КІБЕРБЕЗПЕКА МЕДИЧНОЇ ІНФОРМАЦІЇ ЯК СКЛАДОВА РЕАГУВАННЯ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я НА БІОЛОГІЧНІ, ХІМІЧНІ ТА ЕКОЛОГІЧНІ ЗАГРОЗИ В УМОВАХ ВІЙНИ

CYBERSECURITY OF MEDICAL INFORMATION AS A COMPONENT OF THE HEALTHCARE SYSTEM'S RESPONSE TO BIOLOGICAL, CHEMICAL AND ENVIRONMENTAL THREATS IN WARTIME

Макух Христина Ігорівна, кандидат фармацевтичних наук, доцент, клінічний фармацевт, Благодійна організація «Благодійний фонд «СУПЕРЛЮДИ», makuh.hrystyna@gmail.com, https://orcid.org/0000-0002-6796-7342

Ривак Тетяна Богданівна, кандидат фармацевтичних наук, ДНТ «Львівський національний медичний університет імені Данила Галицького», tanusha1905@gmail.com, https://orcid.org/0000-0002-9491-1109

Федоришин Тарас Михайлович, кандидат медичних наук**,** лікар-хірург, КНП «Львівське територіальне медичне об'єднання "Багатопрофільна клінічна лікарня інтенсивних методів лікування та швидкої медичної допомоги"», ВП «Лікарня Святого Пантелеймона», fedoryshyn.tm@gmail.com, https://orcid.org/0000-0002-8683-1221

https://doi.org/10.32447/bcet.2026.24

Анотація. У роботі розглянуто кібербезпеку медичної інформації як складову реагування системи охорони здоров'я на біологічні, хімічні та екологічні загрози в умовах війни. Обґрунтовано, що медична інформація є критичним ресурсом для забезпечення безперервності лікування, евакуації постраждалих, інфекційного контролю, епідеміологічного нагляду, безпечної фармакотерапії, реабілітації та управління ресурсами закладу охорони здоров'я. Показано, що цифрова трансформація охорони здоров'я, зокрема впровадження медичних інформаційних систем, електронних медичних записів, телемедицини, аналітики великих даних, штучного інтелекту та інтернету речей у медицині, створює нові можливості для підвищення якості медичної допомоги, однак одночасно формує ризики для конфіденційності, цілісності та доступності медичних даних. Проаналізовано основні кіберзагрози для медичної інформації: витік, втрату, несанкціоновану модифікацію даних, *DDoS*-атаки, фішинг, людський фактор, несанкціонований доступ і ризики неконтрольованого використання штучного інтелекту. Запропоновано концептуальну модель кіберстійкості медичної інформації в умовах війни, яка включає стратегічний, організаційний, технологічний, кадровий, клініко-безпековий, воєнно-кризовий та *AI*-рівень. Обґрунтовано, що кібербезпека медичної інформації має розглядатися як складова безпеки пацієнта, громадського здоров'я, управління якістю та кризової стійкості закладу охорони здоров'я.

Ключові слова: кібербезпека, біологічні, хімічні та екологічні загрози, цифрова трансформація охорони здоров'я, медична інформаційна система, безпека пацієнта, штучний інтелект.

Abstract. This paper analyses the role of medical information cybersecurity as a component of the healthcare system's response to biological, chemical and environmental threats in wartime. It is

substantiated that medical information constitutes a critical resource for ensuring continuity of treatment, evacuation of casualties, infection control, epidemiological surveillance, safe pharmacotherapy, rehabilitation, and healthcare facility resource management. The paper demonstrates that the digital transformation of healthcare – including the implementation of health information systems, electronic medical records, telemedicine, big data analytics, artificial intelligence, and the Internet of Medical Things – creates new opportunities for improving the quality of medical care while simultaneously generating risks to the confidentiality, integrity, and availability of medical data. The main cyber threats to medical information are analysed, including data breaches, data loss, unauthorised data modification, DDoS attacks, phishing, the human factor, unauthorised access, and the risks of uncontrolled use of artificial intelligence. A conceptual model of medical information cyber-resilience in wartime is proposed, comprising seven levels: strategic, organisational, technological, personnel, clinical safety, military-crisis, and AI. It is substantiated that cybersecurity of medical information should be considered as an integral component of patient safety, public health, quality management, and crisis resilience of a healthcare facility.

Keywords: cybersecurity, biological, chemical and environmental threats, digital transformation of healthcare, health information system, patient safety, artificial intelligence (AI).

ВСТУП

Цифрова трансформація охорони здоров'я є одним із ключових напрямів модернізації медичної галузі, що спрямований на підвищення якості, доступності, безпечності та ефективності медичної допомоги. У сучасних умовах цифрові технології дедалі активніше інтегруються у клінічні, управлінські, освітні та аналітичні процеси закладів охорони здоров'я. До основних складових цифрового здоров'я належать електронна система охорони здоров'я (ЕСОЗ), медичні інформаційні системи, електронні медичні записи, телемедицина, мобільні медичні застосунки, аналітика великих даних, штучний інтелект, інтернет речей у медицині та комплексні рішення з кібербезпеки[1,2].

Цифрова трансформація охорони здоров'я є не лише технічним оновленням або переходом від паперової до електронної документації. Її сутність полягає у зміні самої логіки функціонування медичної системи, переході від автоматизації окремих процесів до побудови інтегрованої екосистеми цифрового здоров'я. Тому поряд із перевагами цифровізації виникає низка нових ризиків, пов'язаних із безпекою, достовірністю, цілісністю та доступністю медичної інформації.

