УДК: 342.77:614:004.738.5
DOI https://doi.org/10.24144/2788-6018.2022.06.39

ПРАВОВІ АСПЕКТИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ У ТЕЛЕМЕДИЦИНІ

Ілюшик О.М.,
кандидат юридичних наук, доцент,
доцент кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ

Ярема О.Г.,
кандидат юридичних наук, доцент,
доцент кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ
https://orcid.org 0000-0002-4619-5785

Ілюшик О.М., Ярема О.Г. Правові аспекти електронного документообігу у телемедицині.

У статті з позиції теорії адміністративного та інформаційного права розглянуто, на основі чинного законодавства та нормативних вимог Європейського Союзу, теоретичні та практичні аспекти електронного документообігу у телемедицині. Актуальність теми зумовлена необхідністю удосконалення законодавства з метою комплексного теоретичного обґрунтування підвищення ефективності діяльності у сфері телемедицини в умовах цифрової трансформації України. У ході дослідження застосовано методологію системного комплексного аналізу правових явищ із застосуванням факторного та еволюційного методів дослідження. Вказано, що у країнах Європейського Союзу сформувалися три основні моделі інформаційних систем охорони здоров'я, що розрізняються за способами зберігання медичної інформації та управління: децентралізована, централізована та пацієнт-орієнтована. Зазначено, основні правові питання оновлення медичної системи України та напрями діяльності в умовах реформування охоплюють телемедицину, та її складову – електронний документообіг. Уточнено сутність та особливості електронний документообіг в телемедицині в країнах Європейського Союзу. Розглянуто електронні системи охорони здоров'я окремих країн Європейського Союзу приділено увагу досвіду щодо використання. Досліджено стан правового забезпечення інформаційної безпеки в телемедицині щодо електронного документообігу з урахуванням досвіду країн Європейського Союз. Проведено аналіз забезпечення інформаційної безпеки у контексті персональних даних в медичних системах європейських країн та в Україні. Визначено подальший вектор та напрям розвитку національної системи охорони здоров'я в розрізі Концепції розвитку електронної охорони здоров'я, що має значення для медичного обслуговування та реабілітації громадян, які постраждали в насадок війни. Виділено важливі аспекти та заходи оптимізації діяльності у сфері телемедицини на які потрібно звернути увагу при подальшому реформуванні та створенні нових цифрових ресурсів для більш комфортнішого переходу та використання новітніх цифрових технологій в сфері охорони здоров'я.

Ключові слова: телемедицина, інформаційна безпека, електронні системи, медична діяльність, персональні дані.

Ilyushyk O.M., Yarema O. Legal aspects of electronic document management in telemedicine.

In the article from the standpoint of the theory of administrative and information law, based on the current legislation and regulatory requirements of the European Union, the theoretical and practical aspects of electronic document flow in telemedicine are considered. The topicality of the topic determined by the need to improve the legislation with the aim of comprehensive theoretical justification of increasing the effectiveness of telemedicine activities in the conditions of digital transformation of Ukraine. In the course of the study, the methodology of a systematic complex analysis of legal phenomena was applied using factorial and evolutionary methods of research. It is indicated that in the countries of the European Union, three main models of health care information systems have been formed, which differ in the ways of storing medical information and management: decentralized, centralized and patient-oriented. It was noted that the main legal issues of the renewal of the medical system of Ukraine and the directions of activity in the conditions of reform include telemedicine, and its component - electronic document flow. The essence and features of electronic document management in telemedicine in the countries of the European Union have

been clarified. The electronic health care systems of individual countries of the European Union considered, attention is paid to the experience of use. The state of legal provision of information security in telemedicine with regard to electronic document flow studied, taking into account the experience of the countries of the European Union. The analysis of ensuring information security in the context of personal data in the medical systems of European countries and Ukraine was carried out. The further vector and direction of the development of the national health care system in terms of the Concept of the development of electronic health care, which is important for medical care and rehabilitation of citizens who suffered during the war, was determined. Important aspects and measures to optimize activities in the field of telemedicine highlighted, which need to be paid attention to during further reform and creation of new digital resources for a more comfortable transition and use of the latest digital technologies in the field of health care.

