кіберзагрозам воєнного характеру, кібершпигунству, кібертероризму та кіберзлочинності, а також розвитку міжнародного співробітництва; кіберзахисту державних електронних ресурсів та критичної інформаційної інфраструктури.

У Законі «Про основні засади забезпечення кібербезпеки України» [11] зазначено, що забезпечення кібербезпеки ґрунтується на принципах верховенства права, пріоритету національних інтересів, відкритості та захищеності кіберпростору, державно-приватного партнерства, пропорційності заходів, пріоритетності превенції, невідворотності покарання, підтримки науково-технічного потенціалу та міжнародної взаємодії, а також демократичного цивільного контролю над військовими та правоохоронними структурами, що діють у сфері кібербезпеки.

Медична реформа в Україні, стрімкий розвиток електронної системи охорони здоров'я та цифровізація всіх процесів у медичній сфері актуалізують проблеми кібербезпеки та захисту даних. Сьогодні медичні заклади та держава стикаються з необхідністю не просто впровадження нових технологій, а із забезпеченням надійного захисту конфіденційної інформації пацієнтів. Це вимагає від медичних працівників не лише глибоких знань у своїй галузі, а й розуміння основ кібербезпеки та вміння захистити дані в цифровому середовищі. Шахраї, кіберзлочинці регулярно здійснюють атаки на електронні адреси чи офіційні сайти державних органів, зокрема закладів охорони здоров'я (заклади освіти, що готують майбутніх фахівців галузі охорони здоров'я, лікуально-консультативні заклади тощо). Тож, кібербезпека є досить актуальним питанням у галузі охорони здоров'я, не лише в контексті захисту даних від зловмисників, а й в питанні державної безпеки. Заклади охорони здоров'я, а також стоматологічні клініки є досить об'ємними сховищами конфіденційних даних пацієнтів, де зберігається історія хвороби пацієнта.

В той же час, відсутні підґрунтя для опанування тематики цифрової безпеки: наявність відповідних тем чи вибіркових курсів в освітньому процесі М(Ф) ЗВО України [8; 13; 12].

Проте, питання кібербезпеки є важливим на державному рівні. Оскільки 12 листопада 2025 року було представлено проєкт Національної стратегії кібергігієни на заході «Кіберстійкість: стоїмо на принципах безпеки». Зазначена стратегія до 2030 року має на меті [16]: навчити українців базових цифрових навичок; підвищити

обізнаність про кіберзагрози та безпечну поведінку онлайн; підтримати впровадження стандартів кібергігієни в державному секторі та бізнесі.

Мета статті полягає у дослідженні рівнів сформованості практичних навичок кібергігієни та умінь розпізнавати найпоширеніші види кіберзагроз, а також оцінюванні готовності здобувачів вищої освіти до захисту персональних і медичних даних у процесі навчання та майбутньої професійної діяльності.

Результати дослідження. На веб-сайті Microsoft [5] сформульоване визначення кібербезпеки як комплексу процесів, рекомендацій і технологічних рішень, які допомагають захистити важливі системи, дані й мережу від цифрових атак. На веб-сайті МОЗ України [6] розміщено наступне визначення: «Кібербезпека – це стан захищеності даних в електронному вигляді від їх несанкціонованого використання або кримінальних дій з цими даними, а також набір заходів для досягнення такого стану захищеності даних». Дослідження цифрової компетентності, зокрема напрямку кібербезпеки в НМУ імені О.О. Богомольця проводились в рамках грантової діяльності [8; 13; 12], та підтвердили низький рівень сформованості цієї компетентності у здобувачів вищої освіти.

З огляду на актуальність цього питання було проведено анкетування здобувачів вищої освіти в НМУ імені О.О. Богомольця стосовно самооцінки рівня компетентностей з кібербезпеки. Участь в анкетуванні була анонімною, та добровільною. До анкетування доєдналось 211 респондентів першого (бакалаврського) та другого (магістерського) рівнів вищої освіти.

