Чорноморський національний університет імені Петра Могили
(повне найменування вищого навчального закладу)

Навчально-науковий інститут публічного управління та адміністрування
(повне найменування інституту, назва факультету (відділення))

кафедра публічного управління та адміністрування
(повна назва кафедри (предметної, циклової комісії))

«Допущено до захисту»
Завідувач кафедри публічного
управління та адміністрування,
д. політ.н., професор
_____ О. Н. Євтушенко
“____” _____20___року

КВАЛІФІКАЦІЙНА РОБОТА
на здобуття ступеня вищої освіти

магістр
(ступінь вищої освіти)

на тему: **ЕТИКА УПРАВЛІННЯ ДАНИМИ В СИСТЕМІ ОХОРОНИ ЗДОРОВ’Я: ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ**

Керівник: ст. викладач
Верба Світлана Миколаївна
(вчене звання, науковий ступінь, П.І.Б.)

Рецензент: д. н. держ. упр., професор
Андріяш Вікторія Іванівна
(посада, вчене звання, науковий ступінь, П.І.Б.)

Виконав: студент VI курсу групи 639МЗ
Педаченко Юрій Євгенович
(П.І.Б.)

Спеціальності: 281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

ОПП: «Публічне управління закладами охорони здоров’я»

Миколаїв – 2024 рік

ЗМІСТ

ВСТУП

Актуальність та постановка проблеми. Сучасний розвиток інформаційних технологій у медицині докорінно змінює способи збирання, обробки та зберігання медичних даних. Завдяки цифровим технологіям медична інформація стала значно доступнішою, що полегшує її використання для досліджень, розробки інноваційних методів лікування та оптимізації роботи медичних установ. Однак, разом із цим зростає низка нових викликів, зокрема в контексті забезпечення етичності управління такими даними.

Одним із найбільш критичних аспектів є проблема конфіденційності та безпеки медичних даних. Пацієнти довіряють свої медичні дані лікарям і установам, очікуючи, що ці дані будуть належним чином захищені. Але поширення цифрових систем зберігання інформації створює додаткові ризики зловживання чи несанкціонованого доступу до цієї інформації. Нещодавні кіберзагрози та витоки персональних даних у медичній сфері як в Україні, так і за кордоном показали, наскільки вразливою є система, і якою важливою стає побудова ефективних етичних та правових механізмів захисту.

Цифрова трансформація охорони здоров’я також викликає необхідність вирішення питань щодо згоди пацієнтів на використання їх даних. Якщо раніше інформація була доступною лише вузькому колу фахівців, то тепер, завдяки цифровим технологіям, вона може бути використана у значно ширших масштабах, зокрема у наукових дослідженнях, обміні між медичними закладами, страховими компаніями або навіть приватними організаціями. Це викликає питання щодо дотримань прав пацієнтів на приватність і необхідності отримання інформованої згоди на використання їх даних.

Окрім того, слід зазначити, що на сучасному етапі цифрові технології відкривають широкі можливості для розвитку нових підходів у медицині, таких як телемедицина, дистанційний моніторинг здоров’я та використання великих даних для аналізу і прогнозуванню захворювань. Ці процеси

потребують чітких етичних рамок, щоб забезпечити відповідальне використання технологій і мінімізувати ризики для пацієнтів. Зокрема, питання постають щодо того, як повинні бути обмежені права доступу до медичних даних і яким чином можна ефективно контролювати використання таких даних для забезпечення прозорості та відповідальності.

Нарешті, актуальність дослідження також визначається потребою у вдосконаленні нормативно-правової бази управління медичними даними в Україні. Незважаючи на численні міжнародні практики та рекомендації поки що не всі аспекти етики в управлінні медичними даними в умовах цифрової трансформації враховані. Впровадження сучасних підходів до управління медичними даними та забезпечення їх захисту вимагає не лише технічних інновацій, а й правових змін, що дозволить належним чином регулювати питання етики та безпеки у цій сфері.

Дослідженням правового забезпечення етики медичних даних займаються велика кількість науковців, серед яких можна виділити таких дослідників та авторів: Л. Антонова, І. Берн, Т. Езер, О. Деміхов, І. Діордіца, О. Кабанов, Дж. Коен, Л. Козлова, Г. Миронова, А. Мусієнко, В. Мусієнко, Дж. Оверал, Б. Островська, І. Пономаренко, І. Сенюта – всі вони, займаються питаннями гармонізації українського законодавства відповідно до міжнародних стандартів, досліджують етичні та правові аспекти впровадження цифровізації в систему охорони здоров’я.

Також варто відзначити таких, як Г. Кассел (США), який вивчає питання конфіденційності медичних даних в умовах телемедицини та електронних медичних записів, А. Квінн (Канада), яка досліджує інформовану згоду пацієнтів у контексті цифрових технологій, Е. Коцц (Німеччина), який досліджує аспекти кібербезпеки у медичних установах, зокрема ризики незаконного доступу до медичних записів, Л. Савоньї (Італія), яка розглядає правові питання захисту даних відповідно до регламенту GDPR, Л. Тейлор (Великобританія), що акцентує увагу на етичних аспектах прозорості управління даними та багато інших.

Мета дослідження – проаналізувати етичні аспекти управління медичними даними в умовах цифрової трансформації системи охорони здоров'я та розробити рекомендації щодо вдосконалення нормативно-правового регулювання в цій сфері.

Для досягнення цієї мети були поставлені такі завдання:

– проаналізувати класифікацію медичних даних та їх функціональну значущість у системі охорони здоров'я;

– розглянути основні етичні засади управління медичною інформацією та їх застосування;

– оцінити вплив діджиталізації на управління медичними даними;

– визначити етичні ризики, які виникають в умовах цифрової трансформації;

– провести аналіз чинного нормативно-правового регулювання етики управління медичними даними в Україні;

– розробити рекомендації щодо вдосконалення правової бази у сфері етичного управління медичними даними.

Об'єктом дослідження є процес управління медичними даними в системі охорони здоров'я.

Предметом дослідження є етичні аспекти управління медичними даними в умовах цифрової трансформації.

Методи дослідження. У процесі роботи були використані загальнонаукові методи: аналіз та синтез для вивчення існуючих підходів до управління медичними даними, порівняння – для оцінки міжнародного досвіду, а також методи правового аналізу для вивчення нормативно-правових актів. Статичні методи дозволили оцінити вплив цифрових технологій на управління даними, а метод SWOT-аналізу застосовувався для розробки рекомендацій.

Наукова новизна одержаних результатів полягає в тому, що було проведено комплексне дослідження етичних аспектів управління медичними

даними в умовах цифрової трансформації охорони здоров’я, що дозволило виявити ключові проблеми та запропонувати шляхи їх вирішення.

Практичне значення одержаних результатів. Розроблені рекомендацій щодо вдосконалення етичного управління медичними даними можуть бути використані для підвищення ефективності функціонування системи охорони здоров’я. Впровадження цих етапів розвитку сприятиме підвищенню рівня захисту прав пацієнтів та забезпеченню безпеки медичних даних у цифрову епоху.

Апробація результатів дослідження. За результатами дослідження автором було підготовано та опубліковано тези для XXVII Всеукраїнської щорічної науково-практичної конференції «Могилянські читання – 2024: досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти» на тему «Управління медичними даними: виклики цифрової трансформації».

Структура роботи зумовлена її метою та завданнями і складається зі вступу, трьох розділів, шести підрозділів, списку використаних джерел (80 найменувань). Загальний обсяг роботи становить 85 сторінок, з яких 75 основного тексту.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ЕТИКИ ТА УПРАВЛІННЯ ДАНИМИ В ОХОРОНІ ЗДОРОВ'Я

1.1. Класифікація медичних даних та їх функціональна значущість у системі охорони здоров'я

Медичні дані є однією з найважливіших складових системи охорони здоров'я, забезпечуючи можливість ефективної діагностики, лікування та профілактики захворювань. За визначенням фахового медичного словника, «медичні дані охоплюють будь-яку інформацію, що стосується фізичного або психічного стану пацієнта, наданих медичних послуг, а також результати лабораторних досліджень, історії захворювань, медичних процедур та інших аспектів медичної допомоги» [33, с. 35].

Згідно із законодавством України, медичні дані включають інформацію про стан здоров'я пацієнта, результати лікування, медичні висновки та рекомендації лікарів. Стаття 39 Конституції України визначає, що «кожен громадянин має право на захист своїх медичних даних та їх конфіденційність». Водночас, закон України «Про захист персональних даних» №2297-VI від 01.06.2010, деталізує порядок збору, зберігання та використання медичної інформації, зокрема з урахуванням електронних медичних систем [48].

Науковці визначають медичні дані як «інформаційні ресурси, що відображають динаміку стану здоров'я населення», або як «засоби забезпечення об'єктивної картини перебігу захворювання та наданих медичних послуг». Л. Тейлор, акцентує увагу на клінічних даних, вважаючи їх основою для розробки медичних стратегій, які базуються на фактичних результатах обстежень і діагностики. За його визначенням, «медичні дані є основою інформатизації охорони здоров'я і можуть бути використані для

підтримки клінічних рішень та оцінки якості медичних послуг». З правової точки зору, згідно з нормативно-правовими актами України, медичні дані є конфіденційною інформацією і повинні використовуватися лише за згодою пацієнта або на основі чинного законодавства. Розглянемо деякі дослідження науковців в цій галузі (табл. 1.1) [5, с. 24-29].

Таблиця 1.1

Дослідження вітчизняних та зарубіжних науковців щодо медичних даних

Науковець	**Внесок у тему дослідження**	**Основні праці та ідеї**
Андрій Коваленко (Україна)	Вивчення електронних медичних записів в Україні	Досліджує особливості впровадження електронних записів у вітчизняній медицині
Віктор Долинський (Україна)	Дослідження електронних медичних записів в Україні	Автор публікацій про переваги та недоліки електронних медичних систем в українських лікарнях
Гері Кассел (США)	Дослідження впровадження електронних медичних записів (EHR)	Працює над оптимізацією використання EHR у медичних закладах для покращення обслуговування пацієнтів
Деніел Мерз (Велика Британія)	Вивчення використання генетичних даних у охороні здоров’я	Автор робіт про застосування геноміки в персоналізованій медицині
Меріл Декстер (США)	Класифікація медичних даних у системах охорони здоров’я	Розробила методи покращення управління медичними даними в лікарнях
Михайло Кальчук (Україна)	Дослідження в галузі охорони здоров’я та управлінні медичними даними	Автор численних статей про оптимізацію медичних даних в Україні
Ольга Романюк (Україна)	Вплив медичних даних на якість лікування	Досліджує роль медичних даних у підвищенні якості надання медичних послуг в Україні
Судхір Раві (Індія)	Дослідження застосування великих даних у медицині	Працює над впровадженням аналітики даних у клінічній практиці для покращення результатів лікування
Тетяна Мартиненко (Україна)	Вивчення етики в охороні здоров’я	Розробила рекомендації щодо етичних стандартів у медичних дослідженнях
Хейлі Джонсон (Австралія)	Дослідження конфіденційності даних у медичних системах	Спеціалізується на етичних аспектах використання медичних даних

Медичні дані мають достатньо різних класифікації, але загальною прийнято вважати таку, що формує основні типи за своєю природою, способом збору та використанням. Д. Горбатова виділяє три головні типи медичних

даних: персональні, клінічні та генетичні, кожен з яких відіграє унікальну роль у системі охорони здоров'я, що дозволяє ефективніше ними керувати, аналізувати і використовувати для медичних рішень (табл. 1.2) [9, с. 167].

Таблиця 1.2

Типологія медичних даних та їх значення для охорони здоров'я

Тип медичних даних	Зміст	Значення для охорони здоров'я
Персональні дані	Інформація, що стосується конкретної особи і включає її ідентифікаційні дані (ім'я, адреса, дата народження)	Ідентифікація пацієнта, персоналізація медичної допомоги для правильного встановлення діагнозу, надання допомоги та ведення електронної медичної документації
Клінічні дані	Відомості, що описують медичну історію пацієнта (діагнози, результати обстежень, лікування, рекомендації лікарів)	Розробка діагнозів, планів лікування та моніторинг здоров'я, що дозволяють приймати обґрунтовані рішення щодо подальшої медичної допомоги
Генетичні дані	Генетичний код, схильність до хвороб	Прогнозування ризиків, персоналізоване лікування, що дозволяє побудувати лікування на основі індивідуальних генетичних характеристик пацієнта

Медичні дані також можна класифікувати на структуровані та неструктуровані [9, с. 169]:

– структуровані дані – це стандартизована інформація, що зберігається в чітко визначених форматах, таких як електронні таблиці, бази даних або формати, придатні для автоматизованого аналізу (наприклад демографічні відомості про пацієнтів, результати діагностичних тестів і медичні звіти);

– неструктуровані дані – включають текстові документи, нотатки лікарів, медичні зображення та іншу інформацію, яку складніше аналізувати автоматизованими методами [9, с. 169].

Так, структуровані дані забезпечують можливість швидкого та точного аналізу завдяки стандартизованим форматам, що спрощує їх інтеграцію в електронні системи та використання в прийнятті рішень на основі доказових даних. Натомість неструктуровані дані, які становлять значний обсяг медичної інформації, вимагають більш складних методів обробки та аналізу.

Як зазначає Д. Курт, «медичні дані мають вирішальне значення для розвитку персоналізованої медицини», оскільки вони дозволяють аналізувати великий масив інформації для виявлення індивідуальних особливостей пацієнтів і розробки персоналізованих методів лікування. Крім того, сучасні підходи до обробки медичних даних, включаючи використання штучного інтелекту (ШІ), відкривають нові можливості для швидкої діагностики та прогнозування перебігу захворювань [70, с. 52].

Стандартизація медичних даних за допомогою загальновизнаних форматів, таких як ICD (International Classification of Diseases) або HL7 (Health Level 7), є ключовим інструментом у забезпеченні уніфікації інформації в медичних системах. ICD, який широко використовується для класифікації захворювань та інших медичних станів, дозволяє медичним установам стандартизувати діагностичну інформацію, що є критично важливим для надання узгодженої медичної допомоги і ведення медичних статистик. Стандарт HL7, з іншого боку, регулює обмін електронними медичними даними між різними системами, забезпечуючи їх сумісність та коректність. Впровадження цих стандартів значно полегшує передачу медичних записів між країнами, де використання систем могло бути перешкодою для забезпечення своєчасної допомоги пацієнтам [29, с. 258-260].

У загальному сенсі стандартизація медичних даних через ICD та HL7 сприяє поліпшенню якості медичної допомоги завдяки доступності структурованої і надійної інформації. Це також підвищує ефективність управління медичними ресурсами та сприяє проведенню аналітичних досліджень у сфері охорони здоров’я. Таким чином, ці стандарти є основою для формування єдиного інформаційного простору в медичній галузі, що забезпечує безперервність догляду за пацієнтами і полегшує їх результати лікування. Використання таких загальноприйнятих форматів дозволяє уникнути дублювання даних та забезпечує їх інтеграцію на національному і міжнародному рівнях [29, с. 262].

Важливим аспектом є те, що медичні дані не лише сприяють покращенню індивідуального лікування, але й відіграють роль у стратегічному управлінні медичними закладами. Наприклад, дані дозволяють відстежувати ефективність роботи установ, моніторити якість наданих послуг, виявляти недоліки у процесах і оптимізувати розподіл ресурсів. Це є актуальним для великих медичних інституцій і систем охорони здоров'я на національному рівні, які постійно стикаються з необхідністю оптимізації управлінських процесів [33, с. 47].

Використання медичних даних також стимулює розвиток медичних досліджень. Завдяки доступу до великої кількості даних, дослідники можуть проводити аналіз для виявлення нових закономірностей і кореляцій, що дозволяє розробляти нові методи лікування та медичні технології. М. Новіцькі зазначає, що «аналіз великих масивів даних є особливо корисним для розробки нових ліків та терапевтичних методів» [70, с. 91].

Особливу роль у сучасній системі охорони здоров'я відіграють електронні медичні дані (EMR – Electronic Medical Record), які є цифровими версіями паперових медичних записів. Вони містять всю медичну інформацію пацієнта, таку як історія захворювань, результати обстежень, діагнози та плани лікування. Впровадження електронних медичних даних значно підвищило ефективність охорони здоров'я, забезпечивши швидкий доступ до інформації, зменшивши адміністративне навантаження та підвищивши точність медичних рішень. За словами Т. Гребер, «електронні медичні записи сприяють інтеграції медичних послуг та полегшують доступ до інформації, необхідної для лікування» [76, с. 203].

Електронні медичні дані можуть бути класифіковані за кількома критеріями [10, с. 64-66]:

– електронна медична картка пацієнта (EMR) – це детальна інформація про пацієнта, його історію хвороби, проведені обстеження та призначене лікування. В Україні електронна медична картка є основою для надання

медичних послуг, однак рівень її впровадження поки що є недостатньо поширеним у порівнянні з іншими країнами;

– електронна медична історія (EHR) – це більш широкий набір медичних даних, який може включати інформацію про соціальний та демографічний статус пацієнта, історію хвороб, записи від кількох медичних установ. В Україні EHR тільки починають впроваджувати, тоді як у США, Німеччині, Великобританії – це вже стандартна практика;

– персоналізовані медичні дані (PHR) – це дані, які пацієнт може самостійно збирати, зберігати, зокрема інформація про здоров'я, отримана від лікарів або навіть з особистих медичних пристроїв;

– дані телемедицини – це інформація, що збирається під час віддалених консультацій та моніторингу пацієнтів через телемедичні системи, дуже допомогає пацієнтам, які живуть у віддалених регіонах;

– дані з медичних пристроїв і сенсорів – це дані, отримані від приладів, які моніторять стан здоров'я пацієнтів у режимі реального часу (наприклад, пристрої для вимірювання рівня глюкози, тиску тощо) [10, с. 64-66].

Д. Францвог підкреслює, що «електронні медичні записи є важливим елементом сучасної охорони здоров'я, що сприяє зниженню витрат та покращенню якості надання медичних послуг». Водночас впровадження електронних систем зберігання медичних даних вимагає суворого дотримання етичних і правових норм, особливо щодо конфіденційності пацієнтів [76, с. 207].

Важливою складовою аналізу електронних медичних даних є порівняння їх використання в Україні та за кордоном. У більшості розвинених країн електронні медичні дані є невід'ємною частиною національних систем охорони здоров'я. Наприклад, у США існує програма Meaningful Use, яка стимулює лікарні до впровадження електронних систем управління медичними даними. У Німеччині та Великобританії система EHR є обов'язковою, що дозволяє значно підвищити ефективність медичних послуг,

зокрема через швидкий доступ до даних, покращену комунікацію між лікарнями та пацієнтами [73, с. 560-561].

Впровадження таких систем в Україні лише тільки набирає обертів, що обумовлено як недоліками правового регулювання, так і відсутністю необхідною інфраструктури, належного фінансування і кваліфікованих кадрів. Однак з часом, розвиток електронних медичних даних дозволить покращити якість медичних послуг і зробити охорону здоров'я більш доступною та ефективною.

Медичні дані, особливо їх класифікація та правильне використання, є необхідною складовою для забезпечення якості медичних послуг. Вони є джерелом для прийняття рішень на всіх етапах лікування – від діагностики до реабілітації. В той же час, електронні медичні дані – їх структура, види та специфіка використання є важливим елементом для подальшої цифровізації охорони здоров'я як в Україні, так і у світі. Розвиток сучасних технологій дозволяє забезпечити більш ефективну діагностику, лікування та моніторинг стану здоров'я пацієнтів, зменшуючи при цьому адміністративні витрати і ризики помилок [30, с. 9].

Однією з основних тенденцій сучасної медицини є використання, так званих, великих даних (Big Data) для оптимізації медичних рішень та підвищення якості лікування. Великі дані охоплюють різні типи інформації, включаючи клінічні, геномні, біометричні та фінансові дані, які об'єднуються для створення комплексних моделей аналізу пацієнтів і прогнозування можливих результатів лікування (табл. 1.3) [68].

