

УДК 342.9:351.77

DOI 10.33244/2617-4154.3(24).2026.107-117

А. Ю. Тарасюк,*доктор філософії у галузі права, учений секретар,**ПВНЗ «Інститут екології, економіки і права»***A. Yu. Tarasiuk,***PhD in Law, Academic Secretary,**Private Higher Educational Institution "Institute of Ecology, Economics and Law"**email: andy.tarasiuk@gmail.com***ORCID 0009-0008-7115-1072**

ЦИФРОВА ІНФРАСТРУКТУРА ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ТА БЕЗПЕРЕРВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

DIGITAL INFRASTRUCTURE AS A MEANS OF ENSURING THE RESILIENCE AND CONTINUITY OF UKRAINE'S HEALTHCARE SYSTEM UNDER MARTIAL LAW

У статті використано формально-юридичний, системно-структурний, порівняльно-правовий та аналітичний методи. Емпіричну основу становлять офіційні дані Міністерства охорони здоров'я України (МОЗ України), Всесвітньої організації охорони здоров'я (ВООЗ) та електронної системи охорони здоров'я (ЕСОЗ), а також дослідження 2021–2026 років. Цифрову інфраструктуру системи охорони здоров'я запропоновано розуміти як нормативно й організаційно впорядковану сукупність центральної бази даних ЕСОЗ, електронних медичних інформаційних систем, реєстрів, телемедичних сервісів, електронних комунікацій, хмарних і резервних ресурсів, стандартів інтероперабельності, засобів кіберзахисту та процедур відновлення. Встановлено, що в умовах війни цифрові інструменти виконують сервісну й частково компенсаторну функції, підтримуючи доступ до медичної інформації, електронні направлення й рецепти, телемедичну взаємодію та маршрутизацію пацієнтів. Безперервність функціонування цифрової інфраструктури водночас залежить від електропостачання, електронних комунікацій, технічної сумісності



Ця робота ліцензується відповідно до [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

© Тарасюк А. Ю., 2026

та кібербезпеки. Обґрунтовано перехід від фрагментарного регулювання електронних сервісів до моделі нормативного забезпечення стійкості цифрової інфраструктури. Запропоновано мінімальні секторальні вимоги щодо резервування компонентів і копій даних, альтернативних каналів зв'язку, режимів роботи з обмеженою функціональністю, планів безперервності й аварійного відновлення, цільового часу та точки відновлення, регулярного тестування й аудиту, а також урахування підходів NIS2 і Європейського простору даних про здоров'я.

Ключові слова: електронна система охорони здоров'я, телемедицина, кібербезпека, електронні медичні записи, охорона здоров'я, управління даними, цифрова інфраструктура, *acquis* ЄС.

The article aims to determine the administrative and legal significance of the digital infrastructure of Ukraine's healthcare system as a means of ensuring its resilience and continuity under martial law and to substantiate requirements for its fault tolerance, recoverability, interoperability and security. Formal legal, systemic-structural, comparative legal and analytical methods are used. The empirical basis includes official data from the Ministry of Health of Ukraine, the World Health Organization (WHO) and Ukraine's electronic health care system (eHealth), as well as relevant studies published in 2021–2026. The digital infrastructure of the healthcare system is proposed to be understood as a legally regulated and organizationally structured set of the central eHealth database, electronic medical information systems, registries, telemedicine services, electronic communications, cloud and backup resources, interoperability standards, cybersecurity safeguards and recovery procedures. It is established that during wartime digital tools perform service and partly compensatory functions by supporting access to medical information, electronic referrals and prescriptions, telemedicine interaction and patient routing. At the same time, continuity of the digital infrastructure depends on electricity, electronic communications, technical compatibility and cybersecurity. The study substantiates a shift from fragmented regulation of electronic services to a regulatory model for digital-infrastructure resilience. Minimum sectoral requirements are proposed for redundancy of components and data copies, alternative communication channels, limited-functionality modes, business-continuity and disaster-recovery plans, recovery-time and recovery-point objectives, regular testing and audits, and consideration of the NIS2 framework and the European Health Data Space.

Keywords: eHealth, telemedicine, cybersecurity, electronic medical records, healthcare, data governance, digital infrastructure, EU *acquis*.

