МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УНІВЕРСИТЕТ МИТНОЇ СПРАВИ ТА ФІНАНСІВ

Кваліфікаційна наукова праця
на правах рукопису

ПОНОМАРЕНКО ІРИНА СЕРГІЇВНА

УДК 342.951:347.77

ДИСЕРТАЦІЯ

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

12.00.07 – адміністративне право і процес; фінансове право;
інформаційне право (081 – Право)

Подається на здобуття наукового ступеня **доктора філософії**

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ І.С. Пономаренко

Науковий керівник – **Шевченко Михайло Вікторович,** доктор філософії

Дніпро – 2025

АНОТАЦІЯ

Пономаренко І.С. **Правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я**. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Університет митної справи та фінансів, Дніпро, 2025.

У дисертації проведено комплексне наукове дослідження правового регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я.

Розглянуто теоретичні засади інформаційної безпеки людини у сфері охорони здоров'я; проаналізовано зміст та особливості інформаційної безпеки у медичній сфері, медичної інформації; визначено об'єкти та суб'єкти забезпечення інформаційної безпеки людини у медичній сфері; досліджено еволюцію нормативно-правового регулювання захисту інформації у досліджуваному напрямі, виокремлено проблемні питання та окреслено перспективи удосконалення у даному напрямі; визначено сучасний стан та проблематику інформаційної приватності у медичній сфері; окреслено основні джерела загроз для інформаційних систем у медичній сфері; здійснено аналіз міжнародного досвіду правового забезпечення інформаційної безпеки людини та окреслено перспективи імплементації його у вітчизняне законодавство; досліджено особливості міжнародних стандартів захисту інформації в електронних медичних системах, а також практику Європейського суду з прав людини щодо організації та правового регулювання захисту інформації у медичній сфері.

У вступі обґрунтовано актуальність теми дисертації, визначено її зв'язок з науковими програмами, планами, темами, окреслено мету, завдання, об'єкт та предмет дослідження, методи дослідження, нормативну базу, наукову новизну та

практичне значення отриманих результатів, особистий внесок здобувача та апробацію результатів дослідження.

Перший розділ роботи присвячено теоретичним засадам інформаційної безпеки людини у медичній сфері. У його межах розкрито зміст, особливості та стан дослідження інформаційної безпеки у сфері охорони здоров'я, досліджено сутність медичної інформації, визначено об'єкти та суб'єкти забезпечення інформаційної безпеки у даному напрямі.

Теоретично обгрунтовано, що проблематика інформаційної безпеки у сфері охорони здоров'я виникла через певні невідповідності між можливостями функціоналу інформаційних технологій та інформаційних загроз, а також через відсутність належного рівня інформаційної культури як серед працівників медичної сфери, так і суспільства загалом. Здійснено класифікацію механізмів комплексної системи інформаційної безпеки у сфері охорони здоров'я – правовий, технічний, комунікаційний та освітній.

Сформульовано авторське визначення поняття «інформаційна безпека у сфері охорони здоров'я», розмежовано поняття «лікарська таємниця» та «медична інформація», сформульовано їх авторське визначення, визначено поняття «суб'єкти та об'єкти інформаційної безпеки у сфері охорони здоров'я». Розглянуто основні випадки розголошення медичної інформації без згоди пацієнта чи його законних представників. Запропоновано імплементувати позитивний міжнародний досвід Сполучених штатів Америки (Закон США «Про мобільність та підзвітність медичного страхування» (HIPAA)).

Другий розділ присвячено аналізу вітчизняних та міжнародних правових норм, які регламентують інформаційну безпеку людини у медичній сфері. У його межах розкрито проблемні питання правового регулювання інформаційного захисту у медичній сфері, інформаційної приватності у даному напрямі, джерел загроз для медичних інформаційних систем, визначено проблеми та окреслено

перспективи удосконалення правового забезпечення захисту інформації у медичній сфері.

Проаналізовано еволюцію правового регулювання захисту інформації у медичній сфері. Констатовано, що правові норми, які регулюють захист інформації у сфері охорони здоров'я, передбачають зовнішню і внутрішню, пов'язану між собою, систему як законів, так і підзаконних нормативно-правових актів. Крім того, вітчизняна правова база захисту інформації ґрунтується на основних міжнародних принципах та практиці ЄСПЛ. Обгрунтовано думку, що як міжнародним законодавством, так і вітчизняним, у окремих випадках дозволено обробляти персональні дані осіб без надання їх згоди. Разом з тим, у міжнародному законодавстві гарантовано захист такої інформації. Проаналізовано рішення ЄСПЛ у справах «Z проти Фінляндії», «Л.Л. проти Франції», «М.С. проти Швеції», «Gillberg v. Sweden».

Визначено, що одним з основних проблемних питань щодо захисту персональних даних у медичній сфері є відсутність належного правового регулювання у частині координації та взаємодії при розробці та упровадженні відповідних інформаційних систем. Встановлено, що за порушення норм чинного законодавства у частині, що стосується захисту інформації у медичній сфері, передбачено дисциплінарну, цивільно-правову, адміністративну та кримінальну відповідальність.

Проаналізовано основні норми та принципи Загального регламенту із захисту персональних даних Європейського Союзу у частині щодо захисту інформації у медичній сфері. Обгрунтовано думку, що право на захист медичної інформації виникає не в момент його порушення, а одночасно з суб'єктивним правом. За результатами аналізу рішення ЄСПЛ від 29.04.2017 (справа «Л.Х. проти Латвії» № 52019/07), Верховного Суду України від 04.12.2019 (справа № 760/8719/17) зроблено висновок, що повноваження державних органів у частині щодо збирання та збереження персональних даних визначаються законодавчо.

Констатовано, що пандемія коронавірусу актуалізувала ряд проблемних питань щодо забезпечення захисту інформації в медичній сфері. Окреслено проблематику щодо неврегулювання на законодавчому рівні дій працівників медичних закладів у разі відмови пацієнтів від обробки персональних даних та внесення своїх персональних даних до електронного реєстру. Визначено типові проблемні питання електронної системи охорони здоров'я.

Окреслено переваги і ризики упровадження медичних інформаційних систем. З'ясовано, що розробниками медичних інформаційних систем є як юридичні особи, так і фізичні особи-підприємці, яких попередньо перевірено на предмет сумісності з Центральною базою даних, якими з адміністратором бази даних (держпідприємством «Електронне здоров'я»)підписано відповідний договір, а також які відповідають встановленим технічним нормам. Проаналізовано угоди медичних інформаційних систем Helsi, Health24, Asker, Moniheal у частині щодо збору, обробки, зберігання та надання доступу третім особам до медичної інформації. Надано пропозиції щодо удосконалення даного напряму. Визначено основні інформаційні загрози МІС: великий обсяг медичної інформації, яка зберігається в одній базі даних і розміщена в одному місці; відсутність контролю та нагляду державними органами за діяльністю операторів медичних інформаційних систем приватних компаній. Визначено проблемні питання щодо технічного захисту Електронного реєстру відомостей про генетичні ознаки людини та дотримання порядку надання геномної інформації органам інших держав.

Теоретично обгрунтовано, що: інформатизація у сфері охорони здоров'я повинна здійснюватися з дотриманням вимог вітчизняного законодавства України, яке регламентує захист персональних даних, Генерального регламенту ЄС із захисту персональних даних, міжнародних стандартів ISO/IEC, а також інших документів, які регулюють даний напрям. Звернено увагу на дотримання принципу визначеної мети та мінімізації даних. Аргументовано, що для подальшого розвитку

та ефективного функціонування дієвої системи електронної системи охорони здоров’я в Україні необхідна надійна система захисту інформації.

Визначено проблемні питання, які перешкоджають активному упровадженню МІС у медичну сферу. Запропоновано чотири основні напрями удосконалення нормативно-правового забезпечення інформаційної безпеки у медичній сфері. Аргументовано необхідність подальшого доопрацювання питання щодо захисту інформаційного права особи під час обов’язкового медичного страхування, та, відповідно, обробки, зберігання та захисту медичної інформації у даному напрямі. Запропоновано розробити та прийняти Закон України «Про загальнообов'язкове державне медичне соціальне страхування». Констатовано, що у нормах Закону України «Про державну реєстрацію геномної інформації людини»: прослідковується певна правова невизначеність щодо відповідності її міжнародним стандартам про дотримання прав людини на інформацію; виникають питання щодо належного технічного захисту Електронного реєстру відомостей про генетичні ознаки людини. Запропоновано інтегрувати інформаційні системи та забезпечити їх технічний захист відповідно до норм міжнародних стандартів.

Третій розділ присвячено аналізу вітчизняних та міжнародних правових норм, які регламентують забезпечення інформаційної безпеки у медичній сфері. У його межах досліджено: основні норми міжнародного правового регулювання, а також особливості застосування практики ЄСПЛ щодо захисту інформації у медичній сфері; міжнародні та європейські стандарти захисту інформації у електронних системах сфери охорони здоров’я та перспективи їх імплементації у вітчизняне законодавство.

Досліджено міжнародні правові норми з питань захисту медичної інформації. Проаналізовано основні міжнародні нормативні акти загальних, спеціальних та основних правових норм. Розглянуто особливості прецедентних рішень ЄСПЛ у справах «I. проти Фінляндії», «К.Н. та інші проти Словакії», «Z проти Фінляндії»,

«M. C. проти Швеції», «L.H. v. Latvia», «*R v. RC*», «S. And Marper v. the United Kingdom», «M.K. v. France».

Констатовано, що у міжнародному законодавстві виокремлюють три напрями закріплення прав пацієнта: універсальний (акти, які носять декларативний характер і виступають, в основному, у якості рекомендацій для світової спільноти), регіональний (документи, прийняті Радою Європи, які мають обов'язковий характер) та спеціалізований (документи, які прийнято спеціально створеною організацією).

Проаналізовано норми захисту медичної інформації, регламентовані: Загальним регламентом із захисту персональних даних та Законом про мобільність та підзвітність медичного страхування «HIPAA», окреслено їх спільні та відмінні ознаки; Правилом взаємодії CMS і доступу пацієнтів та Заключним правилом Закону про лікування ONC (основною метою яких є спрощення доступу пацієнтів до їх медичних даних з дотриманням відповідних заходів безпеки і конфіденційності). Звернено увагу на дотримання принципу необхідності та пропорційності при зборі медичної інформації. Окреслено проблемні питання захисту медичної інформації.

Констатовано, що найвищими міжнародними та європейськими стандартами є Загальний регламент із захисту персональних даних та модернізована Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних.

Теоретично обгрунтовано необхідність імплементації позитивного досвіду США (у частині щодо приватності медичної інформації, правові норми якого урегульовано Законом США про мобільність та підзвітність медичного страхування (HIPAA)); Великобританії (базові модулі для медичних інформаційних систем закуповуються за рахунок держави, а додаткові кожен медичний заклад докуповує самостійно).

Розглянуто: особливості захисту медичної інформації у медичних інформаційних системах при клінічних випробуваннях (дослідження нових

препаратів на пацієнтах у документально зафіксованому дослідницькому середовищі). Окреслено проблематику – порушення вимог щодо знищення медичних відомостей на електронних носіях (після видалення інформації не застосовується форматування електронного носія, відповідно, за допомогою сучасного програмного забезпечення наявна можливість відновлення видалених файлів); особливості захисту медичної інформації у загальнонаціональних системах електронних медичних записів під час взаємообміну медичною інформацією. Констатовано, що найбільш ефективними є єдині бази даних ДНК у США, Німеччині, Іспанії, Франції, Італії, Великобританії, Польщі, законодавством яких передбачено одного держателя та адміністратора. З'ясовано, що на підставі Прюмського договору, країни-члени ЄС отримали як правовий механізм, так і додаткові можливості щодо обміну відомостями з базами даних ДНК національного рівня.

Визначено основні внутрішні правила, які сприятимуть підвищенню рівня інформаційної безпеки в медичних інформаційних системах сфери охорони здоров'я: забезпечення технічного захисту доступу до місцезнаходження апаратного і програмного забезпечення; дотримання правових норм щодо технічного захисту інформації; підвищення професійної грамотності; використання медичної інформації відповідно до норм законодавства; постійний моніторинг дотримання порядку авторизації доступу; перевірка системи протоколів доступу до медичної інформації наглядовим чи контролюючим органом.

Проаналізовано рішення ЄСПЛ у частині щодо: незаконного доступу до бази даних («I. v. Finland», «Gardel v. France», «Z проти Фінляндії»); гарантування захисту чутливої інформації («Перуццо і Мартенс проти Німеччини», «M.C. проти Швеції»); порушення умов і термінів зберігання біологічного матеріалу та ДНК-профілів («S. andMarper v. the United Kingdom», «M.K. v. France»). Вартим уваги є те, що справа «S. andMarper v. the United Kingdom» внесла суттєві зміни у

законодавство не лише Великобританії та наразі враховується при підготовці профільних законів інших держав.

Розглянуто право на забуття медичної інформації, яке передбачає видалення медичної інформації із загального доступу. Констатовано, що відповідно до норм GDPR, як національне, так і міжнародне законодавство потребує суттєвого удосконалення у цьому напрямі. Окрім GDPR право суб'єкта персональних даних вимагати у контролера їх видалення регламентовано іншими міжнародними договорами, разом з тим визнання права на забуття гарантовано не у кожному з них.

З метою посилення інформаційної безпеки медичних інформаційних систем створено Європейське агентство з мережевої та інформаційної безпеки (ENISA), до повноважень якого належить аналіз стану безпеки інформаційних загроз, надання пропозицій щодо шляхів їх запобігання та усунення. Крім технічних характеристик агентством розглядаються юридичні питання, які безпосередньо пов'язано з функціонуванням бази даних ДНК. Теоретично обгрунтовано, що суттєвий вплив на формування міжнародних стандартів у напрямі захисту чутливої інформації має прецедентна практика ЄСПЛ.

***Ключові слова*:** адміністративно-правове регулювання, публічна безпека, інформаційна безпека, публічна інформація, медична інформація, інформаційно-аналітичне забезпечення, персональні дані, інформаційна приватність, захист персональних даних, технічний захист інформації, медичні інформаційні системи, міжнародні стандарти, прецедентна практика ЄСПЛ, права людини, репродуктивні права людини, права осіб з інвалідністю, захист прав пацієнтів.

SUMMARY

Ponomarenko I.S. **Legal regulation of ensuring human information security in the field of health care.** – Qualifying scientific work on manuscript rights.

Dissertation for the Doctor of Philosophy degree in specialty 081 "Law". – University of Customs and Finance, Dnipro, 2025.

In the dissertation, a comprehensive scientific study of the legal regulation of ensuring human information security in the field of health care was carried out.

The theoretical principles of human information security in the field of health care are considered; the essence and features of information security in the field of health care and medical information were analyzed; the objects and subjects of ensuring human information security in the field of health care are defined; the evolution of the legal regulation of information protection in the field of health care has been studied, problematic issues have been identified and prospects for improvement in this direction have been outlined; the current state and problems of information privacy in the medical field are defined; the main sources of threats to information systems in the field of health care are outlined; the international experience of legal provision of human information security in the field of health care was analyzed and the prospects of its implementation into domestic legislation were determined; the peculiarities of international standards of information protection in electronic medical systems, as well as the practice of the European Court of Human Rights regarding the organization and legal regulation of information protection in the medical field, were investigated.

The introduction substantiates the relevance of the topic of the dissertation, defines the connection of the work with scientific programs, plans, topics, outlines the goal, task, object and subject of research, research methods, normative and empirical basis, scientific novelty and practical significance of the obtained results, approbation of the results research, personal contribution of the acquirer.

The first section of the work is devoted to the theoretical foundations of human information security in the field of health care. Within its limits, the concept, features and state of information security research in the field of health care are revealed, the essence of medical information is investigated, and the objects and subjects of information security in this area are defined.

It is theoretically justified that the problem of information security in the field of health care arose due to the contradiction between the possibilities of information technologies and the threats of their use, as well as the lack of an appropriate level of information culture among both medical workers and society in general. The classification of the mechanisms of the complex system of information security in the field of health care was carried out - legal, technical, communication and educational.

The author's definition of the concept of "information security in the field of health care" was formulated, the concepts of "medical confidentiality" and "medical information" were distinguished, their author's definition was formulated, the concept of "subjects and objects of information security in the field of health care" was defined ". The main cases of disclosure of medical information without the consent of the patient or his legal representatives are considered. It is proposed to implement the positive international experience of the United States of America (the US Health Insurance Portability and Accountability Act (HIPAA)).

The second section is devoted to the analysis of domestic and international legal norms that regulate the provision of personal information security in the field of health care. Within its limits, the problematic issues of legal regulation of information protection in the medical field, information privacy in this direction, sources of threats to medical information systems are revealed, problems are identified and prospects for improving the legal provision of information protection in the field of health care are outlined.

The evolution of the legal regulation of information protection in the field of health care is analyzed. It was established that the legal norms that regulate the protection of information in the field of health care provide for an external and internal interconnected system of laws and by-laws. In addition, the domestic legal framework for information protection is based on the main international principles and practice of the European Court of Human Rights. International legislation, as well as domestic legislation, in exceptional cases allows the processing of personal data of individuals without their consent, however, a feature of international legislation is that the state guarantees their information

protection. The decision of the European Court of Human Rights in the cases "Z v. Finland", "L.L. against France", "M.S. v. Sweden", "Gillberg v. Sweden".

It was established that despite certain positive developments in the field of health care, there are problematic issues in the direction of personal data protection, in particular: information resources and information processing technologies are developed without ensuring the necessary level of centralization and coordination of work, which indicates the need improvement of domestic legislation in this regard of human rights dated 04.29.2017 (case "L.H. v. Latvia" No. 52019/07), the Supreme Court of Ukraine dated 04.12.2019 (case No. 760/8719/17) concluded that the discretionary powers of the state authority to collect and storage of a person's personal data must be clearly defined by law.

It was established that the coronavirus pandemic has actualized a number of problematic issues regarding the provision of information protection in the medical field. The issue of non-regulation at the legislative level of the actions of medical institution employees in case of patients' refusal to process personal data and enter their personal data into the electronic register is outlined.

The main problematic issues of the electronic health care system have been identified. The advantages and risks of implementing medical information systems are outlined. It was found that the developers of medical information systems are either legal entities or individual entrepreneurs who have passed the check for compatibility with the Central Database, signed a contract with the database administrator (the state-owned enterprise "ElektronneZdrovya"), and also meet the technical norms The agreements of the medical information systems Helsi, Health24, Asker, Moniheal were analyzed in terms of the collection, processing, storage and provision of access to third parties to medical information. Suggestions for improvement of this area have been provided. The main information threats of MIS have been identified: a large amount of medical information stored in one database and geographically located in one place; lack of control by state bodies over the activities of private companies (MIS operators). The issues of technical protection of the Electronic Register of information on human genetic traits and

compliance with the procedure for providing genomic information to the bodies of foreign states are outlined.

It is theoretically justified that: informatization in the field of health care should be carried out in compliance with the requirements of the domestic legislation of Ukraine regarding the protection of personal data and the EU General Regulation on the protection of personal data, international ISO/IEC standards, other international documents and requirements in this field. It is especially worth paying attention to the principle of the defined goal and data minimization (only data that is necessary for the realization of the established goal should be collected and processed); a reliable information protection system is necessary for the effective further development and functioning of an effective electronic health care system in Ukraine. Problematic issues that prevent the active implementation of medical information systems in the field of health care have been identified. Four main directions for improving the legal provision of information security in the field of health care are proposed.

The need for further elaboration of the issue regarding the protection of a person's informational right during mandatory medical insurance, and, accordingly, the processing, storage and protection of medical information in this direction, is argued. It is proposed to develop and adopt the Law of Ukraine "On mandatory state medical social insurance". It was established that in the provisions of the Law of Ukraine "On State Registration of Human Genomic Information": there is a certain legal uncertainty regarding its compliance with international standards in the part that concerns the observance of human rights to information; questions arise regarding the proper technical protection of the Electronic Register of Information on Human Genetic Characteristics. It is proposed to integrate information systems and ensure their technical protection in accordance with international standards. The third section is devoted to the analysis of domestic and international legal norms that regulate the provision of human information security in the field of health care.

The main norms of international legal regulation, as well as the peculiarities of the application of the practice of the European Court of Human Rights regarding the protection of information in the medical field were investigated within its limits; international and European standards for the protection of information in electronic systems in the field of health care and prospects for their implementation in domestic legislation. International legal norms on the protection of medical information have been studied. The main international normative acts of general, special and basic legal norms have been analyzed. Peculiarities of precedent decisions of the European Court of Human Rights in the cases of "I. against Finland", "K.H. and others v. Slovakia", "Z v. Finland", "M. S. v. Sweden", "L.H. v. Latvia", "R v. RC", "S. and Marper v. the United Kingdom", "M.K. v. France".

It has been established that international legislation distinguishes three directions of securing patient rights: universal (acts that are declarative in nature and act mainly as recommendations for the world community), regional (documents adopted by the Council of Europe that are binding) and specialized (documents adopted by a specially created organization).

The norms of the protection of medical information regulated by: the General Regulation on the Protection of Personal Data and the Law on Mobility and Accountability of Health Insurance "HIPAA" were analyzed, their common and distinctive features were outlined; The CMS Interoperability and Patient Access Rule and the ONC Care Act Final Rule (the primary purpose of which is to facilitate patient access to their health data while maintaining appropriate security and privacy measures). Attention is drawn to compliance with the principle of necessity and proportionality when collecting medical information. Problematic issues of medical information protection are outlined.

Problematic issues of medical information protection are outlined. It was established that the highest international and European standards are the General

Regulation on the Protection of Personal Data and the modernized Convention on the Protection of Individuals in Connection with Automated Processing of Personal Data.

The need to implement the positive experience of the USA is theoretically substantiated (in the part regarding the privacy of medical information, the legal norms of which are regulated by the US Health Insurance Portability and Accountability Act (HIPAA)); Great Britain (basic modules for medical information systems are purchased at the expense of the state, and additional ones are purchased independently by each medical institution).

Considered: features of medical information protection in medical information systems during clinical trials (research of new drugs on patients in a documented research environment). The problem is outlined - violation of the requirements for the destruction of medical information on electronic media (after the information is deleted, the formatting of the electronic media is not applied, accordingly, with the help of modern software, it is possible to restore deleted files); peculiarities of protection of medical information in national systems of electronic medical records during mutual exchange of medical information. It was established that the most effective are the single DNA databases of the USA, Great Britain, Poland, Germany, Italy, Spain, France, in which one database holder and administrator is defined. It was found that on the basis of the Prm Treaty, the EU member states received both a legal mechanism and additional practical opportunities regarding the exchange of information with national DNA databases.

The main internal rules that will contribute to increasing the level of information security in medical information systems in the field of health care have been determined: compliance with norms regarding technical information protection; increasing professional literacy; use of medical information in accordance with legislation; proper technical protection of access to the location of hardware and software; constant monitoring of compliance with the access authorization procedure; inspection of the system of protocols for access to medical information by a supervisory or controlling body.

The decision of the ECPL was analyzed in the part related to: illegal access to the database ("I. v. Finland", "Gardel v. France", "Z v. Finland"); guaranteeing the protection of sensitive information ("Peruzzo and Martens v. Germany", "M.S. v. Sweden"); violation of the terms and conditions of storage of biological material and DNA profiles ("S. and Marper v. the United Kingdom", "M.K. v. France"). It is noteworthy that the case of "S. and Marper v. the United Kingdom" made significant changes in the legislation not only of Great Britain and is currently taken into account when developing relevant laws in many countries of the world/

Considered the right to be forgotten, which involves the removal of medical information from public access through search engines, that is, links to those data that, in her opinion, may harm her. It was established that, in accordance with GDPR, both national and international legislation needs significant improvement in this direction. In addition to the GDPR, the right of the subject of personal data to demand from the data controller the deletion of this information is enshrined in many international treaties and decisions of international organizations, but not all of them guarantee their recognition of the right to be forgotten.

In order to strengthen the information security of medical information systems, the European Agency for Network and Information Security (ENISA) was established in 2004, whose mandate is to analyze the current state of security threats and provide recommendations for their elimination. In addition to technical aspects, the reviews and recommendations of the working group also pay attention to certain legal issues related to the functioning of DNA databases. It is theoretically justified that the precedent practice of the European Court of Human Rights has a significant influence on the formation of international standards in the direction of protecting sensitive information.

Keywords: administrative and legal regulation, public safety, information security, public information, medical information, information and analytical support, personal data, information privacy, personal data protection, technical protection of information,

medical information systems, international standards, ECHR case law, human rights, reproductive human rights, rights of persons with disabilities, protection of patients' rights.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації

Пономаренко І.С. Основні аспекти правового регулювання відповідальності за порушення прав інтелектуальної власності. *Науковий вісник публічного та приватного права.*2020. Вип. 1. С. 227–231. DOI: https://doi.org/10.32844/2618-1258.2020.1.39.

Пономаренко І.С. Правове регулювання захисту персональних даних у медичній сфері: вітчизняний та міжнародний досвід. *Право і суспільство*. 2020. № 6. Ч. 2. С. 120–125. DOI: https://doi.org/10.32842/2078-3736/2020.6.2.2.18.

Arifkhodzhaieva T., Ponomarenko I. Economic policy of the state in conditions of informatization of health care in Ukraine as an integral part of the social sphere. *Baltic Journal of Economic Studies.* 2021 Vol. 7, No 5. P. 228–234. DOI: https://doi.org/10.30525/2256-0742/2021-7-5-228-234.

Пономаренко І.С. Актуальні питання правового регулювання захисту інформації у сфері охорони здоров’я. *Науковий вісник Міжнародного гуманітарного університету.* Серія: «Юриспруденція». 2021 № 53. С. 55–58. DOI: https://doi.org/10.32841/2307-1745.2021.53.11.

Пономаренко І.С., Гуз А.М. Міжнародна та вітчизняна практика впровадження медичних інформаційних систем. *Наукові записки Міжнародного гуманітарного університету: збірник.* Одеса: «Гельветика». 2022. *Вип. 36. 244 с. С.* 26–30. URL: http://www.sci-notes.mgu.od.ua/archive/v36/36_2022.pdf.

Наукові праці, які засвідчують апробацію матеріалів дисертації

Пономаренко І.С. Актуальні питання захисту персональних даних у сфері охорони здоров'я. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали науково-практичної конференції (м. Київ, 10 грудня 2020 р.). м. Київ: Фенікс, 2020. 272 с.

Пономаренко І.С. Особливості правового захисту інформації у Сполучених Штатах Америки. *Актуальні проблеми правових наук в євроінтеграційному вимірі*: матеріали Міжнародної науково-практичної конференції (м. Харків, 18-19 грудня 2020 р.). Харків: ГО «Асоціація аспірантів-юристів», 2020. 116 с. С. 61–67.

Пономаренко І.С., Ткачук Т.Ю. Правове регулювання інформаційної приватності у медичній сфері України та США. *Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції*: матеріали *Всеукраїнської науково-практичної конференції* (м. Київ, 29 квітня 2021 р.). м. Київ: КПІ ім. Ігоря Сікорського, 2021. 192 с. С. 164–167.

Пономаренко І.С. Особливості захисту інформації в електронній системі охорони здоров'я. *Роль і місце інформаційного права і права інтелектуальної власності в сучасних умовах. Креативні індустрії*: матеріали *ІІІ Всеукраїнської науково-практичної конференції* (м. Київ, 11 листопада 2021 р.). м. Київ, 2021. 327 с. С. 235–243.

Пономаренко І.С., Тугарова О.К. Проблемні питання організації захисту інформації в медичних інформаційних системах. *Актуальні проблеми управління інформаційною безпекою держави:* матеріали XV Всеукраїнської науково-практичної конференції *(м. Київ, 27 березня 2024 р.)*. м. Київ, 2024. Ч. 1. С. 685–689.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

МОЗ	– Міністерство охорони здоров’я;
СЗІБ	– система захисту інформаційної безпеки;
КСЗІ	– комплексна система захисту інформації;
ІКТ	– інформаційно-комунікаційні технології;
ІБ	– інформаційна безпека;
МІС	– медичні інформаційні системи;
GDPR	– General Data Protection Regulation;
ЄСПЛ	– Європейський суд з прав людини;
ЦК України	– Цивільний кодекс України;
КПК України	– Кримінальний процесуальний кодекс України;
ООН	– Організація об’єднаних націй;
РНБО	– Рада національної безпеки та оборони України;
ТЗІ	– технічний захист інформації;
ЗМІ	– засоби масової інформації;
ЦБД	– центральна база даних;
ЕСОЗ	– електронна система охорони здоров’я.

ВСТУП

Обґрунтування вибору теми дослідження. Розвиток інформаційного суспільства нерозривно пов'язаний як з розвитком інформаційних технологій, так і із забезпеченням прав людини. Сфера охорони здоров'я не є винятком. Адже обсяг інформації, якою оперує лікар, постійно збільшується. Щорічно до міжнародних реєстрів вносяться десятки нових діагностичних методів і реєструються тисячі нових ліків. Все більше закладів охорони здоров'я для покращення ефективності діяльності застосовують інформаційно-комунікаційні технології, які поступово зайняли центральне місце в організації охорони здоров'я, та охоплюють цілий ряд електронних чи цифрових процесів реєстрації, діагностики, лікування, обміну інформацією, у тому числі і транскордонному. Проте величезні обсяги «чутливих» даних у медичних інформаційних системах певною мірою можуть сприяти несанкціонованому доступу до інформації, можливим витокам чи втраті медичної інформації. І це зважаючи на те, що наразі, під час перебування країни в умовах воєнного стану, прослідковується тенденція щодо суттєвого збільшення кількості кібератак на критичну інформаційну інфраструктуру, до якої належать й установи медичного сектору.

Отже реформування медичної системи у напрямі інформатизації буде ефективним лише за умови належного правового захисту медичної інформації під час збору, зберігання, оброблення та передавання інформації. Адже обмін інформацією щодо стану здоров'я між надавачами медичних послуг, інформаційними мережами охорони здоров'я, медичними працівниками та пацієнтами ускладнюється проблемою як технічного, так і правового захисту так званих «чутливих» персональних даних, що мають підвищені вимоги до захисту. Залишається також проблемним питанням і рівень обізнаності громадян, адже досить часто вони просто ігнорують проблеми, пов'язані із захистом медичної

інформації, у тому числі через неповне розуміння законодавчих стандартів і вимог у цій сфері.

Зважаючи на суттєві зміни, які відбуваються у ході проведення медичної реформи, виникає потреба суттєвих змін у чинному законодавстві у частині, що стосується правового регулювання захисту інформації у сфері охорони здоров'я. Адже захист чутливої інформації є не просто обов'язком держави і предметом державно-правового регулювання, його необхідно розглядати у поєднанні із захистом прав людини. Тим більше, що створення належної системи захисту персональних даних передбачено міжнародними зобов'язаннями України, відповідно до яких національні медичні асоціації повинні використовувати всі можливі заходи для забезпечення таємниці, захищеності і конфіденційності інформації, яка стосується їх пацієнтів і зберігається в інформаційних системах.

Дослідження проблематики правового регулювання забезпечення інформаційної безпеки було здійснено у наукових працях, які, безумовно, заклали фундамент у контексті теми нашого дослідження, а саме таких як: К.І. Бєляков «Деякі питання щодо формування реформи інформаційного законодавства України…», О.Д. Довгань «Правові засади формування і розвитку системи забезпечення інформаційної безпеки України», А.Ю. Нашинець-Наумова «Інформаційна безпека: питання правового регулювання», А.І. Марущак «Інформаційна безпека: правовий аналіз», В.М. Фурашев, О.Г. Радзієвська «Правове забезпечення інформаційної безпеки», Т.М. Мужанова «Інформаційна безпека держави», Т.Ю. Ткачук «Правове забезпечення інформаційної безпеки в умовах євроінтеграції України», О.К. Юдін, В.М. Богуш «Інформаційна безпека держави», В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський «Інформаційна безпека України в умовах євроінтеграції». Питанням щодо особливостей захисту персональних даних приділяли увагу О.С. Дяковський «Правове забезпечення захисту персональних даних», М.В. Бем, І.М. Городиський, О.М. Родіоненко «Захист персональних даних», О.В. Легка «Правова регламентація реєстрації

геномної інформації людини …», Є.А. Кобрусєва «Інформаційна безпека у медичній сфері у період правового режиму воєнного стану». Проблематику забезпечення інформаційної безпеки прав та свобод людини, а також загрози її інформаційній безпеці досліджували О.О. Золотар «Інформаційна безпека людини: теорія і практика», О.Г. Радзієвська «Проблеми захисту прав і безпеки дитини у інформаційній сфері» та О.В. Топчій «Адміністративно-правове забезпечення інформаційної безпеки неповнолітніх в Україні». Особливості юридичної відповідальності за правопорушення в інформаційній сфері розглядали О.О. Тихомиров, О.К. Тугарова «Юридична відповідальність за правопорушення в інформаційній сфері», Є.В. Кузьмічова-Кисленко, Л.Д. Удалова «Лікарська таємниця в кримінальному процесі» та інші. Разом з тим, у більшості наукових праць основну увагу приділено ретроспективному аналізу розвитку інформаційної безпеки, теоретико-правовим аспектам та проблемним питанням нормативно-правового забезпечення інформаційної безпеки, особливостям впливу процесів глобалізації на інформатизацію суспільства в сучасних умовах.

У той же час, незважаючи на існуючі наукові здобутки, на сьогодні практично поза увагою залишається питання щодо правового регулювання інформаційної безпеки у сфері охорони здоров’я, яке з урахуванням пандемії коронавірусу та дії в Україні правового режиму воєнного стану, наразі є досить актуальним. Деякі питання щодо подальшого розвитку інформаційних технологій у медичній сфері досліджували І.О. Гулівата, Л.П. Гусак, К.В. Копняк, Л.Б. Ліщинська, П.С. Лютіков, Т.П. Мінка, Н.Б. Новицька, Д.В. Приймаченко, С.А. Яремко, окремі аспекти права на медичну інформацію розглядали Г.О. Блінова, А.І. Марущак, О.Г. Марценюк, С.Г. Стеценко, В.Ю. Стеценко, І.Я. Сенюта, І.В. Шатковська, Х.Я. Терешко. Разом з тим, поза увагою залишилися питання як щодо правового регулювання, так і технічного захисту медичних інформаційних систем, джерел загроз для МІС, інформаційної приватності у сфері охорони здоров’я, включаючи дослідження нормативно-правових аспектів та технічного захисту інформації відповідно до

норм міжнародних стандартів та прецедентної практики Європейського суду з прав людини. Тобто єдиного комплексного підходу щодо забезпечення інформаційної безпеки людини у сфері охорони здоров'я у контексті реформування системи не вироблено.

Зазначені обставини і обумовили вибір теми дослідження у зв'язку з її актуальністю для науки адміністративного права.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася відповідно до Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 року № 722/2019, Стратегії розвитку Національної академії правових наук України на 2021-2025 роки, затвердженої постановою загальних зборів Національної академії правових наук України від 26 березня 2021 р., Стратегії інформаційної безпеки, затвердженої рішенням Ради національної безпеки і оборони України від 15 жовтня 2021 року, а також у межах дослідної роботи Науково-дослідного інституту інформатики і права Національної академії правових наук України «Теоретико-правові основи захисту прав, свобод і безпеки людини в інформаційній сфері» (номер державної реєстрації: 0117U007745).

Мета і задачі дослідження. *Мета* дисертаційної роботи полягає у тому, щоб на основі аналізу вітчизняних та зарубіжних правових норм, а також практики їх застосування, узагальнення сучасних наукових досліджень розкрити особливості правового регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я, окреслити проблематику та надати пропозиції щодо шляхів удосконалення.

Для досягнення мети у роботі визначено наступні *задачі:*

– з'ясувати особливості та стан дослідження інформаційної безпеки у сфері охорони здоров'я;

– розглянути зміст поняття «медична інформація»;

– визначити об’єкти та суб’єкти забезпечення інформаційної безпеки у сфері охорони здоров’я;

– проаналізувати еволюцію правового регулювання захисту інформації у медичній сфері;

– окреслити основні засади інформаційної приватності у медичній сфері;

– дослідити основні джерела загроз для медичних інформаційних систем;

– визначити проблеми та окреслити перспективи удосконалення правового забезпечення захисту інформації у сфері охорони здоров’я;

– з’ясувати особливості застосування міжнародних та європейських правових норм щодо захисту інформації у медичній сфері;

– окреслити перспективи імплементації у вітчизняне законодавство міжнародних та європейських стандартів щодо захисту інформації у електронних системах сфери охорони здоров’я.

Об’єктом дослідження є суспільні відносини при забезпеченні інформаційної безпеки людини у сфері охорони здоров’я.

Предметом дослідження є правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров’я.

Методи дослідження. Методологічні засади у дослідженні ґрунтувалися на наукових методах. Основою став метод діалектичного матеріалізму, за допомогою якого узагальнено інформацію про сучасний стан та подальший розвиток правового регулювання інформаційної безпеки людини у сфері охорони здоров’я (підрозділи 1.1., 2.1., 3.3.). За допомогою логіко-семантичного методу проаналізовано сутність та особливості ключових термінів, які використовуються у дослідженні та сформульовано наступні авторські дефініції: «інформаційна безпека», «інформаційна безпека у сфері охорони здоров’я», «лікарська таємниця», «медична інформація», «суб’єкти інформаційної безпеки у сфері охорони здоров’я» (підрозділи 1.2., 1.3.). Системно-структурний підхід застосовано для визначення основних механізмів забезпечення інформаційної безпеки людини у сфері охорони

здоров’я (підрозділи 2.2., 2.3., 3.3.). За допомогою порівняльно-правового методу здійснено комплексний аналіз міжнародного законодавства (підрозділ 3.1., 3.2.). Методи аналізу та синтезу надали можливість визначити основні проблемні питання щодо забезпечення інформаційної безпеки у сфері охорони здоров’я (підрозділи 2.1., 2.3., 3.3.) та, відповідно, запропонувати науково обґрунтовані висновки даної роботи (підрозділи 2.2., 2.3., 3.2.).

Нормативно-правова основа дисертації: Конституція України, закони України, міжнародно-правові акти, акти Президента України, Кабінету Міністрів України.

Емпірична основа дослідження: правова публіцистика, статистичні дані Міністерства охорони здоров’я, Міністерства інформаційної політики, прецедентні рішення Європейського суду з прав людини, аналітичні вітчизняні та міжнародні звіти, інтернет-джерела, результати емпіричних досліджень автора.

Наукова новизна одержаних результатів полягає у тому, що дисертація є одним із перших комплексних досліджень правового забезпечення інформаційної безпеки людини у сфері охорони здоров’я. За результатами дослідження запропоновано нові наукові положення, обґрунтовано висновки та рекомендації, які містять наукову новизну, зокрема:

уперше:

– визначено основні проблемні питання інформаційної безпеки у сфері охорони здоров’я: протиріччя технічних можливостей інформаційних систем та загроз щодо їх використання; відсутність належного рівня інформаційної культури як серед працівників медичної сфери, так і суспільства загалом;

– теоретично обґрунтовано необхідність розроблення та затвердження єдиного нормативно-правового акта, який на законодавчому рівні врегулював би збір, обробку, захист та передачу медичної інформації, за прикладом GDPR (структурувати медичні інформаційні системи, передбачити сертифікацію щодо захисту інформації, розмежувати права доступу медичних працівників до

інформації, передбачити доступ до інформації з обов'язковим використанням електронного підпису, проходженням медичними працівниками короткострокових курсів та реєстрацією працівниками служби захисту інформації (передбачення: визначення прав доступу та, відповідно, можливості зміни його рівня; надання логіну для ідентифікації та автентифікації), корегування даних та внесення нової інформації здійснюється з підтвердженням електронного підпису, розробити алгоритм передачі інформації між закладами охорони здоров'я);

– визначено типові інформаційні загрози медичних інформаційних систем (великий обсяг медичної інформації, яка зберігається в одній базі даних та територіально знаходиться у одному місці, а також відсутність контролю з боку державних органів за діяльністю приватних компаній, надано пропозиції щодо шляхів їх запобігання;

– обґрунтовано, що незважаючи на чіткі правові норми, мають місце факти порушення у частині, що стосується: відсутності як мети, так і доцільності такого об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутності підстави для подальшого зберігання та обробки інформації;

– запропоновано створити спеціальний незалежний наглядовий орган за дотриманням законодавства у сфері захисту персональних даних (наразі функції наглядового органу у сфері захисту персональних даних здійснює Уповноважений Верховної Ради України з прав людини, проте такий контроль не притаманний його конституційно-правовому статусу), повноваження якого повинні відповідати вимогам, передбаченим Загальним Регламентом Європейського Парламенту і Ради (ЄС) 2016/679;

удосконалено:

- змістовне тлумачення таких понять як «інформаційна безпека», «інформаційна безпека у сфері охорони здоров'я», «лікарська таємниця», «медична інформація», «суб'єкти інформаційної безпеки у сфері охорони здоров'я»;

– положення щодо необхідності закріплення на законодавчому рівні гарантій захисту персональних даних у сфері охорони здоров'я, що є першочерговим для реалізації захисту прав людини;

– напрями правового забезпечення інформаційної безпеки у сфері охорони здоров'я: систематизація законодавства; удосконалення вимог щодо програмного забезпечення, сертифікації, технічного захисту інформації та вимог щодо забезпечення медичних закладів комп'ютерним устаткуванням, яке відповідає вимогам міжнародних стандартів; удосконалення питань щодо організаційного та кадрового забезпечення інформатизації сфери охорони здоров'я (підвищення рівня цифрової грамотності працівників медичної сфери (курси підвищення кваліфікації, семінари, круглі столи)); перехід до загальноприйнятих у міжнародній практиці методів збору, обробки та захисту інформації, а також подальший розвиток міжнародного співробітництва;

– підходи до систематизації типових проблемних питань щодо інформаційної безпеки у медичній сфері (недостатній рівень комп'ютерної грамотності медичних працівників, а також порушення законодавчих норм щодо порядку реєстрації та автентифікації користувачів МІС (надано пропозиції щодо удосконалення правових норм щодо автентифікації користувачів у МІС, запропоновано імплементувати позитивний досвід Естонії, де доступ до МІС здійснюється виключно за ідентифікатором особи (персональним ID-паспортом), що мінімізує можливість зазначених вище помилок); відсутність спеціального інформаційного відділу у закладах охорони здоров'я; невідповідність технічних характеристик комп'ютерного обладнання встановленим вимогам; невідповідність функціоналу медичних інформаційних систем вимогам міжнародних стандартів);

дістало подальшого розвитку:

– зміст поняття «інформаційна безпека у сфері охорони здоров’я», під яким запропоновано розуміти комплексну систему захисту інформаційного середовища, яка забезпечує запобігання, виявлення і нейтралізацію інформаційних загроз, а також цілісність, конфіденційність та доступність інформації, тим самим забезпечуючи формування та розвиток інформаційного середовища у медичні сфері в інтересах держави, суспільства та особистості;

– обґрунтування необхідності: систематизації вітчизняного законодавства; доповнення (п. 1 розділу «Етапи та основні напрями реалізації» Стратегії розвитку інформаційного суспільства у частині щодо передбачення належного технічного захисту як автоматизованих інформаційних галузевих систем, так і взагалі медичної інформації; пп. 1 п. 2 розділу ІІ Закону України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» у частині щодо визначення мети обробки персональних даних);

– положення про необхідність розроблення та прийняття: Закону України «Про внесення змін до Закону України «Про захист персональних даних» з урахуванням норм Загального регламенту із захисту персональних даних; Закону України «Про загальнообов'язкове державне медичне соціальне страхування», у якому визначити: перелік інформації, яка відноситься до «чутливої» медичної інформації; перелік суб’єктів, які під час виконання службових повноважень, мають доступ до «чутливої» медичної інформації; вимоги щодо збору, обробки та зберігання «чутливої» медичної інформації; строки зберігання «чутливої» медичної інформації; заходи юридичного впливу у разі порушення встановлених вимог;

– аргументація необхідності зведення термінологічного апарату у сфері охорони здоров’я до терміна «медична інформація»;

– обґрунтування необхідності імплементації позитивного досвіду Сполучених штатів Америки (Закон США «Про мобільність та підзвітність медичного страхування» (HIPAA)), відповідно, потребує розроблення окремий

нормативно-правовий акт, який на законодавчому рівні врегулював би збір, обробку, розкриття та передачу медичної інформації.

Практичне значення отриманих результатів визначається можливістю їх використання у:

– *правотворчій діяльності* – з метою вдосконалення норм правового регулювання інформаційної безпеки людини у сфері охорони здоров'я;

– *науково-дослідній сфері* – у процесі підготовки підручників, навчальних посібників, методичних рекомендацій (Акт про впровадження у науково-дослідну діяльність Університету митної справи та фінансів від 03.10.2025 р.);

– *правозастосовчій діяльності* – з метою вдосконалення механізмів захисту інформації у сфері охорони здоров'я;

– *навчальному процесі* – при викладанні дисципліни «Адміністративна діяльність публічної адміністрації» за темами: «Контрольно-наглядові провадження», «Ліцензійно-дозвільні провадження», «Провадження за зверненнями громадян», «Забезпечення законності в діяльності публічної адміністрації», а також у процесі підготовки навчально-методичних комплексів із відповідних навчальних дисциплін (Акт про впровадження у навчальний процес Університету митної справи та фінансів від 10.10.2025 р.).

Особистий внесок здобувача. Дисертаційна робота є самостійно виконаною науковою працею, усі результати якої одержані безпосередньо здобувачем і знайшли відображення у наукових публікаціях. Внесок здобувача в роботи, виконані у співавторстві, відображені у списку публікацій.

Апробація результатів дисертації. Результати дослідження, висновки та рекомендації оприлюднено на 5 міжнародних та всеукраїнських науково-практичних конференціях: «Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання» (м. Київ, 10 грудня 2020 р.); «Актуальні проблеми правових наук в євроінтеграційному вимірі» (м. Харків, 18-19 грудня 2020 р.); «Інтернет речей: теоретико-правові та практичні аспекти

впровадження в умовах Європейської інтеграції» (м. Київ, 29 квітня 2021 р.); «Роль і місце інформаційного права і права інтелектуальної власності в сучасних умовах. Креативні індустрії» (м. Київ, 11 листопада 2021 р.); «Актуальні проблеми управління інформаційною безпекою держави» (м. Київ, 27 березня 2024 р.).

Публікації. Основні положення, висновки та результати дисертаційного дослідження опубліковано дисертантом самостійно та у співавторстві у 5 наукових працях, загальним обсягом 26,5 д.а., з яких особисто автору належить 20,5 д.а., з них: 4 у наукових фахових виданнях України; 1 – у наукових періодичних виданнях, проіндексованих у базах даних Scopus та/або Web of Science, а також у п’яти тезах доповідей на міжнародних та всеукраїнських науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається із основної частини (вступу, трьох розділів, що об’єднують дев’ять підрозділів, висновків), списку використаних джерел. Загальний обсяг дисертації становить 240 сторінок, з яких 176 сторінок основного тексту. Список використаних джерел складається із 276 найменувань.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

1.1. Понятійно-категоріальний синтез інформаційної безпеки у сфері охорони здоров'я

Однією з основних характеристик держави, яка суттєво впливає на всі процеси соціально-економічного розвитку суспільства, є рівень інформаційного забезпечення державної влади [119, с. 2]. Застосовуючи та стимулюючи попит на сучасні ІТ-рішення, впроваджуючи новітні електронні адміністративні послуги та інтегруючи інноваційні моделі, держава має стати зразком для всієї України в переході до «цифрових» технологій. Для країн, що розвиваються, та країн з перехідною економікою, досить актуальним є впровадження та подальший розвиток інформаційних та комунікаційних технологій (далі – ІКТ) [137].

Актуальний етап розвитку українського соціуму безпосередньо пов'язаний із поширенням і впровадженням інноваційних інформаційно-комунікаційних технологій. На рівні законодавства вже зафіксовано становлення цифрової економіки, електронного урядування та інститутів електронної демократії, розроблено комплексні плани реалізації цих концепцій. У практичній площині започатковано процес інтероперабельності інформаційних систем медичних закладів, функціонує Національний реєстр електронних інформаційних ресурсів, відбувається поступове створення «цифрових» робочих місць, а класичне паперове діловодство трансформується у систему електронного документообігу.

Слід зазначити, що проблема інформаційної безпеки виникла внаслідок протиріччя між технічними можливостями інформаційних ресурсів і загрозами,

пов'язаними з їхнім використанням. Тобто, поряд із зовнішніми (об’єктивними) загрозами інформаційній безпеці людини, які пов’язані із зловживанням ІКТ, недостатнім або неефективним правовим регулюванням інформаційних відносин, існують і внутрішні (суб’єктивні) – відсутність належного рівня інформаційної культури (грамотність, небажання протистояти негативним чи надмірним інформаційним впливам, нездатність адаптуватися до нових соціальних умов, пов’язаних із постійним збільшенням інформаційної насиченості всіх сфер життя). Ось чому інформаційну безпеку людини не можна вивчати ізольовано від системи інформаційної безпеки суспільства, держави та глобальної інформаційної безпеки людства [137].

Важливо усвідомлювати, що інформаційна безпека є також невід'ємною частиною і національної безпеки держави, що пов’язано із наступними факторами:

– національні інтереси, загрози їм та заходи щодо їхнього захисту у всіх сферах національної безпеки знаходять своє відображення та реалізуються через інформацію та інформаційну сферу;

– особа та її права, а також інформація, інформаційні системи та права на них є основними об’єктами, що охороняються в контексті інформаційної безпеки. Наразі нормативно-правове регулювання прав людини в інформаційному просторі доволі недосконале. Що стосується терміна «цифрові права» – то це питання для широкої дискусії. Все більше держав визнають цифрові права частиною загальних прав людини, а доступ до мережі Інтернет розглядається як одне з основних таких прав. Уже в 1946 році Генеральна Асамблея ООН ухвалила одну з перших своїх резолюцій, яка встановила, що свобода інформації є основним правом людини та критерієм для всіх інших свобод [200, с. 8];

– вирішення питань національної безпеки на сучасному етапі тісно пов'язане з використанням інформаційно-комунікаційних засобів та технологій як основних інструментів [62].

В Україні правові засади забезпечення інформаційної безпеки формуються на основі Конституції України [78], а також таких спеціальних нормативно-правових актів, як закони України «Про інформацію» [171], «Про Національну програму інформатизації» [176], а також Стратегії інформаційної безпеки [224]. Реалізація державної політики у цій сфері покладається на низку суб'єктів: Раду національної безпеки і оборони України, органи внутрішньої безпеки, державні інституції, уповноважені на розроблення стандартів захисту інформації та безпеки інформаційних потоків, наукові організації, інститути громадянського суспільства та інші структури.

За останні десятиліття світ значно змінився, і більшість комунікацій, фінансових операцій та інформаційних архівів перейшли в Інтернет. Це призвело до збільшення їх доступності для сторонніх осіб у порівнянні з епохою, коли використовувалися лише матеріальні носії. Водночас, разом із підвищеною доступністю, зросла й їхня вразливість. Таким чином, інтереси особистості та суспільства, пов'язані зі збереженням інформації або захистом від деструктивного інформаційного впливу, постійно знаходяться під загрозою [125].

