УДК 343.94
https://orcid.org/0000-0001-6667-9034
Мусієнко Анатолій Володимирович
кандидат юридичних наук, доцент, завідувач кафедри кримінального права,
Державний університет інфраструктури та технологій, м. Київ.

https://orcid.org/0000-0001-8529-8181
Мусієнко Володимир Володимирович
кандидат юридичних наук, доцент, завідувач кафедри цивільного права,
Державний університет інфраструктури та технологій, м. Київ.

АКТУАЛЬНІ АСПЕКТИ НОРМАТИВНО-ПРАВОВИХ МЕХАНІЗМІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЕЛЕКТРОННИХ МЕДИЧНИХ РЕЄСТРАХ В УКРАЇНІ

Анотація. *У статті на основі аналізу документів, публікацій наукових періодичних видань, національного законодавства, міжнародних нормативно-правових документів, досліджено актуальні аспекти нормативно-правових механізмів захисту персональних даних в електронних медичних реєстрах в Україні. Зокрема, розглянуто питання забезпечення вільного доступу кожного суб'єкта цивільних правовідносин до інформаційного простору у сфері охорони здоров'я суспільства, відстеження правопорушення в сфері інформатизації та притягнення до юридичної відповідальності суб'єктів правовідносин. Досліджено проблему захисту персональних даних взагалі, а у медичній сфері зокрема не лише в Україні, але й у глобальному масштабі, впровадження електронних систем обліку медичної інформації потребує якісно нових підходів щодо захисту персональних даних пацієнтів та медичних працівників.*

Ключові слова: електронні системи обліку медичної інформації, інформація, кіберзлочин, кіберзлочинність, персональні дані, комп'ютерні технології, електронні бази даних, цифрові технології, цифрова трансформація.

Annotation. *The article, based on the analysis of documents, publications of scientific periodicals, national legislation, international legal documents, examines current aspects of legal mechanisms for personal data protection in electronic medical records in Ukraine.*

The legal regime of information as an object of civil law, its features such as non-consumption from a moral point of view, the possibility of replication, as well as the fact that the law does not enshrine the exclusive right to own and use information, except for aspects related to creative intellectual activity. This issue, today, is becoming increasingly important. Therefore, taking into account the constitutional rights, a person not only exercises his rights, but also has the right to their protection, which is embodied not only in the elimination of violations, but also in compensation for material and moral damage. This purposeful approach stimulates the further development of information as an object of civil rights and responsibilities, as evidenced by the adoption of a number of regulations.

These norms created a strong basis for the introduction of new terms into civil circulation, in particular: database, information tools, information technology, information services and information products, information resources, information sovereignty of the state.

In the field of information use, the Doctrine stipulates the comprehensive satisfaction of the needs of public entities of all forms of ownership in access to reliable and objective information. Deepening the digital transformation of society, such as "country in a smartphone", together with the benefits increases society's vulnerability to cyber threats. In order to minimize such threats, steps need to be taken to improve cybersecurity, both in a single country and on a global scale, as network systems spread around the world. An important part of

the cybersecurity system is its legal framework, without which it is impossible to effectively combat cybercrime and cybercrime. The problem of effective cybersecurity became relevant with the beginning of the Russian-Ukrainian war. Solving such problems is not possible locally, without taking into account the global level and the experience of world leaders. Developed countries with leading positions in the field of computer and information technology, naturally aware of this problem, have previously begun to develop scientific and practical measures to combat and prevent cybercrime, gaining considerable experience.In particular, the issues of ensuring free access of each subject of civil law to the information space in the field of public health, tracking offenses in the field of information and bringing to justice the subjects of legal relations. The problem of personal data protection in general, and in the medical field in particular not only in Ukraine but also globally, the introduction of electronic medical information systems requires qualitatively new approaches to the protection of personal data of patients and health professionals.

Key words: electronic systems of medical information accounting, information, cybercrime, cybercrime, personal data, computer technologies, electronic databases, digital technologies, digital transformation.

Постановка проблеми. З моменту появи Загальної декларації прав людини, прийнятої та проголошеної резолюцією 217 А(III) Генеральної Асамблеї ООН від 10 грудня 1948 року, розпочався новий етап розвитку цивілізованого соціуму. Це зумовлено не тільки появою самого міжнародного документа, приєднанням до нього країн-членів ООН, прогресивного людства, а й тим, що він став відправною точкою подальшого розвитку прав людини, вдосконалення їх захисту, розвитку суспільства, в умовах ускладнення суспільних відносин, поява нових правил появі нових правами людини у нових галузях суспільної діяльності.