Постановка проблеми. Повномасштабна збройна агресія проти України перетворила забезпечення безперервності надання медичної допомоги з переважно організаційного завдання на складову національної стійкості та реалізації конституційного права людини на охорону здоров'я. Заклади охорони здоров'я функціонують в умовах руйнування будівель, переміщення персоналу й пацієнтів, перебоїв електропостачання та електронних комунікацій, а також зростання навантаження на територіальні громади, що приймають внутрішньо переміщених осіб. Станом на 1 липня 2026 р. Міністерство охорони здоров'я

Тарасюк А. Ю. Цифрова інфраструктура як засіб забезпечення стійкості та безперервності функціонування системи охорони здоров'я України в умовах воєнного стану

України (далі – МОЗ України) підтвердило пошкодження або знищення 2 647 об'єктів у складі 846 закладів охорони здоров'я; 335 об'єктів у складі 124 закладів, зруйнованих повністю [1]. Всесвітня організація охорони здоров'я (ВООЗ) станом на травень 2026 р. верифікувала понад 3 000 атак на охорону здоров'я в Україні, причому приблизно 80 % підтверджених атак стосувалися амбулаторій, лікарень та інших місць надання допомоги [2]. За таких обставин залежність доступу до медичної інформації від паперового документообігу та конкретного місця її зберігання підвищує ризик порушення наступності надання медичної допомоги.

Водночас в Україні сформовано масштабну цифрову інфраструктуру системи охорони здоров'я. У квітні 2026 р. електронна система охорони здоров'я (далі – ЕСОЗ) централізовано зберігала інформацію про здоров'я 34,6 млн осіб, а кількість електронних медичних записів перевищила 5 млрд [3]. Це свідчить, що цифрові рішення вже не можуть розглядатися лише як засіб підвищення зручності адміністративних процедур. За наявності належної правової, технічної та організаційної архітектури вони підтримують доступність медичної інформації, її переносимість між надавачами медичних послуг, дистанційну взаємодію та інформаційно-аналітичне забезпечення управління. Проте цифрова інфраструктура є лише одним із засобів забезпечення безперервності функціонування системи охорони здоров'я й не замінює фізичної інфраструктури, кадрового, енергетичного та логістичного забезпечення. Саме тому актуальним є перехід від логіки оцифрування окремих послуг до правового забезпечення стійкості цифрової інфраструктури як взаємопов'язаної системи.

Аналіз останніх досліджень і публікацій. Проблематика цифрової трансформації охорони здоров'я впродовж останніх п'яти років досліджувалася з різних правових і міждисциплінарних позицій. Н. В. Коробцова розкрила механізм упровадження електронної охорони здоров'я (eHealth), її складові та значення для реалізації інформаційних прав пацієнта [4, р. 117–126]. О. М. Геглюк систематизувала нормативно-правові засади цифровізації охорони здоров'я та окреслила роль електронних сервісів у реформуванні галузі [5, с. 36–43]. О. А. Музика-Стефанчук, М. О. Стефанчук і Н. Я. Якимчук пов'язали цифровізацію з трансформацією фінансування та використанням даних у процесах управління системою охорони здоров'я [6, с. 359–365]. К. С. Малахов проаналізував архітектуру, стандарти й нормативні зміни української системи електронної охорони здоров'я, окремо звернувши увагу на роль телемедицини в умовах війни [7, р. 1–21].

С. Б. Булеца, М. В. Менджул та А. І. Калько розглянули цифровізацію крізь призму права на медичну допомогу та показали її значення для доступності допомоги у воєнний період [8, с. 356–360]. О. В. Батрин, В. І. Теремецький та О. А. Івахненко дослідили правові гарантії доступності медичної та реабілітаційної допомоги під час воєнного стану, акцентувавши на потребі в адаптації системи до переміщення населення й руйнування мережі закладів [9, с. 46–58]. Я. Хабіхт, М. Гелловелл і Дж. Кутзін встановили, що сформовані до повномасштабного вторгнення інституційні механізми фінансування та єдина інформаційна система електронної охорони здоров'я сприяли збереженню основних функцій системи охорони здоров'я під час війни [10, р. 799–802]. М. С. Вальчук звернув увагу на роль дистанційного моніторингу, дистанційних медичних сервісів та інших цифрових рішень у забезпеченні пацієнтоорієнтованості [11, с. 14–22].