Сьогодні інформаційна безпека є однією з основних цінностей держави, забезпечення якої гарантує її стабільне функціонування та поступальний розвиток. Ми притримуємося у контексті досліджуваного наукової точки зору М. Присяжнюка, що саме активне упровадження ІКТ сприяє актуальності подальшого удосконалення інформаційної безпеки, у зв'язку з чим дане питання потребує системного та комплексного підходу [153]. Я. Жаркова також акцентує увагу на тому, що одним із основних завдань розвиненої держави є гарантія інформаційної безпеки особистості [44]. Таким чином, питання інформаційної безпеки в умовах глобальної інформатизації та розвитку Інтернету набувають стратегічного значення.

Крім того, у статті 17 Конституції України визначено, що найважливішими функціями держави є захист суверенітету та територіальної цілісності України,

забезпечення її економічної та інформаційної безпеки [78], що, як зазначає В. Цимбалюк, свідчить про те, що інформаційна безпека набуває у правовому відношенні конституційного статусу [250, с. 30].

Наразі, в умовах війни за незалежність, першочергового значення набувають питання щодо удосконалення інформаційної безпеки, адже ефективність управлінської діяльності напряму залежить від належного інформаційного забезпечення [63]. Відповідно, ключові завдання як держави, так і суспільства – усвідомлення загроз інформаційній безпеці та якнайшвидший пошук шляхів щодо їх протидії [60].

Розглянемо сутність та особливості дефініцій «інформаційна безпека», «сфера охорони здоров'я».

В англійській мові існують два терміни для позначення поняття «інформаційна безпека», які однаково перекладаються українською мовою, але мають різний зміст: «safety» і «security». Перший термін означає стан захищеності об'єкта, а другий підкреслює діяльність, спрямовану на забезпечення цього стану. Тому інформаційну безпеку визначають як стан відсутності загроз з боку інформаційно-комунікаційного середовища, а також як здатність об'єкта протидіяти різним інформаційним загрозам [110].

Що стосується правової науки, то серед дослідників цієї тематики поки що немає єдності щодо шляхів якісної трансформації інформаційного законодавства України. Це є цілком зрозумілим, враховуючи складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [117, с. 252].

Інформаційну безпеку класифікують за двома напрямами – захист інформації, відповідних інформаційних ресурсів, держави, суспільства від негативного інформаційного впливу, та загрози інформаційній безпеці [238].

Що стосується чинного вітчизняного законодавства, то термін «інформаційна безпека» визначено: у Законі України «Про Основні засади розвитку

інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 р. № 537-V, як стан захисту інтересів держави, суспільства та людини, який сприяє запобіганню нанесення шкоди через: неповноту, невчасність та невірогідність інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації [178]; в Угоді про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав-учасниць СНД від 11.09.1998 р. № 997/889, відповідно до якої під інформаційною безпекою розуміють стан захисту інформаційної сфери, що забезпечує його формування, використання та розвиток в інтересах громадян, організацій, держави [240].

Варто зазначити, що на підставі Указу Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» було затверджено Стратегію інформаційної безпеки (далі – Стратегія), у якій визначено організацію діяльності із забезпечення інформаційної безпеки України як одну з ключових функцій держави [224]. Згодом, 30 березня 2023 року, Кабінет Міністрів України ухвалив розпорядження, яким затвердив План заходів із реалізації Стратегії на період до 2025 року [163]. При цьому слід підкреслити, що відповідно до п. 3 згаданого Указу втратив чинність попередній Указ Президента України від 25 лютого 2017 року № 47, яким вводилося в дію рішення РНБО від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».

Відповідно до Стратегії, під інформаційною безпекою розуміють складову національної безпеки, стан захисту інтересів держави, суспільства та особи, при якому встановлюється ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, зокрема через координоване поширення недостовірної інформації, негативні наслідки застосування інформаційних технологій, несанкціоноване розповсюдження, використання й

порушення цілісності, конфіденційності та доступності інформації [224]. Тобто основними завданнями є організація забезпечення інформаційної безпеки, протидія загрозам інформаційній сфері, захист прав осіб на інформацію.

Як бачимо, останнім часом прослідковуються позитивні тенденції щодо внесення змін до вітчизняного законодавства у частині, що стосується інформаційної безпеки. Разом з цим, як слушно зазначають В. Горбулін та М. Биченко, ключовою причиною невідповідності правових норм законодавства про інформацію вимогам сучасності є як відсутність систематизації, так і «несформованість» цілісного розуміння інформаційної безпеки. Тому саме комплексний підхід до подальшого розвитку та удосконалення правових норм у даному напрямі наразі є вкрай актуальним завданням [204, с. 89].

Проаналізуємо наукові підходи у контексті досліджуваного. На думку В.А. Ліпкана та А.Ю. Нашинець-Наумової, під поняттям «інформаційна безпека» доцільно розуміти стан захисту інформаційного простору та національних інтересів, порядок дій при запобіганні інформаційних загроз [95, с. 25-30, 113, с. 15].

Б.А. Кормич акцентує увагу на тому, що інформаційна безпека (далі – ІБ) – це стан захисту інтересів особи, суспільства та держави, яке характеризується відсутністю збитків через неповність, несвоєчасність, та недостовірність інформації або негативного інформаційного впливу через несанкціоноване поширення інформації [85, с. 77; 8, с. 73]. Даної позиції притримується і О.П. Баранов [9, с. 60-62] та В.М. Торяник, який під ІБ розуміє захист інформаційної сфери з метою забезпечення її формування і розвитку в інтересах громадян, організацій і держав, а також захист від неправомірного зовнішнього і внутрішнього втручання [236].

Іншої наукової точки зору притримується А.А. Тер-Акопов, який під ІБ розуміє стан захисту інформації, яка забезпечує права та інтереси особи [227, с. 9].

Інші науковці (В.Т. Білоус, Н.Р. Нижник, Г.П. Ситник) під ІБ розглядають як відповідні правові норми, так і інститути безпеки, які гарантують захист

інформаційних ресурсів [117, с. 240]. К.І. Бєляков також зазначає, що під ІБ слід розуміти правову захищеність інформаційної сфери, що забезпечує її формування та розвиток [13, с. 255].

М. Галамба інформаційну безпеку розглядає як забезпечення належних умов щодо реалізації інформаційних технологій – захист інформації, інформаційного ринку, а також упровадження безпечних умов щодо функціонування та подальшого розвитку інформаційних процесів [23]. І. Громико, Т. Саханчук, О. Зіновьєв вважають, що ІБ – це захист державних та суспільних інтересів, який передбачає запобігання, виявлення та нейтралізацію інформаційних загроз, а також подальший розвиток інформаційного міжнародного співробітництва [28]. Л.С. Харченко та О.В. Логінов також притримуються позиції, що ІБ – це відповідний порядок щодо управління загрозами державними та недержавними інститутами, який сприятиме належному забезпеченню інформаційного суверенітету країни [66, с. 75]. О.Г. Данільян, О.П. Дзьобань та М.І. Панов визначають дефініцію «інформаційна безпека» як захист певного об’єкта від інформаційних загроз чи інших факторів, які пов’язано з інформацією та нерозголошенням даних, які є конфіденційними [29, с. 165].

Узагальнюючи наукові підходи правознавців, можна дійти висновку про те, що у науці права під поняттям «інформаційна безпека» розуміють:

– систему правових норм і відповідних їм інститутів безпеки (Н. Нижник, Г. Ситник, В. Білоус, К. Бєляков);

– стан захисту інтересів держави, суспільства та особи (Б. Кормич, О. Баранов, Т. Ткачук та В. Торяник);

– стан захисту інформації, яка забезпечує виключно життєво важливі інтереси людини (А. Тер-Акопов);

– запобігання, виявлення і нейтралізацію інформаційних загроз (М. Галамба, І. Громико, О. Данільян, О. Дзьобань, М. Панов, Т. Саханчук, О. Зіновьєв, Л. Харченко та О. Логінов).

Зокрема, Т.Ю. Ткачук, досліджуючи правове забезпечення інформаційної безпеки в умовах євроінтеграції України, окреслив проблемні питання щодо нормативно-правового регулювання інформаційної безпеки, здійснив порівняльний аналіз вітчизняної та європейської практики. Крім того, вчений наголошує на недоцільності законодавчого закріплення фіксованого переліку загроз інформаційній безпеці, адже він як не має, так і не може мати вичерпного характеру [234]. На думку Т.Ю. Ткачука, основна мета інформаційної безпеки України – створення безпечного інформаційного простору (захист національних інтересів (пасивна форма), протидія, контрзаходи (активна форма) [235]. Науковець розробив авторську модель комплексної системи інформаційної безпеки держави на основі поєднання національних цінностей, інтересів, цілей та надбань у сфері інформаційних правовідносин, яку втілив у авторському проєкті Закону України «Про інформаційну безпеку України».

О.Д. Довгань, досліджуючи інформаційну безпеку у контексті глобалізації [36], акцентує основну увагу на організаційно-правових аспектах нейтралізації загроз інформаційній сфері розвитку українського суспільства, у тому числі організації правового гарантування безпеки.

О.М. Головко, вивчаючи медіабезпеку людини у контексті інформаційно-правової політики» [25], запропонувала політико-правові заходи попередження загроз медіабезпеці людини.

М.М. Присяжнюк, досліджуючи інформаційну безпеку України в сучасних умовах [153], окреслив особливості впливу процесів глобалізації на інформатизацію суспільства в сучасних умовах, проаналізував загрози інформаційної безпеки України в умовах глобальної інформатизації та розвитку Інтернету.

Т.М. Мужанова у науковій праці щодо інформаційної безпеки держави [110], здійснила класифікацію національних інтересів та загроз, ретроспективний аналіз історичного розвитку, проаналізувала вітчизняну нормативно-правову базу у

зазначеній сфері, напрями державної політики, розглянула структуру та повноваження органів, що забезпечують даний напрям, висвітлила теоретичні основи та окреслила перспективи забезпечення кібербезпеки України.

Слід зазначити, що питання кібербезпеки розглядали В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа [67]. Основну увагу вчені зосередили на аналізі системи заходів із захисту від соціотехнічних атак, а також запропонували типовий алгоритм здійснення процедур із тестування систем захисту інформації в інформаційно-комунікаційних системах на предмет проникнення, а також порядок оцінювання їх параметрів на різних рівнях.

Разом з тим, у науці права мають місце і неоднозначні позиції правознавців. Так, наприклад, В.М. Лопатін, Г.Г. Почепцов, С.П. Расторгуєв, В.Я. Рубан, Г.В. Ємельянов, М.М. Потрубач під інформаційною безпекою розуміють певний стан щодо відсутності небезпеки (передумов та чинників, що загрожують безпосередньо індивідові, державі, спільноті з боку інформаційно-комунікаційного середовища) [234].

Проте ми погоджуємося із Т.Ю. Ткачуком, який не підтримує зазначену вище точку зору правознавців і вважає слушною наукову позицію І.Ф. Коржа, котрий наголошує на утопічності постановки такого питання, так як зважаючи на той факт, що соціум у процесі свого розвитку піддавався, піддається і піддаватиметься різним деструктивним впливам (загрози, небезпеки, виклики), які стають все складнішими для протидії та деструктивними за наслідками, стверджувати про «захищеність» соціуму буде надміру сміливо. Тут можна говорити про ступінь захищеності, але це ускладнить розуміння вказаного феномена [84, с. 38]. Вчений вважає, що більш реалістичним і адекватним є підхід, згідно з яким ІБ являє собою збалансований стан функціонування інститутів держави і суспільства, за якого забезпечується мінімальний вплив негативних факторів на національні інтереси держави та її громадян в інформаційному просторі. Отже, негативний вплив завжди буде і він завдаватиме певної шкоди

соціуму. Однак, за умови мінімізації цього негативного впливу, можна досягти належного функціонування вітчизняного інформаційного простору і його подальшого розвитку [84; 234].

Як бачимо, у науці права дослідженню питання щодо сутності та особливостей інформаційної безпеки приділено суттєву увагу. Разом з тим, варто акцентувати увагу на тому, що дослідження останніх років у даному напрямі охоплюють не всі сфери діяльності. Так, практично поза увагою залишилася сфера охорони здоров'я. І це з урахуванням того, що наразі в умовах прискореного науково-технічного прогресу особливої актуальності набуває подальше впровадження інформаційних технологій у різні сфери медицини. Зазначимо, що впродовж останніх років накопичено значний позитивний досвід застосування інформаційних технологій в управлінні охороною здоров'я, комп'ютерній діагностиці (в тому числі телемедичній діагностиці), в медичній освіті та науці тощо.

Аналіз наукових праць у сфері інформатизації медицини свідчить про значний інтерес дослідників до проблеми впровадження госпітальних (лікарняних) інформаційних систем та цифрових технологій у сфері охорони здоров'я. Зокрема, у працях Р.Р. Ларіної, А.В. Владзимирського, О.В. Балуєвої розкрито механізми державного забезпечення процесів інформатизації у медичній галузі [90]; Г.О. Слабкий, О.Ю. Качур та Є.М. Кривенко розробили методологічні підходи до оцінки рівня цифровізації системи охорони здоров'я України [207]; В.В. Бичков, О.С. Коваленко та Ю.С. Синекоп досліджували можливості використання телемедичних технологій у системі медицини катастроф [14]; А.Б. Зіменковський акцентував увагу на стандартизації медичної інформації в умовах реформування галузі [61]; у роботах В.М. Пономаренка, О.Ю. Майорова, В.В. Кальниша та М.В. Олиніна проаналізовано застосування інформаційних технологій у системі охорони здоров'я [133]; Г.О. Блінова зосередила увагу на проблематиці інформаційної приватності у медичній сфері [15]; Є.Б. Радзішевська та О.В. Висоцька розкрили особливості

функціонування електронної медицини (E-health) [187]; Л.Д. Удалова та Є.В. Кузьмічова-Кисленко дослідили питання забезпечення лікарської таємниці у кримінальному процесі [241]. Таким чином, коло досліджень у цій сфері охоплює як організаційно-правові аспекти інформатизації охорони здоров'я, так і технологічні, етичні та правові проблеми.

У той же час, на сьогодні практично поза увагою залишається питання щодо правових аспектів інформаційної безпеки у сфері охорони здоров'я, впровадження позитивного практичного досвіду країн Європи, і це зважаючи на те, що становлення української держави, в умовах проголошення курсу на інтеграцію до Європейського Союзу, повинно відбуватися паралельно, що, як наслідок, посприяє комплексному реформуванню усіх галузей права відповідно до законодавства ЄС.

Зазначимо, що сфера охорони здоров'я – сфера, яка надає комплексну, високоякісну та доступну допомогу всім людям, одночасно сприяючи рівності в здоров'ї та забезпечуючи стійкість розвитку країни в цілому [124]. Основне завдання медичної сфери – покращення здоров'я та благополуччя населення шляхом надання своєчасної, ефективної та високоякісної медичної допомоги.

Інформаційна безпека у сфері охорони здоров'я – комплексна система захисту інформаційного середовища, яка забезпечує запобігання, виявлення і нейтралізацію інформаційних загроз, а також цілісність, конфіденційність та доступність інформації, тим самим забезпечуючи формування та розвиток інформаційного середовища у медичні сфері в інтересах держави, суспільства та особистості.

У контексті забезпечення інформаційної безпеки у сфері охорони здоров'я важливе значення має Стратегія розвитку інформаційного суспільства в Україні, затверджена розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р. У документі визначено новий для України підхід до модернізації медичної галузі, який полягає у створенні єдиної інтегрованої інформаційно-аналітичної системи обліку стану здоров'я населення. Передбачається охоплення як громадян України, так і іноземців та осіб без громадянства, що перебувають на території

держави на законних підставах. Основою цієї системи є електронна ідентифікація пацієнтів у медичних закладах та збір даних профілактичних обстежень з подальшим використанням їх в аналітичних, експертних і статистичних цілях. Згідно з положеннями Стратегії, електронна медицина (е-медицина) визначається як діяльність, пов'язана з використанням електронних інформаційних ресурсів у сфері охорони здоров'я та забезпеченням оперативного доступу до них як медичних працівників, так і пацієнтів [226].

Разом з цим, важливою умовою створення зазначеної системи є саме забезпечення дотримання норм ст. 8 Конвенції про захист прав людини і основоположних свобод, створення системи дистанційного консультування та діагностики з використанням інформаційно-комунікаційних технологій, що об'єднують великі заклади охорони здоров'я та наукові установи. Е-медицина повинна забезпечувати взаємодію між пацієнтами, медичними працівниками та установами за допомогою інформаційно-комунікаційних технологій.

Серед основних напрямів діяльності у сфері розвитку е-медицини, передбачених Стратегією розвитку інформаційного суспільства в Україні, варто виокремити:

– впровадження автоматизованих інформаційних галузевих систем, які, зокрема, дають змогу перейти до ведення медичної документації в електронному вигляді; розвиток телемедицини;

– удосконалення розвитку системи моніторингу стану здоров'я населення;

– створення та впровадження нових комп'ютерних технологій профілактики захворювань, діагностики, забезпечення лікувальних процесів;

– створення загальнодоступних електронних медичних ресурсів [226].

Як бачимо, у передбачених Стратегією розвитку інформаційного суспільства напрямах не звернено увагу на належний технічний захист як автоматизованих інформаційних галузевих систем, так і взагалі медичної інформації. Відповідно, пропонуємо доповнити п. 1 сфери діяльності «Е-

медицина», розділу «Етапи та основні напрями реалізації» Стратегії розвитку інформаційного суспільства та викласти його у наступній редакції: упровадження автоматизованих інформаційних систем, які сертифіковано на відповідність КСЗІ, що надають змогу перейти до ведення медичної документації в електронному вигляді.

Крім того, Закон України «Про захист персональних даних» не регулює у повній мірі можливі ризики, які виникають під час обробки даних у мережі Інтернет. Тобто недосконалість правових норм у даному напрямі як наслідок призводить до масових витоків даних, які характерні як для України, так і міжнародних країн. Так, наприклад, у 2018 році в Сінгапурі група медичних закладів «SingHealth» стала жертвою цілеспрямованої хакерської атаки – викрадено персональні дані 1,5 мільйонів осіб, а також амбулаторні рецепти 160 тисяч чоловік, включаючи прем'єр-міністра країни та інших членів уряду [71]. У грудні 2020 року у відкритому доступі в Інтернеті виявилися персональні дані громадян, інфікованих коронавірусом у квітні-травні 2020 року. За результатами перевірки в архіві виявлено понад 105 тисяч записів (повні імена хворих, номери телефонів, супутні діагнози і результати перевірок дотримання карантину). На думку керівника компанії «Інтернет-розшук» І. Бедерова, найбільш вірогідною є версія, що списки хворих формувались у Excel у медичних закладах, а потім пересилались у мерію чи Міністерство охорони здоров'я. Таблиці могли «гуляти» по міністерствах, відомствах у вигляді посилань на GoogleDrive, де їх і виявили [101]. І це зважаючи на те, що розголошена інформація відноситься до «чутливих даних» – категорія персональних даних, які потребують вищого рівня захисту.

Слід зазначити, що у вересні 2017 року в Україні розроблено та запроваджено Електронну систему охорони здоров'я «E-Health», інформаційно-телекомунікаційну систему, яка забезпечує єдиний інформаційний простір та обмін даними через Центральну базу даних [242]. В систему інтегровано укладання

електронних декларацій з сімейними лікарями, виписки рецептів, медичні направлення, статистику щодо хворих на коронавірус тощо.

Функціоналом упровадженої у медичну сферу електронної системи «E-Health» передбачено збір і обмін інформацією між центральним «компонентом» і безпосередньо користувачами, відповідно, медичні інформаційні системи(далі – МІС) є посередниками. Згідно з чинним вітчизняним законодавством, у разі збору, зберігання та оброблення інформації, яка становить персональні дані, у контексті досліджуваного «чутливі дані», – передбачено її належний технічний захист, який забезпечить надійність інформації, що генерується, зберігається та обробляється.

Проте дана система, у порушення вимог норм з технічного захисту інформації, майже рік існування не мала сертифікату про відповідність КСЗІ, а тому безпечним назвати зберігання даних пацієнтів не можна було. Крім того, навіть при наявності сертифікату, будь-яка інформаційна система має певні загрози. Слід зазначити, що сертифікат комплексної системи захисту інформації не дає відповідних гарантій. Для прикладу, під час аудиту будь-якої інформаційної системи (як локальної, так і хмарної) проводиться перевірка програмного забезпечення. Підтверджуючим документом, який за результатами перевірки видає Держспецзв'язок, є висновок про програмне забезпечення. Проте у разі, якщо ви придбали програмне забезпечення, яке відповідає вимогам безпеки, проте виготовлене іншою компанією, необхідно чітко усвідомлювати, що інформаційна система не є безпечною. Тобто аудит чи сертифікація Держспецзв'язку охоплює всю інформаційну систему, а не програму чи сервер [39].

Крім того, сертифікований захист потребує значних фінансових витрат. Так, наприклад, при упровадженні МІС у Києво-Святошинському районі (42 відокремлені амбулаторії), компанія звернулася за аудитом, вартість аудиту (для КСЗІ) однієї точки – 50 тис. грн. [39].

Наразі Міністерство охорони здоров'я разом з Міністерством цифрових трансформацій працює над інтеграцією системи «E-Health» у портал та додаток

«Дія». З метою покращення ефективності захисту інформації у даній системі пропонуємо при розробці програмного забезпечення дотримуватись вимог HIPAA (закон США про мобільність та підзвітність медичного страхування, особливістю якого є передбачення, за певних умов, можливості здійснення розкриття інформації про стан здоров'я чи надання медичних послуг (PHI) в цілях лікування без попередньої згоди пацієнта).

Підсумовуючи, ми дійшли висновку, що на сьогодні, зважаючи на активну фазу розвитку інформаційного суспільства, інформаційна безпека виступає як основна цінність держави, забезпечення якої гарантує її стабільне функціонування та поступальний розвиток. Проблематика інформаційної безпеки у сфері охорони здоров’я, яка має місце на сьогодні, виникла через певні протиріччя між технічними можливостями інформаційних ресурсів та загрозами щодо їх реалізації, а також відсутністю належного рівня інформаційної культури як серед працівників медичної сфери, так і суспільства загалом.

Зміст дефініції «інформаційна безпека» поділяють на дві групи: до першої відноситься захист інформації, інформаційних ресурсів, держави, суспільства та особистості; до другої – загрози інформаційної безпеки. Констатовано відсутність єдності поглядів серед правознавців щодо визначення сутності інформаційної безпеки. Окреслено основні напрями, у яких розглядається інформаційна безпека: стан правових норм і відповідних їм інститутів безпеки; стан захищеності життєво важливих інтересів держави, суспільства та особи; запобігання, виявлення і нейтралізація внутрішніх та зовнішніх інформаційних загроз.

Теоретично обгрунтовано, що у передбачених Стратегією розвитку інформаційного суспільства напрямах подальшого розвитку «Е-медицини» не звернено увагу на належний технічний захист як автоматизованих інформаційних галузевих систем, так і взагалі медичної інформації. Відповідно, запропоновано доповнити п. 1 сфери діяльності «Е-медицина», розділу «Етапи та основні напрями реалізації» Стратегії розвитку інформаційного суспільства та викласти його у

наступній редакції: упровадження автоматизованих інформаційних систем, які сертифіковано на відповідність КСЗІ, що надають змогу перейти до ведення медичної документації в електронному вигляді.

У дослідженні сформульовано авторське визначення інформаційної безпеки у сфері охорони здоров'я, яке пропонується розглядати як цілісну систему захисту інформаційного середовища, спрямовану на запобігання, виявлення та нейтралізацію інформаційних загроз, забезпечення конфіденційності, цілісності й доступності медичних даних. Такий підхід створює умови для сталого розвитку інформаційного простору у медичній сфері в інтересах держави, суспільства та кожної особи.

Запропоновано класифікацію ключових механізмів функціонування комплексної системи інформаційної безпеки в охороні здоров'я, зокрема:

– правовий механізм – включає правові норми та гарантії захисту даних в автоматизованих інформаційних системах (АІС), що використовуються у медичних закладах, заходи із запобігання витокам інформації, проведення службових розслідувань у разі порушення режиму інформаційної безпеки та притягнення винних осіб до відповідальності;

– технічний механізм – передбачає застосування засобів і технологій для забезпечення цілісності, конфіденційності та доступності інформації;

– комунікаційно-освітній механізм – спрямований на підвищення рівня інформаційної культури та доступності АІС, у тому числі через впровадження обов'язкових навчальних курсів (зокрема дистанційних) з питань інформаційної безпеки, а також щорічного підвищення кваліфікації працівників, які працюють з інформаційними системами. У межах цього напряму особливу увагу приділено ознайомленню персоналу з новими нормативно-правовими актами та адаптації позитивного міжнародного досвіду.

Для підвищення ефективності діяльності в цьому напрямі необхідно систематизувати чинне законодавство та привести його у відповідність до міжнародних стандартів. Зокрема, запропоновано імплементувати позитивний

міжнародний досвід Сполучених штатів Америки (Закон США «Про мобільність та підзвітність медичного страхування»(HIPAA)), відповідно, розробити окремий нормативно-правовий акт, який на законодавчому рівні регулював би збір, обробку, розкриття та передачу медичної інформації.

Крім того провести комплексний аудит правового, технічного, комунікаційного та освітнього компонентів у медичній сфері, за результатами якого розробити план щодо подальшого удосконалення даного напряму діяльності із передбаченням внесення корегувань до Стратегії інформаційної безпеки.

1.2. Поняття медичної інформації: сутність, види, особливості

Що б при лікуванні – також без лікування – я не побачив чи не почув стосовно життя людського з того, що не потрібно коли-небудь розголошувати, я змовчу про те, рахуючи подібні речі таємницею

Клятва Гіппократа

У сучасних умовах життя людини нерозривно пов’язане з інформаційними процесами, що визначають рівень її правової та соціальної захищеності. У сфері медичного права одним із ключових чинників забезпечення належного правового статусу пацієнта є законодавче врегулювання обігу медичної інформації. Конституційне право на доступ до інформації закріплено у ст. 34 Конституції України, де воно розглядається як право кожного громадянина на свободу думки та слова, вільне висловлення поглядів і переконань, а також на отримання, зберігання, використання та поширення відомостей [78]. Разом із тим закон передбачає можливість встановлення обмежень у визначених випадках, зокрема: для забезпечення національної безпеки, територіальної цілісності чи громадського

порядку; з метою охорони здоров’я; а також для запобігання розголошенню інформації, отриманої під час виконання службових обов’язків тощо [231].

Відповідно до міжнародних правових норм, медичні записи (інформація) є частиною права на інформаційну приватність [149]. Приватність (від латин. Privatus – приватний, окремий, домашній) пов’язують з людською гідністю [7]. Право на приватність – кодифіковане основоположне право людини, регламентоване Загальною декларацією ООН про права людини 1948 року (ст. 12), Міжнародним пактом про громадянські та політичні права 1966 року (ст. 17), Конвенцією ООН про права дитини (ст. 16), Європейською конвенцією з прав людини (ст. 8). Складовою права на приватність є право на інформаційну приватність (захист інформаційних даних), яке урегульовано Керівними принципами ОЕСР щодо захисту конфіденційності та транскордонних потоків персональних даних, Конвенцією Ради Європи про захист фізичних осіб щодо автоматичної обробки персональних даних, Хартією Європейського Союзу про основні права та іншими нормативними актами.

Беручи до уваги, що життя і здоров'я людини є найвищими суспільними цінностями, інформація про неї стає важливою складовою соціальної характеристики громадянина як учасника всіх суспільних відносин. Нам імпонує наукова позиція О.В. Негодченка, який стверджує, що тільки при «виваженому» використанні інформації про стан здоров'я особи можливо врятувати її життя. Водночас, необмежене, вільне та бездумне поширення такої інформації може спричинити погіршення стану здоров'я, включаючи й інших осіб [116].

Зазначена проблематика, як слушно зазначає Х.Я. Терешко, «сенситивна, людиноцентристська», адже є особливо вразливою, про що неодноразово у своїх рішеннях наголошував Європейський суд з прав людини: охорона інформації особистого характеру (особливо медичної) має ключове значення для забезпечення права щодо поваги як до приватного, так і сімейного життя. Крім того, саме дотримання конфіденційності інформації про здоров’я – основний принцип держав-

учасниць Конвенції (справа «М.С. проти Швеції», 1997) [229] у частині щодо дотримання прав людини.

Кожна людина протягом життя звертається за медичною допомогою й, звичайно, не зацікавлена в розголошенні фактів як безпосереднього звернення за медичною інформацією, так і про діагноз та лікування. Так, звертаючись до лікаря, пацієнт очікує, що медичний працівник дотримається конфіденційності щодо відомостей, отриманих під час надання медичної допомоги. Проте часто трапляються ситуації, коли лікар, оглянувши пацієнтів у палаті, без їхньої згоди оголошує результати огляду, лабораторні дослідження та діагноз у присутності інших хворих. Після операції хірург, не враховуючи волю пацієнта, надає інформацію про оперативне втручання та перспективи одужання його близьким та родичам. Медичний персонал, відповідаючи на телефонні дзвінки, надає інформацію людям, які представилися членами родини. Багато телепрограм демонструють шоу, використовуючи медичну інформацію, що призводить до знецінення морально-етичних принципів. Таких випадків на сьогодні існує безліч. Однак більшість лікарів навіть не замислюються над тим, що розголошення інформації без згоди пацієнта є прямим порушенням його права на конфіденційність інформації [100].

Так, наприклад у справі «Пантелеєнко проти України» (заява № 11901/02 від 29.06.2006 р.) заявник поскаржився на розголошення під час судового засідання конфіденційної інформації стосовно його психічного стану та психіатричного лікування. Європейський суд з прав людини (далі –ЄСПЛ) постановив, що отримання відомостей від психіатричної лікарні про психічний стан заявника та відповідне лікування, а також їх розголошення на відкритих слуханнях, становило втручання в право заявника на повагу до особистого життя. ЄСПЛ визнав порушення статті 8 Конвенції про захист прав людини і основоположних свобод у частині, що стосується обшуку офісу заявника та розповсюдження відомостей конфіденційного характеру щодо його психічного стану. Суд зазначив, що деталі

цього питання не могли вплинути на результат судового процесу, і що запит суду першої інстанції на отримання цієї інформації був зайвим, оскільки вона не була «важливою для розслідування, попереднього розслідування чи суду», що зробило цей запит незаконним згідно із Законом про психіатричну лікарську допомогу [212].

Підсумовуючи, ми дійшли висновку, що право на здоров'я є багатогранним і включає: право на доступ до інформації та її конфіденційність; право на медико-соціальну допомогу; право на згоду на лікування та медичне втручання [134].

Правове забезпечення конфіденційності медичної інформації в Україні зазнало суттєвого вдосконалення після прийняття Закону України «Про захист персональних даних». У статті 7 цього Закону передбачено заборону на обробку персональних даних, що здійснюється у цілях охорони здоров’я, встановлення діагнозу, організації догляду чи лікування та надання медичних послуг, за умови, що така обробка відбувається виключно медичним працівником або іншою уповноваженою особою закладу охорони здоров’я, на яку поширюється обов’язок збереження лікарської таємниці та відповідне законодавче регулювання [168].

Як слушно зазначає Г.О. Блінова, закріплення такої норми формує подвійний механізм захисту чутливих відомостей про стан здоров’я пацієнта: з одного боку – у режимі лікарської таємниці, а з іншого – у правовому режимі персональних даних [15]. Водночас заслуговує на увагу той факт, що в окремих нормативно-правових актах поряд із категорією «лікарська таємниця» використовується й поняття «медична інформація». У результаті виникає колізійна ситуація, коли одна і та сама інформація охороняється у межах різних правових режимів – лікарської таємниці, медичної таємниці та персональних даних.

Положення про лікарську таємницю вперше було чітко сформульовано в клятві Гіппократа: «Що б я не побачив або не почув під час лікування чи поза ним, стосовно життя людського, що не слід розголошувати, я збережу мовчання, вважаючи такі речі таємницею» [24, с. 88]. Слід зазначити, що за аналогією зазначеної клятви у XX столітті створено сестринську клятву «Клятва Лоренс

Найтінгейл», у якій зазначено про нерозголошення будь-якої інформації, яка буде у розпорядженні під час роботи з пацієнтами та його рідними [70]. Зазначені норми закріплено і в «Клятві лікаря», затвердженій Указом Президента України від 15.06.1992 р. № 349: дотримуватися норм чинного законодавства щодо збереження лікарської таємниці, та жодним чином не використовувати її на шкоду особі. Вірність цій Клятві присягаю пронести через усе своє життя [172].

Відповідно до Конституції України, кожна особа має гарантоване право на охорону здоров'я та страхування (ст. 49), а також захищене право на конфіденційність особистої інформації, зокрема медичної, яка не може збиратися, зберігатися, використовуватися або поширюватися без згоди суб'єкта, за винятком випадків, прямо передбачених законом (ст. 32) [78]. Крім того, положення частини 1 статті 286 Цивільного кодексу України та частини 1 статті 39-1 Основ законодавства України про охорону здоров'я встановлюють, що фізична особа має право на захист інформації про власний стан здоров'я, включно з фактами звернення за медичною допомогою, діагнозами та результатами обстежень [249; 121].

На думку А.С. Дворніченко, ключовим завданням у процесі європейської інтеграції медичної сфери є закріплення та впровадження європейських принципів у законодавство України, яке регулює права пацієнтів[31].Пацієнту, який звернувся за медичною допомогою, повинна гарантуватися інформаційна конфіденційність [134].

Разом з цим, у вітчизняному законодавстві поряд із поняттям «медична інформація» вживається дефініція «лікарська таємниця». З цього приводу у науці права тривають дискусії. Одні вчені (В. Головченко, Л. Грузова, І Купова, І. Петрухіна) вважають, що лікарська таємниця – один із видів медичної інформації. Інші (А. Марущак, М. Хавронюк) притримуються позиції, що це абсолютно різні поняття.

Що ж являє собою поняття «лікарська таємниця»? Первинне теоретичне уявлення про сутність та особливості лікарської таємниці формують словники. Зокрема, відповідно до Академічного тлумачного словника, лікарська таємниця – конфіденційна інформація про звернення громадянина за медичною допомогою щодо стану його здоров'я, діагнозу та інших відомостей, отриманих у зв'язку із лікуванням, що забезпечується морально-правовими гарантіями [1]. Лікарська таємниця у трактуванні Великого юридичного енциклопедичного словника – це інформація щодо звернення за допомогою до медичної установи, стану здоров'я громадянина, діагнозу його захворювання, інших відомостей, отриманих при обстеженні та лікуванні [10, с.95].

На думку М.І. Хавронюка, лікарська таємниця охоплює документи, що містять відомості про діагнози, проведені обстеження, огляди, а також інформацію особистого та сімейного характеру. Зокрема, правознавець включає до цього поняття такі аспекти: звернення за психіатричною допомогою, лікування або перебування у відповідних медичних закладах, інші дані про психічний стан особи та її приватне життя; факти зараження інфекційними хворобами, що передаються статевим шляхом, результати відповідних медичних оглядів; відомості інтимного характеру, отримані медичними працівниками та посадовими особами у процесі виконання професійних обов'язків; результати медичних обстежень осіб, які подали заяву на реєстрацію шлюбу [111; 116].

До зазначеного вище переліку І.В. Смолькова та В.Н. Лопатін також відносять інформацію щодо факту звернення громадянина за медичною допомогою, про його особисті та сімейні таємниці, дані про трансплантацію, штучне запліднення ембріона, а також відомості про особу донора [210, с. 12; 99, с. 36].

А.І. Марущак зазначає, що до лікарської таємниці також належать відомості про перенесені та наявні захворювання у особи, яка бажає здати кров або її компоненти, а також інформація про вживання нею наркотичних речовин та інші форми ризикованої поведінки [102].

В.І. Акопов під даним поняттям розуміє усю інформацію, отриману чи встановлену від пацієнта при чи за результатами його обстеження чи лікування, яка не розголошується без його згоди [2].

Зарубіжні вчені лікарську таємницю розуміють як зобов'язання лікаря, який, не зважаючи на згоду пацієнта на розкриття інформації, обирає мовчання [260, с. 6], договірні відносини, у яких лікар виступає зобов'язаною особою, а пацієнт – уповноваженою особою [260, с. 6-7].

Об'єктом лікарської таємниці, відповідно до ст. 286 Цивільного кодексу України та ст. 39-1 і 40 Основ законодавства України про охорону здоров'я, є інформація, що стосується факту звернення за медичною допомогою, стану здоров'я, результатів огляду та діагностичних обстежень, методів лікування, а також дані інтимного або сімейного характеру.

Згідно із Законом України «Про застосування трансплантації анатомічних матеріалів людині», до лікарської таємниці належать відомості про реципієнтів та осіб, які дали або не дали згоду на донорство після смерті [161]. Додатково, п. 2 ст. 14 розділу IV Закону України «Про безпеку та якість донорської крові та компонентів крові» встановлює, що лікарська таємниця охоплює інформацію про перенесені та поточні захворювання донорів, вживання ними наркотичних речовин та інші форми ризикованої поведінки, що потенційно можуть сприяти зараженню інфекційними хворобами, передаваними через кров, та обмежувати виконання донорської функції [155].

Таким чином, лікарська таємниця – інформація конфіденційного змісту про звернення особи за медичною допомогою, стан здоров'я, лікування (обстеження, діагноз, реабілітація), яка не підлягає розголошенню без її згоди.

Перейдемо до аналізу поняття «медична інформація». Уперше це поняття закріплено рішенням Конституційного Суду України (далі – КСУ) у справі К. Г. Устименка від 30 жовтня 1997 року. Відповідно до зазначеного вище рішення, медична інформація – інформація щодо стану здоров'я особи, історії хвороби, мети

досліджень та лікування, можливого подальшого прогнозу, у тому числі ризику для життя та здоров'я, яка за правовим режимом належить до конфіденційної [192; 179].

Відповідно до частини 3 статті 39 Основ законодавства України про охорону здоров'я, медична інформація – інформація щодо стану здоров'я пацієнтів, мети проведення досліджень і, відповідно, лікування, прогнозу можливого подальшого розвитку хвороби, у тому числі і наявності ризику для життя і здоров'я [121].

Порівнюючи наведене визначення з тлумаченням, запропонованим рішенням Конституційного Суду України, слід зауважити, що їхній зміст значною мірою збігається. Водночас визначення поняття «медична інформація» в Основах законодавства України про охорону здоров'я не включає відомості про історію хвороби пацієнта, що, на нашу думку, є важливим недоліком, оскільки саме ця інформація має вирішальне значення для забезпечення повного захисту прав пацієнта та належного медичного обслуговування.

Продовжуючи аналіз зазначимо, що в Етичному кодексі лікаря [41] дефініцію поняття «медична інформація» не закріплено, зазначено лише про право пацієнта на вичерпну інформацію. Проте чіткого регламентування обсягу наданої інформації не передбачено.

У статті 285 Цивільного кодексу України (далі – ЦК України) термін «медична інформація» законотворцями розглянуто під іншим кутом. Вони співвідносять поняття «медична інформація» та «інформацію щодо стану здоров'я». Інформація щодо стану здоров'я – сукупність відомостей щодо стану здоров'я, у тому числі можливість ознайомитися з документами медичного характеру [249]. Як бачимо, інформація щодо стану здоров'я, згідно з ЦК України, складова медичної інформації.

Варто акцентувати увагу, що лише у 2018 році, з урахуванням стрімкого реформування медичної сфери та актуалізації «інформаційної революції» у даному напрямі, у вітчизняному законодавстві визначено дефініцію «медична інформація». Зокрема, відповідно до Порядку функціонування електронної системи охорони

здоров’я, затвердженого постановою КМУ від 25.04.2018 р. № 411, медична інформація – це інформація щодо стану здоров’я пацієнтів, їх діагнозів, відомостей, отриманих за результатами медичного огляду, у тому числі відповідні медичні документи [144].

Наказом Міністерства охорони здоров’я (далі – МОЗ) «Про затвердження Порядку проведення судово-психіатричної експертизи» від 08.05.2018 р. № 8657 визначено, що під відомостями, які належать до медичної інформації розуміються копія рішення суду про застосування примусового заходу медичного характеру, копія акту судово-психіатричної експертизи або акту психіатричного огляду, листування адміністрації психіатричного закладу з установами й родичами з приводу психічного стану цієї особи, її соціально-побутових питань і, за потреби, медичні довідки [164]. Відповідно до п. 16 зазначеного наказу, у разі надходження документів, що містять відомості щодо стану здоров’я особи, щодо якої призначено відповідну експертизу, факту звернення за допомогою, діагнозу, інформації інтимного та сімейного змісту, а також інших відомостей, одержаних під час її медичного обстеження, експерт зобов’язаний запросити у органу (особи), який (яка) призначив(ла) експертизу (залучив(ла) експерта), згоду цієї особи на використання зазначеної інформації. У разі проведення посмертної СПЕ або призначеної слідчим суддею чи судом, зазначена інформація використовується без згоди особи [164].

Пунктом 2.5 наказу Міністерства охорони здоров’я «Про інфекційну безпеку донорської крові та її компонентів» від 01.08.2005 р. № 385 передбачено, що інформація про захворювання осіб (ВІЛ, вірусні гепатити, сифіліс та інші інфекції, визначені МОЗ України), завірена належним чином, негайно надається регіональним закладам переливання крові відповідними територіальними службами з дотриманням вимог чинного законодавства щодо медичної інформації [170].

Об'єктом медичної інформації є усі відомості, отримані як у процесі, так і під час надання медичної допомоги. Тобто відомості, витік яких може зашкодити пацієнту. Медичну інформацію поділяють на медичну інформацію та інформацію немедичного характеру (особисте та сімейне життя) [221].

Пунктом 12 Рекомендацій щодо охорони здоров'я працівників на місцях № 97 передбачено необхідність вжиття відповідних заходів щодо нерозголошення медичної інформації при проведенні медичних оглядів, реєстрації та зберіганні документів, що їх стосуються [191].

Таким чином, ще раз наголосимо на тому, що поняття «медична інформація» охоплює не лише медичні аспекти взаємовідносин між лікарем і пацієнтом, але й увесь обсяг відомостей, яку лікарі, медичний чи обслуговуючий персонал отримують від пацієнта під час спілкування з ним [6].

Що стосується міжнародно-правових норм, то вони під поняттям «медична інформація» розуміють:

– інформацію про пацієнта щодо стану його здоров'я, які містяться у будь-яких медичних записах. Право бути повністю поінформованим щодо стану здоров'я. Однак конфіденційна інформація щодо третіх осіб, яка міститься у записах пацієнта, не повинна надаватися пацієнтові без дозволу такої третьої особи. У надзвичайних випадках відомості можуть не надаватися пацієнтові за наявності достатніх підстав для припущення, що така інформація створить серйозну загрозу його життю чи здоров'ю. Інформацію необхідно повідомляти відповідно до особливостей місцевої культури й так, аби вона була зрозумілою пацієнту. На пряме прохання пацієнта інформація може йому не надаватися, якщо тільки цього не потрібно для врятування життя іншої особи. Йому також надається право обрати особу, якій необхідно повідомляти відомості про нього (Лісабонська декларація про права пацієнтів, принцип 7 (1981)) [96];

– інформація щодо стану здоров’я пацієнта, відповідні послуги медичного характеру та способи їх отримання, а також про все, що доступно завдяки науково-технічному прогресові (Європейська хартія прав пацієнтів, ст. 3 (2002)) [43];

– відомості щодо стану здоров’я, діагноз, можливі ризики і переваги методів лікування, інформацію про подальший план лікування (Декларація про політику в галузі дотримання прав пацієнта в Європі, ч. 2 ст. 2 (1994) [32].

Не можна оминути увагою і те, що відповідно до ст. 10 Конвенції про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину від 04.04.1997 р., підписаної, але не ратифікованої Україною 22.03.2002 р.: кожна особа має право на повагу до її особистого життя стосовно інформації про її здоров’я. Кожна особа має право на ознайомлення із будь-якою зібраною про її здоров’я інформацією. Однак бажання осіб не отримувати такої інформації має також поважатися. У виняткових випадках в інтересах пацієнта здійснення викладених у п. 2 прав може обмежуватися законом [75].

Таким чином, медична інформація – це конфіденційна інформація про фізичну особу, яка стала відома у процесі звертання її до медичного закладу з метою отримати допомогу (факт звернення, стан здоров'я, огляд, діагноз, результати обстеження, методи лікування), а також уся інформація, яку працівники медичних закладів (лікарі, медичний чи обслуговуючий персонал) одержують від пацієнта у процесі спілкування з ним, розголошення якої може зашкодити пацієнтові.

Який же із цих двох термінів більш прийнятний для використання? На думку М.І. Мельника та М.І. Хавронюка, лікарська таємниця (інформація про пацієнта – щодо стану здоров’я, історію хвороби), відрізняється від медичної інформації (інформації для пацієнта – окрім відомостей щодо стану здоров’я людини, історії її хвороби, передбачено визначення мети запропонованих обстежень та відповідного лікування, а також можливий подальший прогноз, які лікар повинен надавати на вимогу пацієнта, членів його родини або законних

представників, за винятком випадків, коли така повна інформація може зашкодити здоров'ю пацієнта) [111, с. 332]. Таким чином, основним критерієм поділу інформації на ці два види науковці визнають саме мету її збереження та використання [235].

С.Г. Стеценко вважає, що термін «лікарська таємниця» не зовсім точно відображає обов'язок щодо збереження конфіденційної інформації про пацієнта. Він пропонує використовувати більш точний термін «медична інформація», який охоплює всю сферу медицини та підкреслює, що обов'язок зберігати в таємниці отримані відомості стосується не лише лікарів, але й інших медичних працівників. Особливо з огляду на стрімкий розвиток інформаційних технологій, реформи в медичній сфері та комплексний характер сучасної медичної допомоги, конфіденційна інформація часто стає доступною не лише лікарям, а й представникам інших професій [222]. Даної наукової позиції притримується і І.Я. Сенюта та Г.О. Блінова [235].

З урахуванням доктринальних позицій зазначених вище науковців, міжнародних правових норм, а також зважаючи на результати дослідження, ми дійшли висновку, що поняття «медична інформація» набагато ширше аніж «лікарська таємниця», так як «лікарська таємниця» – це інформація конфіденційного змісту про звернення особи за медичною допомогою, стан здоров'я, лікування (обстеження, діагноз, реабілітація), а «медична інформація» – конфіденційна інформація про фізичну особу, яка стала відома у процесі звертання за допомогою (факт звернення, стан здоров'я, огляд, діагноз, результати обстеження, методи лікування, інформація інтимного та сімейного характеру), а також інформація, яку працівники медичних закладів (лікарі, медичний чи обслуговуючий персонал) одержують від пацієнта у процесі спілкування з ним, розголошення якої може зашкодити. Відповідно, пропонуємо, на законодавчому рівні звести термінологічний апарат у даній сфері до терміна «медична інформація».

Держава виступає гарантом захисту прав людини, у тому числі і на інформацію. Доречною в цьому контексті є наукова думка О.Г. Марценюка, який зазначає, що забезпечення права людини, зокрема на доступ до медичної інформації, визначає як рівень демократичності держави, так і ступінь інтеграції національного права у світове співтовариство, відповідність правових норм міжнародно-правовим стандартам [103].

Статтею 6 Основ законодавства України про охорону здоров'я та статтею 285 ЦК України визначено, що пацієнту надано право на таємницю інформації щодо стану здоров'я та діагнозу, який йому встановлено при обстеженні. Тобто медичний працівник має право розголошувати медичну інформацію тільки за умови отримання згоди пацієнта, її законних представників та в інших випадках, передбачених вітчизняним законодавством.

В окремих випадках чинним законодавством встановлено певні обмеження щодо можливості одержання пацієнтом відомостей щодо стану здоров'я. Так, ч. 3 ст. 285 ЦК України передбачено, що у разі, коли відомості щодо стану здоров'я фізичної особи можуть погіршити його стан або ж стан здоров'я батьків (усиновлювачів), опікунів, піклувальників, зашкодити лікуванню, лікарям надано право на надання неповної інформації щодо стану здоров'я фізичної особи, обмеження можливості ознайомлення їх з деякими медичними документами [249].

Варто зазначити, що надання «повної» інформації передбачає передачу всіх наявних у медичному закладі документальних даних, зібраних про пацієнта, а також відомостей про стан його здоров'я, історію захворювання, можливі ризики, пов'язані із захворюванням або запропонованим лікуванням. Крім того, це включає інформацію про освіту, кваліфікацію та компетенцію лікаря і медичного персоналу, а також дані про надання відповідних послуг та способи їх отримання в лікувально-профілактичному закладі, що надає допомогу пацієнту [103].

Крім ЦК України, це передбачено і статтею 39 Основ законодавства України про охорону здоров'я. Зокрема, право на отримання достовірної та повної

інформації щодо стану здоров’я, у тому числі щодо ознайомлення з документами, які його стосуються, мають: повнолітній пацієнт (щодо стану здоров’я); батьки (усиновлювачі), опікун, піклувальник (відомості щодо стану стан здоров’я дитини чи підопічного).

Крім того, зазначеною вище статтею передбачено, що лікар повинен надати пацієнтові відомості щодо стану його здоров’я, ознайомити з метою досліджень, планом лікування, можливим прогнозом розвитку хвороби, а також повідомити про ймовірні ризики. У разі ж, якщо відомості про діагноз пацієнта можуть погіршити його стан здоров’я чи інших фізичних осіб, визначених ч. 2 цієї статті, зашкодити лікуванню, лікарі надають неповну інформацію та обмежують доступ до деяких медичних документів. У випадку, коли пацієнт помирає, членам його родини чи уповноваженим ними особам надається можливість бути присутніми при проведенні дослідження щодо встановлення причин його смерті та, відповідно, ознайомлення з їх результатами, а також право щодо їх, у разі необхідності, оскарження [121].

Дану норму ще у грудні 2007 року було передбачено і в проєкті Закону України «Про захист прав пацієнтів» № 1132,поданому на розгляд народним депутатом України Ю. Каракаєм. Зокрема, відповідно до ст. 14 законопроєкту: пацієнту надається право на одержання інформації щодо стану здоров'я, діагнозу, історії хвороби, лікування, способів профілактики, можливих ризиків, пов'язаних з медичним втручанням. Медична інформація (документація) може не надаватися пацієнту для ознайомлення, не видаватися у вигляді виписок і копій у разі, якщо ця інформація може завдати серйозної шкоди здоров'ю пацієнта чи здоров'ю члена його родини, спричинивши тим самим порушення права на його безпеку, стосується інших осіб, обставин їхнього життя і може призвести до порушення прав цих осіб на недоторканість особистого життя, стосується виключно адміністративних питань діяльності медичної установи [73].

Розглянемо це на конкретному прикладі. Так, досить розповсюдженими є випадки, коли від пацієнта, у якого діагностовано онкозахворювання чи інший вид тяжкого за наслідками захворювання (відповідно до чинного законодавства пацієнту надано право знати повну інформацію про захворювання, його наслідки, способи лікування і прогноз) лікарі, з метою запобігання погіршення стану здоров'я пацієнта, у разі отримання фактичної інформації про діагноз, повідомляють про нього найближчим родичам.