Комп'ютерні технології міцно увійшли до всіх сфер суспільного життя, принесли неймовірні зміни суспільних відносин. Такий прогрес дозволив удосконалити всі сфери суспільного життя, у тому числі покращити надання медичної допомоги, впроваджувати якісно нові методи лікування. Але закономірно, що водночас із запровадженням комп'ютерних технологій виникли й нові проблеми.

Аналіз останніх досліджень та публікацій.

Окремі питання присвячені кіберзлочинам та кіберзлочинності висвітлювались в роботах таких вітчизняних та зарубіжних вчених як Алпеєв А., Архіпов О., Ахтирська Н.М., Біленчук П.Д., Болгов В. Бутузов В., Кравцова М. О., Литвинов О.М., Марущак А.І., Музика А.А., М., Погорецький М.А., Фоменко О.В. та інші.

Однак, не применшуючи наукового внеску вказаних вчених, але беручи до уваги швидкий розвиток комп'ютерних мережевих технологій та розширення сфери застосування комп'ютерної техніки ця тема потребує подальших досліджень, оскільки кіберзлочинці є одними з найнебезпечніших, по причині використання новітніх технологій для здійснення своєї злочинної діяльності.

Мета статті полягає в теоретичному дослідженні актуальних аспектів нормативно-правових механізмів захисту персональних даних в електронних медичних реєстрах в Україні.

Виклад основного матеріалу.

Інформація є новелою, Цивільного Кодексу, а також має особливість відноситись як до немайнових прав так і до майнових, загалом, що пов’язані з майновими.

Згідно зі ст.200 ЦК України, інформацією є документовані або публічно оголошені відомості про події та явища, що мали або мають місце у суспільстві, державі та навколишньому середовищі [1.]. Тому з огляду на вищезазначене змістом інформації є саме обумовлені законодавством юридичні факти.

Досліджуючи правовий режим інформації, як об’єкта цивільних правовідносин не можна оминути увагою такі її особливості, як неприйнятність з моральної точки зору, можливість тиражування, а також те, що законодавчо не закріплено виключного права володіння та користування інформацією, крім аспектів, пов’язаних з результатами творчої інтелектуальної діяльності.

Так, з прийняттям Закону України «Про інформацію» відбувся чіткий , але на наш погляд невичерпний поділ на види, зокрема: медична інформація [2].

Останній вид інформації безумовно заслуговує особливої уваги і зокрема, що стосується її поширення та захисту. Більше того, дані аспекти можуть у відомій мірі торкаючись не тільки цивільного права, а також кримінального, адміністративного та інших галузей права.

Визнаючи правовий режим інформації, згідно ч. 2 ст. 200 Цивільного Кодексу України, загалом, відбувається поділ інформації на дві групи: зокрема правовідносин в сфері використання інформації, а також ті, які слід віднести до аспектів захисту права на інформацію. Дана проблематика, на сьогодні, набуває все більшої актуальності. Тому з урахуванням конституційних прав, особа не тільки здійснює свої права, а й має право на їх захист, що уособлюється не тільки в усуненні порушень, а й у відшкодуванні матеріальної та моральної шкоди. Такий цілеспрямований підхід стимулює подальший розвиток інформації, як об'єкта цивільних прав та обов'язків, що підтверджується прийняттям низки нормативно-правових актів. Зокрема, Закон України «Про Національну програму інформатизації»; Закон України «Про основні засади забезпечення кібербезпеки України»; Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29.12.2016 року «Про доктрину інформаційної безпеки України»».

З прийняття цих та інших нормативно-правових актів законодавства, правовідносини в сфері інформації та комп'ютерних технологій набули нового витку у своєму розвитку та перейшли на більш високий рівень функціонування в суспільстві. Дані норми створили потужне підґрунтя до введення в цивільний обіг нових термінів, зокрема: база даних, засоби інформатизації, інформаційні технології, інформаційні послуги та інформаційна продукція, інформаційний ресурс, інформаційний суверенітет держави.

Як наслідок вищезазначеного, слід підкреслити, що створено Національну програму інформатизації.