На питання «Як Ви оцінюєте свій загальний рівень знань у сфері кібербезпеки в галузі охорони здоров'я?»: 31,2% респондентів вказали що оцінюють свій рівень як високий, 48,8% – оцінили як середній, а 20,4% – як низький. Аналізуючи розуміння сенсу поняття «конфіденційність медичних даних» 73% респондентів зазначили, що розуміють, 21,3% – оцінили рівень розуміння даного терміну як середній, а 5,7% – як низький. Щодо частоти роботи із цифровими медичними системами, то переважна частина респондентів не працює з ними (45%), в той же час майже 80% розуміють високий рівень важливості кібербезпеки в майбутній професійній діяльності. Також, 73% респондентів висловили готовність до підвищення своєї компетентності у сфері кібербезпеки. Крім того, як зазначили респонденти в відповідях (рис. 1) стосовно рівня кіберзахисту в медичних закладах: 19,9% – вважають його

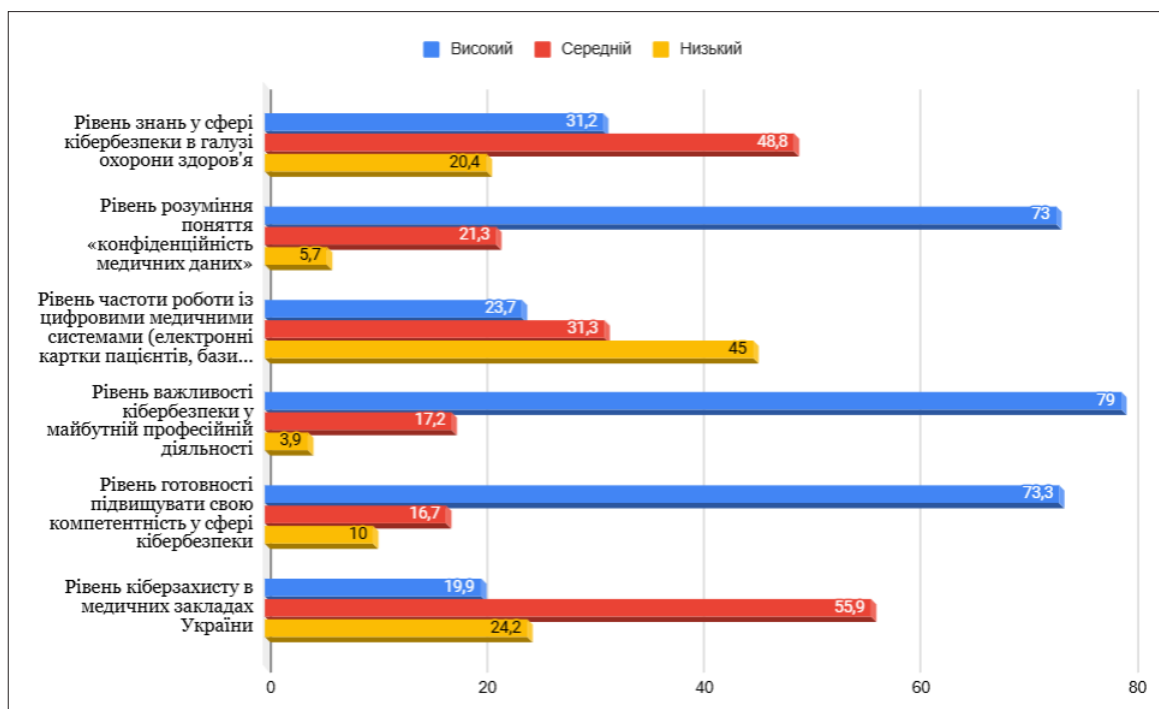


Рис. 1. Розподіл відповідей респондентів на загальні питання кібербезпеки

досить високим, 24% – низьким, а основна частина 60% – середнім.