Таблиця 1.3

Модель використання Big Data у медицині

№	Етап	Завдання
1.	Збір даних	• клінічні дані (електронні медичні записи, лабораторні аналізи); • геномні дані (генетичне тестування, секвенування ДНК); • біометричні дані (носимі пристрої, медичні сенсори); • фінансові дані (страхові виплати, медичні витрати)

2.	Обробка даних	• інтеграція різних джерел; • стандартизація за допомогою загальновизнаних протоколів (ICD, HL7); • створення аналітичних моделей для аналізу даних
3.	Аналіз і прогнозування	• використання алгоритмів комп'ютерного навчання для прогнозування результатів лікування; • створення індивідуальних терапевтичних планів; • оцінка ефективності терапії на основі зібраних даних
4.	Використання результатів	• поліпшення клінічних рішень; • оптимізація ресурсів у системі охорони здоров'я; • зниження витрат та підвищення якості і доступності медичних послуг

Big Data також сприяють розвитку персоналізованої медицини, що полягає у застосуванні даних для створення індивідуальних терапевтичних планів на основі геномної інформації, фізіологічних даних і результатів аналізів. Згідно з сучасними дослідженнями, інноваційні технології обробки даних, такі як комп'ютерне навчання та штучний інтелект, дозволяють лікарям поліпшити планування лікувальних процесів, розроблювати індивідуальні терапевтичні підходи та моніторити якість медичних втручань [72].

Використання великих даних для медичних досліджень і практик поширене в багатьох країнах світу. У США великі медичні бази даних активно застосовуються для управління системою медичного страхування, досліджень у галузі охорони здоров'я, а також для розвитку персоналізованої медицини. У Європі великі дані використовуються для аналізу ефективності лікувальних заходів і оцінки здоров'я населення. Водночас питання захисту персональної інформації пацієнтів регулюються жорсткими нормативами, такими як GDPR (General Data Protection Regulation). Українська система охорони здоров'я також поступово впроваджує цифрові рішення та використання Big Data для контролю за результативністю лікування і управління ресурсами. Одним із найбільш перспективних напрямів наразі є розвиток електронних медичних карток, що спрощує доступ до історії хвороб пацієнтів та дає змогу покращити надання усіх необхідних медичних послуг [67; 75].

На основі проведеного аналізу можна стверджувати, що медичні дані мають суттєве значення для більш якісного управління охороною здоров'я.

Вони не лише сприяють прийняттю обґрунтованих рішень на всіх рівнях медичної системи, а й забезпечують можливість постійного моніторингу, аналізу та оптимізації медичних послуг. Типологія медичних даних, яка включає клінічні, адміністративні, фінансові і особисті дані пацієнтів, дозволяє охоплювати всі аспекти медичної діяльності, що сприяє підвищенню стандартів медичного обслуговування. Правове регулювання використання медичних даних та розвиток електронної системи охорони здоров'я є ключовими факторами у підвищення ефективності управлінських процесів, а також у гарантуванні захисту особистих даних пацієнтів.

1.2. Етичні засади управління медичною інформацією: концептуальний огляд та застосування

Етичні принципи в управлінні медичними даними є фундаментальними для забезпечення захисту прав пацієнтів, а також для підтримки належної якості медичних послуг. Використання медичних даних у сучасному світі регулюється чітко визначеними етичними засадами. Ці принципи охоплюють як міжнародні стандарти, так і національні нормативні акти, і, попри важливість їхнього дотримання, на практиці часто виникають проблеми, пов'язані із забезпеченням етичності використання медичних даних. У контексті цифрової трансформації ці принципи набувають ще більшого значення, оскільки електронні медичні записи та інші цифрові платформи створюють нові виклики щодо безпеки даних [28, с. 20].

Існує декілька підходів до класифікації етичних принципів, що застосовуються в медичних даних. Один із найпоширеніших підходів базується на таких основних елементах, як конфіденційність, інформована згода, забезпечення рівноправного доступу до медичних послуг, ідентифікація та анонімність даних і прозорість в управлінні даними. Розглянемо детальніше

основні етичні принципи, що сприяють безпечному та відповідальному управлінню медичними даними (табл. 1.4) [39, с. 40-53].

Таблиця 1.4

Основні етичні принципи та їх характеристики

Принцип	Опис	Застосовування
Конфіденційність	Захист персональної інформації від несанкціонованого доступу і розголошення	Правила доступу до медичних даних регулюються як на національному, так і на міжнародному рівні
Інформована згода	Добровільна згода пацієнта на обробку його медичних даних після отримання відповідної інформації	Кожен пацієнт повинен бути детально поінформований про те, як його дані будуть використовуватися
Рівний доступ	Забезпечення рівних прав усіх осіб на доступ до медичної допомоги	Відповідна політика розробляється на національному рівні
Ідентифікація та анонімність	Збереження ідентифікації осіб, або, навпаки, анонімність їх даних для захисту особистих даних	Анонімність особливо важлива в наукових дослідженнях
Прозорість	Забезпечення ясності та відкритості в обробці даних	Пацієнти повинні бути поінформовані про те, хто і як обробляє їх дані

Розкриття етичних засад зосереджується на їх ключових аспектах. Конфіденційність, як один із найважливіших принципів, вимагає забезпечення високого рівня захисту медичних даних від стороннього втручання. Згідно з дослідженням науковців, це питання стає критичним, коли дані передаються між різними системами. Інформована згода, за висновками І. Берна, є важливим елементом етики, оскільки пацієнт повинен розуміти, як саме будуть використані його дані. Однак існують і певні виклики, наприклад, при застосуванні інформованої згоди виникає питання достатнього інформування пацієнтів, особливо в умовах масової діджиталізації, де не всі розуміють складні технічні аспекти управління даними. Автори посібника зазначають, що «це стає серйозною проблемою, яка потребує створення простих та зрозумілих алгоритмів інформування пацієнтів» [4, с. 194-197].

Розглянувши більш детально, можна зосередити увагу на тому, що принцип захисту конфіденційності є центральним елементом етичного

управління медичними даними. Як зазначає доктор Дж. Андерсон, «конфіденційність є базовою етичною вимогою, яка охороняє приватність пацієнта та запобігає несанкціонованому доступу до його медичних даних. У сучасному цифровому світі ця вимога стає ще важливішою через ризики, пов’язані з хакерськими атаками та витоками даних. Електронні медичні записи мають бути захищені на всіх рівнях доступу за допомогою шифрування та авторизаційних механізмів, щоб забезпечити конфіденційність інформації. У системі охорони здоров’я для захисту електронних медичних записів зазвичай використовуються кілька ключових методів шифрування, зокрема [8]:

1) Advanced Encryption Standard (AES) – симетричне шифрування, яке забезпечує високий рівень безпеки та використовується для захисту даних як під час передачі, так і під час зберігання;

2) Transport Layer Security (TLS) – забезпечує захист під час передачі даних, часто використовується в телемедицині для безпечної комунікації;

3) Rives Shamir Adleman (RSA) – асиметричне шифрування, яке застосовується для безпечного обміну ключами між організаціями;

4) Hashing – забезпечує цілісність даних, важливе для автентифікації користувачів;

5) Elliptic Curve Cryptography (ECC) – підходить для мобільних додатків завдяки ефективності в умовах обмеження ресурсів, забезпечуючи високу безпеку [8].

Використання цих технологій в комплексі формує багатошарову систему безпеки, яка не лише захищає дані на різних етапах їх обробки, але й відповідає вимогам сучасних стандартів безпеки.

Дослідження Б. Островської вказує, що порушення конфіденційності можуть не лише нашкодити репутації медичних закладів, але й спричинити значні правові наслідки, такі як штрафи або судові позови. Особливо важливо це для електронних систем охорони здоров’я, оскільки вони надають ширший доступ до даних [39, с. 51].

Іншим, не менш важливим, принципом етичного управління медичними даними є інформована згода. Як зазначає науковиця Б. Островська, цей принцип забезпечує право пацієнта на свідоме і добровільне надання дозволу на обробку своїх даних. Сенс інформованої згоди полягає в тому, щоб пацієнти розуміли, як їх дані будуть використовуватися, хто матиме до них доступ, а також можливі ризики, пов'язані з обробкою інформації. Цей процес включає декілька важливих етапів [39, с. 46-47]:

– пояснення мети збору даних;

– детальний опис обробки та зберігання інформації;

– підтвердження розуміння пацієнтом своїх прав і можливостей відкликати згоду;

– обговорення потенційних ризиків і переваг від надання даних;

– надання інформації про осіб або організації, які матимуть доступ до даних;

– уточнення строку, на який надається згода, та умов її поновлення або анулювання;

– відповіді на запитання пацієнта для усунення будь-яких сумнівів щодо використання його інформації [39, с. 46-47].

В умовах цифровізації процес отримання інформованої згоди став більш складним. Оскільки цифрові платформи для збору даних потребують адаптації стандартних процедур отримання згоди пацієнтів. Це включає цифрові підписи, відео-інструкції або інтерактивні платформи, які дозволяють краще зрозуміти всі аспекти згоди.

Справедливість та рівний доступ до медичних даних постає принципом, який забезпечує, щоб всі пацієнти, незалежно від соціального, економічного чи етнічного статусу, мали рівний доступ до медичних послуг та інформації. Професорка Н. Дацій підкреслює, що в контексті цифровізації виникають нові виклики, пов'язані із забезпеченням рівного доступу до медичних даних, зокрема в країнах з нерозвиненою цифровою інфраструктурою [12].

Цифрові системи повинні бути розроблені таким чином, щоб уникнути дискримінації і сприяти інклюзивності. Це означає, що особи з обмеженими можливостями, люди, які живуть у віддалених районах, та меншини повинні мати рівні можливості для доступу до своїх медичних даних і участі у прийнятті рішень щодо свого здоров'я. Як приклад, можна навести електронні платформи, які пропонують багатомовну підтримку та інтерфейси, адаптовані до різних рівнів комп'ютерної грамотності (табл. 1.5) [57, с. 53-56].

Таблиця 1.5

Приклади інклюзивних електронних платформ у сфері охорони здоров'я

Країна	Назва платформи	Опис та особливості
Україна	eHealth	Електронна система охорони здоров'я, яка дозволяє пацієнтам отримувати рівний доступ до своїх медичних даних, записуватися на прийом до лікарів і переглядати історію хвороб. Платформа розроблена для покращення якості медичних послуг, сприяння збереженню конфіденційності та оптимізації процесів у системі охорони здоров'я. Має адаптації для різних рівнів цифрової грамотності
США	MyChart	Платформа, що дозволяє пацієнтам управляти своїми медичними записами, мати доступ до історії хвороб, результатів тестів та можливість комунікації з лікарями. Платформа підтримує різні мови і включає функції, які сприяють інклюзивності, зокрема адаптації для осіб з обмеженими можливостями. Вона є частиною екосистеми охорони здоров'я Epic Systems одного з провідних розробників медичних інформаційних систем у США
Канада	Lifelabs	Платформа, яка пропонує пацієнтам доступ до лабораторних тестів та медичних послуг через зручний інтерфейс. Має функції, які дозволяють користувачам легко знаходити та записуватися на аналізи, а також переглядати результати. Інтерфейс розроблений з урахуванням потреб різних користувачів, включаючи тих, хто може мати труднощі з використанням технологій
Великобританія	NHS App	Додаток для управління медичними послугами, що забезпечує доступ до медичних записів і можливість запису на прийом, має підтримку осіб з обмеженими можливостями. NHS App стала важливим інструментом для покращення доступності медичних послуг у Великобританії

Німеччина	TeleClinic	Платформа телемедицини, що дозволяє пацієнтам отримувати медичні консультації в режимі онлайн, з адаптованими функціями для людей з особливими потребами. Ця платформа також сприяє зменшенню фізичних бар'єрів у доступі до медичних послуг, особливо у віддалених районах
Австралія	HealthEngine	Платформа для запису на прийом до лікаря, що пропонує інтерфейси для осіб з обмеженими можливостями та користувачів з різним рівнем комп'ютерної грамотності

Щодо прозорості, то цей принцип означає, що пацієнти повинні знати, як і для яких цілей використовуються їх медичні дані. Це включає як обмін даними між лікарями та медичними закладами, так і їхнє використання у наукових дослідженнях. Однією з проблем у дотриманні цього принципу є складність відстеження даних у великих цифрових системах, де вони можуть бути використані без відома пацієнтів для комерційних або наукових цілей [60, с. 82].

Принцип відповідальності вимагає, щоб організації, які зберігають або обробляють медичні дані, забезпечували їх належний захист [78, с. 14-16]:

– в Україні цей принцип регулюється Законом «Про інформацію» №2657-XII від 02.10.1992 року, який передбачає відповідальність за порушення умов зберігання або обробки даних;

– у США принцип відповідальності регулюється Законом про переносимість і підзвітність медичної інформації (HIPAA), який передбачає жорсткі вимоги щодо захисту медичних даних та накладає великі штрафи на організації, які не виконують вимог безпеки, включаючи фінансові санкції у разі витоку даних;

– у Німеччині регулювання відбувається завдяки Загальному регламенту захисту даних (GDPR), який надає особам більше контролю над їх даними і накладає суворі вимоги на організації щодо їх обробки – у разі порушення GDPR організації можуть бути оштрафовані на значні суми, до 20 млн євро або 4 % від світового обороту;

– у Великобританії принцип регулюється Законом про захист даних 2018 року, який узгоджений з GDPR, він контролює як організації можуть обробляти особисті дані, включаючи медичні, порушення також можуть призвести до штрафів до 17 млн фунтів стерлінгів або 4 % від світового обороту;

– у Австралії регулювання принципу відбувається на основі Закону про захист приватності 1988 року, який встановлює правила для збору, використання та обробки особистих даних, у випадку недотримання законодавства можуть бути накладені штрафи [78, с. 14-16].

Принцип анонімізації також є одним із способів забезпечити конфіденційність, особливо в наукових дослідженнях або при обміні даними між медичними установами. GDPR вимагає, щоб усі персональні дані були або анонімізовані, або оброблялися таким чином, щоб ідентифікація пацієнта була неможливою. Однак проблема полягає в тому, що анонімізація може бути неповною або легко відворотною, що може призвести до незаконного розкриття інформації [12].

У контексті етики в медицині важливим є розуміння основних принципів, які регулюють взаємодію між медичними працівниками, пацієнтами та суспільством. Тому слід розглянути ще одну класифікацію, яку запропонував Б. Варкі у своїй статті, виокремивши чотири базові принципи, що стали основою для сучасної етичної практики у медичній сфері [78, с. 19]:

1) автономія – принцип, що захищає право пацієнтів приймати рішення про власне здоров’я і дані (передбачає обізнаність, згоду на використання медичних даних та повагу до особистих рішень пацієнта);

2) справедливість – принцип стосується рівного доступу до медичних послуг та даних, а також розподілу ресурсів з урахуванням потреб суспільства;

3) доброякісність (благодійність) – принцип, що закликає до дій в інтересах пацієнта, з акцентом на добробут і мінімізацію шкоди, особливо у використанні конфіденційних медичних даних;

4) ненасення шкоди – принцип вимагає від медичних працівників та організацій уникати дій, які можуть нашкодити пацієнтам, зокрема в аспектах приватності та безпеки даних [78, с. 19].

Варто також звернути увагу на етичні принципи використання медичних даних у вітчизняному просторі. В Україні існують різні нормативно-правові акти та стандарти, що в свою чергу виділяють певні етичні засади використання медичних даних. Одним з ключових нормативних актів є Закон України «Про захист персональних даних» №2297-VI від 01.06.2010 року, який передбачає [48]:

– законність обробки: медичні установи можуть збирати та використовувати дані лише з дозволу пацієнта або на законних підставах;

– цільова спрямованість: використання даних повинно відповідати конкретним цілям, вказаним під час їх збору;

– пропорційність: використання медичних даних повинно бути мінімальним і відповідати цілям для яких вони були зібрані [48].

Міжнародний стандарт, який використовується у системі охорони здоров'я України – ISO/IEA 27001 (Система управління інформаційною безпекою). Він регламентує безпеку інформаційних систем, включаючи ті, що обробляють медичні дані та визначає такі принципи, як конфіденційність, цілісність і доступність інформації, що є фундаментальними для захисту медичних даних [38].

У порівнянні з класифікацією Б. Варкі, українське законодавство більше акцентує увагу на правових аспектах використання медичних даних, тоді як міжнародні стандарти зосереджені на захисті інформаційної безпеки. Законодавство України визначає жорсткі вимоги до законності збору та обробки даних, тоді як у науковій класифікації підкреслюється моральний обов'язок медичних працівників і захист автономії.

Пацієнти повинні мати можливість вільно отримувати доступ до своїх медичних даних і використовувати їх для власних потреб, наприклад, для консультацій із лікарями або отримання іншої думки. Це право закріплено в

українському законодавстві, але на практиці його реалізація часто ускладнена через бюрократичні процедури або технічні перешкоди. Наукові дослідження також часто потребують доступу до великих масивів медичних даних. В Україні це питання регулюється етичними комітетами при медичних закладах, які контролюють, щоб дані використовувалися відповідно до етичних стандартів [59, с. 213]:

1) Національна комісія з питань біоетики при Кабінеті Міністрів України – розробляє етичні принципи для медичної практики та захисту прав пацієнтів, співпрацює з міжнародними організаціями;

2) Етичний комітет при Міністерстві охорони здоров'я України – розглядає етичні аспекти наукових досліджень і клінічних випробувань;

3) Локальні етичні комітети при медичних закладах – контролюють дотримання етичних стандартів у повсякденній медичній практиці [59, с. 213].

Принцип мінімізації даних є ще одним важливим етичним аспектом у сфері управління медичними даними. Він полягає у тому, що для будь-яких цілей – лікування, дослідження чи обробки інформації – має бути зібрано мінімально необхідну кількість даних, що дозволяє уникнути надмірного збору конфіденційної інформації. Важливість цього принципу зростає в умовах цифровізації, оскільки обробка великих обсягів даних допомогає знизити ризики, пов'язані з можливими витоками або неналежним використанням персональних даних пацієнтів, що в свою чергу сприяє дотриманню етичних стандартів у сфері охорони здоров'я [12].

Етичні аспекти, що виникають при збереженні та координації медичних даних, становлять суттєвий аспект у контексті управління інформацією в охороні здоров'я. З одного боку, лікарі та медичні установи потребують доступу до повних медичних даних для забезпечення якісного і точного лікування. З іншого боку, пацієнти можуть не бажати надавати абсолютний доступ до своїх даних, особливо якщо мова йде, наприклад, про таку особисту інформацію, як психічні розлади чи інфекційні захворювання. Ці дилеми створюють конфлікт між правом пацієнта на конфіденційність та

необхідністю медичного персоналу мати доступ до даних для дієвого лікування. Вирішення таких етичних суперечностей вимагає комплексного підходу, що включає правові норми, технологічні рішення і етичні засади, які враховуватимуть інтереси всіх сторін.

Регулювання використання та впровадження етичних принципів у сфері охорони здоров'я України відбувається на декількох рівнях – державному, регіональному і місцевому [40, с. 69-71]:

1) На державному рівні основну роль відіграють відповідні законодавчі акти, які встановлюють рамки для збору, обробки та використання медичних даних. На рівні державних органів, таких як Міністерство охорони здоров'я України, створюються нормативні документи і рекомендації щодо етики в медичній сфері. Ці документи включають етичні кодекси, методичні рекомендації та настанови, які деталізують, як саме слід впроваджувати етичні принципи на практиці. Міністерство також забезпечує моніторинг дотримання цих стандартів, контролюючи діяльність медичних установ через регулярні перевірки і аудит.

2) На регіональному рівні відповідальність за реалізацію етичних принципів мають обласні та міські органи охорони здоров'я. Вони розробляють регіональні програми, які враховують місцеві особливості і потреби населення, а також можуть ініціювати освітні кампанії для медичних працівників щодо важливості дотримання етичних норм. Взаємодія між місцевими органами влади та медичними установами є важливою для адаптації національних стандартів до конкретних умов.

3) На місцевому рівні, відповідальність покладається на медичні установи, такі як лікарні та клініки, де формуються внутрішні етичні комітети, які займаються питаннями дотримання етичних норм на практиці. Ці комітети можуть розглядати конкретні випадки, пов'язані із використанням медичних даних, і пропонувати рекомендації щодо їх етичного обґрунтування. Вони також можуть проводити тренінги для медичних працівників, щоб забезпечити підвищення рівня обізнаності про етичні питання [40, с. 69-71].