Особливої актуальності питання кібербезпеки медичної інформації набуває в умовах воєнного стану. Повномасштабна війна в Україні створила не лише безпосередні фізичні, біологічні, хімічні, екологічні та гуманітарні загрози, а й посилила вразливість цифрової інфраструктури охорони здоров'я. Медичні заклади в умовах війни працюють із великим обсягом чутливої інформації про пацієнтів, зокрема даними про бойові травми, хірургічні втручання, інфекційні ускладнення, результати лабораторних досліджень, антибіотикотерапію, реабілітацію, евакуаційні маршрути та соціальний статус пацієнтів. Втрата, витік або спотворення такої інформації може мати не лише

[1]Міністерство охорони здоров'я України. Цифрова трансформація охорони здоров'я України. URL: https://moz.gov.ua/uk/cifrova-transformaciya-ohoroni-zdorov-ya-ukrayini-2 (дата звернення: 21 травня 2026).
[2]World Health Organization. Global strategy on digital health 2020-2025. Geneva: World Health Organization, 2021. URL: https://www.who.int/publications/i/item/9789240020924 (дата звернення: 21 травня 2026).

правові чи етичні наслідки, а й безпосередньо впливати на безпеку пацієнта, якість лікування та стійкість закладу охорони здоров'я загалом[3,4].

У контексті біологічних, хімічних та екологічних загроз на тлі повномасштабної війни медична інформація виконує не лише клінічну, а й безпекову та управлінську функцію. Дані про інфекційні ускладнення, мікробіологічні результати, антибіотикорезистентність, вплив токсичних речовин, екологічні фактори, маршрути евакуації та потребу в медичних ресурсах є основою для своєчасного реагування системи охорони здоров'я. Тому захист такої інформації від витоку, втрати, спотворення або блокування має розглядатися як складова не лише інформаційної безпеки, а й біологічної, хімічної та екологічної безпеки в умовах воєнного стану.

У межах політики інформаційної безпеки медична галузь розглядається як одна з найбільш вразливих до кібератак, оскільки медичні працівники працюють із надзвичайно чутливими даними, а їх втрата, знищення або спотворення може мати критичні наслідки для пацієнта, закладу охорони здоров'я та системи медичної допомоги загалом. Окремо наголошується на зростанні кібератак і *DDoS*-атак від початку повномасштабного вторгнення в Україні[5,6,7].

Отже, кібербезпека в охороні здоров'я в умовах війни має розглядатися не як вузька технічна функція, а як складова управління ризиками, безпеки пацієнта та безперервності медичної допомоги.

Мета дослідження – обґрунтувати значення кібербезпеки медичної інформації як складової реагування системи охорони здоров'я на біологічні, хімічні та екологічні загрози в умовах війни та запропонувати концептуальну модель кіберстійкості медичних даних для забезпечення безпеки пацієнта, управління якістю й кризової стійкості закладу охорони здоров'я.

МЕТОДОЛОГІЯ

Дослідження виконано у форматі оглядово-аналітичної роботи з елементами концептуального моделювання. Матеріалами для аналізу стали наукові публікації, навчально-методичні матеріали, нормативно-правові акти та міжнародні рекомендації, присвячені питанням цифрової трансформації охорони здоров'я, кібербезпеки медичної інформації, функціонування медичних інформаційних систем, захисту персональних даних, електронних медичних записів, телемедицини, аналітики великих даних, використання штучного інтелекту та управління ризиками в закладах охорони здоров'я.

Методи дослідження включали бібліографічний метод, системний аналіз, структурно-логічний аналіз, порівняльний аналіз, узагальнення та моделювання. Бібліографічний метод використовувався для опрацювання джерел щодо цифрової трансформації та кібербезпеки в охороні здоров'я. Системний аналіз дозволив розглянути медичну інформацію як критичний ресурс реагування на біологічні, хімічні та екологічні загрози в умовах війни. Структурно-логічний аналіз застосовано для побудови взаємозв'язку між цифровими компонентами охорони здоров'я,

[3]Ляшук А. Загрози і виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2023. № 6. С. 113–121. DOI: https://doi.org/10.31470/2786-6246-2023-6-113-121.
[4]Трофименко О., Дубовой Я., Логінова Н., Прокоп Ю., Задерейко О. Аналіз проблем забезпечення кібербезпеки медичних комп'ютерних систем. Захист інформації. 2021. Т. 23, № 1. С. 30-39.
[5]Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 року № 2801-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2801-12 (дата звернення: 20 травня 2026).
[6]Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я: Наказ Міністерства охорони здоров'я України від 28 лютого 2020 року № 587. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0236-20 (дата звернення: 19 травня 2026).
[7]Про затвердження Порядку ведення Реєстру пацієнтів в електронній системі охорони здоров'я: Наказ Міністерства охорони здоров'я України від 30 листопада 2020 року № 2755. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/z0044-21 (дата звернення: 21 травня 2026).

кіберризиками та клінічними наслідками. Метод моделювання використано для розроблення концептуальної моделі кіберстійкості медичної інформації.

РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

ЦИФРОВА ТРАНСФОРМАЦІЯ ОХОРОНИ ЗДОРОВ'Я ЯК ПЕРЕДУМОВА НОВИХ РИЗИКІВ

Цифрова трансформація системи охорони здоров'я охоплює комплексне впровадження цифрових технологій у клінічні, управлінські та комунікаційні процеси. Вона передбачає не лише переведення медичної документації в електронний формат, а й створення цифрової інфраструктури, яка забезпечує обмін, зберігання, аналіз і використання медичних даних для прийняття клінічних та управлінських рішень. До такої інфраструктури належать ЕСОЗ, медичні інформаційні системи, телемедицина, кібербезпека, мережеві сервіси обміну медичними даними, мобільні застосунки, дистанційний моніторинг, штучний інтелект, інтернет речей у медицині, роботизовані системи та аналітичні платформи.

З одного боку, ці інструменти створюють значні можливості для підвищення ефективності медичної допомоги. Електронні медичні записи дозволяють забезпечити безперервність інформації про пацієнта, зменшити дублювання обстежень, покращити доступ до результатів лабораторних та інструментальних досліджень, оптимізувати призначення лікарських засобів і забезпечити кращу координацію між різними фахівцями. Телемедицина розширює доступ до медичних консультацій, особливо для пацієнтів у віддалених, тимчасово переміщених або небезпечних регіонах. Аналітика великих даних і штучний інтелект можуть використовуватися для прогнозування ризиків, підтримки клінічних рішень, моніторингу стану здоров'я населення та управління ресурсами.