Key words: telemedicine, information security, electronic systems, medical activity, personal data.

Постановка проблеми. Право на охорону здоров'я та медичну допомогу в цифрову епоху наповнюється новим змістом та набуває додаткових гарантій його реалізації. Сучасні гарантії цього права сприяють забезпеченню рівного доступу до медичної допомоги, підвищенню якості охорони здоров'я за рахунок дистанційного характеру взаємодії, автоматизованого оброблення медичної інформації, персоналізації медичної допомоги.

Стан опрацювання проблематики. Аналіз проблем правовідносин у сфері охорони здоров'я, у тому числі щодо електронного документообігу здійснювали науковці різних галузей правознавства, з-поміж яких особливо помітними праці: Ю. Бисаги, С. Булеци, Т. Волинець, А. Герц, В. Галая, З. Гладуна, О. Дроздової, С. Дутчак, О. Клименко, Ю. Козаченка, В. Кондратенка, С. Коханчук, О. Люблинець, Р. Майданика, Я. Марко, О. Паровишника, О. Прасова, Д. Пугача, І. Сенюти, Г. Слабкого, Є. Соболя, Р. Стефанчука, В. Стеценко, С. Стеценка, А. Суббота, Т. Тихомирова, Ю. Турянського, Я. Триньова, І. Шатковської, Я. Шатковськогота ін.

Розвиток інформаційних технологій прискорює технічний прогрес, що вимагає дослідження у сфері правового регулювання.

Метою статті є дослідження правових аспектів електронного документообігу у телемедицині.

У країнах Європейського Союзу сформувалися три основні моделі інформаційних систем охорони здоров'я, що розрізняються за способами зберігання медичної інформації та управління: децентралізована, централізована та пацієнт-орієнтована.

Децентралізована модель передбачає зберігання персональних записів про здоров'я пацієнтів та управління ними на локальному рівні. У Бельгії інформація про пацієнтів в електронному вигляді зберігається на локальних серверах кожного провайдера медичних послуг [1]. Взаємодія локальних систем здійснюється через центрального оператора (національний пункт обміну інформацією). Сукупність усіх інформаційних систем, механізмів їхньої взаємодії, інструментів управління складають національну платформу електронної охорони здоров'я Бельгії.

Централізована модель установи інформаційних систем охорони здоров'я заснована на централізованому зберіганні медичних даних та управлінні ними. Така модель застосована у скандинавських країн. У Фінляндії ухвалено Закон «Про систему електронних записів про здоров'я», на підставі якого засновано національний архів електронних записів про здоров'я пацієнтів [2]. Оператором архіву є агентство соціального страхування Фінляндії. Згідно законодавства Фінляндії всі установи сфери охорони здоров'я, публічні та приватні, повинні брати участь у національній системі електронних записів про здоров'я.

Третя модель, умовно звана пацієнт-орієнтованою, набула розвитку у Франції. У цій моделі пацієнт обирає оператор хостингу, який здійснює зберігання персональної інформації про здоров'я. Відповідно до Кодексу охорони здоров'я Франції оператори хостингу, які здійснюють обробку персональної інформації про здоров'я пацієнтів, повинні пройти процедуру акредитації в державному органі [3]. Оператори хостингу повинні відповідати вимогам професіоналізму, мати надійну безпекову політику, дотримуватися конфіденційності зобов'язані надавати медичним установам, до яких вони звертаються, доступ до персональних електронних записів про здоров'я.

Усі розглянуті вище моделі установи інформаційних систем охорони здоров'я мають свої переваги та недоліки. Централізована модель є зручною для оперативної інформаційної взаємодії суб'єктів медичної діяльності, однак таїть більш високий ступінь уразливості з точки зору захисту персональних даних. Інші моделі більшою мірою відповідають цілям забезпечення інформаційної безпеки, але створюють більше перешкод для інформаційної взаємодії.

Децентралізоване зберігання відомостей зовсім не гарантує абсолютну безпеку, а порушення безпеки навіть на одному з елементів

розподіленої системи може завдати істотних збитків суб'єктам телемедичної діяльності.