Шукаючи готові та швидкі рішення з підвищення рівня компетентностей з кібербезпеки можна виокремити низку сервісів. Так, з метою підвищення рівня обізнаності з питання кібербезпеки компанія Google [18, 3] пропонує навчання з кібербезпеки на платформі Coursera [17] де можна отримати:

- розуміння важливості практик кібербезпеки та їх впливу на установи;
- навички визначати загальні ризики, загрози та вразливі місця, а також використовувати методи їх пом'якшення;

– навички захисту мережі, пристроїв та даних від несанкціонованого доступу та кібератак за допомогою інструментів безпеки інформації та керування подіями (SIEM);

– практичний досвід роботи з Python, Linux і SQL.

Однією з проблем у ході опитування було визначену, таку як недостатня регулярність оновлення паролів. Створення надійних паролів є досить важливим як в особистому, так і в навчальному та професійному просторі. Компанії Google [3] та Microsoft [4] на своїх сторінках технічної підтримки надають рекомендації щодо створення надійних паролів.

Таблиця 1

Рекомендації компаній Google [3] та Microsoft [4] щодо створення надійних паролів

Компанія	Рекомендації щодо створення надійних паролів
	Пароль може складатися з будь-якої комбінації літер, цифр і символів ASCII. Діакритичні знаки й символи з діакритиками не підтримуються. Не можна використовувати паролі, які: – легко вгадати, наприклад, «пароль123», – використовувалися раніше для облікового запису, – починаються або закінчуються пробілом
	Пароль може складатися з будь-якої комбінації літер, цифр і символів ASCII. Діакритичні знаки й символи з діакритиками не підтримуються. Не можна використовувати паролі, які: – легко вгадати, наприклад, «пароль123», – використовувалися раніше для облікового запису, – починаються або закінчуються пробілом, – легко запам'ятати, але важко вгадати іншим Радимо використовувати пам'ятну фразу, як-от "6MonkeysRLooking^"

Також, для створення надійних паролів рекомендують використовувати онлайн генератори: ESET [2], AVAST [1], Ukraine [9]. Крім цього для генерації паролів можуть стати в нагоді чат GPT, Gemini чи інші застосунки на основі штучного інтелекту (ШІ). Проте, не варто забувати, що оскільки паролі згенеровані за допомогою ШІ, вони технічно вже не є повністю конфіденційними. Найкраще використовувати їх як шаблон (змінивши кілька символів). У ході анкетування респонденти зазначили, що в основному досить відповідально ставляться до створення паролів: 39,8% – використовують складні паролі, 43,6% – застосовують паролі середньої складності. Проте, є респонденти, що мають однакові паролі до всіх облікових записів (14,2%) та використовують прості та короткі паролі (2,4%). На рис. 2 представлено розподіл відповідей респондентів на питання щодо регулярності оновлення паролів: регулярно, зокрема раз на 3–6 місяців змінює 19% респондентів, раз на рік – понад 12%, раз на кілька років понад 30% і ніколи не змінюють паролі понад 38% респондентів.

Як зазначено на веб-сайті МОЗ України [15]: «Фішинг – це один із різновидів шахрайства в інтернеті, що використовується зловмисниками з метою отримання незаконного доступу до конфіденційних даних користувачів». Також, на веб-сайті МОЗ України можна завантажити інформаційні матеріали, та розмістити в ЗОЗ чи М(Ф) ЗВО для ознайомлення [18]. Щодо фішингу, то 21,8% респондентів можуть розпізнати та запобігти фішинговим повідомленням, 23,7% – добре розуміють, що отримали фішинговий лист,

загальне уявлення щодо фішингу мають 31,3% респондентів, 13,7% – чули про фішинг, але не розуміють що це, а 9,5% респондентів ніколи не чули та не стикались з фішингом. У той же час, з обережністю ставляться до підозрілих листів 79,1% респондентів, інколи перевіряють відправника – 11,4%, а 9,5% – відкривають та переглядають без аналізу змісту. На рахунок антивірусного забезпечення, то 23,7% – використовують постійно з оновленням, 29,9% – мають антивіруси на всіх пристроях, 20,9% мають антивіруси лиш на одному пристрої, і 25,5% – не мають або рідко застосовують антивіруси. Крім того, здобувачі висловили необхідність оновлення змісту навчальних дисциплін, з поглиблення теми кібербезпеки, та впровадження вибіркової дисципліни з основ кібербезпеки.