На практиці часто виникають питання щодо того, хто, на якій підставі та в якому порядку має право отримувати інформацію про пацієнта, ознайомлюватися з документами, що містять медичну інформацію, вимагати їхні копії, а також витребувати чи вилучати оригінали таких документів [27].

Статтею 29 Закону України «Про інформацію» передбачено, що інформація з обмеженим доступом може бути поширена у разі, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення [171].

Н.В. Кірнос вважає, що інформація конфіденційного характеру може бути надана лише за умови наявності персональної згоди пацієнта або у випадках, передбачених законом. Лікувальний заклад, так само як і медичні працівники, несе відповідальність за збереження та нерозголошення інформації про стан здоров'я пацієнтів, включаючи дані про їхнє особисте життя, які стали відомі під час надання медичної допомоги, а також інформації, що міститься в письмових документах, архівах та комп'ютерних базах даних [69; 136].

Доступ до документів, що містять медичну інформацію, можливий на підставі ухвали слідчого судді про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження, крім обставин, передбачених частиною 5 статті 163, доведе можливість використання як доказів відомостей, що містяться в цих речах і документах, та неможливість іншими способами довести обставини, які передбачається довести за допомогою цих речей і документів [89].

Для прикладу, у справі «Л.Л. проти Франції» (заява № 7508/0) від 10.10.2006 р.) заявник скаржився на те, що його медичні документи були передані на розгляд і використані судами в контексті шлюборозлучного процесу без його згоди та без участі медичного експерта. Європейський суд з прав людини постановив, що було порушено статтю 8 Конвенції (право на повагу до особистого та сімейного життя), оскільки втручання в особисте життя заявника не було виправданим з огляду на важливість захисту персональних даних. Суд зазначив, що французькі суди використовували оскаржуваний медичний висновок лише як допоміжний засіб для ухвалення рішень, але їхні рішення могли бути такими ж і без цього документа [217].

Також законодавчо передбачено випадки розголошення інформації медичного характеру без згоди пацієнта чи його законних представників:

– у цілях забезпечення національної безпеки, територіальної цілісності чи громадського порядку (запобігання злочинам), з метою охорони здоров'я, прав осіб, запобігання розголошенню інформації конфіденційного характеру, підтримання неупередженості правосуддя (ч. 2 ст. 34 КУ) [78];

– при наданні допомоги неповнолітньому (до 14 років) чи особі, визнаній законодавчо недієздатною, з метою надання інформації її батькам (усиновлювачам) чи законним представникам (ч. 2 ст. 285 ЦК України; ч. 2 ст. 39, ч. 1 ст. 43 Основ законодавства України про охорону здоров'я) [249; 121];

– при проведенні дізнання, досудового слідства або судового розгляду, зважаючи на письмовий запит особи, що проводить дізнання (слідчий, прокурор, суд) (ч. 4 ст. 6 Закону України «Про психіатричну допомогу»; ч. 5 ст. 14 Закону України «Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними») [182;169];

– у разі подій і ситуацій надзвичайного характеру (загроза здоров'ю, погіршення санітарного і епідемічного стану) з метою інформування відповідних

державних органів(ч. 2 ст. 26 Закону України «Про захист населення від інфекційних хвороб [167];

– відповідно до Сімейного кодексу України, наречені повинні повідомляти один одного про стан свого здоров'я (п. 1 ст. 30). Приховування даної інформації одним з наречених, наслідком чого може стати порушення фізичного або психічного здоров'я іншого нареченого чи їх нащадків, може бути підставою для визнання шлюбу недійсним (п. 5) [205];

– при загрозі поширення інфекційних захворювань, а також ухилянні від медичного обстеження, щеплення проти інфекцій; усуненні, за відповідним поданням державної санітарно-епідеміологічної служби від роботи, навчання, а також відвідування дошкільних закладів осіб, які є носіями інфекційних захворювань, хворих та осіб, які були в контакті з такими хворими. Також тих, хто ухиляється від обов’язкових обстежень та щеплень проти інфекцій згідно переліку, визначеного МОЗ (ч. 2 ст. 26 Закону України «Про захист населення від інфекційних хвороб) [167];

– у разі встановлення ВІЛ-інфекції у неповнолітніх (до 18 років) та осіб, яких визнано недієздатними, з метою повідомлення про даний факт батьків чиїх представників (ч. 2 ст. 8 Закону України «Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ») [181];

– у разі звільнення хворого на туберкульоз з місць позбавлення волі (арештного дому) установа виконання покарань, в якій такий хворий відбував покарання, інформує його про стан здоров’я та необхідність продовження лікування за обраним місцем проживання чи перебування, а також повідомляє про клінічну та диспансерну категорію його захворювання відповідний протитуберкульозний заклад (ч. 2 ст. 18 Закону України «Про протидію захворюванню на туберкульоз»)» [180].

Крім того, на бланку лікарняного листка, як правило, вказано заклад, де перебував пацієнт. Цей факт також суперечить законодавству, а саме, праву пацієнта на нерозголошення медичної інформації. Адже вона порушується, якщо відомо, що людина лікувалась у протитуберкульозному закладі або ж у психіатричній лікарні. Цю норму у МОЗ обіцяють змінити, але строки, коли це відбудеться, не вказують. Натомість нещодавно Міністерство охорони здоров'я ініціювало зміни в частині кодексу про права на медичну інформацію 16 річних підлітків. Зокрема, ініційовано положення про те, що у разі, якщо підліткові виповнилося 16 років, батьки матимуть доступ до медичної інформації винятково за згодою підлітків [256].

Також варто наголосити, що деталізовані відомості щодо стану здоров'я пацієнта (діагноз і методи лікування), відповідно до ст. 286 ЦК України, не мають права вимагати за місцем роботи чи навчання.

Зазначене вище свідчить про те, що медична інформація може бути розголошена виключно у випадках, якщо її збереження зашкодить суспільству та якщо нерозголошення матиме наслідки для оточення хворого. Крім того, лікарі повинні обов'язково інформувати суспільство про народження та смерть людини, випадки жорстокого поводження з дітьми, та у разі небезпечної інфекційної хвороби. Найчастіше саме поширення інфекцій і є тим чинником, який запускає процес розголошення медичної інформації. Тобто всі законодавчі акти про збереження медичної інформації втрачають силу, якщо мова йде про інфекційну хворобу і небезпеку здоров'ю та життю інших людей.

Зокрема, відповідно до Закону України «Про захист населення від інфекційних хвороб», уся інформація про випадки зараження під час епідемії, пандемії та карантину є соціально важливою. Відповідно, повинна розголошуватись [167]. Дана норма передбачена і стандартами Всесвітньої організації охорони здоров'я, відповідно до яких держава зобов'язана інформувати суспільство про зараження пацієнтів і лікарів [22]. У Рекомендаціях № R (2000) 5

Комітету міністрів Ради Європи також зазначено, що держави повинні вдосконалити й посилити систему поширення інформації, а інформаційні стратегії повинні бути адаптовані, зважаючи на особливості тих груп населення, на які вони спрямовані [190].

Вітчизняне ж законодавство у даному напрямі потребує систематизації, а також розроблення чіткого алгоритму дій медичних працівників щодо збереження медичної інформації, переліку документів про умови, за яких можливе розголошення інформації, дозволів суб'єктів первинної медичної інформації, зобов'язань медичних працівників про нерозголошення медичної інформації.

Досить слушною є думка І.Я. Сенюти, яка зазначила, що однією з найважливіших проблем є законодавча. Вона підкреслила, що якісний нормативний фундамент є запорукою належної правореалізації та правозастосування, проте нинішня нормативна техніка, яку застосовують органи влади, часто не відповідає належному рівню. Особливо гостро ці проблеми проявилися під час пандемії коронавірусу, коли стало очевидно, що існують не лише труднощі в досягненні балансу між приватним і публічним інтересом, але й серйозні виклики у сфері захисту персональних даних, зокрема у контексті епідеміологічного нагляду та інфекційного контролю [201].

Підсумовуючи, ми дійшли наступних висновків у даному підрозділі.

Одним із ключових чинників забезпечення правового статусу пацієнта в медичному праві є законодавче врегулювання обігу медичної інформації. Дотримання конфіденційності даних про здоров'я є основним принципом, якого повинні дотримуватися держави-учасниці Конвенції. Держава виступає гарантом захисту прав людини, у тому числі і на інформацію. Правове регулювання питання конфіденційності медичної інформації в Україні покращилося з прийняттям Закону України «Про захист персональних даних». За результатами проведеного дослідження встановлено, що право на здоров'я має комплексний характер і

включає: право на доступ до інформації та її конфіденційність; право на медико-соціальну допомогу; право на згоду на лікування та медичне втручання та інше.

Розмежовано поняття «лікарська таємниця» та «медична інформація», сформульовано їх авторське визначення. Теоретично обгрунтовано, що поняття «медична інформація» набагато ширше аніж «лікарська таємниця», так як «лікарська таємниця» – це інформація конфіденційного змісту про звернення особи за медичною допомогою, стан здоров'я, лікування (обстеження, діагноз, реабілітація), а «медична інформація» – конфіденційна інформація про фізичну особу, яка стала відома у процесі звернення за медичною допомогою (факт звернення за медичною допомогою, стан здоров'я, огляд, діагноз, результати обстеження, методи лікування, інтимну і сімейну сторони життя), а також інформація, яку працівники медичних закладів (лікарі, медичний чи обслуговуючий персонал) одержують від пацієнта у процесі спілкування з ним, розголошення якої може зашкодити. Відповідно, запропоновано на законодавчому рівні звести термінологічний апарат у даній сфері до терміна «медична інформація».

Констатовано, що в окремих випадках чинним законодавством встановлено певні обмеження щодо можливості одержання пацієнтом повної інформації щодо стану свого здоров'я. Розголошення медичної інформація можливе лише у разі, якщо її збереження зашкодить суспільству та якщо нерозголошення матиме наслідки для оточення хворого. Розглянуто основні випадки розголошення медичної інформації без згоди пацієнта чи його законних представників.

Теоретично обгрунтовано, що вітчизняне законодавство у даному напрямі потребує систематизації, а також розроблення чіткого алгоритму дій медичних працівників щодо збереження медичної інформації, переліку документів про умови, за яких можливе розголошення інформації, дозволів суб'єктів первинної медичної інформації, зобов'язань медичних працівників про нерозголошення медичної інформації. Лише у взаємозв'язку прав та обов'язків, що формують правову систему України, можна підвищити ефективність їх забезпечення. Це не лише

зменшить прогалини в нормативному регулюванні, але й сприятиме приведенню національного законодавства у відповідність із загальновизнаними міжнародними правовими стандартами.

1.3. Об’єкти та суб’єкти забезпечення інформаційної безпеки у сфері охорони здоров’я

Система інформаційної безпеки України (СЗІБ) формується та функціонує на основі Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в інформаційній сфері. Її основу становлять державні органи та підрозділи інформаційної безпеки, які реалізують комплекс адміністративно-правових, організаційно-управлінських, інформаційно-аналітичних та інших заходів, спрямованих на забезпечення стабільного функціонування системи державного управління.

В умовах правового режиму воєнного стану особливої актуальності набуває вдосконалення взаємодії між суб’єктами інформаційного простору, що безпосередньо впливають на об’єкти інформаційної безпеки на підставі визначених заходів [147]. Від ефективності дій цих суб’єктів залежить стан і перспективи реалізації державної політики у сфері інформаційної безпеки. За визначенням Д.І. Федченка, інформаційна безпека – це діяльність спеціально уповноважених суб’єктів, спрямована на запобігання виникненню та нейтралізацію інформаційних загроз [245, с. 654].

Інформаційна ж безпека – здатність: системи протистояти випадковим або навмисним внутрішнім і зовнішнім загрозам; забезпечити захист суб’єктів від негативного інформаційного впливу. Таким чином, система інформаційної безпеки тісно пов'язана з діяльністю держави, оскільки в більшості випадків йдеться про певні несанкціоновані дії з інформацією. Головним інститутом інформаційної безпеки є держава, яка через низку політичних інституцій реалізує заходи щодо забезпечення безпеки в цій сфері [53].

На жаль, на сьогоднішній день не прийнятий закон, який визначав би концепцію державної інформаційної політики України (далі – Концепція). Це свідчить про відсутність єдиного плану або стратегії розвитку інформаційної індустрії. Роблячи екскурс в історію, зазначимо, що упродовж 2002–2010 років в Україні було три спроби прийняти Концепцію: в 2002, 2009 і 2010 роках, 11 січня 2011 року наступний проєкт Концепції [80] був прийнятий в першому читанні і відправлений до Комітету Верховної Ради з перевірки. Нова хвиля актуалізації проблеми була викликана соціально-політичною ситуацією в країні, агресією Росії, окупацією Криму і бойовими діями на Сході. Одна з причин цих подій – вплив засобів масової інформації (далі – ЗМІ) Росії, з якою Україна не змогла протистояти через певні проблеми у інформаційному просторі [257].

У 2015 році було створено Міністерство інформаційної політики, основним завданням якого була розробка стратегічного документа, який визначив би інформаційну політику України, урегулював внутрішні і зовнішні інформаційні потоки в країні і регламентував способи протидії іноземному інформаційному впливу. В результаті 9 червня 2015 року було оприлюднено Концепцію інформаційної безпеки України. Документ викликав багато питань і критики. Офіс Представника ОБСЄ з питань свободи слова представив свої рекомендації в липні 2015 року [150]. Обговорення серед українських експертів наразі все ще тривають. Проте систематичного аналізу положень документа немає, схвалення на законодавчому рівні даний проєкт не отримав.

Що стосується структури системи ІБ України, включаючи структуру системи суб’єктів та об’єктів, що її впроваджують, то вона є похідною від пріоритетів та завдань, поставлених державою в інформаційній сфері [203]. Ключовим завданням державної інформаційної політики є упровадження та подальша ефективна реалізації ІБ.

Функціонування системи забезпечення інформаційної безпеки досягається через реалізацію ряду завдань, зокрема:

- подальше вдосконалення розвитку вітчизняної інформаційної сфери шляхом створення нормативно-правових та економічних передумов, таких як розвиток інформаційних ресурсів і впровадження передових технологій;
- забезпечення інформаційної безпеки всіх складових елементів системи державного управління;
- забезпечення високого інформаційно-аналітичного потенціалу країни;
- функціонування політики інформаційної безпеки;
- моніторинг стану інформаційної безпеки у зв'язку з впливом загроз та небезпек як зсередини, так і ззовні системи державного управління;
- запобігання можливій протиправній та іншій негативній діяльності суб'єктів інформаційної безпеки всередині системи, що може завдати їй шкоди;
- забезпечення ефективного контролю за станом інформаційної безпеки держави [203].

Ефективність захисту ІБ досягається завдяки злагодженій діяльності кожної складової її державно-правового механізму. Цей механізм включає систему взаємопов'язаних та узгоджених державно-правових інституцій, основним завданням яких є створення умов для ефективної реалізації інформаційної політики.

Центральним органом державної влади у сфері інформаційної безпеки є Національна комісія з державного регулювання інформаційної безпеки (Комісія), яка підпорядковується Кабінету Міністрів України та перебуває під контролем Президента України. Основними завданнями Комісії є участь у формуванні та

реалізації державної політики у сфері інформаційної безпеки, моніторинг її стану та забезпечення державного регулювання, а також координація діяльності органів влади з відповідних питань.

Окремі аспекти інформаційної безпеки регламентуються Законом України «Про основні засади забезпечення кібербезпеки України» від 08.07.2017 р. № 2163-VIII [177]. Згідно з рішенням Ради національної безпеки і оборони України від 15.10.2021 р. «Про Стратегію інформаційної безпеки», ключовими суб’єктами національної системи інформаційної безпеки є Кабінет Міністрів України, Міністерство інформаційної політики України, Міністерство закордонних справ, Міністерство оборони, Міністерство культури, Державне агентство з питань кіно, Національна рада з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, а також розвідувальні органи. Ці органи відповідають за розробку та реалізацію заходів у сфері інформаційної безпеки та визначають обсяги фінансування відповідно до напряму діяльності [224].

Стаття 3 Закону України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII визначає, що державна політика у сферах національної безпеки та оборони спрямована на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної безпеки та кібербезпеки країни. Відповідно до статті 27 цього закону, комплексний огляд сектору безпеки і оборони проводиться за рішенням Ради національної безпеки і оборони України, що вводиться в дію указом Президента, і включає, зокрема, оцінку стану кіберзахисту інформаційних ресурсів та ресурсів критичної інфраструктури [175].

Водночас, якщо законодавчо визначено коло суб’єктів, які забезпечують національну безпеку України, то нормативне закріплення кола суб’єктів інформаційної безпеки країни відсутнє, що створює прогалини у регулюванні їх повноважень та відповідальності. Це підкреслює необхідність подальшого уточнення правового статусу учасників системи інформаційної безпеки України.

Відповідно до філософського енциклопедичного словника, термін «суб’єкт» визначається як особа, організована група осіб, соціальна, етнічна та політична спільнота, суспільство загалом, що здійснюють властиву їм діяльність, спрямовану на практичне перетворення предметної дійсності, теоретичне й духовно-практичне освоєння об’єктивної реальності; носій означених якостей, що уможливлюють виконання ним суспільно значущих функцій [246, с. 613]. Академічний тлумачний словник визначає поняття «суб’єкт» як особу, групу осіб, організацію і т.ін., яким належить активна роль у певному процесі, акті [209]. Подібне визначення зустрічаємо і в словнику іншомовних слів: суб’єкт: 1) істота, здатна до пізнання навколишнього світу, об’єктивної дійсності й до цілеспрямованої діяльності; 2) особа, група осіб, організація і т.ін., яким належить активна роль у певному процесі, акті [208].

Поняття «суб’єкт інформаційної безпеки» має як широке, так і вузьке значення. У широкому сенсі –це державні інституції, які залучені до формування та впровадження політики інформаційної безпеки. У вузькому сенсі, крім інститутів публічної влади, до суб’єктів інформаційної безпеки належать також інститути громадянського суспільства. Цей перелік не обмежується лише державними органами, оскільки опрацювання питань, пов’язаних із політикою інформаційної безпеки, може бути доручено певним науковим установам і групам експертів[86, с. 172]. Тобто, суб’єкти забезпечення ІБ– це не лише державні органи влади, а й недержавні органи, що відповідає правовим нормам, які регламентують діяльність у даному напрямі.

На думку Т.М. Мужанової, до суб'єктів забезпечення ІБ варто віднести: державу, громадські організації та об'єднання, громадяни [110].

При чому, головна роль належить державі, яка забезпечує ІБ особи (права і свободи в інформаційному просторі, формування мислення, захист інформації конфіденційного характеру), суспільства (багатоканальність отримання інформації, незалежна діяльність ЗМІ) і держави (інформаційне забезпечення як діяльності

органів державної влади, так і політики держави, розвиток системи захисту інформації, протидія правопорушенням та злочинам у даному напрямі).

Подібної точки зору притримуються і О.К. Юдін та В.М. Богуш, які до суб'єктів інформаційної безпеки відносять:

- державу, яка виконує свої функції через відповідні органи;
- громадян, суспільні та інші організації і об'єднання, які мають повноваження в цій сфері [255].

Згідно зі статтею 9 Розділу ІІІ проєкту Концепції інформаційної безпеки України від 9 червня 2015 року, до суб’єктів, відповідальних за забезпечення інформаційної безпеки, належать як окремі громадяни та об’єднання громадян, так і громадські організації та інші інститути громадянського суспільства; вищі органи державної влади, включаючи Президента, Верховну Раду, Кабінет Міністрів та центральні органи виконавчої влади, а також структури сектору безпеки і оборони; засоби масової інформації, підприємства та установи різних форм власності, що ведуть інформаційну діяльність; крім того, до суб’єктів віднесено наукові, освітні та навчальні заклади, які проводять дослідження та готують фахівців у сфері інформаційної діяльності й інформаційної безпеки [186].

О.Д. Довгань пропонує модель комплексної системи ІБ, яка утворюється як її об’єктами, так і суб’єктами відповідно.

До об’єктів інформаційної безпеки належать: права і свободи людини, фізичне та психологічне здоров’я населення, захист від деструктивного та маніпулятивного впливу інформації; забезпечення інформаційних прав та гарантії розвитку населення всіх регіонів України; збереження інформаційного суверенітету, безпека національної частини глобального інформаційного простору та інформаційної інфраструктури, а також захищеність, цілісність, доступність і безпечність інформаційних ресурсів, продукції та послуг.

До суб’єктів, які забезпечують інформаційну безпеку в Україні, належать: Президент, Верховна Рада та Кабінет Міністрів України; РНБО та Національний

банк України; Міністерство інформаційної політики, Державний комітет телебачення і радіомовлення та Національна рада з питань телебачення і радіомовлення; Державна служба спеціального зв'язку та захисту інформації, Національна комісія з питань регулювання зв'язку та інформатизації; Служба безпеки України, розвідувальні органи, Державна прикордонна служба, Збройні Сили та інші військові формування відповідно до законів України; центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, суди, прокуратура та інші правоохоронні органи; засоби масової інформації, підприємства, установи й організації різних форм власності, які здійснюють інформаційну діяльність; наукові установи та вищі навчальні заклади інформаційного профілю; інститути громадянського суспільства, а також громадяни України та інші особи за їхньою згодою [37, с. 13].

О. Стоєцький пропонує класифікувати суб'єктів інформаційної безпеки на державні інституції (Президент України, державні органи та організації) і недержавні інституції (органи місцевого самоврядування, об'єднання громадян), а також включає громадян України, визначаючи поняття «суб'єкти інформаційної безпеки» як сукупність державних і недержавних інституцій та громадян, об'єднаних спільною метою – захистом національних інтересів у інформаційній сфері [223, с. 164].

Подібну позицію підтримує В.О. Негодченко, який також розділяє суб'єктів ІБ на державні та недержавні. До державних він відносить: загальні суб'єкти, до яких входять центральні органи влади та створені при них координаційні та консультативні органи (Верховна Рада України, Кабінет Міністрів, РНБО), а також спеціальні суб'єкти – центральні органи виконавчої влади та їх територіальні підрозділи, зокрема Міністерство інформаційної політики України, Державна служба спеціального зв'язку та захисту інформації, Державне агентство з питань науки, інновацій та інформатизації, Державна служба з питань захисту

персональних даних, Міністерство оборони, Служба безпеки України, Міністерство внутрішніх справ та інші.

Відповідно до чинного законодавства, яке регулює діяльність у сфері інформаційної безпеки, забезпечення інформаційного суверенітету України – тобто поширення важливої суспільної інформації як всередині країни, так і за її межами – а також підтримка функціонування та захист державних інформаційних ресурсів, охорона інформації, що підлягає правовій охороні, у інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності покладені на Міністерство інформаційної політики України, Державну службу спеціального зв'язку та захисту інформації, Державне агентство з питань науки, інновацій та інформатизації України та Державну службу з питань захисту персональних даних [129; 159].

До недержавних суб'єктів належать органи місцевого самоврядування та інституції громадянського суспільства – різноманітні об'єднання громадян, окремі громадяни та засоби масової інформації [115]. Враховуючи, що недержавні суб'єкти контролюють значну частину інформаційної інфраструктури, вони відіграють вагому роль у формуванні державної інформаційної політики.

У контексті сфери охорони здоров'я під суб'єктами інформаційної безпеки слід розуміти як державні органи на регіональному та місцевому рівнях, так і недержавні інституції – громадян та організації, уповноважені забезпечувати інформаційну безпеку. До державних органів регіонального рівня відносяться Міністерство охорони здоров'я та Національна служба здоров'я України, на місцевому рівні – керівники медичних закладів та уповноважені департаментів, управлінь і служб за даним напрямом діяльності. До недержавних суб'єктів відносяться спеціалізовані організації, зокрема державне підприємство «Електронне здоров'я», ТОВ «ТЗІ» та інші.

Слід зауважити, що відповідно до постанови Кабінету Міністрів України від 25.04.2018 р. № 411 «Деякі питання електронної охорони здоров'я», право власності

на центральну базу даних належить державі, що реалізується через Національну службу здоров'я України. Управління та адміністрування реєстрів, зокрема реєстрів медичних спеціалістів, суб'єктів господарювання у сфері охорони здоров'я та медичних висновків, здійснюють Міністерство охорони здоров'я і Національна служба здоров'я України [35].

Нам імпонує наукова точка зору О.Д. Довганя, який класифікує суб'єктів ІБ, у тому числі і медичній сфері на суб'єктів, до повноважень яких віднесено: моніторинг та аналіз загроз; програмування та планування; виконавчі функції [37, с. 15].

Зважаючи на тісний взаємозв'язок між суб'єктами як формування, так і реалізації інформаційної безпеки у сфері охорони здоров'я, необхідно реалізовувати державну політику у інформаційному просторі виключно на підставі комплексного підходу, основним акцентом якого повинно бути усвідомлення суб'єктом інформаційної безпеки рівня відповідальності за дії в інформаційному просторі [136].

Слушною у даному контексті є наукова позиція І.Р. Березовської та Д.М. Русак [12]: необхідно сформувати у громадян інформаційну культуру та усвідомлення відповідальності при доступі та використанні інформаційних ресурсів. Адже подальший розвиток системи інформаційної безпеки має ґрунтуватися не лише на правових нормах, але й на неухильному виконанні взятих на себе зобов'язань [245, с. 654; 147].

Здатність суб'єкта ефективно реалізовувати надані йому права та виконувати встановлені обов'язки є визначальною умовою його участі в адміністративно-правових відносинах.

Інформація, яка виникає в процесі організації та безпосереднього надання медичної допомоги, виступає основою правовідносин у сфері медичного обслуговування. У вузькому розумінні вона відповідає безпосередньо медичній допомозі, має приватноправову природу та регулюється специфікою правового

інформаційного обігу між учасниками системи охорони здоров’я. Класичним прикладом такого обігу є процес отримання інформованої згоди на надання медичної допомоги.

Пацієнт у правовідносинах з медичним закладом отримує від лікаря інформацію щодо необхідності дотримання призначеного режиму лікування, прийому медикаментів та рекомендацій щодо способу життя, оскільки самовільні дії можуть ускладнити терапевтичний процес та негативно вплинути на стан здоров’я. Вказана інформація відображається у формі № 003-6/о «Інформована добровільна згода пацієнта на проведення діагностики, лікування, операції та знеболення» [229, с. 134].

Надання медичної допомоги – це комплексна система, в якій відображені передбачені законом права громадян. Це стосується як прав пацієнтів на одержання кваліфікованої медичної допомоги, так і прав лікарів, які надають таку допомогу.

Медичні правовідносини виникають внаслідок дії норм медичного права на поведінку учасників, що призводить до формування правовідносин між ними. Реалізація права на медичну допомогу є складовою частиною цих правовідносин. Для того, щоб бути учасником медичних правовідносин, необхідно володіти правосуб’єктністю, яка включає правоздатність і дієздатність. Правосуб’єктність учасників медичних правовідносин – це здатність і можливість, передбачені нормами права, мати та реалізовувати права, а також виконувати юридичні обов’язки.

Залежно від співвідношення взаємних прав і обов'язків учасників, медичні правовідносини поділяються на два типи: вертикальні та горизонтальні. Вертикальні правовідносини виникають тоді, коли одна зі сторін має державно-владні повноваження стосовно іншої сторони (наприклад, відносини в сфері державного регулювання медичної діяльності). Горизонтальні правовідносини характеризуються рівністю сторін (наприклад, відносини між медичним закладом і громадянином).

На думку С.Г. Стеценко, суб'єктами права є учасники правовідносин, тобто носії суб'єктивних прав і обов'язків [220]. Зважаючи на багатогранність медичної діяльності та різноманітність суспільних відносин, що виникають у цій сфері, можна виділити такі групи учасників медичних правовідносин: ті, хто надає медичну допомогу; ті, хто отримує медичну допомогу; та ті, хто сприяє наданню медичної допомоги (підрозділи забезпечення) [220].

З огляду на це, кожна із зазначених груп учасників медичних правовідносин поділяється на окремі підгрупи. Зокрема, ті, хто надає медичну допомогу, можуть бути державними, комунальними та приватними закладами. Отримувачі медичної допомоги, залежно від політико-правового зв'язку з державою, можуть бути громадянами України, іноземними громадянами або особами без громадянства. Нарешті, ті, хто сприяє наданню медичної допомоги, представлені підрозділами забезпечення, такими як фінансово-економічні, кадрові, соціальні та юридичні служби закладів охорони здоров'я.

Отже, система інформаційної безпеки формується через комплекс суб’єктів, що реалізують державну політику в інформаційному середовищі у різних галузях, зокрема в охороні здоров’я. Ці суб’єкти класифікуються на дві категорії: ті, для яких забезпечення інформаційної безпеки є безпосереднім обов’язком, та ті, що виконують цю функцію опосередковано [255].

Перейдемо до аналізу об’єктів ІБ. Об’єкт (лат. Objectum – предмет): 1) пізнавана дійсність, що існує поза свідомістю людини і незалежно від неї; 2) явище, предмет, особа, на які спрямована певна діяльність, увага і т.ін. [208]. У словнику української мови термін «об’єкт» визначено як «явище, предмет, особа, на які спрямована певна діяльність, увага і т. ін.» [209].

У кожній країні основними об’єктами ІБ є громадяни та держава як єдине ціле. Основним каналом інформаційного впливу на них є свідомість (переконання, утвердження тощо). Коли йдеться про захист інформаційного простору, мається на увазі державний інформаційний суверенітет, що означає належне володіння та

розповсюдження відповідних інформаційних ресурсів усією спільнотою в державі. Інформаційний суверенітет передбачає виняткове право держави на формування та використання всіх інформаційних засобів, створених на основі державної політики і за державний кошт [68, с. 60].

У якості об'єктів інформаційної безпеки виступають: особа та її права; громадськість; держава.

За оцінкою О.К. Юдіна та В.М. Богуша, об'єктами інформаційної безпеки можуть виступати свідомість і психіка людей, а також інформаційні системи. До соціальних об'єктів ІБ вони відносять особистість, колективи, суспільство, державу та світове співтовариство [255]. В.В. Зайцев підкреслює, що сьогодні організацію забезпечення інформаційної безпеки покладено на державні органи різного рівня підпорядкування та різних функціональних напрямів [50].

Згідно із Законом України «Про Концепцію Національної програми інформатизації» від 04.02.1998 р., об'єктами ІБ є інформаційні ресурси, канали обміну інформацією, телекомунікаційні системи та мережі, а також механізми забезпечення їх функціонування та інші складові інформаційної інфраструктури країни [173]. Технічними об'єктами ІБ виступають інформаційні ресурси, інфраструктура, технології та системи.

У контексті медичної сфери об'єктом правовідносин слід вважати матеріальні та духовні блага, на досягнення яких спрямовані права та обов'язки учасників. Складність медичних правовідносин обумовлює формування комплексного об'єкта, що включає особисті немайнові блага людини, такі як життя і здоров'я, а також сам процес надання медичної допомоги та його результати. Важливо враховувати різні цільові установки учасників: для медичних працівників пріоритетом є належне виконання лікувальних заходів, тоді як для пацієнтів ключовим є досягнення кінцевого результату – одужання [221].

Відносини, що виникають у процесі обігу інформації в медичній сфері, підлягають правовому регулюванню та захисту. Одним із ключових напрямів

впливу інформаційної сфери є забезпечення безпеки особистості від широкого спектра негативних факторів, які можуть впливати на життя та здоров'я людини. Основними об’єктами інформаційної безпеки у сфері охорони здоров’я є індивідуальні права в інформаційному просторі, зокрема право на доступ до інформації та її захист.

Як зазначає Х.Я. Терешко, в інформаційних правовідносинах об’єктами права виступають також інформація, дані, бази даних, різноманітні інформаційні ресурси, програми, комп’ютери, інформаційні системи, засоби інформатизації та зв’язку тощо [229].

На думку Т. Перуна, найважливішими інтересами особистості в інформаційній сфері є: повна реалізація права на доступ до інформації, можливість вільного та безпечного використання інформації в рамках законної діяльності, захист персональних даних, а також захист особистої та сімейної таємниці [127].

Таким чином, до основних об’єктів інформаційної безпеки у сфері охорони здоров’я слід віднести: індивідуальні права та свободи людини в інформаційному просторі; інформаційні ресурси, до яких належать медичні інформаційні системи, електронні реєстри та медична інформація (чутливі персональні дані, відомості про психічний стан, результати медичних обстежень, рецепти, направлення, геномні дані); а також канали обміну інформацією та телекомунікаційні мережі.

Підсумовуючи, можна зазначити, що суб’єкти ІБ становлять ключовий елемент системи забезпечення національної безпеки в інформаційному просторі України, від координації їх дій напряму залежить ефективність реалізації державної політики у цій сфері. У контексті охорони здоров’я до суб’єктів ІБ належать як державні органи на регіональному та місцевому рівнях, так і недержавні інституції – громадяни та організації, яким делеговані повноваження щодо забезпечення інформаційної безпеки. До державних суб’єктів відносяться Міністерство охорони здоров’я та Національна служба здоров’я України на регіональному рівні, а на місцевому – керівники медичних закладів та уповноважені працівники

департаментів, управлінь, відділів і служб медичних закладів. До недержавних суб’єктів відносять спеціалізовані організації, такі як державне підприємство «Електронне здоров’я», ТОВ «ТЗІ» та інші подібні установи.

Основними об’єктами ІБ у сфері охорони здоров’я є індивідуальні права у інформаційному просторі, інформаційні ресурси (медичні інформаційні системи, реєстри), канали інформаційного обміну і телекомунікації.

Зважаючи на тісний взаємозв'язок між суб'єктами як формування, так і реалізації інформаційної безпеки у сфері охорони здоров’я, необхідно реалізовувати інформаційну політику виключно на підставі системного підходу, основним акцентом якого повинно бути усвідомлення суб’єктом інформаційної безпеки рівня відповідальності за дії в інформаційному просторі, а також дотримання відповідного рівня інформаційної культури.

Висновки до розділу 1

1. В умовах розвитку інформаційного суспільства, інформаційна безпека стає однією з основних цінностей держави, забезпечення якої є запорукою її стабільного функціонування та поступального розвитку. Проблематика інформаційної безпеки у сфері охорони здоров'я, яка має місце на сьогодні, виникла через протиріччя між можливостями інформаційних технологій та загрозами їх використання, а також відсутністю належного рівня інформаційної культури як серед працівників медичної сфери, так і суспільства загалом. Зміст поняття «інформаційна безпека» поділяють на дві групи: до першої відноситься захист інформації, інформаційних ресурсів, держави, суспільства та особистості від негативного інформаційного впливу; до другої – загрози інформаційної безпеки.

2. Сформульовано авторське визначення поняття «інформаційна безпека у сфері охорони здоров'я», яке запропоновано розглядати як комплексну систему захисту інформаційного середовища, яка забезпечує запобігання, виявлення і нейтралізацію інформаційних загроз, а також цілісність, конфіденційність та доступність інформації, тим самим забезпечуючи формування та розвиток інформаційного середовища у медичній сфері в інтересах держави, суспільства та особистості.

3. Теоретично обгрунтовано, що у передбачених Стратегією розвитку інформаційного суспільства напрямах подальшого розвитку «Е-медицини» не звернено увагу на належний технічний захист як автоматизованих інформаційних галузевих систем, так і взагалі медичної інформації. Відповідно, пропонуємо доповнити п. 1 сфери діяльності «Е-медицина», розділу «Етапи та основні напрями

реалізації» Стратегії розвитку інформаційного суспільства та викласти його у наступній редакції: упровадження автоматизованих інформаційних систем, які сертифіковано на відповідність КСЗІ, що надають змогу перейти до ведення медичної документації в електронному вигляді.

4. Надано пропозиції щодо класифікації ключових механізмів комплексної системи інформаційної безпеки у сфері охорони здоров'я: правовий (юридичні норми та гарантії системи захисту інформації в АІС, які використовують медичні заклади; запобігання витокам; проведення службових розслідувань за фактами порушення інформаційної безпеки; відповідальність); технічний (забезпечення конфіденційності, цілісності та доступності інформації); комунікаційний та освітній (забезпечення доступності АІС; передбачення: обов'язкових спецкурсів, у тому числі дистанційних, з питань інформаційної безпеки при використанні АІС; щорічного підвищення кваліфікації працівників, які працюють з системами, з обов'язковим вивченням як щойно прийнятих нормативно-правових актів у даному напрямі, так і ознайомленням з позитивним міжнародним досвідом).

5. З метою покращення ефективності діяльності у даному напрямі необхідно систематизувати чинне законодавство та привести його у відповідність до міжнародних стандартів. Зокрема, запропоновано імплементувати позитивний міжнародний досвід Сполучених штатів Америки (Закон США «Про мобільність та підзвітність медичного страхування» (HIPAA)), відповідно, розробити окремий нормативно-правовий акт, який на законодавчому рівні врегулював би збір, обробку, розкриття та передачу медичної інформації.

6. Одним з найважливіших чинників забезпечення правового статусу пацієнта у медичному праві є законодавче врегулювання обігу медичної інформації, адже саме дотримання конфіденційності інформації про здоров'я – основний принцип держав-учасниць Конвенції. Держава виступає гарантом захисту прав людини, у тому числі і на інформацію. За результатами проведеного дослідження встановлено, що право на здоров'я має комплексний характер і включає: право на

доступ до інформації та її конфіденційність; право на медико-соціальну допомогу; право на згоду на лікування та медичне втручання та інше.

7. За результатами аналізу норм чинного та міжнародного законодавства, наукових позицій правознавців розмежовано поняття «лікарська таємниця» та «медична інформація», сформульовано їх авторське визначення. Теоретично обгрунтовано, що поняття «медична інформація» набагато ширше аніж «лікарська таємниця», відповідно, запропоновано на законодавчому рівні звести термінологічний апарат у даній сфері до терміна «медична інформація».

8. Констатовано, що в окремих випадках чинним законодавством встановлено певні обмеження щодо можливості одержання пацієнтом повної інформації про стан свого здоров'я. Розголошення медичної інформація можливе лише у разі, якщо її збереження зашкодить суспільству та якщо нерозголошення матиме наслідки для оточення хворого. Розглянуто основні випадки розголошення медичної інформації без згоди пацієнта чи його законних представників.

9. Теоретично обгрунтовано, що вітчизняне законодавство у даному напрямі потребує систематизації, а також розроблення чіткого алгоритму дій медичних працівників щодо збереження медичної інформації, переліку документів про умови, за яких можливе розголошення інформації, дозволів суб'єктів первинної медичної інформації, зобов'язань медичних працівників про нерозголошення медичної інформації.

Ефективність захисту інформаційної безпеки держави визначається результативністю діяльності всіх елементів її державного механізму, який формується системою взаємопов'язаних і координованих державно-правових інституцій. Головним завданням цих інституцій є створення умов для реалізації державної інформаційної політики на високому рівні. Система забезпечення інформаційної безпеки України охоплює комплекс суб'єктів, відповідальних за втілення державних стратегій у інформаційній сфері, і від їхньої взаємодії залежить стан, динаміка та ефективність реалізації цієї політики. Особливий статус у цій

сфері належить центральному органу виконавчої влади – Національній комісії з державного регулювання інформаційної безпеки.

Суб'єкти інформаційної безпеки становлять критично важливий елемент у системі забезпечення національної безпеки в інформаційному просторі України, оскільки ефективність реалізації державної політики значною мірою залежить від узгодженості їхніх дій. У сфері охорони здоров'я під суб'єктами ІБ слід розуміти як державні органи на регіональному та місцевому рівнях, так і недержавні інституції – фізичних осіб та організації, які наділені повноваженнями щодо захисту інформаційної безпеки. До державних органів на регіональному рівні належать Міністерство охорони здоров'я та Національна служба здоров'я України, на місцевому – керівники медичних закладів та уповноважені фахівці департаментів, управлінь, відділів і служб відповідних закладів. До недержавних суб'єктів відносяться спеціалізовані організації, зокрема державне підприємство «Електронне здоров'я», ТОВ «ТЗІ» та подібні установи.

З огляду на тісну взаємодію між усіма суб'єктами у процесі формування та реалізації інформаційної безпеки у медичній сфері, впровадження державної інформаційної політики має здійснюватися на основі системного підходу. Його ключовим елементом є усвідомлення суб'єктами ІБ своєї відповідальності за дії в інформаційному просторі, а також підтримання належного рівня інформаційної культури та професійної підготовки.

Основними об'єктами ІБ у сфері охорони здоров'я є індивідуальні права та свободи особи у інформаційному просторі, інформаційні ресурси (медичні інформаційні системи, реєстри, медична інформація (чутливі дані, відомості про стан психічного здоров'я, інформація про результати медичних обстежень, рецепти, направлення, геномна інформація)), канали інформаційного обміну і телекомунікації.

РОЗДІЛ 2
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

2.1. Правове регулювання захисту інформації у сфері охорони здоров'я

Нормативно-правове забезпечення захисту інформації в медичній сфері України базується на комплексі взаємопов'язаних законів та підзаконних актів. До основних положень належать: ст. 32 Конституції України, ст. 286 Цивільного кодексу України, ст. 40 Основ законодавства України про охорону здоров'я, ст. 30 Сімейного кодексу України; а також окремі закони України, серед яких – ст. 46 «Про інформацію», ст. 7 «Про захист персональних даних», ст. 6 «Про психіатричну допомогу», ст. 26 «Про захист населення від інфекційних захворювань», ст. 7 «Про забезпечення санітарного та епідеміологічного благополуччя населення». Додатково питання відповідальності за порушення захисту інформації врегульовані ст. 132 та 145 Кримінального кодексу України та положеннями Кримінального процесуального кодексу України. Виконання та деталізація правових норм забезпечується через Укази Президента України, постанови Кабінету Міністрів України, накази, інструкції та розпорядження Міністерства охорони здоров'я й інших органів державної влади.

Як зазначають С.Г. Стеценко, В.Ю. Стеценко та І.Я. Сенюта, національна правова база захисту медичної інформації спирається на принципи, запозичені з міжнародного законодавства у сфері охорони здоров'я. Так, п. 2 ст. 2 Декларації про політику у сфері забезпечення прав пацієнта в Європі (1994 р.) [33] надає

пацієнтові право отримувати інформацію про стан власного здоров’я, включно з відомостями про потенційні ризики, методи лікування, наслідки відмови від терапії, діагноз, план лікування та гарантії захисту інформації. Крім того, пункт «c» ч. 2 Лісабонської декларації про права пацієнта (1981 р.) [96] передбачає право пацієнта на вільне погодження або відмову від лікування після отримання відповідної інформації [221].

Правове регулювання захисту медичної інформації в Україні здійснюється через комплекс взаємопов’язаних нормативно-правових актів, що охоплюють як конституційні, так і спеціальні джерела права. Основні гарантії закріплені у ст. 32 Конституції України, яка забезпечує недоторканність приватного життя, а також у ст. 286 Цивільного кодексу України, що надає фізичній особі право на доступ до медичних даних про себе. Специфічні положення містяться в Основах законодавства України про охорону здоров’я (ст. 40), Сімейному кодексі України (ст. 30), а також у ряді спеціальних законів, зокрема: «Про інформацію» (ст. 46), «Про захист персональних даних» (ст. 7), «Про психіатричну допомогу» (ст. 6), «Про захист населення від інфекційних захворювань» (ст. 26), «Про забезпечення санітарного та епідеміологічного благополуччя населення» (ст. 7). Додатково, захист інформації забезпечується положеннями Кримінального кодексу України (ст. 132, 145), Кримінального процесуального кодексу України, а також підзаконними актами, такими як укази Президента, постанови Кабінету Міністрів, накази та інструкції Міністерства охорони здоров’я й інших органів виконавчої влади.

Національна система інформаційного захисту у сфері охорони здоров’я, як зазначають С.Г. Стеценко, В.Ю. Стеценко та І.Я. Сенюта, розвивається з урахуванням міжнародного досвіду та загальновизнаних принципів. Зокрема, відповідно до пункту 2 статті 2 Декларації про політику у сфері забезпечення прав пацієнтів у Європі (1994 р.), кожна особа має право на повну та зрозумілу інформацію щодо стану свого здоров’я, включаючи можливі ризики, варіанти

лікування, наслідки відмови від терапії, поставлений діагноз, план лікування та умови збереження конфіденційності персональних медичних даних. Аналогічна норма закріплена й у Лісабонській декларації про права пацієнтів (1981 р.) [96], згідно з якою пацієнт має право приймати усвідомлене рішення щодо лікування після отримання повної інформації (п. «с» ч. 2) [221].

Таким чином, нормативне забезпечення захисту медичної інформації в Україні інтегрує норми національного законодавства з положеннями міжнародно-правових актів, що формує правове підґрунтя для забезпечення прав пацієнтів та дотримання етичних стандартів у сфері медичної діяльності.

Аналіз чинного вітчизняного законодавства свідчить, що згідно зі ст. 32 Конституції України, без згоди особи, окрім випадків, які визначено законом, у інтересах національної безпеки та з дотриманням прав людини, можливо збирати, зберігати, використовувати та поширювати конфіденційну інформації [78; 139].

Дещо суворіші вимоги передбачено для обробки чутливих даних. Слід зазначити, що чутливі дані – персональні дані (далі – ПД) щодо стану здоров’я суб’єкта. Частиною 1 статті 7 Закону «Про захист персональних даних» заборонено обробляти ПД щодо расового, етнічного походження, … даних щодо стану здоров’я, статеве життя, інформацію стосовно біометричного чи генетичного змісту. Частина 1 статті 7 не застосовується у разі, коли обробку ПД здійснюють при умові однозначної згоди суб'єкта ПД на їх оброблення (п. 1 ч. 2) чи така згода потрібна з метою охорони здоров’я (п. 6 ч. 2) [168; 139].

Стаття 39-1 Основ законодавства України про охорону здоров’я гарантує пацієнту право на збереження конфіденційності інформації щодо його стану здоров’я, фактів звернення за медичною допомогою, діагнозу та результатів медичних обстежень [121].

Пунктом 4 ст. 30 Сімейного кодексу України «Взаємна обізнаність наречених щодо стану здоров’я» передбачено, що результати медичного обстеження є конфіденційними та повідомляються виключно нареченим [205]. Знаковою у

даному контексті є справа «Л.Л. проти Франції» від 10.10.2006 р. №7508/02. Заявник подав скаргу щодо неправомірної передачі на розгляд та використання судами документів з його історії хвороби в контексті шлюборозлучних процесів без його згоди та без медичного експерта. За результатами розгляду матеріалів суд постановив, що мало місце порушення ст. 8 (право на повагу особистого та сімейного життя) Конвенції, вважаючи, що втручання в особисте життя заявника не було виправдане з точки зору основної важливості захисту ПД. Було зазначено, зокрема, що суди Франції використовували оскаржуваний медичний висновок як допоміжний засіб для підтримки своїх рішень, однак виявилося, що вони могли дійти такого ж висновку і без нього. Тобто нормами внутрішнього законодавства не забезпечено достатніх гарантій використання інформації щодо особистого життя сторін в цьому типі судових процесів, тим самим виправдовуючи необхідність точного розгляду необхідності використання таких мір [59; 139].

Також нормами Закону «Про захист населення від інфекційних хвороб» (ч. 2 ст. 26) визначено, що інформація щодо зараження інфекційною хворобою суб'єкта, яка може передаватися статевим шляхом, медичні огляди та обстеження, які проводяться, відомості інтимного змісту, які отримано при виконанні службових повноважень медичними працівниками становлять лікарську таємницю. Розповсюдження чи надання такої інформації дозволено лише у законодавчо передбачених випадках [167; 139].

Зазначимо, що у окремих напрямах медичної галузі, наприклад психіатрії, не завжди можливо гарантувати дотримання конфіденційності інформації, адже її правовий захист пацієнтів має певні особливості. Саме тому у правових актах, що регулюють діяльність у даному напрямі, особливе значення приділяється питанням збереження лікарської таємниці.

Медичні працівники та інші спеціалісти, які залучаються до надання психіатричної допомоги, а також особи, що дізналися про психічні розлади, факти звернення за такого роду допомогою, лікування у закладах даного напряму чи іншу

інформацію у даному контексті, зобов'язані дотримуватися правових норм щодо конфіденційності, окрім винятків, передбачених законом [221; 139].

Так, частинами 3, 4 статті 6 Закону «Про психіатричну допомогу» передбачено можливість передачі інформації щодо психічного стану особи та надання їй такої психіатричної допомоги без згоди суб'єкта чи його представника або відкриття провадження досудового розслідування чи складання досудової доповіді про обвинувачених чи розгляду інформаційного запиту слідчого, прокурора, суду та представника уповноваженого органу з питань пробації [182].

Статтею 286 Цивільного кодексу України гарантовано право на таємницю щодо стану здоров'я, а ч. 3 цієї статті визначено, що фізична особа, якій стала відома інформація щодо стану здоров'я, факту звернення, обстеження, діагнозу зобов`язана утримуватися від її поширення [249].

Відповідно до частини 1 статті 40 Основ законодавства про охорону здоров'я, як медичним працівникам, так іншим особам, які під час виконанням службових повноважень дізналися про хворобу, обстеження, діагноз заборонено розголошувати таку інформацію, крім випадків, визначених законодавчо [121].

Особливу увагу слід приділити Закону України № 555-IX від 13 квітня 2020 року «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)». Відповідно до підпункту 1 пункту 2 розділу II цього закону, протягом дії карантину або інших обмежувальних заходів, пов'язаних із COVID-19, а також протягом 30 днів після їх завершення, дозволяється обробка персональних даних громадян (стан здоров'я, місце госпіталізації чи самоізоляції, прізвище, ім'я, по батькові, дата народження, місце проживання, місце роботи або навчання) без згоди особи з метою протидії поширенню коронавірусу у порядку, визначеному рішенням про встановлення карантину. Використання таких даних дозволяється виключно для проведення протиепідемічних заходів [156; 139]. Після завершення карантинного

періоду зазначена інформація протягом 30 днів підлягає знеособленню, а у разі неможливості – знищенню.

Як бачимо, формулювання закону досить неоднозначне, так як визначення мети обробки персональних даних як можливість їх використання виключно з метою здійснення протиепідемічних заходів – дуже широке за своїм змістом поняття. Поточна редакція закону може отримувати довільну інтерпретацію з боку органів державної влади, підприємств, установ та організацій, які надають медичну допомогу.

Для уникнення неоднозначності та забезпечення більш чіткого визначення мети і кола суб'єктів обробки персональних даних пропонується доповнити підпункт 1 пункту 2 розділу II Закону України «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» та викласти його у такій редакції: «Дозволяється обробка персональних даних щодо стану здоров'я, місця госпіталізації або самоізоляції, прізвища, імені, по батькові, дати народження, місця проживання, місця роботи або навчання без згоди особи, у порядку, визначеному рішенням про встановлення карантину, за умови належного технічного захисту даних та їх використання виключно з метою протидії поширенню COVID-19, а також за наявності у працівника, який безпосередньо здійснює обробку таких даних, зобов'язання щодо нерозголошення інформації» [139].