З іншого боку, чим глибше цифрові технології інтегруються у систему охорони здоров'я, тим більшою стає залежність медичного закладу від цифрової інфраструктури. Якщо раніше порушення роботи окремого паперового документа мало локальний характер, то в умовах цифрової трансформації збій медичної інформаційної системи, блокування доступу до електронних медичних записів або кібератака на цифрову інфраструктуру може впливати на значну кількість пацієнтів, підрозділів і процесів одночасно. Таким чином, цифровізація створює не лише нові можливості, а й нову поверхню ризику для закладу охорони здоров'я.

Особливо важливим вважаємо і те, що цифрова трансформація в медицині пов'язана з обробкою великих масивів персональних і клінічних даних. Такі можливості є цінними для розвитку доказової медицини, епідеміологічного нагляду та управління якістю медичної допомоги, однак вони одночасно вимагають високого рівня захисту даних, прозорого управління доступами, контролю за використанням інформації та дотримання етичних принципів[8].

Окрему групу ризиків формує застосування штучного інтелекту та систем підтримки прийняття клінічних рішень. *AI*-інструменти можуть використовуватися для аналізу складних медичних даних, підтримки клінічних рішень, ранньої діагностики, автоматизації аналізу медичних зображень, оптимізації дозування лікарських засобів і прогнозування побічних реакцій. Водночас їх впровадження потребує правового регулювання, оцінки точності алгоритмів, етичного контролю, прозорості прийняття рішень і захисту персональних даних[9].

[8]Токар П. Ю. Методи захисту конфіденційності даних пацієнтів у медичних інформаційних системах: аналітичний огляд. Наукові праці Вінницького національного технічного університету. 2025. № 3. С. 133–137. DOI: https://doi.org/10.31649/2307-5376-2025-3-133-137.

[9]World Health Organization. Ethics and governance of artificial intelligence for health. Geneva: WHO; 2021.

Кібербезпека у цьому контексті стає невід'ємною складовою цифрової трансформації охорони здоров'я. Для медичної сфери конфіденційність, цілісність і доступність даних мають безпосередній клінічний зміст. Конфіденційність означає захист персональних і медичних даних пацієнта; цілісність – недопущення спотворення діагнозів, лабораторних результатів, алергій чи призначень; доступність – можливість своєчасного отримання необхідної інформації для надання медичної допомоги[10,11].

МЕДИЧНА ІНФОРМАЦІЯ ЯК КРИТИЧНИЙ РЕСУРС РЕАГУВАННЯ НА ЗАГРОЗИ В УМОВАХ ВІЙНИ

В умовах воєнного стану медична інформація набуває значення критичного ресурсу, від якого залежить безперервність лікування, своєчасність клінічних рішень, безпека пацієнта, координація між закладами охорони здоров'я та ефективність реагування на надзвичайні ситуації. Медичні дані перестають бути лише адміністративним або обліковим ресурсом. Вони стають основою для маршрутизації пацієнтів, організації евакуації, планування хірургічних втручань, призначення фармакотерапії, моніторингу інфекційних ускладнень, контролю антибіотикорезистентності, організації реабілітації та оцінки потреб у лікарських засобах. Окрім клінічного значення, цифрові медичні дані мають управлінську роль, оскільки використовуються для обліку наданих медичних послуг, планування ресурсів, забезпечення безперервності медичної допомоги та реалізації державних гарантій медичного обслуговування населення[12]. У контексті реагування системи охорони здоров'я на біологічні, хімічні та екологічні загрози медична інформація є інструментом раннього виявлення, документування, моніторингу та реагування. При біологічних загрозах вона дозволяє відстежувати інфекційні ускладнення, результати мікробіологічних досліджень, поширення мультирезистентних мікроорганізмів, спалахи інфекцій та ефективність антимікробної терапії. При хімічних загрозах медичні дані необхідні для фіксації факту експозиції до токсичних речовин, оцінки клінічних проявів, призначення антидотної або симптоматичної терапії та подальшого спостереження. При екологічних загрозах цифрові медичні дані можуть використовуватися для довготривалого моніторингу наслідків забруднення води, повітря, ґрунту, впливу продуктів горіння, промислових аварій або інших факторів довкілля на здоров'я населення.

До критично важливої медичної інформації в умовах війни можна віднести персональні дані пацієнта, анамнез, характер і механізм травми, діагнози, результати лабораторних та інструментальних досліджень, дані про оперативні втручання, алергії, інфекційний статус, мікробіологічні результати, антибіотикотерапію, використання лікарських засобів високого ризику, реабілітаційний план, функціональний стан пацієнта, потребу в протезуванні чи довготривалому спостереженні.

Водночас використання медичної інформації як критичного ресурсу має здійснюватися з дотриманням принципів захисту персональних даних і лікарської таємниці. Персональні та медичні дані повинні оброблятися відповідно до визначеної законної мети, бути точними, достовірними, адекватними та не надмірними щодо цієї мети. У контексті цифрової трансформації це означає, що навіть за потреби швидкого обміну інформацією між закладами охорони здоров'я необхідно

[10]Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05 липня 1994 року № 80/94-ВР. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 18 травня 2026).

[11] Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21 травня 2026).

[12]Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19 жовтня 2017 року № 2168-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2168-19 (дата звернення: 21 травня 2026).

забезпечувати правомірність доступу, обмеження кола користувачів і захист від несанкціонованого поширення чутливих даних.

