DOI https://doi.org/10.31392/NZ-udu-158.2024.14
УДК 37.09:004.77:378.147:616.314-051

Стучинська Н. В., Паламарчук Ю. В., Ніжегородцев В. О.

КІБЕРБЕЗПЕКА ЯК НЕОБХІДНА СКЛАДОВА В ПІДГОТОВЦІ МАЙБУТНІХ СТОМАТОЛОГІВ

У період повномасштабного вторгнення, значна кількість закладів охорони здоров'я зазнають атак з боку росії. Мова йде не лише про ракетні атаки, а й про кібератаки. Кібератаки є загрозою як для бізнесу, так і для приватних осіб. Зловмисники націлені на пошкодження систем, викрадення конфіденційних даних та отримання несанкціонованого доступу до інформації. Мотиви таких атак можуть бути різноманітними: від політичних до фінансових. Медичним працівникам необхідно володіти інструментами для захисту та збереження даних в закладі охорони здоров'я, адже в них міститься персональна інформація та контактні дані як медичного персоналу, так і пацієнтів. Кібербезпека стала невід'ємною частиною будь-якої діяльності, особливо тієї, що пов'язана з обробкою персональних даних. Стоматологія не є винятком. З кожним роком зростає кількість цифрових даних, які стоматологи збирають про своїх пацієнтів: рентгени, 3D-моделі щелеп, історії хвороб тощо, а крім того, відповідно і кількість персональних даних. Ця інформація є надзвичайно цінною і потребує надійного захисту. Уся інформація про пацієнтів повинна зберігатися відповідно до законодавства про захист персональних даних. Виток цих даних може призвести до серйозних наслідків для репутації клініки та благополуччя пацієнтів.

Кібератаки на заклад охорони здоров'я можуть призвести до фінансових втрат, крадіжки банківських даних та інших фінансових операцій. Будь-який інцидент, пов'язаний з витоком даних або порушенням безпеки, може серйозно підірвати довіру пацієнтів до клініки та інші репутаційні втрати. Звісно, для надійного захисту даних має використовуватись ліцензійне програмне забезпечення оновлене до останньої версії, паролі мають бути складними та унікальними, відповідальні працівники не повинні надавати доступ до баз даних третім особам, а технічна підтримка в свою чергу має забезпечувати супровід.

Ключові слова: *цифрова компетентність, майбутні стоматологи, кібербезпека.*

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, лікульно-консультативні заклади тощо). Тож, кібербезка 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,

особисті дані, результати обстежень та діагностики. Ця інформація є досить привабливою для кіберзлочинців. Вони можуть використовувати її не лише для шахрайства та фінансового шантажу, а й для створення детальних профілів пацієнтів, які потім продаються на злочинних онлайн-майданчиках.

Питанню кібербезпеки присвячені праці Ю. Білявської та Я. Шестак [5], В. Вишнівський та А. Пампуха [8] стосовно впливу на підприємства та бізнес в період війни праці О. Кузьменко та О. Маклюка [4]. Ю. Славінська [9] досліджувала значення цифрових технологій для інтелектуального розвитку майбутніх стоматологів. Формування цифрової компетентності майбутніх лікарів під час вивчення освітнього компонента "Медична інформатика" досліджували Л. Батюк, О. Жерновникова [12], а О. Сілкова та Н. Лобач досліджували вплив на формування інформаційно-цифрової компетентності у студентів закладів вищої медичної освіти вивчення медичних інформаційних систем [10]. МОЗ України активно займається питаннями кібербезпеки та розміщує достатньо корисної інформації та інфографік з цього питання на офіційному сайті. В свою чергу питання кібербезпеки та кібергігієни в медичному (фармацевтичному) закладі вищої освіти наразі недостатньо висвітлене в праця сучасних науковців, незважаючи на значну увагу МОЗ до цього питання. Тож, можемо зазначити, що на сьогодні недостатньо праць з розкриття особливостей кібербезпеки та кібергігієни закладів охорони здоров'я в умовах воєнного стану та її популяризації.

Мета статті полягає у вивченні сучасних умов формування цифрової компетентності майбутніх стоматологів.

Для досягнення поставленої мети дослідження були використані загальнонаукові теоретичні й емпіричні методи, а саме: бібліосемантичний метод – аналіз науково-методичної літератури та нормативних документів з проблеми дослідження; метод системного аналізу для порівняння й узагальнення досвіду щодо питання кібербезпеки при підготовці майбутніх магістрів стоматології.