Висновки. Отримані результати засвідчують недостатній рівень сформованості компетентностей з кібербезпеки серед здобувачів вищої освіти НМУ імені О.О. Богомольця. Попри загальне усвідомлення важливості кібербезпеки у професійній діяльності та готовність більшості респондентів підвищувати власний рівень обізнаності, значна частка здобувачів вищої освіти демонструє фрагментарне або поверхневе розуміння ключових понять, зокрема фішингу та конфіденційності медичних даних. Практичні навички кіберзахисту, зокрема управління паролями та використання антивірусного забезпечення, також залишаються на недостатньому рівні.

Аналіз отриманих даних підкреслює потребу у системній інтеграції навчального контенту з кібербезпеки у підготовку майбутніх фахівців

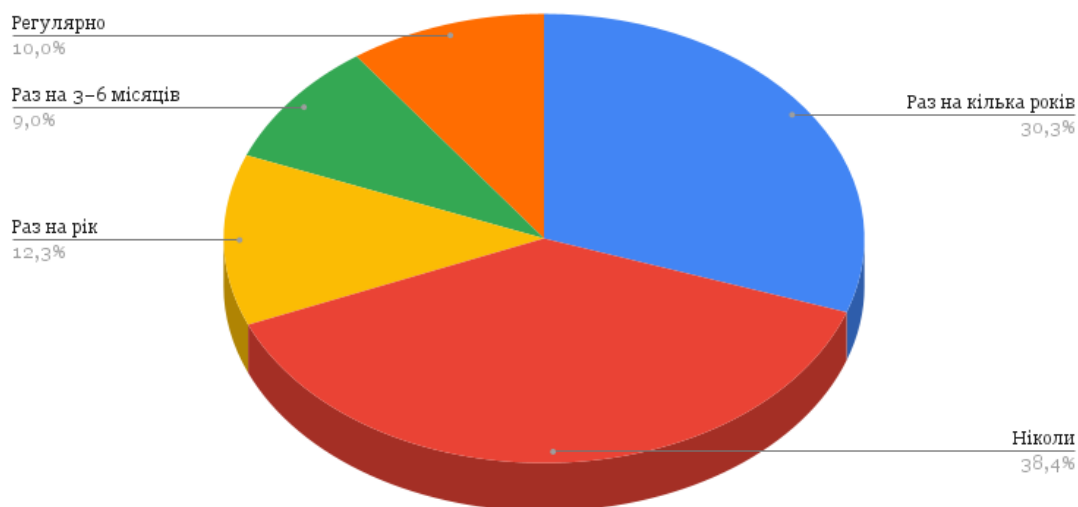


Рис. 2. Розподіл відповідей респондентів на питання щодо регулярності оновлення паролів

галузі охорони здоров'я. Доцільним є оновлення змісту чинних дисциплін та впровадження окремого вибіркового курсу, спрямованого на фор-

мування практичних навичок протидії кіберзагрозам, що відповідає сучасним викликам цифровізації медицини.