Крім того, важливу роль у регулюванні етичних принципів відіграють професійні асоціації та наукові товариства. Вони розробляють власні етичні кодекси, які стають основою для професійної етики в медичній практиці. Ці організації також можуть впливати на формування державної політики, лобіюючи зміни в законодавстві або сприяючи обговоренню етичних питань на рівні суспільства. Таким чином, регулювання етичних принципів в медицині є складним і багаторівневим процесом, що потребує активної співпраці між державними органами, медичними установами та професійними асоціаціями (рис. 1.1) [40, с. 73-74].

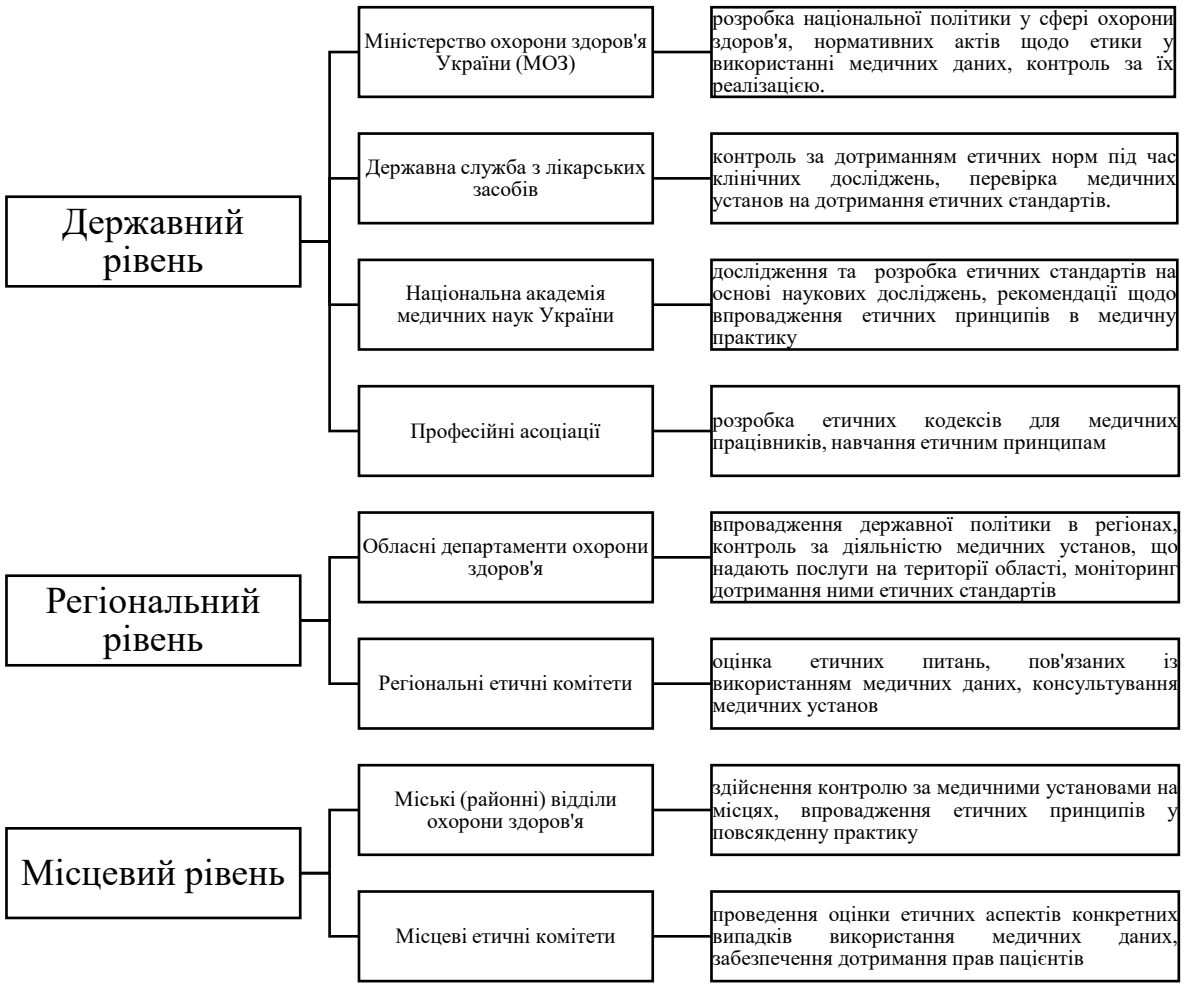


Рис. 1.1. Модель регулювання застосування етичних принципів у сфері охорони здоров’я

Використання етичних принципів в управлінні медичними даними може допомогти вирішувати певні труднощі, що з’являються внаслідок розвитку

сучасних інформаційних технологій та трансформації системи охорони здоров’я. Тому важливо, щоб в країні, на всіх рівнях, відбувалася збалансована робота, спрямована на впровадження етичних стандартів та забезпечення безпеки даних. Це включає не лише дотримання законодавчих норм, але й активне залучення усіх учасників системи охорони здоров’я, таких як медичні працівники, пацієнти і технологічні компанії, для спільного вирішення питань етики і кібербезпеки.

Таким чином важливо усвідомлювати, що реалізація етичних принципів є невід’ємною складовою ефективного функціонування охорони здоров’я в умовах цифровізації. Принципи конфіденційності, інформованої згоди та рівного доступу до медичних послуг не лише захищають права пацієнтів, але й сприяють формуванню довіри до медичних установ. Визначення та дотримання етичних стандартів у цій сфері є невід’ємним фактором для забезпечення справедливості та безпеки в обробці медичних даних. В умовах швидкого розвитку технологій, застосування цих принципів вимагає постійного моніторингу та адаптації до нових викликів, що виникають у процесі впровадження цифрових рішень у медичній сфері.

Висновок до Розділу 1

Проведене дослідження дозволяє зробити низку важливих висновків щодо управління медичними даними в контексті сучасних вимог до цифровізації та забезпечення етичних стандартів у сфері охорони здоров’я. Медичні дані, зважаючи на їхню унікальність та значущість, вимагають чітко визначених підходів до збору, зберігання і обробки, які повинні враховувати як специфіку самих даних, так і вимоги до забезпечення їх безпеки та конфіденційності. З огляду на значущість інформаційного ресурсу у сфері медицини, медичні дані є ключовим інструментом для прийняття стратегічних рішень в охороні здоров’я та підвищенні якості медичних послуг.

Аналіз існуючих підходів до класифікації медичних даних свідчить, що у сучасних умовах все більшої актуальності набуває питання інтеграції

медичної інформації в електронні системи і їх адаптація до міжнародних стандартів обробки та захисту даних. Це забезпечує зручний доступ до медичних даних, їх оперативний обмін і сприяє науково-дослідній діяльності у галузі медицини. Однак, це також вимагає глибокого перегляду етичних принципів, зокрема конфіденційності та згоди на обробку, оскільки цифрові технології суттєво змінюють традиційні підходи до управління даними пацієнтів.

Етичні принципи у сфері медичних даних, такі як: конфіденційність, інформована згода, забезпечення рівного доступу та анонімізація даних, потребують ретельної адаптації до умов цифровізації. Особливу роль відіграє принцип прозорості у взаємовідносинах між медичними установами та пацієнтами, який передбачає доступне і зрозуміле пояснення процесів обробки та зберігання даних. Забезпечення відповідальності та захисту персональної інформації є ключовим аспектом, що сприяє підвищенню довіри до системи охорони здоров’я загалом і цифрових медичних послуг зокрема.

Завдяки впровадженню цифрових технологій та телемедицини, Україна має змогу підвищити якість надання медичних послуг, створюючи єдині інтегровані системи для роботи з медичними даними. Однак, цей процес також потребує суттєвого вдосконалення нормативно-правової бази, адаптації міжнародних стандартів захисту інформації до національних умов. Особливо важливо враховувати досвід країн, які вже досягли високого рівня уніфікації та захисту медичних даних, що дозволяє забезпечити безпечний обмін інформацією між медичними установами.

Таким чином, управління медичними даними потребує комплексного підходу, який включає технічне вдосконалення електронних систем, забезпечення належного захисту інформації, а також дотримання етичних та правових стандартів. Це дозволить не лише оптимізувати управління медичною інформацією, але й підвищити рівень довіри пацієнтів до системи охорони здоров’я, стимулюючи розвиток телемедицини та інших інноваційних напрямів у медичній сфері.

РОЗДІЛ 2
ВИКЛИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В УПРАВЛІННІ МЕДИЧНИМИ ДАНИМИ

2.1. Вплив діджиталізації на управління медичними даними в охороні здоров'я

Цифрові технології кардинально змінюють підходи до управління медичними даними в системі охорони здоров'я, трансформуючи традиційні процеси обробки, зберігання та обміну інформацією. Упродовж останніх років спостерігається зростаючий інтерес до цифрових рішень, таких як електронні медичні записи, використання штучного інтелекту для аналізу даних і прогнозування, а також хмарні технології для централізованого зберігання інформації (табл. 2.1) [24, с. 62].

Таблиця 2.1

Основні технології в управлінні медичними даними

Технологія	Опис
Електронні медичні записи (ЕМЗ)	Заміна паперових карток пацієнтів на цифрові аналоги, що містять повну історію захворювань
Штучний інтелект (ШІ)	Аналіз великих обсягів даних для автоматизованого діагностування і прогнозування хвороб
Хмарні сервіси	Зберігання даних в захищених хмарних сервісах, що дозволяє лікарям отримувати доступ до інформації будь-де і будь-коли

Важливість цифровізації обумовлена не лише підвищенням ефективності роботи медичних установ, але й потребою адаптувати охорону здоров'я до нових соціальних викликів і потреб, пов'язаних із швидким зростанням обсягів даних та необхідністю забезпечення доступу до них у будь-який час. Як зазначає професорка Н. Діденко, «цифровізація здоров'я вимагає не тільки технологічних змін, але й перебудови управлінських процесів, оскільки впровадження інноваційних рішень передбачає зміну парадигм у

збиранні, обробці та зберіганні даних». Особливо важливо, щоб технології були не просто нововведенням, а інтегрованою частиною загальної стратегії управління даними в медичній сфері, яка забезпечить доступ до повної і актуальної інформації для прийняття клінічних та управлінських рішень [16, с. 149].

Сьогодні значна увага приділяється використанню електронних медичних записів, які стали основою сучасних систем охорони здоров'я багатьох країн світу, зокрема й України. Вони забезпечують повний і точний облік історії захворювань пацієнта, що дає змогу лікарям швидко оцінювати стан здоров'я, контролювати попередні діагнози та призначення, а також мінімізувати ймовірність помилок, пов'язаних із неточним введенням або повторним записом даних. За оцінками Міністерства охорони здоров'я України, електронізація медичних записів дозволила скоротити витрати на обслуговування паперових архівів і знизила кількість дубльованих записів майже на третину [32, с. 142].

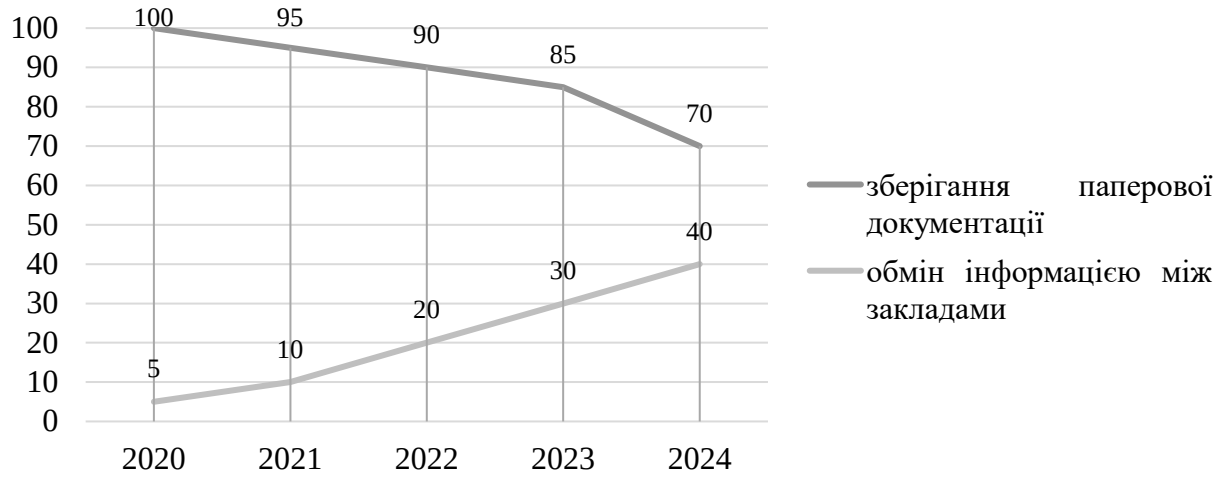
Крім електронних медичних записів, інновації в управлінні медичними даними охоплюють використання штучного інтелекту, який здатен аналізувати великі масиви даних, виявляти патерни та тенденції, а також прогнозувати ризики захворювань. За словами С. Козьякова, «впровадження алгоритмів штучного інтелекту може стати проривом у діагностиці захворювань, оскільки вони не тільки допомагають виявляти відхилення на ранніх стадіях, але й дозволяють швидко і точно оцінювати стан здоров'я пацієнтів у невідкладних випадках». Водночас такі технології вимагають серйозних інвестицій у розробку та навчання, а також надійної інфраструктури для забезпечення безпеки і конфіденційності даних [25].

Вплив цифровізації на ефективність управління медичними даними підтверджено численними дослідженнями, які показують, що автоматизовані системи знижують час обробки даних і полегшують адміністративні процеси. Наприклад, результати аналізу Національної служби здоров'я України (НСЗУ) демонструють, що завдяки впровадженню цифрових платформ обсяг

зберігання паперової документації знизився на 25 %, а обмін інформацією між закладами прискорився майже на 40 % (діаграма 2.1) [65, с. 423].

Діаграма 2.1

Аналіз НСЗУ щодо впровадження цифрових платформ у роботі медичних закладів



У дослідженнях, проведених Інститутом цифрових трансформацій Київського університету, вказано, що цифрові платформи дозволяють покращити процес прийняття рішень у медичних закладах, адже зростає прозорість інформаційного обміну.

Процес діджиталізації суттєво змінює процес обробки інформації, прискорюючи її передачу між різними медичними установами та витрати на її зберігання. Це не лише економить ресурси, але й оптимізує робочий процес, дозволяючи працівникам зосередитися на основних професійних завданнях. Як зазначають І. Корчинський та Н. Фірман, «цифрові технології надають можливість скоротити час обробки медичних даних, забезпечуючи оперативний доступ до інформації, що є критично важливою для ефективного прийняття рішень» [26, с. 104].

Проте цифрові зміни мають і певні складнощі. Однією з них є значні фінансові витрати на впровадження інноваційних технологій, особливо в державних установах, де бюджет часто обмежений. На думку науковиці Г. Давиденко, «успішна цифровізація вимагає комплексного підходу, який

включає не лише фінансування, але й правову підтримку та підвищення кібербезпеки медичних систем». Вона наголошує на важливості створення безпечного середовища для захисту даних пацієнтів, що сприятиме довірі до цифрових рішень серед населення. Крім того, технології потребують регулярного оновлення забезпечення їх ефективності, що може створювати додаткове навантаження на бюджет медичних установ [11, с. 37].

Адаптація медичного персоналу до нових систем також вимагає часу та навчання, особливо в регіонах, де досвід роботи з цифровими інструментами є обмеженим. У цьому контексті В. Жуковська у своїй статті підкреслює: «Без належної підготовки кадрів навіть найкращі технології не зможуть бути повноцінно інтегровані у систему охорони здоров’я. Навчання та адаптація лікарів до нових цифрових систем є не менш важливими, ніж технологічні оновлення». Її думка наголошує на тому, що саме людський фактор може стати як рушійною силою так і викликом для ефективної цифровізації [18, с. 14-15].

Наслідки цифровізації, як показує практика, позитивно впливає на якість медичного обслуговування. Пацієнти отримують швидший доступ до інформації про своє здоров’я, а прозорість у діяльності медичних установ сприяє підвищенню довіри до системи охорони здоров’я. Водночас цифровізація створює ризики, зокрема для кібербезпеки. Науковці Н. Костенок і А. Пєнкова, розглядаючи особливості розвитку інструментів цифрової трансформації системи охорони здоров’я в Україні, підкреслюють необхідність серйозних заходів захисту та шифрування для запобігання витоку конфіденційної інформації пацієнтів [27, с. 122].

Покращення точності та швидкості діагностики є ще одним важливим досягненням завдяки впровадженню цифрових технологій. Програми, засновані на алгоритмах штучного інтелекту, використовуються для аналізу медичних зображень, наприклад, рентгенівських і комп’ютерних томограм, що дозволяє автоматично ідентифікувати патології з високою точністю. На онлайн-конференції «Штучний інтелект у медицині», яка була організована Міністерством цифрової трансформації разом з Національним медичним

університетом імені О. О. Богомольця та університетами із Сінгапуру, було зазначено, що застосування штучного інтелекту у діагностиці допомогло зменшити час постановки діагнозу в середньому на 30 %, особливо в екстрених випадках. Також наголошено, що точність діагнозу може зростати завдяки вдосконаленню алгоритмів ШІ [62].

Програми цифровізації охорони здоров'я в Україні [11, с. 53-56]:

– система eHealth – єдина електронна система обліку медичних записів;

– впровадження стандартів ВООЗ для забезпечення сумісності з міжнародними системами охорони здоров'я;

– програми навчання медичних працівників для роботи з цифровими системами [11, с. 53-56].

Сучасні програми цифровізації в охороні здоров'я, такі як eHealth, що була ініційована Міністерством охорони здоров'я України та Національною службою здоров'я України, дозволяють не лише стандартизувати облік пацієнтів, а й створити єдину базу даних, доступну для лікарів усієї країни. Це дозволяє уникнути втрати медичної інформації та пришвидшує доступ до даних пацієнтів. У 2024 році НСЗУ звітувала, що близько 85 % державних медичних закладів підключені до системи eHealth, що дозволяє зберігати та обробляти інформацію про більш ніж 12 мільйонів пацієнтів. Науковець І. Шишка зазначає, що такі програми змінюють парадигму доступу до медичних даних, роблячи їх доступними в будь-який момент для усіх учасників медичного процесу [65, с. 418-419].

Національні програми цифровізації охорони здоров'я також включають активну інтеграцію міжнародних стандартів, таких як Health Level Seven International (HL7) та Fast Healthcare Interoperability Resources (FHIR), розроблених ВООЗ для забезпечення сумісності з іншими глобальними системами охорони здоров'я. Впровадження цих стандартів, дозволяє Україні приєднатися до світової медичної спільноти та забезпечити швидкий обмін даними з закордонними медичними центрами. Це критично важливо для

діагностики і лікування українців, що проходять лікування за кордоном, або потребують екстреної допомоги під час подорожей [23, с. 79; 74].

Один із важливих напрямів державної цифровізації – це підвищення грамотності медичного персоналу. Міністерство охорони здоров'я, у співпраці з українськими університетами та центрами підвищення кваліфікації, впроваджує освітні курси і тренінги для лікарів та медичного персоналу, що дозволяє їм освоїти навички роботи з цифровими системами. Державні програми включають також інтеграцію практичних курсів у медичні навчальні заклади і регулярні вебінари, організовані національними та міжнародними експертами. Це є важливою умовою для ефективного функціонування цифрових систем, оскільки навіть найкращі технологічні нововведення потребують кваліфікованого персоналу для їх використання [34].

У доповнення до державних ініціатив у сфері цифровізації, приватні медичні компанії також розробляють і впроваджують власні цифрові рішення для управління медичними даними. Наприклад, приватні клініки, такі як «Добробут» та «Медіком», розробляють власні медичні платформи, які дозволяють пацієнтам записуватися на прийом онлайн, отримувати доступ до медичних карток та результатів аналізів через особистий кабінет. Такі приватні платформи створюють зручність для пацієнтів і забезпечують їх бажання мати прямий доступ до своїх даних.