Однією з найзначніших кібератак у сфері охорони здоров'я стала атака програми-вимагача WannaCry у травні 2017 року. Вона зашифрувала дані та файли на 230 000 комп'ютерах у 150 країнах, порушивши функціональність NHS в Англії. Ключові системи були заблоковані, що завадило персоналу отримати доступ до даних пацієнтів і критичних послуг. Однак атака WannaCry не була спрямована безпосередньо на NHS, постраждали також інші великі організації, зокрема Telefonica, FedEx, Nissan і Банк Китаю. Тим не менш, найбільший вплив відчула Національна служба охорони здоров'я, підкресливши, наскільки галузь охорони здоров'я вразлива до кіберзагроз [14].

У травні 2021 року атака програми-вимагача на Управління охорони здоров'я (HSE) в Ірландії призвела до того, що 80 % IT-середовища HSE стали зашифрованими, що порушило роботу медичних послуг по всій країні. Були скасовані амбулаторні та медичні послуги, а відвідування лікарів скоротилося до 80 %, що значно вплинуло на послуги променевої терапії [14].

Інформаційні системи п'яти різних лікарень також були виведені з ладу

через атаку, яка сталася в Новій Зеландії в травні 2021 року [14].

Подібним чином у вересні 2020 року записи пацієнтів у близько 400 лікарнях і медичних закладах у Сполучених Штатах і Великобританії стали недоступними, що призвело до затримки надання допомоги пацієнтам і зміни маршрутів машин швидкої допомоги. Цей збій тривав три тижні [14].

Згідно з Рішенням Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України", забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [6]. Як зазначається в стратегії "Швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища, гарантуючи громадянам України безпечне функціонування національного сегмента кіберпростору, передбачивши нові можливості для цифровізації всіх сфер суспільного життя" [6]. Проблема ефективного забезпечення кібербезпеки потребує комплексного вирішення і вимагає скоординованих дій на національному, регіональному та міжнародному рівнях для запобігання, підготовки, реагування та відновлення інцидентів з боку органів влади, приватного сектора і громадянського суспільства [4]. Сфера охорони здоров'я – одна із лідерів у світі за зростанням кількості кібератак. У 2022 році на тиждень відбувалось 1 463 кібератаки, що на 74 % більше, ніж у 2021-му. Витоки даних у медичній сфері найдорожчі – у середньому вони обходились медичним закладам західних країн у $10 млн (дані CHECK POINT RESEARCH (CPR) TEAM за 2022 рік) [11]. Кібератаки загрожують не лише даним чи фінансам, а й безпосередньо людському життю, оскільки можуть призвести до тимчасового припинення надання медичної допомоги. Кібербезпека у сфері охорони здоров'я стає одним із ключових питань для медичних закладів та держави. Розвиток електронної системи охорони здоров'я (ЕСОЗ) та активна цифровізація процесів вимагають від медичної спільноти не лише цифрових знань і навичок, а й знань щодо основ кібербезпеки і навичок захисту власних даних і даних пацієнта у цифровому просторі [11], крім того, необхідно постійно вдосконалювати системи безпеки та адаптувати їх до нових загроз. Запроваджена з початком медичної реформи дворівнева електронна система охорони здоров'я (ЕСОЗ) забезпечує безпосередню, надійну та безпечну інформаційну взаємодію між надавачами медичних послуг та державними органами виконавчої влади, які формують політики в охороні здоров'я та забезпечують фінансування за надані послуги з медичного обслуговування населення [8]. Необхідно зазначити, що галузь охорони здоров'я, зокрема стоматологія, є основним сегментом критичної національної інфраструктури в Україні. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, регулярно попереджає про появу різного роду кібератак в українському інформаційному просторі, тож медичні та стоматологічні фахівці, працюючи з ЕСОЗ чи робочою електронною адресою чи месенджерами, можуть стикатись з кіберзагрозами.

Переважно, на заклади можуть піддаватись наступним типам кібер

загроз: викрадення даних, блокування доступу до даних (ransomware), DDoS-атаки, фішинг та внутрішні загрози. Стосовно останніх, то загрозу можуть становити не тільки зовнішні крадії інформації, а й внутрішні – привілейовані користувачі та адміністратори безпеки хмарного середовища, який мають прямий доступ до даних користувачів та їх програмного забезпечення [17].

Одним із типових форматів кібератак ворога є розповсюдження електронних листів начебто від імені державних установ з заголовками, які мають привернути увагу читача. Наприклад, "Повідомлення про несплату податку" та ін. Такі листи можуть містити "zip" або "rtf" архіви з docx-документами чи іншими файлами, відкриття яких призводить до завантаження та запуску шкідливих програм [15].