Тарасюк А. Ю. Цифрова інфраструктура як засіб забезпечення стійкості та безперервності функціонування системи охорони здоров'я України в умовах воєнного стану

Практичний вимір стійкості цифрової інфраструктури відображено також в англomовних дослідженнях, присвячених українському досвіду. А. Нараян і співавтори на матеріалах TeleHelp Ukraine показали можливості децентралізованої міжнародної телемедичної мережі для підтримання дистанційного доступу до консультацій у гуманітарній кризі [12, р. 1–3]. У дослідженні функціонування цифрового сервісу «АРТ поруч» (антиретровірусна терапія) продемонстровано можливість відновлення зв'язку людей, які живуть з ВІЛ, із закладами охорони здоров'я за допомогою вебсайту, чат-бота та бази даних. Зокрема, вебсайт сервісу зафіксував 20 619 відвідувань, а чат-бот було активовано 2 950 користувачами [13, р. 1–3]. А. В. Сидорук 2026 року обґрунтував потребу в системних адміністративно-правових засадах державної політики цифровізації та вказав на фрагментарність нормативного регулювання [14, с. 143–151]. У монографії В. І. Теремецького та співавторів стійкість (резильєнтність) охарактеризовано як здатність систем ідентифікувати ризики, протидіяти їм, адаптуватися та відновлювати функціонування; стале функціонування медичної інфраструктури розглянуто як важливий компонент резильєнтності [15, с. 202, 217].

Наведені дослідження підтверджують значення цифровізації, телемедицини та переносимості даних для забезпечення доступності й безперервності медичної допомоги. Водночас у науковій літературі переважно аналізуються окремі сервіси, інформаційні права пацієнтів або цифрова трансформація загалом. Недостатньо досліджено цифрову інфраструктуру системи охорони здоров'я як цілісний об'єкт адміністративно-правового регулювання, для якого мають бути визначені вимоги безперервності, відновлюваності, резервування, інтеперабельності, кібербезпеки та розподілу відповідальності між суб'єктами.

Виділення невирішених раніше частин загальної проблеми. Невирішеними залишаються три взаємопов'язані аспекти. По-перше, законодавство визначає окремі елементи електронної охорони здоров'я, ЕСОЗ і телемедицини, однак не містить комплексного визначення цифрової інфраструктури системи охорони здоров'я та єдиних критеріїв її стійкості. По-друге, не встановлено комплексних секторальних вимог до забезпечення безперервності цифрових процесів у разі поєднання фізичних руйнувань, тривалих перебоїв енергопостачання, втрати електронних комунікацій і кібератак. По-третє, централізований обмін медичними даними потребує узгодження з вимогами резервування, інтеперабельності, захисту інформації та європейської інтеграції. Водночас запропонована в статті доктринальна категорія не означає автоматичного віднесення всіх її елементів до об'єктів критичної чи критичної інформаційної інфраструктури: відповідний юридичний статус визначається у встановленому законодавством порядку [16; 17].

Метою статті є визначення адміністративно-правового значення цифрової інфраструктури системи охорони здоров'я України як засобу забезпечення її стійкості та безперервності функціонування в умовах воєнного стану й обґрунтування вимог до її відмовостійкості, відновлюваності, інтеперабельності та захищеності. Для досягнення цієї мети поставлено такі **завдання**: уточнити зміст відповідної юридичної категорії; визначити її місце в системі чинного нормативно-правового регулювання електронної охорони здоров'я; на підставі емпіричних даних з'ясувати функції цифрової інфраструктури

Тарасюк А. Ю. Цифрова інфраструктура як засіб забезпечення стійкості та безперервності функціонування системи охорони здоров'я України в умовах воєнного стану

під час війни; виявити основні організаційно-правові ризики та ризики у сфері кібербезпеки; обґрунтувати мінімальні секторальні вимоги до безперервності й відновлення цифрових сервісів. Методологічну основу дослідження становлять формально-юридичний, системно-структурний, порівняльно-правовий та аналітичний методи, застосовані відповідно для аналізу нормативно-правових актів, встановлення взаємозв'язку складових цифрової інфраструктури, зіставлення національного регулювання з підходами Європейського Союзу та опрацювання емпіричних даних. З огляду на обмежений доступ до частини технічної інформації в умовах воєнного стану емпіричний аналіз обмежено даними з відкритих джерел, що враховано під час формулювання висновків.