Також, українські IT-компанії, такі як «Helsi», у співпраці з приватними та державними медичними установами, розробили зручну платформу для пацієнтів, де можливо переглядати історію візитів до лікаря, записуватися на прийом до спеціалістів, замовляти лабораторні дослідження і отримувати результати аналізів. Це не лише підвищує рівень обслуговування пацієнтів, але й допомагає знизити навантаження на лікарів, автоматизуючи багато адміністративних процесів. Всі ці ініціативи цифровізації в Україні є багатовекторними та інтегрують зусилля як державних, так і приватних структур для забезпечення зручності, прозорості та доступності медичних даних [14, с. 84-85].

Аналізуючи різні дослідження можна закцентувати увагу на тому, що протягом 2024 року вплив цифрових технологій на управління медичними даними в Україні став більш значущим, продовжуючи сприяти [13, с. 75-76]:

– оптимізації процесів надання медичних послуг;
– розвитку пацієнт-орієнтованого підходу;
– розширенню цифрових сервісів для пацієнтів;
– зниженню витрат на медичне обслуговування через автоматизацію;
– зміцненню національної безпеки завдяки захисту медичних даних [13, с. 75-76].

Одним з ключових аспектів став розвиток єдиної Електронної системи охорони здоров'я (ЕСОЗ), яка дозволяє вести централізований облік медичних даних, зберігаючи їх на рівні державної бази, доступ до якої можуть отримати медичні працівники за згодою пацієнта. Такий підхід забезпечує доступність даних для лікарів по всій країні, що критично важливо в умовах децентралізованої системи охорони здоров'я [36].

Серед реальних прикладів нових ініціатив у рамках цифровізації медичної системи – впровадження особистих кабінетів пацієнтів – це стало можливим завдяки програмі ZDOROVI, яка активно обговорювалася на eHealth Summit 2024. На цьому саміті міністр цифрової трансформації Михайло Федоров підкреслив стратегічну важливість таких технологій не тільки для модернізації, але і для ефективного функціонування медичної системи під час війни.

Також важливим напрямом стало розширення функціоналу медичних інформаційних систем (МІС), які підключені до централізованої Єдиної електронної системи охорони здоров'я та забезпечують автоматизацію адміністративних і логістичних процесів у лікарнях. А. Пироженко, експерт у галузі цифрових систем охорони здоров'я, зазначив, що МІС вже надають комплексні рішення для звітності, логістики, бухгалтерського обліку та управління запасами лікарських засобів, що дозволяє значно зменшити

навантаження на медичних працівників і підвищити ефективність роботи медичних установ [80].

Нині основними стратегічними напрямами цифровізації, відповідно до національної стратегії Міністерства охорони здоров'я, є впровадження реєстрів, які дозволяють [79]:

1) ефективно керувати пацієнтами з хронічними захворюваннями;
2) моніторити випадки захворювань у реальному часі;
3) здійснювати комплексний контроль за доступом до лікування;
4) підвищувати точність діагности через обробку великих обсягів медичних даних;
5) забезпечувати швидкий доступ до історії хвороби для медичних працівників у різних закладах охорони здоров'я [79].

Варто зазначити, що в Україні активно розвиваються партнерства між державним і приватним секторами, а також із міжнародними організаціями, що сприяють впровадженню інновацій у сфері медичних даних. Одним із прикладів є ініціатива Програми розвитку ООН (UNDP) у співпраці з урядом Канади, яка забезпечила Центр громадського здоров'я України сучасним комп'ютерним обладнанням та ліцензованим програмним забезпечення. Ця програма націлена на забезпечення своєчасного доступу до якісних даних для покращення медичного обслуговування, особливо для вразливих категорій населення [55].

Важливу роль у цифровізації охорони здоров'я також відіграє використання блокчейн-технологій для забезпечення прозорості та безпеки обробки медичних даних. Дослідження, проведене Київським національним університетом, показало, що блокчейн може використовуватися для створення незмінних записів про медичні процедури, що підвищує рівень довіри до медичних закладів [66, с. 158].

Одним із основних елементів, який забезпечує ефективне управління медичною інформацією, покращуючи якість послуг і знижуючи ризики є маркування даних. У сучасних системах охорони здоров'я зростаюча

залежність від електронних медичних карток та автоматизованих систем збору даних потребує чітких і стандартизованих підходів до систематизації даних. Відповідно, маркування даних охоплює процеси ідентифікації, класифікації та структуризації інформації, що надає можливість медичним працівникам швидко та точно виконувати свої функції.

Головне застосування маркування даних відбувається саме у електронній документації, де маркування забезпечує унікальну ідентифікацію медичних записів. Це важливо не тільки для швидкого доступу до даних, але й для запобігання помилкам у лікуванні та діагностиці [31].

Кодування є ще одним важливим аспектом маркування даних, адже воно дозволяє систематизувати медичну інформацію відповідно до міжнародних стандартів. Використання кодів, таких як ICD (Міжнародна класифікація хвороб) і CPT (Актуальна термінологія процедур), допомагає стандартизувати інформацію про захворювання та лікувальні процедури [77].

Ефективність маркування даних має значний вплив на якість медичних послуг, а також може сприяти ефективному збору статистичної інформації, що необхідна для досліджень і планування в галузі охорони здоров’я. Наявність якісно маркованих даних дозволяє проводити аналіз епідеміологічних тенденцій, що є необхідним для розробки нових лікувальних стратегій і політик охорони здоров’я [3].

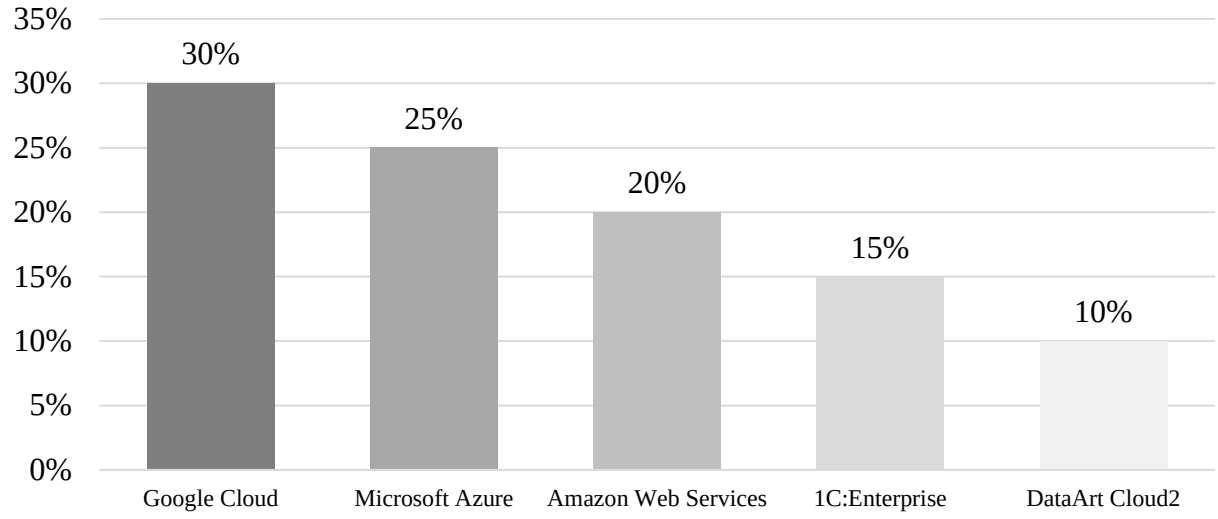
Хмарні технології в медицині є ще одним цінним нововведенням цифровізації, що продовжує набирати популярності, відкриваючи нові можливості для управління медичними даними, зберігання інформації та взаємодії між медичними працівниками. Вони дозволяють медичним установам отримувати доступ до ресурсів без необхідності великих витрат на інфраструктуру. Однією з ключових переваг хмарних технологій є їх гнучкість. Вони дозволяють медичним установам адаптувати свої ресурси відповідно до потреб у різні періоди часу.

Впровадження хмарних технологій також полегшує обмін інформацією між медичними установами. З використанням електронних медичних записів

у хмарах медичні працівники можуть швидко отримувати доступ до історії хвороб пацієнтів, що сприяє більш швидкому прийняттю рішень. Згідно з дослідженнями, близько 70 % медичних закладів, які використовують хмарні рішення, поліпшили обмін даними та зменшили час на пошук інформації (діаграма 2.2) [21, с. 221].

Діаграма 2.2

Хмарні середовища, які часто використовують медичні заклади в Україні



Не менш важливою є роль хмарних технологій у забезпеченні безпеки медичних даних. У світі, де загроза кібератак постійно зростає, хмарні системи можуть забезпечити більш високий рівень безпеки порівняно з локальними. Науковець І. Кириченко зазначає, що «сучасні хмарні рішення використовують шифрування та багаторівневу автентифікацію, що суттєво знижує ризик витоку інформації» [21, с. 222].

У контексті аналітики даних, хмарні технології пропонують потужні інструменти для обробки великих обсягів інформації. Вони дозволяють проводити складні аналітичні процедури, виявляючи тенденції в даних, які можуть бути використанні для покращення медичних послуг. За словами Р. Сета, «аналітика на базі хмари стає основним інструментом для дослідження та прогнозування медичних потреб населення» [69].

Проте, впровадження хмарних технологій у медицину пов’язане з певними викликами. Необхідність дотримання законодавчих вимог і етичних норм поєднаних із захистом персональних даних, є важливою проблемою. Інакше кажучи, медичні установи повинні забезпечити не лише захист даних, але й транспарентність у їх використанні, щоб зберегти довіру пацієнтів.

З метою кращого розуміння поточного стану хмарних технологій у медицині слід систематизувати переваги та недоліки їх впровадження (табл. 2.2) [1].

Таблиця 2.2

Основні переваги та недоліки впровадження хмарних технологій у систему охорони здоров’я

Переваги	Недоліки
– гнучкість ресурсів: хмарні технології дозволяють масштабувати ресурси відповідно до потреб, що особливо важливо в умовах змінюваного попиту на медичні послуги	– залежність від Інтернет-з’єднання: відсутність стабільного Інтернет-з’єднання може ускладнити доступ до критично важливих даних, що може негативно вплинути на медичні рішення
– поліпшення обміну інформацією: електронні медичні записи, доступні в хмарі, покращують координацію між фахівцями та пришвидшують прийняття рішень	– проблема з конфіденційністю: хоча хмарні технології мають системи безпеки, існує ризик витоку персональних даних, особливо в умовах кібератак
– високий рівень безпеки даних: сучасні хмарні платформи застосовують шифрування та інші технології для захисту даних	– проблеми з інтеграцією: впровадження хмарних технологій може потребувати значних зусиль для інтеграції з існуючими системами
– доступ до аналітики даних: хмара дозволяє виконувати складні аналітичні процеси для покращення медичних послуг	– витрати на навчання: медичні працівники можуть потребувати додаткового навчання для ефективного використання нових технологій
– зниження витрат на інфраструктуру: використання хмарних технологій допомагає знизити витрати на підтримку та оновлення обладнання	– регуляторні виклики: необхідність дотримання законодавчих норм може бути складною для медичних установ

Отже хмарні технології в медицині пропонують значні переваги для управління медичними даними, забезпечуючи кращу координацію, безпеку і доступність. Проте для їх успішної адаптації необхідно вирішити низку викликів, зокрема забезпечити відповідність законодавчим нормам і навчити

медичних працівників новим технологіям. Таким чином, хмарні середовища стають важливим компонентом сучасної системи охорони здоров’я та одними з головних чинників впливу цифрових технологій на управління медичними даними, здатними значно покращити якість медичних послуг.

З урахуванням вищезазначеного аналізу, можна стверджувати що цифрова трансформація в управлінні медичними даними в Україні, станом на 2024 рік, суттєво впливає на ефективність медичних послуг, водночас створюючи нові етичні виклики. Важливим є те, що успішна реалізація цифрових технологій вимагає не лише інноваційних рішень, але й чіткого дотримання етичних принципів, які регулюють обробку медичних даних. Це підкреслює необхідність розробки та впровадження ефективних механізмів контролю та управління, що допоможуть забезпечити відповідність етичним стандартам у контексті цифровізації охорони здоров’я.

2.2. Етичні ризики та загрози, що виникають в умовах цифрової трансформації

Процес цифрової трансформації медичних даних зумовлює появу великої кількості етичних ризиків та загроз, які охоплюють комплексну сукупність питань, пов’язаних із захистом прав пацієнтів і безпекою інформації. В умовах стрімкого розвитку технологій та автоматизації процесів охорони здоров’я зростає необхідність виявлення й управління етичними ризиками, таким як [14, с. 86]:

- порушення конфіденційності через кіберзагрози;
- проблеми коректності медичних даних;
- ризики дискримінації та нерівності доступу до цифрових послуг;
- питання відповідальності за роботу алгоритмів штучного інтелекту;
- складнощі з отриманням інформованої згоди [14, с. 86].

Кожна з цих загроз має свої специфічні особливості і вимагає розробки належних регуляторних і технічних заходів для зменшення потенційних ризиків (табл. 2.3) [73, с. 564-567].

Таблиця 2.3

Види загроз та ризиків у медичній сфері та приклади їх вирішення

Етичний ризик/загроза	**Особливості**	**Регуляторні заходи**	**Технічні заходи**
Конфіденційність та ризик витоку даних	Поширеність кіберзагроз, зокрема хакерські атаки на медичні установи	Введення стандартів захисту даних (GDPR), обов'язковий аудит безпеки	Використання шифрування даних, багатофакторна автентифікація
Надійність і коректність медичних даних	Помилки в автоматизованих системах збору даних, людський фактор	Розробка настанов щодо верифікації медичних записів	Впровадження автоматизованих систем контролю якості даних
Дискримінація та нерівність доступу	Обмежений доступ до медичних послуг у сільських районах	Політики рівного доступу до медичних послуг, підтримка сільських установ	Створення телемедичних платформ, медичних додатків, розширення інфраструктури
Відповідальність за автоматизовані рішення	Невизначеність у розподілі відповідальності за помилки штучного інтелекту	Введення чітких норм щодо відповідальності за автоматизовані рішення	Розробка прозорих алгоритмів, ведення журналів рішень штучного інтелекту
Отримання згоди пацієнтів	Ускладнення в процесі інформування про використання даних	Вимоги до документування згоди пацієнтів, стандарти інформування	Використання електронних платформ для отримання і зберігання згоди
Регуляторні виклики	Відсутність адаптованих норм для нових технологій	Перегляд існуючих регуляцій, розробка нових стандартів	Залучення експертів для формування рекомендацій та адаптацій

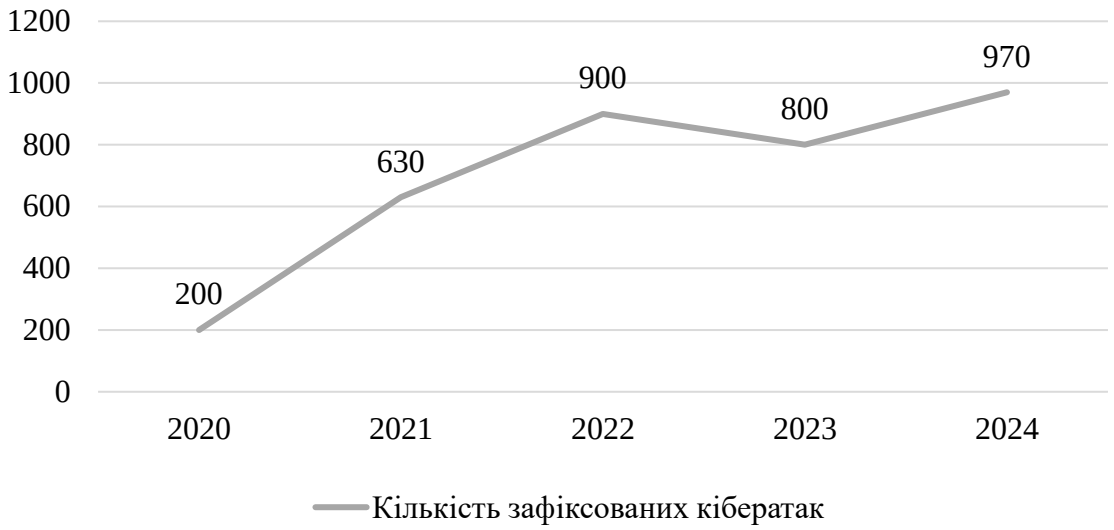
Ризики витоку даних набувають дедалі більшого значення, оскільки цифрові системи охорони здоров'я збирають і зберігають значні обсяги персональної інформації. Особливо гостро це питання постало після кібератаки вірусу Petya у 2017 році, яка завдала суттєвих збитків державним і приватним медичним закладам по всій Україні, тимчасово паралізувавши

роботу багатьох установ. Ця атака продемонструвала вразливість медичної інфраструктури та стала сигналом для перегляду систем безпеки даних [43].

Протягом останніх років Україна активізувала заходи з підвищення рівня кібербезпеки, однак експерти, зокрема Д. Шевченко, продовжують наголошувати на застарілості значної частини програмного забезпечення у медичних установах. На його думку, такі системи є особливо вразливими до новітніх загроз через відсутність своєчасних оновлень та належного захисту, що сприяє більшій частоті інцидентів витоку даних (діаграма 2.3) [56].

Діаграма 2.3

Ретроспектива кібератак на медичні заклади за період 2020-2024 рр.



Серед основних наслідків для системи охорони здоров’я України були зафіксовані: витоки даних пацієнтів; зупинка роботи медичних систем; підробка медичних даних; системні збої в лікарнях. Для їх вирішення Міністерством охорони здоров’я України спільно з різними державними, приватними структурами, а також міжнародними партнерами було вжито ряд заходів, серед яких [22]:

1) впровадження нових стандартів кібербезпеки;
2) створення централізованих систем реагування;
3) навчання персоналу з кібербезпеки;

4) інвестування у новітні технології захисту [22].

Згідно з даними Державної служби спеціального зв'язку та захисту інформації України, кількість кібератак на медичні установи у 2022 році зросла на понад 30 % порівняно з 2021 роком, а загалом у 2023 році було зафіксовано понад 800 випадків порушень безпеки, пов'язаних із викраденням або знищенням особистих даних пацієнтів. Це вимагає впровадження новітніх засобів захисту та розробки стандартів кібербезпеки, що відповідають сучасним загрозам. Прикладом використання таких технологій є Threat Intelligence, що дозволяє вчасно ідентифікувати потенційні атаки [41].

Мобільні додатки для збору та моніторингу стану здоров'я стають невід'ємною частиною діджиталізації медичної системи, однак вони також несуть значні ризики для збереження конфіденційності. На відміну від стаціонарних медичних систем, які часто мають багаторівневий захист і відповідність стандартам безпеки, мобільні додатки нерідко залишаються поза сферою регуляції, що значно підвищує їхню вразливість до кіберзагроз. Так, за даними Національного комітету з питань кібербезпеки України, у 2024 році відбулося понад 2 тисячі випадків витоку даних через мобільні додатки для здоров'я, 60 % цих витоків було спричинено недоліками в алгоритмах шифрування даних або неправомірним використанням персональної інформації користувачів. Наприклад, деякі додатки зчитують геолокацію користувачів навіть у тих випадках, коли ця інформація не є необхідною для надання послуг, що створює ризики порушення приватності [58, с. 23-24].

Ці ризики також викликає відсутність уніфікованих стандартів безпеки для мобільних додатків. Український експерт з кібербезпеки Д. Іванченко, наголошує, що «забезпечення безпеки мобільних додатків має стати пріоритетом, оскільки користувачі часто не підозрюють про те, що їх дані можуть бути доступні третім сторонам». Як результат, цифрова трансформація у сфері охорони здоров'я несе не тільки значні можливості, а й нові виклики, що вимагають термінових регуляторних заходів [58, с. 26].

Ще одним аспектом етичних ризиків, пов’язаних із впровадженням цифрових технологій, є відсутність належної регуляції для обробки великих даних у медичній сфері. У сучасних медичних інформаційних системах обробка великих обсягів даних є необхідністю, однак зберігання та обробка таких даних нерідко відбувається без належного контролю. В Україні наразі немає чітких настанов щодо того, як саме повинні і можуть зберігатися дані, і як має здійснюватися їх обробка. За даними Міністерства цифрової трансформації України, у 2022-2023 роках виявлено понад 500 випадків незаконної обробки персональних даних у медичних установах, зокрема через недостатнє знання працівниками основних принципів роботи з великими даними та їх захисту. Це створює ситуацію, коли ця інформація може використовуватися для вторинного аналізу без згоди пацієнтів, що прямо порушує принцип інформованої згоди [67].