Саме тому на рівні закладу необхідно дотримуватися базових рекомендацій із захисту безпеки як-от:

– регулярно оновлювати програмне забезпечення (операційну систему, програмні бібліотеки та ін.). Надавайте перевагу саме ліцензованому ПЗ;

– контролювати цілісність та автентичність програмного забезпечення;

– забезпечувати мережевий захист: фільтрація та аналіз мережевого трафіку, виявлення і протидія мережевим атакам тощо;

– унеможливлювати втрату інформації;

– забезпечувати резервне копіювання даних;

– захист від несанкціонованого доступу;

– розмежування прав доступу тощо;

– забезпечувати реєстрації подій, пов'язаних з отриманням користувачами доступу до ресурсів ЗОЗ;

– резервувати конфігураційні файли та критично важливі системні файли;

– забезпечувати антивірусний захист, перевірку на наявність шкідливого програмного коду всіх вкладень що завантажуються користувачами.

Як зазначено на сайті МОЗ, понад 60 % кібератак відбувається через недотримання правил кібергігієни та кібербезпеки. На допомогу закладам охорони здоров'я в розділі Кібербезпека [11] розміщено додатково ще 9 вкладок: шаблони для впровадження кіберстандартів у медичних закладах; кіберзахист; фішинг; чутливі дані; програми-вимагачі; розблоковані екрани; соціальна інженерія; дії при кіберінциденті; організація робочих документів. До кожної вкладки наявні безкоштовні, доступні до завантаження плакати, флаєри, скрінсейвери.

Згідно з "Рамками цифрової компетентності працівника охорони здоров'я України" [2] кібербезпека, кібергігієна та захист даних відносяться є 3-м компонентом сфери 1 Загальна цифрова грамотність – С1К3.

Таблиця 1

Дикриптор	Операції
Захист комп'ютерних пристроїв та безпечне підключення до мережі Інтернет	Розуміти ризики та загрози у цифрових середовищах. Знати про заходи безпеки та захисту і

Дикриптор	Операції
	належним чином враховувати питання надійності та приватності. Електронна ідентифікація – здійснення контролю доступу за допомогою біометричних даних, текстових паролів, маркерів, смарт-карт, штрих-кодів, PIN-кодів тощо. Дотримуватися політики щодо паролів конкретної організації / установи / закладу.
Захист даних	Захист персональних даних і приватності, використання паролів та шифрування для захисту файлів і даних, безпека сховищ даних та хмарних технологій, використання захищених каналів комунікації, дотримання правил безпечного використання мобільних пристроїв, безпека в Інтернеті.
Захист здоров'я і благополуччя	Уміти уникати ризиків і загроз для фізичного та психологічного здоров'я при користуванні цифровими технологіями. Уміти захистити себе та інших від можливих небезпек у цифрових середовищах (наприклад, фішингу). Дотримуватись ергономічних правил, режиму праці-відпочинку задля збереження власного здоров'я.
Дотримання конфіденційності інформації і контроль доступу в ЕСОЗ	Уміння реалізовувати ключові принципи безпеки в межах ЕСОЗ: визначати можливі вразливості системи, дотримуватись вимоги формального погодження з політикою організаційної безпеки на особистісному, професійному та організаційному рівні. Вміння запобігати основним загрозам витоку інформації в МІС: випадковий перегляд, несанкціонований запит, зловмисне пошкодження, неконтрольований доступ, ризик передачі даних на зовнішні носії інформації. Реалізація засобів захисту від загроз безпеці даних в МІС, зберігання та резервне копіювання. Розуміння як користуватися та обмінюватися інформацією, яка дозволяє встановити особу, зі збереженням можливості захистити себе та пацієнтів від шкоди. Використання систем, що включають багатофакторну автентифікацію для передачі як особистих даних, так і для професійної діяльності. Знання порядку дій під час виникнення ситуації кіберзагрози та вміти їх застосувати.

Звісно, нині закладам охорони здоров'я необхідно розробити детальну політику безпеки і ознайомити з нею всіх співробітників. Політика повинна охоплювати всі аспекти кібербезпеки, від паролів до процедур у разі інцидентів. А також, проводите регулярні навчання для співробітників з питань кібербезпеки, навчати їх розпізнавати фішингові повідомлення, захищати свої облікові записи і повідомляти про підозрілу активність. На сайті МОЗ (https://moz.gov.ua/uk/osnovi-kiberbezpeki), на сторінці База знань eHealth в розділі "Захист інформації та робота з персональними даними у закладі охорони здоров'я" [18] доступно 6 тем (рисунок 1): Основи кібербезпеки; Принципи запровадження кіберкультури; Автоматизоване робоче місце

працівника сфери охорони здоров'я; Принципи побудови стійкої системи кіберзахисту. Вимоги законодавства щодо захисту інформації та основи захисту інформації в закладі охорони здоров'я; Удосконалення системи кібербезпеки; Захист персональних даних пацієнта при роботі з інформаційно-комунікаційними системами електронної охорони здоров'я.

