УДК 342.951:004.056:614.2
DOI https://doi.org/10.32782/2307-1745.2026.83.5

Донченко О. С.,
доктор філософії в галузі знань
«Публічне управління та адміністрування»,
доцент кафедри публічного управління та права
Навчально-наукового інституту управління
КЗВО «Дніпровська академія неперервної освіти» ДОР
ORCID: https://orcid.org/0000-0002-8654-4572

Ольшанська О. С.,
доктор філософії в галузі знань
«Публічне управління та адміністрування»,
асистент кафедри публічного управління
та адміністрування Інституту права
Державного університету економіки і технологій
ORCID: https://orcid.org/0009-0002-8832-8192

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ МЕДИЧНИХ ДАНИХ ПРИ ВИКОРИСТАННІ ТЕЛЕМЕДИЧНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Анотація. Статтю присвячено комплексному дослідженню правового забезпечення кібербезпеки медичних даних у процесі використання телемедичних технологій в Україні. Актуальність проблематики зумовлена активним розвитком цифрових форм надання медичної допомоги, розширенням обсягів оброблення медичної інформації та необхідністю належного забезпечення її конфіденційності, цілісності й доступності. Метою статті є аналіз чинного нормативно-правового регулювання кібербезпеки медичних даних у телемедичних правовідносинах та визначення напрямів його вдосконалення з урахуванням сучасних європейських підходів. Методологічну основу становлять системний, формально-юридичний, порівняльно-правовий і структурно-функціональний методи, а також аналіз нормативно-правових актів та наукових джерел. Досліджено положення законодавства України у сферах охорони здоров'я, захисту персональних даних, електронного документообігу, інформаційної безпеки та кібербезпеки, що регулюють оброблення медичних даних у телемедичній взаємодії. Встановлено, що чинне законодавство охоплює основні аспекти роботи з медичною інформацією, однак відповідні вимоги закріплені в різних нормативних актах і не формують цілісної моделі її кіберзахисту. Виявлено проблеми у визначенні правового статусу та розподілі обов'язків між учасниками телемедичних правовідносин, зокрема закладами охорони здоров'я, медичними працівниками, адміністратором електронної системи охорони здоров'я та постачальниками цифрових і хмарних сервісів. Визначено недостатньо врегульовані питання контролю доступу, резервування та збереження даних, реагування на кіберінциденти, використання зовнішньої цифрової інфраструктури й транскордонного передавання медичної інформації. Порівняльно-правовий аналіз положень GDPR, EHDS і NIS2 дав змогу визначити європейські підходи, які можуть бути використані як орієнтири для вдосконалення українського регулювання. Особливу увагу приділено підзвітності учасників, управлінню кіберризиками, контролю доступу, повідомленню про інциденти, координації дій та забезпеченню безперервності цифрових медичних сервісів. Обґрунтовано доцільність уточнення розподілу обов'язків між учасниками телемедичної взаємодії та нормативного визначення процедур реагування на кіберінциденти. Практичне значення результатів полягає в можливості їх використання для вдосконалення правового регулювання телемедицини, узгодження вимог різних галузей законодавства та підвищення рівня захисту медичних даних у цифровому середовищі. Результати дослідження також дають підстави розглядати кібербезпеку медичних даних не лише як технічне завдання, а як комплексний правовий механізм, пов'язаний із реалізацією права на приватність, охорону здоров'я та безперервне отримання медичної допомоги. Перспективи подальших досліджень пов'язані з аналізом практики застосування відповідних норм і судової практики.

Ключові слова: телемедицина, персональні дані, електронна система охорони здоров'я, захист інформації, правове регулювання, GDPR, кіберінцидент.

Постановка проблеми. Використання телемедичних технологій трансформує організацію медичної допомоги, оскільки взаємодія пацієнта з медичним працівником здебільшого здійснюється через інформаційно-комунікаційні системи. Це передбачає збирання, передавання, зберігання та обмін інформацією про стан здоров'я, що належить до персональних даних із підвищеним рівнем правового захисту. Відповідно, правове забезпечення кібербезпеки медичних даних є важливою умовою гарантування права на приватність, охорону здоров'я та безперервне отримання медичної допомоги.