У той же час, одним із найбільших викликів залишається людський фактор, оскільки часто витоки даних стаються через помилки персоналу або невиконання правил кібербезпеки. Хоча технічні заходи і є важливими, але найбільша загроза може виникати саме через недостатній рівень підвищення кваліфікації персоналу, особливо в умовах швидкої діджиталізації. Він підкреслює, що «розвиток компетентностей у сфері кібергігієни та регулярне навчання персоналу є необхідними для забезпечення належного захисту особистих даних» [56].

Надійність і достовірність медичних даних є наступним основним етичним викликом цифрових змін. Проблеми з коректністю даних можуть виникати як через людські помилки, так і через технічні збої, оскільки, автоматизовані системи збору та внесення інформації не завжди працюють бездоганно. Дослідження проведене Міністерством цифрової трансформації України у 2023 році, показало, що майже 18 % зібраних автоматично медичних даних містило помилки, що потребували подальшої перевірки та корекції. Це створює додаткове навантаження на медичний персонал, адже навіть невеликі неточності можуть призвести до неправильного діагнозу чи лікування.

Зокрема, С. Квітка та М. Миргородська, наголошують на важливості впровадження стандартів перевірки даних на всіх етапах їх обробки, що дозволило б значно знизити ризики для пацієнтів [20, с. 18].

Значним етичним питанням також є дискримінація та нерівність доступу до цифрових медичних послуг, які особливо відчутні у сільських регіонах. Відповідно до статистики МОЗ України, станом на 2024 рік близько 30 % медичних закладів у віддалених населених пунктах досі мають проблеми з доступом до стабільного Інтернету, що ускладнює використання електронних медичних записів і доступ до дистанційної консультації лікарів (діаграма 2.4) [65, с. 420].

Діаграма 2.4

Рівень доступності до цифрових медичних послуг

Це створює значні бар’єри для пацієнтів, особливо літніх людей та підриває принцип рівності. Програми розвитку інфраструктури, такі як «Доступ до медицини для кожного», ініційовані державою, покликані забезпечити ширший доступ до цифрових послуг, але все ще вимагають значних зусиль і ресурсів [65, с. 421].

Іншою складною проблемою є питання відповідальності у разі використання автоматизованих рішень, що часто застосовуються для лікування. Системи штучного інтелекту, які аналізують симптоми та надають рекомендації, можуть помилятися через неточності алгоритмів або недостатню інформацію в базах даних. У 2023 році було виявлено, що найбільш точні алгоритми мають похибку близько 3 %, що може бути

критичним для здоров’я пацієнтів. На основі цього виникає необхідність розробки чітких механізмів відповідальності, а також створенні незалежного контролю для перевірки точності та безпеки автоматизованих рішень у медичні сфері, зокрема самим лікарем, задля зменшення ймовірних помилок при діагностиці стану пацієнтів [25].

Одержання інформованої згоди на обробку медичних даних ускладнюється з впровадженням діджиталізації. Процес згоди став менш зрозумілим для багатьох пацієнтів, які часто не повністю розуміють, як саме будуть оброблятися їх дані, особливо в умовах автоматичного збору інформації. Відповідно до дослідження Національної служби здоров’я України, понад 43 % респондентів у 2024 році вказали, що не мали достатньої інформації про те, як використовуватимуться їх медичні дані, що може призвести до ризиків неправомірного використання особистої інформації. Юристи, зазначають, що необхідно розробити прості й доступні механізми для пояснення пацієнтам процесу обробку даних, а також забезпечити можливість відмови від цієї функції, якщо це не є критично важливим для надання медичних послуг [42].

Щодо регуляторних викликів у сфері цифрової медицини, то вони також залишаються актуальними, через те, що законодавство України ще не повною мірою адаптоване до сучасних вимог цифровізації. Чинні нормативні акти, хоча і регулюють основні аспекти, але все одно не враховують всієї специфіки обробки великих обсягів цифрових даних, особливо в системі охорони здоров’я. Представники Міністерства цифрової трансформації України у своїх доповідях підкреслюють нагальну потребу в оновленні нормативної бази, щоб охопити всі етичні аспекти та захист безпеки у цифровому середовищі [20, с. 14].

Під час повномасштабного вторгнення Росії в Україні з’явилися нові етичні ризики, пов’язані із медичною сферою, які ускладнюють вже існуючі проблеми. Однією з найбільш критичних загроз стала нестабільність інформаційних систем внаслідок атак на медичні установи. Військові дії

підвищили ймовірність кіберзлочинів, таких як, злом медичних баз даних. На думку фахівців з кібербезпеки, цей фактор став каталізатором для подальшого посилення ризиків витоку особистих даних у медичних установах, що значно ускладнює забезпечення конфіденційності.

Додатково, в умовах війни зросли виклики, які стосуються доступу до медичних послуг, особливо у віддалених районах. Це стало складно також, через значну кількість прифронтових та окупованих територій, де ця складність є гостро відчутною. Експерти вказують на те, що наявність інфраструктури для телемедицини у селах і малих містах є надзвичайно важливою, але війна призвела до ще більшої цифрової нерівності, оскільки багато лікарень не мають можливості, ані фінансової, ані технологічної, реалізувати такі сервіси [6].

Окрім цього, зростання стресу та травм, викликаних війною, вплинуло на психічне здоров’я населення. Нестача ресурсів і підтримки призводить до того, що пацієнти не отримують необхідної медичної допомоги, що в свою чергу загострює етичні аспекти, пов’язані з реалізацією права на отримання лікування у період війни. Психологи та соціальні працівники підкреслюють, що в таких умовах важливо зосередитися на створенні безпечного простору для пацієнтів, що потребують психічної підтримки [7].

Необхідність у мобільних медичних командах також стала нагальною потребою. У випадку, якщо лікарні не можуть забезпечити доступ до лікування в умовах бойових дій, медичні працівники повинні бути готовими працювати на місцях, що підвищує ризики відносно надання невідкладної допомоги. Це створює відповідні виклики для медичного персоналу, які повинні вміти діяти у стресових ситуаціях, одночасно забезпечуючи високий рівень етики у своїй роботі.

Не менш важливою є роль міжнародної допомоги в покращенні етичних стандартів у медичній сфері. Організації, які надають гуманітарну допомогу, зазвичай пропонують нові моделі для впровадження етичних принципів в умовах кризових ситуацій [6]:

– модель допомоги на основі потреб – орієнтована на найбільш уразливі групи населення, що потребують термінової медичної допомоги;

– міждисциплінарні команди – залучення спеціалістів з різних галузей для комплексного підходу до вирішення медичних та етичних потреб;

– навчання медичних працівників – проведення тренінгів і семінарів для лікарів і медичного персоналу з етичних аспектів роботи в кризових умовах;

– моніторинг та оцінка – впровадження механізмів для постійного контролю за дотриманням етичних стандартів у наданні медичних послуг;

– адаптивне реагування – створення гнучких механізмів для швидкого реагування на зміни в медичних потребах під час криз, що дозволяє ефективніше розподіляти ресурси і забезпечувати доступ до лікування;

– біоетичний консорціум – створення міжнародних мереж з обміну досвідом щодо етичних принципів у медичній сфері [6].

У контексті повномасштабного вторгнення Росії в Україну, виклики у сфері охорони здоров’я зумовили необхідність запровадження нових стратегій для подолання етичних ризиків та загроз, пов’язаних з медичною інформацією і доступом до медичних послуг. Відповідні дії впроваджуються державними та приватними установами, а також спеціалізованими комітетами, які активно співпрацюють над забезпеченням безпеки даних і поліпшенням умов надання медичної допомоги [71].

Одним із основних шляхів боротьби з кіберзагрозами в медичних закладах стало впровадження програм кібербезпеки. Міністерство охорони здоров’я України спільно з Міністерство цифрових технологій України розробило спеціальні курси для медичних працівників, яких навчають основам захисту інформації та вмілому реагуванню на кіберінциденти. Ці програми допомагають не лише у створенні належного рівня обізнаності серед медичного персоналу, але й формують культуру безпеки даних у державних та приватних установах системи охорони здоров’я.

Національні та регіональні комітети з кібербезпеки активно працюють над створенням безпечного середовища для медичних установ. Вони координують дії між закладами охорони здоров'я різних форм власності, а також забезпечують проведення регулярних аудитів систем безпеки. За словами одного з керівників регіонального комітету, «систематична перевірка медичних баз даних і електронних карток пацієнтів є запорукою збереження їх конфіденційності та безпеки» [20, с. 21].

Необхідно зазначити, що зростання стресу серед медичних працівників також стало предметом уваги державним установ. Для цього організовуються програми психологічної підтримки для медиків, які допомагають їм справлятися з емоційним навантаженням, пов'язаним з їхньою роботою в умовах війни. Експерти вважають, що психічне здоров'я медичних працівників є важливою складовою загальної ефективності системи охорони здоров'я [7].

Підсумовуючи вищезазначене можна стверджувати, що цифрова трансформація у сфері управління медичними даними суттєво змінює спосіб зберігання, обробки та доступу до медичної інформації, породжуючи значні етичні ризики, які потребують ретельного регулювання і контролю. Зокрема, виклики, пов'язані із захистом персональних даних пацієнтів, ризиками щодо точності та достовірності даних, зростанням потенціалу дискримінації та нерівного доступу, відповідальністю за рішення, прийняті на основі автоматизованих систем і труднощами у забезпеченні належної інформованої згоди, становлять ключові елементи сучасних загроз у цій галузі. Зазначено, що міжнародна допомога та співпраця між державними і приватними структурами може відігравати важливу роль у підвищенні етичних стандартів у медичній сфері, пропонуючи нові моделі для впровадження етичних принципів в умовах криз. Аналіз проблем вказує на необхідність комплексного підходу до забезпечення етичних засад в системі охорони здоров'я.

Висновок до Розділу 2

Розвиток цифрових технологій у медичному секторі зумовив значне переосмислення підходів до управління медичними даними. Поглиблений аналіз впливу цифрових рішень щодо збереження, обробки та використання медичної інформації засвідчує як позитивні зрушення, так і нові виклики. Відзначено, що впровадження електронних систем зберігання даних та автоматизованих систем аналізу сприяє оперативності, точності й узгодженості медичної допомоги. Проте стрімкий темп трансформацій викликає значне занепокоєння щодо безпеки даних, зокрема конфіденційності та цілісності інформації в умовах цифрових загроз.

Серед основних етичних ризиків, пов’язаних з цифровою трансформацією в управлінні медичними даними, виділено забезпечення безпеки персональних даних, точність цих даних, рівність доступу та виклики інформованої згоди. З одного боку, технології штучного інтелекту і автоматизованого прийняття рішень створюють перспективи для оптимізації медичних процесів, але з іншого – несуть ризик дискримінації та нерівності у доступі до послуг через можливу упередженість алгоритмів. Недосконалість законодавчого регулювання ускладнює забезпечення прозорості і відповідальності у використанні таких технологій, підкреслюючи необхідність удосконалення правових механізмів на державному рівні.

Ретроспективний аналіз ситуації в Україні з 2020 по 2024 рік демонструє тенденцію до поступового впровадження інноваційних рішень у сфері охорони здоров’я, проте водночас відображає низку проблем, пов’язаних з кібербезпекою та недостатньою готовністю інфраструктури до захисту великих об’ємів медичних даних. Ці фактори створюють підґрунтя для розробки національних стратегій захисту медичної інформації з урахування міжнародного досвіду і сучасних викликів цифровізації.

Зважаючи на все вищезазначене, нагальною стає потреба у розробці інтегрованих механізмів управління ризиками, що охоплюють технічні, етичні і правові аспекти. Запровадження програм підвищення кіберстійкості та

посилення державного контролю за дотриманням етичних норм у процесі обробки медичних даних сприятиме побудові стійкої цифрової екосистеми у сфері охорони здоров’я.

Поглиблене дослідження свідчить про те, що задля досягнення сталих результатів цифровізації в медичній сфері необхідно забезпечити належну підготовку фахівців з інформаційної безпеки та етики. Лише інтеграція кваліфікованих кадрів і високих стандартів захисту даних дозволить зменшити ризики витоку та неправомірного використання медичної інформації. Крім того, важливим завданням залишається формування культури відповідального використання цифрових інструментів серед медичних працівників і управлінців.

Загалом висновки розділу підкреслюють важливість адаптації української системи охорони здоров’я до швидкоплинних цифрових змін на основі національних пріоритетів та міжнародного досвіду. Вдосконалення механізмів управління і регулювання медичних даних у цифровому середовищі є стратегічним завданням, яке вимагає системного підходу та скоординованих дій на всіх рівнях. Лише так можна забезпечити безпечне, етичне і ефективне використання медичних даних на благо суспільства.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ НОРМАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЕТИКИ УПРАВЛІННЯ ДАНИМИ В МЕДИЧНІЙ СФЕРІ

3.1. Аналіз чинного нормативно-правового регулювання медичними даними в Україні

У контексті дослідження правової бази, що регулює медичні дані в Україні, важливим аспектом є управління, обробка, зберігання та захист цієї інформації. Медичні дані містять інформацію про стан здоров’я, діагнози, лікування, а також інші відомості, що стосуються індивідуальних характеристик пацієнта. Такі дані мають підвищену цінність не лише для медичної науки, але й для соціальної сфери, оскільки їх витік або неналежне використання може завдати шкоди приватності та безпеці осіб. З огляду на це, система регулювання медичних даних в Україні повинна відповідати як внутрішнім вимогам захисту інформації, так і міжнародним стандартам у цій галузі [35, с. 18].

Для кращого розуміння регуляторного середовища в Україні, що стосується захисту медичних даних та прав пацієнтів, необхідно звернути увагу на основні законодавчі акти, які визначають правову базу у системі охорони здоров’я України. Вони встановлюють не лише основні принципи і процедури, а й деталізовані обов’язки для всіх учасників процесу. Ретельне дотримання цих документів дозволяє запобігти витокам інформації та забезпечує високий рівень конфіденційності, що особливо важливо в медичній сфері. До того ж, нормативні акти приводять у відповідність українське законодавство відповідно до міжнародних стандартів, що підвищує довіру громадян до системи охорони здоров’я. Вони сприяють злагодженій роботі

медичних установ і забезпечують захист прав пацієнтів на всіх етапах надання медичних послуг (табл. 3.1) [17, с. 144-145].

Таблиця 3.1

Основні законодавчі акти України щодо регулювання медичних даних

Назва законодавчого акту	Опис
Закон України «Про інформацію» № 2657-XII від 02.10.1992	Регламентує доступ громадян до різних видів інформації та визначає заходи щодо її захисту
Закон України «Основи законодавства України про охорону здоров'я» № 2801-XII від 19.11.1992	Встановлює загальні засади функціонування системи охорони здоров'я та визначає права й обов'язки медичних працівників і пацієнтів
Постанова Кабінету Міністрів України «Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»» № 208 від 24.02.2003	Окреслює заходи щодо розробки та впровадження електронного урядування в Україні
Наказ МОЗ України «Про затвердження Концепції галузевої програми «Електронна система реєстрації та обміну медичною інформацією між закладами, установами і організаціями охорони здоров'я»» № 409 від 25.07.2008	Концепція, що визначає стратегію створення системи для реєстрації та обміну медичною інформацією між закладами охорони здоров'я
Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010	Встановлює основні правила захисту та обробки персональних даних громадян
Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017	Регламентує основні принципи кіберпростору України
Закон України «Про підвищення доступності та якості медичного обслуговування у сільській місцевості» № 2206-VIII від 14.11.2017	Зосереджений на покращенні медичного обслуговування у сільських районах
Постанова КМУ «Деякі питання електронної системи охорони здоров'я» № 411 від 25.04.2018	Описує заходи з впровадження електронної системи обліку у сфері охорони здоров'я
Розпорядження КМУ «Про схвалення Концепції розвитку електронної охорони здоров'я» № 1671-р від 28.12.2020	Приймає концепцію розвитку технологічних інструментів для охорони здоров'я
Наказ МОЗ України «Про затвердження Порядку надання медичної та/або реабілітаційної допомоги із застосуванням телемедицини на період дії воєнного стану в Україні або окремих її місцевостях» № 1695 від 17.09.2022	Визначає правила надання медичної та реабілітаційної допомоги з використанням телемедицини під час воєнного стану

Огляд нормативно-правової бази, що регулює управління медичними даними в Україні, логічно розпочати із Закону України «Про інформацію» № 2657-XII, ухваленого ще в 1992 році. Цей акт заклав основи національної інформаційної політики та визначив ключові засади доступу, зберігання і захисту інформації різних типів, включаючи й медичну. Закон формує нормативну основну для контролю конфіденційності інформації, що має приватний або державний характер. Науковці зазначають, що на ранніх етапах розвитку інформаційного права в Україні Закон «Про інформацію» виконував функції базового документа, який заклав фундамент для подальшого удосконалення законодавства у сфері інформаційної безпеки [50].

Наступним важливим документом, що вплинув на функціонування медичної системи в Україні, є Закон «Основи законодавства України про охорону здоров'я» № 2801-XII від 19.11.1992 року, який встановив правові засади для діяльності медичних установ, визначив основні принципи роботи медичних працівників і закріпив права пацієнтів. Цей документ акцентує увагу на необхідності захисту інформації, що стосується стану здоров'я громадян, забезпечуючи приватність даних і обмежуючи доступ до них сторонніх осіб [37].

Подальший розвиток правових норм, спрямованих на захист медичної інформації, відбувся з прийняттям у 2003 році Кабінетом Міністрів України Постанови № 208, яка розпочала впровадження електронного урядування в Україні. Нормативний акт підкреслював необхідність розробки інформаційних систем, які повинні відповідати стандартам захисту та конфіденційності. Це створило підґрунтя для подальшого розвитку електронних медичних систем і поступового переходу на цифровий облік медичних даних. Наукові дослідження, зокрема О. Головченко, наголошують на важливості цього етапу, зазначаючи, що «перехід до електронного урядування в Україні створив передумови для якісного оновлення сфери медичного обліку», проте постанова також вимагала значного доопрацювання для належного захисту медичних даних [49].

Впродовж наступних п’яти років державою активно розроблялися подальші дії щодо законодавчого регулювання розвитку електронної медичної системи. Як результат у 2008 році Наказом МОЗ України № 409 було затверджено концепцію створення системи реєстрації та обміну медичною інформацією між закладами охорони здоров’я. Було вперше офіційно визначено необхідність єдиного медичного інформаційного простору, що дозволило б медичним установам обмінюватися інформацією ефективно і безпечно [46].

Розробка правових механізмів захисту персональних даних досягла важливого етапу у 2010 році з ухваленням Закону України «Про захист персональних даних» № 2297-VI. Закон встановив ключові положення захисту конфіденційної інформації, зокрема, щодо її обробки та зберігання, яка може ідентифікувати особу. В. Ігнатенко вказує у своїй монографії, «Закон спрямований на встановлення єдиних правил для захисту персональних даних, і це є критичним елементом у забезпеченні прав пацієнтів у медичній сфері» [48].

Подальші зміни у сфері захисту медичних даних відбулися після прийняття Закону «Про основні засади забезпечення кібербезпеки України» № 2163-VIII у 2017 році. Він визначає засади кібербезпеки в Україні та запроваджує заходи для захисту інформаційних систем, зокрема, у сфері охорони здоров’я. Закон акцентує увагу на захисті від кіберзагроз, що стає особливо актуальним у зв’язку зі збільшенням кількості кіберзлочинів, пов’язаних із викраденням медичних даних [51].

Закон «Про підвищення доступності та якості медичного обслуговування у сільській місцевості» № 2206-VIII в тому ж 2017 році, зосереджений на покращенні медичного обслуговування у віддалених районах. У законі зазначено, що нові стандарти обслуговування також повинні відповідати вимогам конфіденційності, оскільки це дозволяє уникнути порушень приватності пацієнтів [52].