Особливого значення медична інформація набуває для лікування пацієнтів із бойовими травмами, складними реконструктивними втручаннями, інфекційними ускладненнями та тривалою реабілітацією. У таких пацієнтів клінічні рішення часто залежать від попередньої історії лікування, результатів мікробіологічних досліджень, даних про попереднє застосування антибіотиків, наявність мультирезистентної флори, алергій, побічних реакцій, функції нирок, показників запалення та динаміки ранового процесу. Втрата або недоступність таких даних може призвести до дублювання обстежень, затримки лікування, нераціонального застосування антибіотиків, медикаментозних помилок або неправильного вибору тактики ведення пацієнта.

Медична інформація є також необхідною для організації евакуації та передачі пацієнта між закладами охорони здоров'я. Під час переміщення пацієнта важливо забезпечити передачу даних про діагноз, проведене лікування, оперативні втручання, призначені лікарські засоби, алергії, інфекційний статус, результати обстежень і подальший план лікування. У разі втрати або неповної передачі цієї інформації приймаючий заклад змушений повторно збирати анамнез, дублювати діагностику або приймати рішення в умовах інформаційної невизначеності.

У контексті біологічних загроз медична інформація є основою інфекційного контролю. Дані про мікробіологічні посіви, антибіотикограму, колонізацію мультирезистентними мікроорганізмами, інфекційні ускладнення, ізоляційні заходи та проведену антибіотикотерапію мають значення не лише для окремого пацієнта, а й для безпеки інших пацієнтів і персоналу. Цифрові медичні дані можуть використовуватися для моніторингу поширення інфекцій, аналізу антибіотикорезистентності, контролю спалахів, оцінки ефективності антимікробної терапії та прийняття управлінських рішень щодо інфекційної безпеки. При цьому обмін медичною інформацією для цілей інфекційного контролю, організації лікування або протиепідемічних заходів має здійснюватися в межах законодавчо визначених підстав і з дотриманням вимог щодо лікарської таємниці. Такий підхід дозволяє поєднати потребу в оперативному реагуванні на біологічні загрози із захистом прав пацієнта на конфіденційність медичної інформації.

Дані про можливий вплив токсичних речовин, продуктів горіння, забрудненої води, промислових викидів, радіаційних або інших екологічних факторів можуть бути необхідними для діагностики, спостереження, лікування та довгострокового моніторингу постраждалих. У разі масових інцидентів або надзвичайних ситуацій саме достовірні цифрові дані дозволяють оцінити кількість постраждалих, характер уражень, потребу в медикаментах, антидотах, лабораторному контролі та ресурсах системи охорони здоров'я.

Фармакотерапія в умовах війни також значною мірою залежить від якості й доступності медичної інформації. Дані про призначення лікарських засобів, дози, кратність введення, тривалість лікування, алергічні реакції, побічні реакції, лікарські взаємодії, функцію нирок і печінки, результати терапевтичного моніторингу та ефективність лікування є необхідними для безпечного використання медикаментів. У цифровій системі ці дані можуть використовуватися для зменшення медикаментозних помилок, контролю призначень, підтримки клінічних рішень і фармацевтичної опіки. Узагальнення ролі медичної інформації у реагуванні на біологічні, хімічні та екологічні загрози наведено в таблиці 1.

Таблиця 1

Роль медичної інформації у реагуванні на біологічні, хімічні та екологічні загрози в умовах війни

Тип загрози	Які медичні дані є критичними	Для чого використовуються	Ризик при втраті, витоку або спотворенні даних
Біологічні загрози	Дані про інфекційний статус, мікробіологічні посіви, антибіотикограму, колонізацію мультирезистентними мікроорганізмами, ізоляційні заходи, антибіотикотерапію	Інфекційний контроль, епідеміологічний нагляд, вибір антимікробної терапії, попередження спалахів	Поширення інфекцій, нераціональна антибіотикотерапія, затримка ізоляційних заходів, ризик для інших пацієнтів і персоналу
Хімічні загрози	Дані про можливу експозицію до токсичних речовин, симптоми ураження, лабораторні показники, призначення антидотів, динаміку стану	Діагностика, вибір лікування, спостереження, оцінка потреби в антидотах і спеціалізованій допомозі	Помилкова оцінка тяжкості стану, затримка лікування, неправильне призначення терапії
Екологічні загрози	Дані про вплив забрудненої води, повітря, ґрунту, продуктів горіння, промислових викидів, радіаційних або інших факторів	Довготривалий моніторинг здоров'я населення, громадське здоров'я, планування ресурсів, профілактика ускладнень	Неможливість оцінити масштаби впливу, втрачений зв'язок між фактором довкілля і станом здоров'я, слабке планування медичної відповіді
Воєнні травми та евакуація	Дані про характер травми, оперативні втручання, крововтрату, інфекційні ускладнення, алергії, фармакотерапію, маршрут пацієнта	Передача пацієнта між закладами, безперервність лікування, реабілітація, протезування	Дублювання обстежень, затримка лікування, медикаментозні помилки, порушення реабілітаційного маршруту
Фармакотерапія в умовах криз	Дані про призначення ЛЗ, дози, взаємодії, алергії, побічні реакції, функцію нирок і печінки	Безпечне застосування ліків, клінічна фармація, попередження медикаментозних помилок	Неправильне дозування, небезпечні взаємодії, повторне призначення препарату при алергії, шкода пацієнту

ОСНОВНІ КІБЕРЗАГРОЗИ ДЛЯ МЕДИЧНОЇ ІНФОРМАЦІЇ

Цифрова трансформація охорони здоров'я супроводжується не лише підвищенням ефективності медичної допомоги, але й формуванням нового спектра інформаційних і кібернетичних ризиків. У галузі охорони здоров'я ці ризики мають особливе значення, оскільки об'єктом захисту є не лише технічна інфраструктура чи програмне забезпечення, а насамперед медична інформація, від якої залежить якість, безпечність і безперервність лікування пацієнта.

До основних напрямів можливих порушень інформаційної безпеки медичних інформаційних систем належать витік даних, втрата даних та несанкціонована модифікація даних. Для медичної сфери класична тріада інформаційної безпеки – конфіденційність, цілісність і доступність – має безпосереднє клінічне значення. Конфіденційність забезпечує захист персональних і медичних даних пацієнта; цілісність гарантує незмінність і достовірність клінічних записів; доступність означає можливість своєчасного отримання необхідної інформації для прийняття клінічних рішень.