Правовий режим медичних даних визначається нормами конституційного, адміністративного, інформаційного та медичного законодавства, а також законодавства про захист персональних даних і кібербезпеку. Його міжгалузевий характер

зумовлює необхідність узгодження правових підстав оброблення даних, порядку доступу до них, обов'язків і відповідальності закладів охорони здоров'я, медичних працівників, адміністраторів інформаційних систем, постачальників цифрових послуг та інших залучених суб'єктів. Це актуалізує питання узгодженості нормативних вимог і виявлення прогалин у правовому регулюванні.

Додаткової актуальності проблемі надає наближення законодавства України до права Європейського Союзу у сферах захисту персональних даних і кібербезпеки. Регламент (ЄС) 2016/679 (GDPR) [1], Регламент (ЄС) 2025/327 про Європейський простір медичних даних [2] та Директива (ЄС) 2022/2555 [3] визначають сучасні підходи до захисту медичних даних, розподілу обов'язків між учасниками їх оброблення та управління кіберризиками. Порівняння цих положень із законодавством України дає змогу оцінити його відповідність європейським підходам, виявити проблемні аспекти та визначити напрями подальшого вдосконалення.

Стан дослідження. Наукові дослідження правового регулювання телемедичних технологій охоплюють питання цифровізації охорони здоров'я, захисту персональних даних, функціонування електронних медичних систем та кібербезпеки цифрової інфраструктури. Українські автори переважно аналізують нормативні засади цифровізації охорони здоров'я та реалізації права на медичну допомогу із застосуванням інформаційно-комунікаційних технологій. Зокрема, О. Капітан та Х. Дідух розкривають конституційно-правові засади реалізації права на медичну допомогу в умовах цифровізації та розвиток телемедицини в Україні, акцентуючи на взаємозв'язку права на охорону здоров'я, приватність та використання електронних інформаційних ресурсів [4].

У зарубіжних дослідженнях увага зміщується до правового захисту чутливих даних і кібербезпеки цифрової медицини. Так, Г. Малджієрі обґрунтовує диференційований підхід до захисту персональних даних залежно від їх чутливості, пов'язаних ризиків та вразливості суб'єкта [5]. Взаємозв'язок вимог до безпеки медичних технологій, захисту персональних даних і кібербезпеки розглядають Е. Бізін та колеги, наголошуючи на необхідності комплексного правового підходу до цифрової медичної екосистеми [6]. На ризики для конфіденційності та захисту інформації звертають увагу А. Джат та Т.-М. Грьонлі, аналізуючи застосування мобільних технологій для дистанційного моніторингу пацієнтів [7].

Важливе значення для формування нормативної основи дослідження мають документи ВООЗ, матеріали European Union Agency for Cybersecurity (ENISA) [8], а також положення GDPR, Регламенту (ЄС) 2025/327 про Європейський простір медичних даних [2] та Директиви (ЄС) 2022/2555 [3], які визначають сучасні підходи до захисту медичних даних, кібербезпеки та розподілу відповідальності між учасниками їх оброблення.

Водночас у науковій літературі недостатньо системно розглянуто взаємозв'язок правового режиму медичних даних, захисту персональних даних і кібербезпеки саме в умовах телемедичної взаємодії в Україні. Потребують подальшого уточнення правові обов'язки основних учасників оброблення медичних даних та узгодження вимог законодавства про охорону здоров'я, персональні дані, інформаційну безпеку і кібербезпеку. Саме на комплексному аналізі цих питань зосереджене це дослідження.

Мета статті полягає в комплексному аналізі правового забезпечення кібербезпеки медичних даних під час використання телемедичних технологій в Україні та розробленні пропозицій щодо його вдосконалення з урахуванням сучасних європейських підходів.