У 2018 році Постанова Кабінету Міністрів України № 411 продовжила впровадження діджиталізації у різних сферах держави, спрямувавши зусилля на підвищення ефективності державного управління та забезпечення доступу громадян до сучасних технологій. Цією Постановою було затверджено електронну систему охорони здоров'я, що запровадила принципи обробки медичних даних в електронному форматі та встановила стандарти безпеки [15].

Розпорядження КМУ № 1671-р від 28.12.2020 року про схвалення «Концепції розвитку електронної охорони здоров'я» ознаменувало новий етап в інтеграції цифрових технологій у медичну систему. Ця Концепція заклала стратегічний підхід до створення сучасної інформаційної інфраструктури, яка сприяла не лише оптимізації обробки медичних даних, але й безпеці самих пацієнтів. Також було охоплено питання обміну даними між медичними закладами, інтеграції з іншими державними реєстрами і передбачено використання електронних записів пацієнтів. При цьому особлива увага приділялась відповідності національним та міжнародним стандартам кібербезпеки, що, вважалося, допоможе мінімізувати ризики витоку даних або їх незаконного використання [54].

Цей нормативно-правовий акт також розглядає питання впровадження телемедицини, яка дає можливість отримувати медичні послуги на відстані, що стало особливо актуальним під час пандемії COVID-19, а в подальшому стане необхідною послугою в період повномасштабного вторгнення Росії в Україну у 2022 році. Враховуючи потенціал цієї технології для забезпечення медичної допомоги в складнодоступних або віддалених регіонах, Концепція передбачала поступову інтеграцію телемедичних послуг у загальну систему охорони здоров'я. Дослідження О. Лобортас підтверджують, що «впровадження телемедицини суттєво знизить навантаження на медичні заклади та забезпечить своєчасне надання медичної допомоги, навіть у критичних умовах» [64].

Існуюча правова система в Україні на своєму шляху стикається з труднощами щодо регулювання новітніх технологій, таких як телемедицина та обмін медичними даними на міжнародному рівні. Законодавство не завжди встигає реагувати на нові виклики, які виникають у процесі використання цифрових інструментів у медицині.

Так, подальший розвиток правового регулювання у сфері електронної медицини набув особливого значення у зв'язку з війною в Україні, Наказ МОЗ України № 1695 від 17 вересня 2022 року, який встановив порядок надання медичної та реабілітаційної допомоги із застосуванням телемедицини під час воєнного стану. Цей наказ визначає чіткі правила щодо використання телемедичних технологій для надання медичних послуг у зоні бойових дій або у віддалених районах, де фізичний доступ до медичних установ є обмеженим або небезпечним. Інакше кажучи, документ забезпечує правове підґрунтя для роботи медичних працівників у дистанційному режимі, а також захищає права пацієнтів на отримання якісної медичної допомоги навіть в умовах критичних ситуацій [47].

Незважаючи на наявність достатньої нормативної бази, існують значні виклики у сфері регулювання медичних даних. Одним із таких викликів є неповне узгодження українського законодавства з нормами Європейського Союзу, зокрема Загальним регламентом про захист даних (GDPR). Хоча Закон України «Про захист персональних даних» частково враховує положення цього Регламенту, але все ще відсутні чіткі механізми захисту, такі як зобов'язання повідомляти громадян про порушення конфіденційності їх даних, що є обов'язковим у країнах ЄС [19].

Актуальність цього питання зростає і з огляду на поширення цифрових технологій у медичній сфері та зростання обсягів персональних даних, що обробляються у медичних установах. Використання ж міжнародних стандартів у законодавстві України допоможе краще регулювати забезпечення захисту медичних даних. Оскільки ці стандарти включають [14, с. 81]:

– принцип прозорості (пацієнти мають знати, як і з якою метою використовуються їх дані);

– згода суб’єктів даних (пацієнти повинні давати явну згоду на обробку своїх медичних даних);

– право на доступ (пацієнти мають право отримувати доступ до своїх медичних даних та вимагати їх виправлення у разі необхідності);

– захист даних за замовчуванням (системи, що обробляють медичні дані, повинні бути налаштовані на максимальний рівень захисту) [14, с. 81].

З початком повномасштабного вторгнення Росії в Україну у 2022 році зросла потреба в посиленні захисту персональних даних через ризики, пов’язані з кіберзагрозами. У зв’язку з цим були прийняті нові заходи кібербезпеки, включаючи нову редакцію Закону України «Про електронну ідентифікацію та електронні довірчі послуги» № 2155-VIII від 01.01.2024, яка зобов’язала всі медичні установи забезпечувати багаторівневу автентифікацію та регулярні перевірки захисту систем. За словами голови Державної служби спеціального зв’язку А. Марущака, «ці нововведення є важливим кроком у забезпеченні національної безпеки та захисту медичних даних» [45].

Особливий акцент у сучасному законодавстві робиться на етику обробки даних. У 2024 році МОЗ України була запущена Національна програма етичного управління медичними даними, що передбачає розробку етичних рекомендацій для медичних установ. Керівниця Школи охорони здоров’я Національного університету Т. Юрочко зазначає, що «етичні норми мають стати основою для формування довіри пацієнтів у цифрову еру, а також забезпечити їх права на безпеку та конфіденційність» [61].

Еволюція регулювання медичних даних в Україні свідчить про поступовий перехід від традиційних моделей до цифрових. З переходом на електронні системи обліку медичних даних з’явилася потреба в розробці нових стандартів, що також зможуть забезпечувати належний захист даних.

Ця Програма покликана узгодити українське законодавство з існуючими міжнародними нормами. Згідно з планами, до 2026 року Україна має право

повністю адаптувати своє законодавство до європейських стандартів, що, безумовно вплине на якість забезпечення регулювання етичного управління медичними даними. Основні принципи захисту персональних даних, які можуть бути інтегровані в дану стратегію, включають в себе [48]:

1) законність і прозорість – обробка медичних даних повинна здійснюватися згідно з чинним законодавством та бути відкритою і зрозумілою для пацієнтів; передбачає інформування громадян про їх права);

2) обмеження цілей обробки – дані повинні збиратися та оброблятися лише з конкретною, чітко визначеною метою, що стосується надання медичних послуг;

3) мінімізація даних – медичні установи зобов'язані збирати тільки ту інформацію, яка є необхідною для досягнення конкретних цілей, аби знизити ризик зловживань та порушень;

4) точність даних – забезпечення точності та актуальності медичної інформації пацієнтів, включаючи своєчасне внесення змін і виправлень, щоб уникнути потенційних помилок у лікуванні та діагностиці;

5) обмеження строку зберігання – персональні дані пацієнтів повинні зберігатися тільки протягом часу, необхідного для досягнення цілей обробки, після чого вони повинні бути видалені або анонімізовані;

6) цілісність і конфіденційність – реалізація заходів для захисту даних від несанкціонованого доступу, втрати, викривлення та поширення, що є особливо актуальним у контексті кібербезпеки;

7) відповідальність і звітність – медичні установи та відповідальні особи повинні дотримуватися стандартів обробки даних і бути готовими звітувати про свої дії перед регулюючими органами та громадянами тощо [48].

Для ефективного управління медичними даними в Україні важливо розуміти, які установи та органи регулюють питання розробки законів, стратегій і програм у цій сфері. Дані знання дозволяють з'ясувати, хто відповідає за забезпечення прав пацієнтів, захист персональних даних і

впровадження сучасних інформаційних технологій в медичну практику (табл. 3.2) [53].

Таблиця 3.2

Суб'єкти відповідальні за державне регулювання у сфері захисту медичних даних в Україні

Установа / орган	Функції
Міністерство охорони здоров'я	Розробка нормативно-правових актів, моніторинг реалізації законодавства, контроль за якістю медичних послуг
Міністерство цифрової трансформації України	Впровадження цифрових технологій у сферу охорони здоров'я, координація цифрової трансформації, розробка стандартів кібербезпеки та управління даними
Верховна Рада України	Прийняття законів щодо захисту персональних даних, медичної діяльності та охорони здоров'я
Комітет Верховної Ради України з питань здоров'я нації, медичної допомоги та медичного страхування	Розробка законодавчих ініціатив для поліпшення правових норм у сфері охорони здоров'я, зокрема щодо обробки медичних даних і забезпечення безпеки інформації
Секретаріат Уповноваженого Верховної Ради України з прав людини	Захист прав на приватність і доступ до персональних даних, контроль за дотриманням законодавства з питань захисту конфіденційності, включаючи медичну інформацію
Державна служба спеціального зв'язку	Контроль за захистом інформації, запобігання кіберзагрозам у медичній сфері
Державна агенція з питань електронного урядування	Розробка та впровадження електронних сервісів у медицині, стандартизація інформаційних систем
Національна комісія з питань регулювання зв'язку та інформатизації	Регулювання питань, пов'язаних із захистом даних у телекомунікаціях та Інтернеті
Національна агенція з питань запобігання корупції	Контроль за прозорістю і відкритістю у медичній сфері, запобігання зловживанням
Національний координаційний центр кібербезпеки при РНБО	Розробка стратегій кібербезпеки, координація дій з протидії кіберзагрозам, зокрема у сфері охорони здоров'я

В Україні державні установи використовують ряд механізмів для нормативно-правового регулювання захисту етичних принципів в управлінні медичними даними. Саме вони спрямовані на забезпечення етики, прозорості та безпеки в обробці медичної інформації. Основні з них включають [2]:

– законодавче регулювання: основною механізмів захисту етичних принципів є наявність законодавства, яке встановлює правила та вимоги до обробки медичних даних;

– кодекси етики: державні установи, такі як Міністерство охорони здоров’я, розробляють кодекси етики, які формулюють основні принципи етичної поведінки у сфері медичних послуг;

– контроль та моніторинг: суб’єкти державного регулювання здійснюють контроль за дотриманням етичних норм і стандартів через регулярні перевірки медичних установ та аудит обробки медичних даних – це дозволяє виявляти порушення і вживати заходи для їх усунення;

– освітні програми та тренінги: важливим аспектом є проведення навчальних програм для медичних працівників, які охоплюють питання етики, прав пацієнтів та правил роботи з медичними даними, що в свою чергу допомагає формувати свідомість і відповідальність у галузі охорони здоров’я;

– системи скарг та апеляцій: для захисту прав пацієнтів створено механізми, через які вони можуть подавати скарги на порушення етичних норм тощо [2].

Перелічені механізми взаємодіють між собою, створюючи цілісну систему етичного регулювання в сфері управління медичними даними, яка має на меті захист прав пацієнтів і забезпечення високих стандартів якості медичних послуг в Україні.

Узагальнюючи, можна стверджувати, що правове регулювання медичних даних в Україні перебуває на етапі активної трансформації. Основними завданнями залишаються забезпечення прав пацієнтів, адаптація законодавства до нових викликів цифровізації, а також створення ефективних механізмів контролю за дотриманням норм. Це вимагає зусиль не лише з боку держави, а й від медичних установ та суспільства в цілому. Тільки спільна робота усіх учасників процесу досягти високого рівня захисту медичних даних і забезпечити довіру пацієнтів до системи охорони здоров’я.

3.2. Розробка рекомендацій щодо вдосконалення нормативної бази етичного управління даними в сфері охорони здоров’я

В сучасних умовах цифровізації медичної галузі та зростаючого обсягу медичних даних, що обробляються, вдосконалення нормативної бази етичного управління даними в сфері охорони здоров’я є важливим пріоритетом для забезпечення прав пацієнтів. Динаміка діджиталізації охоплює безліч інновацій, включаючи електронні медичні записи і дистанційне медичне обслуговування, що безпосередньо працюють з їх персональними даними. Впровадження цих інструментів потребує комплексного законодавчого підходу, який охоплював б етичні принципи, що зможуть забезпечити збереження приватності, інформаційну безпеку та дотримання прав пацієнтів [44, с. 122].

Національне законодавство України наразі охоплює лише частину питань пов’язаних з етичним управління даними в медицині. Основні нормативні акти, які визначають рамки захисту у сфері охорони здоров’я, часто виявляються недостатньо деталізованими для цифрових реалій. У свою чергу, це створює ситуацію, коли нові технології стають значною мірою непідконтрольними з точки зору етичного регулювання. Таким чином, виникає необхідність розробки більш гнучкої та адаптованої нормативно-правової бази, що враховуватиме як національні особливості, так і міжнародні стандарти у сфері захисту даних [35, с. 20].

Особливої уваги потребують питання щодо дотримання прав пацієнтів на збереження їх даних. У процесі діджиталізації конфіденційність є одним з найбільш вразливих аспектів, адже медична інформація стає доступною не лише лікарям, а й самим системам, що можуть мати неналежний рівень захисту. Відповідно, важливо, щоб усі цифрові технології відповідали єдиним високим стандартам безпеки, а обробка даних була чітко регламентована. Ці

механізми дозволять мінімізувати ризики несанкціонованого доступу до інформації та посилити довіру населення до системи охорони здоров'я.

Додатково, необхідним є і створення єдиної національної політики для забезпечення належного регулювання технологій, що обробляють медичні дані. Для цього варто залучити різних суб'єктів регулювання, таких як Міністерство охорони здоров'я України, Національну службу здоров'я України та інші державні органи, до процесу створення єдиних стандартів і механізмів контролю. Цей підхід сприятиме кращій координації між різними відомствами, що підвищить ефективність управління даними [61].

Аналіз чинного законодавства показує наявність декількох суттєвих проблем, які потребують вирішення. Однією з них є недостатня адаптованість правових норм до умов цифрового середовища, що сприяє виникненню прогалин у регулюванні. До цього можна віднести відсутність чітких інструкцій щодо застосування нових цифрових інструментів, таких як штучний інтелект, а також проблеми, що виникають при роботі з великими об'ємами даних. На основі цього пропонується внести зміни до існуючих законів України для посилення захисту прав громадян, підвищення рівня безпеки та конфіденційності особистих даних, а також створення більш чіткої і прозорої системи регулювання обробки їх інформації (табл. 3.3) [61].

Таблиця 3.3

Пропозиції щодо удосконалення нормативно-правового регулювання обробки персональних даних в Україні

Закон	Зміни
Закон України «Про основи соціальної захищеності осіб з інвалідністю» №875-XII від 21.03.1991	Рекомендується доповнити цей закон вимогами щодо доступу осіб з інвалідністю до персональних даних, що стосуються їхнього здоров'я або соціального статусу. Закон повинен зобов'язувати установи забезпечувати спеціальні інтерфейси та канали комунікації для таких осіб, аби гарантувати рівний доступ до інформації та послуг, зокрема через інформаційні технології
Закон України «Про інформацію» № 2657-XII від 02.10.1992	Необхідно уточнити вимоги щодо обробки даних для наукових і дослідницьких цілей. Важливо запровадити зобов'язання застосовувати анонімізацію чи псевдонімізацію персональних даних, щоб зменшити ризики витоків особистої інформації при використанні таких даних в дослідженнях, одночасно підтримуючи наукову свободу

Закон України «Про охорону здоров'я» № 2801-XII від 19.11.1992	У цьому законі пропонується ввести вимогу для установ охорони здоров'я щодо забезпечення доступу пацієнтів до їх персональних даних через безпечні електронні платформи. Це дозволить громадянам бути більш інформованими про свої дані і забезпечить прозорість в управлінні ними, відповідно до міжнародних стандартів захист прав людини
Закон України «Про електронні документи та електронний документообіг» № 851-IV від 22.05.2003	У цьому законі доцільно ввести положення, що визначає вимоги до електронного підпису та автентифікації даних, що зберігаються в електронному вигляді. Необхідно визначити, що будь-яка обробка персональних даних повинна бути підтверджена електронним підписом суб'єкта даних для забезпечення прозорості та контролю за обробкою інформації
Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010	Пропонується уточнити положення закону, що стосується обробки персональних даних без згоди суб'єкта даних. Враховуючи сучасні технології, доцільно ввести чітке регулювання обробки даних, яке передбачатиме обов'язкове отримання чіткої, підтвердженої згоди суб'єкта через електронні засоби. Це дозволить забезпечити більший контроль над персональними даними і зменшити ризики маніпуляцій
Закон України «Про державну службу» №889-VIII від 10.12.2015	З метою підвищення етичних стандартів у сфері обробки персональних даних, пропонується ввести вимогу для державних службовців, які працюють з персональними даними, проходити сертифікацію з етичних стандартів обробки цих даних. Це забезпечить підвищення рівня професіоналізму і відповідальності серед працівників, що мають доступ до чутливої інформації громадян

Запропоновані зміни до чинних нормативно-правових актів сприятимуть створенню більш ефективної та етичної системи управління персональними даними в Україні, зокрема в контексті медичних даних.

Також, для посилення законодавчої бази етичного управління медичними даними в Україні необхідно розробити загальні рекомендації, які не лише визначатимуть принципи обробки даних, але й встановлюватимуть певні чіткі вимоги до кожного з етапів:

1. На першому етапі доцільно ухвалити окремий закон, що буде присвячений етичним аспектам управління медичними даними. У цьому законі слід передбачити базові принципи, враховуючи чутливий характер такої інформації та її особливе значення для захисту прав пацієнтів.

2. Наступний напрям удосконалення нормативної бази полягає у впровадженні системи обов'язкового аудиту етичних стандартів для медичних

установ. Даний аудит повинен регулярно перевіряти дотримання конфіденційності та надійності інформації, зокрема у сфері цифрового обміну даними.

3. Розробка національних стандартів анонімізації медичних даних є важливим компонентом захисту інформації. Пропонується розробити національні стандарти, що будуть регулювати процеси анонімізації з урахуванням передових міжнародних підходів, забезпечуючи захист пацієнтів і зменшуючи ризики несанкціонованого доступу до інформації.

4. Необхідно також законодавчо закріпити цифрові механізми ідентифікації осіб, які матимуть доступ до медичних даних, використовуючи багатофакторну автентифікацію. Це допоможе посилити контроль за доступом та зменшити ризики втручання в приватне життя пацієнтів.

5. З огляду на розвиток штучного інтелекту та його використання у медицині, рекомендується розробити спеціальні нормативні акти, які визначатимуть етичні та правові рамки для нього. Сюди слід включити положення щодо відповідальності за прийняття рішень, а також забезпечення прозорості алгоритмів, що обробляють персональні дані пацієнтів.

6. Для того, щоб забезпечити ефективність нормативно-правових актів, необхідно також заснувати інститут етичного омбудсмена, що дозволить мати незалежного представника, відповідального за моніторинг і розгляд скарг, пов’язаних з етичними порушеннями щодо роботи з медичною інформацією пацієнтів. Омбудсмен зможе надавати рекомендації щодо вдосконалення законодавства та впроваджувати механізми для посилення прав пацієнтів у системі охорони здоров’я.

7. Важливо внести зміни до законодавства, які передбачатимуть суворі санкції за порушення етичних стандартів при роботі з медичними даними. Це сприятиме зменшенню кількості інцидентів, пов’язаних із незаконним доступом чи неправомірною обробкою інформації.