Таким чином, незважаючи на те, що оброблення ПД без згоди суб'єкта даних є порушенням прав людини, вітчизняне законодавство у окремих випадках дозволяє їх обробку [139].

У 2017 році Верховна Рада України ухвалила Закон України «Про державні фінансові гарантії медичного обслуговування населення», на підставі якого запроваджено електронну систему охорони здоров'я. Відповідно до положень цього Закону, електронна система охорони здоров'я є інформаційно-телекомунікаційною системою, що забезпечує автоматизований облік медичних

послуг та управління медичною інформацією, включно зі створенням, зберіганням, оприлюдненням і обміном даними. Система розміщена на серверах українських дата-центрів, обладнаних комплексними системами захисту інформації (КСЗІ) та атестованих Державною службою спеціального зв'язку та захисту інформації. До її складу входять центральна база даних і електронні медичні інформаційні системи, інтегровані в єдину функціональну мережу [157].

Слушною у контексті досліджуваного є наукова думка Х.Я. Терешко, що із урахуванням науково-технологічного прогресу, роль і значення інформаційних відносин постійно зростає.

З урахуванням вище викладеного, упровадження електронної системи (e-health), поширення інформації як у межах країни, так і за кордон, можливість електронного консультування, створення електронних реєстрів (пацієнтів; декларацій про вибір лікаря; суб'єктів господарювання у медичній сфері; медичних спеціалістів; медичних працівників; договорів про медичне обслуговування населення; договорів про реімбурсацію) наразі є актуальними.

На думку Х. Я. Терешка, така електронна система створює можливість формування єдиного медичного простору, забезпечує координацію між різними рівнями надання медичної допомоги та сприяє впровадженню сучасної системи управління якістю медичних послуг [230].

Слід зазначити, що відповідно до пункту 2 статті 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення», доступ до інформації про пацієнта, що зберігається в електронній системі охорони здоров'я (ЕСОЗ), допускається лише за умови письмової згоди пацієнта або його законного представника.

Без письмової згоди доступ до відомостей про пацієнта при ознаках прямої загрози життю та здоров'ю пацієнта; неможливості отримання згоди такого пацієнта чи його законних представників (до часу, коли отримання згоди стане можливим); за рішенням суду [157].

Надання пацієнтам повної та прозорої інформації щодо збору, обробки та зберігання їхніх даних, а також контроль за цими процесами, що повністю відповідає вимогам GDPR, регламентується Порядком функціонування електронної системи охорони здоров'я України від 25.04.2018 № 411 [144].

Відповідно до Закону України «Про захист персональних даних» [168], пацієнт особисто надає письмову згоду на обробку своїх персональних даних. Це забезпечує реалізацію права на конфіденційність та контроль над власною інформацією, що є ключовим принципом GDPR. Зокрема, порядок передбачає: прозорість обробки даних – пацієнт отримує чітку інформацію про мету збору даних, строки їх зберігання та осіб, які матимуть до них доступ; добровільність та свідомість згоди – обробка медичних даних можливе лише за письмовою згодою пацієнта, що відповідає принципу добровільного надання згоди GDPR; обмеження доступу та захист інформації – дані зберігаються у захищеній електронній системі, доступ до них мають лише уповноважені медичні працівники; право пацієнта на контроль – пацієнт може отримувати інформацію про обробку своїх даних та вимагати їх коригування чи видалення у разі відсутності необхідності їх обробки.

Таким чином, регламент функціонування електронної системи охорони здоров'я у поєднанні із Законом України «Про захист персональних даних» створює національну правову основу, що адаптує стандарти GDPR до сфери медичних послуг і гарантує високий рівень захисту прав пацієнтів та конфіденційності їхніх медичних даних.

Законодавчо закріплено, що доступ до даних пацієнта, які зберігаються в ЕСОЗ, можливий виключно за наявності письмової згоди пацієнта або його законного представника, або іншої форми, що дозволяє підтвердити факт надання такої згоди.

Проте, варто акцентувати увагу на тому, що ч. 2 ст. 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення» передбачено випадки можливого отримання доступу до ПД без надання згоди пацієнта: наявні

ознаки безпосередньої загрози життю пацієнта; неможливо отримати згоду пацієнта чи його законних представників (до моменту можливості отримати згоду); за рішенням суду [157; 139].

Отже, здійснення обробки ПД у медичній сфері без згоди особи, яких вона стосується, законно виключно у випадку, якщо вона проводиться з метою охорони здоров'я відповідним колом осіб.

Як ми попередньо зазначали, у 2017 році в Україні розроблено та запроваджено Електронну систему охорони здоров'я «E-Health», інформаційно-телекомунікаційну систему, яка забезпечує єдиний інформаційний простір та обмін даними через Центральну базу даних [242]. В систему інтегровано укладання електронних декларацій з сімейними лікарями, виписки рецептів, медичні направлення, статистику щодо хворих на коронавірус тощо. Проте дана система, практично упродовж року застосування, у порушення вимог норм з технічного захисту інформації, не мала сертифікату про відповідність комплексній системі захисту інформації (далі – КСЗІ).

Наразі МОЗ разом з Міністерством цифрових трансформацій працює над інтеграцією системи «E-Health» у портал та додаток «Дія». З метою покращення ефективності захисту інформації у даній системі пропонуємо при розробці програмного забезпечення дотримуватись вимог HIPAA, як перевіреного та налагодженого стандарту.

Продовжуючи зазначимо, що однією з реформ у медичній сфері є введення декларації про вибір лікаря, який надає первинну медичну допомогу (затверджена наказом МОЗ України від 19.03.2018 № 503). Пацієнт (чи його законний представник) шляхом підписання декларації про вибір лікаря, який надає первинну медичну допомогу, підтверджує, що усвідомлює мету збирання і обробки своїх персональних даних [198]. Тобто, підписуючи декларацію з терапевтом, педіатром або сімейним лікарем, пацієнт надає згоду на те, що його персональні дані (або дані його дитини чи підопічного) будуть внесені до ЕСОЗ. Це забезпечує доступ до цих

даних лікарю, з яким укладена декларація, а також іншим лікарям, до яких пацієнт звернеться за медичною допомогою на підставі направлення від основного лікаря [134].

В електронну систему охорони здоров’я персональні дані пацієнтів можуть вносити виключно уповноважені співробітники медичних закладів. До них відносяться медичні працівники або інші особи з відповідними повноваженнями, наприклад, лікарі-ФОП із ліцензією на медичну діяльність та їхній персонал. Вони зобов’язані суворо дотримуватися вимог законодавства щодо лікарської таємниці та гарантувати надійний захист таких даних. Розголошення інформації, отриманої у процесі виконання службових обов’язків, заборонено, за винятком випадків, прямо передбачених законодавством [198; 135]. *Отже, персоналізовані дані пацієнта, що включають інформацію з декларації, а також дані з електронного рецепта і медичної картки, доступні лише лікарю, з яким укладено декларацію, і лікарю, до якого пацієнт звертається за направленням.*

Варто акцентувати увагу і на тому, що, на жаль, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» 1994 року та серія нормативних документів про технічний захист інформації (далі – НД ТЗІ) безнадійно застарілі. Окрім цього, вони зобов'язують органи державної влади, об'єкти критичної інфраструктури та приватні компанії, що надають послуги державним установам, впроваджувати комплексну систему захисту інформації. Ця система, хоча й є морально застарілою, не забезпечила ефективного захисту протягом багатьох років [4].

За недотримання норм чинного законодавства, що регулюють захист медичної інформації, передбачена дисциплінарна, адміністративна, цивільно-правова та кримінальна відповідальність. Зокрема, у разі неправомірного розголошення відомостей про стан здоров’я, що спричинило матеріальну чи моральну шкоду, винна особа зобов’язана відшкодувати збитки у повному обсязі відповідно до статей 23, 1167 та 1172 Цивільного кодексу України [249].

Кримінальний кодекс України [88] встановлює як загальну відповідальність за порушення лікарської таємниці (ст. 145), так і спеціальну відповідальність за розголошення результатів медичного огляду, проведеного для виявлення невиліковних інфекційних хвороб (ст. 132).

Крім того, систематичне недотримання вимог законодавства щодо захисту медичних даних пацієнтів тягне за собою дисциплінарні санкції у сфері ліцензування. Зокрема, відповідно до ст. 21 Закону України «Про ліцензування певних видів господарської діяльності» [174], порушення правил може призвести до анулювання ліцензії на провадження медичної практики.

Слід також звернути увагу, що ст. 2 Конвенції про захист прав і основоположних свобод (далі – Конвенція) гарантує кожному право на життя [76; 134]. Практика Європейського суду з прав людини (ЄСПЛ) демонструє, що порушення цього права може мати місце не лише у разі позбавлення життя, але й при серйозних ушкодженнях здоров’я, які створюють реальну загрозу життю, навіть якщо смерть не настала [58].

Складовими права на здоров’я є право на інформацію та її конфіденційність, закріплене ст. 8 Конвенції. Так, у рішенні ЄСПЛ у справі «М.С. проти Швеції» (27.08.1997) наголошено, що збереження конфіденційності медичної інформації є ключовим принципом правової системи держав-учасниць, а національне законодавство зобов’язане забезпечувати захист відомостей про стан здоров’я у відповідності до ст. 8 Конвенції [58].

Міжнародний кодекс медичної етики (1949 р.) [108] встановлює обов’язок лікарів зберігати конфіденційність інформації про пацієнта навіть після його смерті. Подібні положення містить Міжнародна клятва лікаря (1948 р.), що передбачає повагу до довіреної лікареві таємниці й після смерті пацієнта [109]. У документі «Дванадцять принципів надання медичної допомоги у будь-якій національній системі охорони здоров’я» (1963 р.) шостий принцип підкреслює обов’язок всіх

учасників лікувального процесу дотримуватися конфіденційності у відносинах лікар–пацієнт, зокрема ця норма застосовується й до органів державної влади [221].

Відповідно до Директиви про захист персональних даних (ст. 8 (1)) та Конвенції № 108 (ст. 6), персональні дані щодо стану здоров'я відносяться до чутливих і підлягають посиленому режиму обробки. Хоча ці міжнародні стандарти значно підсилюють захист прав пацієнтів, на практиці їхнє дотримання у медичних закладах часто залишається недостатнім.

Наприклад, у справі «Z проти Фінляндії» (рішення ЄСПЛ від 25.01.1997 № 22009/93) стосовно розголошення інформації про ВІЛ-інфікованість особи, Суд постановив, що таке втручання не було виправданим у демократичному суспільстві. Суд зазначив, що захист медичних даних є критично важливим для забезпечення права на повагу до приватного і сімейного життя, особливо коли йдеться про інформацію про ВІЛ-інфекцію, враховуючи стигматизацію, що супроводжує цю хворобу в багатьох спільнотах. Згідно з рішенням Суду, надання доступу до інформації про особу заявника та стан її здоров'я, яке відбулося в рішенні апеляційного суду після завершення 10-річного періоду з моменту винесення рішення, порушувало ст. 8 Європейської конвенції про права людини [194].

Таким чином, виникає необхідність запровадження ефективних механізмів захисту медичної інформації, закріплення яких у національному законодавстві є ключовою умовою реалізації права людини на недоторканність приватного життя.

Згідно з Конвенцією про захист осіб у зв'язку з автоматизованою обробкою персональних даних, персональні відомості про расову належність, політичні, релігійні або інші переконання, а також дані про стан здоров'я не можуть оброблятися автоматизовано без встановлення законодавчо визначених гарантій [74]. Подібний підхід передбачено й у статті 8 Директиви Європейського Парламенту та Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних», де встановлено заборону на обробку даних

щодо расового або етнічного походження, стану здоров’я чи сексуального життя особи.

Винятки з цього правила допускаються лише у випадках, коли обробка інформації є необхідною для: захисту життєво важливих інтересів суб’єкта даних або інших осіб у разі неможливості отримати згоду через недієздатність чи неправоздатність; цілей профілактичної медицини, медичної діагностики, надання медичних послуг або лікування; адміністрування діяльності служб охорони здоров’я, за умови, що обробка здійснюється медичним працівником, який зобов’язаний дотримуватися лікарської таємниці [165; 139].

В Україні захист персональних даних пацієнтів реалізовано через Закон України «Про захист персональних даних», який зобов’язує отримувати письмову згоду пацієнта на обробку його персональної інформації у медичній сфері [168]. Крім того, Порядок функціонування електронної системи охорони здоров’я (№ 411 від 25.04.2018) регламентує збір, обробку та доступ до медичних даних, забезпечуючи їх захист відповідно до стандартів GDPR [144]. Таким чином, доступ до інформації про пацієнта, що зберігається в ЕСОЗ, можливий лише за наявності письмової згоди пацієнта або його законного представника, або іншого підтвердженого способу згоди.

Згідно із Загальним регламентом Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб у зв’язку з обробкою персональних даних і про вільний рух таких даних» (GDPR), дані, що мають підвищену чутливість для прав і свобод людини, підлягають особливому захисту. Їх обробка без згоди суб’єкта можлива лише з метою захисту суспільних інтересів у медичній сфері [47].

Таким чином, міжнародне законодавство, подібно до вітчизняного, дозволяє обробку персональних даних без згоди осіб лише в особливих випадках. Проте міжнародне законодавство також передбачає обов'язок держави забезпечити інформаційний захист таких даних. Незважаючи на важливість міжнародних норм захисту персональних даних пацієнтів для забезпечення їх прав, на практиці ці

норми не завжди реалізуються належним чином [139]. Так, наприклад, знаковою для науковців стала справа «Gillberg v. Sweden» [193]. Крістофер Гілберг, дослідник дитячої психіатрії в Гетеборзькому університеті, опинився у центрі правового спору після того, як два інші науковці звернулися до нього з проханням надати документи його дослідження. Гетеборзький університет, як розпорядник інформації, спочатку відмовив у наданні цих документів. Однак запитувачі звернулися до суду, який ухвалив рішення про надання документів за певних умов секретності. Гілберг та університет відмовилися виконати рішення суду і знищили документи, що призвело до кримінального покарання для Гілберга, його колег та віце-президента університету. Гілберг звернувся до ЄСПЛ, стверджуючи, що його права, згідно зі статтями 8 (право на повагу до приватного життя) та 10 (право на свободу вираження поглядів) Конвенції були порушені. Він аргументував, що стаття 10 Конвенції передбачає не лише позитивне право на передачу і отримання інформації, але й негативне право не розголошувати інформацію, яку він не бажає поширювати. У 2010 році справа була розглянута палатою суддів ЄСПЛ, а у 2012 році – Великою палатою. Суд спростував позицію Гілберга щодо негативного права не надавати інформацію. За шведським законодавством, Гетеборзький університет є публічною установою, і його працівники – посадовими особами, а інформація, якою розпоряджається університет, має статус публічної. ЄСПЛ зазначив, що дії Гілберга перешкоджали вільному обміну думками та ідеями щодо дослідження. Суд також підкреслив, що підтримка позиції Гілберга порушила б права запитувачів на доступ до публічних документів відповідно до статті 10 Конвенції [195; 139]. Таким чином, стало очевидним, що позиція ЄСПЛ, що повинно вплинути на підходи національних судових інстанцій.

У травні 2018 року в Європейському Союзі почав діяти Загальний регламент із захисту персональних даних (General Data Protection Regulation – GDPR) [48]. Цей документ скасував попередні акти у сфері захисту даних та встановив єдині правила для їх обробки й вільного обігу як у публічному, так і в приватному секторі.

Особлива увага у Регламенті приділяється даним про стан здоров'я, для яких передбачено додаткові запобіжники з метою гарантування конфіденційності та дотримання прав суб'єктів даних. Найсуттєвішим нововведенням стало закріплення принципу, за яким саме пацієнти, а не лікарі чи медичні установи, отримали першочергове право контролювати та розпоряджатися інформацією про власне здоров'я [139].

Україна визначила імплементацію вимог GDPR пріоритетним напрямом у межах виконання Угоди про асоціацію з ЄС, зокрема через оновлення національного законодавства у сфері захисту персональних даних відповідно до Регламенту (ЄС) 2018/1725. У листопаді 2019 року при Секретаріаті Уповноваженого Верховної Ради України з прав людини було створено міжвідомчу робочу групу для підготовки законодавчих ініціатив щодо персональних даних та координаційну групу для внесення змін до Закону України «Про захист персональних даних» з урахуванням принципів GDPR [139].

У 2020 році робоча група розробила законопроєкт № 2671-1 «Про внесення змін до Закону України "Про захист персональних даних" (щодо форм та умов надання згоди на обробку персональних даних)», який мав деталізувати механізми надання згоди суб'єктами даних та легітимізувати обробку персональних даних органами державної влади й місцевого самоврядування у межах їх компетенції. Документ також передбачав поетапне впровадження стандартів Регламенту (ЄС) 2016/679. Проте вже 4 березня 2020 року законопроєкт повернули на доопрацювання, а згодом його зняли з розгляду у парламенті.

Підсумовуючи, можна констатувати, що попри деякі позитивні зміни у медичній сфері, є ряд проблем у захисті персональних даних. Інформаційні ресурси та технології обробки даних часто розробляються без належного рівня централізації та координації, що свідчить про необхідність удосконалення вітчизняного законодавства. Програмно-технічні комплекси, зазвичай, створюються без достатнього врахування позитивного зарубіжного досвіду та сучасних технологій

для єдиних інформаційних систем. Недостатня взаємодія між інформаційними системами медичної сфери і системами інших регіонів ускладнює обмін даними і координацію. Часто ці системи проєктуються як тимчасові, що не дозволяє проводити довгостроковий аналіз їх діяльності. Заклади охорони здоров'я накопичують великі обсяги конфіденційної інформації, але питання інформаційної безпеки, зазвичай, не є пріоритетними при проєктуванні та експлуатації цих систем. Ці проблеми вказують на необхідність кардинальної зміни підходу до правового захисту інформації у медичній сфері.

Крім того, для гармонізації національного законодавства із положеннями Загального регламенту Європейського Парламенту і Ради (ЄС) 2016/679 та Регламенту (ЄС) 2018/1725 доцільним є здійснення низки заходів. Насамперед необхідно створити спеціалізований незалежний наглядовий орган у сфері захисту персональних даних. На сьогодні контрольні функції виконує Уповноважений Верховної Ради України з прав людини, проте такий механізм не відповідає його конституційно-правовому статусу. Відповідно, новий орган має бути наділений повноваженнями, передбаченими європейським законодавством.

Окрім цього, важливим є: зобов'язання медичних закладів отримувати чітко виражену згоду пацієнтів на обробку їхніх персональних даних; введення посади відповідальних осіб із питань захисту персональних даних у кожному медичному закладі; закріплення права суб'єктів даних на «стирання» (право на забуття) у випадках, коли подальше зберігання інформації є необґрунтованим; надання наглядовому органу права накладати санкції (штрафи) на установи та компанії, які порушують правила обробки персональних даних [139].

2.2. Інформаційна приватність у медичній сфері

Життя і здоров'я людини визнаються найвищими суспільними цінностями, а відомості про стан здоров'я становлять важливий елемент соціального статусу громадянина в системі суспільних відносин [78]. Захист прав людини, включаючи право на інформацію, становить фундамент конституційного правопорядку. Реалізація цього права, зокрема в частині доступу до таємниці медичних даних, відображає не лише рівень демократичності держави, а й міру інтегрованості національного законодавства у міжнародний правовий простір та його відповідність світовим стандартам [103].

Ще з античних часів лікарі дотримувалися етичного обов'язку не розголошувати інформацію про пацієнта. У Клятві Гіппократа зазначено: «Що б при лікуванні – також і поза лікуванням – я не побачив чи не почув про життя людське, те, що не слід розголошувати, я збережу у таємниці». Цей припис заклав основу для одного з головних принципів взаємовідносин лікаря і пацієнта – конфіденційності. В українському правовому полі цей принцип знайшов відображення, зокрема, у статті 286 Цивільного кодексу України та статті 40 Закону України «Основи законодавства України про охорону здоров'я».

Однак, як зазначають фахівці з інформаційної безпеки: «в медичних установах, де обробляються персональні дані пацієнтів, залишається традиційно низький рівень захисту даних, а недостатнє фінансування заходів із забезпечення безпеки інформації спричиняє її розголошення» [151]. Ця проблематика, на думку Х.Я. Терешко є сенситивною, людиноцентристською, адже є особливо вразливою, про що неодноразово у своїх рішеннях наголошував ЄСПЛ: захист інформації особистого характеру (особливо медичної інформації) має ключове значення для забезпечення права на повагу до приватного і сімейного життя. Дотримання

правових норм щодо їх конфіденційності – основний принцип правових систем держав – учасниць Конвенції (справа «М. С. проти Швеції», 1997) [228].

Питання захисту чутливих відомостей в медичній сфері досліджували як вітчизняні, так і зарубіжні вчені, зокрема, А.С. Андрійчук, В.І. Акопов, Н.Б. Болотіна, Г.О. Блінова, Т.Д. Гурська, О.В. Легка, М.М. Малеїна, О.Г. Марценюк, А.І. Марущак, І.Я. Сенюта, С.Г. Стеценко, В.М. Соловйов, Х.Я. Терешко та О.О. Тихомиров. Однак, з огляду на активне впровадження цифровізації у сферу охорони здоров'я, це питання потребує подальшого дослідження.

Аналіз «… інцидентів за перше півріччя 2020 року показав, що медична сфера не змогла забезпечити захист основного артефакту цифрової епохи – персональних даних громадян, включаючи інформацію щодо стану здоров'я. Основним каналом витоку інформації (візьмемо, як приклад, інформацію, пов'язану з пандемією коронавірусу), стала Мережа. У 64,2% випадків в усьому світі персональні дані поширилися у формі списків – документи, зведення, фрагменти записів, у 35,8% витік відбувся за результатами злому сховищ даних, нелегітимного доступу до них, випадкового розкриття інформації через невірні налаштування серверів або помилок в додатках» [72; 262].

За даними Експертно-аналітичного центру ГК Info Watch, який досліджував факти витоку медичної інформації, пов’язаної із COVID-19, лише у першому півріччі 2020 року зафіксовано 72 випадки витоку інформації у світі. Наприклад, через помилку одного з співробітників лікарні, який ненавмисно опублікував на Git Hub електронну таблицю з особистими даними, паролями та доступами до конфіденційних державних систем, стало відомо про персональні та медичні дані 16 мільйонів бразильців, які лікувалися від COVID-19. Після того, як інформація стала публічно доступною, її було видалено з Git Hub, а урядові представники змінили паролі і відкликали ключі доступу для забезпечення безпеки своїх систем [239; 91]. Подібні факти витоку інформації мали місце в Німеччині, Уельсі, Новій

Зеландії, Індії та інших країнах. Гірше того, за інформацією аналітиків компанії Inter trust, близько 85% додатків для відстеження контактів COVID-19 так чи інакше допускають витік даних. Як бачимо, пандемія коронавірусу актуалізувала ряд проблемних питань щодо захисту інформації у медичній сфері [262].

Разом з цим, як показали результати соціологічного опитування, проведеного Black Book Market Research LLC у кінці 2020 року, серед понад 3600 респондентів (спеціалісти по безпеці, організації-провайдери): «витрати медичних організацій країн Європи на кібербезпеку з 2019 року мають тенденцію до зниження, а 92% медичних закладів взагалі не мають штатного персоналу служби безпеки [21; 262].

І це не зважаючи на те, що з травня 2018 року набув чинності дійсно «епохальний» документ у напрямі захисту інформації, у тому числі і у медичній сфері – Загальний регламент із захисту персональних даних Європейського Союзу. У порівнянні з попередніми нормативними актами, що регулювали захист даних про здоров'я, GDPR надає набагато більше уваги новим вимогам, що з'явилися внаслідок збільшення цифровізації у медичній сфері, що забезпечує покращення рівня захисту ПД. Згідно з GDPR, обробка ПД повинна відповідати наступним принципам: бути законною, справедливою та прозорою; збиратися з конкретною законною метою; бути адекватною, актуальною і обмеженою лише тим, що необхідно; бути точною; зберігатися лише протягом необхідного часу; та забезпечуватися належним рівнем безпеки, цілісності та конфіденційності [48; 91]. GDPR встановлює вищі стандарти стосовно інформованої згоди та обов’язків щодо повідомлення (ст. 7), посилює захист права на доступ до персональних даних про здоров’я. Заслуговує на увагу і те, що у разі витоку персональних даних (ст.ст. 33, 34) контролери даних інформують контролюючий орган протягом 72 год., а у разі порушення безпеки даних, вони повинні інформувати пацієнтів [48; 262].

Як бачимо, GDPR дійсно заслуговує уваги, проте незважаючи на те, що він діє вже протягом двох років, мають місце проблемні питання. Так, наприклад, лише протягом лютого 2021 року: а) Sky Med International звинуватили у невжитті заходів

у частині забезпечення особистої інформації відносно осіб, які підписалися на її план екстреного членства в поїздках, в результаті компанія залишила незахищеною базу даних, що містить 130 000 записів про членство (незахищена база даних містила особисту інформацію членів, що зберігається у звичайному тексті, таку як імена, дати народження, домашні адреси, інформацію щодо стану здоров'я та номери рахунків членів). Крім того FTC стверджував, що Sky Med увів в оману споживачів, вивісивши на кожній сторінці свого веб-сайту печатку «Відповідність HIPAA», що створило помилкове враження, що її політика конфіденційності була переглянута і відповідала вимогам безпеки та конфіденційності Закону про переносимість та підзвітність медичного страхування (HIPAA) [267]; б) у Польщі наклали штраф (85 000) злотих на підприємця, який надавав послуги у медичній сфері. Так, відповідно до вказівок Управління захисту ПД Польщі, підприємець повинен був повідомляти своїх пацієнтів про порушення їхніх персональних даних, а також надавати їм рекомендації щодо мінімізації потенційних негативних наслідків інциденту. З урахуванням того, що адміністратор цього не робив, на нього, згідно із ст. 58 сек. 2 GDPR, накладено адміністративний штраф [128].

Варто зазначити, що право на захист відомостей у медичній сфері повинне виникати разом суб'єктивним правом, а не в момент його порушення. Іншими словами, з моменту надходження інформації про здоров'я медичному працівнику, або ж інформацію отримав лікар під час надання медичної допомоги, починає діяти правовий режим медичної інформації з відповідним ступенем захисту.

Правове регулювання у контексті досліджуваного передбачає зовнішню і внутрішню взаємопов'язану систему законів і підзаконних нормативних актів. Проте єдиного закону, який урегулював би збір та обробку медичної інформації, на жаль, наразі немає [135].

Проблема забезпечення інформаційної приватності у медичній сфері набула особливої актуальності після прийняття Закону України «Про захист персональних даних». Відповідно до статті 7 цього Закону, обробка персональних даних у

медичних цілях – зокрема для встановлення діагнозу, надання лікування, догляду або медичних послуг – забороняється, крім випадків, коли її здійснює лікар або інша уповноважена особа медичного закладу. У таких випадках ці особи зобов'язані дотримуватися як законодавства про захист персональних даних, так і норм, що регламентують лікарську таємницю [168].

Як слушно зазначає Г. О. Блінова, законодавець, сформулювавши цю норму, фактично закріпив подвійний механізм охорони медичної інформації: з одного боку – у форматі дотримання лікарської таємниці, з іншого – у режимі захисту персональних даних [15].

Незважаючи на те, що цифровізація медичної сфери сприятиме покращенню ефективності забезпечення прав людини, аналіз чинних правових норм свідчить про наявність чисельних законодавчих колапсів у даному напрямі[235].

Наприклад, 4 грудня 2019 року Верховний Суд України розглянув справу № 760/8719/17 у спрощеному позовному провадженні. У 2017 році ОСОБА_2 подала позов проти Київського міського психоневрологічного диспансеру № 5. Позивачка вимагала спростування інформації про її перебування на обліку у лікаря-психіатра з 1972 по 2003 рік з діагнозом «психічні розлади». Вона також вимагала, щоб відповідач видалив довідку про її лікування з документів поліції Солом'янського району, Київської міської державної адміністрації, Київської місцевої прокуратури № 9, а також з інших організацій, де була розповсюджена ця інформація. Крім того, позивачка просила зобов'язати відповідача припинити поширення незаконних і необ'єктивних довідок про її лікування в диспансері [135].

Верховний Суд України постановив касаційну скаргу задовольнити, адже інформація щодо стану здоров`я є персональними чутливими даними, їх збір здійснюється виключно за згодою заявника, за виключенням випадків, передбачених законом (організація надання особі, яка страждає на тяжкий психічний розлад, психіатричної допомоги; провадження досудового розслідування або судового розгляду за письмовим запитом слідчого, прокурора та суду).

Матеріали справи не містять даних про наявність досудового розслідування. Відомості щодо стану здоров'я позивача, яку вона оскаржувала, була надана Диспансером № 5 інспектору Солом'янського Управління Національної поліції під час перевірки скарги сусідів позивача. Установлені фактичні обставини не підтверджують правомірність збору та використання даних про психічне здоров'я позивача в такій формі і контексті, в якому вони були використані. Мета обробки даних не була виправданою, оскільки інформація стосувалася подій, що мали місце у 1972-2003 роках. Зазначена інформація, надана інспектору Солом'янського Управління Головного управління Національної поліції в м. Києві, відноситься до медичної інформації. Збирання, зберігання, поширення та інша обробка такої інформації підпадають під дію статті 8 Конвенції [146; 135].

Крім того, у рішенні ЄСПЛ від 29.04.2017 (справа «Л.Х. проти Латвії» № 52019/07) Європейський суд також дійшов висновку про порушення ст. 8 Конвенції у зв'язку із тим, що втручання в гарантоване право шляхом збору інформації про медичне лікування заявниці державною установою без її згоди не відповідало нормам закону, оскільки закон не було сформульовано з достатньою чіткістю та він не надавав належний юридичний захист від свавілля. Зокрема у 1997 році під час пологів у результаті хірургічного втручання лікар без згоди заявниці застосував перев’язку маткових труб. У 2005 році заявниця, попередньо не дійшовши згоди з лікарнею, звернулася з позовом до суду з вимогою компенсації, який було задоволено. Директор зазначеної лікарні звернувся до Інспекції з контролю якості медичного лікування та працездатності (MADEKKI) з проханням оцінити медичне втручання, яке заявниця отримала під час пологів згідно з чинним законодавством 1997 року. MADEKKI розпочала адміністративне розслідування. Запит, надісланий ними, стосувався медичної допомоги, зокрема гінекологічної та під час пологів, яку заявниця отримувала з 1996 по 2003 роки. Європейський суд вказав на відсутність юридичного захисту від свавілля, зазначивши, що Закон, надавши повноваження щодо збору інформації про особу, не визначав чітко обсяг

цих повноважень та способи їх застосування. Це дозволяло державній установі збирати інформацію за будь-який період, не перевіряючи необхідність цієї інформації для досягнення легітимної мети та не оцінюючи відповідність запитуваної інформації щодо подій, які розслідувались[247].

Слід зазначити, що наявні законодавчі суперечності стали предметом розгляду у поданні Уповноваженого Верховної Ради України з прав людини від 6 листопада 2017 року № 1-2499/17-107 до Конституційного Суду України. У цьому поданні ставилося питання відповідності Конституції України (ч. 1 ст. 8 та ч. 1 у поєднанні з ч. 2 ст. 32) положенню абзацу першого пункту 40 Розділу VI «Прикінцеві та перехідні положення» Бюджетного кодексу України, яке надавало Міністерству фінансів України право отримувати інформацію, включно з медичними даними, що містять персональні дані.

Як наголошувалося у зверненні, закон не може вважатися таким, що відповідає принципу верховенства права, якщо він дозволяє державі втручатися у приватне та сімейне життя людини через збір і зберігання персональних даних, але при цьому не визначає: обсягу та порядку застосування таких заходів; мінімальних гарантій, серед яких – повідомлення особи про зібрану інформацію, отримання її згоди на обробку, строк зберігання даних; правил доступу третіх осіб до інформації; вимог до забезпечення її конфіденційності та порядку знищення.

Відсутність цих положень фактично надає державним органам необмежену дискрецію та робить втручання у право людини на приватність непередбачуваним, що, у свою чергу, призводить до свавільного обмеження конституційних прав [135].

Беручи до уваги фундаментальне значення права людини на приватне життя та обов’язок держави його захищати, можна стверджувати, що дискреційні повноваження органів державної влади щодо збору, обробки та зберігання персональних даних повинні бути чітко визначені законом. На це також звертає увагу пункт 1 статті 92 Конституції України, згідно з яким лише законами України

встановлюються права і свободи людини та громадянина, а також гарантії їх реалізації [77].

Продовжуючи аналіз чинної нормативної бази, слід зазначити, що пункт 1 статті 11 Закону України «Про захист персональних даних» передбачає, що обробка персональних даних можлива за умови отримання згоди суб'єкта даних [168]. У виняткових випадках, передбачених законом, дані можуть оброблятися без згоди особи, проте лише в межах, визначених правових норм.

Водночас виникає низка практичних питань, пов'язаних із відмовою пацієнта надавати згоду щодо обробки його персональних даних. Зокрема, законодавство наразі не визначає порядок фіксації інформації про осіб, які відмовляються від внесення своїх даних до електронного реєстру. Як показує практика, відмови, як правило, пов'язані з релігійними чи світоглядними переконаннями. Водночас слід підкреслити, що обробка персональних даних здійснюється для конкретних і законних цілей, і відмова пацієнта надавати згоду не може слугувати підставою для відмови у наданні медичної допомоги [135].

Зважаючи на вищевикладене, пропонуємо на законодавчому рівні розробити та затвердити Алгоритм дій у разі відмови пацієнта надати згоду на обробку персональних даних чи відмови внесення своїх персональних даних до електронного реєстру [135].

Відповідно до статті 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення», уповноважений орган має право публікувати на своєму офіційному веб-ресурсі інформацію, що накопичена в електронній системі охорони здоров'я (ЕСОЗ), лише у знеособленому вигляді, відповідно до вимог Закону України «Про захист персональних даних» [135].

Крім того, частина 3 цієї ж статті передбачає, що підписуючи декларацію про вибір лікаря первинної медичної допомоги, пацієнт або його законний представник одночасно надає згоду на доступ до своїх даних у ЕСОЗ для цього лікаря, а також

для інших медичних працівників у межах їхніх професійних повноважень та потреб, пов’язаних із наданням медичних послуг [157].

Щодо змісту Декларації, її форму затверджено наказом МОЗ України від 19.03.2018 № 503 «Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу». У тексті Декларації зазначено: «… своїм підписом підтверджую добровільність вибору лікаря, вказаного в розділі 2 цього документа, а також достовірність наданих відомостей; засвідчую, що мене поінформовано про мої права відповідно до Закону України „Про захист персональних даних“ [168], а також про мету збору та обробки моїх персональних даних, відображених у цій Декларації» [135].

Виникає питання щодо співвідношення норм Закону України «Про державні фінансові гарантії медичного обслуговування населення» та наказу МОЗ № 503 як з точки зору юридичної сили, так і за характером регулювання. Безумовно, з позиції ієрархії нормативних актів перевага належить Закону. Водночас, аналізуючи взаємодію загальних і спеціальних норм, слід зазначити: Закон «Про державні фінансові гарантії…» носить загальний характер щодо обробки персональних даних, тоді як Закон України «Про захист персональних даних» виступає спеціальним регулюючим актом. Відтак пріоритет у питаннях захисту персональних даних пацієнтів належить спеціальним нормам Закону «Про захист персональних даних» [230; 135].

Мають місце проблемні питання і в запровадженій ЕСОЗ: постійне підвисання системи; недосконалість безпосередньо системи; відсутність: відповідного досвіду у медичних працівників щодо роботи з даною системою; комп’ютерного обладнання з відповідним технічним та програмним забезпеченням; належного захисту інформації; законодавча неврегульованість відмови у наданні згоди на обробку ПД.

Це сприяє порушенню захисту медичної інформації. Для прикладу, Національним координаційним центром кібербезпеки (далі – НКЦК) при Раді безпеки і оборони України у ході моніторингу виявлено витік ПД з однієї із найбільших клінік Дніпра. «Серед інформації, яка опинилася у відкритому доступі, – персональні дані працівників і клієнтів цієї клініки, зокрема ПІБ, дати народження, адреси проживання, телефон, e-mail, діагнози, дані медичної карти (що становить медичну інформацію), включаючи результати аналізів, діагнози, інформацію про захворювання, результати проведення ПЛР-тестів, списки хворих COVID-19» [21]. Даний факт стався у результаті помилок конфігурації в інформаційних системах і базах даних клініки, які мали доступ до мережі Інтернет. Варто звернути увагу на те, що вільний доступ до баз даних надавав можливість не лише викрадення персональної інформації, але і несанкціонованого внесення змін, включаючи модифікацію призначень ліків, результатів аналізів і обстежень, редагування записів в протоколах. Дніпровська клініка досить пасивно відреагувала на даний факт і відомості про пацієнтів тривалий час перебували у вільному доступі [21]. Зазначене порушує пп. 13 п. 2 Загальної частини Порядку функціонування електронної системи охорони здоров'я України, оскільки саме Дніпровська клініка несе відповідальність за невжиття заходів із захисту інформації, будучи розпорядником відповідного реєстру.

Відповідно до ст. 8 Конвенції про захист прав людини і основних свобод, кожна особа має право на повагу до свого приватного та сімейного життя [76]. Конфіденційність медичної інформації, що стосується стану здоров'я, є одним із ключових аспектів реалізації цього права та визнається життєво важливим принципом у правових системах усіх держав – учасниць Конвенції.

Стаття 17 Закону України «Про виконання судових рішень та застосування судової практики Європейського суду з прав людини» встановлює, що судова практика ЄСПЛ є джерелом права для України. Це означає, що національні суди та органи влади зобов'язані враховувати висновки та прецеденти ЄСПЛ під час

розгляду справ, пов’язаних із захистом персональних даних, включаючи медичні дані.

На практиці це забезпечує додатковий рівень охорони конфіденційності: будь-яке порушення права пацієнта на приватність може бути оцінене не лише у контексті національного законодавства, але й з огляду на стандарти Європейського суду. Зокрема, ЄСПЛ у своїй практиці неодноразово підкреслював, що державні органи повинні забезпечувати надійні гарантії збереження медичних даних, обмежувати доступ третіх осіб та впроваджувати ефективні механізми контролю за обробкою такої інформації. Таким чином, ст. 8 Конвенції та прецеденти ЄСПЛ формують правову основу для удосконалення національної системи захисту медичних даних та інтеграції її у європейські стандарти.Проте на практиці такі проблеми мають місце. У першу чергу варто звернути увагу на питання захисту медичної інформації під час та після проведення планових та позачергових медичних оглядів. Зокрема, законодавчо передбачено після проведення медичних оглядів результати обстеження заносити до особистої медичної карти, на підставі чого робиться загальний висновок щодо можливості допущення працівника до роботи. Мають місце випадки, коли ще до встановлення остаточного діагнозу роботодавець попереджається про те, що у його працівника можливо наявні протипоказання до певного виду діяльності [46]. Тобто, лікар прямо порушує чинне законодавство щодо захисту медичної інформації. Однак у деяких випадках лікар є «прямим заручником» недосконалості вітчизняного законодавства.

Як приклад можна навести рішення Печерського районного суду м. Києва у справі за адміністративним позовом лікаря-анестезіолога-реаніматолога МКЛ № 2 м. Вінниці щодо незаконності наказу «Про затвердження зразка, технічного опису листка непрацездатності та Інструкції про порядок заповнення листка непрацездатності». Лікар звернула увагу на незаконність норми, що передбачала включення у листок непрацездатності відомостей про діагноз та код захворювання

відповідно до Міжнародної класифікації хвороб, оскільки це порушує конституційне право на приватність та конфіденційність медичної інформації [94].

Судова колегія Печерського районного суду м. Києва задовольнила позовні вимоги, визнавши оскаржуваний нормативний документ частково нечинним. Зокрема, подання відомостей про діагноз у лікарняному листку було визнано таким, що суперечить нормам вищої юридичної сили, зокрема: Конституції України (ст. 3, 19, 21, 22, 32, 55, 64, 68), Європейській конвенції про захист прав людини та основоположних свобод (ст. 8), Основам законодавства України про охорону здоров'я (ст. 4, 6, 7, 8, 14, 40, 41), Цивільному кодексу України (ст. 285, 286) та Закону України «Про інформацію» (ст. 23) [94].

Виходячи з цього, вказування лікарського діагнозу у листках непрацездатності без застосування відповідного коду медичних даних є незаконним. Код медичних даних – це буквено-цифровий запис, який перетворює словесно сформульований діагноз на стандартизовану форму для зручності зберігання, обробки та аналізу інформації.

Слід зазначити, що лікарі стаціонару тривалий час користуються Міжнародною класифікацією хвороб десятого перегляду (МКХ-10), яка ратифікована Всесвітньою організацією охорони здоров'я (ВООЗ). Утім, починаючи з квітня 2020 року, у рамках реформи вторинної ланки медичної допомоги в Україні, медичні працівники перейшли на використання Міжнародної класифікації хвороб десятого перегляду в австралійській модифікації (МКХ-10-АМ) [252].

Крім того, відповідно до пункту 3.2 Інструкції про порядок заповнення листка непрацездатності, затвердженої спільним наказом МОЗ України, Міністерства праці та соціальної політики, Фонду соціального страхування з тимчасової втрати працездатності та Фонду соціального страхування від нещасних випадків на виробництві і професійних захворювань України від 03.11.2004 р. № 532/274/136-

ос/1406532, у графі «Діагноз первинний» лікар фіксує діагноз, встановлений на перший день видачі листка непрацездатності.

У графі «Діагноз заключний» фіксується остаточний діагноз, а у графі «Шифр МКХ-10» – відповідний код діагнозу згідно з Міжнародною статистичною класифікацією хвороб та споріднених проблем охорони здоров'я десятого перегляду (МКХ-10), прийнятою 43-ю Всесвітньою асамблеєю охорони здоров'я 1 січня 1993 року.

Внесення даних у графи «Діагноз первинний», «Діагноз заключний» та «Шифр МКХ-10» можливе лише за письмової згоди пацієнта. Якщо така згода відсутня, ці відомості до листка непрацездатності не вносяться, що захищає права людини на конфіденційність [65].

Пандемія COVID-19 продемонструвала, що права на медичну інформацію можна легко порушити: кількість повідомлень про втручання у доступ до інформації у 2023 році зросла майже в півтора рази порівняно з попереднім роком [254]. Працівники Секретаріату Уповноваженого Верховної Ради України з прав людини склали понад 190 протоколів за порушення ч. 1 та 2 ст. 212-3 КУпАП.

Це підтверджує, що захист медичної інформації – не формальність, а питання безпеки пацієнта та реалізації його конституційного права на приватність. Будь-яке недбале ставлення до обробки персональних даних може призвести до серйозних наслідків – від втрати довіри до медичних установ до юридичної відповідальності [65; 254].

Зазначимо, що право на отримання інформації, пов'язаної з охороною здоров'я та медичною допомогою, регламентовано ч. 4 ст. 15 Закону України «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI [160]. Звернення громадян, отримані Уповноваженим у 2023 році, свідчать про порушення їх прав на отримання медичної інформації, в тому числі на можливість отримання медичної допомоги.

Для прикладу, до Уповноваженого з прав людини надійшла скарга щодо порушення ДУ «Інститут проблем ендокринної патології ім. В.Я. Данилевського Національної академії медичних наук України» права на інформацію в частині необґрунтованого обмеження доступу до інформації про перелік аналізів і досліджень, які структурні підрозділи та консультативна клініка Інституту проводять безоплатно для визначених категорій пацієнтів. За результатами розгляду у відношенні посадової особи вказаного закладу складено протокол про адміністративне правопорушення. Згідно із постановою Київського районного суду м. Харкова, заступника директора Інституту визнано винним у вчиненні адміністративного правопорушення, передбаченого ч. 2 ст. 212-3 КУпАП, та накладено адміністративне стягнення у виді штрафу [254].

У розрізі аналізованої проблематики варто звернути увагу і на низький рівень правової грамотності медичних працівників, адже саме проблема незнання законів позбавляє можливості медичних працівників орієнтуватися, в яких випадках і кому вони можуть передати відомості про здоров'я, діагноз та факт звернення за допомогою громадянина. Слушною з цього приводу є наукова думка К.Г. Попової, яка вважає, що система знань про здоров'я людини наразі не обмежується медичними аспектами, а передбачає соціально-гуманітарний підхід, тобто вивчення всієї сукупності відносин між лікарем і пацієнтом в діапазоні від традиційної турботи про психічний стан хворого до принципів етичного та законодавчого регулювання лікарської діяльності [142, с. 9].

Таким чином, якісна медична реформа можлива лише за умови впровадження сучасних методів інформатизації та, відповідно, захисту інформації. Як засвідчив аналіз, наразі в Україні система правового забезпечення захисту інформації у медичній сфері потребує негайного удосконалення [135].

Для забезпечення ефективного управління медичною інформацією в Україні необхідним є системний підхід до кодифікації та гармонізації національного законодавства із нормами європейського права та міжнародних стандартів.

Доцільним є створення комплексного нормативно-правового акта, який на законодавчому рівні визначав би порядок збору, обробки, збереження та передачі медичної інформації, з урахуванням кращих практик GDPR. Такий документ має передбачати:

– структурування медичної інформаційної системи та інтеграцію її компонентів;

– встановлення обов'язкової сертифікації для захисту інформації й використання сучасних технологій криптографії та кодування;

– розмежування прав доступу медичних працівників відповідно до їхньої компетенції, із запровадженням електронного підпису для підтвердження внесених даних;

– обов'язкове проходження короткострокових навчальних курсів із захисту інформації та реєстрацію користувачів у службі інформаційної безпеки, включно з визначенням рівнів доступу, можливістю їх зміни, а також наданням персонального логіну для автентифікації;

– розробку алгоритмів обміну інформацією між медичними закладами з метою забезпечення цілісності, конфіденційності та доступності даних.

Окрім цього, пропонується внести зміни до Закону України «Про захист персональних даних» щодо форм та умов надання згоди на обробку персональних даних пацієнтів. При створенні програмного забезпечення для медичних інформаційних систем слід керуватися вимогами стандарту HIPAA. Законодавчо також доцільно посилити відповідальність за порушення норм захисту медичної інформації, що сприятиме підвищенню рівня довіри пацієнтів до системи охорони здоров'я та забезпеченню захисту їхніх прав у інформаційному просторі.

2.3. Джерела загроз для інформаційних систем у сфері охорони здоров'я України

Сучасний етап розвитку медичної галузі в Україні, у контексті триваючих реформ та дії правового режиму воєнного стану, підкреслює необхідність подальшої цифровізації сектору охорони здоров'я та забезпечення надійного технічного захисту електронної інформації. Відповідно до Стратегії національної безпеки України, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020, принцип «безпека людини – безпека держави» є ключовим орієнтиром державної політики [225].

Прийнята у 2021 році Стратегія інформаційної безпеки України закладає основи комплексної взаємодії на основі Конституції України, чинних законів, Стратегії національної безпеки, Стратегії кібербезпеки, а також міжнародних договорів, ратифікація яких здійснена Верховною Радою України [141]. У документі визначено, що «забезпечення інформаційної безпеки України є однією з найважливіших функцій держави», при цьому реалізація зазначеної Стратегії планується до 2025 року [224]. Таким чином, правова та організаційна база формує необхідні передумови для захисту медичної інформації та забезпечення безпеки електронних систем охорони здоров'я на національному рівні.

Положенням всесвітньої медичної асоціації щодо використання комп'ютерів в медицині [131], а також Положенням про захист прав та конфіденційність пацієнта [132] також визначено норми, відповідно до яких національні медичні асоціації повинні використовувати всі можливі заходи для забезпечення таємниці, захищеності і конфіденційності інформації, яка стосується їх пацієнтів і зберігається в інформаційних системах. Вартою уваги є і Декларація про політику в галузі забезпечення прав пацієнта в Європі, якою визначено перелік інформації, що є конфіденційною – вся інформація про стан здоров'я пацієнта, діагноз,

прогнози та лікування його захворювання, а також будь-яка інша інформація особистого характеру повинна зберігатися в секреті, навіть після смерті пацієнта» (п. 4.1); містить вказівку на обов'язковість згоди пацієнта на розкриття інформації; встановлює можливість прийняття на національному законодавчому рівні винятків розголошення інформації без згоди (п. 4.2); захищає особисті дані пацієнта (п. 4.3) [33; 141].

Останнім часом МІС займають центральне місце у забезпеченні організації охорони здоров'я. Впровадження та подальший розвиток МІС сприятиме: покращенню ефективності надання та доступності медичних послуг; підвищенню якості процесу лікування; оптимізації діяльності працівників медичної сфери; розробленню та упровадженню стандартів щодо збору, обміну та зберігання медичної інформації; розробленню нових пропозицій та ініціатив за результатами проведення аналізу архівних матеріалів науковцями [275, с. 1589; 140; 141].

Акцентуємо увагу на тому, що даний напрям активно підтримується і проєктами Європейського Союзу (для прикладу, програма «Єдиний цифровий ринок», основна мета якої – реалізація безпечного доступу та транскордонного обміну медичними даними, яке орієнтовано на пацієнта. Серед інших програм розвитку ЕСОЗ в країнах ЄС – «Third EU Health Programme» (2014-2020 рр.), «Horizon 2020» та «Structural and Investment funds» [123].

«Цифрова трансформація сфери охорони здоров'я, на думку науковців (О. Трофименко, Я. Дубовой, Н. Логінова, Ю. Прокоп, О. Задерейко), за умов пандемії COVID-19, дозволила надавати медичні послуги дистанційно та передавати медичні дані між пацієнтами та постачальниками медичних послуг засобами мережі Інтернет. При цьому в комп'ютерних системах формуються і циркулюють величезні обсяги «чутливих» даних про пацієнтів, медпрацівників …. Це утворює вразливе середовище щодо кібератак, які можуть стосуватися несанкціонованого доступу, можливих витоків, викрадення або взагалі втрати особистих даних. При цьому не виключені ситуації заволодіння

кіберзловмисниками дистанційним контролем над комп'ютерними системами, їх пошкодження або недоступності, що може спричинити серйозні наслідки [237].

Медична інформаційна система (далі – МІС) – це спеціально розроблене для медичної сфери програмне забезпечення. Функціоналом МІС передбачено автоматизацію документообігу (заповнення медичних карток, дані діагностики та лікування пацієнта, фінансова звітність тощо). На відміну від інших інформаційних систем у МІС одночасно може зберігатися та оброблятися особиста, демографічна та медична інформація про пацієнта.

Крім того, функціоналом МІС передбачено взаємодію з eHealth та Національною службою здоров'я України. Також передбачено можливість щодо автоматизації процесів (реєстрація та систематизація інформації, відомості про медичні служби та персонал, черги на місця у стаціонарі, відслідковування руху лікарських засобів на складах та безпосередньо між відділеннями, оптимізація роботи діагностичних кабінетів, передача інформації про результати досліджень іншим фахівцям, збір статистика, звіти та аналітичні довідки [140].