Правове регулювання країн Європейського Союзу у галузі електронної охорони здоров'я в останні роки демонструє тенденцію до більшої централізації та одночасного підвищення ролі пацієнта в установи інформаційних систем охорони здоров'я [4, с. 25]. У Франції організовано централізоване зберігання даних, але збереглися права пацієнтів щодо управління персональними записами про здоров'я. Такі тенденції простежуються у законодавстві інших країн. У зарубіжній літературі неоднозначно оцінюється ідея централізованого зберігання електронних записів здоров'я. Серед недоліків централізованого зберігання в доктрині відзначаються більш високі ризики порушення конфіденційності та витоку інформації, але й складності в управлінні доступом до записів про здоров'я на локальному рівні.

Третій компромісний підхід передбачає координацію інформаційних систем охорони здоров'я з централізованим зберіганням не всіх медичних даних, а тих, які необхідні для виконання координуючої функції, тоді як основний масив даних зберігається децентралізовано, але забезпечується доступ і обмін даних.

Такий підхід є найбільш зваженим, оскільки він дозволяє оптимізувати ризики інформаційної безпеки за рахунок розподіленого зберігання даних, враховувати потреби конкретних установ, забезпечує умови для координації діяльності медичних установ та оперативного обміну інформацією.

Досвід країн ЄС демонструє велику увагу до розвитку інформаційних систем охорони здоров'я, їх поширення та широкого використання. У всіх країнах усвідомлюється необхідність подальшого вдосконалення правових і технічних аспектів, пов'язаних з функціонуванням інформаційних систем, з метою адаптації до сучасних телемедичних технологій.

У країнах ЄС не сформовано єдиного підходу до установи інформаційних систем охорони здоров'я, проте простежується стримана тенденція до централізації інформаційних систем, широкого впровадження електронних записів про здоров'я та забезпечення пацієнтів доступом до персональних електронних записів про здоров'я.

У Україні з року розвивається Електронна система охорони здоров'я (далі – ЕСОЗ) [5]. Відповідно Закон України «Про основи законодавства України про охорони здоров'я» в інформаційних системах у сфері охорони здоров'я здійснюються збір, зберігання, обробка та надання інформації про органи, установи державної, муніципальної та приватної систем охорони здоров'я та про здійснення медичної та іншої діяльності у сфері охорони здоров'я [6].

Законодавство Україні передбачає можливість взаємодії інших інформаційних систем з інформаційними системами у сфері охорони здоров'я та медичними організаціями. Порядок такої взаємодії встановлено Кабінетом Міністрів Україні відповідно до Концепції розвитку електронної охорони здоров'я [7].

Всі зазначені інформаційні системи охорони здоров'я, включаючи інші інформаційні системи, утворюють Електронну систему охорони здоров'я. Порядок доступу до інформації, що міститься в ній, порядок та строки подання інформації в єдину систему, порядок обміну інформацією з використанням системи та низку інших правових питань встановлені Кабінетом Міністрів Україні у Порядку функціонування електронної системи охорони здоров'я [5].

Зі змісту правових актів, що регламентують порядок створення та функціонування ЕСОЗ, можна зробити висновок, що в України формується централізована модель інформаційних систем, яка не передбачає зберігання всієї інформації у сфері охорони здоров'я на єдиному сервері. ЕСОЗ виступає як інфраструктурна платформа та координатор інформаційної взаємодії.

Централізований характер управління інформаційними системами охорони здоров'я дозволяє забезпечити оперативний інформаційний обмін у системі та з зовнішніми користувачами та постачальниками інформації. Така організація інформаційних систем охорони здоров'я є оптимальною, оскільки забезпечує зберігання даних переважно на серверах постачальників інформації з передачею даних у центральний сервер тільки в обсязі, які необхідні для досягнення загальних цілей та виконання функцій оператора ЕСОЗ.

Захист конфіденційної інформації потребує комплекс правових і технічних заходів. Рівні безпеки та співвідношення цих заходів залежать від багатьох факторів: обсягу даних, ступеня чутливості даних, кількості осіб, які мають доступ до даних, добровільності або обов'язковості передачі даних в обробку, динамізму чи статичності даних, що зберігаються в базі. Впровадження інформаційних технологій у різні сфери суспільного життя, включаючи охорону здоров'я, ставить перед суспільством нові виклики і вимагає розробки нових підходів до забезпечення інформаційної безпеки.