8. На законодавчому рівні доцільно впровадити механізми інформованого контролю за використанням медичних даних пацієнтів. Це

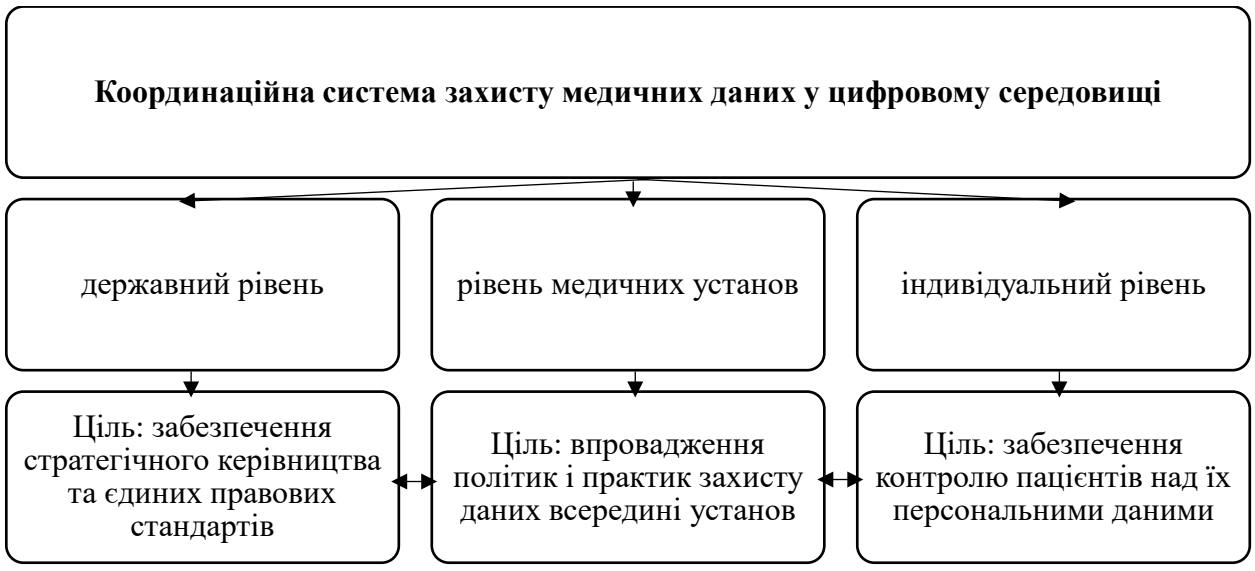
означає, що пацієнти мають право не лише знати, як і для чого будуть використовуватись їх дані, але і впливати на процес, надаючи обмежену або часткову згоду на обробку даних. Такий підхід, дозволить більш чітко регулювати використання приватної інформації у дослідницьких та медичних цілях.

9. Враховуючи досвід інших країн, рекомендується створити державну грантову програму для підтримки досліджень, спрямованих на розробку етичних підходів до обробки медичних даних. Фінансування таких досліджень сприятиме активному залученню науковців до вирішення етичних проблем і посиленню стандартів відповідальності в медичній сфері.

10. Пропонується також запровадити законодавчі вимоги щодо використання динамічного шифрування медичних даних, що буде оновлюватися відповідно до сучасних кіберзагроз. Такі технології шифрування, адаптовані до реальних умов роботи медичних установ забезпечать високий рівень захисту приватної інформації пацієнтів.

Комплекс цих заходів сприятиме гармонізації законодавства України з сучасними цифровими викликами, забезпечуючи захист прав пацієнтів і безпечну роботу з їх даними. Координація зусиль на кожному рівні управління підвищить надійність реалізації цих заходів (схема 3.1) [63, с. 256]:

Схема 3.1



На державному рівні координаційні дії зосереджені на створенні загальної стратегії для захисту даних, що буде охоплювати оновлення законів і положень, які забезпечують чіткі правила для цифрового управління медичною інформацією. Це включає розробку або оновлення законів, щодо прав пацієнтів на доступ та контроль свої даних, вимог до безпеки інформаційних систем і відповідальність медичних установ за порушення захисту даних. Також необхідне посилення міжвідомчої взаємодії для швидкого реагування на нові виклики та підтримка міжнародних стандартів для інтеграції європейських практик захисту даних.

На рівні медичних установ важливо організувати локальні етичні комітети, які здійснюватимуть моніторинг виконання стандартів безпеки та етичного управління медичною інформацією. Ці комітети координуватимуть зусилля персоналу, забезпечуватимуть навчання співробітників, інформуватимуть пацієнтів про їх права щодо використання даних і контролюватимуть відповідність до етичних норм у цифровому середовищі. Крім того, медичні установи мають забезпечити надійність своєї інфраструктури, впроваджуючи сучасні технології, такі як блокчейн і штучний інтелект, для децентралізованого зберігання та моніторингу даних.

На індивідуальному рівні важливо надати пацієнтам можливість брати активну участь у процесах управління їхніми даними та забезпечити їм зручний доступ до цифрових платформ для перегляду і контролю своєї інформації. Для цього необхідне введення механізмів для отримання згоди пацієнтів на використання даних, інформування їх про будь-які зміни в політиці конфіденційності та можливість обмежити або відкликати доступ до цих даних. Завдяки таким заходам пацієнти зможуть відчувати більше довіри до медичних установ, оскільки матимуть безпосередній контроль над власними персональними даними.

Підсумовуючи, слід ще раз наголосити на тому, що вдосконалення нормативної бази етичного управління даними в сфері охорони здоров’я України є необхідним кроком до створення системи, що відповідає вимогам

сучасного цифрового середовища. Запропоновані рекомендації, які передбачають інтеграцію сучасних технологій, адаптацію до міжнародних стандартів і активну участь пацієнтів у прийнятті рішень, допоможуть створити ефективну, прозору та довірливу медичну систему. У результаті реалізації цих ініціатив Україна зможе не лише покращити захист прав пацієнтів, але й зміцнити позиції в сфері діджиталізації медичної галузі.

Висновки до Розділу 3

В межах третього розділу дослідження було проведено детальний аналіз існуючих нормативно-правових актів, що регулюють управління медичними даними в Україні. Було виявлено, що, незважаючи на наявність законодавчої бази, деякі аспекти залишаються недостатньо врегульованими, особливо в частині етичного використання медичних даних. Ці питання вимагають подальшого вдосконалення для підвищення рівня захисту прав пацієнтів та забезпечення належного управління інформаційними ресурсами.

Одним із головних висновків є те, що поточна нормативна база не повністю відповідає сучасним викликам, пов’язаним із захистом конфіденційності та безпекою медичних даних. Для цього необхідно розробити більш чіткі та конкретні правила, які б враховували як національні особливості, так і міжнародний досвід у цій сфері.

Запропоновані рекомендації щодо вдосконалення законодавства наголошують на важливості адаптації існуючих норм до специфіки діджиталізації, що сприятиме забезпеченню надійного захисту персональних даних і прозорості обробки інформації.

Крім того, впровадження національної політики, орієнтованої на координацію роботи всіх державних органів, які беруть участь у регулюванні медичних даних, є необхідною умовою для результативного управління цифровою інформацією. Лише комплексний підхід до реформування законодавства, що враховує всю специфіку роботи у системі охорони здоров’я,

дозволить створити правове середовище, яке забезпечить належний рівень безпеки та етичності у сфері медичної інформації.

Головним пріоритетом у покращенні нормативно-правового регулювання є забезпечення пацієнтів правом на доступ, контроль та безпечне використання їх особистих даних. Це у свою чергу вимагає в законодавстві посилення принципів прозорості та відповідальності у процесах збору, обробки і передачі цих даних. Особливо важливим є забезпечення прав пацієнтів на інформовану згоду, яка має бути не лише формальністю закріпленою статтями у законах, але й діючим інструментом усвідомленого контролю над своєю медичною інформацією. Дане переосмислення зможе забезпечити більш збалансовані відносини між пацієнтом і медичними установами, що використовують його дані.

Також суттєвою складовою є навчання медичних працівників та керівництва закладів охорони здоров’я принципам етичного управління даними, щоб вони були готові до взаємодії з цифровими технологіями в рамках встановлених етичних норм. Професійне навчання у сфері етичного менеджменту медичних даних підвищить обізнаність фахівців про загрози порушення конфіденційності та шляхи їх попередження, що сприятиме створенню культури відповідальності та поваги до прав пацієнтів.

Загалом, реалізація запропонованих заходів сприятиме створенню ефективної системи етичного управління медичними даними, що забезпечить високий рівень захисту інформації та підвищення довіри громадян до системи охорони здоров’я. Впровадження цих заходів є важливим кроком на шляху до забезпечення відповідності національного законодавства міжнародним стандартам і покращення якості медичних послуг.

ВИСНОВКИ

Проведене автором дослідження етики управління даними в системі охорони здоров’я через призму викликів цифрової трансформації дає змогу сформувати наступні висновки.

1. Аналіз класифікації медичних даних показав, що їх основні типи відрізняються за природою, методами збору і цілями використання, а кожен тип виконує певну функцію в системі охорони здоров’я. Було встановлено, що медичні дані поділяються на персональні, клінічні та генетичні, що служать для точної ідентифікації пацієнта, розробки індивідуальних планів лікування і прогнозування ризиків. Кожен з цих типів даних потребує особливого підходу до організації, збереження та захисту, що є основою для забезпечення якості медичних послуг. Дослідження також виявило загальновизнані формати стандартизації медичних даних, такі як International Classification of Diseases (ICD) і Health Level 7 (HL7), які створюють уніфіковані правила для обміну інформацією між медичними закладами, запобігаючи помилкам та дублюванню. Медичні дані, окрім функціонального значення, також є важливим інструментом для стратегічного управління медичними установами, адже дозволяють оцінювати якість роботи, виявляти проблемні аспекти й оптимізувати процеси. Особливу увагу приділено електронним медичним даним, які є цифровими версіями традиційних записів і включають всю необхідну інформацію про пацієнтів. Електронні медичні дані поділяються на електронну медичну карту, електронну історію хвороби, персоналізовані дані, дані телемедицини, а також дані з медичних пристроїв і сенсорів. Зазначено, що впровадження цифрових технологій у медичну сферу вимагає дотримання етичних і правових стандартів для захисту прав пацієнтів. Крім того, було описано використання великих даних (Big Data) у медицині, де процес включає збір, обробку, аналіз та прогнозування результатів для подальшого застосування.

2. В рамках дослідження основних етичних засад управління медичною інформацією було встановлено, що серед ключових принципів вирізняються конфіденційність, інформована згода, рівний доступ, ідентифікація, анонімність і прозорість. Забезпечення цілісності та достовірності медичних даних є важливим, адже на основі цих даних ухвалюються рішення, що безпосередньо впливають на здоров'я пацієнтів. Недотримання цих принципів може призвести не лише до втрати довіри до медичних установ, а й до правових наслідків. Інформована згода є особливо необхідною, оскільки пацієнти повинні бути обізнані про використання своїх медичних даних у цифрових системах. Прозорість дозволяє пацієнтам та громадськості отримувати чітке уявлення про політику медичних установ щодо обробки медичних даних. Дотримання етичних принципів управління медичною інформацією є основою для підтримки довіри до медичної системи і захисту прав пацієнтів. Дослідження також підкреслило необхідність захисту електронних медичних записів через шифрування та авторизаційні механізми, зокрема багатофакторну автентифікацію. Виявлено, що цифрові системи повинні знижувати ризик дискримінації і враховувати інклюзивність. З цією метою складено таблицю з прикладами основних платформ у сфері охорони здоров'я в різних країнах, таких як: eHealth (Україна), MyChart (США), Lifelabs (Канада), NHS app (Великобританія), TeleClinic (Німеччина) HealthEngine (Австралія), які надають багатомовну підтримку та зручні інтерфейси. У дослідженні також було наведено класифікацію етичних принципів за Б. Варкі, який виділив автономію, справедливість, доброякісність та ненасення шкоди, що регулюють взаємодію в системі охорони здоров'я. Водночас були розглянуті вітчизняні принципи, такі як законність обробки, цільова спрямованість і пропорційність. Аналіз підкреслив важливість етичного регулювання на державному, регіональному та місцевому рівнях, що вимагає співпраці між усіма суб'єктами надання медичних послуг. Для наочного розуміння розроблено модель регулювання,

яка включає ключових суб'єктів системи охорони здоров'я України та їх основні завдання.

3. Оцінка впливу діджиталізації на управління медичними даними виявила кардинальні зміни у функціонуванні медичної сфери. Серед основних цифрових рішень, що використовуються, особливу роль відіграють електронні медичні записи, штучний інтелект та хмарні сервіси. Використання цих технологій значно пришвидшує доступ до медичних даних, їх обробку та передачу, підвищуючи ефективність діагностики і лікування. Аналіз Національної системи здоров'я України засвідчив, що впровадження цифрових платформ спричинило зменшення обсягу паперової документації на 25 % за останні п'ять років, а швидкість обміну інформацією між закладами зросла майже на 40 %. Проте, ці зміни супроводжуються новими викликами, зокрема, зростає потреба в належному захисті даних, інтеграції різних систем та підготовці медичного персоналу до роботи з новими технологіями. Необхідним стало розроблення чітких методологічних засад для регулювання впровадження цифрових рішень у медичну практику. Серед важливих ініціатив цифровізації охорони здоров'я України – система eHealth, впровадження стандартів ВООЗ та навчальні програми для медичних працівників. Згідно з даними НСЗУ, станом на 2024 рік близько 82 % державних медичних установ вже функціонують на основі цих програм. Окрім того, активно впроваджуються міжнародні стандарти Health Level 7 (HL7) і Fast Healthcare Interoperability Resources (FHIR) для забезпечення сумісності з глобальними системами охорони здоров'я. Цифрові технології впливають на оптимізацію медичних процесів, розвиток пацієнт-орієнтованого підходу та розширення можливостей для пацієнтів через цифрові платформи. Ініціативи в рамках цифровізації медичної системи включають розбудову єдиної Електронної системи охорони здоров'я, впровадження особистих кабінетів для пацієнтів і розширення функцій медичних інформаційних систем. Серед стратегічних напрямків цифровізації охорони здоров'я виділяються: ефективне управління пацієнтами з хронічними захворюваннями, моніторинг

захворювань у реальному часі та контроль за доступом до лікування. Блокчейн-технології сприяють забезпеченню високого рівня прозорості і безпеки медичних даних. Ефективне управління медичними даними також передбачає маркування, кодування інформації та використання хмарних середовищ, що забезпечують швидкий доступ до даних, зменшення помилок у діагностиці і лікуванні, а також зниження витрат на управління. Аналіз показав популярні хмарні сервіси, які використовують медичні установи України та на основі цього створено порівняльну таблицю з основними перевагами та недоліками хмарних технологій у медичній сфері. Серед переваг було виділено: гнучкість ресурсів, поліпшення обміну інформацією, високий рівень безпеки даних, доступ до аналітики даних і зниження витрат на інфраструктуру. А до основних недоліків віднесено: залежність від Інтернет-з'єднання, проблема з конфіденційністю, проблеми з інтеграцією, витрати на навчання та регуляторні виклики.

4. Визначення етичних ризиків, що виникають під час цифрової трансформації у медичній сфері, виявило низку серйозних викликів. Серед найбільш актуальних ризиків – порушення конфіденційності через кіберзагрози, коректність та достовірність медичних даних, ризики дискримінації та нерівномірного доступу до цифрових послуг, труднощі з отриманням інформованої згоди і проблема відповідальності за роботу алгоритмів штучного інтелекту. Для наочності було складено таблицю ключових загроз і запропоновано регуляторні та технічні заходи для їх подолання. Виділено, що рівень кібератак на медичні установи значно зріс за останні роки. Дослідження показує, що у 2024 році кількість атак становила 970 штук. Ці загрози призводять до серйозних наслідків, таких як витоки пацієнтських даних, припинення роботи медичних систем, підробка медичної інформації тощо. Це, в свою чергу, вимагає впровадження сучасних технологій захисту даних та розробки стандартів кібербезпеки, здатних ефективно реагувати на нові типи загроз. Окремо увага приділяється мобільним додаткам для моніторингу стану здоров'я, які також можуть стати

джерелом ризиків через недоліки в шифруванні даних або незаконне використання персональної інформації. Крім того, відсутність належного регулювання обробки великих обсягів даних підвищує загрозу їхнього використання без згоди пацієнтів. До проблем також належить людський фактор – помилки персоналу та недотримання правил кібербезпеки, а також технічні збої через несправності або помилки у пристроях. Значним етичним питанням постає і нерівність доступу до цифрових медичних послуг. Станом на 2024 рік близько 30 % медичних закладів не мають стабільного доступу до Інтернету. Військові дії ускладнюють цю ситуацію, погіршуючи доступність медичних послуг та посилюючи етичні проблеми, пов'язані з правом на своєчасну медичну допомогу. Так, виникає нагальна потреба у підтримці мобільних медичних команд, які надають допомогу на місцях, попри високі ризики для медичного персоналу. Міжнародні партнери для цього пропонують нові моделі впровадження етичних принципів у кризових умовах, що базуються на потребах населення. Такі моделі включають міждисциплінарний підхід, навчання медичного персоналу, моніторинг і оцінку надання допомоги. На національному рівні Міністерство охорони здоров'я та Міністерство цифрових технологій України розробляють курси для медичних працівників з кібербезпеки. Загалом можна підсумувати, що всі державні та регіональні комітети, а також різні приватні установи медичної сфери працюють над створенням безпечного середовища для медичних закладів.

5. Проведений аналіз нормативно-правової бази України щодо регулювання етики управління медичними даними виявив потребу в її подальшому вдосконаленні. Незважаючи на поступовий розвиток законодавства в цій сфері, багато нормативних актів не враховують сучасні цифрові технології, які дуже активно впроваджуються. Було створено таблицю ключових законодавчих актів, що регулюють медичні дані, із зазначенням аспектів, які вони охоплюють. Зокрема, Закон України «Основи законодавства України про охорону здоров'я» № 2801-XII від 19.11.1992 р. наголошує на захисті інформації про стан здоров'я громадян та обмеженні доступу

сторонніх осіб до цієї інформації. У 2008 році прийнято Концепцію для створення єдиної системи реєстрації і обміну медичною інформацією, що передбачала інтеграцію медичних установ у спільних інформаційний простір. Подальші кроки включали впровадження електронної системи охорони здоров'я у 2018 році, затвердженої Постановою Кабміну № 411, а також прийняття «Концепції розвитку електронної охорони здоров'я» для стратегічного вдосконалення інфраструктури обробки та безпеки медичних даних. Проте, з поширенням цифрових технологій зріс рівень кіберзагроз, що став особливо гостро відчутним після початку повномасштабного вторгнення Росії на території України у 2022 році. Це викликало необхідність ухвалення нових законів і постанов, спрямованих на протидію новим викликам. На додаток, виявлено проблеми з контролем за дотриманням етичних стандартів у сфері медичних даних, що є важливим для забезпечення прав пацієнтів на якісну медичну допомогу. Тоді, у 2024 році МОЗ України запустило Національну програму етичного управління медичними даними, яка передбачає створення етичних рекомендацій для закладів охорони здоров'я. Було також виокремлено основні суб'єкти державного регулювання у цій сфері: Міністерство охорони здоров'я України, Міністерство цифрової політики України, Верховна Рада України та її відповідні комітети, Секретаріат Уповноваженого Верховної Ради України з прав людини, Державна служба спеціального зв'язку, Державна агенція з питань електронного урядування, Національна комісія з питань регулювання зв'язку та інформатизації, Національна агенція з питань запобігання корупції і Національний координаційний центр кібербезпеки при РНБО. Кожен з цих суб'єктів застосовує різні механізми для захисту етичних принципів управління медичними даними, такі як, законодавче регулювання, кодекси етики, моніторинг, освітні програми, а також системи скарг та апеляцій. Така комплексна система етичного регулювання спрямована на захист прав пацієнтів і забезпечення високих стандартів якості медичних послуг в Україні.

6. Розроблені рекомендації для вдосконалення правової бази етичного управління медичними даними націлені на створення єдиного та цілісного підходу до регулювання обробки медичної інформації в умовах цифровізації. Одним із ключових кроків є оновлення положень чинних законів. Пропонується забезпечити обов'язкове отримання згоди від суб'єктів через електронні засоби для зниження ризику маніпуляцій; чітко регламентувати вимоги до електронного підпису й автентифікації для прозорості обробки даних; впровадити анонімізацію персональної інформації, щоб мінімізувати ризик витоку особистих даних; покращити рівні захисту платформ, на яких пацієнти користуються електронними сервісами; розробити спеціальні інтерфейси для осіб з обмеженими можливостями. Додатково, запропоновано запровадити обов'язкову сертифікацію для державних службовців і медичного персоналу, які працюють з персональними даними, стосовно етичних стандартів обробки даних. Важливо також покращити контроль за дотриманням етичних норм, здійснюючи регулярні перевірки та аудит. Для зменшення етичних ризиків пропонується вдосконалити процедури отримання інформованої згоди і розробити систему навчання для медичних працівників з акцентом на використання новітніх технологій у межах етичних норм. Для забезпечення ефективності законодавчих актів важливим здається заснування інституту етичного омбудсмена, який буде незалежним відповідальним за моніторинг і розгляд етичних порушень у сфері медичних даних. Також рекомендовано створити державну грантову програму для підтримки досліджень, що розробляють етичні підходи до обробки медичних даних та впровадити динамічне шифрування даних, що оновлюватиметься відповідно до кіберзагроз. На завершення, було розроблено координаційну систему захисту медичних даних на державному, індивідуальному рівні і рівні медичних установ. Запропоновано посилити регуляцію між державними і приватними медичними закладами, створюючи єдину правову структур, що відповідає міжнародним стандартам і захищає права пацієнтів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз переваг та ризиків при переході до хмарних послуг [Електронний ресурс]. – 2024. – URL: https://eska.global/blog/analiz-perevag-ta-rizikiv-pri-perehodi-do-hmarnih-poslug.