Рис. 1. Зміст розділу 6 "Захист інформації та робота з персональними даними у закладі охорони здоров'я", База знань eHealth, МОЗ

На сторінці Дія. Освіта (https://osvita.diia.gov.ua/catalog/topic/cyber-security) доступні наступні освітні серіали (ОС), симулятори тощо: Кібергігієна для молоді (ОС); Базові знання з кібергігієни (ОС); Кібергігієна: як захиститися від фішингу (2 ОС); Аналітик із кібербезпеки (симулятор); Персональна кібергігієна (ОС та симулятор); Обережно! Кібершахраї (ОС); Основи кібергігієни (ОС); Персональні дані (ОС); Кіберняні (ОС); Про кібербулінг для підлітків (ОС); Навіщо нам кібергігієна? (гайд); Як військовослужбовцям безпечно користуватися смартфоном (гайд); Безпека дітей в Інтернеті для батьків (ОС); Кіберграм (Цифроґрам).

Рис. 2. Наповнення категорії "Кібербезпека" на сайті Дія. Освіта

Завдяки останній вкладці Кіберграм (https://osvita.diia.gov.ua/digigram), працівники охорони здоров'я мають змогу оцінити рівень знань щодо безпеки в цифровому середовищі.

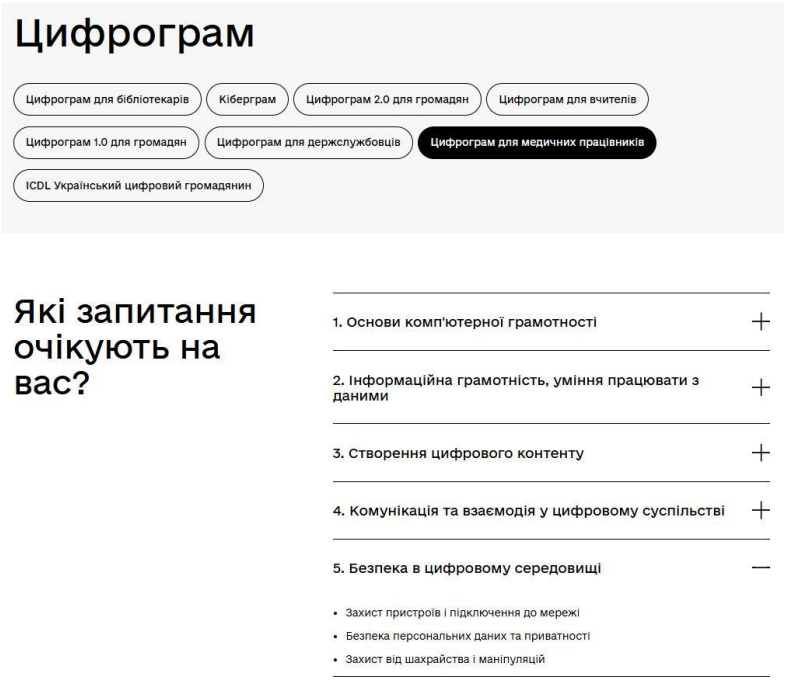

Рис. 3. Перелік тестів щодо безпеки в цифровому просторі на сайті Цифрограм

Також Google пропонує безкоштовно отримати сертифікат з кібербезпеки (https://grow.google/intl/ua/google-career-certificates/cybersecurity/):

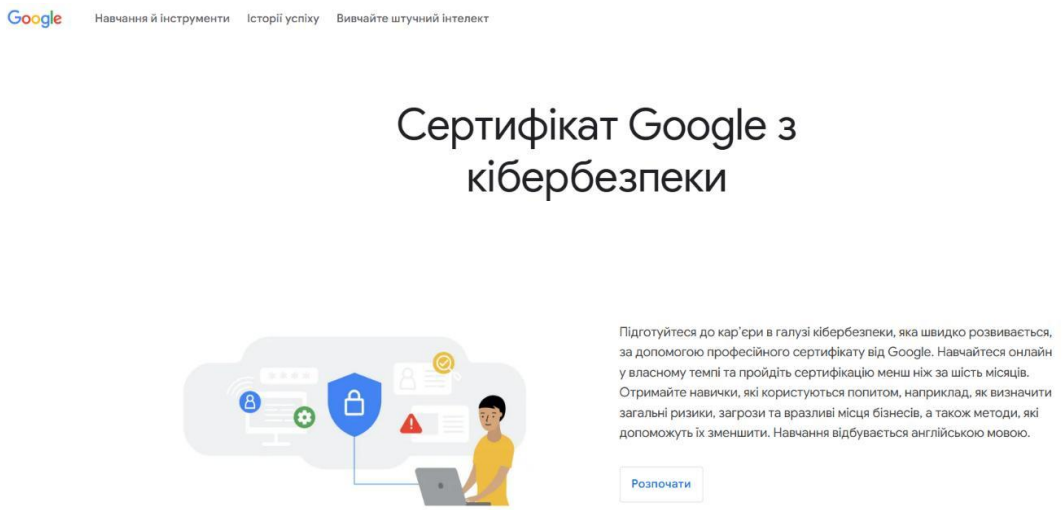

Рис. 4. Пропозиція сертифікату Google з кібербезпеки

Google пропонує безкоштовне навчання на платформі Coursera, а слухачам в межах вивчення курсу надається можливість:

– зрозуміти важливість практик кібербезпеки та їх вплив на організації;

– визначити загальні ризики, загрози та вразливі місця, а також методи їх пом'якшення;

– захистити мережі, пристрої, людей і дані від несанкціонованого доступу та кібератак за допомогою інструментів безпеки інформації та керування подіями (SIEM);

– отримати практичний досвід роботи з Python, Linux і SQL.

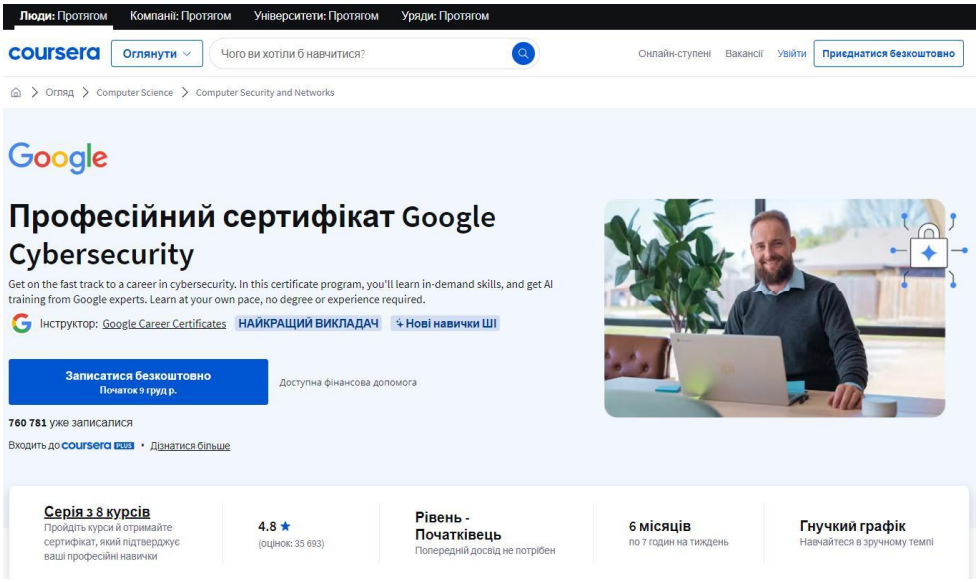

Рис. 5. Сторінка курсу "Професійний сертифікат Google Cybersecurity" на сайті Coursera

З метою вчасного реагування, попередження та відсутності наслідків кіберзагроз, майбутнім фахівцям галузі охорони здоров'я, зокрема майбутнім стоматологам, необхідно ще на додипломному рівні знати про можливі ризики

у цифровому середовищі, про необхідність захисту комп'ютерних пристроїв, безпечне підключення до мережі Інтернет, електронну ідентифікацію, контроль доступу, політику безпеки, способи захисту персональних даних і приватності, захист даних в Інтернеті і хмарному середовищі, захист власного здоров'я і благополуччя в цифровому просторі, захист даних і дотримання конфіденційності при використанні сервісів ЕСОЗ, порядок дій під час виникнення ситуацій кіберзагроз та методи їх уникнення, локальну політику безпеки, комп'ютерну та Інтернет залежності [2].

Висновки. Щоб ефективно протистояти сучасним викликам, необхідно враховувати широкий спектр потенційних загроз та їхню взаємодію. Враховуючи значне зростання кіберзагроз, та їх постійне вдосконалення та масштабування, майбутнім магістрам стоматології необхідно ще на початку навчання сформувати необхідні компетентності щодо боротьби з загрозами. Кожен користувач повинен забезпечити максимальний захист своїх та чужих даних шляхом використання надійних методів аутентифікації, регулярного оновлення програмного забезпечення та дотримання встановлених правил безпеки, а також несе персональну відповідальність за збереження конфіденційності даних. Для попередження кіберзагроз, як мінімум необхідно використовувати складні паролі, хоча б двоетапну аутентифікацію, шифрувати дані, створювати резервні копії, регулярно оновлювати програмне забезпечення та блокувати пристрої з метою запобігання несанкціонованому доступу та не надавати доступ до паролів та електронних цифрових підписів іншим особам тощо.