Виклад основного матеріалу. Чинне законодавство містить вихідні елементи для формування юридичної конструкції цифрової інфраструктури системи охорони здоров'я. Основи законодавства України про охорону здоров'я визначають електронну систему охорони здоров'я як інформаційно-комунікаційну систему, що автоматизує облік медичних послуг та управління інформацією про охорону здоров'я і складається з центральної бази даних та електронних медичних інформаційних систем, між якими здійснюється автоматичний обмін через відкритий програмний інтерфейс (API) [18]. Порядок функціонування ЕСОЗ, затверджений постановою Кабінету Міністрів України № 411, деталізує структуру центральної бази даних, реєстри, права доступу та взаємодію компонентів [19]. Закон України № 3301-IX закріпив поняття електронної охорони здоров'я, телемедицини, телемедичної мережі, засобів і методів телемедицини; ст. 35-6 Основ прямо пов'язує телемедицину з використанням інформаційної, електронної комунікаційної та програмно-апаратної інфраструктури [20]. Спеціальний для періоду воєнного стану Порядок, затверджений наказом МОЗ України № 1695, регламентує організацію медичної та/або реабілітаційної допомоги із застосуванням телемедицини, поширюється на телемедичні платформи, інформаційно-комунікаційні системи та програмно-апаратні комплекси й вимагає внесення відповідних медичних записів до ЕСОЗ [21].

З огляду на це цифрову інфраструктуру системи охорони здоров'я доцільно визначити як нормативно й організаційно впорядковану сукупність центральної бази даних ЕСОЗ, електронних медичних інформаційних систем, державних і локальних реєстрів, телемедичних сервісів, засобів електронної ідентифікації та довірчих послуг, електронних комунікацій, хмарних і резервних обчислювальних ресурсів, стандартів інтероперабельності, засобів кіберзахисту, а також процедур управління даними, резервування та відновлення, які спільно підтримують юридично значущі процеси надання медичної та реабілітаційної допомоги. Таке визначення має доктринальний характер: воно відмежовує цифровізацію як процес упровадження технологій від цифрової інфраструктури у формі організаційно-технічної та правової основи їхнього стабільного функціонування. Для цілей цієї статті стійкість розглядається як ширша властивість системи – її здатність протистояти дестабілізаційним впливам, адаптуватися до них і відновлювати ключові функції, тоді як безперервність функціонування характеризує здатність підтримувати або оперативно відновлювати виконання критично важливих процесів. У такому співвідношенні безперервність є одним із функціональних проявів стійкості, а цифрова інфраструктура – засобом забезпечення обох властивостей [15, с. 202; 16].

Нормативні документи стратегічного характеру підтверджують потребу саме в інфраструктурному підході. Стратегія розбудови телемедицини пов'язує обмеження доступу до медичних послуг із руйнуванням медичної та транспортної інфраструктури, а серед напрямів розвитку називає сервіс-орієнтовану ієрархічну інфраструктуру, сумісність технічних рішень і взаємодію з ЕСОЗ [22]. Стратегія розвитку системи охорони здоров'я на період до 2030 року, чинна в редакції від 6 січня 2026 р., визначає технологізацію та цифровізацію управління, планування й організації послуг одним із напрямів розвитку системи [23]. Отже, у документах стратегічного планування цифрові рішення розглядаються як умова доступності та керованості охорони здоров'я, однак вимірювані критерії їх безперервності та відновлення не конкретизовано.

Емпіричні дані дають підстави виділити чотири основні функції цифрової інфраструктури в забезпеченні стійкості системи охорони здоров'я. Перша – забезпечення переносимості медичних даних: у разі переміщення пацієнта або зміни місця роботи закладу електронний запис зменшує залежність від паперової документації та конкретного місця її зберігання. Друга – підтримання безперервності окремих сервісів: електронні направлення, рецепти, медичні висновки та дистанційне консультування дають змогу підтримувати окремі етапи маршруту пацієнта за зміни звичайної організації роботи. Третя – розширення доступу до фахівців завдяки дистанційній взаємодії незалежно від місця перебування пацієнта. Четверта – інформаційно-аналітичне забезпечення управління, фінансування та оцінювання навантаження. Приклади проєктів «TeleHelp Ukraine» та «АРТ поруч» підтверджують, що цифрові рішення здатні забезпечувати зв'язок між пацієнтом і надавачем медичної допомоги в разі порушення звичних логістичних маршрутів [12, р. 1–3; 13, р. 1–3].