2. Антонова Л. В. Міжнародний досвід регулювання й дотримання етичних норм в сфері охорони здоров’я [Електронний ресурс] / Л. В. Антонова, Л. В. Козлова // Державне управління: удосконалення та розвиток. – 2020. – № 4. – URL: http://www.dy.nayka.com.ua/?op=1&z=1882.

3. Баликіна О. Охорона здоров'я у хмарах. Хмарні технології у медицині [Електронний ресурс] / О. Баликіна. – 2024. – URL: https://www.sim-networks.com/ukr/blog/cloud-technologies-for-medicine.

4. Берн І. Права людини у сфері охорони здоров’я: [практичний посібник] / І. Берн , Т. Езер, Дж. Коен, Дж. Оверал, І. Сенюта. – Львів: Медицина і право, 2012. – 552 с. – URL: https://healthrights.org.ua/?id=158.

5. Білоконь С. В. Основи біоетики та біобезпеки: [навчальний посібник] / С. В. Білоконь. – Одеса : Одеський національний університет імені І. І. Мечникова, 2017. – 155 с.

6. Вітрова Ю. Медицина в умовах війни: ІТ-революція і розвиток після конфлікту [Електронний ресурс] / Ю. Вітрова. – 2023. – URL: https://lb.ua/ news/2023/09/15/574951_meditsina_umovah_viyni.html.

7. Вплив війни на психічне здоров’я-колосальний [Електронний ресурс]. – URL: https://www.kmu.gov.ua/news/vpliv-vijni-na-psihichnezdorovya-kolosalnij-viktor-lyashko.

8. Гончаренко Д. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? [Електронний ресурс] / Д. Гончаренко. – 2020. – URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/.

9. Горбатова Д. І. Форми державного управління у сфері охорони здоров’я [Електронний ресурс] / Д. І. Горбатова // Право і суспільство. – 2019.

– № 4. – С. 166–173. – URL: http://pravoisuspilstvo.org.ua/archive/2019/4_2019/26.pdf.

10. Гриценко В. І. Сучасний стан та перспективи розвитку цифрової медицини / В. І. Гриценко, Л. С. Файнзільберг // Кібернетика та обчислювальна техніка. – 2020. – 1(199). – С. 59-84.

11. Давиденко Г. Цифрова інклюзія та доступність: соціальна діджиталізація: [монографія] / Г. Давиденко. – Вінниця: ТВОРИ, 2023. – 240 с.

12. Дацій Н. В. Теоретичні підходи до системи надання медичних послуг в умовах цифрової трансформації [Електронний ресурс] / Н. В. Дацій, А. М. Никитюк // Державне управління: удосконалення та розвиток. – 2023. – № 1. – URL: https://www.nayka.com.ua/index.php/dy/issue/view/54.

13. Деміхов О. І. Актуальні тенденції впровадження елементів електронного урядування в сфері громадського здоров'я в умовах епідеміологічної загрози [Електронний ресурс] / О. І. Деміхов, І. О. Бєлова, Л. М. Таранюк // Університетські наукові записки. – 2020. – № 3-4(75-76). – С. 86-92. – URL: https://doi.org/10.37491/UNZ.75- 76.9.

14. Деміхов О. І. Розвиток організаційно-правових засад застосування цифрових технологій у сфері громадського здоров'я в Україні / О. І. Деміхов, І. О. Дегтярьова // Збірник наукових праць НАДУ. – 2020. – № 1. – С. 80-87.

15. Деякі питання електронної системи охорони здоров'я: постанова Кабінету Міністрів України від 25.04.2018 р. № 411 [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text.

16. Діденко Н. Г. Трансформація національної системи охорони здоров'я під час війни й повоєнного відновлення [Електронний ресурс] / Н. Діденко // Public policy, governance and communications in the EU member states and candidate countries : post-conference monograph / [V. Burksiene et al. ; gen. ed. by G. Riabtsev and V. Tertychka] ; National University of Kyiv-Mohyla Academy [et al.]. – K. : NaUKMA, 2023. – С. 148-156. – URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/941e6608-c088-4417-8c39-db9a63264e3a/content.

17. Діордіца І. В. Правова охорона персональних даних у сфері охорони здоров'я в Україні / І. В. Діордіца, І. А. Коваленко, О. М. Коваль // Науковий вісник Ужгородського Національного Університету. Серія: Право. – 2024. – Вип. 82, Ч. 2. – С. 141-146.

18. Жуковська В. М. Цифрові виклики кадрового забезпечення підприємства [Електронний ресурс] / В. М. Жуковська // Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку. – 2019. – Вип. 2. – С. 10-17. – URL: http://science.lpnu.ua/sites/default/files/journal-paper/2020/jan/20629/zhukovska.pdf.

19. Кабанов О. Відповідність законодавства України окремим положенням правового регулювання сфери відкритих даних у Європейському Союзі [Електронний ресурс] / О. Кабанов, Т. Олексіюк. – URL: https://eef.org.ua/wp-content/uploads/2023/07/Vidpovidnist-zakonodavstva-Ukrayiny-okremym-polozhennyam-pravovogo-regulyuvannya-sfery-vidkrytyh-danyh-u-YEvropejskomu-Soyuzi.pdf.

20. Квітка С. Цифрова трансформація системи охорони здоров’я: фактори впливу на якість життя населення [Електронний ресурс] / С. Квітка, М. Миргородська // Аспекти публічного управління. – 2024. – № 12(1). – С. 14-21. – URL: https://doi.org/10.15421/152402.

21. Кириченко І. В., Ніколайчук А. Використання хмарного сервісу для розгортання та підтримки медичної системи. // Інформаційні системи та технології : матеріали 9-ї Міжнар. наук.-техн. конф., 17–20 листопада 2020 р. – Харків : Друкарня Мадрид, 2020. – С. 221–222.

22. Кіберзахист закладів охорони здоров’я [Електронний ресурс]. – 2023. – URL: https://medplatforma.com.ua/news/60432-kiberzakhist-zakladiv-okhoroni-zdorovya-moz-rozrobilo-rekomendatsii.

23. Коваленко О. С. (2019). Трансформація систем підтримки прийняття клінічних рішень у структури FHIR для забезпечення якості медичної допомоги [Електронний ресурс] / О. С. Коваленко, Р. Ф. Міщенко, Л.

М. Козак // Кібернетика та обчислювальна техніка. – 2019. – № 4(198). – С. 78-94. – URL: https://doi.org/10.15407/kvt198.04.078.

24. Козак Л. М. Цифрова трансформація в медицині: від формалізованих медичних документів до інформаційних технологій цифрової медицини [Електронний ресурс] / Л. М. Козак, А. С. Коваленко, О. А. Кривова, О. А. Романюк // Кібернетика і вичислювальна техніка. – 2018. – № 4(194). – С. 61-78. – URL: https://doi.org/10.15407/kvt194.04.061.

25. Козьяков С. Штучний інтелект у медицині: чого більше — ризиків чи користі? [Електронний ресурс] / С. Козьяков. – 2024. – URL: https://zn.ua/ukr/TECHNOLOGIES/shtuchnij-intelekt-u-meditsini-choho-bilshe-rizikiv-chi-koristi.html.

26. Корчинський І. Цифрова медицина: особливості та проблеми становлення в Україні [Електронний ресурс] / І. Корчинський, Н. Фірман // Цифрова економіка та економічна безпека. – 2022. – № 1(01). – С. 100-105. – URL: https://doi.org/10.32782/dees.1-16.

27. Костенок Н. Особливості розвитку інструментів цифрової трансформації системи охорони здоров’я в Україні / Н. Костенок, А. Пєнкова // Актуальні проблеми державного управління. – 2021. – № 3(84). – С. 121–125.

28. Кришталь О. О. Біоетика: від теорії до практики [Електронний ресурс] / О. О. Кришталь, М. О. Чащин, К. В. Скребцова. – Київ : ВД «Авіцена», 2021. – 144 с. – URL: https://philpapers.org/archive/KRYBFT.pdf.

29. Лазебник Ю. О. Міжнародні статистичні класифікації в національній системі електронної охорони здоров’я [Електронний ресурс] / Ю. О. Лазебник // БІЗНЕСІНФОРМ. – 2018. – № 7. – С. 257-263. – URL: https://www.business-inform.neexport_pdf/business-inform-2018-7_0-pages-257_263.pdf.

30. Лехан В. М. Аналіз реформ охорони здоров’я в Україні: від здобуття незалежності до сучасності [Електронний ресурс] / В. М. Лехан, Л. В. Крячкова, М. І. Заярський // Україна. Здоров’я нації. – 2018. – № 4(52). – С. 5-11. – URL: https://repo.dma.dp.ua/4987/.

31. Маркування даних в охороні здоров'я: застосування та вплив [Електронний ресурс]. – URL: https://www.facerua.com/markuvannia-danikh-u-okhoroni-zdorovia-zastosuvannia-ta-vpliv/.

32. Миронова Г. Впровадження електронних медичних записів пацієнта: проблеми правового регулювання в Україні [Електронний ресурс] / Г. Миронова // Приватне право і підприємництво. – 2022. – № 21. – С. 140-149. – URL: http://ppp-journal.kiev.ua/archive/2022/21/18.pdf.

33. Модернізація менеджменту та публічного управління в системі охорони здоров’я: [монографія] / [Р. Р. Августин, О. З. Апостолюк, А. І. Артимович та ін.]. – Тернопіль : Крок, 2020. – 560 с.

34. МОЗ: Презентовано Рамку цифрової компетентності працівника охорони здоров’я [Електронний ресурс]. – URL: https://www.kmu.gov.ua/news/moz-prezentuvano-ramku-tsyfrovoi-kompetentnosti-pratsivnyka-okhorony-zdorovia.

35. Мусієнко А. В. Актуальні аспекти нормативно-правових механізмів захисту персональних даних в електронних медичних реєстрах в Україні / А. В. Мусієнко, В. В. Мусієнко / Dictum Factum. – 2022. – Вип. 1(11). – С. 17-22.

36. НСЗУ: Які дані пацієнтів зберігаються в електронній системі охорони здоров’я. [Електронний ресурс]. – URL: https://www.kmu.gov.ua/news/nszu-iaki-dani-patsiientiv-zberihaiutsia-v-elektronnii-systemi-okhorony-zdorovia.

37. Основи законодавства України про охорону здоров’я: Закон України від 19.11.1992 р. № 2801-XII [Електронний ресурс]. – URL: https://zakon.rada. gov.ua/laws/show/2801-12#Text.

38. Основні переваги сертифікації ISO/IEC 27001 [Електронний ресурс]. – URL: https://www.issp.training/post/osnovni-perevahy-sertyfikatsiyi-iso-iec-27001/.

39. Островська Б. В. Біоетичні принципи як утвердження в міжнародному праві нового рівня захисту прав людини / Б. В. Островська // Юридичний часопис Національної академії внутрішніх справ. – 2018. – № 2. – С. 38-54.

40. Островська Б. В. Міжнародно-правове регулювання права людини на життя в контексті біоетики: [монографія] / Б. В. Островська. – Київ: Логос, 2019. – 604 с.

41. Офіційний сайт «Державна служба спеціального зв’язку та захисту інформації України» [Електронний ресурс]. – URL: https://cip.gov.ua/ua.

42. Офіційний сайт «Національної служби здоров’я України» [Електронний ресурс]. – URL: https://nszu.gov.ua/.

43. Патрікєєва Н. Рік після атаки вірусу Petya: що змінилося в кібербезпеці України [Електронний ресурс]. – 2023. – URL: https://www.radiosvoboda.org/a/29336511.html.

44. Пономаренко І. С. Правове регулювання захисту персональних даних у медичній сфері: вітчизняний та міжнародний досвід [Електронний ресурс] / І. С. Пономаренко // Право і суспільство. – Дніпро : Дніпровський гуманітарний університет. – 2020. – № 6-2. – С. 120-126. – URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/1d53be22-5113-4bc1-af2d-0cd00370cd32/content.

45. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII (редакція від 01.01.2024, підстава – 1909-IX) [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.

46. Про затвердження Концепції галузевої програми «Електронна система реєстрації та обміну медичною інформацією між закладами, установами і організаціями охорони здоров'я»: наказ Міністерства охорони здоров’я України від 25.07.2008 р. № 409 [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/rada/show/v0409282-08#Text.

47. 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 р. № 1695 [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/z1155-22#Text.

48. Про захист персональних даних: Закон України №2297-VI від 01.06.2010 р. [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

49. Про заходи щодо створення електронної інформаційної системи «Електронний Уряд»: постанова Кабінету Міністрів України від 24.02.2003 р. № 208 [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/208-2003-%D0%BF#Text.

50. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

51. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

52. Про підвищення доступності та якості медичного обслуговування у сільській місцевості: Закон України від 14.11.2017 р. № 2206-VIII [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2206-19#Text.

53. Про систему громадського здоров'я: Закон України від 06.09.2022 р. № 2573-IX [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/2573-20#Text.

54. Про схвалення Концепції розвитку електронної охорони здоров'я: розпорядження Кабінету Міністрів України від 28.12.2020 р. № 1671-р [Електронний ресурс]. – URL: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text.

55. ПРООН та Уряд Канади цифровізують інфраструктуру охорони здоров'я в Україні [Електронний ресурс]. – URL: https://www.undp.org/uk/ukraine/press-releases/proon-ta-uryad-kanady-tsyfrovizuyut-infrastrukturu-okhorony-zdorovya-v-ukrayini.

56. Рапіта О. Кіберінциденти в медицині : нові виклики та шляхи захисту [Електронний ресурс]. – 2024. – URL: https://icsa.team/167-2/.

57. Романюк О. Формування інтероперабельного цифрового медичного інформаційного середовища: персональні медичні дані [Електронний ресурс] / О. Романюк, Л. Козак, О. Коваленко // Наука та інновації. – 2021. – № 17 (5). – С. 50-62. – URL: https://doi.org/10.15407/scine17.05.050.

58. Семидоцька Ж. Д. Здоров'я людини і сучасні біомедичні технології : [навчальний посібник] / Ж. Д. Семидоцька, І. О. Чернякова, А. Б. Борзенко. – Харків : ХНМУ, 2020. – 96 с.

59. Сенюк Ю. І. Сучасна державна політика у сфері охорони здоров’я: аналіз реформування системи [Електронний ресурс] / Ю. І. Сенюк, З. О. Надюк // Право та державне управління. – 2020. – № 2. – С. 211-220. – URL: http://pdu-journal.kpu.zp.ua/archive/2_2020/34.pdf.

60. Сердюк А. М. Етика і культура безпеки в медичній практиці [Електронний ресурс] / А. М. Сердюк, М. Ю. Риган, Ю. М. Скалецький // Міжнародний журнал: Реабілітація та паліативна медицина. – 2023. – № 1(8). С. 138. – URL: https://med-expert.com.ua/journals/download.php?file=https://med-expert.com.ua/journals/wp-content/uploads/2023/06/RPM_01_23_web.pdf.

61. Система охорони здоров’я в Україні (СОЗ) [Електронний ресурс]. – URL: https://uareforms.org/pages/new-page-655.

62. Спеціалісти НМУ вивчали використання штучного інтелекту в освіті та медицині [Електронний ресурс]. – 2024. – URL: https://nmuofficial.com/news/ spetsialisty-nmu-vyvchaly-vykorystannya-shtuchnogo-intelektu-v-osviti-ta-medytsyni/.

63. Тарасюк А. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі [Електронний ресурс] / А. Тарасюк // Підприємництво, господарство і право. – 2020. – № 7. – С. 254-258.

64. «Телемедицина наближає пацієнтів до лікаря, дає можливість бути почутими і здоровішими», – експерти з провадження телемедичних послуг [Електронний ресурс]. – URL: https://caritas.ua/news-en/telemedyczyna-nablyzhaye-pacziyentiv-do-likarya-daye-mozhlyvist-buty-pochutymy-i-zdorovishymy-eksperty-z-provadzhennya-telemedychnyh-poslug/.

65. Шишка І. Аналіз результатів реформування системи охорони здоров’я на основі звітної документації НСЗУ / І. Шишка // Економічні науки. – 2024. – № 334(5). – С. 418-424.

66. Шматко О. Модель децентралізованої системи обміну електричними медичними картками на основі технології блокчейн / О. Шматко, С. Сальніков // Системи управління, навігації та зв’язку. Збірник наукових праць. – 2024. – Т. 2 (76). – С. 155-162.

67. Big Data в охороні здоров'я: аналіз масивних даних для покращення медичних послуг. [Електронний ресурс]. – URL: https://med-expert.com.ua/news-uk/big-data-v-ohoroni-zdorovya-analiz-masivnih-danih-dlya-pokrashennya-medichnih-poslug.

68. Big data in healthcare: management, analysis and future prospects [Електронний ресурс]. – URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0217-0.

69. CLOUD Computing Services for the Healthcare Industry [Електронний ресурс]. – URL: https://www.innovativearchitects.com/KnowledgeCenter/industry-specific/healthcare-and-cloud-computing.aspx.

70. Darr K. Managing Health Services Organizations and Systems / K. Darr, M. Nowicki. – Baltimore : Health Professions Press, Inc, 2021. – 720 p.

71. Every fifth person in Ukraine has problems with access to essential medicines - Dr. Jarno Habicht, WHO Representative in Ukraine [Електронний ресурс]. – 2023. – URL: https://ukraine.un.org/en/240516-every-fifth-person-ukraine-has-problems-access-essential-medicines-dr-jarno-habicht-who.

72. How is Big Data Helping in the Development of Healthcare? [Електронний ресурс]. – URL: https://www.analyticsvidhya.com/blog/2022/09/how-is-big-data-helping-inthe-development-of-healthcare/.

73. Kraus S. Digital transformation in health care: an analysis of the current state of research [Електронний ресурс] / S. Kraus, F. Schiavone, A. Pluzhnikova, A. S. Invernizzi // Journal of Business Research. – 2021. – № 123. – P. 557-567. – URL: https://doi.org/10.1016/j.jbusres.2020.10.030.

74. Official site «Health Level Seven International (HL7)» [Електронний ресурс]. – URL: http://www.hl7.org.

75. Pramanik P. K. D. Healthcare Big data: A comprehensive overview [Електронний ресурс] / P. K. D. Pramanik, S. Pal, M. Mukhopadhyay // Research anthology on big data analytics, architectures, and applications. – 2022. – P. 119-147. – URL: https://doi.org/10.4018/978-1-5225-7071-4.ch004.

76. Seymour T. Electronic Health Records (EHR) [Електронний ресурс] / T. Seymour, D. Franzvog, T. Greber // American Journal of Health Sciences. – 2012. – 3(3). – P. 201-209. – URL: https://doi.org/10.19030/ajhs.v3i3.7139.

77. The Alphabet Soup of Medical Coding: Decoding ICD, CPT, and HCPCS [Електронний ресурс]. – URL: https://hialearn.com/blog/alphabet-soup-of-medical-coding-icd-cpt-hcpcs.

78. Varkey B. Principles of Clinical Ethics and Their Application to Practice [Електронний ресурс] / B. Varkey // Medical Principles and Practice. – 2021. – № 30(1). – P. 17-28. – URL: https://doi.org/10.1159/000509119.

79. WHO Country Cooperation Strategy, Ukraine 2024–2030 [Електронний ресурс]. – 2024. – URL: https://www.who.int/europe/publications/i/item/WHO-EURO-2024-9329-49101-73236.

80. ZDOROVI на eHealth Summit 2024 [Електронний ресурс]. – URL: https://www.prostir.ua/?news=zdorovi-na-ehealth-summit-2024-tsyfrovizatsiya-medytsyny-v-ukrajini-tryvaje-popry-vyklyky.