Як правило, розробниками таких систем є або юридичні особи, або фізичні особи-підприємці, які пройшли перевірку на сумісність з Центральною базою даних, підписали договір з адміністратором бази даних (держпідприємством «Електронне здоров’я») і відповідають технічним вимогам. Найбільш відомими серед них є Helsi, Medcard24, Moniheal, Health24 та інші.

Функціонал бази даних передбачає, що при підключенні медичних інформаційних систем до них, вони отримують доступ до реєстрів. Однак можливість обробки інформації про конкретну особу можливе лише за умови надання згоди цієї особи. Тобто для реєстрації в МІС користувач має прийняти угоду між користувачем і системою та надати згоду на обробку своїх персональних даних.

На сьогодні над розробкою МІС в Україні працює багато компаній, деякі з них спеціалізуються у даному напрямі уже понад 15 років. Наказом Національної

служби здоров’я України від 05.11.2021 № 527 «Про внесення змін наказу Національної служби здоров’я України від 06.02.2019 № 28» затверджено технічні вимоги до електронних МІС у частині щодо її підключення до центральної бази даних ЕСОЗ [232; 140].

Варто зазначити, що всі МІС збирають приблизно однакові категорії даних, проте формулювання в угодах щодо збору цих даних можуть суттєво відрізнятися. Наприклад, Helsi збирає як загальні дані про особу (ім'я, адреса проживання, паспортні дані тощо), так і чутливі дані про стан здоров’я. Medcard24 також збирає загальні дані, але конкретизація їх типу відсутня, і посилання є на Закон «Про захист персональних даних». Водночас у положеннях цієї системи зазначено, що сервіс збирає дані, що містять лікарську таємницю, такі як факт звернення до лікаря, медичні послуги, препарати, які необхідні чи можуть бути необхідні для пацієнта. У положеннях про Health24 визначено, що збираються лише загальні дані, тоді як інформація про медичні дані відсутня. В угоді Asker зазначено, що МІС «збирає дані, щоб ефективно керувати своїми продуктами та надавати вам найкращі можливості для роботи з ними. Деякі дані ви надаєте напряму, наприклад, коли створюєте обліковий запис в системі Аскеп, адмініструєте обліковий запис, надсилаєте на eHealth інформацію про заклад, лікаря, пацієнта, декларації» [18; 141]. Як бачимо, зазначене не свідчить про належне інформуванням користувачів про зміст і склад даних, які збираються.

З огляду на наведену інформацію, пропонується, щоб при введенні в дію МІС та медичних сервісів на законодавчому рівні було обов’язковим ознайомлення користувачів з умовами угоди або положенням про відповідну систему перед реєстрацією. Це повинно включати чітке визначення інформації, яку система збирає, обробляє та використовує стосовно користувача. Крім того, користувачі повинні бути детально ознайомлені з порядком захисту зібраної інформації, що стосується їх особистих даних.

Наявні проблеми також виникають при наданні доступу до медичних даних третім особам. Наприклад, у положенні про медичну систему Moniheal зазначено, що система має право розкривати певні персональні дані не лише органам слідства, прокуратури, суду та іншим законодавчо визначеним органам, але і за вимогою «посадових осіб будь-якого державного органу» або в випадках, коли система вважає розкриття необхідним для запобігання шкоді здоров'ю чи фінансовим збиткам [18].

Таке положення суперечить як чинному національному законодавству, так і усталеній практиці Європейського суду з прав людини. Зокрема, у справі «Gardel v. France» ЄСПЛ чітко визначив, що доступ до персональних даних у державних реєстрах можливий виключно для публічних службовців, які зобов’язані забезпечувати конфіденційність інформації. Будь-які інші особи не мають права на такий доступ. Крім того, використання інформації повинно відбуватися лише на законних підставах, зокрема для проведення слідчих дій, захисту населення або забезпечення національної безпеки [141].

Окрім зазначеного, в Україні упроваджено Портал ЕСОЗ (онлайн-платформа для медичного обслуговування, основними функціями якої є: планування походу до лікаря; доступ пацієнтів до медичної інформації (дана функція має зашифрований і захищений паролем вхід, історію здоров’я, результати лабораторних тестів, звіти про виписку, лікування); конфіденційне спілкування між лікарем і пацієнтом (завдяки цій функції обмін повідомленнями між лікарем і пацієнтом, відеоконсультації та опитування пацієнтів після візиту є безпечними); управління оплатою та страхуванням пацієнтів [248].

Також серед веб-порталів, пов'язаних з медициною, варто виокремити медичні веб-портали: «Itmed» (інтерактивний інструмент для пошуку медичних закладів, лікарів, медтехніки, комерційних компаній та аптек; запису на прийом до лікаря) [106]; «Портал пацієнта» (пошук медиків та медичних закладів, перевірка можливості отримання безкоштовної вакцини від Covid-19. Зазначений портал

забезпечує надійний захист ПД та конфіденційної медичної інформації) [143]; «HELSI.ME» (електронна медична платформа, створена для пацієнтів, лікарів, державних та приватних закладів охорони здоров'я. Портал забезпечує надійне шифрування та безпеку особистих даних пацієнтів. Helsi забезпечує надійний захист даних пацієнтів, що зберігаються у їхньому дата-центрі, який сертифікований як комплексна система захисту інформації Державною службою спеціального зв'язку та захисту інформації України [154] та інші).

Таким чином, основними перевагами подальшої цифровізації медичної сфери є: доступність та ефективність надання медичних послуг; можливість технічної і консультативної підтримки, що сприятиме підвищенню ефективності якості надання медичних послуг.

Проте, упровадження МІС має і свої ризики, адже через кібератаку медична інформація може опинитися у вільному доступі, навмисний злив чи помилки лікарів або самих медичних сервісів. «Цифрові системи охорони здоров'я еволюціонували на вершині хмарних платформ, технологій IoT, мобільних обчислень, штучного інтелекту та машинного навчання для медичної аналітики. Хоча такі інформаційні системи формують майбутнє загальнодоступної та інтелектуальної охорони здоров'я, конфіденційність пацієнтів, лікарів, медсестер та постачальників медичних послуг сьогодні викликає велике занепокоєння» [237].

Зазначимо, що поняття «загроза» в інформаційній безпеці – це «будь-хто або будь-що, що підпадає під небезпеку будь-яких негативних впливів у сфері інформаційної діяльності» [87]. Відповідно до Стратегії інформаційної безпеки, дефініція «інформаційна загроза» – це потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [224].

Акцентуємо увагу на тому, що інформаційні загрози можуть бути як внутрішніми (відбувається за умови недостатньої кваліфікованості, розуміння процесів і наслідків), так і зовнішніми. А.В. Погребняк класифікує інформаційні загрози на випадкові та навмисні. До випадкових загроз відносяться помилки адміністраторів і користувачів, втрата інформації через неправильне збереження, випадкове знищення або заміна даних, збій в електроживленні або в комплектуючих елементах мережі, а також некоректна робота програмного забезпечення, зокрема через комп'ютерні віруси. Навмисні загрози включають несанкціонований доступ до інформації та мережевих ресурсів, розкриття і модифікацію даних, їх копіювання, розробку і поширення вірусів, крадіжку магнітних носіїв, а також руйнування або навмисне знищення архівної інформації [130, с. 46-50].

Класифікація загроз інформаційній безпеці може бути здійснена за кількома ознаками: за природою виникнення, де можливі як природні, так і штучні загрози; за ступенем навмисності загрози, що включає випадкові загрози, такі як помилки адміністраторів або технічні збої, а також навмисні загрози, наприклад, зловмисні атаки або крадіжка даних; залежно від джерела загрози, яке може бути пов’язане з людиною, санкціонованими програмними або апаратними засобами, а також несанкціонованими програмними чи апаратними засобами; за місцем розташування джерела загрози, де загрози можуть виходити ззовні контрольованої зони або зсередини цієї зони; за впливом на інформаційні системи, де загрози можуть бути пасивними (не впливають на роботу системи безпосередньо) або активними (викликають прямі зміни або порушення); за способом доступу до ресурсів інформаційних систем, де загрози можуть використовувати стандартні методи доступу або нестандартні підходи [40].

Стратегією кібербезпеки України визначено, що *інформаційні загрози актуалізуються через вплив таких факторів: невідповідність інфраструктури електронних комунікацій сучасним вимогам щодо її розвитку та захищеності;*

недостатній рівень захищеності критичної інформаційної інфраструктури, державних електронних інформаційних ресурсів та інформації, захист якої передбачено законом, від кіберзагроз; безсистемність заходів кіберзахисту; недостатній розвиток організаційно-технічної інфраструктури забезпечення кібербезпеки як для критичної інформаційної інфраструктури, так і для державних та приватних електронних інформаційних ресурсів; недостатній рівень координації, взаємодії та інформаційного обміну між суб'єктами забезпечення захисту інформації та кібербезпеки [183].

Політика інформаційної безпеки медичних закладів включає в себе наступні етапи: аналіз об'єкту захисту (дослідження фізичного середовища об'єкта, інформаційного середовища та середовища користувачів); ідентифікація цінних активів (дослідження ресурсів об'єкта захисту. Так, відповідно до ДСТУ ISO/IEC 27005:2019, активи організації поділяються на: інформацію, апаратно-програмний комплекс, носії інформації, мережа, користувачі); аналіз загроз для досліджуваного об'єкту (ідентифікація загроз проводиться за допомогою експертного підходу.

За даними статистичних досліджень, серед найпоширеніших загроз для медичних закладів виділяють: умисні зловмисні дії, помилки персоналу, технічні збої в інформаційних системах та пошкодження мережевої інфраструктури. Процес оцінки ризиків повинен здійснюватися відповідно до стандарту ДСТУ ISO/IEC 27001:2013 [38], базуючись на інформації, зібраній із зазначених джерел. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» (п. 2 ст. 6), медичні установи відносяться до категорії об'єктів критичної інфраструктури. У зв'язку з цим їх політика захисту інформації має відповідати вимогам постанови Кабінету Міністрів України № 518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» [162; 258].

На сьогодні тенденція щодо збільшення кібератак на інфраструктуру, у тому числі і медичні заклади, продовжується як в Україні, так і за кордоном. Для прикладу, Секретаріатом уповноваженого перевірок ДП «Електронне здоров'я»

(адміністратор ЦБД НСЗУ) за результатами проведених перевірок 4 МІС та 3 медичних закладів з питань додержання прав на приватність інформації, встановлено ризики як щодо обробки ПД, так і функціонування ЕСОЗ [140].

Слушною у контексті досліджуваного є думка представника уповноваженого у сфері захисту ПД І. Берназюк про те, що найбільшою загрозою щодо безпеки МІС є значний обсяг медичної інформації, яку зберігають, як правило, в одній системі та розміщують територіально в одному місці. Як наслідок, лише одна кібератака може «знищити» повністю базу даних. Наступним проблемним питанням у частині, що стосується витоку та незаконного використання медичної інформації, є низький рівень технічного захисту ЕСОЗ ЦБД та МІС [17; 140].

На наш погляд, вартим уваги є позитивний досвід Естонії, де медичну інформацію зберігають у кількох базах даних, які територіально віддалені, мають різні сервери з індивідуальною системою захисту. Це дійсно важливо, адже ми говоримо про персональні чутливі дані (діагнози, обстеження, діагностику, медичні призначення, листи непрацездатності тощо) [17].

Наступною загрозою є відсутність державного контролю щодо діяльності приватних компаній (операторів МІС). Для прикладу, МІС здійснюється обмін інформацією з центральною базою через сервери операторів МІС («хмарні» МІС), при цьому інформація про пацієнтів зберігається на серверах операторів МІС, які є суб'єктами приватної власності та на які МОЗ не впливає [140].

Як зазначає І. Козаченко, член Української академії кібербезпеки та незалежний експерт з питань інформаційної безпеки і протидії кіберзагрозам, персональні «чутливі» дані не повинні зберігатися на комерційних серверах без атестату відповідності вимогам захисту інформації, затвердженим КСЗІ. Така інформація може бути здобута злочинним шляхом (передана чи придбана) третіми особами. Оскільки медицина є частиною критичної інфраструктури, будь-яке втручання в інформаційну медичну систему може мати серйозні наслідки,

включаючи потенційну зупинку всієї апаратури в разі кібератаки на медичний заклад [104].

Зважаючи на це пропонуємо розробити дієвий алгоритм забезпечення контролю з боку держави щодо дотримання операторами МІС, які підключені до ЦБД, норм щодо ТЗІ медичного характеру [140].

Також, є питання і щодо відповідності міжнародним стандартам ТЗІ Електронного реєстру відомостей про генетичні ознаки людини – підсистеми єдиної ІС Міністерства внутрішніх справ України (далі – МВС України). На думку V. Marchese, N. Cerri та L. Caenazzo, незважаючи на цінність баз ДНК, основною метою держави є саме «визначення балансу» між суспільним інтересом (боротьба із злочинністю) та особистими правами (конфіденційність приватної інформації), що може бути проблемою [269]. Важлива роль у частині щодо захисту інформації в ІС належить адміністраторам. Зазначимо, що відповідно до наказу МВС України від 31.01.2018 р. № 70 «Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України», нагляд та контроль забезпечується Департаментом інформатизації МВС України.

Однак, незважаючи на значні позитивні зрушення у напрямі запровадження новітніх інформаційних технологій у даному напрямі діяльності, ефективність забезпечення інформаційної безпеки «чутливої» інформації, – на думку О.В. Легкої, – бажає чекати кращого. Адже сучасні системи безпеки мають високі характеристики тільки в окремих напрямах забезпечення безпеки. Крім того, варто наголосити, що вирішення даної проблеми шляхом створення на кожну інформаційну систему власної системи безпеки не є ефективним та не забезпечує можливості практичної реалізації на всіх рівнях. Ми притримуємося думки правознавців та практиків щодо необхідності інтеграції окремих інформаційних систем та систем безпеки [93].

Також варто акцентувати увагу і на той факт, що у зв’язку із військовою агресією Російської Федерації мільйони громадян України переміщені, органам

влади необхідно буде звертатись до сімей зниклих безвісти осіб у різних куточках України та за її межами. Пунктом 2 ст. 17 Закону України «Про державну реєстрацію геномної інформації людини» від 09.07.2022 № 2391-IX визначено, що надання органам іноземних держав геномної інформації, отриманої згідно із цим Законом, можливе лише у разі, якщо ці органи та відповідний компетентний орган України можуть установити такий режим доступу до інформації, який унеможливлює розкриття інформації для інших цілей чи її розголошення в будь-який спосіб, у тому числі шляхом несанкціонованого доступу [126; 93].

Таким чином, до основних проблем у захисті медичної інформації слід віднести: недостатній рівень комп'ютерної грамотності медичних працівників і відсутність ІТ-відділу в медичних закладах; технічні характеристики комп'ютерного обладнання, яке в переважній більшості випадків не відповідає встановленим вимогам; наявність випадків, коли медичний заклад впроваджує медичну інформаційну систему, функціонал якої не відповідає міжнародним стандартам. Як результат, замість підвищення ефективності у цьому напрямі спостерігається прямо протилежний ефект [140].

Також зазначимо, що при виборі МІС важливо не лише тестування на відповідність вимогам МОЗ, але і відповідність стандартам з ТЗІ. Як бачимо, підключенню до центрального компоненту eHealth підлягають ті МІС, які успішно верифіковано та якими отримано позитивні висновки. Як приклад, МІС ЕМСІМЕД, якою пройдено перевірки та всі її модулі підключені до центральної бази даних урядової інформаційної системи.

Впровадження правового режиму воєнного стану в Україні внесло суттєві корективи у сферу захисту інформації, зокрема в медичній галузі. В умовах воєнного стану акцент у виявленні та протидії інформаційним загрозам зміщується в бік обмеження окремих прав людини з метою забезпечення реагування на потенційні та наявні ризики [87].

Указом Президента України «Про введення воєнного стану в Україні» від 24.02.2023 № 64/2022 передбачено, що під час дії воєнного стану можуть тимчасово обмежуватися конституційні права і свободи, передбачені статтями 30–34, 38, 39, 41–44 та 53 Конституції України. Серед них – і норми, що регулюють інформаційні права громадян. У контексті захисту чутливої медичної інформації особливу увагу слід приділяти статті 32 Конституції України, яка гарантує недоторканність особистого і сімейного життя, дозволяючи втручання лише у випадках, передбачених Конституцією [78].

Такі тимчасові обмеження зумовлені необхідністю адаптації правового механізму захисту інформації до реалій ведення бойових дій та окупованих територій, де неможливо забезпечити повне виконання конституційних гарантій.

Що стосується вимог, передбачених Законом України «Про захист інформації в інформаційно-комунікаційних системах», то під час введення в країні правового режиму воєнного стану, вони не змінюються. Інформаційні системи, в яких обробляється та зберігається інформація з обмеженим доступом, функціонують за умови застосування комплексної системи захисту інформації з підтвердженою відповідністю. Підтвердження відповідності КСЗІ здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог і норм інформаційної безпеки у порядку, встановленому законодавством. Для захисту інформаційних систем, в яких не обробляється інформація з обмеженим доступом, але захист яких вимагає українське законодавство, може бути також використана альтернативна система інформаційної безпеки відповідно до європейських стандартів ISO/IEC27.

Якщо інформаційну систему перенесено до хмарного сервісу, системи захисту мають бути переглянуті та модернізовані, якщо була змінена технологія оброблення інформації в ІКС або програмно-апаратному чи програмному складі ІКС тощо. Функціонування інформаційної системи без атестата відповідності КСЗІ або сертифіката відповідно до стандартів ISO/IEC27 заборонено [19].

Відповідальність за забезпечення захисту інформації в інформаційній системі покладено на власника системи.

Адміністрування Центральної бази даних (ЦБД) електронної системи охорони здоров'я (ЕСОЗ) України здійснює Державне підприємство «Електронне здоров'я», відповідно до Порядку функціонування ЕСОЗ, затвердженого постановою Кабінету Міністрів України від 25.04.2018 № 411.

У зв'язку з виявленням серйозних порушень вимог щодо захисту інформації операторами електронних медичних інформаційних систем (МІС), 01 червня 2022 року адміністратор ЦБД прийняв рішення про тимчасове відключення частини електронних МІС від ЦБД ЕСОЗ. До переліку відключених систем, станом на 30 липня 2022 року, увійшли: Ademrius (ТОВ «Адемріус»), простоМед (ТОВ МІС-сервіс), Apteka24 (ТОВ МІС-сервіс), ePrisonHealth (Центр охорони здоров'я державної кримінально-виконавчої служби України), Hernes-medical (ТОВ НВФ «ГЕРМЕС-КОМП»), Iconx CRM (ФОП Чернов Михайло Петрович), Medcore (ТОВ МЕДКОР), Медікіт (ТОВ МЕДІКІТ), MoniHeal (ТОВ «Моі Здоров'я»), Нейрон (ТОВ АЛЮР), Парацельс (ФОП Харченко Лариса Геннадіївна), Prolisok (ТОВ «ПРОЛІСОК АІ»), Selenium (ФОП Стоянов Л.А.), UASMART (ТОВ ЮАСМАРТ) та Цифровий пацієнт (ТОВ «Центр сучасних інформаційних технологій «БРАВО»») [253].

Такі дії адміністратора спрямовані на забезпечення безпеки та цілісності медичних даних, оскільки порушення норм захисту інформації може становити загрозу правам пацієнтів і безпеці національної електронної медичної інфраструктури.

Не менше проблем виникає і внаслідок порушення встановленого порядку реєстрації та автентифікації користувачів МІС. Внаслідок правової неграмотності, а інколи й просто нерозуміння наслідків витоку персональної чутливої інформації, користувачі розголошують логіни та паролі стороннім особам. Мають також місце непоодинокі факти, коли лікарі при реєстрації пацієнта помилково вносять в МІС

інформацію про іншу особу. Для прикладу, у 2021 році під час входу в систему HELSI один із юристів юридичної компанія Legal Support у особистому акаунті побачив персональні дані про зовсім іншу людину [107]. Це сталося внаслідок внесення лікарями під час реєстрації пацієнта помилкових даних .

Зазначене свідчить про необхідність удосконалення правового регулювання з питань автентифікації користувачів у МІС. Вартим уваги у даному напрямі є позитивний досвід Естонії, де доступ до МІС здійснюється виключно за ідентифікатором особи (персональним ID-паспортом), що зводить до мінімуму можливість зазначених вище помилок.

Перебування України в умовах правового режиму воєнного стану висвітлило значні прогалини як у теоретичному, так і практичному законодавчому забезпеченні сфери охорони здоров'я. Ці обставини стимулювали внесення змін до нормативно-правових актів, спрямованих на адаптацію до реалій війни. Зокрема, було урегульовано такі питання: обмеження поширення окремих видів інформації з огляду на її суспільно-небезпечний характер; забезпечення технічного фіксування та збереження даних у воєнних умовах; встановлення й посилення відповідальності за незаконне розповсюдження або витік інформації; регламентація алгоритмів процесуальних дій щодо вилучення інформаційних даних.

Аналізуючи наведене, можна виокремити основні передумови та чинники формування інформаційних загроз у сфері охорони здоров'я:

– значна технологічна залежність України від іноземних постачальників продукції інформаційно-комунікаційних технологій та відсутність системи оцінки її відповідності стандартам технічної безпеки;

– недосконаліть нормативно-правового регулювання, уповільнена імплементація положень європейського законодавства та недостатній рівень юридичної відповідальності за порушення вимог у цій сфері;

– відсутність належного контролю щодо захисту медичної інформації у медичній сфері (багатофакторна автентифікація користувачів, контроль доступу, застосування ефективних криптографічних схем шифрування);

– низький рівень захисту державних інформаційних ресурсів, проблематика щодо вразливості до кібератак хмарних середовищ;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації адміністраторів та користувачів МІС;

– відсутність системи підвищення цифрової грамотності у сфері охорони здоров'я.

Отже, гарантування інформаційної безпеки у медичній сфері передбачає формування єдиного механізму, який поєднує інформаційні обмеження та захист прав і свобод громадян. Підтримуючи позицію І.Б. Котерліна, можна виділити три ключові компоненти ефективної системи інформаційної безпеки:

– технічний компонент, що охоплює розробку, впровадження та функціонування всіх необхідних технічних елементів системи, включно із засобами шифрування, контролю доступу та моніторингу;

– політичний компонент, який передбачає спрямування державної політики на забезпечення належного рівня інформаційної безпеки та координацію з іншими державними стратегіями;

– правовий компонент, що забезпечує наявність узгоджених і дієвих нормативно-правових актів, які регламентують обробку, збереження та захист інформації [87].

Технічний захист медичних інформаційних систем повинен будуватися на комплексному підході, що передбачає інтеграцію всіх заходів і засобів захисту інформації на кожному рівні системи інформаційного забезпечення, формуючи єдиний захищений комплекс.

2.4. Проблеми та перспективи удосконалення правового забезпечення захисту інформації у сфері охорони здоров'я

З 2017 року в Україні триває реформування медичної сфери, важливим інструментом якої є інформатизація (Е-здоров'я), основними принципами якого є: *орієнтованість на пацієнта* (накопичування та зберігання інформації, яка прив'язана до облікових записів пацієнта в медичній інформаційній системі, забезпечення можливості пацієнтові управляти особистими медичними відомостями, мати доступ до них); *пріоритетом є електронна форма* (надання пріоритету при накопиченні, обміні та зберіганні інформації електронній формі, яка оброблятиметься за допомогою ІКТ); *багаторазове використання інформації* (при потребі можливо неодноразово користуватися даними, наявними у МІС); є*диний медичний інформаційний простір (*інтеграція між системами як на рівні України, так і на міждержавному рівні).

Разом з тим, відповідно до Концепції розвитку цифрових компетентностей від 03.03.2021 № 167-р [83], інформатизація у медичній сфері повинна здійснюватися з дотриманням вимог вітчизняного законодавства України щодо захисту ПД та Генерального регламенту ЄС із захисту персональних даних (General Data Protection Regulation (EU) 2016/679, GDPR), міжнародних стандартів ISO/IEC, інших міжнародних документів та вимог в цій сфері. Особливо варто звернути увагу на дотримання принципу визначення мети, а також мінімізації інформації (забезпечується збір та обробка лише необхідних для реалізації відомостей) [79].

Концепцією розвитку цифрової економіки та суспільства України (сьомий принцип цифровізації) закріплено підвищення рівня довіри і безпеки, який означає, що інформаційна безпека, кібербезпека, захист ПД, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у

кіберпросторі є передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками [185].

Проте, на жаль, на сьогодні у даному напрямі прослідковуються певні проблемні питання. Зокрема, Концепцією розвитку електронного урядування в Україні, схваленою розпорядженням Кабінету Міністрів України від 20.09.2017 № 649, однією із першочергових проблем, що демонструє значне відставання України від світових темпів розвитку електронного урядування та такої, що потребує удосконалення державної політики у цій сфері, спрямованої на її першочергове розв'язання, визначено недостатній рівень інформаційної безпеки та захисту інформації в ІТС [184].

Сутність правового механізму забезпечення інформаційної безпеки особи в медичній сфері полягає у тому, що держава, застосовуючи систему правових інструментів, впорядковує суспільні відносини в цій галузі, надає їм юридичного закріплення та забезпечує їх охорону.

Механізм правового забезпечення у сфері охорони здоров'я формується через комплекс правових засобів та регуляторних актів; у період 2017–2020 років було ухвалено ключові нормативні документи, зокрема Закон України «Про державні фінансові гарантії медичного обслуговування населення», постанову Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» від 25.04.2018 № 411 [35], а також низку підзаконних актів, що визначають електронну систему охорони здоров'я та цифрові інструменти як основні засоби розвитку медичної сфери. До числа цифрових інструментів належать: електронна система охорони здоров'я (ЕСОЗ), що забезпечує централізоване зберігання медичних даних, контроль доступу та моніторинг обробки персональної інформації пацієнтів; електронні медичні карти та декларації, які дозволяють документувати стан здоров'я і лікувальні заходи у структурованій формі з дотриманням конфіденційності; цифрові засоби автентифікації та електронного підпису, що гарантують достовірність наданих медичних даних та підтверджують згоду

пацієнта на обробку його персональної інформації; а також системи шифрування та контролю доступу, які обмежують коло осіб, уповноважених працювати з чутливою медичною інформацією, відповідно до принципів GDPR та національного законодавства [35; 38; 162; 258].

Використання таких цифрових інструментів дозволяє реалізувати принципи законності, цілісності та конфіденційності даних у медичній сфері, підвищуючи рівень захисту прав пацієнтів та інтегруючи національну практику у європейські стандарти інформаційної безпеки.

Разом з тим, як зазначено у Концепції інформатизації охорони здоров'я України, рівень цифровізації, у тому числі і упровадження медичних інформаційних систем, у медичній сфері залишається низьким (несумісність інформаційних систем, недосконалість інформаційної інфраструктури та, відповідно, інтеграції між реєстрами, низький управлінський рівень фахівців у даному напрямі, відсутність належного технічного забезпечення (техніка та мережеве обладнання) [79].

На жаль, наразі немає єдності серед дослідників і нормотворців щодо шляхів якісної трансформації інформаційного законодавства України. Це зрозуміло, враховуючи складність, динаміку та масштабність сучасних інформаційних процесів, що відбуваються в умовах формування національної правової системи [117, с. 252].

Суттєвими викликами стали також пандемія та повномасштабне вторгнення РФ на територію України. Саме тому подальше упровадження державної політики України щодо подальшої інформатизації медичної сфери потребує суттєвих змін у вітчизняному законодавстві, яке повинно відповідати вимогам європейських та міжнародних стандартів, потребам сучасності. Адже охорона відомостей особистого характеру (особливо медичних даних) має основоположне значення для здійснення права на повагу до приватного і сімейного життя. Дотримання

конфіденційності відомостей про здоров'я є основним принципом правової системи усіх держав – учасниць Конвенції (справа «М. С. проти Швеції», 1997) [228].

Для ефективного подальшого розвитку та функціонування дієвої системи ЕСОЗ в Україні, необхідна надійна система захисту інформації. З цією метою, відповідно до Концепції розвитку електронної охорони здоров'я від 28.12.2020 № 1671-р, потребують негайного законодавчого урегулювання у частині, що стосується інформаційної безпеки системи ЕСОЗ, наступні напрями:

– удосконалення підходів щодо електронної ідентифікації, автентифікації користувачів ЕСОЗ, а також стандартів обміну інформацією у медичній сфері, порядків ведення реєстрів у центральній базі даних ЕСОЗ, ведення медичної документації, функціонування медичної статистики тощо;

– визначення вимог щодо розроблення медичних систем, реєстрів, сервісів ЕСОЗ, контролю за якістю розробленого функціоналу;

– урегулювання питання щодо доступу суб'єктів надання адміністративних та інших послуг до відомостей щодо стану здоров'я клієнта з урахуванням законодавчих норм щодо захисту інформації та персональних даних;

– забезпечення інтеграції та електронної взаємодії ЕСОЗ з іншими інформаційно-комунікаційними системами;

– урегулювання питання щодо оброблення ПД, які відносяться до категорії «чутливих», їх повторного знеособленого використання з метою статистичних чи наукових досліджень, або з іншою метою, не пов'язаною з наданням медичної допомоги;

– норми щодо ТЗІ, удосконалення механізму підтвердження відповідності систем захисту інформації у ІТС у складі ЕСОЗ, забезпечення відповідних робіт щодо створення систем захисту інформації, а також відповідної їх експертизи у порядку, визначеному МОЗ;

– гармонізація національних стандартів з міжнародними стандартами та класифікаторами, щоб забезпечити інтеграцію України у світовий інформаційний

простір. Це включає впровадження міжнародно визнаних стандартів, таких як Міжнародна статистична класифікація хвороб і споріднених проблем охорони здоров'я, Міжнародна класифікація функціонування, обмеження життєдіяльності і здоров'я, Міжнародна класифікація первинної допомоги, Австралійський класифікатор медичних інтервенцій (ACHI), систематизована медична номенклатура клінічних термінів (SNOMED), найменування та коди ідентифікаторів логічних спостережень (LOINC), міжнародні технічні стандарти обміну даних FHIR та ISO/IEC, оригінальний класифікатор МНН, АТХ (ATC)-код, та ТАС (форми випуску лікарських засобів) [82].

На наш погляд, правове забезпечення інформаційної безпеки у медичній сфері повинно відповідати вимогам щодо створення єдиного надійно захищеного медичного інформаційного простору в Україні, до якого повинні входити галузеві та регіональні бази даних, системи медико-статистичної інформації та аналіз.

Зважаючи на це, пропонуємо удосконалення правового забезпечення інформаційної безпеки у медичній сфері проводити за наступними напрямами:

– перший – систематизація законодавства;

– другий – удосконалення вимог щодо програмного забезпечення, сертифікації, ТЗІ та вимог щодо забезпечення медичних закладів комп'ютерним устаткуванням, яке відповідає вимогам міжнародних стандартів;

– третій – удосконалення питань щодо організаційного та кадрового забезпечення інформатизації медичної сфери (покращення рівня цифрової грамотності працівників медичної сфери (курси підвищення кваліфікації, семінари, круглі столи));

– четвертий – перехід до загальноприйнятих у міжнародній практиці методів збору, обробки та захисту інформації, а також подальший розвиток міжнародного співробітництва.

Інформатизація медичної сфери спрямована, перш за все, на забезпечення прав людини у сфері охорони здоров'я. Як зазначають дослідники, «права пацієнта в сучасному правовому вимірі супроводжуються суттєвими змінами, що проявляються у переході від патерналістського підходу до людиноцентричного розуміння» [251]. Одним із ключових елементів правового статусу пацієнта є забезпечення конфіденційності його даних. Саме тому захист персональної інформації пацієнтів становить фундаментальний принцип регулювання медичних відносин і є невід'ємною складовою ефективної системи охорони здоров'я.

В Україні правове регулювання права на приватність пацієнта стикається з кількома проблемами, які потребують вирішення. По-перше, відсутній спеціальний нормативний акт, що регулює права пацієнтів, а також єдиний підхід в законодавстві до розуміння принципу конфіденційності.

Також, на сьогодні не розроблено критеріїв щодо можливості встановлення винятків конфіденційності інформації про пацієнта. Окрему увагу необхідно приділити дітям, які мають особливий статус у правовідносинах дитина-пацієнт, так як мова йде про її фізичний та психологічний стан при наданні медичної допомоги. Преамбулою Декларації ООН прав дитини передбачено, що саме дитина, зважаючи на свою як фізичну, так і розумову незрілість, потребує спеціального правового захисту [152]. У науці права виділяють два види таких медичних інформаційних відносин: відносини щодо персональних даних дитини; відносини щодо захисту медичної (лікарської) таємниці стосовно дитини.

У даному контексті, на наш погляд, актуальною є наукова точка зору С. Булеци, який пропонує імплементувати європейський досвід щодо розподілу «чутливої» медичної інформації за критерієм чутливості: інформація загального значення (прізвище, ім'я, по батькові, дата та місце народження, громадянство, місце проживання); особисті персональні дані (стан фізичного та психічного здоров'я); етнічного походження, расової приналежності, ідентифікаційних кодів відбитків пальців і т.п.) [16, с. 58].

Наступним питанням, яке потребує подальшого доопрацювання, є питання щодо захисту інформаційного права особи під час обов’язкового медичного страхування, та, відповідно, обробки, зберігання та захисту «чутливої» інформації у даному напрямі. Так, відповідно до договору страхування, на випадок хвороби страхувальнику необхідно надати об’єктивну та ґрунтовну інформацію про стан свого здоров’я страховику, що, в окремих випадках, може призвести до порушення прав особи. Страховики, перевіряючи інформацію, можуть звертатися до медичних працівників, які законодавчо не мають права надавати дані про стан здоров'я пацієнта без його дозволу.

Слушною у даному контексті є наукова думка А. Загороднього, який звертає увагу на те, що запланований у подальшому перехід до обов’язкового медичного страхування призведе до необхідності надання страховим компаніям первинної медичної інформації про хід хвороби пацієнта та використання призначених медичних препаратів, що, як наслідок, збільшить обсяг інформаційної звітності та може сприяти виникненню проблем у сфері конфіденційності [49, с. 39].

Зважаючи на це, необхідно розробити та прийняти Закон України «Про загальнообов'язкове державне медичне соціальне страхування», у якому чітко окреслити:

– перелік інформації у розрізі даного напряму діяльності, яка відноситься до «чутливої» медичної інформації;

– перелік суб’єктів, які під час виконання службових повноважень, мають доступ до «чутливої» медичної інформації;

– вимоги щодо збору, обробки та зберігання «чутливої» медичної інформації;

– строки зберігання «чутливої» медичної інформації;

– заходи юридичного впливу у разі порушення встановлених вимог.

Проблематика інтеграції медичного страхування у систему державного соціального забезпечення в Україні досліджувалася законодавцем у кілька етапів. Так, у жовтні 2018 року Верховна Рада розглядала законопроєкт «Про

загальнообов’язкове державне медичне соціальне страхування в Україні», однак у серпні 2019 року його було відкликано. Нині регулювання цих питань здійснюється через Закон України «Основи законодавства України про загальнообов'язкове державне соціальне страхування», який у статті 4 визначає медичне страхування як окремий вид загальнообов’язкового державного соціального страхування, що забезпечує захист прав громадян у сфері охорони здоров’я.

Закон також встановлює ключові принципи функціонування системи загальнообов’язкового соціального страхування. Зокрема, стаття 5 передбачає гарантії реалізації застрахованими особами своїх прав, а стаття 13 регламентує порядок використання інформації про страхові випадки, страхову історію та результати медичних обстежень, підкреслюючи, що розголошення таких даних без письмової згоди застрахованої особи забороняється, за винятком випадків, прямо передбачених законодавством [120].

Крім того, внаслідок воєнної агресії РФ на території України наразі актуальним залишається питання щодо відповідності правового регулювання державної реєстрації геномної інформації людини міжнародним стандартам. Зазначимо, що Законом України «Про державну реєстрацію геномної інформації людини», який набув чинності у лютому 2023 року, визначено правові засади оброблення і реєстрації геномної інформації.

Геномна інформація – відомості щодо генетичних ознак людини (зразки ДНК), яку віднесено до категорії «чутливих» ПД. Даний вид інформації використовується для: ідентифікації осіб, які вчинили кримінальне правопорушення; розшуку осіб, які зникли безвісти; ідентифікації невпізнаних трупів людей, їх останків та частин тіла людини; ідентифікації осіб, які не здатні через стан здоров’я, вік або інші обставини повідомити інформацію про себе [126]. Геномна інформація вноситься до Електронного реєстру геномної інформації людини, держателем якого є Міністерство внутрішніх справ.

«Світовий досвід з ведення подібних обліків свідчить про доцільність створення єдиної бази даних ДНК, адже за таким принципом успішно ведуться бази даних ДНК в США, Великобританії, Польщі, Німеччині, Італії, Іспанії, Франції» [126; 93]. Відповідно до Прюмського договору 2005 року (підписаного Австрією, Бельгією, Іспанією, Люксембургом, Нідерландами, Німеччиною та Францією), державам-членам Європейського Союзу надано автоматичний доступ до генетичних баз даних, відбитків пальців і інформації про злочини, пов'язані з торгівлею наркотиками. Сьогодні автоматичний обмін даними ДНК здійснюється також між такими країнами: Австрія, Бельгія, Великобританія, Греція, Данія, Ірландія, Іспанія, Італія, Кіпр, Латвія, Литва, Люксембург, Мальта, Нідерланди, Польща, Португалія, Румунія, Словаччина, Словенія, Угорщина, Фінляндія, Франція та Швеція.

Проте, не зважаючи на той факт, що Закон України «Про державну реєстрацію геномної інформації людини» нещодавно набув чинності, у його окремих нормах прослідковується певна правова невизначеність щодо відповідності її міжнародним стандартам у частині, що стосується дотримання прав людини на інформацію.

Як зазначалося раніше, геномна інформація відноситься до категорії «чутливих медичних даних», обробка яких заборонена без належних гарантій. Відповідно до статті 6 Конвенції Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних, персональні дані не підлягають автоматизованій обробці, якщо національним законодавством не передбачено відповідного захисту.

Закон України «Про державну реєстрацію геномної інформації людини» встановлює, що інформація, яка міститься в Електронному реєстрі, відноситься до даних обмеженого доступу та не підлягає оприлюдненню (підпункт 5 статті 4). Перед внесенням до реєстру орган заповнює реєстраційну картку, у якій персональні дані знеособлюються шляхом присвоєння індивідуального буквено-

цифрового коду (пункт 2 статті 11). Дані, що зберігаються в Електронному реєстрі, не можуть передаватися або розкриватися стороннім особам і органам, не зазначеним у статті 16 цього Закону, за винятком випадків, передбачених законодавством (пункт 4 статті 16) [126].

Справедливим у цьому контексті є погляд О.В. Легкої, яка зазначає, що хоча Закон України «Про державну реєстрацію геномної інформації людини» формально передбачає обробку «чутливих» категорій персональних даних відповідно до підпунктів 1 та 7 частини 2 статті 7 Закону України «Про захист персональних даних», фактичні цілі збору та використання геномної інформації не відповідають цілям, визначеним цим Законом. Це створює умови для того, що Міністерство внутрішніх справ має можливість збирати обсяг даних, який перевищує необхідний для законних цілей [93, с. 74].

Крім того, Законом визначено, що геномна інформація – інформація про генетичні ознаки людини, як бачимо, законодавець вкладає у поняття досить широкий зміст (чітко не окреслено, які біологічні матеріали будуть збиратися), що, як наслідок, дозволяє збирати значний обсяг «чутливих» персональних даних.

Також, у зв’язку із тим, що право на використання інформації геномного змісту віднесено до широкого переліку суб’єктів (ст. 16 Закону), а терміни зберігання доволі тривалі, виникає потенційна загроза витоку інформації, відповідно порушуються права особи на захист інформації.

Згідно зі статтею 15 Закону України «Про державну реєстрацію геномної інформації людини», обробка геномної інформації здійснюється через автоматизовану систему формування та ведення Електронного реєстру, що забезпечує запобігання її втраті, пошкодженню, викривленню або несанкціонованому доступу (п. 2). Крім того, порядок обробки геномної інформації визначається держателем цього Електронного реєстру (п. 1), що формує правові рамки для організації безпечного та контрольованого обігу чутливих даних.

Разом з тим, Законом не передбачено гарантій попередження ризику втрати чи витоку такої інформації, не закріплено обов'язкове повідомлення особи володільцем про порушення безпеки ПД (дані норми передбачено лише з питань обміну відомостями геномного характеру з іншими міжнародними країнами).

Крім того, з урахуванням тривалого терміну зберігання геномної інформації, зазначеним Законом не конкретизовано питання щодо можливості її вилучення у зв'язку зі смертю особи, яка її надала (мінімізація ризику доступу до ПД родичів такої особи). Відсутні положення і про право особи з питань відкликання згоди на обробку геномної інформації особою, яка їх надала.

Відповідно до пункту 1 статті 19 Закону «Про державну реєстрацію геномної інформації людини», контроль за дотриманням прав людини у частині реєстрації геномної інформації покладено на Уповноваженого Верховної Ради України з прав людини [126]. Водночас, згідно з його службовими повноваженнями, він не має прямого впливу на діяльність Міністерства внутрішніх справ України. Таким чином, по-перше, законодавство не визначає конкретний алгоритм контролю за дотриманням норм при обробці геномних даних, а по-друге, відсутній незалежний наглядовий орган, який міг би здійснювати перевірки, надавати консультації та застосовувати санкції за порушення законодавства щодо захисту персональних даних [118].

Постає питання щодо ефективності технічного захисту Електронного реєстру даних про генетичні ознаки людини. Згідно з наказом МВС України від 31.01.2018 № 70 «Про затвердження Положення про Департамент інформатизації Міністерства внутрішніх справ України», адміністрування та контроль інформаційних систем покладено на Департамент інформатизації МВС. Водночас слід зауважити, що не всі інформаційні системи забезпечують належний рівень технічного захисту, що створює потенційні ризики для конфіденційності та цілісності чутливих даних. *Зважаючи на це, вважаємо за доцільне інтегрувати інформаційні системи та забезпечити їх технічний захист відповідно до норм міжнародних стандартів.*

Тим більше, що відповідно до п. 2 ст. 17 Закону України «Про державну реєстрацію геномної інформації людини», надання органам іноземних держав геномної інформації, отриманої згідно із цим Законом, можливе лише у разі, якщо ці органи та відповідний компетентний орган України можуть установити такий режим доступу до інформації, що гарантуватиме неможливість розкриття чи розголошення інформації з іншою метою та в інший спосіб [126].

Тобто Законом передбачено можливість обмінюватися інформацією геномного змісту з іншими міжнародними організаціями під час кримінального провадження, що сприятиме ефективності у розслідуванні воєнних злочинів, які вчинено на території України.

Крім того, як ми зазначали у попередніх підрозділах, потребують доповнення та внесення змін:

– через застарілість Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» 1994 року № 80/94-ВР та ряду нормативних актів щодо технічного захисту інформації (НД ТЗІ) необхідно оперативно оновити їх положення у відповідності до положень Загального регламенту ЄС про захист персональних даних (GDPR 2018/1725);

– створити незалежний наглядовий орган, який здійснюватиме контроль за дотриманням норм у сфері захисту персональних даних. Нині ці функції покладені на Уповноваженого Верховної Ради України з прав людини, проте його конституційний статус не передбачає повноцінного наглядового впливу. Повноваження нового органу мають відповідати вимогам, закріпленим у Загальному регламенті Європейського Парламенту і Ради (ЄС) 2016/679;

– законодавчо закріпити комплексні гарантії захисту персональних даних у медичній сфері;

– встановити законодавчий механізм контролю державних органів за діяльністю приватних операторів медичних інформаційних систем;

– прийняти зміни до Закону України «Про захист персональних даних» з урахуванням норм GDPR, зокрема щодо форм і умов надання згоди на обробку персональних даних. Нагадаємо, що у лютому 2020 року міжвідомча робоча група при Уповноваженому Верховної Ради України з прав людини розробила проєкт Закону № 2671-1, спрямований на деталізацію процедур надання згоди та врегулювання обробки персональних даних органами державної влади та місцевого самоврядування, однак у березні 2020 року цей проєкт було повернено на доопрацювання.

У жовтні 2022 року Р.О. Стефанчуком та іншими народними депутатами винесено на розгляд проєкт Закону України «Про внесення змін до Закону України «Про захист персональних даних» № 8153. Разом з тим, його норми, за висновком Міністерства юстиції України, не в повній мірі відповідають положенням Регламенту (ЄС) 2016/679 та Директиви 2002/58 Європейського Парламенту та Ради від 12 липня 2002 року стосовно обробки ПД та захисту конфіденційності у сфері електронних комунікацій [20], відповідно, потребують доопрацювання. Зокрема, у розрізі теми нашого дослідження, потребують доопрацювання:

а) визначення терміну «персональні дані» (ч. 1 ст. 2), так як воно не відповідає нормам Регламенту 2016/679;

б) розділ Х «Відповідальність за порушення законодавства у сфері захисту персональних даних», у якому «відсутні положення стосовно обставин, які мають враховуватися під час вирішення питання про вид та розмір відповідальності контролера або оператора. У зв'язку з цим, у проєкті Закону необхідно врахувати положення п. 1 ст. 83 Регламенту 2016/679, яка встановлює, що кожен наглядовий орган повинен забезпечити, щоб накладення адміністративних штрафів було ефективним, пропорційним і стримуючим, а також п. 2 ст. 83 Регламенту 2016/679, який передбачає перелік пом’якшуючих та обтяжуючих обставин, які мають бути враховані контролюючим органом;

в) п. 6 ч. 1 ст. 5 у частині трактування, що обробка персональних даних є законною у разі необхідності для цілей легітимного інтересу контролера або третьої особи, крім випадків, коли такі інтереси не переважають інтереси або основоположні права та свободи суб'єкта ПД, які вимагають захисту ПД, особливо якщо суб'єктом ПД є дитина. Легітимний інтерес контролера може полягати, зокрема, у обробці ПД для запобігання шахрайству, забезпечення інформаційної безпеки. Тобто обробка ПД без згоди суб'єкта ПД вважатиметься законною, якщо вона буде здійснюватися для цілей легітимного інтересу контролера або третьої особи. При цьому проєктом Закону не визначено, ким буде здійснюватися оцінка законних інтересів та надаватись за її результатом відповідний висновок [20];

г) п. 1 ч. 1 ст. 41 проєкту Закону передбачено, що контролер та оператор зобов'язані призначити відповідальну особу з питань захисту ПД, зокрема, у випадку, коли обробка ПД здійснюється суб'єктом владних повноважень. Проте ч.1 ст. 42 визначено, що суб'єкт владних повноважень може призначити особу на посаду відповідальної особи з питань захисту ПД лише у разі, якщо вона пройшла кваліфікаційний іспит та отримала відповідний сертифікат. Таке трактування суперечить Закону України «Про державну службу», так як призначення держслужбовців на посаду здійснюється за результатами конкурсу, разом з тим відповідних змін до вказаного Закону у проєкті Закону не передбачено.

– розробити та затвердити на законодавчому рівні алгоритм дій у разі відмови пацієнта надати згоду на обробку ПД.

Таким чином, якісна медична реформа можлива лише за умови впровадження сучасних методів інформатизації та, відповідно, захисту інформації. Як засвідчив аналіз, наразі в Україні система правового забезпечення захисту інформації у медичній сфері потребує негайного удосконалення. Адже саме «… якісний нормативний фундамент є запорукою належної правореалізації й правозастосування» [201].

Забезпечення права людини на медичну інформацію є важливим показником як демократичності держави, так і інтеграції національного права у світове співтовариство. Воно також повинно відповідати міжнародно-правовим стандартам.

Основними чинниками забезпечення інформаційної безпеки держави є:

– гарантування безпеки інформації загального доступу, мереж зв’язку, інформаційно-телекомунікаційних систем, технічних і програмних засобів для маніпуляцій з інформацією; забезпечення доступу до інформації;

– конфіденційність медичної інформації;

– захищеність особи, суспільства і держави від шкідливого впливу певних видів інформації, яка не є конфіденційною.

Висновки до розділу 2

1. Розвиток інформаційного суспільства невід'ємно пов'язаний з прогресом інформаційних технологій і забезпеченням прав людини. Право на здоров'я охоплює також право на інформацію та конфіденційність даних, що закріплено в ст. 8 Конвенції. Згідно з рішенням ЄСПЛ у справі «М.С. проти Швеції», конфіденційність інформації про здоров'я є основним принципом правової системи країн-учасниць. Отже, національне законодавство повинно забезпечувати нерозголошення інформації про стан здоров'я.

У зв’язку з істотними змінами, що відбуваються в рамках медичної реформи, виникає нагальна потреба у суттєвому перегляді чинного законодавства, що регулює правовий захист інформації у сфері охорони здоров’я. Охорона чутливих даних є не лише обов’язком держави та предметом державно-правового регулювання, але й невід’ємною складовою забезпечення прав людини. Крім того,

формування ефективної системи захисту персональних даних сприяє виконанню міжнародних зобов'язань України.

2. Ключовим нормативним документом, що визначає захист прав суб'єктів персональних даних та забезпечує конфіденційність інформації у медичній сфері, є Загальний регламент ЄС із захисту персональних даних (GDPR). Цей регламент передбачає передачу контролю та права володіння медичними даними безпосередньо пацієнтам замість медичних працівників та закладів охорони здоров'я. Одночасно порядок збору, обробки, надання та зберігання даних пацієнтів у відповідності до стандартів GDPR визначається Порядком функціонування електронної системи охорони здоров'я України.

3. Теоретично обґрунтовано, що незважаючи на те, що обробка персональних даних без надання згоди межує з порушенням фундаментальних прав та свобод людини, вітчизняне законодавство у виняткових випадках дозволяє обробку персональних даних. Так, здійснювати обробку персональних даних у медичній сфері без згоди особи, якої вони стосується, законно лише якщо вона проводиться в цілях охорони здоров'я встановленим колом осіб.

4. Встановлено, що за порушення законодавства у сфері охорони здоров'я щодо захисту інформації передбачено дисциплінарну, адміністративну, цивільно-правову та кримінальну відповідальність. Проведено аналіз ключових принципів та положень Загального регламенту ЄС із захисту персональних даних у частині медичної інформації. Обґрунтовано позицію, що право на охорону медичних даних виникає одночасно з виникненням самого суб'єктивного права, а не лише у момент його порушення. На підставі дослідження рішень Європейського суду з прав людини від 29.04.2017 (справа «Л.Х. проти Латвії», № 52019/07) та Верховного Суду України від 04.12.2019 (справа № 760/8719/17) зроблено висновок, що дискреційні повноваження державних органів щодо збору та обробки персональних даних повинні бути чітко визначені та регламентовані законом.

5. Звертається увага на те, що Закон України № 555-IX «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» у частині запобігання поширенню COVID-19» потребує більш точного визначення цілей обробки персональних даних. Зокрема, пропонується викласти пп. 1 п. 2 розділу II цього Закону у такій редакції: «дозволяється обробка персональних даних щодо стану здоров'я, місця перебування на госпіталізації або самоізоляції, прізвища, імені, по батькові, дати народження, місця проживання, роботи або навчання особи без її згоди, відповідно до встановленого рішенням про карантин порядку, за умови застосування належних технічних заходів захисту, використання даних виключно з метою запобігання поширенню COVID-19, а також за наявності обов'язку працівника, який безпосередньо здійснює обробку таких даних, щодо їх конфіденційності та нерозголошення».