Однією з найважливіших загроз є витік медичної інформації, тобто порушення її конфіденційності. Медичні дані містять інформацію про факт звернення за медичною допомогою,

діагнози, результати обстежень, інфекційний статус, хірургічні втручання, призначення лікарських засобів, психоемоційний стан, реабілітаційні потреби та інші чутливі відомості. В умовах воєнного стану витік таких даних може мати не лише етичні та юридичні наслідки, а й створювати ризики для фізичної безпеки пацієнтів, особливо військових, постраждалих від бойових дій, внутрішньо переміщених осіб або інших вразливих категорій.

Другою критичною загрозою є втрата медичних даних. Втрата інформації може бути наслідком технічного збою, кібератаки, шкідливого програмного забезпечення, помилки персоналу, неналежного резервного копіювання або руйнування інфраструктури внаслідок бойових дій. У клінічному вимірі втрата даних означає відсутність доступу до анамнезу, алергій, попередньої антибіотикотерапії, результатів лабораторних досліджень, даних про оперативні втручання чи реабілітаційний план.

Третьою загрозою є несанкціонована модифікація медичних даних, тобто порушення їх цілісності. Така модифікація може стосуватися діагнозів, лабораторних показників, алергій, доз лікарських засобів, режимів антибіотикотерапії, записів про введення препаратів або результатів мікробіологічних досліджень. На відміну від простого витоку інформації, спотворення медичних записів може безпосередньо спричинити неправильне клінічне рішення.

Окрему групу складають атаки типу *DoS / DDoS*, спрямовані на порушення доступності цифрових сервісів. Для закладу охорони здоров'я це означає ризик втрати доступу до медичної інформаційної системи (МІС), електронних медичних записів, результатів обстежень, електронних призначень або інших критичних цифрових сервісів. В умовах війни недоступність МІС може порушити маршрутизацію пацієнтів, надання невідкладної допомоги, ведення антибіотикотерапії та передачу пацієнтів між закладами.

Важливим джерелом кіберризиків залишається людський фактор. У медичному закладі він може проявлятися у використанні слабких паролів, передачі облікових даних іншим особам, відкритті фішингових листів, роботі з незахищених пристроїв, залишенні відкритого доступу до МІС, надсиланні медичних даних через неофіційні канали комунікації або введенні персональних даних у неперевірені цифрові сервіси.

Особливо небезпечним механізмом реалізації людського фактору є фішинг. Фішингові атаки можуть бути спрямовані на отримання логінів, паролів, електронних підписів або доступу до внутрішніх систем закладу. В умовах високого навантаження на медичних працівників, дефіциту часу, воєнного стану та постійної роботи з електронними повідомленнями й документами ризик фішингу зростає. Саме тому кібергігієна персоналу має розглядатися як обов'язкова складова безпеки пацієнта, а не лише як технічне навчання.

Ще однією загрозою є несанкціонований доступ до медичної інформації. Він може виникати через надмірні права користувачів, відсутність регулярного перегляду ролей доступу, використання спільних облікових записів, недостатній контроль за діями користувачів або порушення процедур автентифікації. З організаційної точки зору, профілактика таких ризиків потребує не лише технічних засобів захисту, а й внутрішніх нормативних документів закладу охорони здоров'я: політик, регламентів, інструкцій і процедур, які визначають мету та підстави обробки персональних даних, порядок доступу до них, строки й умови зберігання, процедури зміни, видалення або знищення даних, а також заходи захисту й порядок фіксації операцій, пов'язаних з обробкою персональних даних.

В умовах впровадження штучного інтелекту з'являється додатковий напрям ризиків. *AI*-інструменти можуть використовуватися для аналізу клінічних даних, підтримки прийняття рішень,

прогнозування ризиків, оптимізації дозування лікарських засобів або адміністративної аналітики. Водночас неконтрольоване використання відкритих або неперевірених *AI*-сервісів може створювати ризик витоку персональних даних, формування помилкових рекомендацій, не прозорості алгоритмічного рішення або надмірної довіри до автоматизованого висновку. Узагальнення цифрових компонентів охорони здоров'я та пов'язаних із ними кіберризиків наведено в таблиці 2.

Таблиця 2

Цифрові компоненти охорони здоров'я та пов'язані кіберризики в умовах війни

Цифровий компонент	**Функціональне значення**	**Потенційний кіберризик**	**Можливі наслідки в умовах війни**
МІС / ЕСОЗ	Ведення електронної медичної документації, доступ до даних пацієнта	Несанкціонований доступ, блокування, втрата даних	Порушення безперервності лікування, неможливість швидкого прийняття клінічних рішень
EHR (Electronic Health Record) / електронні медичні записи	Збереження анамнезу, діагнозів, призначень, алергій, лабораторних даних	Спотворення або видалення записів	Помилки у лікуванні, ризик неправильного призначення лікарських засобів
Телемедицина	Дистанційні консультації, підтримка пацієнтів у віддалених або небезпечних регіонах	Незахищений канал зв'язку, перехоплення даних	Витік медичної інформації, зниження довіри до дистанційної допомоги
Big Data	Аналітика, прогнозування, епідеміологічний нагляд, управління ресурсами	Повторна ідентифікація пацієнтів, неконтрольований доступ до масивів даних	Розкриття чутливої інформації про групи пацієнтів або медичні заклади
Штучний інтелект	Підтримка клінічних і управлінських рішень	Помилкові рекомендації, непрозорість алгоритму, витік даних у зовнішні сервіси	Ризик клінічної помилки, порушення конфіденційності
IoT (Internet of Things) / медичні пристрої	Моніторинг стану пацієнта, дистанційний контроль показників	Втручання в роботу пристрою, передача даних через незахищені мережі	Хибні клінічні сигнали, ризик для безпеки пацієнта
Електронні рецепти / е-направлення	Оптимізація маршруту пацієнта та призначень	Несанкціонована зміна або блокування	Затримка лікування, помилки у фармакотерапії

Клінічне значення основних компонентів інформаційної безпеки медичних даних представлено в таблиці 3.