Природа інформаційних систем, що використовуються в телемедицини та характер медичної діяльності потребує застосування складної моделі інформаційної безпеки, оскільки всі три фактори: зберігання чутливої інформації в єдиному віртуальному просторі змінює харак-

тер потенційної шкоди від витоку відомостей; зберігання персональних даних на паперових носіях у різних місця; захист даних у віртуальному просторі потребує заходів інформаційної безпеки – конфіденційності, цілісності і доступності [8, с. 119].

Одночасне забезпечення конфіденційності та доступності інформації пов'язане з низкою додаткових складнощів. В інформаційному суспільстві, в умовах розвитку медицини, важливу роль у забезпеченні інформаційної безпеки відіграють технічні засоби захисту, оскільки великі обсяги інформації, наявність великої кількості задіяних в інформаційному обміні суб'єктів, дистанційний характер взаємодії та інші фактори абстрагують потенційних порушників і потенційних постраждалих осіб.

Захист баз даних, на відміну захисту конкретної інформації, отриманої медичним працівником від пацієнта, меншою мірою пов'язані з міжособистісними відносинами, які успішніше регулюються етико-правовими нормами. За всієї важливості технічних засобів без правових заходів неможливо забезпечити конфіденційність даних, що обробляються в інформаційних системах. Існують ризики недбалого ставлення працівників до дотримання конфіденційності інформації, ризики порушення правил експлуатації інформаційних систем.

Застосування технічних заходів потребує правової регламентації. До засобів забезпечення інформаційної безпеки електронного документообігу в медичній галузі належать: процедури ідентифікації та автентифікації суб'єктів телемедичних відносин; розмежування прав доступу до записів про стан здоров'я; шифрування переданих даних; анонімність та псевдо анонімність даних; безпека IT-інфраструктури, угоди про інформаційний обмін із закріпленням обов'язків щодо забезпечення інформаційної безпеки.

Дистанційний характер телемедицини потребує установи належної ідентифікації та автентифікації суб'єктів відносин. Пацієнт, якому надається дистанційна медична послуга, має бути впевненим у особистості лікаря та його професійної кваліфікації. Лікар повинен переконатися, що він надає медичну допомогу певній особі.

Типову для інформаційних відносин проблему ідентифікації та автентифікації суб'єктів вирішується через використання електронних підписів, Єдиного державного демографічного реєстру та надання інформації, взаємодії між уповноваженими суб'єктами, здійснення ідентифікації та верифікації [9].

Документування інформації про надання медичної допомоги пацієнту із застосуванням телемедичних технологій здійснюється з використанням кваліфікованого електронного підпису медичного працівника. На рівні підзаконного нормативного регулювання необхідно встановити технологічно нейтральні вимоги до таких способів ідентифікації та автентифікації, що забезпечують надійність та достовірність, а також технічну можливість інтеграції відомостей про пацієнтів у ЕСОЗ.

Розширені способи ідентифікації та автентифікації повинні використовуватися для надання поінформованої згоди на медичне втручання, інакше будуть збережені чинні законодавчі бар'єри для дистанційної взаємодії при наданні медичної допомоги із застосуванням телемедичних технологій.

У літературі пропонується використати трьох факторну автентифікацію фізичних осіб – суб'єктів телемедичних відносин. При такій автентифікації використовуються три ключі: пароль, смарт-карта та біометричні дані. Такий підхід до автентифікації є найбільш надійним, може бути рекомендований до використання учасниками інформаційної взаємодії.

Встановлення подібних вимог до автентифікації як загальнообов'язкових при наданні медичних послуг створить правові та технічні бар'єри, що не відповідає меті широкого впровадження та використання телемедичних технологій. У цьому питанні слід дотримуватись оптимального балансу між забезпеченням інформаційної безпеки та доступності телемедичних послуг.