Виклад основного матеріалу. Правовий аналіз телемедичних правовідносин потребує розмежування основних юридичних категорій. Медичні дані охоплюють інформацію, створену або використану під час надання медичної допомоги, тоді як дані про здоров'я належать до спеціальної категорії персональних даних відповідно до Закону України «Про захист персональних даних» та Регламенту (ЄС) 2016/679 [9; 1]. Телемедицина визначає організаційну форму дистанційної взаємодії пацієнта, медичного працівника та інших учасників надання медичної допомоги.

Водночас необхідно розмежовувати захист персональних даних і кібербезпеку. Перший визначає законність оброблення інформації та права суб'єкта даних, друга – вимоги до конфіденційності, цілісності й доступності інформаційних систем. Кіберінцидент є подією, що порушує або створює загрозу функціонуванню систем електронних комунікацій або управління технологічними процесами та потребує передбаченого законом реагування [10; 11].

Правове регулювання телемедицини поєднує два взаємопов'язані блоки, зокрема Закон України «Про захист персональних даних» [9] і GDPR [1] визначають правила оброблення медичних даних та права їх суб'єктів, тоді як Закон України «Про основні засади забезпечення кібербезпеки України» [11] і Директива (ЄС) 2022/2555 (NIS2) [3] регулюють захист цифрової інфраструктури, кіберризики та реагування на інциденти. Таким чином, один блок забезпечує правомірність оброблення даних, а інший – безпеку цифрового середовища.

Практика Європейського суду з прав людини (далі – ЄСПЛ) у справах I v. Finland та L. H. v. Latvia пов'язує захист медичної інформації з гарантіями статті 8 Конвенції та необхідністю ефективного контролю доступу до таких даних [12; 13]. Конституція України також формує загальну основу їх захисту через гарантії права на приватне життя, охорону здоров'я та інформацію [14]. Водночас для телемедичних правовідносин необхідним залишається узгодження цих гарантій зі спеціальними нормами про конфіденційність медичної інформації, персональні дані та кібербезпеку.

Спеціальне законодавство у сфері охорони здоров'я конкретизує конституційні гарантії, визначаючи права пацієнтів, обов'язки медичних працівників і вимоги до конфіденційності інформації про стан здоров'я. Правові засади телемедицини та електронної системи охорони здоров'я визначено спеціальними нормативними актами [15–18]. Водночас традиційна модель медичної таємниці орієнтована переважно на взаємодію пацієнта й медичного працівника, а телемедицина передбачає цифрове оброблення даних із залученням додаткових суб'єктів і технологічних посередників. Це потребує чіткого розподілу прав, обов'язків і відповідальності учасників цифрового обміну медичними даними.

Закон України № 3301-IX визначає телемедицину як спосіб організації надання медичної допомоги та встановлює засади дистанційної взаємодії між пацієнтом і медичним працівником [16]. Організаційні форми телемедичного консультування та інформаційної взаємодії регламентує наказ МОЗ України № 681,

а функціонування електронної системи охорони здоров'я та обіг електронних медичних записів – постанова Кабінету Міністрів України № 411 [17; 18].

Водночас чинне регулювання переважно зосереджене на організації телемедичної допомоги та інформаційному обміні, залишаючи недостатньо врегульованими питання кібербезпеки медичних даних. Зокрема, потребують чіткішого визначення обов'язки учасників щодо запобігання кіберінцидентам, повідомлення про порушення безпеки, реагування на несанкціонований доступ і відновлення даних. З огляду на це, подальше вдосконалення телемедичного регулювання має передбачати його узгодження з вимогами законодавства про захист персональних даних і кібербезпеку.

Особливе значення для телемедичних правовідносин має Закон України «Про захист персональних даних», який визначає підстави оброблення персональних даних, права їх суб'єктів та обов'язки власників і розпорядників [9]. Водночас українське законодавство не забезпечує такого рівня деталізації процедур захисту медичних даних, як GDPR, зокрема щодо безпеки оброблення, повідомлення про порушення та відповідальності відповідних суб'єктів. Для телемедицини це особливо важливо, оскільки медичні дані послідовно обробляються пацієнтом, медичним працівником, закладом охорони здоров'я та інформаційними системами. Недостатня визначеність розподілу обов'язків між ними може ускладнювати реагування на витоки й несанкціонований доступ та свідчить про необхідність узгодження вимог захисту персональних даних із вимогами кібербезпеки.