6. Встановлено, що пандемія COVID-19 підкреслила низку нагальних проблем у сфері захисту медичної інформації. Виявлено прогалини у законодавчому врегулюванні дій медичних працівників у разі відмови пацієнтів від надання згоди на обробку персональних даних та внесення їх до електронного реєстру. Окреслено ключові проблеми, що виникають у процесі функціонування електронної системи охорони здоров'я, та визначено напрямки їх подальшого вирішення.

7. Окреслено переваги та ризики упровадження медичних інформаційних систем. З'ясовано, що розробниками медичних інформаційних систем є або юридичні особи або ж фізичні особи-підприємці, які пройшли перевірку на сумісність з Центральною базою даних, підписали договір з адміністратором бази даних (держпідприємством «Електронне здоров'я»), а також відповідають технічним нормам. Проаналізовано угоди медичних інформаційних систем Helsi, Health24, Asker, Moniheal у частині щодо збору, обробки, зберігання та надання доступу третім особам до медичної інформації.

Визначено основні інформаційні загрози МІС: великий обсяг медичної інформації, яка зберігається в одній базі даних та територіально розташована в одному місці; відсутність контролю з боку державних органів за діяльністю приватних компаній (операторів МІС). Окреслено проблематику технічного захисту Електронного реєстру відомостей про генетичні ознаки людини та дотримання порядку надання геномної інформації органам іноземних держав.

8. Визначено низку проблемних аспектів, що гальмують ефективне впровадження медичних інформаційних систем у сфері охорони здоров'я. У зв'язку з цим запропоновано чотири основні напрями удосконалення правового забезпечення інформаційної безпеки у зазначеній сфері. Зокрема, обґрунтовано необхідність подальшого доопрацювання правового регулювання захисту інформаційного права особи під час обов'язкового медичного страхування, включно з обробкою, зберіганням та охороною «чутливої» інформації.

Надано рекомендації щодо розробки та прийняття Закону України «Про загальнообов'язкове державне медичне соціальне страхування». Виявлено, що положення Закону України «Про державну реєстрацію геномної інформації людини» містять певні правові прогалини стосовно відповідності міжнародним стандартам захисту прав людини на інформацію, а також виникають проблеми щодо належного технічного забезпечення Електронного реєстру даних про генетичні ознаки особи. У зв'язку з цим запропоновано здійснити інтеграцію інформаційних систем та посилити їхній технічний захист відповідно до міжнародних стандартів.

Крім того, рекомендовано розробити ефективний механізм контролю за дотриманням операторами медичних інформаційних систем, підключених до центральної бази, вимог щодо захисту персональних даних, зокрема щодо інформованої та добровільної згоди пацієнта на їх обробку. Такі вимоги мають бути врегульовані й у договорах із Державним підприємством «Електронне здоров'я». На законодавчому рівні доцільно також розробити акти, що посилюють

відповідальність за порушення вимог захисту чутливої інформації, з урахуванням норм Загального регламенту Європейського Союзу з захисту персональних даних (GDPR).

9. Теоретично обґрунтовано, що інформатизація у сфері охорони здоров'я повинна здійснюватися з дотриманням вимог національного законодавства України щодо захисту персональних даних, Генерального регламенту ЄС із захисту персональних даних (GDPR), міжнародних стандартів ISO/IEC та інших відповідних міжнародних документів. Особлива увага має приділятися дотриманню принципів визначеної мети та мінімізації даних, тобто збирати та обробляти лише ті відомості, які є необхідними для реалізації конкретної мети.

Для ефективного розвитку та функціонування дієвої ЕСОЗ в Україні критично важлива надійна система захисту інформації. Крім того, потребує вдосконалення правове регулювання автентифікації користувачів у медичних інформаційних системах (МІС). У цьому контексті доцільно врахувати позитивний досвід Естонії, де доступ до МІС здійснюється виключно за персональним ідентифікатором (ID-паспортом), що значно зменшує ризики помилок та несанкціонованого доступу.

10. Наразі в Україні система правового забезпечення захисту інформації у медичній сфері потребує термінового удосконалення: необхідно систематизувати та кодифікувати національне законодавство відповідно до норм європейського права та міжнародних стандартів; розробити єдиний нормативно-правовий акт за прикладом GDPR, який врегулював би збір, обробку, захист та передачу медичної інформації, передбачаючи структурування медичної інформаційної системи, обов'язкову сертифікацію на захист інформації, застосування технологій криптографії та кодування, розмежування прав доступу медичних працівників, доступ до інформації з електронним підписом, короткострокові навчальні курси та реєстрацію фахівцями служби захисту інформації, корегування та внесення нової інформації з підтвердженням електронного підпису, а також безпечну передачу

інформації між закладами; внести зміни до Закону України «Про захист персональних даних» щодо форм та умов надання згоди на обробку ПД, доповнити ч. 3 ст. 1 розділу І Закону України «Про інформацію», дотримуватись вимог HIPAA при розробці програмного забезпечення медичних інформаційних систем та законодавчо посилити відповідальність за порушення захисту інформації у медичній сфері.

Крім того, законодавчо потребує врегулювання ряд напрямів, що стосуються інформаційної безпеки системи електронної охорони здоров'я, а саме:

– удосконалення електронної ідентифікації та автентифікації користувачів, стандартів обміну інформацією, порядків ведення реєстрів у центральній базі даних, форм медичної документації та функціонування медичної статистики;

– визначення вимог до розробки медичних систем, реєстрів та сервісів, а також контролю якості їх функціоналу;

– врегулювання доступу суб'єктів надання адміністративних та інших послуг до відомостей про стан здоров'я клієнта з урахуванням законодавства про захист інформації та персональних даних;

– забезпечення інтегрованої роботи та електронної взаємодії медичної інформаційної системи з іншими інформаційно-комунікаційними платформами;

– регламентація оброблення персональних даних, особливо тих, що становлять підвищений ризик для прав і свобод суб'єктів (дані про стан здоров'я), та їх повторного знеособленого використання для статистичних, наукових та інших цілей поза медичною допомогою;

– визначення вимог до технічного захисту інформації, вдосконалення процедур підтвердження відповідності систем захисту інформації, створення систем захисту та проведення державної експертизи таких систем у порядку, встановленому МОЗ.

– гармонізація національних стандартів із міжнародними та впровадження світових стандартів для інтеграції медичної інформаційної системи в глобальний

інформаційний простір, зокрема: Міжнародна статистична класифікація хвороб і споріднених проблем охорони здоров'я (МКХ), Міжнародна класифікація функціонування, обмежень життєдіяльності та здоров'я, Міжнародна класифікація первинної допомоги, Австралійський класифікатор медичних втручань (ACHI), систематизована медична номенклатура клінічних термінів (SNOMED), коди ідентифікаторів логічних спостережень (LOINC), міжнародні стандарти обміну даними FHIR та ISO/IEC, а також оригінальні класифікатори МНН, АТХ (ATC)-код і ТАС (форми випуску лікарських засобів).

11. Запропоновано удосконалення правового забезпечення інформаційної безпеки у сфері охорони здоров'я проводити за наступними напрямами:

– перший – систематизація законодавства;

– другий – удосконалення вимог щодо програмного забезпечення, сертифікації, технічного захисту інформації та вимог щодо забезпечення медичних закладів комп'ютерним устаткуванням, яке відповідає вимогам міжнародних стандартів;

– третій – удосконалення питань щодо організаційного та кадрового забезпечення інформатизації сфери охорони здоров'я;

– четвертий – впровадження загальноприйнятих міжнародних методик збору, обробки та захисту медичної інформації, а також активне розширення співпраці з міжнародними організаціями у сфері охорони здоров'я та інформаційної безпеки.

РОЗДІЛ 3
МІЖНАРОДНИЙ ТА ЄВРОПЕЙСЬКИЙ ДОСВІД ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

3.1. Застосування міжнародної та європейської практики щодо захисту інформації у медичній сфері

Міжнародний досвід правового забезпечення захисту інформації серед основних напрямів виокремлює: захист прав особистості в інформаційній сфері; захист державних інтересів; захист підприємницької та фінансової діяльності; захист інформації від комп'ютерних злочинів [98].

Захист персональних даних, особливо «чутливих», є не лише обов'язком держави та предметом державного регулювання, а й важливою складовою реалізації прав людини. Інформація про стан здоров'я тісно пов'язана з правом на повагу до приватного життя, і ці права мають взаємозв'язок. Як зауважує І.С. Демченко, доцільно виділити два основні напрями таких відомостей: право особи на доступ до інформації про власне здоров'я або пов'язаних із ним аспектів та право на захист цієї інформації завдяки її конфіденційному характеру [34].

Розглянемо це на практиці Європейського суду з прав людини (далі – ЄСПЛ). Так, у справі «І. проти Фінляндії» [213] судом акцентовано увагу на тому, що інформація про пацієнта є складовою частиною його приватного життя. У справі «К.Н. та інші проти Словакії» розглянуте питання щодо доступу до медичної документації. За рішенням Суду, заборона виготовлення копій медичної документації пояснюється необхідністю захисту такої інформації від зловживань [214]. У справі «Z проти Фінляндії» підкреслено, що повага до конфіденційності інформації про стан здоров'я є невід'ємним принципом правових систем країн – учасниць Конвенції. Важливо не лише дотримуватись конфіденційності медичної інформації, але й забезпечувати довіру пацієнта до медичної професії та медичних послуг загалом [215].

У міжнародному законодавстві виокремлюють три напрями закріплення прав пацієнта: універсальний, регіональний та спеціалізований [105]:

1) *універсальні нормативно-правові акти*, які носять декларативний характер і виступають, в основному, у якості рекомендацій для світової спільноти (Загальна декларація прав людини, 1948; Міжнародний пакт про економічні, соціальні й культурні права, 1966; Декларація про права інвалідів, 1975; Декларація про права розумово відсталих осіб, 1971 та ін.). Зазначений напрям забезпечення права на охорону здоров'я – гарантія щодо визнання міжнародним товариством даного права. Крім того, він зобов'язує держави, які ратифікували зазначені документи, незважаючи на їх рівень економічного розвитку, розробляти та впроваджувати дієві механізми щодо його забезпечення;

2) *нормативно-правові акти регіонального рівня* – це, як правило, документи, прийняті Радою Європи, які мають обов'язковий характер (зважаючи на традиції та рівень розвитку країни, зазначені акти, на відміну від універсальних, більш конкретні, а також мають свій політико-правовий механізм реалізації);

3) *спеціалізовані акти* – документи, які прийнято спеціально створеною організацією, основна мета яких – класифікація працівників за певними категоріями

та визначення стандартів трудової діяльності, які не впливають негативно на здоров'я (Конвенції й рекомендації Міжнародної організації праці, які стосуються медичної допомоги, допомоги при хворобі, праці дітей, матерів, інвалідів).

Разом з тим, як слушно зазначають М.В. Банчук, В.Ф. Москаленко та Б.В. Михайличенко, зазначений науковий підхід щодо визначення рівня захисту прав пацієнтів не зовсім коректний, так як здійснено лише зміну понять «права пацієнтів» та «права осіб у медичній сфері [105].

Зазначимо, що до другої половини XX століття система захисту прав громадян, у тому числі і захисту інформації, у медичній сфері регулювалась в основному правилами медичної етики. Першими документами у даному напрямі стали Рекомендації щодо правил надання медичної допомоги, 1944 р. та Нюрнберзький кодекс (підготовлений у формі інформаційного протоколу Міжнародного військового трибуналу «Суд над лікарями») 1946 р. З метою покращення ефективності системи захисту та реалізації прав пацієнтів, у березні 1994 року у Амстердамі прийнято Основи концепції прав пацієнта в Європі (Амстердамська декларація), якою визначено основні принципи щодо підтримки і захисту прав пацієнтів на території європейських держав-членів ВООЗ [33].

Що стосується регламентації діяльності з питань захисту «чутливої» інформації», то, відповідно до норм міжнародного права, вони поділяються на три групи: загальні норми, спеціальні норми та основні норми.

До загальних норм відноситься право на приватність (право на недоторканність особистого і сімейного життя) – ст. 12 Загальної декларації прав людини, ст. 17 Міжнародного пакту про громадянські і політичні права, ст. 8-1 Конвенції про захист прав людини і основоположних свобод, Міжнародна конвенція про охорону осіб при автоматизованій обробці особистих даних, Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою ПД щодо органів нагляду та транскордонних потоків даних (ETS № 181),

Директива 95/46/ES про охорону фізичних осіб у зв'язку з обробкою ПД та про вільний рух таких даних [11].

Загальні норми захисту «чутливої інформації» закріплено і в прецедентних рішеннях ЄСПЛ. Так, у рішенні ЄСПЛ у справі «М. С. проти Швеції» звертається увага на те, що конфіденційність відомостей про здоров'я є основним принципом правової системи держав-учасниць. Подібні висновки ЄСПЛ за результатами розгляду прослідковуються і у наступних справах: «I. v. Finland» (заява № 20511/03) – відсутність обліку фактів щодо надання доступу до медичної документації заявниці призвело до унеможливлення встановлення особи, яка ймовірно поширила інформацію, що містилася у ній; «L.H. v. Latvia» (заява № 52019/07) – відсутність легітимної мети збору персональних даних, надмірний об'єм зібраної інформації, неврахування інтересів пацієнта (збір інформації контролюючим органом з метою оцінки якості наданої пацієнту медичної допомоги лікарнею); «Z. v. Finland» (заява № 22009/93) – недостатність строків, впродовж яких обмежувався доступ до рішення суду, що містив чутливу інформацію про заявницю; «Avilkina and Others v. Russia» (заява № 1585/09) – законодавча невизначеність повноважень прокуратури щодо збору медичної інформації про особу та інші [11].

До речі, типові положення зазначених вище рішень ЄСПЛ стали основою для прийнятої Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» № 108, у якій вперше окреслено ключові принципи обробки персональних даних, права особи у зв'язку з обробкою її персональних даних, базові норми щодо транскордонної передачі даних. Дещо пізніше прийнято Додатковий протокол до цього міжнародного договору, яким конкретизовано положення Конвенції. Крім того, важливим є те, що саме цим документом передбачено необхідність створення сторонами Конвенції наглядового органу, який безпосередньо буде забезпечувати контроль щодо дотримання норм законодавства про захист ПД [11].

Спеціальними нормами визначено питання щодо захисту інформації у медичній сфері. Вперше поняття «конфіденційність» на міжнародному рівні закріплено в Женевській декларації як «обов'язок берегти таємницю, яку довірили, навіть після смерті пацієнта» [45], у подальшому його закріплено у: Міжнародному кодексі медичної етики [108], шостому з Дванадцяти принципів організації охорони здоров'я для будь-якої національної системи охорони здоров'я [30], Лісабонській декларації стосовно прав пацієнта [96].

Переходячи безпосередньо до аналізу основних норм міжнародного законодавства, зазначимо, що у міжнародно-правовому регулюванні питань інформаційної безпеки важливим кроком стало прийняття резолюції Генеральної Асамблеї ООН 54/90 «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки», в якій визначено питання щодо розробки міжнародних механізмів, які сприятимуть зміцненню інформаційної безпеки глобальних інформаційних та телекомунікаційних систем.

У подальшому розроблено «Керівні принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних», які схвалено Рекомендацією Ради ОЕСР та прийнято Генеральною Асамблеєю ООН резолюцією № 95 (XLV) «Керівні принципи регулювання комп'ютерних файлів, які містять персональні дані».

Крім того, Концепцією про захист прав людини і основоположних свобод передбачено, що державні органи не можуть втручатись у здійснення цього права, крім випадків, коли воно здійснюється відповідно до норм Закону та необхідне для інтересів національної та громадської безпеки, економічного добробуту країни, у тому числі захисту прав і свобод людини [81].

Відповідно до Конвенції про захист осіб у зв'язку із автоматизованою обробкою персональних даних, ПД, що розкривають расову приналежність, політичні переконання, дані щодо стану здоров'я та статевого життя, не підлягають

автоматизованій обробці, якщо внутрішнім законодавством не забезпечено відповідні гарантії [74].

Директива Європейського Парламенту і Ради (ст. 8) забороняє обробку персональних даних, що розкривають расове або етнічне походження, стан здоров'я чи статеве життя людини, за винятком випадків, коли це необхідно для захисту життєво важливих інтересів суб'єкта або іншої особи, суб'єкт даних не може надати згоду через недієздатність чи неправоздатність, обробка потрібна для діагностики, надання медичних послуг або лікування, або коли дані обробляє медичний працівник, який зобов'язався зберігати їх конфіденційність [165].

Декларація про політику в галузі забезпечення прав пацієнта в Європі передбачає, що вся інформація щодо стану здоров'я пацієнта, прогноз і лікування його захворювання, а також будь-яка інша інформація особистого характеру повинна зберігатися у таємниці навіть після смерті пацієнта (п. 4.1), а пацієнти, які перебувають у лікувально-профілактичних закладах, мають право на наявність устаткування, необхідного для гарантії зберігання медичної таємниці (п. 4.8) [33].

Загальний регламент Європейського Парламенту і Ради (ЄС) щодо захисту фізичних осіб при обробці персональних даних визначає, що особливо чутливі персональні дані потребують спеціального захисту, а їх обробка та використання без згоди об'єкта даних дозволяється лише для забезпечення суспільних інтересів у медичній сфері [47]. Крім того, Пропозиція Комітету міністрів державам-учасницям № R(81)1 розширює сферу суб'єктів, на яких поширюються правила конфіденційності, та встановлює вимоги щодо автоматизованих банків медичних даних.

Вартим уваги є принцип необхідності та пропорційності збору персональних «чутливих» даних. Відповідно до ч. 1 ст. 5 Конвенції про захист осіб у зв'язку із автоматизованою обробкою персональних даних, ПД, які підлягають автоматизованій обробці, зберігаються виключно для легітимних цілей і використовуються у спосіб, який не суперечить їм. Персональні дані, зібрані для

різних цілей, не повинні об'єднуватися, крім випадків, коли вказані цілі є сумісними, а склад ПД, які необхідні для досягнення обох цілей, збігається [74; 11].

Разом з тим, незважаючи на чіткі законодавчі норми, мають місце факти порушення у частині, що стосується: відсутності як мети, так і доцільності такого об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутності підстави для подальшого зберігання та обробки інформації.

Так, у справі «R v. RC» Канадський Верховний Суд розглянув питання щодо зберігання в національному банку зразків ДНК неповнолітнього, яким уперше було вчинено правопорушення. Згідно з рішенням Суду, наслідки від зберігання зразків ДНК будуть надзвичайно непропорційними. Зокрема статтею 8 Хартії передбачено захист персональної інформації, яку фізичні особи у вільному та демократичному суспільстві хотіли б утримувати та запобігати її розголошенню державі. Зважаючи на те, що ДНК становить найвищий рівень особистої і приватної інформації, їх відбір та зберігання є грубим втручанням у право суб'єкта на персональну та інформаційну приватність [197].

Розглянемо зазначені вище порушення у контексті аналізу рішень ЄСПЛ. У справі «S. and Marper v. the United Kingdom» (заяви №№ 30562/04та30566/04) заявники поскаржилися на те, що владні органи продовжили зберігання їх відбитків пальців та зразків ДНК після закриття кримінальних проваджень. Першого заявника було арештовано у 2001 році у віці 11 років та обвинувачено у замаху на розбій, у зв'язку із чим відібрано відбитки пальців та зразки ДНК. У цьому ж році його було виправдано. Другого заявника арештовано у 2001 році та звинувачено у переслідуванні свого партнера, у зв'язку із чим відібрано відбитки пальців та зразки ДНК. Слід зазначити, що до початку розгляду справи у суді, вони дійшли згоди, відповідно, обвинувачення припинилося. На вимогу заявників знищити їх відбитки пальців та зразки ДНК, вони отримали відмову у поліції. З метою перегляду рішень

поліції, заявники звернулися до суду. Суд постановив, що мало місце порушення ст. 8 Конвенції основоположних свобод та прав людини [215].

У справі «M.K. v. France» у заявника, якого затримали за крадіжку, було відібрано відбитки пальців. Після закриття справи заявник звернувся до прокурора з вимогою видалити відбитки пальців, проте йому відмовили (на підставі виключення його причетності до інших злочинів та з метою зібрання якомога більшої бази даних). Суди рішення прокурора залишили без змін, вказуючи на легітимність мети. Розглядаючи пропорційність втручання, Суд зазначив: мета обробки відбитків пальців у інформаційній базі даних не визначена, тому зібрання відбитків всього населення є надмірним та непотрібним. Разом з тим, Суд зазначив, що відбитки пальців необхідно збирати як у справах щодо серйозних, так і найдрібніших злочинів. Відбитки зберігаються незалежно чи засуджено особу у подальшому, чи виправдано, чи закрито провадження. Відповідно, імовірність видалення відбитків пальців за скаргою, зважаючи на мету – накопичення якнайбільшої кількості зразків, є ілюзорною [11].

Таким чином, на думку Суду, держава перевищила межі наданої їй свободи розсуду, не забезпечивши збалансованість між інтересами особи та суспільними інтересами. Втручання було непропорційним і не відповідало вимогам статті 8 Конвенції про захист осіб у зв’язку з автоматизованою обробкою персональних даних [218; 11; 57].

Вартим особливої уваги у частині щодо захисту медичної інформації, у тому числі і «чутливої», став прийнятий у травні 2018 року Загальний регламент із захисту персональних даних. Зазначимо, що саме цим документом суттєво змінено попередні закони щодо захисту інформації у країнах Європейського союзу, визначено її правила обробки та використання у публічному та приватному просторі. Передбачено винятки щодо обробки відомостей щодо стану здоров’я, які спрямовано як на захист інформаційних прав суб’єктів, так і конфіденційності даної інформації [56].

Згідно із Загальним регламентом із захисту персональних даних, відомості про стан здоров’я відносяться до категорії чутливих персональних даних, які потребують посиленого рівня захисту, оскільки їхня обробка в певному контексті може створювати значний ризик порушення прав і свобод людини.

GDPR передбачає суттєві зміни у контролі та володінні даними про здоров’я, які переходять від лікарів, науковців, лікарень та закладів охорони здоров’я до пацієнтів. Тепер пацієнти повинні надати згоду на використання інформації про їхній стан здоров’я і мають право відкликати цю згоду за потреби [57].

Як бачимо, Загальний регламент із захисту персональних даних надає значну увагу новим вимогам, що виникають у зв'язку з підвищенням рівня цифровізації у сфері охорони здоров’я. Це, у свою чергу, сприятиме посиленню захисту інформації про стан здоров’я.

Зазначимо, що у GDPR уперше надано визначення поняття «дані, що стосуються здоров’я» – інформація, яка змістовно пов’язана з фізичним чи психічним здоров’ям, з урахуванням сукупності даних щодо стану здоров’я у минулому, теперішньому чи майбутньому, які зібрано як під час реєстрації, так і безпосередньо при наданні медичних послуг. Зазначеним регламентом передбачено нові стандарти захисту відомостей щодо стану здоров’я, яким посилено відповідальність контролерів (організація, яка відповідальна за збір та управління інформацією. Для прикладу, лікарня, яка збирає інформацію) та процесорів (організацій, що допомагають у наданні послуг з обробки даних, а також власників програмних продуктів, у яких вони зберігаються та обробляються), які їх обробляють [56].

Загальним регламентом із захисту персональних даних передбачено також вищі стандарти стосовно інформованої згоди та обов’язків щодо повідомлення (ст. 7), а також посилення захисту права на доступ до ПД щодо стану здоров’я. Заслуговує на увагу і те, що у разі витоку ПД (ст.ст. 33, 34) контролери упродовж

72 год. повинні проінформувати контролюючий орган, у разі ж порушення безпеки даних – інформують пацієнтів [57].

Даним документом розширено і питання щодо прав пацієнтів – передбачено право вимагати від контролерів та процесорів видаляти інформацію щодо стану їх здоров'я. Також GDPR визначено, що найвищий рівень конфіденційності автоматично застосовується до нового сервісного продукту щодо стану здоров'я [56].

За недотримання правових норм GDPR для організацій охорони здоров'я передбачено відповідні санкції. Зокрема, збільшено адміністративні штрафи – 10 млн. євро у випадку незначних порушень чи 20 млн. євро при виявленні серйозних порушень (ст. 83) [48].

Як видно, Загальний регламент із захисту персональних даних вказує на те, що організації несуть відповідальність за управління зібраними персональними даними. Це забезпечується через проведення юридичного аудиту, який оцінює не лише типи зібраних даних, але й рівень їх захисту. Зазначимо, що Директивою Європейського Парламенту і Ради ЄС «Про заходи для високого рівня безпеки мережевих та інформаційних систем на території Союзу» також передбачено здійснення контролюючими органами аудиту операторів (операторами у медичній сфері визначено постачальників медичних послуг – медичні заклади) [166; 140].

Як бачимо, GDPR дійсно заслуговує уваги, проте незважаючи на те, що він діє вже протягом чотирьох років, мають місце проблемні питання. Так, наприклад, лише протягом лютого 2021 року:

а) Sky Med International звинуватили у невжитті відповідних заходів щодо забезпечення особистої інформації відносно осіб, які підписалися на її план екстреного членства в поїздках, в результаті компанія залишила незахищеною базу даних, що містить 130 000 записів про членство (незахищена база даних містила особисту інформацію членів, що зберігається у звичайному тексті, таку як імена, дати народження, домашні адреси, інформацію щодо стану здоров'я та номери

рахунків членів). Крім того FTC стверджував, що Sky Med увів в оману споживачів, вивісивши на кожній сторінці свого веб-сайту печатку «Відповідність HIPAA», що створило помилкове враження, що її політика конфіденційності була переглянута і відповідала вимогам безпеки та конфіденційності Закону про переносимість та підзвітність медичного страхування (далі – HIPAA) [267];

б) у Польщі наклали штраф (85 000) злотих на підприємця, який надає послуги у медичній сфері. Зокрема, відповідно до вказівок Управління захисту персональних даних Польщі, підприємець повинен був повідомляти своїх пацієнтів про порушення їх ПД, а також надавати їм рекомендації щодо мінімізації потенційних негативних наслідків інциденту. З урахуванням того, що адміністратор цього не робив, на нього, згідно із ст. 58 сек. 2 GDPR, накладено адміністративний штраф [128; 140].

Вартим уваги є і те, що у 1996 році, з метою правового врегулювання захисту інформації у медичній сфері, у Сполучених Штатах Америки (далі – США) було прийнято Закон про мобільність та підзвітність медичного страхування «Health Insurance Portability and Accountability Act» або «HIPAA», основна мета якого – врегулювання мобільності та підзвітності медичного страхування і встановлення стандартів захисту медичної звітності та особистих медичних даних пацієнтів) [52; 138].

HIPAA дозволяє використовувати правило «Необхідного мінімуму» [276] при проєктуванні систем, які відповідають усім вимогам конфіденційності, система повинна докладати всіх необхідних зусиль для використання, вимагання або розкриття лише мінімальної кількості інформації, необхідної для досягнення поставленої мети. Додатки, сумісні з HIPAA, визнані як найбільш надійні в усьому світі.

Основною відмінністю GDPR і HIPAA є те, що HIPAA охоплює лише медичні персональні дані і регулює їх збір та обробку для певного кола осіб, які мають доступ до таких даних. Натомість GDPR має більш широкий обсяг дії,

поширюючись на всі види персональних даних в Європейському Союзі і охоплюючи різні аспекти їх захисту та обробки, незалежно від специфіки даних або сфери їх застосування. Крім того, досить важливим є те, що відповідно до HIPAA можна здійснювати розкриття PHI (медична інформація, яка ідентифікує конкретну людину – імена, телефонні номери, адреси, дати народження, номери соціального страхування, платіжну інформацію, результати аналізів, медичні записи, фотографічні зображення, результати рентген-обстеження і т.д.) [259] без попередньої згоди пацієнта в цілях лікування. Натомість GDPR вимагає однозначної згоди пацієнта для розкриття даних про стан здоров'я, якщо пацієнт здатний надати таку згоду. Крім того, HIPAA не надає пацієнту права вимагати видалення своїх медичних даних з бази даних закладу охорони здоров'я, у той час як GDPR забезпечує це право.

Повну конфіденційність даних користувачів забезпечує, відповідно до HIPAA, платформа Curogram. Це унікальна розробка у сфері телемедицини, яка підтримує режим відеозв'язку, двосторонній обмін текстовими повідомленнями через смартфон та працює напряму з будь-якою системою електронних медичних архівів. Curogram допомагає постачальникам медичних послуг автоматизувати робочі процеси, оптимізувати взаємодію між лікарями та медсестрами, краще координувати догляд за пацієнтами, швидше знаходити контакти інших медичних закладів чи партнерів та зв'язуватися з ними [265; 259].

Об'єктами захисту в інформаційній системі медичного закладу є інформація в базах даних систем керування базами даних (далі – СКБД); ресурси файлового сервера лікувально-профілактичного закладу; резервні копії баз даних СКБД і архівні копії ресурсів файлового сервера; керуюча інформація операційної системи, СКБД, автоматизоване робоче місце (далі – АРМ) адміністратора медичної інформаційної системи та адміністратора інформаційної безпеки (далі – ІБ); технологічний процес збору, обробки, зберігання та передачі інформації в МІС; а також апаратно-програмний комплекс, що забезпечує роботу МІС [64; 261]. Будь-

який користувач медичного закладу, який отримав доступ до медичної інформаційної системи несе моральну, адміністративну і кримінальну відповідальність за конфіденційність інформації, яку він вносить, використовує або передає іншим користувачам.

Акцентуємо увагу і на тому, що у лютому 2021 року у США набули чинності два нормативні акти, які будуть діяти разом з HIPAA – Правило взаємодії CMS і доступу пацієнтів (впровадження і підтримання безпечного, заснованого на стандартах інтерфейсу прикладного програмування, який дозволяє пацієнтам легко отримувати доступ до своїх заявок. Правило CMS також вимагає, щоб постачальники програм Medicare і Medicaid відправляли електронні повідомлення про надходження, виписку або переведення пацієнта в новий медичний заклад, до постачальника послуг в громаді або до практикуючого лікаря) [148] та Заключне правило Закону про лікування ONC (застосовується до IT-систем охорони здоров'я, а також до постачальників медичних послуг, обміну медичною інформацією і мереж медичної інформації, які використовують такі системи. Правило вимагає, щоб системи реалізували стандартизовані API-інтерфейси, пацієнти і їх постачальники медичних послуг могли легко отримувати електронну інформацію про здоров'я за допомогою додатків для смартфонів [268].

Центральним компонентом правила є положення про блокування інформації, яка забороняє дії, що перешкоджають доступу та обміну EHI з певними винятками щодо конфіденційності та безпеки [51]. Основною метою даних документів є спрощення доступу пацієнтів до їх медичних даних з дотриманням відповідних заходів безпеки і конфіденційності.

Таким чином, захист медичної інформації є не лише обов'язком держави і предметом державно-правового регулювання, але й важливим аспектом захисту прав людини.

У міжнародному законодавстві права пацієнта на захист інформації регулюються у трьох напрямах – універсальними нормативно-правовими акти,

нормативно-правовими актами регіонального рівня та спеціалізованими актами. Норми міжнародного права поділяються на загальні, спеціальні та основні. Загальні норми захисту «чутливої інформації» закріплено також в прецедентних рішеннях ЄСПЛ. Основною мета документів, які регламентують діяльність у даному напрямі – спрощення доступу пацієнтів до їх медичних даних з дотриманням відповідних заходів безпеки і конфіденційності. Особливістю міжнародного законодавства є те, що держава виступає гарантом захисту медичної інформації.

Епохальним у частині щодо захисту медичної інформації став прийнятий у травні 2018 року Загальний регламент із захисту персональних даних. Зазначимо, що саме цим документом суттєво змінено попередні закони щодо захисту інформації країнах Європейського союзу, визначено її правила обробки та використання у публічному та приватному просторі. Передбачено винятки щодо обробки відомостей щодо стану здоров'я, які спрямовано як на захист інформаційних прав суб'єктів, так і конфіденційності даної інформації. Саме даним документом чітко визначено у яких випадках пацієнти можуть видалити інформацію щодо стану їх здоров'я, а також передбачено санкції у разі недотримання правових норм GDPR організаціями охорони здоров'я.

Таким чином, саме системність, послідовність та повнота закріплення прав особи на захист медичної інформації на законодавчому рівні мають важливе значення для отримання кожним пацієнтом тих послуг, які передбачено відповідним правом [97].

3.2. Міжнародні та європейські стандарти захисту інформації у електронних системах сфери охорони здоров'я та перспективи їх імплементації у вітчизняне законодавство

Одним із ключових завдань удосконалення української системи охорони здоров'я є інтеграція міжнародних стандартів у національне законодавство, що регламентує права пацієнтів, зокрема право на захист медичної інформації. Водночас слід зазначити, що проблеми витоку «чутливих» персональних даних спостерігаються і за кордоном. Сьогодні у світі фіксується зростання кількості кібератак на критичну інформаційну інфраструктуру, включаючи медичні заклади. Так, у вересні 2020 року у США хакерська атака вірусу-здирника на національну мережу лікарень Universal Health Services призвела до збою інформаційної системи, масштабних відключень, затримок у доступі до лабораторних результатів та перенаправлення пацієнтів у інші заклади для отримання медичної допомоги. Втрата контролю над даними пацієнтів визнається однією з найсерйозніших загроз безпеці медичного обслуговування [140].

У грудні 2020 року британська мережа косметологічних клінік Transform Hospital Group стала об'єктом атаки вірусів-вимагачів, внаслідок якої було викрадено близько 900 Гб даних та з'явилась загроза публікації фотографій пацієнтів до та після процедур. Того ж року зафіксовано кібератаки на сервери Дюссельдорфської університетської лікарні (Німеччина), університетської лікарні в Нью-Джерсі (США), дитячої лікарні в Бостоні та на установи, що займаються дослідженнями вакцин, серед інших [270; 237, с. 31; 140]. Подібні інциденти підкреслюють необхідність дотримання міжнародних стандартів щодо захисту персональних даних, зокрема модернізованої Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108+) та Загального регламенту ЄС із захисту персональних даних (GDPR).

Саме нормами GDPR передбачено можливість накладати штраф на порушників до 20 млн євро або ж до 4% річного обігу компанії [48]. Два з 5 найсуттєвіших по розміру штрафів за порушення норм GDPR було накладено за невідповідність його положенням (контролери та процесори несуть відповідальність не лише за витік даних, але і за будь-яку невідповідність

стандартам GDPR). Для прикладу, найбільшим штрафом є штраф, накладений французьким DPA (CNIL) за скаргами приватних позивачів у справі «Google LLC» у розмірі п’ятдесят млн євро за невиконання наданого зобов’язання про прозорість та поінформованість, а також нездатність отримання правової підстави щодо оброблення інформації. Наступним прикладом є справа «Deutsche Wohnen SE», у якій німецьким DPA накладено штраф у розмірі 14,5 млн євро за порушення відповідних норм щодо встановлення відповідної системи зберігання інформації з функціоналом стирання даних, які не потрібні [3; 92].

Згідно з рекомендаціями CM/Rec (2019) 2 Ради Європи щодо захисту медичних даних, лікарі зобов’язані забезпечувати охорону персональної інформації пацієнтів [189]. Водночас міжнародні правові норми визначають, що особи набувають статусу працівників медичної сфери лише за умови взяття на себе обов’язку дотримуватися медичної таємниці.

Мають місце також факти витоку чутливої інформації внаслідок недбалих чи необережних дій осіб, відповідальних за її збереження. Для прикладу, у 2009 році стався витік медичної інформації (персональні дані, результати аналізів, анамнези тощо) однієї із лабораторій «Laboratory Corporation of America» США. Під час транспортування документів з персональними чутливими даними, вони просто випали з вантажної машини.

У випадку чутливих персональних даних, що зберігаються у медичних інформаційних системах, відповідальність за їх збереження, обробку та захист покладається на саму систему або сервіс, з яким пацієнт укладає угоду. Згідно з Директивою про захист персональних даних, держави-члени зобов’язують власника системи вживати належні технічні та організаційні заходи для запобігання випадковому або незаконному знищенню, втраті, зміні, несанкціонованому розкриттю чи доступу до персональних даних, особливо у разі їх передачі через мережу [168]. Аналогічно, Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних передбачає, що для захисту таких даних у

автоматизованих файлах необхідно вживати відповідних заходів безпеки, які запобігають випадковому або несанкціонованому знищенню, втраті, несанкціонованому доступу, зміні чи поширенню [74].

Орієнтиром для демократичних принципів щодо поваги до прав та законних інтересів громадян, у тому числі і у частині, що стосується приватності медичної інформації, є Сполучені Штати Америки. Правовий захист у США медичної інформації, яка відноситься до чутливої категорії персональних даних, передбачає більший рівень захисту, ніж інші категорії персональних даних. Даний напрям регламентовано Законом США про мобільність та підзвітність медичного страхування (Health insurance portability and account tability act або HIPAA), прийнятим у 1996 році. HIPAA – закон, який врегульовує мобільність та підзвітність медичного страхування і встановлює стандарти захисту медичної звітності та особистих медичних даних пацієнтів. Він визначає, які дані пацієнтів захищаються, а також хто повинен дотримуватись вимог HIPAA при роботі з відповідною інформацією.

HIPAA охоплює інформацію, що включає минулі та актуальні дані про стан здоров'я особи, такі як анамнез, діагноз, результати медичних досліджень та призначене лікування; інформацію про надання медичних послуг; а також дані про оплату медичних послуг, які дозволяють ідентифікувати особу або створюють обґрунтовану підставу для такої ідентифікації. Важливо зазначити, що базові ідентифікаційні дані особи, такі як місце проживання, ім'я, прізвище та податковий номер, не є охопленими HIPAA окремо. Проте, коли ці дані поєднані з інформацією про стан здоров'я або медичні послуги, вони підпадають під захист HIPAA. Збір, обробка та захист таких даних здійснюються медичними працівниками, страховими компаніями та їх бізнес-партнерами, які виконують функції або надають послуги від імені цих організацій і включають використання чи розкриття цих даних, наприклад, компаніями, що обробляють медичні рахунки або подають запити на страхове відшкодування [54; 137].

Сполучені Штати Америки – лідер щодо інформатизації процедури надання медичних послуг, а також країна, яка найбільше витрачає на медичну сферу. Крім того, Конгресом США ухвалено закон «The American Recovery and Reinvestment Actof 2009 (ARRA)», яким передбачено упровадження електронних МІС. Також Законом визначено, що заклади охорони здоров'я зобов'язані передбачити відповідні штатні посади фахівців з інформаційної безпеки, які супроводжуватимуть роботу МІС та мереж, а також вибрати та придбати програмний продукт [140].

Незважаючи на те, що Великобританія також є лідером інформатизації медичної сфери, її «… ринок цифрових медичних систем складає низьку частку світового ринку і є фрагментарним» [122].

Понад 15 років МІС використовують у Південній Кореї 3500 регіональних закладів. Кількість звернень до МІС щоденно складає понад 154 000. Більше того, Південна Корея постійно працює над подальшим розвитком інформаційної сфери та захистом медичної інформації [272, с. 322]. Варто зазначити, що медичні інформаційні системи, розроблені в Кореї, використовуються в Саудівській Аравії, Об'єднаних Арабських Еміратах та на Філіппінах. Наприклад, інформаційна система Міжнародного медичного центру в Монголії також була розроблена корейською компанією BIT, яка наразі працює над розробкою національної МІС для Іраку [263, с. 161; 140].

Що стосується Японії, то МІС тут переважно регіонального характеру (впровадження їх у великих медичних закладах складає 62,7%, у середніх – 21,7%, у малих – 9,1%) [274, с. 179; 140].

Також варто підкреслити, що в більшості країн світу медичні інформаційні системи, зазвичай, включають п'ять основних модулів: реєстрацію пацієнта, амбулаторний менеджмент, виставлення рахунків та оброблення інформації щодо страхування пацієнта, сервісний модуль та безпековий модуль, який забезпечує контроль доступу до інформації пацієнта. Ці базові модулі є необхідними для

функціонування кожного медичного закладу. Наприклад, у Великобританії базові модулі для МІС закуповуються державою для лікарень, тоді як додаткові послуги кожен медичний заклад може придбати окремо.

Наступним актуальним питанням міжнародної спільноти є захист чутливих персональних даних у медичних системах при клінічних випробуваннях (дослідження нових препаратів на пацієнтах у документально зафіксованому дослідницькому середовищі), які регулюються Директивою 2001/20/ЕС Європейського парламенту і Ради (ЄС) від 04.04.2001 року про клінічні випробування [42]. Для прикладу, у США менеджер з клінічних випробувань залишив без нагляду комп'ютер, на якому зберігались незакодовані дані про клінічне дослідження, що проводилось Національним інститутом захворювань серця, легень та крові (National Heart, Lung and Blood Institute, NHLBI). Внаслідок цього інциденту постраждали 2500 учасників дослідження в галузі кардіології. Усі учасники були повідомлені про витік інформації, що включала їх персональні дані, відомості про стан здоров'я та результати обстежень [55].

За результатами перевірок як вітчизняних, так і міжнародних медичних установ, у яких здійснювалися зазначені клінічні дослідження, встановлено непоодинокі факти порушення норм щодо технічного захисту чутливої інформації. Зокрема, порушуються вимоги щодо знищення медичної інформації на електронних носіях (після видалення інформації не застосовується форматування електронного носія, відповідно, за допомогою сучасного програмного забезпечення наявна можливість відновлення видалених файлів). Це свідчить про неналежний рівень знань з питань технічного захисту інформації працівниками даних установ, які відповідають за збір, обробку та передачу конфіденційної інформації.

Наступним питанням у контексті дослідження є захист медичної інформації у загальнонаціональних системах електронних медичних записів під час взаємообміну медичною інформацією. Першими нормативно-правовими акти у даному напрямі є Criminal Justice and Public Order Act (Великобританія, 1994 р.),

DNA Identification Act (США), Dutch Forensic DNA Typing Act (Нідерланди), якими урегульовано норми щодо створення та функціонування національної бази даних ДНК. Слід зазначити, що в 1997 році рішенням Ради ЄС «EU Council Decision of 9 June 1997 on the exchange of DNA analysis results» країнам – членам ЄС було запропоновано розглянути можливість щодо створення національних баз даних ДНК, які будуть сумісними для взаємного обміну інформацією [219]. З урахуванням ефективності ДНК-аналізу під час ідентифікації особи, а також зважаючи на те, що зазначена інформація потребує додаткового захисту, більшість європейських держав перед створенням баз даних, підготували та затвердили спеціальне законодавство.

Разом з тим, взаємообмін між базами даних таким видом конфіденційної інформації, відповідно, передбачав упровадження єдиних міжнародних стандартів. У зв'язку із чим, у 2001 році Радою Європейського Союзу розроблено стандартний набір локусів для криміналістичного ДНК-аналізу, що сприяло безперешкодному обміну інформацією між базами даних ДНК.

За результатами аналізу міжнародного досвіду у даному напрямі, встановлено, що найбільш ефективним є створення єдиної бази даних ДНК (на кшталт баз даних ДНК в США, Великобританії, Польщі, Німеччині, Італії, Іспанії, Франції, в яких визначено одного держателя та адміністратора бази даних ДНК). Розглянемо, як приклад, комплексну базу даних з інформацією про генетичні послідовності Gen Bank, DDBJ (DNA Data Bank of Japan) та ENA (European Nucleotide Archive). Gen Bank було упроваджено ще у 1979 році, вона містить загальнодоступні послідовності нуклеотидів для 420 тис. офіційно описаних видів З 1981 року база даних підтримується Національним центром біотехнологічної інформації США (NCBI), що входить до складу національних інститутів здоров'я та доступний на безоплатній основі дослідникам усього світу (щоденно Gen Bank обмінюється даними з Європейським архівом нуклеотидів (ENA) та Банком даних ДНК Японії (DDBJ) [202].

Варто зазначити, що у США у 1994 році була впроваджена програма створення лабораторій комбінованої системи ДНК-індексу – CODIS, яка включає три рівні: місцеві системи, системи штатів та національну систему індексів для зберігання профілів ДНК. CODIS охоплює індекси злочинців, заарештованих осіб та профілів, зібраних з місць злочинів. Станом на кінець 2021 року CODIS містив понад 14 мільйонів профілів злочинців та 4,5 мільйона профілів заарештованих осіб [202]. Крім того, у США в 2000 році створено федеральний підрозділ бази даних ДНК (FDDU), яка обслуговує велику спільноту криміналістів, допомагаючи ідентифікувати осіб, профілі яких знаходяться у Національній системі індексу ДНК (NDIS) [126; 93].

Разом з тим, найбільша база ДНК Національної кримінальної розвідки у світі у Великій Британії, в яку до 2020 року внесено 6,6 млн. профілів, що дозволило у період з 2001 по 2020 роки ідентифікувати 731 тис. (на кінець 2022 року вона містила 10% даних ДНК від усього населення). Особливістю зазначеного реєстру є те, що його функціоналом передбачено розгалужену систему та кілька рівнів перевірки для вирішення питання подальшого збереження даних у системі.

У 2005 році Австрією, Бельгією, Францією, Іспанією, Люксембургом, Німеччиною та Нідерландами було підписано Прюмський договір, відповідно до якого держави-члени Європейського Союзу мають можливість надавати одна одній автоматичний доступ до генетичних баз даних. Отже, як бачимо, на підставі Прюмського договору, країни-члени ЄС отримали як правовий механізм, так і додаткові практичні можливості щодо обміну інформацією між національними базами даних ДНК. Для прикладу, саме завдяки обміну інформацією (відповідно до Прюмської угоди) у 2012 році зафіксовано 52507 збігів за ДНК-профілями (для порівняння, 84 збіги ДНК-профілів каналами Інтерполу) [273, с. 153].

Особливої актуальності взаємообмін між базами даних набув у зв’язку із повномасштабним вторгненням країни-агресора на територію України. Сотні тисяч невпізнаних трупів, безвісти зниклих військових та цивільних, переміщених осіб за

межі України, відповідно, нагальна необхідність, з метою ідентифікації, звернення до сімей зниклих безвісти осіб, які наразі знаходяться за межами країни.

Зазначимо, що у січні 2024 року, Міністерством внутрішніх справ України спільно з Міжнародною комісією з питань зниклих безвісти ініційовано створення пунктів збору ДНК-профілів українців, які перебувають за кордоном (працюватимуть на базі закордонних представництв Державної міграційної служби України), які допоможуть у пошуку безвісти зниклих у період активних бойових дій.

Як слушно зазначає директор Міжнародної комісії з питань зниклих безвісти із питань систем даних і координації даних А. Різвіч: «невпізнаних тіл буде дедалі більше і перед вами постане дедалі більше проблем, для вирішення яких необхідно створити систему роботи, яка поєднуватиме збір зразків ДНК та функціонування бази даних» [199]. Відповідно такі бази потребують підвищеного технічного захисту. Згідно із Законом України «Про державну реєстрацію геномної інформації людини» від 09.07.2022 № 2391-IX «надання органам іноземних держав геномної інформації, отриманої згідно із цим Законом, можливе лише у разі, якщо ці органи та відповідний компетентний орган України можуть установити такий режим доступу до інформації, який унеможливлює розкриття інформації для інших цілей чи її розголошення в будь-який спосіб, у тому числі шляхом несанкціонованого доступу (п. 2 ст. 17)» [126; 93].

З метою посилення інформаційної безпеки інформаційних систем у 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки (далі – ENISA) [188], до повноважень якого належить аналіз поточного стану безпеки загроз та рекомендації щодо їх усунення. Крім технічних аспектів в оглядах і рекомендаціях робочої групи звертається увага і на окремі юридичні питання, пов’язані з функціонуванням баз даних ДНК. Для прикладу, «кожній європейській країні рекомендується: впровадити спеціальне законодавство щодо управління

базою даних ДНК; мати окреме законодавство щодо захисту персональних даних стосовно біологічного матеріалу та ДНК-профілів» [271].

За висновками зазначеного агентства, «не буває невразливих компаній, які можуть на 100% захистити себе від збоїв та витоків даних, але цього можна прагнути, використовуючи наступні механізми: підвищення безпеки та шифрування даних; використання приватних та гібридних хмарних інфраструктур; перевірки та покращення політик кібербезпеки» [206].

Крім того, Європейське агентство з мережевої та інформаційної безпеки наголошує на тому, що підвищити рівень інформаційної безпеки можливо не лише удосконаленням програмного забезпечення, але й забезпеченням дотримання відповідних внутрішніх правил. Серед основних вони виокремлюють: постійне дотримання працівниками технічних вимог щодо захисту інформації; підвищення професійної грамотності працівників; чіткий розподіл обов'язків та повноважень у сфері обробки персональних даних (особливо, що стосується обробки даних та передачі їх третім особам); використання персональних даних лише за вказівкою уповноваженої особи чи згідно визначених правил; захист доступу до місцезнаходження апаратного і програмного забезпечення володільця або розпорядника, включаючи здійснення перевірки авторизації доступу; забезпечення об'єктивності надання дозволу на доступ до персональних даних; регулярна перевірка системи протоколів доступу до персональних даних наглядовим органом [145, с. 98-99].

Суттєвий вплив на формування міжнародних стандартів у даному напрямі має прецедентна практика Європейського суду з прав людини. Для прикладу, розглянемо кілька рішень ЄСПЛ у частині, що стосуються:

– незаконного доступу до бази даних:

а) у справі «I. v. Finland» заявниця не змогла підтвердити факт незаконного доступу до її медичної картки з боку колег по лікарні, де вона працювала. В результаті Національний суд відхилив її позов про порушення права на захист

персональних даних. Проте ЄСПЛ ухвалив рішення про порушення ст. 8 ЄКПЛ, так як інформаційна медична система лікарні недосконала і «не дозволяє заднім числом з'ясувати, хто мав доступ до медичної картки пацієнтки, оскільки система висвітлює лише п'ять останніх консультацій, інформація про які видаляється, щойно картка повертається в архів» [195, с. 100]. Таким чином, відсутність обліку фактів щодо надання доступу до медичної документації заявниці призвело до унеможливлення встановлення особи, яка ймовірно поширила інформацію, що містилася у ній;

б) у справі «Gardel v. France», ЄСПЛ ухвалив рішення про те, що доступ до персональних даних у реєстрах можуть отримувати тільки ті публічні службовці, які несуть офіційний обов'язок зберігати конфіденційність інформації. І жодним чином ніхто інший. До того ж такий доступ здійснюється виключно із законною метою (слідство, захист населення, державна безпека тощо) [211];

в) у справі «Z проти Фінляндії» Європейський суд з прав людини визнав, що втручання не було необхідним у демократичному суспільстві, оскільки захист медичних даних має фундаментальне значення для забезпечення права на повагу до приватного і сімейного життя. Це особливо важливо у випадках, коли йдеться про інформацію про ВІЛ-інфекцію, через стигматизацію, яку вона викликає в багатьох спільнотах. Суд встановив, що надання доступу до інформації про особу заявника та стан його здоров'я, як це сталося у рішенні апеляційного суду після завершення 10-річного періоду, порушувало ст. 8 Європейської конвенції про права людини [194];

– гарантування захисту чутливої інформації:

а) у справі «Перуццо і Мартенс проти Німеччини» ЄСПЛ надав наступні пояснення: «національне законодавство повинно надавати адекватні гарантії того, що особисті дані, які зберігаються, ефективно захищені від неправомірного використання. Це особливо важливо щодо захисту особливих категорій найбільш конфіденційних даних, зокрема інформації про ДНК, яка містить генетичні ознаки

особи, що мають велике значення як для відповідної особи, так і для її родичів та членів сім'ї» [266];

б) у справі «М.С. проти Швеції» ЄСПЛ ухвалив рішення: «конфіденційність відомостей про здоров'я є основним принципом правової системи держав-учасниць. Національне законодавство повинно забезпечувати нерозголошення відомостей про стан здоров'я, якщо це не відповідає ст. 8 Конвенції» [58].