У літературі деяким авторам відзначається неприпустимість надання анонімних телемедичних послуг без ідентифікації пацієнта [10]. Такий підхід є частково виправданим, оскільки повна анонімність процесу надання телемедичних послуг позбавляє гарантій захисту прав і законних інтересів, наприклад, у разі виникнення спору щодо якості наданої медичної допомоги та притягнення до відповідальності за шкоду, заподіяну незаконними діями.

Забезпечити повну анонімність у телемедичній практично неможливо, оскільки в інформаційному просторі зберігаються «цифрові сліди», які прямо чи опосередковано дозволяють ідентифікувати пацієнта. Законодавство Україні передбачає можливість надавати пацієнтам медичні послуги анонімно, проте чинні вимоги до ідентифікації та автентифікації суб'єктів телемедичної діяльності не регламентують таку можливість. З метою забезпечення права пацієнтів на анонімну медичну допомогу можна передбачити порядок надання анонімної медичної допомоги із застосуванням телемедичних технологій.

Можливо передбачити два механізми надання анонімної медичної допомоги із застосуванням телемедичних технологій: псевдо

анонімність телемедичної консультації для медичного працівника, яка передбачає попередню ідентифікацію пацієнта в інформаційній системі та подальше знеособлення медичного профілю пацієнта для медичного працівника; псевдо анонімність медичної консультації без внесення відомостей до електронної медичної картки.

Право на отримання анонімної медичної допомоги із застосуванням телемедичних технологій має надаватися у всіх випадках, якщо це не впливає на якість медичної допомоги, що надається і не обмежено законодавчими вимогами. Підзаконним актом передбачено перелік видів медичних втручань, які не можуть здійснюватися анонімно через вимоги законодавства про необхідність обов'язкового отримання поінформованої добровільної згоди.

Для реалізації права на анонімну медичну допомогу медичні пристрої та інформаційні системи повинні передбачати технічну можливість псевдо анонімності консультації, що доцільно закріпити у відповідних технічних вимогах до інформаційної безпеки програмного забезпечення, медичних пристроїв та інформаційних систем.

На думку авторів статті Правове забезпечення цифрової трансформації сфери охорони здоров'я у світлі медичної реформи з огляду на євроінтеграційні процеси Україні» потрібно звернутись до досвіду країн Європейського Союзу та залучити кваліфікованих спеціалістів для врегулювання питань, пов'язаних із проблемами функціонування електронних систем, в особливості таких платформ, як Helsi.me та Doc.ua, адже вони є основними та найбільшими ресурсами для зв'язку пацієнтів та лікарів [11, с. 146].

У контексті забезпечення інформаційної безпеки важливим є розмежування прав доступу до персональних записів про стан здоров'я громадян у медичній установи. Особливість інформаційних систем охорони здоров'я полягає у потенційній можливості отримати доступ до електронних записів про здоров'я пацієнтів медичними установами та медичними працівниками, підключеними до взаємопов'язаних систем зберігання медичних даних.

З цієї причини заходи захисту інформації в т медицині повинні забезпечувати доступ до інформації про о пацієнта тільки в тих випадках, коли медичний працівник має законну підставу на доступ до інформації про пацієнта. У ситуації, коли пацієнт дає згоду на обробку персональних даних медичному працівнику, дана проблема з юридичної точки зору не становить труднощів.

У випадках обробки персональних даних без згоди пацієнта, що у багатьох випадках допускається законодавством, питання законних підстав доступу до даних медичним працівником є проблематичним. Розмежування доступу до персональних електронних медичних записів може здійснюватися по-різному. Наприклад, у Фінляндії медичний працівник повинен звернутися до адміністратора інформаційної системи для отримання прав прочитання та зміни запису в реєстрі.

Використовувані механізми підвищують рівень інформаційної безпеки інформаційних систем охорони здоров'я за рахунок звуження можливостей неавторизованого доступу. Ці механізми повинні удосконалюватися, але вони не повинні обмежувати доступність інформації про пацієнтів для законних цілей.

З метою реалізації права пацієнта на надання доступу до записів про здоров'я, забезпечення прозорості доступу до записів доцільно передбачити у вимогах до інформаційних систем охорони здоров'я технічну можливість контролю пацієнта за доступом до електронних записів про здоров'я через механізми вираження згоди на доступ до записів про здоров'я та ведення електронного журналу запитів на доступ до записів. Така технічна можливість, поряд з висловленням згоди на використання електронної медичної картки, сприятиме підвищенню ролі пацієнта у розпорядженні медичною інформацією та відповідальному контролю за колом осіб, яким інформація була надана.