Таблиця 3

Тріада інформаційної безпеки медичних даних та її клінічне значення

Компонент інформаційної безпеки	**Що означає для медичної інформації**	**Приклад порушення**	**Потенційний клінічний наслідок**
Конфіденційність	Захист персональних і медичних даних від несанкціонованого доступу	Витік діагнозів, даних про травми, результатів обстежень, інфекційного статусу	Порушення прав пацієнта, ризик стигматизації, загроза безпеці військових або постраждалих
Цілісність	Захист даних від несанкціонованої зміни, спотворення або видалення	Зміна призначення, алергії, результату лабораторного аналізу, антибіотикограми	Неправильне лікування, медикаментозна помилка, ризик шкоди пацієнту
Доступність	Можливість своєчасного доступу до даних для надання допомоги	Блокування МІС, *DDoS, ransomware*, відсутність доступу до історії хвороби	Затримка лікування, порушення маршрутизації, зниження якості медичної допомоги

Аналіз тріади інформаційної безпеки дозволяє розглядати кіберризики медичної інформації не лише як технічні порушення, а як фактори, що можуть мати безпосередні клінічні, організаційні та управлінські наслідки. Порушення конфіденційності призводить до розкриття чутливих персональних і медичних даних; порушення цілісності створює ризик спотворення клінічної інформації та прийняття помилкових медичних рішень; порушення доступності унеможливлює своєчасне використання даних для лікування, евакуації, інфекційного контролю або реагування на надзвичайні ситуації.

За умов воєнного стану ці ризики посилюються через підвищене навантаження на заклади охорони здоров'я, потребу в швидкому обміні інформацією між різними рівнями медичної допомоги, загрозу цілеспрямованих кібератак, перебої в роботі цифрової та енергетичної інфраструктури, а також активне використання зовнішніх цифрових сервісів. Тому для практичного управління кібербезпекою доцільно класифікувати загрози за їх походженням, об'єктом впливу, потенційними наслідками для закладу охорони здоров'я та можливими заходами реагування. Такий підхід дозволяє перейти від загального розуміння інформаційної безпеки до формування конкретних управлінських і технічних рішень, спрямованих на захист медичної інформації та підтримання безперервності медичної допомоги.

Основні групи загроз медичній інформації в умовах війни наведено в таблиці 4.

Таблиця 4

Класифікація загроз медичній інформації в умовах війни

Група загроз	**Приклади**	**Об'єкт впливу**	**Наслідки для закладу охорони здоров'я**	**Заходи реагування**
Технічні	*DDoS, malware, ransomware*, збій серверів	МІС, ЕСОЗ, мережі, бази даних	Недоступність систем, втрата або блокування даних	Резервне копіювання, сегментація мережі, антивірусний захист, план аварійного відновлення
Організаційні	Відсутність політики інформаційної безпеки, нечіткі ролі, слабкий контроль доступів	Управлінські процеси закладу охорони здоров'я	Неконтрольоване використання даних, затримка реагування на інциденти	Політика інформаційної безпеки, аудит доступів, визначення відповідальних осіб
Людський фактор	Фішинг, слабкі паролі, передача логінів, помилки персоналу	Користувачі МІС	Витік, втрата або спотворення даних	Навчання, кібергігієна, багатофакторна автентифікація, інструкції для персоналу
Воєнні	Цілеспрямовані атаки на медичну інфраструктуру, руйнування цифрової або енергетичної інфраструктури	Заклади охорони здоров'я, державні реєстри, пацієнтські дані	Дестабілізація роботи, паніка, порушення безперервності допомоги	Кризовий план, резервні процеси, автономні канали зв'язку, взаємодія з державними структурами
AI-ризики	Введення персональних даних у зовнішні *AI*-сервіси, помилкові рекомендації	Клінічні та управлінські рішення	Витік даних, помилкові рішення, надмірна довіра до алгоритму	Політика використання *AI*, заборона персональних даних у відкритих сервісах, людська перевірка рекомендацій

Наведена класифікація демонструє, що кіберзагрози медичній інформації мають багаторівневий характер і не можуть бути усунуті лише технічними засобами. Їх ефективне управління потребує поєднання організаційних рішень, технологічного захисту, навчання персоналу, клінічного контролю та готовності до кризових ситуацій. Саме тому доцільним є

формування концептуальної моделі кіберстійкості медичної інформації, яка поєднує управлінський, технічний, клінічний і безпековий напрямки.

КОНЦЕПТУАЛЬНА МОДЕЛЬ КІБЕРСТІЙКОСТІ МЕДИЧНОЇ ІНФОРМАЦІЇ

З огляду на комплексний характер цифрової трансформації охорони здоров'я та зростання кіберризиків, доцільним є формування концептуальної моделі кіберстійкості медичної інформації в умовах війни. Така модель має поєднувати, на нашу думку, не лише технічні засоби захисту, а й організаційні, кадрові, клінічні, кризові та етичні механізми управління цифровими ризиками.

Кіберстійкість медичної інформації можна розглядати як здатність закладу охорони здоров'я забезпечувати конфіденційність, цілісність і доступність медичних даних, підтримувати безперервність клінічних процесів, своєчасно реагувати на кіберінциденти та відновлювати роботу цифрової інфраструктури без критичного впливу на безпеку пацієнта.

Центральним об'єктом запропонованої моделі є медична інформація як критичний ресурс системи охорони здоров'я. До неї належать персональні дані пацієнта, діагнози, результати лабораторних та інструментальних досліджень, дані про інфекційний статус, алергії, призначення лікарських засобів, антибіотикотерапію, оперативні втручання, реабілітаційний маршрут, дані телемедицини та інформація, що може використовуватися для аналітики або штучного інтелекту.