Таким чином обґрунтовано необхідність існування гарантій захисту персональних даних в сфері охорони здоров'я, закріплення яких в національному законодавстві є першочерговим для реалізації права людини на захист інформації;

– порушення умов і термінів зберігання біологічного матеріалу та ДНК-профілів:

а) у справі «S. And Marper v. the United Kingdom» заявники поскаржилися, що органи влади продовжували зберігати їхні відбитки пальців, зразки клітин та профілі ДНК навіть після закриття кримінальних справ проти них через виправдання або припинення обвинувачення. Обидва заявники просили знищити їхні відбитки пальців і зразки ДНК, але поліція відмовилася, аргументуючи це тим, що відповідно до чинного на той час закону такі профілі могли зберігатися без обмеження терміну. Заявники звернулися до суду, щоб оскаржити рішення поліції. Суд визнав, що безстрокове зберігання їхнього біологічного матеріалу та ДНК-профілів є непропорційним втручанням в особисте життя, що порушує статтю 8 Конвенції про захист прав людини [215].

Вартим уваги є те, що справа «S. and Marper v. the United Kingdom» внесла суттєві зміни у законодавство не лише Великобританії і наразі враховується при розробленні профільних законів у багатьох державах світу;

б) у справі «М.К. v. France» у заявника відібрано відбитки пальців у зв'язку із крадіжкою, надалі справу закрили. На звернення до прокурора з вимогою видалити відбитки пальців, йому відмовили (на підставі виключення його причетності до інших злочинів). Суди рішення прокурора залишили без змін (вказали на

необхідність збору повної бази для порівняння). Суд, не розглядаючи питання законності втручання, звернув увагу на наявність легітимної мети і перейшов до оцінки пропорційності втручання. У цьому контексті Суд зазначив, що цілі обробки відбитків пальців, визначені прокуратурою та судами, не були чітко прописані в законодавстві і фактично санкціонували збирання відбитків усього населення, що виявилось надмірним та непотрібним [11].

Таким чином, Суд вважав, що держава перевищила свою свободу розсуду і не забезпечила баланс між інтересами особи та суспільними інтересами. Втручання було непропорційним і не відповідало вимогам статті 8 Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [218; 11].

Наступним напрямом, який привернув нашу увагу, є «право на забуття» інформації (право, яке передбачає видалення особистих даних із загального доступу через пошукові системи, тобто посилань на ті дані, які, на її думку, можуть завдати їй шкоди) [5]. Відповідно до норм GDPR, як національне, так і міжнародне законодавство потребує суттєвого удосконалення у цьому напрямі. Слушною у контексті досліджуваного є наукова думка В. Майєр-Шенбергер, який акцентує увагу на тому, що однією з основних проблем електронної обробки та зберігання персональних даних є те, що подібним процесам не властиво «забувати», адже така характеристика притаманна лише виключно людині … [264].

Серед європейських держав «право на забуття» було започатковано у Франції, де у 2010 було прийнято Хартію про право на забуття (зведення норм для держави у сфері захисту персональних даних у мережі). Основним завданням визначено доведення до відома користувачів ймовірних ризиків при наданні доступу до персональних даних, захист даних і запровадження «права бути забутим» [26]. Для прикладу, Google виграно судовий процес із Францією перед Судом ЄС (TSUE) в Люксембурзі щодо «права бути забутим» (позов про видалення інформації зі світової мережі, а не тільки з пошукових систем країн ЄС) у 2019 році. Судом ухвалено наступне рішення – право бути забутим повинно поширюватися

виключно на версію пошукової системи в державах-членах ЄС, проте не за їх межами [5; 92].

В Італії з 2003 року діє спеціальний Кодекс із захисту персональних даних, а функції контролю за дотриманням норм покладено на державний орган. У межах італійського законодавства право на «забуття» трактується як можливість громадянина вимагати видалення з публічних архівів та новинних матеріалів біографічної інформації, яка здатна завдати шкоди його честі чи репутації [244, с. 155].

З 2018 року «право бути забутим або право на видалення інформації» закріплене у ст. 17 Загального регламенту ЄС про захист даних від № 679 «Right to erasure (right to be forgotten)» – «право на видалення (право бути забутим)» та доповнене ст. 21 «Right to object» – «право подавати заперечення». Воно застосовується виключно серед країн-членів ЄС.

Окрім GDPR, право суб'єкта персональних даних вимагати в контролера даних видалення цих відомостей закріплено в багатьох міжнародних договорах, рішеннях міжнародних організацій, проте не всі вони гарантують визнання ними права на забуття. Так, відповідно до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, «суб'єкт даних може вимагати виправлення або знищення цих відомостей, якщо їх обробляли всупереч положенням внутрішнього законодавства» [74]. Подібний підхід відображено й у Законі України «Про захист персональних даних», де у п. 6 ч. 2 ст. 8 зазначено, що суб'єкт персональних даних має право вимагати від будь-якого володільця або контролера персональних даних змінити чи знищити його дані, якщо їх обробка відбувається незаконно або дані є недостовірними [168].

Таким чином, концепція «права бути забутим» виступає засобом захисту особистих немайнових прав, забезпечуючи конфіденційність минулого та захист життєвого спокою осіб, які не прагнуть публічності. Це право поширюється на

будь-яку інформацію, що стосується приватного життя та персональних даних людини.

Підсумовуючи, ми дійшли висновку, що у міжнародному праві наразі безліч нормативно-правових актів, які регламентують захист персональних чутливих даних. Разом з цим, проблематика щодо захисту чутливих персональних даних залишається актуальною як у юридичному, так і практичному аспекті.

З метою посилення інформаційної безпеки інформаційних систем у 2004 році було створено Європейське агентство з мережевої та інформаційної безпеки, яке відповідає за аналіз поточного стану загроз безпеки та надання рекомендацій щодо їх усунення. Окрім технічних аспектів, у своїх оглядах і рекомендаціях ENISA звертає увагу на юридичні питання, пов'язані з функціонуванням баз даних ДНК. Суттєвий вплив на формування міжнародних стандартів у напрямі захисту чутливої інформації має і прецедентна практика Європейського суду з прав людини.

Теоретично обгрунтовано необхідність імплементації позитивного досвіду США (у частині щодо приватності медичної інформації, правові норми якого урегульовано Законом США про мобільність та підзвітність медичного страхування (HIPAA)); Великобританії (базові модулі для медичних інформаційних систем закуповуються за рахунок держави, а додаткові кожен медичний заклад докуповує самостійно).

Висновки до розділу 3

1. Особливістю міжнародного законодавства є те, що держава виступає гарантом захисту медичної інформації. У міжнародних нормативних актах права пацієнта формуються за трьома напрямами: універсальним, регіональним та спеціалізованим. Так, універсальні документи носять переважно декларативний

характер і слугують рекомендаціями для світової спільноти; регіональні акти, прийняті Радою Європи, мають обов'язкову силу для держав-членів; спеціалізовані нормативні документи розробляються та затверджуються організаціями, створеними для конкретних цілей у сфері охорони здоров'я.

Міжнародне правове регулювання захисту медичної інформації поділяють на три категорії: загальні норми, закріплені, зокрема, у прецедентних рішеннях Європейського суду з прав людини; спеціальні норми, що регламентують порядок захисту даних у медичній сфері; та основні норми, які визначають фундаментальні принципи інформаційної безпеки та прав пацієнта.

2. Розглянуто особливості застосування принципу необхідності та пропорційності збору персональних «чутливих» даних. Констатовано, що персональні дані, які підлягають автоматизованій обробці, зберігаються виключно у межах чітких та легітимних цілей і не використовуються у спосіб, який їм суперечить. Окреслено основні проблемні питання у даному напрямі – відсутність як мети, так і доцільності такого об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутні підстави для подальшого зберігання та обробки інформації. Проаналізовано прецедентні рішення Європейського суду з прав людини у справах «I. проти Фінляндії», «К.Н. та інші проти Словакії», «Z проти Фінляндії», «M. C. проти Швеції», «L.H. v. Latvia», «*R v. RC*», «S. and Marper v. the United Kingdom», «M.K. v. France».

3. Проаналізовано ключові положення Загального регламенту ЄС із захисту персональних даних, який замінив попередні європейські закони у цій сфері. Регламент встановлює правила обробки та вільного руху персональних даних, що застосовуються до всіх секторів, як державного, так і приватного. Встановлено, що регламент приділяє значну увагу новим викликам, що виникли у зв'язку із зростанням цифровізації у сфері охорони здоров'я, що, у свою чергу, сприятиме посиленню захисту медичної інформації. Документ передбачає високі стандарти

щодо інформованої згоди, обов’язків повідомлення, забезпечення права доступу до персональних даних про стан здоров’я, розширює права пацієнтів (зокрема право вимагати видалення інформації у контролерів та процесорів), а також встановлює посилені санкції для медичних організацій у разі порушення положень GDPR.

Визначено спільні та відмінні ознаки Загального регламенту із захисту персональних даних та Закону про мобільність та підзвітність медичного страхування «HIPAA», основна відмінність між якими полягає у тому, що HIPAA охоплює лише медичні персональні дані і поширюється на особи, які мають доступ до цієї інформації. Згідно з HIPAA, розкриття персональної медичної інформації (імена, телефонні номери, адреси, дати народження, номери соціального страхування, платіжна інформація, результати медичних тестів, медичні записи, фотографії та рентгенівські зображення) може бути здійснено без попередньої згоди пацієнта для цілей лікування. Натомість GDPR вимагає однозначної згоди пацієнта для розкриття даних про стан здоров’я, за умови, що пацієнт здатний надати таку згоду. Крім того, на відміну від GDPR, HIPAA не надає пацієнтам право вимагати видалення своїх медичних даних з медичних установ.

4. Теоретично обґрунтовано, що платформі Curogram, відповідно до HIPAA, вдалося забезпечити повну конфіденційність даних користувачів. Curogram є унікальною розробкою в сфері телемедицини, яка підтримує відеозв’язок і двосторонній обмін текстовими повідомленнями через смартфон, а також інтегрується з будь-якою системою електронних медичних архівів. Платформа допомагає медичним постачальникам автоматизувати робочі процеси, оптимізувати взаємодію між лікарями та медсестрами, покращувати координацію догляду за пацієнтами, а також швидше знаходити і контактувати з іншими медичними закладами і партнерами.

5. Встановлено, що у лютому 2021 року у США набули чинності два нормативні акти, які доповнюють HIPAA. Перший – Правило взаємодії CMS і доступу пацієнтів, що передбачає створення безпечного інтерфейсу прикладного

програмування (API), який дозволяє пацієнтам легко отримувати доступ до своїх медичних заявок. Крім того, правило вимагає від постачальників Medicare і Medicaid надсилати електронні повідомлення про госпіталізацію, виписку або переведення пацієнта до нового закладу, до постачальника послуг у громаді або до лікаря. Другий – Заключне правило Закону про лікування ONC, яке регламентує роботу IT-систем охорони здоров'я, постачальників медичних послуг та мереж обміну медичною інформацією. Правило зобов'язує системи впроваджувати стандартизовані API-інтерфейси, що дозволяють пацієнтам та їхнім лікарям отримувати електронну інформацію про стан здоров'я через мобільні додатки. Основною метою цих нормативних актів є полегшення доступу пацієнтів до їх медичних даних із дотриманням заходів безпеки та конфіденційності.

6. Найвищими міжнародними та європейськими стандартами з питань захисту інформації у автоматизованих системах є модернізована Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Загальний регламент із захисту персональних даних. Країною з найбільшими витратами на охорону здоров'я та лідером з інформатизації медичних послуг є Сполучені Штати Америки.

7. За результатами перевірок як вітчизняних, так і міжнародних медичних установ встановлено непоодинокі факти порушення норм щодо технічного захисту чутливої інформації. Серед основних порушень – відсутність як мети, так і доцільності об'ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутність підстав для подальшого зберігання та обробки інформації; порушення вимог щодо знищення медичної інформації на електронних носіях (після видалення інформації не застосовується форматування електронного носія, відповідно, за допомогою сучасного програмного забезпечення наявна можливість відновлення видалених файлів). Зазначене свідчить про неналежний рівень знань з питань технічного захисту інформації працівниками

даних установ, які відповідають за збір, обробку та передачу конфіденційної інформації.

Для посилення інформаційної безпеки в інформаційних системах у 2004 році було створене Європейське агентство з мережевої та інформаційної безпеки. Це агентство має повноваження аналізувати сучасний стан загроз безпеці та надавати рекомендації щодо їх усунення. Окрім технічних аспектів, в оглядах і рекомендаціях робочої групи також акцентується увага на юридичних питаннях, що стосуються функціонування баз даних ДНК.

За висновками Європейського агентства з мережевої та інформаційної безпеки підвищити рівень інформаційної безпеки можливо не лише удосконаленням програмного забезпечення, але й забезпеченням дотримання відповідних внутрішніх правил. Серед основних вони виокремлюють: постійне дотримання працівниками технічних вимог щодо захисту інформації; підвищення професійної грамотності працівників; чіткий розподіл обов'язків та повноважень у сфері обробки персональних даних (особливо, що стосується обробки даних та передачі їх третім особам); використання персональних даних лише за вказівкою уповноваженої особи чи згідно визначених правил; захист доступу до місцезнаходження апаратного і програмного забезпечення володільця або розпорядника, включаючи здійснення перевірки авторизації доступу; забезпечення об'єктивності надання дозволу на доступ до персональних даних; регулярна перевірка системи протоколів доступу до персональних даних наглядовим органом.

8. Теоретично доведено, що прецедентна практика Європейського суду з прав людини відіграє суттєву роль у формуванні міжнародних стандартів щодо захисту чутливої інформації. Проаналізовано рішення ЄСПЛ у таких справах, як «I. проти Фінляндії», «К.Н. та інші проти Словакії», «Z проти Фінляндії», «M. C. проти Швеції», «L.H. v. Latvia», «R v. RC», «S. and Marper v. the United Kingdom», «M.K. v. France» та інші, що дозволяє визначити ключові принципи захисту персональних і чутливих даних у міжнародному правовому полі.

9. У Європі право на забуття вперше було запроваджено у Франції, де у 2010 році ухвалено Хартію про право на забуття, що систематизувала правила захисту персональних даних в інтернеті, передбачала інформування користувачів про ризики надання доступу до їхніх даних і встановлювала механізм «право бути забутим». З 2018 року аналогічне право закріплено в статті 17 Загального регламенту ЄС із захисту персональних даних (GDPR). Крім GDPR, можливість вимагати видалення персональної інформації у контролера передбачена у численних міжнародних договорах та рішеннях міжнародних організацій, хоча повна гарантія реалізації цього права не завжди забезпечується. Обмеження дії «права на забуття» стосуються виключно даних, що належать до приватного життя та персональної інформації конкретної особи.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення й нове вирішення наукового завдання, що полягає у розкритті особливостей правового регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я. За результатами дисертаційної роботи сформульовано такі основні наукові положення, висновки та рекомендації.

1. З'ясовано особливості та стан дослідження інформаційної безпеки у медичній сфері. Сформульовано авторське визначення поняття «інформаційна безпека у сфері охорони здоров'я». Констатовано, що поняття «інформаційна безпека» має дві складові: перша – захист інформації, інформаційних ресурсів, держави, суспільства та особистості від негативного інформаційного впливу; друга – загрози інформаційної безпеки.

Теоретично обґрунтовано, що у передбачених Стратегією розвитку інформаційного суспільства напрямах подальшого розвитку «Е-медицини» не звернено увагу на належний технічний захист як автоматизованих інформаційних галузевих систем, так і взагалі медичної інформації. Відповідно, запропоновано доповнити п. 1 сфери діяльності «Е-медицина», розділу «Етапи та основні напрями реалізації» Стратегії розвитку інформаційного суспільства та викласти його у наступній редакції: «упровадження автоматизованих інформаційних систем, які

сертифіковано на відповідність КСЗІ, що надають можливість перейти до ведення медичної документації в електронному вигляді».

Надано пропозиції щодо класифікації ключових механізмів комплексної системи інформаційної безпеки у медичній сфері: правовий (юридичні норми та гарантії системи захисту інформації в МІС, які використовують медичні заклади; запобігання витокам; проведення службових розслідувань за фактами порушення інформаційної безпеки; відповідальність); технічний (забезпечення конфіденційності, цілісності та доступності інформації); комунікаційний та освітній (забезпечення доступності МІС; передбачення: обов'язкових спецкурсів, у тому числі дистанційних, з питань інформаційної безпеки при використанні МІС; щорічного підвищення кваліфікації працівників, які працюють з системами, з обов'язковим вивченням як щойно прийнятих нормативно-правових актів у даному напрямі, так і ознайомленням з позитивним міжнародним досвідом).

2. Розглянуто зміст поняття «медична інформація». Констатовано, що уперше це поняття закріплено рішенням Конституційного Суду України у справі К. Г. Устименка (30.10.1997 р.). За результатами аналізу норм вітчизняного та міжнародного законодавства, наукових поглядів правознавців розмежовано зміст понять «лікарська таємниця» та «медична інформація». Обгрунтовано думку, що ключовим критерієм поділу такої інформації є мета її збереження та використання. Звернено увагу на необхідність зведення термінологічного апарату у медичнійсфері до терміна «медична інформація». Сформульовано авторське визначення поняття «медична інформація», під яким запропоновано розуміти конфіденційну інформацію про фізичну особу, яка стала відома у процесі звертання її до медичного закладу з метою отримати допомогу (факт звернення, стан здоров'я, огляд, діагноз, результати обстеження, методи лікування), а також уся інформація, яку працівники медичних закладів одержують від пацієнта під час спілкування з ним, розголошення якої може зашкодити пацієнтові. Констатовано, що розголошення медичної

інформація можливе лише у разі, якщо її збереження зашкодить суспільству та якщо нерозголошення матиме наслідки для оточення хворого.

3. Визначено ключові об’єкти та суб’єкти забезпечення інформаційної безпеки у медичній сфері, при цьому ефективність державної політики у цій галузі залежить від діяльності саме суб’єктів інформаційної безпеки. До них належать як державні органи регіонального та місцевого рівня – Міністерство охорони здоров’я, Національна служба здоров’я України, керівники медичних закладів та уповноважені відповідних департаментів, управлінь і відділів, так і недержавні інституції та громадяни, повноваження яких охоплюють захист інформації, зокрема державне підприємство «Електронне здоров’я» та ТОВ «ТЗІ». Ефективна реалізація інформаційної політики потребує системного підходу, який передбачає чітке усвідомлення суб’єктами відповідальності за свої дії в інформаційному середовищі та дотримання належного рівня інформаційної культури. Основними об’єктами захисту визначено індивідуальні права користувачів у інформаційному просторі, інформаційні ресурси (медичні інформаційні системи та реєстри), канали обміну інформацією та телекомунікаційні мережі.

4. Проаналізовано розвиток нормативно-правового регулювання захисту інформації в медичній сфері, зокрема встановлено, що правові норми формують єдину систему законів і підзаконних актів, що регламентують як зовнішні, так і внутрішні механізми охорони даних. Національна правова база спирається на ключові міжнародні та європейські стандарти, а також практику Європейського суду з прав людини. Центральним документом у сфері захисту персональних даних, зокрема медичних, є Загальний регламент ЄС із захисту персональних даних (GDPR), який передбачає значне посилення нагляду та контролю, а також передачу права володіння медичною інформацією від лікарів та медичних закладів безпосередньо пацієнтам. Організація процесів надання, обробки та зберігання медичних даних здійснюється відповідно до Порядку функціонування електронної системи охорони здоров’я України.

Обґрунтовано думку, що міжнародне законодавство, як і вітчизняне, у виключних випадках дозволяє опрацьовувати персональні дані осіб без їх згоди, однак особливістю міжнародного законодавства є те, що держава гарантує їх інформаційний захист.

Визначено, що у деяких сферах медичної діяльності – психіатрії, де ступінь правової захищеності пацієнтів має певні особливості, не завжди можливо гарантувати дотримання захисту медичної інформації завдяки відповідним правовим нормам. Доступ до даних щодо пацієнтів, які зберігаються у медичних інформаційних системах, надається у випадку отримання згоди пацієнта чи його представника у письмовій формі або у такій формі, яка надасть можливість підтвердити надання відповідної згоди.

Теоретично обґрунтовано, що хоча обробка персональних даних без надання згоди особи потенційно може порушувати фундаментальні права та свободи людини, вітчизняне законодавство допускає її у виняткових випадках, зокрема в медичній сфері, коли обробка здійснюється з метою охорони здоров'я відповідним колом осіб. У цьому контексті Закон України № 555-IX «Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню COVID-19» потребує уточнення щодо чіткого визначення мети обробки персональних даних, пропонуючи викласти пп. 1 п. 2 розділу II у редакції: «дозволяється обробка персональних даних про стан здоров'я, місце госпіталізації або самоізоляції, прізвище, ім'я, по батькові, дату народження, місце проживання, роботи або навчання особи без її згоди, у порядку, визначеному рішенням про встановлення карантину, за умови застосування належних технічних засобів захисту, використання виключно з метою протидії поширенню COVID-19, а також за наявності у працівника, який безпосередньо здійснює обробку таких даних, обов'язку щодо їх конфіденційності та нерозголошення».

5. Окреслено ключові засади інформаційної приватності у медичній сфері та обґрунтовано, що право на захист медичної інформації виникає одночасно із

самим суб'єктивним правом, а не лише у разі його порушення. Аналіз випадків витоку медичних даних в Україні та за кордоном показав, що пандемія COVID-19 загострила низку проблем у сфері захисту медичної інформації, водночас не зменшивши витрат медичних установ на утримання штатів інформаційної безпеки.

Визначено основні проблеми електронної системи охорони здоров'я, серед яких постійне підвисання системи, недосконаліть програмного забезпечення, недостатній досвід медичних працівників у роботі з системою, відсутність належного комп'ютерного обладнання та технічного захисту даних, а також законодавча неврегульованість відмови від надання згоди на обробку персональних даних, що в комплексі створює ризики порушення інформаційної безпеки.

Проаналізовано основні норми та принципи Загального регламенту ЄС із захисту персональних даних у частині охорони медичної інформації, а на основі рішень Європейського суду з прав людини від 29.04.2017 (справа «Л.Х. проти Латвії» № 52019/07) та Верховного Суду України від 04.12.2019 (справа № 760/8719/17) зроблено висновок, що дискреційні повноваження державних органів щодо збору та зберігання персональних даних мають бути визначені виключно законом.

Надано пропозиції щодо систематизації та кодифікації національного законодавства у сфері інформаційної безпеки відповідно до європейських та міжнародних стандартів, внесення змін до Закону України «Про захист персональних даних» стосовно форм і умов надання згоди на обробку персональних даних, а також законодавчого посилення відповідальності за порушення захисту медичної інформації.

6. Досліджено основні джерела загроз для медичних інформаційних систем (МІС), окреслено їх переваги та ризики та констатовано, що МІС наразі відіграють ключову роль у забезпеченні організації охорони здоров'я. Розробниками таких систем є юридичні особи або фізичні особи-підприємці, які пройшли перевірку на сумісність із Центральною базою даних, підписали договір із адміністратором бази

(держпідприємством «Електронне здоров'я») та відповідають технічним нормам; серед найбільш відомих – Helsi, Medcard24, Moniheal, Health24.

Основними інформаційними загрозами МІС визначено: зловмисні дії; низький рівень комп'ютерної грамотності медичних працівників; порушення законодавчих норм щодо реєстрації та автентифікації користувачів; технічні збої та мережеві пошкодження; концентрацію великого обсягу медичної інформації в одній базі даних.

Для зменшення ризику пропонується впровадити досвід Естонії, де дані зберігаються у кількох базах на різних серверах із окремими системами захисту, а також розробити механізм державного контролю за дотриманням операторами МІС вимог щодо захисту медичної інформації. Аналіз угод МІС Helsi, Health24, Asker, Moniheal щодо збору, обробки, зберігання та надання доступу третім особам дозволив запропонувати законодавчо передбачити обов'язкове ознайомлення користувача перед реєстрацією із положенням системи, чітко визначити інформацію, що збирається, обробляється та використовується, та порядок її захисту.

Проаналізовано функціонування Порталу електронної системи охорони здоров'я та медичних веб-ресурсів (Itmed, Портал пацієнта, HELSI.ME), визначено проблеми, пов'язані з технічним захистом Електронного реєстру даних про генетичні ознаки людини, а також питанням надання такої інформації іноземним органам. Аргументовано, що безпечне функціонування медичних інформаційних систем потребує комплексного підходу, який інтегрує всі необхідні заходи й технології захисту даних на всіх рівнях інформаційної інфраструктури в єдину систему.

7. Визначено проблеми та окреслено перспективи вдосконалення правового забезпечення захисту інформації у медичній сфері. Теоретично обґрунтовано, що інформатизація в цій галузі повинна відбуватися з урахуванням вимог українського законодавства, Загального регламенту ЄС із захисту персональних даних,

міжнародних стандартів ISO/IEC та інших нормативних документів, що регламентують безпеку даних. Особливу увагу слід приділяти дотриманню принципів визначеної мети та мінімізації даних, збираючи та обробляючи лише ті відомості, які необхідні для реалізації конкретної мети.

Встановлено причини низького рівня упровадження медичних інформаційних систем: несумісність існуючих систем, недосконаліть інформаційної інфраструктури та інтеграції між реєстрами, низький управлінський рівень фахівців, а також недостатнє технічне забезпечення (комп'ютерна та мережеве обладнання).

Констатовано, що для ефективного функціонування електронної системи охорони здоров'я необхідна надійна система захисту інформації.

Окреслено основні напрями правового забезпечення інформаційної безпеки: відсутність спеціального нормативного акта про права пацієнтів, недостатній захист даних під час обов'язкового медичного страхування, невизначеність норм щодо обробки та зберігання медичної інформації. Аналіз Закону України «Про державну реєстрацію геномної інформації людини» виявив правову невизначеність: широкий обсяг «геномної інформації», тривалі терміни зберігання, відсутність чітких гарантій щодо втрати або витоку даних, відсутність процедур відкликання згоди на обробку, а також відсутність незалежного контролю за дотриманням законності.

Обґрунтовано, що правове забезпечення інформаційної безпеки у медичній сфері має формувати єдиний надійно захищений медичний інформаційний простір в Україні, що охоплює галузеві та регіональні бази даних, а також медико-статистичну інформацію.

8. З'ясовано особливості застосування міжнародних та європейських правових норм щодо захисту інформації у медичній сфері. Констатовано, що особливістю міжнародного законодавства є те, що держава виступає гарантом захисту медичної інформації. Права пацієнта у міжнародному законодавстві у

частині щодо захисту інформації закріплено у трьох напрямах: універсальний (акти, які носять декларативний характер і виступають, в основному, у якості рекомендацій для світової спільноти), регіональний (документи, прийняті Радою Європи, які мають обов'язковий характер) та спеціалізований (документи, які прийнято спеціально створеною організацією).

Норми міжнародного права поділяються на загальні, спеціальні та основні. Загальні норми захисту медичної інформації закріплено також в прецедентних рішеннях Європейського суду з прав людини. Основна мета документів, які регламентують діяльність у даному напрямі – спрощення доступу пацієнтів до їх медичних даних з дотриманням відповідних заходів безпеки і конфіденційності. Відповідно до норм міжнародного законодавства, особи визнаються працівниками, які надають медичні послуги лише у разі, якщо вони взяли на себе зобов'язання зберігати медичну таємницю.

Досліджено особливості правових норм Загального регламенту із захисту персональних даних, яким замінено попередні закони про захист даних у ЄС, встановлено правила обробки та вільного руху персональних даних, які застосовуються до всіх доменів публічного та приватного секторів. Констатовано, що даним документом приділено набагато більше уваги задоволенню нових вимог, що виникли з підвищенням рівня цифровізації у медичній сфері, що, як наслідок, у подальшому сприятиме посиленню захисту інформації щодо стану здоров'я; передбачено вищі стандарти стосовно інформованої згоди і обов'язків щодо повідомлення та посилення захисту права на доступ до персональних даних щодо стану здоров'я, розширено питання щодо прав пацієнтів (передбачено право вимагати від контролерів та процесорів видаляти інформацію щодо стану їх здоров'я), а також посилено для організацій охорони здоров'я санкції у разі недотримання правових норм GDPR.

Визначено спільні та відмінні ознаки Загального регламенту із захисту персональних даних та Закону про мобільність та підзвітність медичного

страхування «HIPAA». Основною відмінністю між законами GDPR і HIPAA є те, що HIPAA поширюється на збір та обробку лише медичної інформації, під його безпосередню дію потрапляє особливе коло осіб, яким надано доступ до цієї групи даних. Крім того досить важливим є те, що відповідно до HIPAA можна здійснювати розкриття PHI (медична інформація, яка ідентифікує конкретну людину – імена, телефонні номери, адреси, дати народження, номери соціального страхування, платіжну інформацію, результати аналізів, медичні записи, фотографічні зображення, результати рентген-обстеження і т.д.) в цілях лікування без попередньої згоди пацієнта, в той час як відповідно до GDPR основною підставою для розкриття даних щодо стану здоров'я є однозначна згода пацієнта (за умови, якщо пацієнт здатний свідомо надати таку згоду). Також HIPAA, на відміну від GDPR, не передбачено надання права пацієнту вимагати від закладу охорони здоров'я видалення його медичних даних.

Розглянуто особливості застосування принципу необхідності та пропорційності збору персональних «чутливих» даних. Констатовано, що персональні дані, які підлягають автоматизованій обробці, зберігаються виключно у межах чітких та легітимних цілей і не використовуються у спосіб, який їм суперечить. Окреслено основні проблемні питання у даному напрямі – відсутність як мети, так і доцільності такого об’ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутні підстави для подальшого зберігання та обробки інформації. Проаналізовано прецедентні рішення Європейського суду з прав людини у справах «I. проти Фінляндії», «K.H. та інші проти Словакії», «Z проти Фінляндії», «M. C. проти Швеції», «L.H. v. Latvia», «*R v. RC*», «S. andMarper v. theUnitedKingdom», «M.K. v. France».

Обґрунтовано, що захист медичної інформації є не просто обов'язком держави і предметом державно-правового регулювання, його необхідно розглядати у поєднанні із захистом прав людини.

9. Окреслено перспективи впровадження міжнародних та європейських стандартів захисту інформації у вітчизняне законодавство електронних систем охорони здоров’я, при цьому визначено, що ключовими нормативними актами є Загальний регламент із захисту персональних даних та модернізована Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних.

Визначено, що у більшості країн світу медичні інформаційні системи складаються з п’яти базових модулів: реєстрація пацієнта; амбулаторний менеджмент; виставлення рахунків та оброблення інформації щодо страхування пацієнта; сервісний модуль; безпековий модуль, що забезпечує контроль доступу до інформації пацієнта.

Визначено: типові порушення правових норм щодо технічного захисту медичної інформації: відсутність як мети, так і доцільності об’ємного збору даних; неврахування індивідуальних обставин осіб, чиї дані зберігаються; зміни визначеної мети обробки «чутливих даних», яка є несумісною з попередньою; відсутність підстав для подальшого зберігання та обробки інформації; порушення вимог щодо знищення медичної інформації на електронних носіях (після видалення інформації не застосовується форматування електронного носія, відповідно, за допомогою сучасного програмного забезпечення наявна можливість відновлення видалених файлів); внутрішні правила, які сприятимуть підвищенню рівня інформаційної безпеки в медичних інформаційних системах сфери охорони здоров’я: дотримання норм щодо технічного захисту інформації; підвищення професійної грамотності; використання медичної інформації відповідно до норм законодавства; належний технічний захист доступу до місцезнаходження апаратного і програмного забезпечення; постійний моніторинг дотримання порядку авторизації доступу; перевірка системи протоколів доступу до медичної інформації наглядовим чи контролюючим органом.

Проаналізовано рішення ЄСПЛ у частині щодо: незаконного доступу до бази даних («I. v. Finland», «Gardel v. France», «Z проти Фінляндії»); гарантування

захисту чутливої інформації («Перуццо і Мартенс проти Німеччини», «М.С. проти Швеції»); порушення умов і термінів зберігання біологічного матеріалу та ДНК-профілів («S. andMarper v. theUnitedKingdom», «М.К. v. France»). Вартим уваги є те, що справа «S. andMarper v. theUnitedKingdom» внесла суттєві зміни у законодавство не лише Великобританії і наразі враховується при розробленні профільних законів у багатьох державах світу;

Досліджено особливості захисту медичної інформації у:

– медичних інформаційних системах при клінічних випробуваннях (дослідження нових препаратів на пацієнтах у документально зафіксованому дослідницькому середовищі). Окреслено проблематику – порушення вимог щодо знищення медичної інформації на електронних носіях (після видалення інформації не застосовується форматування електронного носія, відповідно, за допомогою сучасного програмного забезпечення наявна можливість відновлення видалених файлів);

– загальнонаціональних системах електронних медичних записів під час взаємообміну медичною інформацією. Констатовано, що найбільш ефективними є єдині бази даних ДНК США, Великобританії, Польщі, Німеччині, Італії, Іспанії, Франції, в яких визначено одного держателя та адміністратора бази даних. З’ясовано, що на підставі Прюмського договору, країни-члени ЄС отримали як правовий механізм, так і додаткові практичні можливості щодо обміну інформацією з національними базами даних ДНК.

Розглянуто право на забуття медичної інформації, яке передбачає видалення особистих даних із загального доступу через пошукові системи. Констатовано, що відповідно до норм GDPR, як національне, так і міжнародне законодавство потребує суттєвого удосконалення у цьому напрямі.

Теоретично обґрунтовано необхідність імплементації позитивного досвіду США (у частині щодо приватності медичної інформації, правові норми якого урегульовано Законом США про мобільність та підзвітність медичного страхування

(HIPAA)); Великобританії (базові модулі для медичних інформаційних систем закуповуються за рахунок держави, а додаткові кожен медичний заклад докуповує самостійно).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Академічний тлумачний словник: словник української мови в 11 т., 1973. Т.4. С. 512.

2. Акопов В.І. До історії судової відповідальності лікарів. *Медицина.* 2001. № 10. С. 23.

3. Аналіз законодавства про захист персональних даних України. 14.09.2020. URL: https://ecpl.com.ua/wp-content/uploads.pdf.

4. Андрійчук А.С., Стрєлкіна А.А. Розроблення моделі керування доступом до приватної медичної інформації. *Радіоелектронні і комп'ютерні системи*. 2018. № 2(86). С. 26–32.

5. Андрощук Г. Суд ЄС: Google виграв спір щодо права на забуття. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/sud-es-google-vigrav-spir-shchodo-prava-na-zabuttya.html.

6. Антонов С.В. Цивільно-правова відповідальність за заподіяння шкоди здоров'ю при наданні платних медичних послуг: дис. ... канд. юрид. наук: 12.00.03. Київ, 2006. 206 с.

7. Багатомовний юридичний словник-довідник /І.О. Голубовська, В.М. Шовковий, О.М. Лефтерова та ін. К.: Київський університет, 2012. 543 с.

8. Баранов А. Інформаційний суверенітет чи інформаційна безпека? *Національна безпека і оборона.* 2001. № 1. С. 70–76.

9. Баранов О.П. Передумови створення Державної спеціальної служби транспорту та її завдання в системі національної безпеки України. *Вісник Національної академії державного управління при Президентові України.* 2014. № 3. С. 60–65.

10. Барихін А. Великий юридичний енциклопедичний словник. 2003. 720 с.

11. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних. Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с.

12. Березовська І.Р., Русак Д.М. Державна інформаційна політика та основні напрями її вдосконалення. Міжнародні відносини. Серія: «Економічні науки». Випуск 4. 2014. URL: http://journals.iir.kiev.ua/index.php/ec_n/article/view/2488.

13. Бєляков К.І. Деякі питання щодо формування реформи інформаційного законодавства України. *Систематизація законодавства в Україні: проблеми теорії і практики:* матеріали Міжнародної науково-практичної конференції. К.: Інститут законодавства Верховної Ради України, 1999. С. 253–255.

14. Бичков В.В., Коваленко О.С., Синекоп Ю.С. Телемедичні технології у медицині катастроф. *Україна. Здоров'я нації*. 2009. № 3 (11). С. 102–105.

15. Блінова Г.О. Інформаційна приватність у медичній сфері. *Юридичний вісник.* 2014. № 3. С. 136–141.

16. Булеца С.Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету.* Серія: «Право». 2014. Вип. 25. С. 56–61.

17. В омбудсмена назвали найбільшу загрозу для безпеки персональних медичних даних. URL: www.ukrinform.ua/rubric-society/3063627-v-ombudsmena-nazvali-najbilsu-zagrozu-dla-bezpeki-personalnih-medicnih-danih.html.

18. Ваші діагнози в їхніх руках: що електронні медичні сервіси роблять з персональними даними і чим це загрожує. URL: https://cedem.org.ua/analytics/elektronni-medservisy.

19. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку. URL: https://www.kmu.gov.ua/news/vymohy-do-zakhystu.

20. Висновок Міністерства юстиції України за результатами розгляду проєкту Закону України «Про внесення змін до Закону України «Про захист персональних даних». URL: https:C:/Users/Admin/Downloads/document-3071411.pdf.

21. Виявлено витік персональних даних пацієнтів у одній із приватних клінік Дніпра. URL: interfax.com.ua/news/general/692349.html.

22. Всесвітня організація охорони здоров'я. Постійне представництво України у Женеві. 2012. URL: https://geneva.mfa.gov.ua/posolstvo/2612-who.

23. Галамба М. Інформаційна безпека України: поняття, сутність та загрози. *Юридичний журнал.* URL: http://www.justinian.com.ua/article.phpid2463.

24. Гіпократ /переклад з грецьк. 1994. 736 с.

25. Головко О.М. Медіабезпека людини: засади інформаційно-правової політики: монографія. Київ: «АртЕк». 2019. 168 с.

26. Гордієнко Т. «Право на забуття» – що це таке й чому про нього варто знати? URL: https://ms.detector.media/trends/1411978127.

27. Гревцова Р.Ю. Актуальні правові питання здійснення лікарської діяльності. URL: http://health-ua.com/articles/2247.html.

28. Громико І., Саханчук Т., Зіновьєв О. Державна домінантність визначення інформаційної безпеки України в умовах протидії загрозам. *Право України*. 2008. № 8. С. 130–134.

29. Данильян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: навчальний посібник. Х.: Фоліо, 2002. 285 с.

30. Дванадцять принципів організації охорони здоров'я для будь-якої національної системи охорони здоров'я. 01.10.1963. Всесвітня медична асоціація. URL: http://zakon3.rada.gov.ua/laws/show/990.

31. Дворніченко А.С. Правові підстави та умови регулювання розголошення медичної таємниці. *Юридичний часопис Національної академії внутрішніх справ.* 2014. № 2. С. 174–184.

32. Декларація про політику в галузі дотримання прав пацієнта в Європі, прийнята на Європейській консультативній нараді ВООЗ від 28.06.1994 р. URL: www.who.int/genomics/public/eu_declaration1994.pdf.

33. Декларація про політику у напрямі забезпечення прав пацієнта у Європі. Європейська нарада по правах пацієнта, Амстердам, Нідерланди, березень 1994 р. URL: https://med.sumdu.edu.ua/images/content.pdf.

34. Демченко І.С. Інформація про стан здоров'я у контексті права на повагу до приватного життя: міжнародно-правовий аспект. *Альманах міжнародного права.* Випуск 15. С. 41–50.

35. Деякі питання електронної системи охорони здоров'я: постанова Кабінету Міністрів України від 25.04.2018 р. № 411. *Офіційний вісник України*. 2018. № 46. Ст. 1604. URL: https://zakon.rada.gov.ua/laws/show/411-2018-п.

36. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія. Київ, 2015. 388 с.

37. Довгань О.Д. Правові засади формування і розвитку системи забезпечення інформаційної безпеки України. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3(19). С. 6–17.

38. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. Київ: ДП «УкрНДНЦ», 2019. 76 с.

39. Електронна система охорони здоров'я «E-Health»: те, що мають знати лікарі та пацієнти.

URL: https://www.google.com/search?q=health+24+%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0&rlz=1C1GGRV_enUA903UA903&oq=Health24&aqs=chrome.3.69i59j69i57j0i10l3j0j0i10j69i61.4220j0j4&sourceid=chrome&ie=UTF-8.

40. Електронне урядування та демократія: навчальний посібник у 15 ч. Ч. 13. Київ. 2017. С.19.

41. Етичний кодекс лікаря України від 27.09.2009 р. URL: https://zakon.rada.gov.ua/rada/show/n0001748-09.

42. Європейська комісія (2012). Пропозиція щодо Регламенту Європейського парламенту і Ради (ЄС) щодо клінічних випробувань лікарських засобів для вживання людьми і скасування Директиви 2001/20/ЕС, COM(2012) 369 остаточна версія, Брюссель, 17 липня 2012 р.

43. Європейська хартія прав пацієнтів, прийнята Активною громадською мережею у співпраці з громадськими організаціями з 12 різних країн ЄС від 15.11.2002 р. URL: http://meduniv.lviv.ua/files/press-centre/2014/n180414/evropejska_hartiya_prav_pacientiv.pdf.

44. Жарков Я. Небезпеки особистості в інформаційному просторі. Розділ І. Аналітика. Інформаційна безпека. «Юстініан». 2007. № 2. URL: http://www.justinian.com.ua/ article.php?id=2554.

45. Женевська декларація: міжнар. док. від 01.09.1948. Всесвітня медична асоціація. URL: http://zakon3.rada.gov.ua/laws/show/990_001.

46. Заварза Т.В. Проблеми збереження лікарської таємниці. *Медичне право України: проблеми становлення та розвитку:* матеріали І Всеукраїнської науково-практичної конференції (м. Львів, 19-20 квітня 2007 р.). Львів. С. 139–142.

47. Загальний регламент Європейського Парламенту і Ради (ЄС) «Про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС» від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

48. Загальний регламент із захисту персональних даних Європейського Союзу (GDPR) № 2018/1725. URL: http://aphd.ua/gdpr-ofitsiinyi-ukranskyi-pereklad.

49. Загородній А.Г. Нова обчислювальна технологія для науки. 2005. 106 с.

50. Зайцев В.В. Суб'єкти забезпечення інформаційної безпеки України. *Форум права.* 2013. Випуск 3. С. 231–238.

51. Заключне правило Закону про лікування ONC. URL: https://www.healthit.gov/curesrule.

52. Закон про мобільність та підзвітність медичного страхування. URL: Xippahttps://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha.

53. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. *Науковий вісник*. Серія: «Філософія». Харків: ХНПУ, 2017. Вип. 48. Ч. 1. С. 214.

54. Захист медичних даних пацієнтів США. URL: https://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha.

55. Захист персональних даних осіб, що беруть участь в клінічних випробуваннях лікарських засобів. URL: https://uba.ua/ukr/news/1844.

56. Захист персональних даних у сфері охорони здоров'я в ЄС. 2021. URL: http://medosvita.info/2021/05/09.

57. Захист персональних даних у сфері охорони здоров'я в ЄС: законодавчий ландшафт. Аптека. 07.12.2020 № 47 (1268). URL: https://www.apteka.ua/article/575210.

58. Захист права на здоров'я у Європейському суді з прав людини. URL: https://ukrainepravo.com/international_law/european_court_of_human-prava-na-zdorov-ya-u-evropeys%60komu-sudi-z-prav-lyudyny.

59. Здоров'я та Європейська конвенція з прав людини (справа Л.Л. проти Франції від 10.10.2006 № 7508/02). URL: https://www.coe.int/en/web/help-country/-/zdorov-a-ta-evropejs-ka-konvencia-z-prav-ludini

60. Зеленський В. Держава та суспільство мають усвідомити всі загрози інформаційній безпеці та знайти шляхи для протидії їм: виступ на Всеукраїнському

форумі «Україна 30. Культура, медіа, туризм» 09.03.2021 р. URL: https://www.president.gov.ua/news/derzhava-ta-suspilstvo-mayut-usvidomiti-vsi-zagrozi-informac-67001.

61. Зіменковський А.Б. Медична інформація як об'єкт стандартизації на сучасному етапі реформування галузі охорони здоров'я України. *Вісник наукових досліджень*. 2003. № 4. С. 8–10.

62. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: АртЕк, 2018. 446 с.

63. Зустріч Петра Порошенка з членами Національної Ради з питань телебачення та радіомовлення. URL: http://www.president.gov.ua/news/prezident-zustrivsya.

64. Інформаційний бюлетень про функціональну сумісність та доступ до інформації для пацієнтів. URL: https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index.

65. Інструкція про порядок заповнення листка непрацездатності: спільний наказ Міністерства охорони здоров’я України, Міністерства праці та соціальної політики України, Фонду соціального страхування з тимчасової втрати працездатності, Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань України від 03.11.2004 р. № 532/274/136-ос/1406532. URL: http://kras-centr.pmsd.org.ua/wp-content/uploads/2019/08/instruktsiyi-pro-poryadok-zapovnennya-lysta-nepratsezdatnostii.pdf.

66. Інформаційна безпека України: глосарій /Л.С. Харченко, Н.А. Ліпкан, О.В. Логінов; заг. ред. Р.А. Калюжного. К., 2004. 135 с.

67. Інформаційна та кібербезпека: соціотехнічний аспект: підручник /В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. К.: ДУТ, 2015. 288 с.

68. Кирильчук Є.О. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції. *Наукові праці МАУП*. 2013. Вип. 1. С. 89–95.

69. Кірнос Н.В. Права пацієнта в Україні: методичні рекомендації. Новосанжарське районне управління юстиції (смт. Нові Санжари), 2013. 19 с.

70. Клятва Лоренс Найтінгейл. URL: http://www.medbrat.

71. Князєв С.О. Витік інформації: сучасні світові тенденції: матеріали II Міжнародної науково-практичної конференції (м. Одеса, 24-25 травня 2019 р.). Одеса. С. 54. URL: https://novaosvita.com/wp-content/uploads/2019/05/ModTrSc-Odesa-May2019.pdf.

72. COVID-19 роздав 3,5 млн. персональних даних. URL: https://www.comnews.ru/content/208448/2020-08-05/2020-w32/covid-19.

73. Коментар до проєкту Закону України «Про захист прав пацієнтів» від 06.12.2007 р. № 1132, внесений народним депутатом України Ю. Каракаєм. URL: https://ips.ligazakon.net/document/LF0VG00A?an=2.

74. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. *Офіційний вісник України.* 14.01.2011 р. № 58. Ст. 85.

75. Конвенція про захист прав і гідності людини щодо застосування біології та медицини від 04.04.1997 р. URL: http://zakon2.rada.gov.ua/laws/show/994_334.

76. Конвенція про захист прав людини і основних свобод від 04.11.1950 р. (ратифікована Законом України від 17.07.1997 р. № 475/97-ВР). URL: zakon.rada.gov.ua/laws/show/995_004#Text.

77. Конституційне подання Уповноваженого Верховної Ради України з прав людини до Конституційного Суду України від 06.11.2017 р. № 1-2499/17-107. URL:https://ccu.gov.ua/sites/default/files/kp_redacted.pdf.

78. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. № 30. Ст. 43. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

79. Концепція інформатизації охорони здоров'я України. URL: https://vikisoft.kiev.ua.

80. Концепція інформаційної безпеки України: проєкт. Міністерство інформаційної політики України. 2015. URL: http://mip.gov.ua/done_img/d/30-project_08_06_15. pdf.

81. Концепція про захист прав людини і основоположних свобод від 04.11.1950 (ратифікована 17.07.1997 № 475/97-ВР). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

82. Концепція 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-р#Text.

83. Концепція розвитку цифрових компетентностей: розпорядження Кабінету Міністрів України від 03.03.2021 № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text.

84. Корж І.Ф. Внутрішні фактори загроз і викликів інформаційній безпеці України. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти:* матеріали наук.-практ. конф. Київ: НТУУ «КПІ імені Ігоря Сікорського», 2016. 204 с.

85. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук: 12.00.07. Нац. ун-т внутр. справ. Х., 2004. 42 с.

86. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: дис. ... д-ра юрид. наук: 12.00.07. Нац. ун-т внутр. справ. Х., 2004. 472 с.

87. Котерлін І.Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми вітчизняної юриспруденції.* 2022. № 1. С. 150.

88. Кримінальний кодекс України. *Відомості Верховної Ради України*. 2001. № 25-26. Ст.131.

89. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. URL: http://gska2.rada.gov.ua.

90. Ларіна Р.Р., Владзимирський А.В., Балуєва О.В. Державний механізм забезпечення інформатизації системи охорони здоров'я: монографія /за заг. ред. В.В. Дорофієнко. Донецьк, 2008. 252 с.

91. Легка О.В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. *Правова позиція*. 2021. № 2 (31).С. 74–79.

92. Легка О.В. Імплементація міжнародних стандартів щодо захисту права на доступ до інформації в Україні. *Правова позиція*. 2023. № 2 (39).

93. Легка О.В. Правова регламентація реєстрації геномної інформації людини: міжнародний та вітчизняний досвід. *Науковий вісник Ужгородського національного університету.* Серія: «Право». 2022. Ч. 2 № 72. С. 71–76.

94. Лікар з Вінниці Світлана Побережець відстояла в суді право кожного громадянина на приватність. Українська Гельсінська спілка з прав людини. URL: https://helsinki.org.ua/articles/likar-z-vinnytsi-svitlana-poberezhets-vidstoyala-v-sudi-pravo-kozhnoho-hromadyanyna-na-pryvatnist.

95. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.

96. Лісабонська декларація стосовно прав пацієнта: міжнар. док. від 01.10.1981 р. Всесвітня медична асоціація. URL: http://zakon3.rada.gov.ua/laws/show/990_016.

97. Лісница О. Права пацієнтів у міжнародних документах і національному законодавстві України. *Knowledge, Education, Law, Management 2020 № 4 (32), vol. 2. P. 70.*

98. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: навчальний посібник. Одеса, 2015. 264 с.

99. Лопатін В.М. Правова охорона та захист права на таємницю. 1999. № 7. С. 36.

100. Лугіна Н.А., Горбань С.Ю. Морально-правові аспекти лікарської таємниці в Україні: перспективи та способи вдосконалення. *Юридичний науковий електронний журнал*. 2020. № 3. С. 323–326.