Стійкість цифрової інфраструктури залежить не тільки від центральної бази даних, а й від надійності підключених до неї систем. У червні 2026 р. державне підприємство «Електронне здоров'я» як технічний адміністратор відповідних компонентів центральної бази даних ЕСОЗ повідомило про відключення окремих медичних інформаційних систем, які не підтвердили відповідність актуальним технічним вимогам. У разі відключення МІС від центральної бази даних користувачі мають обрати іншу МІС для роботи в ЕСОЗ або продовжити використання відключеної системи лише щодо функціоналу, не підключеного до ЕСОЗ [24]. Цей приклад засвідчує, що безперервність функціонування цифрової інфраструктури потребує узгоджених вимог до центральних компонентів і підключених електронних медичних інформаційних систем, а також завчасно визначених процедур переходу між сумісними рішеннями без втрати доступу до даних.

Централізація сама собою не забезпечує стійкості цифрової інфраструктури. Критична залежність від окремого цифрового компонента підвищує ризик системних наслідків у разі його недоступності. Закон України «Про критичну інфраструктуру» визначає безпеку критичної інфраструктури як стан її захищеності, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість [16]. Ці властивості доцільно використовувати як орієнтири для оцінювання ключових цифрових компонентів системи охорони здоров'я, не ототожнюючи водночас доктринальне поняття «цифрова інфраструктура системи охорони здоров'я» з нормативними категоріями

Тарасюк А. Ю. Цифрова інфраструктура як засіб забезпечення стійкості та безперервності функціонування системи охорони здоров'я України в умовах воєнного стану

«об'єкт критичної інфраструктури» чи «об'єкт критичної інформаційної інфраструктури» [16; 17]. Для цифрових сервісів принципове значення має здатність продовжити роботу в обмеженому режимі або відновити її у визначений строк після пошкодження центру обробки даних, втрати електропостачання, електронних комунікацій чи кібератаки.

Кібербезпека є самостійною умовою безперервності. За даними Агентства Європейського Союзу з кібербезпеки (ENISA), у масиві з 215 публічно відомих інцидентів у європейському секторі охорони здоров'я програми-вимагачі становили 54 % інцидентів; інциденти, що стосувалися надавачів медичних послуг, становили 53 % досліджених випадків, а лікарень – 42 %. У 22 % інцидентів наслідком було порушення надання медичних послуг [25, р. 3]. Для України ці ризики поєднуються з воєнними атаками на енергетичну та комунікаційну інфраструктуру. Тому кіберзахист ЕСОЗ і підключених систем має оцінюватися не лише з позицій конфіденційності інформації, а й через вплив інциденту на доступність і безперервність надання медичної допомоги.

Європейський вектор дає орієнтири для такого підходу. Стаття 21 Директиви (ЄС) 2022/2555 (NIS2) вимагає від охоплених нею суб'єктів застосовувати пропорційні технічні, операційні й організаційні заходи управління кіберризиками, включно із безперервністю діяльності, управлінням резервними копіями, аварійним відновленням і кризовим управлінням; сектор охорони здоров'я включено до переліку секторів високої критичності [26]. Регламент (ЄС) 2025/327 про Європейський простір даних про здоров'я (EHDS) установлює спільні правила, стандарти, інфраструктури та механізми управління електронними даними про здоров'я та вимоги до інтегрованості систем електронних медичних записів; його основне застосування в ЄС розпочинається поетапно з 26 березня 2027 р. [27]. Для України ці акти є важливими орієнтирами адаптації до *acquis* ЄС, а не нормами прямої дії.