Узагальнення наведених ризиків свідчить, що кібербезпека медичної інформації має міждисциплінарний характер і перебуває на перетині інформаційної безпеки, клінічного управління, громадського здоров'я, біологічної безпеки, фармакотерапії та кризового менеджменту. Тому оцінка кіберризиків у закладі охорони здоров'я повинна враховувати не лише ймовірність технічного інциденту, а й потенційний клінічний вплив на пацієнта, персонал, епідеміологічну ситуацію та здатність закладу функціонувати в умовах війни.

Запропонована нами модель включає сім взаємопов'язаних рівнів: стратегічний, організаційний, технологічний, кадровий, клініко-безпековий, воєнно-кризовий та *AI*-рівень.

Перший рівень – стратегічний. Він передбачає включення кібербезпеки медичної інформації до загальної стратегії розвитку та стійкості закладу охорони здоров'я. На цьому рівні мають бути визначені політика інформаційної безпеки, відповідальність керівництва, пріоритети захисту критичних даних, порядок оцінки ризиків і взаємозв'язок кібербезпеки з управлінням якістю та безпекою пацієнта.

Другий рівень – організаційний. Він охоплює розподіл ролей і відповідальності, управління доступами, регламенти роботи з МІС, порядок повідомлення про інциденти, аудит дій користувачів і внутрішній контроль дотримання правил інформаційної безпеки. На цьому рівні мають бути запроваджені внутрішні документи закладу охорони здоров'я — політики, регламенти, інструкції та процедури, що визначають мету й підстави обробки персональних і медичних даних, порядок доступу до них, строки та умови зберігання, процедури зміни, видалення або знищення даних, а також порядок фіксації операцій, пов'язаних з їх обробкою. Важливою умовою реалізації організаційного рівня є визначення відповідальної особи або створення окремого структурного підрозділу в закладі охорони здоров'я, який організовує роботу, пов'язану з кіберзахистом персональних і медичних даних, координує внутрішні політики, контролює управління доступами, бере участь у реагуванні на інциденти та організовує навчання персоналу з питань кібергігієни.

Третій рівень – технологічний. Він включає застосування технічних засобів захисту: багатофакторної автентифікації, кваліфікованого електронного підпису (КЕП), шифрування,

журналювання дій користувачів, резервного копіювання, антивірусного захисту, контролю мережевого доступу, сегментації мережі та планів відновлення після збоїв.

Четвертий рівень – кадровий. Він передбачає формування цифрової культури та кібергігієни персоналу. Для медичного закладу це означає регулярне навчання працівників щодо фішингу, безпечного використання паролів, правил роботи з медичними даними, недопущення передачі облікових записів і коректного використання цифрових сервісів. Практична реалізація кадрового рівня має включати не лише загальне інформування персоналу, а й регулярне навчання конкретним правилам безпечної цифрової поведінки: використанню складних і унікальних паролів, забороні передачі паролів та кваліфікованого електронного підпису іншим особам, блокуванню робочого комп'ютера при відході від робочого місця, уникненню публічних *Wi-Fi*-мереж для робочих завдань, обережності при роботі з електронною поштою та вкладеннями, а також недопущенню використання невідомих зовнішніх носіїв інформації. Такі заходи зменшують ризики, пов'язані з людським фактором, фішингом і несанкціонованим доступом до медичних даних.

П'ятий рівень – клініко-безпековий. Він відображає зв'язок кібербезпеки з безпекою пацієнта. На цьому рівні визначаються критичні клінічні дані, доступ до яких має бути гарантований навіть у разі цифрових збоїв: алергії, життєво важливі призначення, антибіотикотерапія, результати критичних лабораторних показників, інфекційний статус, дані про оперативні втручання та план лікування. Для забезпечення безперервності медичної допомоги доцільно передбачити внутрішні процедури збереження, резервного доступу та оперативного відновлення мінімального набору критичної клінічної інформації, необхідної для прийняття невідкладних рішень щодо лікування, евакуації, інфекційного контролю та фармакотерапії.

Шостий рівень – воєнно-кризовий. Він передбачає готовність закладу охорони здоров'я до роботи в умовах кібератак, відключення МІС, руйнування інфраструктури, перебоїв електропостачання або зв'язку. Цей рівень має включати резервні алгоритми роботи, паперові або локальні форми критичної документації, плани відновлення доступу до даних, порядок передачі пацієнта при недоступності цифрових систем та взаємодію з відповідальними державними структурами. Воєнно-кризовий рівень має передбачати не лише технічне відновлення роботи МІС, а й заздалегідь визначений план дій у разі несанкціонованого доступу до персональних або медичних даних, пошкодження технічного обладнання, втрати доступу до електронної системи охорони здоров'я чи інших надзвичайних ситуацій. Такий план повинен визначати порядок повідомлення відповідальних осіб, тимчасові резервні способи документування критичних клінічних даних, відновлення доступу, мінімізацію шкоди для пацієнтів і подальший аналіз інциденту.

Сьомий рівень – *AI*-рівень. Він стосується безпечного, етичного та контрольованого використання штучного інтелекту. Цей рівень має передбачати заборону введення ідентифікованих персональних і медичних даних у неперевірені зовнішні *AI*-сервіси, обов'язкову людську перевірку *AI*-рекомендацій, оцінку достовірності алгоритмів, прозорість використання *AI*-інструментів і відповідальність фахівця за кінцеве клінічне рішення (рис. 1).