101. Людський фактор і сором. У мережі з'явились особисті дані громадян, інфікованих коронавірусом. URL: https://www.currenttime.tv/a/koronavirus-utechka-moskva/30992104.html.

102. Марущак А.І. Правове регулювання відносин щодо лікарської таємниці в Україні. *Юридичний радник.* 2007. №3(17). С. 12–18.

103. Марценюк О.Г. Права фізичних і юридичних осіб на медичну конфіденційну інформацію. Медичне право України: правовий статус пацієнтів України та його законодавче забезпечення: матеріали II Всеукраїнської конференції (м. Львів, 17–18 квітня 2008 р.). С. 166–171.

104. Медична реформа: перевірка на відповідність Конституції. URL: https://www.umj.com.ua/article/159084/medichna-reforma-perevirka-na-vidpovidnist-konstitutsiyi.

105. Медичне законодавство: правова регламентація лікарської діяльності: підручник /М.В. Банчук, В.Ф. Москаленко, Б.В. Михайличенко та ін.; за ред. В.Ф. Москаленка, Б.В. Михайличенка. Київ, 2012. Кн. 2. 494 с.

106. Медичний портал ItMed. URL: https://itmed.org/doctors/ua/kiev.

107. Миколайчук Б. Ваші діагнози в їхніх руках: що електронні сервіси роблять з персональними даними і чим це загрожує. URL: https://netfreedom.org.ua/article/vashi-diagnozi.

108. Міжнародний кодекс медичної етики: міжнар. док. від 01.10.1949 р. Всесвітня медична асоціація. URL: http://zakon4.rada.gov.ua/laws/show/990_002.

109. Міжнародна клятва лікаря: Женевська декларація, прийнята Генеральною асамблеєю Всесвітньої медичної асоціації у 1948 році. URL: https://medicine.karazin.ua/student-life/klyatva-ta-prisyaga-likarya.

110. Мужанова Т.М. Інформаційна безпека держави: навчальний посібник. К., 2019. 131 с.

111. Науково-практичний коментар Кримінального кодексу України. /за ред. М. Мельника, М. Хавронюка. 3-є вид. К.: Атіка, 2003. 1056 с.

112. Науково-практичний коментар Кримінального кодексу України /за ред. М.І. Мельника, М.І. Хавронюка. 4-те вид. К.: Юрид. думка, 2007. 1184 с.

113. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Гельветика, 2017. 168 с.

114. Негодченко В.О. Адміністративно-правове забезпечення державної інформаційної політики органами Національної поліції України: автореф. дис. ... д-ра юрид. наук: 12.00.07. Харків, 2017. 40 с.

115. Негодченко В.О. Суб'єкти інформаційної політики в Україні. *Європейські перспективи*. 2016. № 2. С. 54.

116. Негодченко О.В. Медична та лікарська таємниці як гаранти інформаційної приватності. *Адміністративне право та адміністративна діяльність.* 2013. № 2. С. 41–48.

117. Нижник Н.Р. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник /Н.Р. Нижник, Г.П. Ситник, В.Т. Білоус. Ірпінь, 2000. 304 с.

118. Облік ДНК в умовах воєнного стану та ризики під час обробки. URL: https://zib.com.ua/ua/153699.html.

119. Олійченко І.М. Інформаційне забезпечення управління обласною державною адміністрацією. URL: http://www.dridu.dp.ua/zbirnik/2011-01(5)/11oimoda.pdf.

120. Основи законодавства України про загальнообов'язкове державне соціальне страхування: Закон України від 14.01.1998 р. № 16/98-ВР (у редакції від 31.03.2023). URL: https://zakon.rada.gov.ua/laws/show/16/98-вр#Text.

121. Основи законодавства України про охорону здоров’я: Закон України від 19.11.1992 р. № 2801-XII (у редакції від 01.01.2024). *Відомості Верховної Ради України*. 1993. № 4. Ст. 19. URL: http://zakon.rada.gov.ua/laws/show/2801-12.

122. Офіційний сайт Deloitte. URL: https://www2.deloitte.com/uk/en/legal/about-deloitte.html.

123. Офіційний сайт European Commission. URL: https://ec.europa.eu/commission/index_en.

124. Охорона здоров’я в Україні. URL: https://uk.wikipedia.org/wiki/Охорона_здоров%27я_в_Україні.

125. Панченко О.А. Інформаційні технології у забезпеченні державної безпеки. RS Global. 2020. № 5(32). June. P. 32.

126. Парламент прийняв Закон України «Про державну реєстрацію геномної інформації людини». URL: https://www.kmu.gov.ua/news/parlament-pryiniav-zakon-pro-derzhavnu-reiestratsiiu-henomnoi-informatsii-liudyny.

127. Перун Т. Загальна характеристика правовідносин у сфері забезпечення інформаційної безпеки в Україні. URL: https://cyberleninka.ru/article/n/zagalna-harakteristika-pravovidnosin-u-sferi-zabezpechennya-informatsiynoyi-bezpeki-v-ukrayini.

128. Перший штраф за невиконання порядку адміністративного рішення. URL: https://uodo.gov.pl/pl/138/1889.

129. Питання діяльності Міністерства інформаційної політики України: постанова Кабінету Міністрів України від 14.01.2015 р. № 2. URL: http://zakon5.rada.gov.ua/laws/show/2- 2015-%D0%BF.

130. Погребняк А.В. Технології комп'ютерної безпеки: монографія. Рівне: МЕГУ, 2011. 117 с.

131. Положення про використання комп'ютерів в медицині: міжнар. док. від 01.10.1973. Всесвітня медична асоціація. URL: http://zakon5.rada.gov.ua/laws/show/990_010.

132. Положення про захист прав та конфіденційність пацієнта: міжнар. док. від 01.10.1993 р. Всесвітня медична асоціація. URL: http://zakon2.rada.gov.ua/laws/show/990_056.

133. Пономаренко В.М., Майоров О.Ю., Кальниш В.В., Олинін М.В. Інформаційні технології в системі охорони здоров'я. *Панорама охорони здоров'я населення України*. К.: Здоров'я, 2003. С. 335–341.

134. Пономаренко І.С. Актуальні питання захисту персональних даних у сфері охорони здоров'я. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали науково-практичної конференції (м. Київ, 10 грудня 2020 р.). м. Київ: Фенікс, 2020. 272 с.

135. Пономаренко І.С. Актуальні питання правового регулювання захисту інформації у сфері охорони здоров'я. *Науковий вісник Міжнародного гуманітарного університету*. Серія: «Юриспруденція». 2021 № 53. С. 55–58. DOI https://doi.org/10.32841/2307-1745.2021.53.11.

136. Пономаренко І.С. Основні аспекти правового регулювання відповідальності за порушення прав інтелектуальної власності. *Науковий вісник публічного та приватного права.* 2020. Вип. 1. С. 227–231. DOI https://doi.org/10.32844/2618-1258.2020.1.39.

137. Пономаренко І.С. Особливості захисту інформації в електронній системі охорони здоров'я. *Роль і місце інформаційного права і права*

інтелектуальної власності в сучасних умовах. Креативні індустрії: матеріали III Всеукраїнської науково-практичної конференції (м. Київ, 11 листопада 2021 р.). м. Київ, 2021. 327 с. С. 235–243.

138. Пономаренко І.С. Особливості правового захисту інформації у Сполучених Штатах Америки. *Актуальні проблеми правових наук в євроінтеграційному вимірі*: матеріали Міжнародної науково-практичної конференції (м. Харків, 18-19 грудня 2020 р.). Харків: ГО «Асоціація аспірантів-юристів», 2020. 116 с. С. 61–67.

139. Пономаренко І.С. Правове регулювання захисту персональних даних у медичній сфері: вітчизняний та міжнародний досвід. *Право і суспільство*. 2020. № 6. Ч. 2. С. 120–125. DOI https://doi.org/10.32842/2078-3736/2020.6.2.2.18.

140. Пономаренко І.С., Гуз А.М. Міжнародна та вітчизняна практика впровадження медичних інформаційних систем. *Наукові записки Міжнародного гуманітарного університету*. 2022. Вип. 36. С. 26–30.

141. Пономаренко І.С., Тугарова О.К. Проблемні питання організації захисту інформації в медичних інформаційних системах. *Актуальні проблеми управління інформаційною безпекою держави:* матеріали XV Всеукраїнської науково-практичної конференції (м. Київ, 27 березня 2024 р.). м. Київ, 2024. Ч. 1. С. 685–689.

142. Попова Е.Г. Конфлікти у лікувально-профілактичних установах: причини, умови, соціальні наслідки: автореф. дис. … канд. мед. наук. 2005. 20 с.

143. Портал пацієнта. URL: https://medportal.ua.

144. Порядок функціонування електронної системи охорони здоров’я: постанова Кабінету Міністрів України від 25.04.2018 р. № 411. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-elektronnoyi-sistemi-ohoroni-zdorovya.

145. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.

146. Постанова Верховного Суду у складі колегії суддів Третьої судової палати Касаційного цивільного суду від 04.12.2019 (справа № 760/8719/17 провадження № 61-9359св19). URL: https://protocol.ua/ru/vs_ktss_fizichna_osoba_mae_pravo_na_taemnitsyu_pro_stan_svogo_zdorov_ya_fakt_zvernennya_za_medichnoyu_dopomogoyu_diagnoz_a_takog_pro_vidomosti_odergani_pri_ii_medichnomu_obstegenni_(vs_ktss_sprava_760_8719_17_04_12_19).

147. Прав Р.Ю. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України. *Державне управління: удосконалення і розвиток.* URL: http://www.dy.nayka.com.ua/pdf/9_2018/103.pdf.

148. Правило взаємодії CMS і доступу пацієнтів. URL: https://iapp.org/news/a/health-care-interoperability-preparing-to-meet-new-privacy-and-security-obligations.

149. Право на приватність: conditio sineguanon. Харків: Фоліо, 2003. 216 с.

150. Правовий аналіз проєкту Концепції інформаційної безпеки України. Організація з безпеки та співробітництва в Європі. Бюро Представника ОБСЄ з питань свободи ЗМІ. Липень 2015. URL: https://www.osce.org/uk/fom/175046.

151. Правовий режим лікарської таємниці. URL: https://www.google.com/search.

152. Преамбула Декларації ООН прав дитини від 20.11.1959. URL: https://chl.kiev.ua/default.aspx?id=331.

153. Присяжнюк М. Інформаційна безпека України в сучасних умовах /М. Присяжнюк, Я. Бєлошевич. *Вісник Київського національного університету імені Тараса Шевченка.* Серія: «Військові-спеціальні науки». 2013. Вип. 30. С. 42.

154. ПРО HELSI. URL: https://helsi.me/about.

155. Про безпеку та якість донорської крові та компонентів крові: Закон України від 30.09.2020 р. № 931-IX (із змінами). URL: https://zakon.rada.gov.ua/laws/show/931-20.

156. Про внесення змін до Закону України «Про захист населення від інфекційних хвороб» щодо запобігання поширенню коронавірусної хвороби (COVID-19)»: Закон України від 13.04.2020 р. № 555-IX. *Відомості Верховної Ради України*. 2020. № 19. Ст. 127. URL: https://zakon.rada.gov.ua/laws/show/555-20#Text.

157. Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19.10.2017 р. № 2168-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2168-19.

158. Про державну реєстрацію геномної інформації людини: Закон України від 09.07.2022 № 2391-IX. URL: https://zakon.rada.gov.ua/laws/show/2391-20#Text.

159. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 р. № 3475. URL: http://zakon5.rada.gov.ua/laws/show/3475-15.

160. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314. URL: zakon.rada.gov.ua/laws/show/2939-17#Text.

161. Про застосування трансплантації анатомічних матеріалів людині: Закон України від 17.08.2018 р. № 2427-VIII (у редакції від 07.01.2022 р.). *Відомості Верховної Ради* (ВВР). 2018. № 28. Ст. 232.

162. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

163. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року: розпорядження Кабінету Міністрів України від 30.03.2023 р. № 272-р. URL: https://ips.ligazakon.net/document/KR230272.

164. Про затвердження Порядку проведення судово-психіатричної експертизи: наказ Міністерства охорони здоров'я від 08.05.2018 р. № 865. URL: https://zakon.rada.gov.ua/laws/show/z0719-18#Text.

165. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: директива Європейського Парламенту і Ради ЄС від 24.10.1995 р. № 95/46/ЄС. URL: https://zakon.rada.gov.ua/laws/show/994_242#Text.

166. Про заходи для високого рівня безпеки мережевих та інформаційних систем на території Союзу: директива Європейського Парламенту і Ради ЄС від 06.07.2016 р. № 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/984_013-16#Text.

167. Про захист населення від інфекційних хвороб: Закон України від 06.04.2000 р. № 1645-III. *Відомості Верховної Ради України (ВВР)*. 2000. № 29. Ст. 228.URL: http://zakon.rada.gov.ua/laws/show/145-14.

168. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України (ВВР*). 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

169. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживання ними: Закон України від 15.02.1995 р. № 63/95-ВР. URL: http://zakon.rada.gov.ua.

170. Про інфекційну безпеку донорської крові та її компонентів: наказ Міністерства охорони здоров'я від 01.08.2005 р. № 385. *Офіційний вісник України*. 2005. № 34. С. 292.

171. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

172. Про Клятву лікаря: Указ Президента України від 15.06.1992 р. № 349. URL: http://zakon.rada.gov.ua/laws/show/349/92.

173. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. *Відомості Верховної Ради*. 1998. № 27-28. Ст. 182.

174. Про ліцензування певних видів господарської діяльності: Закон України від 01.06.2000р. № 1775-III. *Відомості Верховної Ради України*. 2000. № 36. Ст. 299.

175. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355.

176. Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text.

177. Про основні засади забезпечення кібербезпеки України: Закон України від 08.07.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19/conv.

178. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text.

179. Про прокуратуру: Закон України від 14.10.2014 р. № 1697-VIII. URL: https://zakon.rada.gov.ua/laws/show/1697-18#Text.

180. Про протидію захворюванню на туберкульоз: Закон України від 05.07.2001 р. № 2586-III. *Відомості Верховної Ради України. 2001*. № 49. Ст. 258. URL: https://zakon.rada.gov.ua/laws/show/2586-14.

181. Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ: Закон України від 12.12.1991 р. № 1972-XII. *Відомості Верховної Ради України.* 1992. № 11. Ст. 152. URL: https://zakon.rada.gov.ua/laws/show/1972-12.

182. Про психіатричну допомогу: Закон України від 22.02.2000 р. № 1489-III (у редакції від 20.12.2018). *Відомості Верховної Ради України*. 2000. № 19. Ст. 143. URL: https://zakon.rada.gov.ua/laws/show/1489-14#Text.

183. Про Стратегію кібербезпеки України: рішення Ради національної безпеки і оборони України від 14.05.2021 року №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.

184. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження Кабінету Міністрів України від 20.09.2017 р. № 649-р. *Урядовий кур'єр*. 2017. № 181.

185. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації: розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. *Урядовий кур'єр*. 2018. № 88.

186. Проєкт Концепції інформаційної безпеки України від 09.06.2015 р. URL: https://www.osce.org/files/f/documents/0/2/175056.pdf.

187. Радзішевська Є.Б., Висоцька О.В. Інформаційні технології в медицині. E-health / за ред. В. Г. Книгавка. Харків: ХНМУ, 2019. 72 с.

188. Регламент (ЄС) № 460/2004 Європейського парламенту та Ради від 10.03.2004 р. щодо створення Європейського агентства з мережевої та інформаційної безпеки, OJ. 2004. L 77.

189. Рекомендації CM/Rec (2019) 2 Ради Європи щодо захисту медичних даних. URL: https://rm.coe.int/cm-rec-2019-sexism-ukr-rev-ps-no-track-changes-fin-with-content-al/1680953cb8.

190. Рекомендації № R (2000) 5 Комітету міністрів Ради Європи. URL: http://www.dridu.dp.ua/cpk/Lib/5/Rekomend_poved_DS.pdf.

191. Рекомендація щодо охорони здоров'я працівників на місцях роботи № 97 Генеральної конференції Міжнародної організації права від 04.06.1953 р. URL: https://zakon.rada.gov.ua/laws/show/993_071#Text.

192. Рішення Конституційного Суду України у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» від 30.10.1997 р. № 5-зп. URL: https://zakon.rada.gov.ua/laws/show/v005p710-97.

193. Рішення Великої палати ЄСПЛ у справі «Gillbergv. Sweden» від 03.04.2012 р. §82-97 URL: https://cedem.org.ua/articles/pravo-na-dostup-do-informatsiyi-evolyutsiya-pidhodiv-yevropejskogo-sudu-z-prav-lyudyny.

194. Рішення Європейського суду з прав людини у справі «Z проти Фінляндії» від 25.01.1997 р. № 22009/93. URL:http://medicallaw.org.ua/fileadmin/user_upload/pdf/Z_against_Finland.pdf.

195. Рішення ЄСПЛ у справі «Gillbergv. Sweden» від 02.11.2010 р. §120-127. URL: https://zakonbase.ru/content/base/186728/?print=1.

196. Рішення ЄСПЛ у справі «I. проти Фінляндії» (I. v. Finland), № 20511/03 від 17 липня 2008 р. URL: file:///C:/Users/User/Downloads/CASE%20OF%20C.%20v.%20FINLAND%20-%20[Ukrainian%20Translation]%20(1).pdf.

197. Рішення Канадського Верховного Суду у справі «R v. RC». URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1146800.

198. Роз’яснення Міністерства охорони здоров’я щодо заповнення декларації. URL: https://moz.gov.ua/article/for-medical-staff/jak-medikam-pracjuvati-z-personalnimi-danimi-pacientiv.

199. Салліван К. Країна зниклих безвісти. Забезпечення правосуддя і правди для родин зниклих безвісти в Україні. URL: https://www.ukrinform.ua/rubric-presshall/3748633-prezentacia-knigi-kraina-zniklih-bezvisti.html.

200. Свобода інформації: навчальний посібник для державних службовців /пер. з англ. Р. Тополевського. К.: Тютюкін, 2010. 128 с.

201. Сенюта І.Я. Вважаю за необхідне розробити й прийняти Медичний кодекс України. URL: https://yur-gazeta.com/interview/vvazhayu-za-neobhidne-rozrobiti-y-priynyati-medichniy-kodeks-ukrayini.html.

202. Симоненко О. Державна реєстрація геномної інформації людини: користь та небезпека. *Громадська думка про правотворення*. 2023. №1. URL: https://protocol.ua/ua/v_ukraini_zapochatkovano_bazu_genomnoi_informatsii_ludi ni_shcho_vidomo.

203. Система державних суб'єктів забезпечення інформаційної безпеки України та шляхи її вдосконалення.

URL: https://pidru4niki.com/1501092237031/politologiya/sistema_derzhavnih_subyekti v_zabezpechennya_informatsiynoyi_bezpeki_ukrayini_shlyahi_vdoskonalennya.

204. Ситник Г.П. Національна безпека України: теорія і практика: навчальний посібник /Г.П. Ситник, В.М. Олуйко, М.П. Вавринчук. Київ: Кондор, 2007. 616 с.

205. Сімейний кодекс України від 10.01.2002 р. № 2947-III. URL: https://zakon.rada.gov.ua/laws/show/2947-14.

206. Скільки втрачає бізнес через виток даних? Звіт IBM 2021. URL: https://denovo.ua/blog/vitok-danyh-v-2021-ibm.

207. Слабкий Г.О., Качур О.Ю., Кривенко Є.М. Методологія вивчення рівня впровадження інформатизації в систему охорони здоров'я України: метод. рекомендації. Київ, 2014. 20 с.

208. Словник іншомовних слів. URL: https://www.jnsm.com.ua/cgi-bin/u/book/sis.pl?Qry=%EE%E1%27%BA%EA%F2.

209. Словник української мови: в 11 томах. Т. 5. 1974. С. 495. Т. 9. 1978. С. 814.

210. Смолькова І.В. Таємниця: поняття, види, правовий захист. 1998. С. 66.

211. Справа «Гардель проти Франції» (заява № 16428/05). URL: file:///C:/Users/Admin/Downloads/CASE.pdf.

212. Справа «Пантелеєнко проти України» (заява № 11901/02): рішення ЄСПЛ від 29.06.2006. URL: https://zakon.rada.gov.ua/laws/show/974_274#Text.

213. Справа «I. v. Finland». Judgement ECHR, applicationno. 20511/03. Strasbourg, 17 July2008 URL: http://hudoc.echr.coe.int/eng?i=001-87510.

214. Справа «K.H. and Others v. Slovakia». Judgement ECHR, applicationno. 32881/04.// Strasbourg, 28 April 2009.

215. Справа «S. and Marperv. The United Kingdom» (заяви №№ 30562/04 та 30566/04). URL: http://privacy.khpg.org/1604922641.

216. Справа «Z v. Finland». Judgement ECHR, applicationno. 22009/93. Strasbourg, 25 February1997. URL: http://hudoc.echr.coe.int/eng?i=001-58033.

217. Справа «Л.Л. проти Франції» (заява № 7508/02): рішення ЄСПЛ від 10.10.2006. URL: https://unba.org.ua/publications/1262-praktika-espl-faktichni-dani-zdorov-ya.html.

218. Справа «M.K. v. France». URL: http://www.nsj.gov.ua/files/1529653122Рішення%20ЄСПЛ%20тест%20ВККСУ_ОНОВЛЕНЕ_червень_ОК_20.06_ост.pdf.

219. Степанюк Р.Л., Кікінчук В.В. Напрями вдосконалення правового регулювання криміналістичного ДНК-аналізу в Україні в контексті інтеграції до Європейського Союзу. *Вісник ХНУВС.* 2022. № 2 (97). С. 234-249. DOI: https://doi.org/10.32631/v.2022.2.21.

220. Стеценко С.Г. Медичне право України: підручник. 2008. URL:http://pidruchniki.com/13761025/pravo/medichni.

221. Стеценко С.Г., Стеценко В.Ю., Сенюта І.Я. Медичне право України: підручник /за ред. С.Г. Стеценка. К.: Правова єдність, 2008. 507 с.

222. Стеценко С.Г., Шатковська І.В. Медичне право України (правове забезпечення лікарської таємниці): монографія. К.: Атіка, 2010. 144 с.

223. Стоєцький О. Суб'єкти забезпечення інформаційної безпеки України: адміністративно-правові засади. *Інформаційне право*. 2009. № 11. С. 161–164.

224. Стратегія інформаційної безпеки: указ Президента України від 28.12.2021 № 685/2021 «Про рішення Ради національної безпеки і оборони України від 15.10.2021». URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14.

225. Стратегія національної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/392/2020?find=1&text=

226. Стратегія розвитку інформаційного суспільства в Україні: розпорядження Кабінету Міністрів України від 15.05.2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text.

227. Тер-Акопов А.А. Безпека людини: теоретичні основи соціально-правової концепції. 1998. 196 с.

228. Терешко Х.Я. Види інформації як об'єкта цивільних правовідносин у сфері медичного обслуговування. *Медичне право*. 2019. № 1 (23). С. 65–73.

229. Терешко Х.Я. Інформація як об’єкт цивільних правовідносин у сфері медичного обслуговування: дис. … канд. юрид. наук: 12.00.03. Київ, 2019. 240 с.

230. Терешко Х.Я. Права пацієнтів за умов запровадження електронної системи охорони здоров’я: деякі проблеми дотримання. *Доктрина медичного права*. 2018. С. 50–57. URL: https://doi.org/10.25040/medicallaw2018.02.050.

231. Терешко Х.Я. Право на медичну інформацію: деякі аспекти. *Доктрина медичного права*. Спеціальний випуск. 2017. №3. С. 125–131.

232. Технічні вимоги до електронної медичної інформаційної системи для її підключення до центральної бази даних електронної системи охорони здоров’я: наказ Національної служби здоров’я України від 05.11.2021 р. № 527 «Про внесення змін до наказу Національної служби здоров’я України від 06.02.2019 № 28». URL: ehealth.gov.ua/wp-content/uploads/2021/11/Tehnichni-vymogy-v-redaktsii-nakazu-NSZU-527-vid-05.11.2021.pdf.

233. Тихомиров О.О., Тугарова О.К. Юридична відповідальність за правопорушення в інформаційній сфері: навчальний посібник. К.: Нац. акад. СБУ, 2015. 172 с.

234. Ткачук Т.Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. … д-ра юрид. наук: 12.00.07. ДВНЗ «Ужгородський національний університет», Ужгород, 2019. 487 с.

235. Ткачук Т.Ю., Пономаренко І.С. Правове регулювання інформаційної приватності у медичній сфері України та США. *Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції*: матеріали Всеукраїнської науково-практичної конференції (м. Київ, 29 квітня 2021 р.). м. Київ: КПІ ім. Ігоря Сікорського, 2021. 192 с. С. 164–167.

236. Торяник В.М. Інформаційна безпека як складова національної безпеки держави. Роль ЗМІ у забезпеченні інформаційного суверенітету України. *Право і суспільство*. 2016. № 2. С. 151–155.

237. Трофименко О., Дубовой Я., Логінова Н., Прокоп Ю., Задерейко О. Аналіз проблем забезпечення кібербезпеки медичних комп'ютерних систем. *Захист інформації*. Т. 23. 2021. № 1. Січень-березень. С. 30-39.

238. Турчак А.В. Механізми забезпечення інформаційної безпеки як складової державної безпеки України: дис. … канд.. юрид. наук: 25.00.02. К., 2020. 229 с. С. 22.

239. У Бразилії у відкритий доступ потрапили дані 16 000000 пацієнтів з COVID-19. URL: https://xakep.ru/2020/11/27/covid-leak.

240. Угода про вільний доступ і порядок обміну відкритою науково-технічною інформацією держав-учасниць СНД від 11.09.1998 р. № 997_889. URL: https://zakon.rada.gov.ua/laws/show/997_889.

241. Удалова Л.Д., Кузьмічова-Кисленко Є.В. Лікарська таємниця в кримінальному процесі: монографія. К.: Центр учбової літератури. 2015. 134 с.

242. Устінов О.В. Електронна система охорони здоров'я відкрита для реєстрації лікарів і пацієнтів. URL: https://www.umj.com.ua/article114387.

243. У 4 міліарди доларів оцінено збитки за витік інформації у сфері охорони здоров'я. URL: blackbookmarketresearch.newswire.com/news/healthcare-data-breaches-costs-industry-4-billion-by-years-end-2020-21027640.

244. Федоришина І. С. «Право бути забутим» в системі інформаційних прав: міжнародний та вітчизняний досвід регулювання. *Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: філософсько-правові та прикладні аспекти*: матеріали круглого столу (м. Вінниця, 12 травня 2017 р.). Вінниця. 2017. С. 151–159.

245. Федченко Д.І. Система забезпечення кібербезпеки: проблеми формування та ефективної діяльності. *Молодий вчений*. Випуск 5 (57). 2017. С. 653–658.

246. Філософський енциклопедичний словник: енциклопедія. НАН України, Ін-т філософії ім. Г.С. Сковороди /за ред. В.І. Шинкарук. Київ: Абрис, 2002. 742 с.

247. Фулей Т.І., О.М. Кучів. Право на повагу до приватного і сімейного життя: ключові рішення ЄСПЛ щодо України. URL: http://www.nsj.gov.ua/files/1588588140156207.pdf.

248. Хомицький А.Р. Теоретико-методичні засади проєктування Інтернет-порталу «Науково-інформаційний реабілітаційний хаб». Національний авіаційний університет. Київ, 2022. 86 с.

249. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV (у редакції від 30.01.2024). *Відомості Верховної Ради України*. 2003. № 40. Ст. 356.

250. Цимбалюк В. Окремі питання щодо визначення категорії «інформаційна безпека» у нормативно-правовому аспекті. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. *Науково-технічний збірник.* К., 2004. С. 30–33.

251. Щирба М.Ю. Правовий статус пацієнтів: теоретико-правове дослідження: дис.. … д-ра юрид. наук: 12.00.01. Луцьк. 2020. 519 с. С. 143-144.

252. Що таке коди медичних даних? URL: https://blog.h24.ua/uk/kody-mkh-10.

253. Щодо зменшення обсягу функціональних можливостей МІС «HealthTech» та «Дніпро-МТ». URL: https://ehealth.gov.ua/2022/12/21/shhodo-zmenshennya-obsyagu-funktsionalnyh-mozhlyvostej-mis-healthtech-ta-dnipro-mt.

254. Щорічна доповідь Уповноваженого Верховної Ради з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні. 2020. URL: https://reyestr.court.gov.ua/ Review/91509417.

255. Юдін О.К, Богуш В.М. Інформаційна безпека держави Харків: Консум, 2004. 508 с.

256. Які дані становлять медичну таємницю. URL: https://moz.gov.ua/article/health/pacient-mae-pravo-scho-treba-znati-pro-pravo-na-medichnu-taemnicju.

257. Яковенко О.О. Концепція інформаційної безпеки України в контексті становлення соціально відповідальної журналістики. URL: file:///D:/%D0%9D%D0%95%20%D0%A2%D0%A0%D0%9E%D0%93%D0%90%D0%A2%D0%AC!/Downloads/Nzizh_2016_63_9.pdf.

258. Ясінська Я.О., Куперштейн Л.М. Розробка політики інформаційної безпеки медичного закладу. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/31280/%d0%a2%d0%b5%d0%b7%d0%b8_%d0%af%d1%81%d1%96%d0%bd%d1%81%d1%8c%d0%ba%d0%b0.pdf?sequence=1&isAllowed=y.

259. Achieving Confidentiality in Electronic Health Records using Cloud Systems. URL: IJCNIS-V10-N1-3.pdf (mecs-press.org).

260. Amsatou SOW SIDIBE «Le sekret medicalau jourdhui». URL: http/afrilex.u-bordeaux4.fr/sites.pdf.

261. Analysis of blok chainte chnology recommendations to beapplied to medical record data storage applications. URL: IJIEEB-V12-N6-2.pdf (mecs-press.org).

262. Arifkhodzhaieva T., Ponomarenko I. Economic policy of the state in conditions of informatization of health care in Ukraine as an integral part of the social sphere. *Baltic Journal of Economic Studies.* 2021 Vol. 7, No 5. P. 228–234.

263. Chae Y. M. Going abroad of Korean health information systems. *Healthcare Informatics Research*. 2014. N. 20 (3). P. 161–162.

264. Cofone I.N. The right to be forgotten a Canadian and comparative perspective. Routledge, Taylor & Francis Group, 2020. 130 p.

265. Curogram: a web-baseds msapp for medical practices. URL: www.curogram.com.

266. Decision the European Court of Human Rights «Antonio Peruzzo against Germany and Uwe Martens against Germany» (Applications nos. 7841/08 and 57900/12). 4 June 2013. URL: https://hudoc.echr.coe.

267. FTC Gives final approval to settlement with emergency travel services provider related to allegations it failed to secure sensitive data. URL: https://www.ftc.gov/news-events/press-releases/2021/02/ftc-gives-final-approval.

268. Health care system technology using smart phone sand web apps (Case Study Iraqi Environment). URL: Article (mecs-press.org).

269. Marchese V., Cerri N., Caenazzo L. Italian national Forensic Dna database in an European perspective. *Forensic Science International: Genetics Supplement Series*. 2013. № 4(1). URL: https://doi.org/10.1016/j.fsigss.2013.10.126.

270. Misery of Ransomware Hits Hospitals the Hardest. URL: threatpost.com/ransomware-hits-hospitals-ha rdest/162096.

271. NA database management review and recommendations. ENFSI DNA Working Group April 2019 // ENFSI/ URL: https://enfsi.eu/wp-content/uploads/2021/09/2019.pdf.

272. Ryu S., Park M., Lee J., Kim S.-S. at al. Web-Based integrated public healthcare information system of Korea: Development and Performance. *Health care Informatics Research*. 2013. N. 19 (4). P. 314–323.

273. Soleto M.H., Fiodorova A. DNA and law enforcement in the European Union: tools and human rights

274. Takabayashi K., Doi S., Suzuki S. Japanese EMRs and IT in Medicine: Expansion, Integration, and Reuse of Data. *Healthcare Informatics Research*. 2011. N 17 (3). P. 178–183.

275. Tuckson R.V., Edmunds M., Hodgkins M.L. Telehealth. The new england journal of medicine. 2017. Vol. 377, N. 16. P. 1585–1592.

276. U.S. Department of Health & Human services, HIPAA privacy rules for the protection of Healt hand Mental health information. URL: https://www.omh.ny.gov/omhweb/russian/hipaa/phi_protection.pdf.

ДОДАТКИ

Додаток «А»

«ЗАТВЕРДЖУЮ»

Ректор
Університету митної справи та фінансів
Д.О. Бочаров

«10» 10 2025 р.

АКТ
про впровадження у навчальний процес Університету митної справи та фінансів основних результатів дисертації Пономаренко Ірини Сергіївни на тему «Правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я» на здобуття наукового ступеня доктора філософії за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право

Комісія у складі: проректора з навчальної роботи, к.ю.н., доцента Є.В. Гармаша (голова), директора ННІ права та міжнародно-правових відносин, д.ю.н., професора В.В. Ліпинського, завідувачки кафедри публічного та приватного права д.ю.н., професора Т.П. Мінки, уклала цей акт про те, що основні результати дисертації Пономаренко Ірини Сергіївни на тему «Правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я» використовуються у навчальному процесі Університету митної справи та фінансів, зокрема:

– при підготовці навчально-методичних комплексів з дисциплін «Адміністративне право», «Адміністративна діяльність органів публічної адміністрації»;

– при викладанні лекцій навчальної дисципліни «Адміністративне право» за темами: «Суб'єкти адміністративного права», та «Публічне адміністрування в соціально-культурній сфері»;

– при викладанні лекцій навчальної дисципліни «Адміністративна діяльність публічної адміністрації» за темами: «Контрольно-наглядові провадження», «Ліцензійно-дозвільні провадження», «Провадження за

зверненнями громадян» та «Забезпечення законності в діяльності публічної адміністрації»;

– для підготовки відповідних підрозділів навчальних матеріалів із курсів «Адміністративне право України», «Адміністративна діяльність публічної адміністрації» та при розробці навчальних посібників, підручників з адміністративно-правової тематики та публічного адміністрування тощо.

Проректор з навчальної роботи
Університету митної справи та фінансів,
к.ю.н., доцент Є.В. Гармаш

Директор ННІ права та міжнародно-правових відносин
Університету митної справи та фінансів,
д.ю.н., професор В.В. Ліпинський

Завідувачка кафедри
публічного та приватного права
Університету митної справи та фінансів,
д.ю.н., професор Т.П. Мінка

«ЗАТВЕРДЖУЮ»
Ректор
Університету митної справи та фінансів,
Д.О. Бочаров
«02» 10 2025 р.

АКТ
про впровадження у науково-дослідну діяльність Університету митної справи та фінансів основних результатів дисертації Пономаренко Ірини Сергіївни на тему «Правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я» на здобуття наукового ступеня доктора філософії за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право

Комісія у складі: проректора з наукової роботи Університету митної справи та фінансів, д.ю.н., професора Д.В. Приймаченка (голова), керівника навчально-наукового центру, к.н. з держ. упр., доцента О.О. Марценюк, завідувачки кафедри публічного та приватного права, д.ю.н., професора Т.П. Мінки, уклала цей акт про те, що основні результати дослідження Пономаренко Ірини Сергіївни на тему «Правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я» на здобуття наукового ступеня доктора філософії за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право», використовуються у науково-дослідній діяльності Університету митної справи та фінансів, а саме: у процесі наукового дослідження за науково-дослідною темою кафедри публічного та приватного права «Адміністративно-правове регулювання публічних відносин» (№ державної реєстрації 0119U100014).

До кафедри публічного та приватного права було подано матеріали для ознайомлення та подальшого використання, у яких викладено основні положення дисертації Пономаренко І.С., зокрема:

1. **Пономаренко І.С.** Основні аспекти правового регулювання відповідальності за порушення прав інтелектуальної власності. *Науковий вісник публічного та приватного права.* 2020. Вип. 1. С. 227–231. DOI: https://doi.org/10.32844/2618-1258.2020.1.39.
2. **Пономаренко І.С.** Правове регулювання захисту персональних даних у медичній сфері: вітчизняний та міжнародний досвід. *Право і суспільство*. 2020. № 6. Ч. 2. С. 120–125. DOI: https://doi.org/10.32842/2078-3736/2020.6.2.2.18.

3. **Arifkhodzhaieva T., Ponomarenko I.** Economic policy of the state in conditions of informatization of health care in Ukraine as an integral part of the social sphere. *Baltic Journal of Economic Studies.* 2021 Vol. 7, No 5. P. 228–234. DOI: https://doi.org/10.30525/2256-0742/2021-7-5-228-234.

4. **Пономаренко І.С.** Актуальні питання правового регулювання захисту інформації у сфері охорони здоров'я. *Науковий вісник Міжнародного гуманітарного університету.* Серія: «Юриспруденція». 2021 № 53. С. 55–58. DOI: https://doi.org/10.32841/2307-1745.2021.53.11.

5. **Пономаренко І.С., Гуз А.М.** Міжнародна та вітчизняна практика впровадження медичних інформаційних систем. *Наукові записки Міжнародного гуманітарного університету: збірник.* Одеса: «Гельветика». 2022. *Вип. 36. 244 с.* С. 26–30. URL: http://www.sci-notes.mgu.od.ua/archive/v36/36_2022.pdf.

6. **Пономаренко І.С.** Актуальні питання захисту персональних даних у сфері охорони здоров'я. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали науково-практичної конференції (м. Київ, 10 грудня 2020 р.). м. Київ: Фенікс, 2020. 272 с.

7. **Пономаренко І.С**. Особливості правового захисту інформації у Сполучених Штатах Америки. *Актуальні проблеми правових наук в євроінтеграційному вимірі*: матеріали Міжнародної науково-практичної конференції (м. Харків, 18-19 грудня 2020 р.). Харків: ГО «Асоціація аспірантів-юристів», 2020. 116 с. С. 61–67.

8. **Пономаренко І.С., Ткачук Т.Ю.** Правове регулювання інформаційної приватності у медичній сфері України та США. *Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції*: матеріали *Всеукраїнської науково-практичної конференції* (м. Київ, 29 квітня 2021 р.). м. Київ: КПІ ім. Ігоря Сікорського, 2021. 192 с. С. 164–167.

9. **Пономаренко І.С.** Особливості захисту інформації в електронній системі охорони здоров'я. *Роль і місце інформаційного права і права інтелектуальної власності в сучасних умовах. Креативні індустрії*: матеріали *III Всеукраїнської науково-практичної конференції* (м. Київ, 11 листопада 2021 р.). м. Київ, 2021. 327 с. С. 235–243.

10. **Пономаренко І.С., Тугарова О.К.** Проблемні питання організації захисту інформації в медичних інформаційних системах. *Актуальні проблеми управління інформаційною безпекою держави:* матеріали XV Всеукраїнської науково-практичної конференції *(м. Київ, 27 березня 2024 р.).* м. Київ, 2024. Ч. 1. С. 685–689.

Комісія вважає, що результати дисертаційного дослідження Пономаренко Ірини Сергіївни на тему «Правове регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я», є актуальними, науково обґрунтованими та такими, що вдосконалюють концептуальні засади

подальшого розвитку сучасної доктрини адміністративно-правової науки та теорії публічного адміністрування й сприяють подальшому удосконаленню механізму правового регулювання в обраній сфері.

Проректор з наукової роботи
Університету митної справи та фінансів,
д.ю.н., професор Д.В. Приймаченко

Керівник навчально-наукового центру,
Університету митної справи та фінансів,
к.н. з держ. упр., доцент О.О. Марценюк

Завідувачка кафедри
публічного та приватного права
Університету митної справи та фінансів,
д.ю.н., професор Т.П. Мінка

Додаток «Б»

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації

1. Пономаренко І.С. Основні аспекти правового регулювання відповідальності за порушення прав інтелектуальної власності. *Науковий вісник публічного та приватного права.* 2020. Вип. 1. С. 227–231. DOI: https://doi.org/10.32844/2618-1258.2020.1.39.

2. Пономаренко І.С. Правове регулювання захисту персональних даних у медичній сфері: вітчизняний та міжнародний досвід. *Право і суспільство*. 2020. № 6. Ч. 2. С. 120–125. DOI: https://doi.org/10.32842/2078-3736/2020.6.2.2.18.

3. Arifkhodzhaieva T., Ponomarenko I. Economic policy of the state in conditions of informatization of health care in Ukraine as an integral part of the social sphere. *Baltic Journal of Economic Studies.* 2021 Vol. 7, No 5. P. 228–234. DOI: https://doi.org/10.30525/2256-0742/2021-7-5-228-234.

4. Пономаренко І.С. Актуальні питання правового регулювання захисту інформації у сфері охорони здоров'я. *Науковий вісник Міжнародного гуманітарного університету.* Серія: «Юриспруденція». 2021 № 53. С. 55–58. DOI: https://doi.org/10.32841/2307-1745.2021.53.11.

5. Пономаренко І.С., Гуз А.М. Міжнародна та вітчизняна практика впровадження медичних інформаційних систем. *Наукові записки Міжнародного гуманітарного університету.* 2022. Вип. 36. С. 26–30.

Наукові праці, які засвідчують апробацію матеріалів дисертації

6. Пономаренко І.С. Актуальні питання захисту персональних даних у сфері охорони здоров'я. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання*: матеріали науково-практичної конференції (м. Київ, 10 грудня 2020 р.). м. Київ: Фенікс, 2020. 272 с.

7. Пономаренко І.С. Особливості правового захисту інформації у Сполучених Штатах Америки. *Актуальні проблеми правових наук в євроінтеграційному вимірі*: матеріали Міжнародної науково-практичної конференції (м. Харків, 18-19 грудня 2020 р.). Харків: ГО «Асоціація аспірантів-юристів», 2020. 116 с. С. 61–67.

8. Ткачук Т.Ю., Пономаренко І.С. Правове регулювання інформаційної приватності у медичній сфері України та США. *Інтернет речей: теоретико-правові та практичні аспекти впровадження в умовах Європейської інтеграції*: матеріали *Всеукраїнської науково-практичної конференції* (м. Київ, 29 квітня 2021 р.). м. Київ: КПІ ім. Ігоря Сікорського, 2021. 192 с. С. 164–167.

9. Пономаренко І.С. Особливості захисту інформації в електронній системі охорони здоров'я. *Роль і місце інформаційного права і права інтелектуальної власності в сучасних умовах. Креативні індустрії*: матеріали *III Всеукраїнської науково-практичної конференції* (м. Київ, 11 листопада 2021 р.). м. Київ, 2021. 327 с. С. 235–243.

10. Пономаренко І.С., Тугарова О.К. Проблемні питання організації захисту інформації в медичних інформаційних системах. *Актуальні проблеми управління інформаційною безпекою держави:* матеріали XV Всеукраїнської науково-практичної конференції *(м. Київ, 27 березня 2024 р.).* м. Київ, 2024. Ч. 1. С. 685–689.

Додаток «В»

Шановний колего!

У зв’язку з проведенням наукового дослідження щодо правового регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров’я, просимо Вас взяти участь в соціологічному опитуванні, що проводиться з метою підготовки рекомендацій по вдосконаленню її правового регулювання.

Анкета анонімна. Результати, отримані під час анкетування, будуть використовуватися в узагальненому вигляді лише з науковою метою.

1. Ваша освіта?

– вища;

– середня професійна;

– загальна середня.

2. Стаж роботи?

– від 5 до 10 років;

– від 10 до 20 років;

– до 5 років.

3. Ваша оцінка стану нормативно-правового забезпечення?

– відмінно;

– добре;

– потребує удосконалення;

– незадовільно.

4. Чи дотримано правовими нормами вітчизняного законодавства, на Вашу думку, вимоги Загального регламенту із захисту персональних даних?

– так;

– ні;

– потребують доопрацювання.

5. Чи відповідають норми Закону України «Про державну реєстрацію геномної інформації людини» переліку підстав обробки «чутливих» категорій персональних даних особи, визначених пп. 1, 7 ч. 2 ст. 7 Закону України «Про захист персональних даних»?

– так;

– ні;

– важко відповісти.

6. Чи потребує, на Вашу думку, удосконалення Закон України «Про державні фінансові гарантії медичного обслуговування населення» у частині, що стосується функціонування електронної системи охорони здоров'я?

– так;

– ні;

– важко відповісти.

7. Чи ефективно здійснюється контроль та нагляд з питань безпеки медичної інформації в Україні?

– ефективно;

– неефективно (поясніть, чому);

– важко відповісти.

8. Чи відповідає чинне законодавство у досліджуваному напрямі міжнародним зобов'язанням та стандартам щодо інформаційної безпеки людини у сфері охорони здоров'я?

– так;

– ні;

– важко відповісти.

9. Чи є ефективною безпека медичної інформації під час дії у країні правового режиму воєнного стану?

– так;

– ні;

– потребує удосконалення.

10. Чи забезпечуються органами державної влади правові та організаційні умови для належного застосування механізмів інформаційної безпеки під час дії у країні правового режиму воєнного стану?

– так;

– ні;

– важко відповісти.

11. На Ваш погляд, недостатній контроль з боку органів державної влади з питань інформаційної безпеки у медичній сфері пов'язаний з?

– прогалинами у чинному законодавстві;

– низьким рівнем відповідальності працівників медичної сфери;

– відсутністю належного законодавчо передбаченого механізму контролю.

12. На Ваш погляд, які основні проблемні питання інформаційної безпеки у сфері охорони здоров'я?

– протиріччя технічних можливостей інформаційних систем та загроз щодо їх використання;

– відсутність належного рівня інформаційної культури як серед працівників медичної сфери, так і суспільства загалом.

13. Чи підтримуєте Ви думку про необхідність розроблення та затвердження єдиного нормативно-правового акта, який на законодавчому рівні врегулював би збір, обробку, захист та передачу медичної інформації, за прикладом GDPR?

– так;

– ні.

14. Чи мали місце у Вашому житті чи житті Ваших знайомих факти порушення інформаційної безпеки у медичній сфері у частині, що стосується відсутності як мети, так і доцільності збору медичної інформації**?**

– так;

– ні.

15. Визначте, які основні напрями правового забезпечення інформаційної безпеки у сфері охорони здоров'я:

– систематизація законодавства; удосконалення вимог щодо програмного забезпечення, сертифікації, технічного захисту інформації та вимог щодо забезпечення медичних закладів комп'ютерним устаткуванням, яке відповідає вимогам міжнародних стандартів;

– удосконалення питань щодо організаційного та кадрового забезпечення інформатизації сфери охорони здоров'я (підвищення рівня цифрової грамотності

працівників медичної сфери (курси підвищення кваліфікації, семінари, круглі столи));

– перехід до загальноприйнятих у міжнародній практиці методів збору, обробки та захисту інформації, а також подальший розвиток міжнародного співробітництва.

ЩИРО ВДЯЧНІ ЗА СПІВПРАЦЮ!

Аналітична довідка
за результатами опитування

Під час опитування нами було поставлено за мету виявити проблематику правового регулювання забезпечення інформаційної безпеки людини у сфері охорони здоров'я, окреслити перспективи подальшого удосконалення даного напряму, визначити ефективність наявної нормативно-правової бази.

Анкета складалася із 15 запитань. Запитання в анкеті підготовлено таким чином, щоб отримати оптимальну інформацію за вищезазначеними позиціями.

Зокрема, нами було опитано 165 респондентів: 67 – у Київській, 64 –у Дніпропетровській, 34 – у Запорізькій областях.

Більше 70% опитуваних мають вищу освіту, 23% – середню професійну та 7% загальну середню.

Стаж роботи від 5 до 10 років мають 20%, 26% – від 10 до 20 років; 54% – до 5 років.

Стан нормативно-правового забезпечення оцінюють на відмінно – 17%, добре – 37%, потребує удосконалення – 31%, незадовільно – 15%.

На запитання «Чи дотримано правовими нормами вітчизняного законодавства, на Вашу думку, вимоги Загального регламенту із захисту персональних даних»? 46% респондентів відповіли так, 54% – ні. Практично аналогічні відповіді і щодо запитань про удосконалення Закону України «Про державні фінансові гарантії медичного обслуговування населення»? 40% респондентів відповіли так, 52% – ні, 8% – важко відповісти.

Наступне питання, «Чи відповідають норми Закону України «Про державну реєстрацію геномної інформації людини» переліку підстав обробки «чутливих» категорій персональних даних особи, визначених пп. 1, 7 ч. 2 ст. 7 Закону України «Про захист персональних даних»?, сприяло розумінню того, що рівень обізнаності

респондентів у даному контексті потребує чекати кращого. Відповідь так надали 21%, ні – 26%, важко відповісти – 53%.

Разом з тим, на запитання «Чи ефективно здійснюється контроль та нагляд з питань безпеки медичної інформації в Україні?» 41% відповіли так, 35% – ні, 24% – важко відповісти.

На питання «Чи відповідає чинне законодавство у досліджуваному напрямі міжнародним зобов'язанням та стандартам?» 35% відповіли так, 40% – ні, 25% – важко відповісти.

Цікавим є варіант відповіді на запитання «Чи є ефективною безпека медичної інформації під час дії у країні правового режиму воєнного стану?
Відповідь так надали – 43%, ні – 57%.

На запитання «Чи забезпечуються органами державної влади правові та організаційні умови для належного застосування механізмів інформаційної безпеки під час дії у країні правового режиму воєнного стану?» 33% респондентів вважають так, 51% – ні, 16% – важко відповісти.

Недостатній контроль з боку органів державної влади з питань інформаційної безпеки у медичній сфері, на думку респондентів, пов'язаний з прогалинами у чинному законодавстві – 38%, низьким рівнем відповідальності працівників медичної сфери – 32%, відсутністю належного законодавчо передбаченого механізму контролю – 30%.

Серед основних проблемних питань інформаційної безпеки у сфері охорони здоров’я респонденти виокремлюють: протиріччя технічних можливостей інформаційних систем та загроз щодо їх використання – 58%; відсутність належного рівня інформаційної культури як серед працівників медичної сфери, так і суспільства загалом – 42%.

81% опитаних підтримують думку про необхідність розроблення та затвердження єдиного нормативно-правового акта, який на законодавчому рівні

врегулював би збір, обробку, захист та передачу медичної інформації, за прикладом GDPR, 19% – ні.

На запитання «Чи мали місце у Вашому житті чи житті Ваших знайомих факти порушення інформаційної безпеки у медичній сфері у частині, що стосується відсутності як мети, так і доцільності збору медичної інформації?», 69% відповіли ні, 31% так.

Цікавою є думка респондентів, 46% яких до основного напряму правового забезпечення інформаційної безпеки у сфері охорони здоров'я відносять систематизацію законодавства; удосконалення вимог щодо програмного забезпечення, сертифікацію, технічний захист інформації та вимоги щодо забезпечення медичних закладів комп'ютерним устаткуванням, яке відповідає вимогам міжнародних стандартів; 34% – перехід до загальноприйнятих у міжнародній практиці методів збору, обробки та захисту інформації, а також подальший розвиток міжнародного співробітництва; 20% – удосконалення питань щодо організаційного та кадрового забезпечення інформатизації сфери охорони здоров'я (підвищення рівня цифрової грамотності працівників медичної сфери (курси підвищення кваліфікації, семінари, круглі столи).