Закони України «Про електронні документи та електронний документообіг» і «Про електронну ідентифікацію та електронні довірчі послуги» забезпечують юридичну значущість електронних документів та ідентифікацію учасників цифрової взаємодії [19; 20]. Водночас питання кіберзахисту медичних даних регулюються іншими нормативними актами, що зумовлює фрагментарність правового регулювання. Закон України «Про захист інформації в інформаційно-комунікаційних системах» встановлює загальні вимоги до захисту інформації в електронному середовищі, але не формує спеціальної моделі кіберзахисту медичних даних у телемедичних сервісах [21].

Загальні засади кіберзахисту, управління ризиками та реагування на кіберінциденти визначає Закон України «Про основні засади забезпечення кібербезпеки України» [11]. Для телемедицини його положення мають особливе значення, оскільки порушення роботи Електронної системи охорони здоров'я (далі – ЕСОЗ) може впливати на доступність медичної документації та безперервність надання допомоги. Відповідні підходи узгоджуються з рекомендаціями ENISA та Всесвітньої організації охорони здоров'я щодо кібербезпеки цифрової медичної інфраструктури [8; 22].

Проведений аналіз засвідчує, що чинне законодавство регулює основні етапи оброблення медичних даних. Водночас розподіл юридичних обов'язків між учасниками телемедичної взаємодії залишається недостатньо узгодженим, особливо щодо використання хмарних сервісів, транскордонного передавання даних і реагування на кіберінциденти. Для систематизації виявлених вимог і нормативних прогалин розроблено авторську матрицю правового забезпечення кібербезпеки медичних даних у телемедицині (табл. 1).

Побудована матриця засвідчує, що більшість етапів життєвого циклу медичних даних охоплена українським законодавством, однак відповідні вимоги розподілені між різними нормативними актами. Найбільші прогалини стосуються використання хмарної інфраструктури, транскордонного передавання даних, реагування на кіберінциденти та розподілу відповідальності між учасниками цифрової взаємодії.

Українське законодавство і GDPR мають спільну мету – захист персональних даних, проте відрізняються рівнем деталізації. Закон України «Про захист персональних даних» визначає загальні засади оброблення інформації, права суб'єктів даних та обов'язки володільців і розпорядників [9]. GDPR доповнює ці положення принципом підзвітності, вимогами до безпеки оброблення та відповідальності суб'єктів, формуючи більш цілісну модель захисту даних [23]. Для телемедицини це особливо важливо через використання хмарних сервісів,

Таблиця 1

Матриця правового забезпечення кібербезпеки медичних даних у телемедицині

Етап і правова вимога	Відповідальні суб'єкти	Виявлена прогалина	Пропозиція
Одержання: законне одержання даних	ЗОЗ; лікар	Відсутній єдиний порядок інформування	Уніфікувати електронне інформування
Ідентифікація: ідентифікація користувача	Лікар; адміністратор ЕСОЗ	Неповне регулювання автентифікації	Уніфікувати вимоги до автентифікації
Передавання: забезпечення конфіденційності й цілісності	ЗОЗ; адміністратор ЕСОЗ	Відсутні спеціальні правила для платформ	Установити правила передавання даних
Зберігання: захист і зберігання даних	ЗОЗ; хмарний провайдер	Неповне регулювання використання хмар	Урегулювати використання хмарних сервісів
Доступ: контроль доступу	ЗОЗ; адміністратор ЕСОЗ	Неуніфіковані ролі користувачів	Уніфікувати управління доступом
Журналювання: фіксація дій користувачів	Адміністратор ЕСОЗ	Не визначено строки журналювання	Визначити правила і строки журналювання
Резервування: резервне копіювання	ЗОЗ; хмарний провайдер	Не врегульовано резервування	Урегулювати резервне копіювання
Кіберінцидент: повідомлення про інцидент	ЗОЗ; адміністратор ЕСОЗ	Неузгоджені процедури повідомлення	Запровадити спеціальний порядок реагування
Відновлення: відновлення системи	Адміністратор ЕСОЗ; ЗОЗ	Відсутня єдина процедура відновлення	Уніфікувати порядок відновлення
Видалення: видалення даних	ЗОЗ	Неузгоджені строки видалення	Узгодити правила видалення даних