Використана література:

1. Стучинська Н. В., Паламарчук Ю. В. Формування цифрової компетентності майбутніх стоматологів. *Медицина та фармація: освітні дискурси*. 2024. (2). С. 43–48.
2. Концептуально-референтна рамка цифрових компетентностей працівників сфери охорони здоров'я та забезпечення розвитку інформаційної культури, цифрової грамотності (цифрової освіченості), кібербезпеки і кібергігієни працівників сфери охорони здоров'я. URL : https://bit.ly/ramka-tsyfrovoyi-kompetentnosti-pratsivnyka-okhorony-zdorovya-v1
3. Стандарт вищої освіти за спеціальністю 221 "Стоматологія" для другого (магістерського) рівня вищої освіти. URL : https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2019/06/25/221-Stomatolohiya-mahistr.20.01.22.pdf
4. Кузьменко О., Маклюк О., Чернишова О. Кібербезпека бізнесу під час війни. *Економіка та суспільство*. 2022. (44). doi: 10.32782/2524-0072/2022-44-21
5. Білявська Ю., Шестак Я. Кібербезпека та кібергігієна: нова ера цифрових технологій. *Товари і ринки*. 2022. № 3. С. 47–59.
6. Указ Президента України "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"" від 26.08.2021 № 447/2021. URL : https://zakon.rada.gov.ua/laws/show/447/2021#n12
7. Вишнівський В. В., Пампуха А. І. Кібербезпека в Україні. *Цифрова трансформація кібербезпеки* : науково-практична інтернет-конференція. Державний університет телекомунікацій Навчально-наукового інститут захисту інформації. Київ, 2022. С. 31–33.
8. 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

9. Славінська Ю. С. Практична значущість цифрових технологій для інтелектуального розвитку майбутніх лікарів-стоматологів. Духовно-інтелектуальне виховання і навчання молоді в XXI столітті : міжнар. кол. монографія. Всесвіт. наук. ноосферно-онтолог. тов-во, Харків. нац. пед. ун-т ім. Г. С. Сковороди, Асоц. рос. вчених штату Масачусетс [та ін.] ; за заг. ред. В. П. Бабича, Л. С. Рибалко. Харків : ВННОТ, 2019. С. 439–443.
10. Сілкова О. В., Лобач Н. В. Формування інформаційно-цифрової компетентності у студентів закладів вищої медичної освіти під час вивчення медичних інформаційних систем. *Педагогіка формування творчої особистості у вищій і загальноосвітній школах*. № 74. Т 3. 2021. С. 130–133. doi: 10.32840/1992-5786.2021.74-3.24.
11. Кібербезпека. МОЗ України. URL : https://moz.gov.ua/uk/kiberbezpeka
12. Батюк Л. В., Жерновникова О. А. Формування цифрової компетентності майбутніх лікарів при вивченні освітнього компоненту "Медична інформатика". *Наукові записки кафедри педагогіки.* Харківський національний університет імені В. Н. Каразіна. Харків, 2022. Вип. 50. С. 6–24.
13. ESET. URL : https://www.eset.com/ua/about/newsroom/press-releases/malware/opasnost-kiberatak-na-sektor-zdravookhraneniya-kak-spravitsya-s-novymi-vyzovami/?srsltid=AfmBOoqADxH6ulnwyjwYVQlnZ6HABC9XWTe6uEQxJgNsVEJV7b5j6TO9
14. Eska. URL : https://eska.global/blog/zagrozi-kiberbezpeci-v-galuzi-ohoroni-zdorovya
15. Електронна система охорони здоров'я в Україні. URL : https://ehealth.gov.ua/2022/06/22/nagoloshuyemo-na-dotrymanni-umov-kiberbezpeky-u-vashomu-zakladi-ohorony-zdorov-ya/
16. Худіков П., Петренко Л., Ніжегородцев В. Підходи до аналізу впливу військових конфліктів на соціально-економічні процеси. *Збірник наукових праць Державного податкового університету*. 2024. (1). С. 73–79. doi: 10.32782/2617-5940.1.2024.11
17. Ніжегородцев В. О., Валігура А. Т. Використання хмарних технологій в сфері логістики. *Матеріали IX Міжнародної науково-практичної інтернет-конференції "Проблеми впровадження інформаційних технологій в економіці"*. Ірпінь : Університет державної фіскальної служби України. 2018. С. 52–54.
18. Захист інформації та робота з персональними даними у закладі охорони здоров'я. МОЗ України. URL : https://moz.gov.ua/uk/osnovi-kiberbezpeki

References:

1. 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). S. 43–48 [in Ukrainian].
2. Kontseptualno-referentna ramka tsyfrovykh kompetentnostei pratsivnykiv sfery okhorony zdorovia ta zabezpechennia rozvytku informatsiinoi kultury, tsyfrovoi hramotnosti (tsyfrovoi osvichenosti), kiberbezpeky i kiberhihiieny pratsivnykiv sfery okhorony zdorovia [Conceptual and reference framework of digital competences of health care workers and ensuring the development of information culture, digital literacy (digital education), cyber security and cyber hygiene of health care workers]. URL : https://bit.ly/ramka-tsyfrovoyi-kompetentnosti-pratsivnyka-okhorony-zdorovya-v1 [in Ukrainian].
3. Standart vyshchoi osvity za spetsialnistiu 221 "Stomatolohiia" dlia druhoho (mahisterskoho) rivnia vyshchoi osvity [Standard of higher education in specialty 221 "Dentistry" for the second (master's) level of higher education]. URL : https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2019/06/25/221-Stomatolohiya-mahistr.20.01.22.pdf [in Ukrainian].
4. Kuzmenko O., Makliuk O., Chernyshova O. (2022). Kiberbezpeka biznesu pid chas viiny [Business Cybersecurity in a Time of War]. *Ekonomika ta suspilstvo*. (44). doi: 10.32782/2524-0072/2022-44-21 [in Ukrainian].
5. Biliavska Yu., Shestak Ya. Kiberbezpeka ta kiberhihiiena: nova era tsyfrovykh tekhnolohii [Cyber security and cyber hygiene: the new era of digital technologies]. *Tovary i rynky.* 2022. № 3. S. 47–59 [in Ukrainian].
6. Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy"" vid 26.08.2021 № 447/2021 [Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine" dated August 26, 2021 No. 447/2021]. URL : https://zakon.rada.gov.ua/laws/show/447/2021#n12 [in Ukrainian]
7. Vyshnivskyi V. V., Pampukha A. I. (2022). Kiberbezpeka v Ukraini [Cyber security in Ukraine]. *Tsyfrova transformatsiia kiberbezpeky :* naukovo-praktychna internet-konferentsiia. Derzhavnyi

universytet telekomunikatsii Navchalno-naukovoho instytut zakhystu informatsii. Kyiv. S. 31–33 [in Ukrainian].

8. 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 competences of health care 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 health care]. *Medytsyna ta farmatsiia: osvitni dyskursy*. (3). S. 105–110. doi: 10.32782/eddiscourses/2024-3-15 [in Ukrainian].
9. Slavinska Yu. S. (2019). Praktychna znachushchist tsyfrovykh tekhnolohii dlia intelektualnoho rozvytku maibutnikh likariv-stomatolohiv [The practical significance of digital technologies for the intellectual development of future dentists]. Dukhovno-intelektualne vykhovannia i navchannia molodi v KhKhI stolitti : mizhnar. kol. monohrafiia. Vsesvit. nauk. noosferno-ontoloh. tov-vo, Kharkiv. nats. ped. un-t im. H. S. Skovorody, Asots. ros. vchenykh shtatu Masachusets [ta in.] ; za zah. red. V. P. Babycha, L. S. Rybalko. Kharkiv : VNNOT. S. 439–443 [in Ukrainian].
10. Silkova O. V., Lobach N. V. Formuvannia informatsiino-tsyfrovoi kompetentnosti u studentiv zakladiv vyshchoi medychnoi osvity pid chas vyvchennia medychnykh informatsiinykh system [Formation of information and digital competence among students of higher medical education institutions during the study of medical information systems]. *Pedahohika formuvannia tvorchoi osobystosti u vyshchii i zahalnoosvitnii shkolakh.* № 74. T 3. 2021. S. 130–133. doi: 10.32840/1992-5786.2021.74-3.24 [in Ukrainian].
11. Kiberbezpeka. MOZ Ukrainy. [Cybersecurity. Ministry of Health of Ukraine]. URL : https://moz.gov.ua/uk/kiberbezpeka [in Ukrainian]
12. Batiuk L. V., Zhernovnykova O. A. (2022). Formuvannia tsyfrovoi kompetentnosti maibutnikh likariv pry vyvchenni osvitnoho komponentu “Medychna informatyka” [Formation of digital competence of future doctors when studying the educational component "Medical informatics"]. *Naukovi zapysky kafedry pedahohiky.* Kharkivskyi natsionalnyi universytet imeni V. N. Karazina. Kharkiv. Vyp. 50. S. 6–24 [in Ukrainian].
13. ESET. URL : https://www.eset.com/ua/about/newsroom/press-releases/malware/opasnost-kiberatak-na-sektor-zdravookhraneniya-kak-spravitsya-s-novymi-vyzovami/?srsltid=AfmBOoqADxH6ulnwyjwYVQlnZ6HABC9XWTe6uEQxJgNsVEJV7b5j6TO9 [in Englian].
14. Eska. URL : https://eska.global/blog/zagrozi-kiberbezpeci-v-galuzi-ohoroni-zdorovya [in Englian].
15. Elektronna systema okhorony zdorovia v Ukraini [Electronic health care system in Ukraine]. URL : https://ehealth.gov.ua/2022/06/22/nagoloshuyemo-na-dotrymanni-umov-kiberbezpeky-u-vashomu-zakladi-ohorony-zdorov-ya/ [in Ukrainian].
16. Khudikov P., Petrenko L., Nizhehorodtsev V. (2024). Pidkhody do analizu vplyvu viiskovykh konfliktiv na sotsialno-ekonomichni protsesy [Approaches to the analysis of the impact of military conflicts on socio-economic processes]. *Zbirnyk naukovykh prats Derzhavnoho podatkovoho universytetu*. (1). S. 73–79. doi: 10.32782/2617-5940.1.2024.11 [in Ukrainian].
17. Nizhehorodtsev V. O., Valihura A. T. (2018). Vykorystannia khmarnykh tekhnolohii v sferi lohistyky [The use of cloud technologies in the field of logistics]. *Materialy IKh Mizhnarodnoi naukovo-praktychnoi internet-konferentsii “Problemy vprovadzhennia informatsiinykh tekhnolohii v ekonomitsi”.* Irpin : Universytet derzhavnoi fiskalnoi sluzhby Ukrainy. S. 52–54 [in Ukrainian].
18. Zakhyst informatsii ta robota z personalnymy danymy u zakladi okhorony zdorovia. MOZ Ukrainy [Protection of information and work with personal data in a health care institution. Ministry of Health of Ukraine]. URL : https://moz.gov.ua/uk/osnovi-kiberbezpeki [in Ukrainian].