Забезпечення безпеки електронного документообігу в медицині може здійснюватися й іншими правовими та технічними заходами. Не в повній мірі здійснюється ефективне функціонування системи забезпечення інформаційної безпеки України в силу недостатнього рівня професійної підготовки фахівців з інформаційної безпеки структурних підрозділів із захисту інформації органів державної влади, організацій і підприємств [12].

У Фінляндії у рамках захисту інформаційних систем охорони здоров'я здійснюється комплексне моделювання ризиків інформаційної безпеки. Заходи безпеки, що вживаються, повинні бути спрямовані на нейтралізацію потенційних загроз, виявлених в результаті моделювання. В Україні розроблено та затверджено методику визначення актуальних загроз безпеки персональних даних при обробці в інформаційних системах персональних даних.

У країнах ЄС (наприклад, Великій Британії) передбачено зовнішній аудит безпеки інформаційних систем охорони здоров'я. Такий аудит може бути додатковим підтвердженням дотримання стандартів інформаційної безпеки для пацієнтів і для контролюючих органів.

Для захисту медичних даних має значення безпека IT-інфраструктури. Наприклад, в

Ісландії сервери, на яких зберігаються дані про пацієнтів, знаходяться в закритому приміщенні, доступ до яких здійснюється з використанням спеціальних електронних карток. Усі комп'ютери, які переходять у режим очікування, автоматично блокуються.

Інформація може передаватися захищеними каналами зв'язку, можливе використання технологій шифрування даних. До перспективних технологій шифрування чутливої інформації відносяться алгоритми шифрування даних, коли інформація передається окремими зашифрованими пакетами через незалежні лінії зв'язку. Такі технології дозволяють забезпечити конфіденційність даних, що передаються, про стан здоров'я, оскільки позбавляють сенсу перехоплення зловмисниками окремих пакетів даних.

До потенційно застосовних засобів шифрування чутливої інформації відносять інструменти шифрування, засновані на використанні ідентифікаторів користувачів. Публічним ключем при такому шифруванні є ідентифікатор користувача, наприклад, адреса електронної пошти. Перевагами шифрування є високий рівень захисту інформації, економічність і зручність у використанні.

У науковій літературі активно просувається використання технології блокчейн в архітектурі інформаційних систем охорони здоров'я. Технологія блокчейн дозволить підвищити безпеку зберігання та обміну електронних записів про здоров'я в децентралізованих інформаційних системах, що є аргументом на користь децентралізованого підходу до зберігання та управління медичною інформацією в інформаційних системах охорони здоров'я.

Оператори інформаційних систем повинні використовувати найкращі практики, щоб максимально протидіяти сучасним загрозам безпеці чутливих відомостей про пацієнтів. Лише комплексне застосування сучасних заходів захисту інформаційних систем, що ґрунтується на врахуванні законних інтересів учасників інформаційного обміну, а також потенційних загроз інформаційній безпеці, здатне забезпечити належний рівень довіри до телемедичних технологій. Довіра громадян є фактором, від якого залежить легітимація і поширення телемедицини.

Л.Р. Катинська зазначає, що правове регулювання телемедицини в Україні потребує змін, що відповідають вимогам часу, з метою надання в можливості отримання доступу до телемедичних послуг широкому колу пацієнтів, а отже – розвитку домашньої телемедицини [13, с. 724]. Це має особливе значення у контексті організацію надання медичної допомоги із застосуванням телемедицини в умовах воєнного стану [14].

Висновки. Електронний документообіг становить інфраструктурну базу інформаційного обміну, якого неможлива медична діяльність. Ключові аспекти правового забезпечення інформаційної безпеки електронного документообігу в медичній галузі включають правові основи створення електронних записів про здоров'я пацієнтів, установи інформаційних систем охорони здоров'я, їх взаємодії та захисту інформації, що обробляється у системах.