Примітка:. ЗОЗ – заклад охорони здоров'я; ЕСОЗ – електронна система охорони здоров'я.

Джерело: складено авторами на основі [9; 18; 20; 21].

платформ дистанційного консультування та інших цифрових рішень.

Подальший розвиток європейського регулювання пов'язаний з EHDS, який деталізує правила використання медичних даних, обміну електронними медичними записами, функції учасників цифрової медичної екосистеми та вимоги до інтероперабельності інформаційних систем [24–26]. В Україні відповідні механізми також передбачені, однак залишаються розподіленими між різними нормативними актами, що ускладнює їх системне застосування в телемедицині.

Важливим доповненням до правил захисту даних є Директива (ЄС) 2022/2555 (NIS2), яка встановлює комплексні вимоги до кіберстійкості, зокрема управління кіберризиками, контролю доступу, резервування, безперервності діяльності, реагування на інциденти та державного нагляду [3]. Українське законодавство містить загальні вимоги щодо кібербезпеки, проте спеціальні процедури реагування на інциденти в телемедичних сервісах, координації учасників та відновлення цифрової інфраструктури залишаються недостатньо деталізованими.

Отже, українська модель містить базові механізми захисту медичних даних, але потребує їх системного узгодження. Пріоритетними напрямами вдосконалення є чіткіший розподіл відповідальності між учасниками телемедичної взаємодії, визначення вимог до використання зовнішніх і хмарних сервісів, запровадження узгоджених процедур повідомлення про кіберінциденти та відновлення цифрових сервісів, а також удосконалення правил транскордонного передавання медичних даних з урахуванням підходів GDPR, EHDS і NIS2.

Результати дослідження дають підстави запропонувати узгодження законодавства у сферах охорони здоров'я, інформації, захисту персональних даних і кібербезпеки шляхом формування єдиної моделі розподілу обов'язків між учасниками телемедичних правовідносин. Такий підхід сприятиме чіткому визначенню їхньої відповідальності, удосконаленню правового регулювання та підвищенню стійкості електронної системи охорони здоров'я. На основі виявлених нормативних взаємозв'язків і прогалин розроблено багаторівневу модель правового забезпечення кібербезпеки медичних даних у телемедицині, що відображає взаємодію основних правових, організаційних і технічних елементів цієї системи (рис. 1).

На рисунку представлено авторську модель взаємозв'язку правових елементів, що забезпечують кібербезпеку медичних даних у телемедичних правовідносинах. Її центральним елементом є права пацієнта, реалізацію яких забезпечують учасники телемедичної взаємодії через виконання організаційних і технічних обов'язків, державний нагляд та правові механізми реагування на кіберінциденти. Модель демонструє, що кібербезпека медичних даних забезпечується комплексною взаємодією кількох взаємопов'язаних правових режимів. Її практичне значення полягає у визначенні основних напрямів удосконалення правового регулювання телемедичної взаємодії, насамперед щодо розподілу обов'язків, реагування на кіберінциденти та забезпечення безперервності цифрових медичних послуг.

Висновки. Проведене дослідження засвідчило, що правове забезпечення кібербезпеки медичних даних у телемедицині в Україні ґрунтується на нормах законодавства про охорону здоров'я, персональні дані, інформацію та кібербезпеку. Водночас відповідні вимоги закріплені в різних нормативних актах і не формують цілісної моделі кіберзахисту медичних даних.