Список літератури:

1. Avast. URL: <https://www.avast.ua/>
2. ESET. URL: <https://www.eset.com/ua/>
3. Google. URL: <https://support.google.com/accounts/answer/32040?hl=uk>
4. Microsoft. URL: <https://support.microsoft.com/uk-ua/windows/%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BD%D1%8F-%D1%82%D0%B0-%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-%D0%BD%D0%B0%D0%B4%D1%96%D0%B9%D0%BD%D0%B8%D1%85-%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%96%D0%B2-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>
5. Microsoft. Що таке кібербезпека? Захисний комплекс Microsoft. URL: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity>
6. МОЗ України. Основи кібербезпеки. URL: <https://moz.gov.ua/uk/osnovi-kiberbezpeki-2>
7. Terentiyk V. H., Mykytenko P. V., Vlasenko O. M., Matukova D. G., Kucherenko I. I. Formation of digital competence in the medical educational environment. *Wiadomosci lekarskie (Warsaw, Poland: 1960)*. 2025. 78(5). P. 1106–1111. doi: 10.36740/WLek/205381
8. Аналіз наповнення робочих програм навчальних дисциплін з питань розвитку електронної охорони здоров'я та інформаційних технологій, що викладаються на рівнях фахової передвищої, вищої та післядипломної освіти за спеціальностями медичного спрямування. URL: https://ir.librarynmu.com/bitstream/123456789/13076/1/Analysis%20of%20content%20of%20educational%20programs_NMU.pdf
9. Генератор паролів. URL: <https://www.ukraine.com.ua/info/tools/passwdgenerate/>
10. Дія. Освіта. Представили проєкт Національної стратегії кібергігієни. URL: <https://osvita.diia.gov.ua/news/national-cyber-hygiene-strategy-presentation>
11. Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017. URL: <https://zakon.rada.gov.ua/laws/card/2163-19>
12. Звіт аналізу результатів опитування здобувачів освіти та науково-педагогічних працівників. URL: http://ir.librarynmu.com/bitstream/123456789/13151/1/REPORT_and_ANALYSIS_of_the_results_of_the_survey_of_education_seekers_Grant_program.pdf
13. Концепція оновлення та створення навчальних програм з розвитку цифрових компетентностей та використання інформаційно-комунікаційних технологій (ІКТ) в охороні здоров'я, що викладаються на рівнях фахової, вищої та післядипломної освіти за спеціальностями медичного та фармацевтичного спрямування. URL: https://ir.librarynmu.com/bitstream/123456789/13150/1/Concept_for Updating_and Enriching Educational Programs_Grant_program.pdf
14. Міністерство охорони здоров'я України. *Кібербезпека*. URL: <https://moz.gov.ua/uk/kiberbezpeka>
15. Міністерство охорони здоров'я України. Фішинг. URL: <https://moz.gov.ua/uk/efishing>
16. Міністерство цифрової трансформації України. Як підвищити кіберстійкість країни: презентуємо проєкт Національної стратегії кібергігієни. URL: <https://thedigital.gov.ua/news/technologies/iak-pidvyshchyty-kiberstiykist-krayny-prezentuyemo-proyekt-natsionalnoyi-stratehiyi-kiberhihiyeny>
17. Сертифікат Google з кібербезпеки. URL: <https://grow.google/intl/ua/google-career-certificates/cybersecurity/>
18. Стучинська Н. В., Паламарчук Ю. В., Ніжегородцев В. О. Кібербезпека як необхідна складова в підготовці майбутніх стоматологів. *Наукові записки: Педагогічні науки*. 2024. № 158. С. 133–144. doi: 10.31392/NZ-udu-158.2024.14
19. 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). С. 105–110. doi: 10.32782/eddiscourses/2024-3-15
20. Терентюк В. Г., Матукова-Ярига Д. Г., Кучеренко І. І. Цифрова освіта як невід'ємна складова цифрової трансформації охорони здоров'я. *Scientific and pedagogical intership "The impact of digitalization on higher medical education"*. 2024. URL: <http://ir.librarynmu.com/handle/123456789/12115>
21. Указ «Про рішення Ради національної безпеки і оборони України» № 96/2016 від 27.01.2016. URL: <https://www.president.gov.ua/documents/962016-19836>
22. Цифрова грамотність населення України 2023. URL: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