N. Stuchynska, Y. Palamarchuk, V. Nizhehorodtsev. Cybersecurity as a necessary component in the training of future dentists.

During the full-scale invasion, a significant number of healthcare facilities have been subjected to attacks by Russia. These attacks include not only missile strikes but also cyberattacks. Cyberattacks pose a threat to both businesses and individuals. Malicious actors aim to damage systems, steal sensitive data, and gain unauthorized access to information. The motives behind such attacks can vary from political to financial. Healthcare professionals need to possess the tools to protect and preserve data within healthcare facilities, as this data contains personal information and contact details of both medical staff and patients. Cybersecurity has become an integral part of any activity, especially those involving the processing of personal data. Dentistry is no exception. Each year, the amount of digital data collected by dentists about their patients increases: X-rays, 3D jaw models, medical histories, etc., as well as the amount of personal data. This information is extremely valuable and requires reliable protection. All patient information must be stored in accordance with data protection laws. A data breach can lead to serious consequences for the clinic's reputation and patient well-being. Cyberattacks on healthcare facilities can result in financial losses, theft of banking data and other financial transactions. Any incident related to a data breach or security violation can seriously undermine patient trust in the clinic and lead to other reputational losses. Of course, to reliably protect data, licensed software must be used and updated to the latest version, passwords must be complex and unique, responsible employees should not provide access to databases to third parties, and technical support must, in turn, provide support.

Keywords: *digital competence, future dentists, cybersecurity.*

DOI https://doi.org/10.31392/NZ-udu-158.2024.15
УДК 376.36-053.4:81'234

Теницька О. І., Безверха І. Г., Солодовник М. К.

РОЗВИТОК МОВЛЕННЯ СТАРШИХ ДОШКІЛЬНИКІВ ІЗ ЗНМ

У статті використано теоретичний аналіз наукової літератури з питань логопедії та дошкільної педагогіки, а також власний досвід роботи з дітьми, які мають загальне недорозвинення мовлення III рівня.

Відзначено, що порушення мовлення у дітей, зокрема загальне недорозвинення мовлення, є актуальною проблемою сучасної педагогіки та медицини. Діти із мовленнєвими порушеннями потребують спеціальної корекційної роботи, спрямованої на формування правильної вимови, лексико-граматичних компонентів мовлення, розвитку зв'язного мовлення та комунікативних умінь.

Зазначено, що діти із загальним недорозвиненням мовлення III рівня стикаються з серйозними труднощами у спілкуванні, що значно ускладнює їх соціально-емоційний розвиток. Формування правильного мовлення таких дітей є складним, але надзвичайно важливим завданням, що лягає на плечі логопедів та вихователів спеціальної групи для дітей з порушенням мови.

Стаття присвячена аналізу досвіду вихователя спеціальної групи для дітей з порушенням мови в роботі з дітьми, які мають ЗНМ III рівня. У ній висвітлено особливості мовленнєвого розвитку таких дітей, визначено основні труднощі, з якими стикаються вихователі, та запропоновано комплекс заходів, спрямованих на розвиток різних компонентів мовлення (лексики, граматики, зв'язного мовлення), а також на формування комунікативних навичок.