Виявлено прогалини у визначенні правового статусу та розподілі обов'язків учасників телемедичної взаємодії, а також у регулюванні контролю доступу, резервування даних, реагування на кіберінциденти, використання хмарних сервісів і транскордонного передавання медичної інформації.

Порівняльний аналіз засвідчив, що підходи GDPR, EHDS і NIS2 можуть слугувати орієнтирами для вдосконалення українського законодавства. Передусім потребують уточнення розподіл обов'язків учасників, процедури реагування на кібер-



Рис. 1. Багаторівнева модель правового забезпечення кібербезпеки медичних даних у телемедицині

Джерело: сформовано авторами

інциденти та вимоги до безпечного використання цифрової інфраструктури.

Перспективи подальших досліджень пов'язані з аналізом практики застосування відповідних норм, судової практики та правового регулювання нових телемедичних сервісів.

Література:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 05.08.2026).
2. Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space (EHDS). URL: https://eur-lex.europa.eu/eli/reg/2025/327/oj (дата звернення: 05.08.2026).
3. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj (дата звернення: 05.08.2026).
4. Капітан О. І., Дідух Х. В. Конституційно-правові засади реалізації права на медичну допомогу в умовах цифровізації: досвід впровадження телемедицини в Україні. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2026. № 1(93). С. 239–246. DOI: https://doi.org/10.24144/2307-3322.2026.93.1.35.
5. Malgieri G. Vulnerability and Data Protection Law. Oxford: Oxford University Press, 2023. DOI: https://doi.org/10.1093/oso/9780192870339.001.0001.
6. Biasin E., Kamenjašević E., Ludvigsen K. R. Cybersecurity of AI Medical Devices: Risks, Legislation, and Challenges. In: Barfield W., Pagallo U. (eds.). Research Handbook on Health, AI and the Law. Cheltenham: Edward Elgar Publishing, 2024. P. 57–74. DOI: https://doi.org/10.4337/9781802205657.ch04.
7. Jat A. S., Grønli T. M. Harnessing the Digital Revolution: A Comprehensive Review of mHealth Applications for Remote Monitoring in Transforming Healthcare Delivery. In: International Conference on Mobile Web and Intelligent Information Systems. Cham: Springer Nature Switzerland, 2023. P. 55–67. DOI: https://doi.org/10.1007/978-3-031-39764-6_4.
8. Cybersecurity in Healthcare. *ENISA: вебсайт*. URL: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/health (дата звернення: 05.08.2026).
9. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17 (дата звернення: 05.08.2026).
10. Luidold C., Jungbauer C. Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. Frontiers in Medicine. 2024. Vol. 11. DOI: https://doi.org/10.3389/fmed.2024.1379852.
11. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.08.2026).
12. Case of I v. Finland (Application No. 20511/03): Judgment of the European Court of Human Rights of 17 July 2008. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-87510 (дата звернення: 05.08.2026).
13. Case of L.H. v. Latvia (Application No. 52019/07): Judgment of the European Court of Human Rights of 29 April 2014. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-144584 (дата звернення: 05.08.2026).
14. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 05.08.2026).
15. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12 (дата звернення: 05.08.2026).
16. Про внесення змін до деяких законодавчих актів України щодо функціонування телемедицини: Закон України від 09.08.2023 № 3301-IX. URL: https://zakon.rada.gov.ua/laws/show/3301-20 (дата звернення: 05.08.2026).
17. Про затвердження нормативних документів щодо застосування телемедицини у сфері охорони здоров'я наказ Міністерства охорони здоров'я України від 19.10.2015 № 681. URL: https://zakon.rada.gov.ua/laws/show/z1400-15 (дата звернення: 05.08.2026).
18. Деякі питання електронної системи охорони здоров'я: постанова Кабінету Міністрів України від 25.04.2018 № 411. URL: https://zakon.rada.gov.ua/laws/show/411-2018-п (дата звернення: 05.08.2026).
19. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 05.08.2026).
20. Про електронну ідентифікацію та електронні довірчі послуги: Закон України № 2155-VIII. Редакція від 18.12.2024. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 05.08.2026).
21. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр (дата звернення: 05.08.2026).
22. Global Strategy on Digital Health 2020-2025. World Health Organization. Geneva: World Health Organization, 2021. URL: https://www.who.int/publications/i/item/9789240020924 (дата звернення: 05.08.2026).
23. Casarosa F. European Health Data Space – Is the Proposed Certification System Effective against Cyber Threats? European Journal of Risk Regulation. 2024. Vol. 15, № 4. P. 939–949. DOI: https://doi.org/10.1017/err.2024.25.
24. Proso M. Digital Transformation of Health: Towards the European Health Data Space. Medicine, Law & Society. 2024. Vol. 17. № 1. P. 153–170. DOI: https://doi.org/10.18690/mls.17.1.153-170.2024.
25. Rak R. Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the Secondary Use of Electronic Health Data in the European Health Data Space (EHDS). European Journal of Risk Regulation. 2024. Vol. 15, № 4. P. 928–938. DOI: https://doi.org/10.1017/err.2024.67.
26. Dove E. S. The European Health Data Space as a Case Study. Ethics & Human Research. 2024. Vol. 46, № 6. P. 29–35. DOI: https://doi.org/10.1002/eahr.500228.