Так згідно ст..2 Закону України «Про національну програму інформатизації», дана програма визначає стратегію розв'язання проблеми забезпечення інформаційних потреб та інформаційної підтримки соціально-економічної, економічної, науково-технічної, оборонної, національно-культурної та іншої діяльності у всіх сферах загальнодержавного значення. І в теорії і на практиці вищезазначене окреслюється у повній мірі, і це чітко проявляється вже на так званому первинному, тобто побутовому рівні [3].

Слід, відмітити, що даним законом обумовлено концепцію такої програми, яка передбачає втілення її положень в усі сфери економіки та суспільного життя.

Концепцію створення Національної програми інформатизації обумовлюється формуванням пріоритетів соціально-економічного, науково-технічного, національно-культурного розвитку держави з урахуванням закордонного досвіду в сфері інформатизації і спрямування на розв'язання найважливіших загальносуспільних завдань. Виходячи із змісту Національної програми інформатизації формується комплекс взаємопов'язаних проектів інформатизації, що у підсумку приведе до створення інформаційної інфраструктури України.

Досліджуючи аспекти інформаційної безпеки, розглядаючи підґрунтя вищезазначених положень, ми головну увагу акцентуємо на використанні, а також на захисті прав суб'єктів інформатизації. Реалізація положень Національної програми інформатизації обумовлює співвідношення доступу до використання інформації та захисту прав суб'єктів інформації. Даний аспект підтверджується зазначенням цих положень у Доктрині інформаційної безпеки і стосуються національних інтересів держави, та інших суб'єктів цивільних правовідносин, визначених Конституцією України та Цивільним Кодексом.

В сфері використання інформації Доктриною обумовлюється всебічне задоволення потреб суб'єктів суспільства всіх форм власності у доступі до достовірної та об'єктивної інформації.

З використанням інформації, виникає необхідність її вільного обігу, а разом з тим забезпечення захисту прав на її використання. Але в даному конспекті слід наголосити на розбудові правової системи захисту всіх суб'єктів правовідносин суспільства. І у зв'язку з цим необхідно її адаптувати до норм міжнародного права та механізму захисту з використанням закордонного досвіду і як побічний результат функціонування та розвиток національного інформаційного простору, його інтеграція у європейський та світовий інформаційний простір, а це в свою чергу вплине на розвиток системи стратегічних комунікацій України.

З точки зору проблематики теми, слід сконцентрувати увагу на системі кібербезпеки, її функціонуванні, правового регулювання в сфері охорони здоров'я. Законодавчо чітко визначено

суб'єктний склад даних правовідносин. До яких зокрема, входять: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Національний банк України, а також у рамках теми дослідження Міністерство охорони здоров'я України.

Кожен із суб'єктів у визначеній мірі здійснює функціонування відповідно регламентації. Так, Державна служба спеціального зв'язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимоги щодо захисту якої встановлена законом, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах, координує діяльність інших суб'єктів комунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту, здійснює організаційно-технічні заходи із запобігання виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформує про кіберзагрози та відповідні методи захисту від них, забезпечує впровадження аудиту інформаційної безпеки, на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації), координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури та вразливість, забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT – UA.

Поглиблення цифрової трансформації суспільства, на кшталт «країна в смартфоні», разом із перевагами збільшує вразливість суспільства перед кіберзагрозам. З метою мінімізації подібних загроз необхідно вживати заходів для поліпшення посилення кібербезпеки, як в окремо взятій країні, такі в глобальному вимірі, оскільки мережеві системи поширюється на весь світ. Надважливою частиною системи кібербезпеки є її нормативно-правове забезпечення, без якого неможливо ефективно протидіяти кіберзлочинам та кіберзлочинності. Проблема ефективної кібербезпеки набула актуальності з початком російсько-української війни.

Останні гучні випадки зазіхань на дані користувачів викликають тривогу щодо того, як треті сторони захищають конфіденційність приватних осіб у цифрову епоху, викликали національне занепокоєння правового захисту електронних даних. Навмисне вторгнення в державні та приватні комп'ютерні мережі, неадекватні практики корпоративної конфіденційності та кібербезпеки відкрили особисту інформацію мільйонів користувачів небажаним отримувачам. У той самий час, підключення до Інтернету останніми роками збільшилося і змінювалося формою [4].