Оптимальною моделлю з метою забезпечення безпечного інформаційного обміну є створення електронних записів про здоров'я за мовчанням з правом пацієнта відмови від електронних записів, децентралізоване зберігання медичних даних у єдиній координаційній платформі. Окреме завдання у правовому забезпеченні електронного документообігу у телемедичній справі полягає у реалізації права пацієнта на доступ та управління персональними електронними записами про здоров'я.

У разі розвитку телемедицини зростає значення технічних засобів захисту: ідентифікації та автентифікації, шифрування даних та інших. Технічні засоби повинні застосовуватися разом з правовими заходами: розмежуванням прав доступу до електронних записів про здоров'я, стандартизацією та технічним регулюванням, договірними засобами. З метою реалізації автономії волі пацієнта, захисту недоторканності приватного життя та права на анонімну медичну допомогу вимоги до інформаційних систем охорони здоров'я повинні передбачати технічну можливість вираження згоди пацієнта на доступ до електронних записів про здоров'я, забезпечувати прозорість інформації про доступ третіх осіб до електронних записів про здоров'я, знеособлення профілю пацієнта під час взаємодії з медичним працівником.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Teledermatology in Belgium: a pilot study. URL: https://www.tandfonline. com/doi/abs/10.1080/17843286.2018.1561812.
2. A review of telemedicine services in Finland. URL: https://www.academia.edu/794418/A_REVIEW_OF_TELEMEDICINE_SERVICES_IN_FINLAND.
3. Telemedicine and Geriatrics in France: Inventory of Experiments. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6166386/.
4. Market study on telemedicine. 2018. URL: https://health.ec.europa.eu/system/files/2019-08/2018_provision_marketstudy_telemedicine_en_0.pdf.
5. Деякі питання електронної системи охорони здоров'я: Постанова Кабінету Міністрів України від 25.04.2018 р. № 411.

URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text.
6. Про основи законодавства України про охорони здоров'я: 19.11.1992 р. № 2801-XII. URL: https://zakon.rada.gov.ua/laws/card/2801-12.
7. Про схвалення Концепції розвитку електронної охорони здоров'я: Розпорядження Кабінету Міністрів України від 28.12.2020 р. № 1671-р. URL: https://zakon.rada.gov.ua/laws/show/1671-2020-%D1%80#Text.
8. Ковалів М.В., Єсімов С.С., Ярема О.Г. Інформаційне право України: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2022. 416 с.
9. Про затвердження Порядку ведення Єдиного державного демографічного реєстру та надання з нього інформації, взаємодії між уповноваженими суб'єктами, а також здійснення ідентифікації та верифікації: Постанова Кабінету Міністрів України від 18.10.2017 р. № 784. URL: https://zakon.rada.gov.ua/laws/show/784-2017-%D0%BF#Text.
10. Богомаз В. М., Барзилович А. Д. Самооцінка лікарями досвіду дистанційного консультування пацієнтів. 2020. URL: https://www.umj.com.ua/article/187521/samootsinka-likaryami-dosvidu-distantsijnogo-konsultuvannya-patsiyentiv.
11. Шлапко Т.В., Старинський М.В., Миргород-Карпова В.В., Висоцький А.І., Шеін Д.С. Правове забезпечення трансформації сфери охорони здоров'я у світлі медичної реформи з огляду на євроінтеграційні процеси. *Аналітично-порівняльне правознавство.* 2021. № 3. С. 141–147.
12. Малашко О.Є., Єсімов С.С. Зміст державної діяльності із забезпечення інформаційної безпеки. *Міжнародний науковий журнал «Інтернаука»*. 2020. № 15 (95). Т. 1. С. 46–54/
13. Катинська Л.Р. Поняття телемедицини в законодавстві України. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття*: матеріали науково-практичної конференції (м. Одеса, 17 червня 2022 р.). Одеса: Гельветика, 2022. Т. 1. С. 722–725.
14. Про організацію надання медичної допомоги із застосуванням телемедицини в умовах воєнного стану: Наказ Міністерства охорони здоров'я України від 20.06.2022 р. № 1062. URL: https://zakon.rada.gov.ua/laws/show/z0728-22#Text/