Donchenko O., Olshanska O. Legal framework for cybersecurity of medical data in the use of telemedicine technologies in Ukraine

Summary. The article provides a comprehensive analysis of the legal framework for ensuring the cybersecurity of medical data in the use of telemedicine technologies in Ukraine. The relevance of the study is determined by the rapid development of digital forms of healthcare delivery, the increasing volume of medical information processing, and the need to ensure the confidentiality, integrity, and availability of such information. The aim of the article is to analyze the current legal regulation of medical data cybersecurity in telemedicine relationships and identify areas for its improvement in light of contemporary European approaches. The methodological framework comprises systemic, formal-legal, comparative-legal, and structural-functional methods, as well as the analysis of legal acts and scholarly sources. The study examines Ukrainian legislation in the areas of healthcare, personal data protection, electronic document

management, information security, and cybersecurity governing the processing of medical data in telemedicine interactions. It is established that current legislation covers the main aspects of handling medical information; however, the relevant requirements are set out in different legal acts and do not constitute a comprehensive model for its cybersecurity protection. Problems have been identified concerning the legal status and allocation of responsibilities among participants in telemedicine relationships, including healthcare institutions, healthcare professionals, the administrator of the electronic healthcare system, and providers of digital and cloud services. Insufficiently regulated issues include access control, data backup and storage, response to cyber incidents, the use of external digital infrastructure, and the cross-border transfer of medical information. A comparative legal analysis of the GDPR, EHDS, and NIS2 has made it possible to identify European approaches that may serve as benchmarks for improving Ukrainian regulation. Particular attention is paid to accountability of the participants, cyber risk management, access control, incident notification, coordination of actions, and ensuring the continuity of digital healthcare services. The study substantiates the need to clarify the allocation of responsibilities among participants in telemedicine relationships and establish regulatory procedures for responding to cyber incidents. The practical significance of the findings lies in their potential application to improve the legal regulation of telemedicine, harmonize requirements across different areas of legislation, and strengthen the protection of medical data in the digital environment. The findings also support the understanding of medical data cybersecurity not merely as a technical task but as a comprehensive legal mechanism associated with the exercise of the rights to privacy, healthcare, and continuous access to medical care. Further research should focus on the application of the relevant legal provisions and judicial practice.

Key words: telemedicine, personal data, electronic healthcare system, information protection, legal regulation, GDPR, cybersecurity incident.

Використання штучного інтелекту. Під час підготовки статті інструменти штучного інтелекту використовувалися виключно для мовного редагування, перевірки граматики, перекладу або інших допоміжних завдань, без використання згенерованих ними об'єктів як результатів академічної діяльності.

Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Дата першого надходження статті до видання: 06.09.2026
Дата прийняття статті до друку після рецензування: 11.10.2026
Дата публікації (оприлюднення) статті: 09.11.2026