З огляду на викладене правове забезпечення стійкості має охоплювати не окремі сервіси, а взаємопов'язану сукупність процесів і компонентів, що забезпечують створення, передавання, зберігання, використання та відновлення медичних даних. Нормативне закріплення таких вимог доцільно здійснювати через поєднання загальних обов'язкових правил щодо безперервності критично важливих цифрових функцій із секторальними вимогами, встановленими актами МОЗ України та НСЗУ в межах їхніх повноважень, а технічну конкретизацію – у вимогах і процедурах, що визначаються технічними адміністраторами відповідних компонентів центральної бази даних ЕСОЗ та в передбачених законодавством випадках затверджуються НСЗУ [19]. Закон України «Про хмарні послуги» створює правову основу для використання хмарної інфраструктури, зокрема публічними користувачами, однак для сфери охорони здоров'я потрібні додаткові правила, що враховують особливу чутливість медичних даних і неприпустимість тривалої недоступності електронних сервісів, потрібних для надання медичної допомоги [28]. Доцільно також передбачити обов'язкове оцінювання впливу відмови цифрового компонента на безперервність конкретних медичних процесів.

Мінімальні секторальні вимоги до цифрової інфраструктури системи охорони здоров'я доцільно структурувати за п'ятьма блоками. Перший – архітектурна відмовостійкість: резервування критичних компонентів, географічне резервування копій даних, альтернативні

канали електронних комунікацій і резервне електроживлення ключових вузлів. Другий – операційна безперервність: плани безперервності та аварійного відновлення, цільовий час відновлення (Recovery Time Objective, RTO), цільова точка відновлення (Recovery Point Objective, RPO), а також автономні режими або режими роботи з обмеженою функціональністю за тимчасової недоступності мережі з подальшою безпечною синхронізацією. Третій – кіберстійкість: ризик-орієнтовані заходи захисту, управління вразливостями, журналювання критичних дій, резервне копіювання й процедури реагування на інциденти. Четвертий – інтероперабельність і переносимість даних: використання узгоджених форматів і стандартів, що дають змогу відновити доступ до клінічно значущої інформації в іншому закладі. П'ятий – інституційна підзвітність: чіткий розподіл обов'язків між НСЗУ як власником від імені держави та адміністратором центральної бази даних, технічними адміністраторами її відповідних компонентів, операторами електронних медичних інформаційних систем і закладами охорони здоров'я, регулярне тестування планів та незалежний аудит [19]. Водночас базовим критерієм має залишатися збалансоване забезпечення конфіденційності, цілісності й доступності інформації, оскільки надмірне обмеження доступу в умовах війни так само здатне перешкодити реалізації прав пацієнта, як і неналежне розкриття медичних даних. Вимоги до резервування, синхронізації та аварійного доступу повинні також узгоджуватися із Законом України «Про захист персональних даних», який передбачає захист персональних даних від випадкової втрати чи знищення, незаконної обробки й незаконного доступу [29].

Висновки. Проведене дослідження засвідчило, що цифрова інфраструктура системи охорони здоров'я України в умовах воєнного стану є одним із засобів підтримання її стійкості та безперервності функціонування. Вона зменшує залежність доступу до медичної інформації від конкретного місця її фізичного зберігання, підтримує електронні направлення й рецепти, телемедичну взаємодію, маршрутизацію пацієнтів та інформаційно-аналітичне забезпечення управління. Водночас цифрова інфраструктура не є самодостатньою гарантією безперервності: її функціонування залежить від фізичної інфраструктури, енергопостачання, електронних комунікацій, кадрового забезпечення та кібербезпеки.

Запропоновано визначати цифрову інфраструктуру системи охорони здоров'я як комплексний об'єкт адміністративно-правового регулювання, ширший за ЕСОЗ, що охоплює центральну базу даних, електронні медичні інформаційні системи, реєстри, телемедичні сервіси, засоби електронної ідентифікації, електронні комунікації, хмарні й резервні обчислювальні ресурси, стандарти інтероперабельності, засоби кіберзахисту та процедури відновлення. Таке розуміння відповідає меті дослідження й дає змогу оцінювати не окремий сервіс, а здатність сукупності взаємопов'язаних цифрових компонентів підтримувати юридично значущі процеси у сфері охорони здоров'я.