Такі проблеми не оминули і медичної сфери діяльності. Йдеться про захист персональних даних, насамперед пацієнта, а й медичних працівників. Права пацієнта на сьогодні становлять перелік і серед них право на таємницю про стан свого здоров'я. До конфіденційних даних може належати не тільки інформація про стан здоров'я пацієнта, але й факти або обставини, якими пацієнт ділиться з медичними працівниками під час лікування. Право на приватність та конфіденційність має застосовуватися з урахуванням різних культур, соціальних та релігійних традицій [5].

Для певних, вразливих верств населення дотримання конфіденційності є важливим аспектом отримання медичної допомоги. Наприклад, приватність та конфіденційність особливо важливі у сфері реалізації сексуальних та репродуктивних прав жінок та підлітків [6].

В Україні персональні дані пацієнтів збираються за їхньою письмовою згодою - вона є частиною декларації про вибір лікаря, затвердженої «Порядком вибору лікаря, який надає первинну медичну допомогу». Тому, ставлячи підпис у декларації, людина погоджується на обробку своїх даних у системі «Електронне здоров'я» (e-health).

Персональні дані, які були заплановані використовувати в електронній системі, умовно поділяють на так звані чутливі та нечутливі. На початку запровадження електронної системи передбачалося обробляти лише звані «нечутливі» персональні дані - паспортні дані, індивідуальний податковий номер, адресу проживання. Ці дані надаються для отримання більшості послуг в Україні: у банку, соціальних службах тощо [7].

Зараз у центральному компоненті системи є всі можливі дані. На думку авторів, такий поділ даних звичайно умовний, оскільки адресу проживання можна віднести і до чутливих даних, підтвердженням цього є відсутність адреси реєстрації на сучасній ID картці громадянина України у візуальному доступі.

Конфіденційність є важливими елементами для пацієнтів, які отримують лікування від захворювань, пов'язаних зі стигмою, а саме ВІЛ/СНІД та психічні розлади. Залежно від типу лікування, у деяких медичних закладах лише окремі медичні працівники мають доступ до конкретної медичної інформації про пацієнта. Наприклад, медсестра, яка вакцинує пацієнта, не має права доступу до медичної інформації про психічний стан пацієнта, тому що така інформація не є релевантною. Право на конфіденційність медичної інформації не повинно конфліктувати із правом на доступ до медичної інформації. Особа, яка володіє медичною інформацією, не має права поширювати цю інформацію серед осіб, які не належать до фахівців, які надають медичні послуги. Особа, яка володіє інформацією, має забезпечити належний доступ до медичної інформації лише на запит тієї особи, якої ця інформація стосується.

Право на таємницю про стан свого здоров'я завжди було актуальним і, зрозуміло, забезпечити це право завжди було дуже не просто. У доцифрову епоху, коли вся медична документація була на паперових носіях, вона була доступнішою для сторонніх осіб. Наприклад, зацікавлена особа могла у зручний момент зайти до приміщення, де зберігаються всі історії хвороб пацієнтів, та ознайомитись із необхідною інформацією.

Але сучасні цифрові технології змінили такий стан речей. Електронні реєстри не дають можливості так легко отримати інформацію, але особи, які мають спеціальні знання та навички роботи в комп'ютерних системах, здатні на це.

Треба сказати, що цифрові технології сфери медичного документообігу в Україні поки запроваджено не на всіх рівнях медичної допомоги (інститут сімейної медицини), а там де вони є потребують серйозного вдосконалення. Інші рівні медична допомога ще не підключені до системи e-health, і лікувальні заклади у кращому разі користуються власною локальною комп'ютерною мережею з програмним забезпеченням, яке, на думку авторів, не може гарантувати необхідних стандартів захисту персональної інформації. Ну, а багато лікувальних закладів продовжують користуватися переважно паперовими носіями. Більше того, на думку авторів, головна мета, яка полягала в покращенні надання медичної допомоги населенню, поки залишилась на рівні декларації. Зокрема можна констатувати, що доступність медичної допомоги погіршилась. І така ситуація особливо небезпечна, як з точки зору захисту персональних даних пацієнтів, так і потенційної небезпеки зловживань з боку медичного персоналу або інших осіб, коли в історії хвороби може змінюватися інформація, залежно від того, що там повинно бути.

Тому, на думку авторів, розміщення та обслуговування серверів з подібними базами даних має забезпечуватись державними компаніями, оскільки це дозволить гарантувати високий рівень безпеки. Важливим механізмом, на думку авторів, має бути нормативно-правове визначення вимог до серверів, на яких можуть розміщуватися подібні бази даних.