References:

1. Avast. Retrieved from: <https://www.avast.ua/>
2. ESET. Retrieved from: <https://www.eset.com/ua/>
3. Google. Retrieved from: <https://support.google.com/accounts/answer/32040?hl=uk>
4. Microsoft. Retrieved from: <https://support.microsoft.com/uk-ua/windows/%D1%81%D1%82%D0%B2%D0%BE%D1%80%D0%B5%D0%BD%D0%BD%D1%8F-%D1%82%D0%B0-%D0%B2%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-%D0%BD%D0%B0%D0%B4%D1%96%D0%B9%D0%BD%D0%B8%D1%85-%D0%BF%D0%B0%D1%80%D0%BE%D0%BB%D1%96%D0%B2-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>

5. Microsoft. Shcho take kiberbezpeka? Zakhysnyi kompleks Microsoft [Microsoft. What is cybersecurity? Microsoft Security Complex]. Retrieved from: <https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cybersecurity>
6. MOZ Ukrainy. Osnovy kiberbezpeky. [Ministry of Health of Ukraine. Fundamentals of cybersecurity]. Retrieved from: <https://moz.gov.ua/uk/osnovi-kiberbezpeki-2>
7. Terentiyk, V. H., Mykytenko, P. V., Vlasenko, O. M., Matukova, D. G., Kucherenko, I. I. Formation of digital competence in the medical educational environment. *Wiadomosci lekarskie (Warsaw, Poland: 1960)*. 2025. 78(5). P. 1106–1111. doi: 10.36740/WLek/205381
8. Analiz napovnennia robochych prohran navchalnykh dystsyplin z pytan rozvytku elektronnoi okhorony zdorovia ta informatsiinykh tekhnolohii, shcho vykladaiutsia na rivniakh fakhovoi peredvyshchoi, vyshchoi ta pislidyplomnoi osvity za spetsialnostiamy medychnoho spriamuvannia [Analysis of the content of the working programs of educational disciplines on the development of electronic health care and information technologies, taught at the levels of professional pre-higher, higher and postgraduate education in medical specialties]. Retrieved from: https://ir.librarynmu.com/bitstream/123456789/13076/1/Analysis%20of%20content%20of%20educational%20programs_NMU.pdf
9. Henerator paroliv [Password generator]. Retrieved from: <https://www.ukraine.com.ua/info/tools/passwdgenerate/> [in Ukrainian]
10. Diia. Osvita. Predstavyly proiekt Natsionalnoi stratehii kiberhihiieny [Action.Education. The draft National Cyber. Hygiene Strategy was presented]. Retrieved from: <https://osvita.diia.gov.ua/news/national-cyber-hygiene-strategy-presentation>
11. Zakon Ukrainy «Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy» № 2163-VIII vid 05.10.2017 [Law of Ukraine “On the Basic Principles of Ensuring Cyber Security in Ukraine” No. 2163-VIII of 05.10.2017]. Retrieved from: <https://zakon.rada.gov.ua/laws/card/2163-19>
12. Zvit analizu rezultativ opytuvannia zdobuvachiv osvity ta naukovo-pedahohichnykh pratsivnykiv [Report on the analysis of the results of a survey of education seekers and scientific and pedagogical workers]. Retrieved from: http://ir.librarynmu.com/bitstream/123456789/13151/1/REPORT_and_ANALYSIS_of_the_results_of_the_survey_of_education_seekers_Grant_program.pdf
13. Kontsepsiia onovlennia ta stvorennia navchalnykh prohran z rozvytku tsyfrovyykh kompetentnostei ta vykorystannia informatsiino-komunikatsiinykh tekhnolohii (IKT) v okhoroni zdorovia, shcho vykladaiutsia na rivniakh peredvyshchoi fakhovoi, vyshchoi ta pislidyplomnoi osvity za spetsialnostiamy medychnoho ta farmatsevychnoho spriamuvannia [Concept for updating and creating educational programs for the development of digital competencies and the use of information and communication technologies (ICT) in healthcare, taught at the levels of pre-higher professional, higher and postgraduate education in medical and pharmaceutical specialties]. Retrieved from: https://ir.librarynmu.com/bitstream/123456789/13150/1/Concept_for Updating_and Enriching Educational Programs_Grant_program.pdf