Обґрунтовано доцільність нормативного закріплення мінімальних секторальних вимог до архітектурної відмовостійкості, операційної безперервності, кіберстійкості, інтероперабельності, переносимості даних та інституційної підзвітності. Такі вимоги мають передбачати географічне резервування копій даних, альтернативні канали електронних комунікацій, автономні режими або режими роботи з обмеженою функціональністю, плани безперервності й аварійного відновлення, визначення RTO та RPO, регулярне

тестування, аудит і дотримання вимог щодо захисту персональних даних. Їх доцільно інтегрувати до чинного регулювання функціонування ЕСОЗ і секторальних вимог у сфері охорони здоров'я, а під час подальшої адаптації законодавства враховувати підходи NIS2 та EHDS.

Перспективи подальших досліджень полягають у розробленні ризик-орієнтованої методики категоризації цифрових медичних сервісів за критичністю, визначенні диференційованих показників відновлення для різних видів медичної та реабілітаційної допомоги, а також правових моделей безпечного транскордонного обміну електронними даними про здоров'я.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тривас відновлення медичної інфраструктури, пошкодженої внаслідок російських атак / Міністерство охорони здоров'я України. 2026. 06 липня. URL : <https://moz.gov.ua/uk/trivaye-vidnovlennya-medichnoyi-infrastrukturi-poshkodzheno-yi-vnaslidok-rosijskih-atak>
2. 3 000 attacks on health care in Ukraine verified by WHO since full-scale invasion / World Health Organization. 2026. 08 травня. URL : <https://www.who.int/europe/news/item/08-05-2026-3000-attacks-on-health-care-in-ukraine-verified-by-who-since-full-scale-invasion>
3. В ЕСОЗ кількість електронних медичних записів сягнула понад 5 млрд / Електронна система охорони здоров'я : вебсайт. 2026. 09 квітня. URL : <https://ehealth.gov.ua/2026/04/09/v-esoz-kilkist-elektronnyh-medychnyh-zapysiv-syagnula-ponad-5-mlrd/>
4. Korobtsova N. Electronic health care system (e-Health): implementation mechanism and stages of development. *Problems of Legality*. 2021. Issue 154. P. 117–126. DOI : <https://doi.org/10.21564/2414-990X.154.236921>
5. Геглюк О. М. Нормативно-правове забезпечення цифровізації як пріоритетного напрямку реформування системи охорони здоров'я. *Актуальні проблеми держави і права*. 2022. Вип. 96. С. 36–43. DOI : <https://doi.org/10.32782/apdp.v96.2022.3>
6. Музика-Стефанчук О. А., Стефанчук М. О., Якимчук Н. Я. Система охорони здоров'я в умовах цифровізації та реформування фінансування. *Аналітично-порівняльне правознавство*. 2023. № 5. С. 359–365. DOI : <https://doi.org/10.24144/2788-6018.2023.05.64>
7. Malakhov K. S. Insight into the Digital Health System of Ukraine (eHealth): Trends, Definitions, Standards, and Legislative Revisions. *International Journal of Telerehabilitation*. 2023. Vol. 15, No. 2. Article e6599. DOI : <https://doi.org/10.5195/ijt.2023.6599>
8. Булеца С. Б., Менджул М. В., Калько А. І. Цифровізація права на медичну допомогу: порівняльний аспект. *Аналітично-порівняльне правознавство*. 2024. № 1. С. 356–360. DOI : <https://doi.org/10.24144/2788-6018.2024.01.63>
9. Батрин О. В., Теремецький В. І., Івахненко О. А. Правові гарантії доступності медичної та реабілітаційної допомоги в період дії воєнного стану. *Ірпінський юридичний часопис*. 2024. Вип. 2 (15). С. 46–58. DOI : [https://doi.org/10.33244/2617-4154-2\(15\)-2024-46-58](https://doi.org/10.33244/2617-4154-2(15)-2024-46-58)