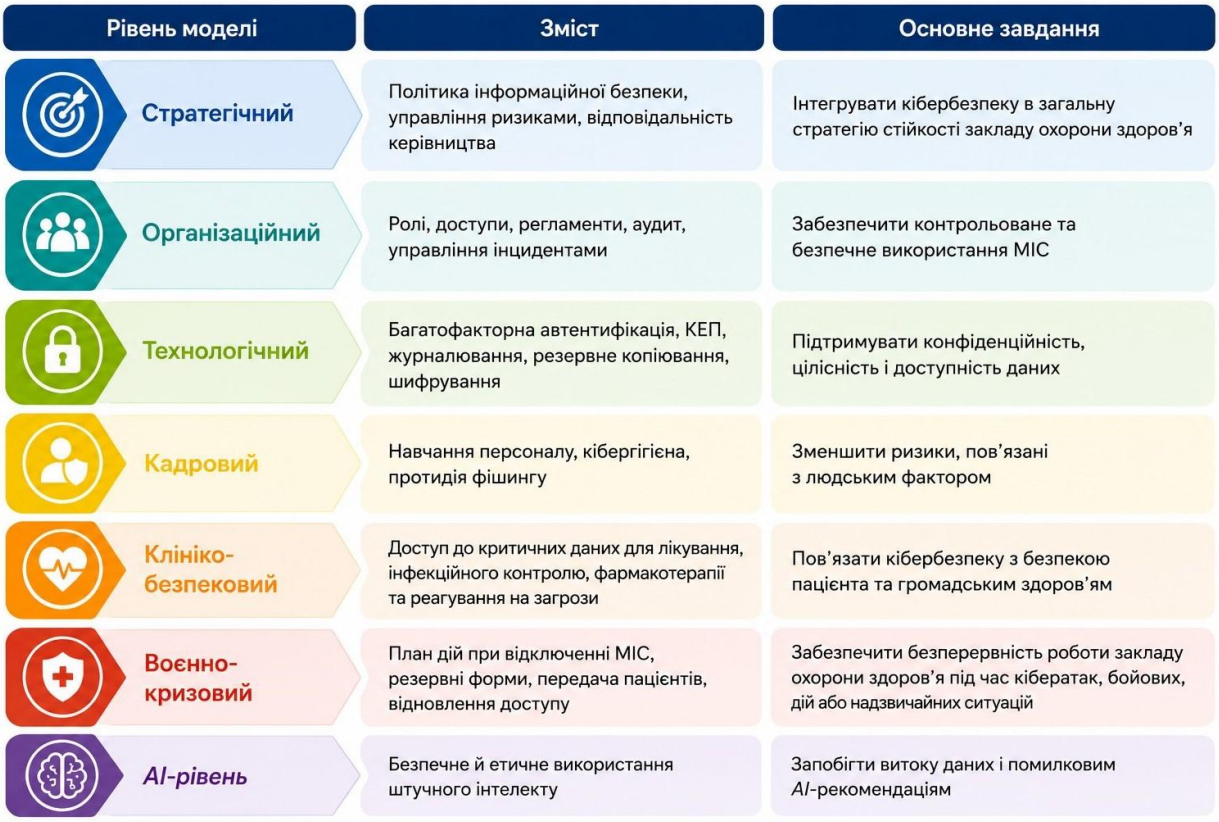

Рисунок 1. Концептуальна модель кіберстійкості медичної інформації, сформована авторами на основі опрацьованих джерел

Таким чином, кібербезпека медичної інформації в умовах війни є складовою не лише цифрової трансформації, а й біологічної, хімічної та екологічної безпеки. Захищені, достовірні та доступні медичні дані необхідні для інфекційного контролю, епідеміологічного нагляду, реагування на хімічні ураження, оцінки наслідків екологічних факторів, безпечної фармакотерапії, евакуації та реабілітації пацієнтів. Тому, кібербезпека має бути інтегрована в систему управління якістю, безпеки пацієнта, громадського здоров'я та кризової стійкості закладу охорони здоров'я.

ВИСНОВКИ

Цифрова трансформація охорони здоров'я є необхідною умовою розвитку сучасної медичної системи, підвищення доступності, якості та ефективності медичної допомоги. Водночас активне впровадження медичних інформаційних систем, електронних медичних записів, телемедицини, аналітики великих даних, штучного інтелекту та інших цифрових інструментів формує нові ризики для конфіденційності, цілісності та доступності медичної інформації.

В умовах війни медична інформація набуває значення критичного ресурсу для лікування, евакуації, інфекційного контролю, епідеміологічного нагляду, фармакотерапії, реабілітації, управління ресурсами та забезпечення безперервності медичної допомоги. Її витік, втрата, спотворення або недоступність можуть мати не лише правові чи організаційні наслідки, а й безпосередньо впливати на безпеку пацієнта.

У межах реагування на біологічні загрози захищені медичні дані необхідні для контролю інфекційних ускладнень, моніторингу антибіотикорезистентності, виявлення мультирезистентних мікроорганізмів та запобігання спалахам. У контексті хімічних загроз вони забезпечують

документування експозиції, оцінку клінічних проявів і вибір лікувальної тактики. При екологічних загрозах цифрові медичні дані є основою для довготривалого моніторингу впливу факторів довкілля на здоров'я населення.

Основними кіберзагрозами для медичної інформації є витік даних, втрата інформації, несанкціонована модифікація медичних записів, *DDoS*-атаки, шкідливе програмне забезпечення, фішинг, несанкціонований доступ, людський фактор і неконтрольоване використання штучного інтелекту. Ці загрози мають розглядатися не ізольовано, а як частина загальної системи управління ризиками закладу охорони здоров'я.

Запропонована концептуальна модель кіберстійкості медичної інформації включає сім рівнів: стратегічний, організаційний, технологічний, кадровий, клініко-безпековий, воєнно-кризовий та *AI*-рівень. Така структура дозволяє розглядати кібербезпеку як комплексну управлінську, клінічну, етичну та кризову систему захисту медичних даних.

Кібербезпека медичної інформації має бути інтегрована в систему управління якістю, безпекою пацієнта, громадським здоров'ям та кризовою стійкістю закладу охорони здоров'я. У сучасних умовах вона є необхідною передумовою безперервності лікування, довіри до цифрової медицини та здатності медичної системи ефективно реагувати на виклики війни, біологічні, хімічні й екологічні загрози.