14. Ministerstvo okhorony zdorovia Ukrainy. Kiberbezpeka [Ministry of Health of Ukraine. Cybersecurity]. Retrieved from: <https://moz.gov.ua/uk/kiberbezpeka>
15. Ministerstvo okhorony zdorovia Ukrainy. Fishynh [Ministry of Health of Ukraine. Phishing]. Retrieved from: <https://moz.gov.ua/uk/efishing>
16. Ministerstvo tsyfrovoy transformatsii Ukrainy. Yak pidvyshchyty kiberstiikist krainy: prezentuiemo proiekt Natsionalnoi stratehii kiberhihiieny [Ministry of Digital Transformation of Ukraine. How to increase the country’s cyber resilience: we present the draft of the National Cyber Hygiene Strategy]. Retrieved from: <https://thedigital.gov.ua/news/technologies/iak-pidvyshchyty-kiberstiikist-krainy-prezentuyemo-proyekt-natsionalnoyi-stratehiyi-kiberhihiieny>
17. Sertyfikat Google z kiberbezpek [Google Certificate in Cybersecurity]. Retrieved from: <https://grow.google/intl/ua/google-career-certificates/cybersecurity/>
18. Stuchynska, N. V., Palamarchuk, Yu. V., Nizhehorodtsev, V. O. (2024). Kiberbezpeka yak neobkhdna skladova v pidhotovtsi maibutnikh stomatolohiv [Cybersecurity as a necessary component in the training of future dentists]. *Scientific notes: Pedagogical sciences*. № 158. P. 133–144. doi: 10.31392/NZ-udu-158.2024.14
19. Terentiuk, V. H., Kucherenko, I. I., Matukova-Yaryha, D. H. (2024). Rol ta znachennia rozvytku tsyfrovyykh kompetentnostei pratsivnykiv okhorony zdorovia, zdobuvachiv medychnoi ta farmatsevychnoi osvity ta naukovo-pedahohichnykh pratsivnykiv zakladiv vyshchoi medychnoi osvity v umovakh tsyfrovizatsii ta tsyfrovoy transformatsii okhorony zdorovia [The role and importance of developing digital competencies of healthcare workers, medical and pharmaceutical education students and scientific and pedagogical workers of higher medical education institutions in the context of digitalization and digital transformation of healthcare]. *Medicine and Pharmacy: Educational Discourses*. (3). P. 105–110. doi: 10.32782/eddiscourses/2024-3-15
20. Terentiuk, V. H., Matukova-Yaryha, D. H., Kucherenko, I. I. (2024). Tsyfrova osvita yak nevidiemna skladova tsyfrovoy transformatsii okhorony zdorovia [Digital education as an integral part of the digital transformation of healthcare]. *Scientific and pedagogical intership “The impact of digitalization on higher medical education”*. Retrieved from: <http://ir.librarynmu.com/handle/123456789/12115>
21. Ukaz «Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy» № 96/2016 vid 27.01.2016 [Decree “On the Decision of the National Security and Defense Council of Ukraine” № 96/2016 dated 27.01.2016]. Retrieved from: <https://www.president.gov.ua/documents/962016-19836>
22. Tsyfrova hramotnist naselennia Ukrainy 2023 [Digital literacy of the population of Ukraine 2023]. Retrieved from: https://osvita.diia.gov.ua/uploads/1/8800-ua_cifrova_gramotnist_naselenna_ukraini_2023.pdf

Дата надходження статті: 23.10.2025

Дата прийняття статті: 03.11.2025

Опубліковано: 17.11.2025