10. Habicht J., Hellowell M., Kutzin J. Sustaining progress towards universal health coverage amidst a full-scale war: learning from Ukraine. *Health Policy and Planning*. 2024. Vol. 39, No. 7. P. 799–802. DOI : <https://doi.org/10.1093/heapol/czae041>
11. Вальчук М. С. Цифровізація сфери охорони здоров'я в Україні на шляху до забезпечення клієнто- та пацієнтоорієнтованості. *Центральноукраїнський вісник права та публічного управління*. 2024. № 3. С. 14–22. DOI : <https://doi.org/10.32782/cuj-2024-3-2>
12. Narayan A., Petryk M., Savchuk S. et al. TeleHelp Ukraine: A distributed international telemedicine response to the ongoing war. *Journal of Global Health*. 2024. Vol. 14. Article 04158. DOI : <https://doi.org/10.7189/jogh.14.04158>
13. Aleksandrenko H., Shevchenko M., Chervak O. Digital health intervention reconnects war-affected people living with HIV to healthcare: Ukraine case study. *Oxford Open Digital Health*. 2025. Vol. 3. Article oqaf001. DOI : <https://doi.org/10.1093/oodh/oqaf001>
14. Сидорук А. В. Державна політика цифровізації охорони здоров'я: адміністративно-правові засади розвитку медичних інформаційних технологій і використання штучного інтелекту. *Київський часопис права*. 2026. № 2. С. 143–151. DOI : <https://doi.org/10.32782/klj/2026.2.20>
15. Правове регулювання медичного туризму в Україні як чинника резильєнтності та повоєнного відновлення : монографія / В. І. Теремецький, А. О. Подзіров, Б. О. Логвиненко, С. Й. Литвин ; за наук. ред. В. І. Теремецького. Київ : НДІ ППіП ім. акад. Ф. Г. Бурчака НАПрН України, 2026. 253 с. DOI : <https://doi.org/10.71404/law-medtour-ua>
16. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX / Верховна Рада України. URL : <https://zakon.rada.gov.ua/go/1882-20>
17. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII / Верховна Рада України. URL : <https://zakon.rada.gov.ua/go/2163-19>
18. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII / Верховна Рада України. URL : <https://zakon.rada.gov.ua/go/2801-12>
19. Деякі питання електронної системи охорони здоров'я : постанова Кабінету Міністрів України від 25.04.2018 № 411 / Кабінет Міністрів України. URL : <https://zakon.rada.gov.ua/go/411-2018-%D0%BF>
20. Про внесення змін до деяких законодавчих актів України щодо функціонування телемедицини : Закон України від 09.08.2023 № 3301-IX / Верховна Рада України. URL : <https://zakon.rada.gov.ua/go/3301-20>
21. Про затвердження Порядку надання медичної та/або реабілітаційної допомоги із застосуванням телемедицини на період дії воєнного стану в Україні або окремих її місцевостях : наказ Міністерства охорони здоров'я України від 17.09.2022 № 1695. URL : <https://zakon.rada.gov.ua/go/z1155-22>
22. Про схвалення Стратегії розбудови телемедицини в Україні : розпорядження Кабінету Міністрів України від 14.07.2023 № 625-р / Кабінет Міністрів України. URL : <https://zakon.rada.gov.ua/go/625-2023-%D1%80>

23. Про схвалення Стратегії розвитку системи охорони здоров'я на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках : розпорядження Кабінету Міністрів України від 17.01.2025 № 34-р / Кабінет Міністрів України. URL : <https://zakon.rada.gov.ua/go/34-2025-%D1%80>

24. Увага: окремі медичні інформаційні системи відключено від ЦБД ЕСОЗ / Електронна система охорони здоров'я : вебсайт. 2026. 01 січня. URL : <https://ehealth.gov.ua/2026/06/01/uvaga-okremi-medychni-informatsijni-systemy-vidklyucheno-vid-tsbd-esoz/>

25. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape: Health Sector (January 2021 to March 2023). 2023. 36 p. DOI : <https://doi.org/10.2824/163953>

26. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152. URL : <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

27. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. *Official Journal of the European Union*. 2025/327. 05.03.2025. URL : <https://eur-lex.europa.eu/eli/reg/2025/327/oj>

28. Про хмарні послуги : Закон України від 17.02.2022 № 2075-IX / Верховна Рада України. URL : <https://zakon.rada.gov.ua/go/2075-20>

29. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI / Верховна Рада України. URL : <https://zakon.rada.gov.ua/go/2297-17>

Дата надходження 05.08.2026

Дата прийняття після рецензування 11.08.2026

Дата рекомендації 27.08.2026

Дата публікації 30.09.2026