Крім того, можливі інші порушення з використанням такої електронної системи. Наприклад, програма «Доступні ліки» вже підсвічує зловживання, коли 5-річній дитині виписали дорослий препарат, не показаний для дітей, ще й найдорожчий [8].

На думку авторів, вирішення подібної проблематики неможливо локально, без урахування глобального рівня та досвіду світових країн-лідерів. Розвинуті країни, які займають лідируючі позиції в галузі комп’ютерних та інформаційних технологій, закономірно усвідомили цю проблему раніше почало напрацьовувати наукові та практичні заходи протидії та запобіганням кіберзлочинності, накопичивши значний досвід. Стрімкий розвиток телекомунікаційних та глобальних комп'ютерних мережевих технологій призвело до появи такого виду злочинного посягання кіберзлочинності, як транскордонне комп'ютерна злочинність. Сучасні кіберзлочинці, яких ще називають хакери, можуть здійснювати свої злочинні посягання щодо певного об’єкта, навіть перебуваючи в зовсім інший локації, за тисячі кілометрів, в іншій країні, на іншому континенті. Такі особливості кіберзлочинів та кіберзлочинності зумовлюють необхідність міжнародної співпраці у протидії та запобіганні.

Основним документом, що регламентує співробітництво правоохоронних органів у боротьбі з транснаціональною кіберзлочинністю безумовно є Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. [9].

Існують і інші міжнародно-правові документи про боротьбу з транснаціональною кіберзлочинністю. Наприклад, Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21 грудня 2010 р. та Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16 червня 2009 р. мають регіональний характер і також спрямовані на боротьбу з транснаціональною кіберзлочинністю.

Однак міжнародна спільнота намагається сформувати додаткові правові і організаційні передумови для підвищення ефективності протидії транснаціональній кіберзлочинності. Наприклад, у лютому 2016 року ЄС та НАТО підписали технічну угоду щодо посилення співпраці у сфері кібербезпеки, спрямованої на створення сприятливих умов за для оперативного обміну інформацією та досвідом між командами екстреного реагування НАТО «Computer Incident Response Capability» (NCIRC) та ЄС [10].

Висновки.

Проведене дослідження дозволило авторам дійти наступних висновків:

1. проблема захисту персональних даних взагалі, а у медичній сфері зокрема, набула особливої актуальності і не лише в Україні, але й у глобальному масштабі;
2. впровадження електронних систем обліку медичної інформації потребує якісно нових підходів щодо захисту персональних даних пацієнтів та медичних працівників;
3. забезпечення вільного доступу кожного суб'єкта цивільних правовідносин до інформаційного простору у сфері охорони здоров'я суспільства;
4. здійснювати постійний моніторинг за достовірністю інформації, яка має обіг в кіберпросторі;
5. відстежувати правопорушення в сфері інформатизації та притягнення до юридичної відповідальності суб'єктів правовідносин.

Література:

1. Цивільний кодекс України. URL:https://zakon.rada.gov.ua/laws/show/435-15#Text (Дата звернення 9.09.2021)
2. Закон про інформацію. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (Дата звернення 9.09.2021)
3. Закон про Національну програму інформатизації. URL: https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80#Text (Дата звернення 9.09.2021)
4. Data Protection Law: An Overview. URL: https://fas.org/sgp/crs/misc/R45631.pdf;
5. Гостін. «Сфери впливу в сфері охорони здоров'я –аналіз прав людини». – Всесвітня організація здоров'я та дослідження прав людини № 2, 2003. URL: www.who.int/hhr/information/en/Series_2%20Domains%20of%20health%20responsiveness.pdf;
6. Міжамериканська комісія з прав людини (IACHR). Доступу до інформації з репродуктивного здоров'я та прав людини (11 листопада 2011 р.). URL: www.oas.org/en/iachr/women/docs/pdf/womenaccessinformationreproductivehealth.pdf;
7. Захист даних в системі E-Health. З. В. Дерен, О. М. Анісімова. URL: http://jvestnik-sss.donnu.edu.ua/article/view/6691/6723;
8. Що не так з медичними картками в Україні. URL: https://project.liga.net/projects/eHealth/
9. Конвенція про кіберзлочинність // URL: https://zakon.rada.gov.ua/laws/show/994_575#top
10. Марущак А.І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. «Інформація і право». № 3(26)/2018. 104-110 с.