УДК 342.5
DOI https://doi.org/10.32782/2524-0374/2025-1/69

ІНФОРМАЦІЙНА БЕЗПЕКА ЕЛЕКТРОННИХ СИСТЕМ ОХОРОНИ ЗДОРОВ'Я: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ

INFORMATION SECURITY OF ELECTRONIC HEALTH SYSTEMS: THEORETICAL AND PRACTICAL ASPECTS

Кобрусєва Є.А., д.ю.н., доцент,
професор кафедри адміністративного і кримінального права
Дніпровський національний університет імені Олеся Гончара

У статті теоретично обґрунтовано, що в умовах дії в Україні правового режиму воєнного стану, все більшої актуальності набуває питання як подальшої цифровізації даного напряму, так і, відповідно, належного технічного її захисту, з урахуванням дотримання міжнародних стандартів у частині щодо захисту інформації в медичних інформаційних системах, так як циркуляція великих обсягів «чутливих» даних як про пацієнтів, так і про медпрацівників створила уразливе середовище для кібератак. Констатовано, що відповідно до законодавчих вітчизняних та міжнародних норм, національні медичні асоціації повинні використовувати всі можливі заходи для забезпечення таємниці, захищеності і конфіденційності інформації, яка стосується їх пацієнтів і зберігається в інформаційних системах. Проаналізовано основні законодавчі та нормативно-правові акти, які ухвалено останнім часом з метою покращення ефективності діяльності у даному напрямі. Виокремлено причини порушень інформаційної безпеки МІС – витік інформації, втрата даних та несанкціонована модифікація даних, а також напрями ІБ МІС – конфіденційність, цілісність, доступність. Досліджено особливості сумісності та взаємодії між медичними електронними ресурсами. Здійснено детальний аналіз: проблемних напрямів, окреслених Концепцією розвитку електронної охорони здоров'я; законопроєктів № 8153 «Про захист персональних даних», та № 6177 «Про створення незалежного контролюючого органу з питань захисту персональних даних». Розглянуто особливості роботи ЕСОЗ. Обґрунтовано основні напрями щодо покращення ефективності захисту медичної інформації у МІС. Звернено увагу на актуальність міжнародного медичного партнерства у даному напрямі.

Ключові слова: захист інформації, медична інформація, МІС, ЕСОЗ, нормативно-правові акти, транскордонний обмін медичними даними.

The article theoretically substantiates that under the conditions of the martial law legal regime in Ukraine, the issue of both further digitalization of this area and, accordingly, its proper technical protection, taking into account compliance with international standards in terms of information protection in medical information systems, is becoming increasingly relevant, since the circulation of large volumes of "sensitive" data about both patients and healthcare workers has created a vulnerable environment for cyberattacks. It is stated that in accordance with domestic and international legislative norms, national medical associations must use all possible measures to ensure the secrecy, security and confidentiality of information concerning their patients and stored in information systems. The main legislative and regulatory acts that have been adopted recently in order to improve the effectiveness of activities in this area are analyzed. The causes of information security violations in the MIS are identified – information leakage, data loss and unauthorized data modification, as well as the areas of IS MIS – confidentiality, integrity, availability. The features of compatibility and interaction between medical electronic resources are studied. A detailed analysis is carried out: problem areas outlined by the Concept of e-Health Development; draft laws No. 8153 "On Personal Data Protection" and No. 6177 "On the Creation of an Independent Supervisory Body for Personal Data Protection". The features of the work of the MIS are considered. The main areas for improving the effectiveness of medical information protection in the MIS are substantiated. Attention is drawn to the relevance of international medical partnership in this area.

Key words: information protection, medical information, MIS, ESOZ, regulatory legal acts, cross-border exchange of medical data.

Вступ. На сьогодні, з урахуванням триваючої реформи медичної сфери, а також дії в Україні правового режиму воєнного стану, все більшої актуальності набуває питання як подальшої цифровізації даного напряму, так і, відповідно, належного технічного її захисту, адже відповідно до Стратегії національної безпеки України, затвердженої указом Президента України 14.09.2020 року № 392/2020, «безпека людини – безпека країни» [1]. Головним постулатом прийнятої у 2021 році Стратегії інформаційної безпеки є саме комплексна взаємодія на основі Конституції України, законів України, Стратегії національної безпеки України, Стратегії кібербезпеки України, міжнародних договорів, згоду на обов'язковість яких надано Верховною Радою України [2]. «Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави», – визначено Стратегією інформаційної безпеки [3].

Цифрова трансформація сфери охорони здоров'я уможливила надання дистанційних медичних послуг, передачу медичних даних між пацієнтами та постачальниками медичних послуг, що доволі актуально наразі, в умовах повномасштабної війни у країні. Разом з тим, циркуляція великих обсягів «чутливих» даних як про пацієнтів, так і про медпрацівників створила уразливе середовище для кібератак (несанкціонований доступ, можливий витік, викрадення або взагалі втрата особистих даних) [4].

Саме тому **метою статті** є аналіз законодавчих та нормативно-правових актів щодо удосконалення захисту інформації у сфері охорони здоров'я, окреслення проблематики з питань технічної сумісності та взаємодії між медичними електронними ресурсами.

Питання щодо інформатизації сфери охорони здоров'я у своїх наукових працях **досліджували** А. Баранов, Г. Блінова, О. Висоцька, Я. Дубовой, О. Задерейко, О. Легка, Н. Логінова, Є. Радзішевська, І. Сенюта, Р. Стефанчук, С. Стеценко, Х. Терешко, О. Трофименко, О. Тугарова, О. Устінов та інші. Разом з тим, наразі залишаються актуальними питання щодо подальшої інформатизації сфери охорони здоров'я, та, відповідно, дотримання міжнародних стандартів у частині щодо захисту інформації в медичних інформаційних системах.

Результати дослідження. Положенням всесвітньої медичної асоціації щодо використання комп'ютерів в медицині [5], а також Положенням про захист прав та конфіденційність пацієнта [6] 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) [7; 2].

Останнім часом питання щодо інформатизації сфери охорони здоров'я займає центральне місце, адже це надасть можливість: покращити ефективність надання та доступності медичних послуг; підвищити якість процесу лікування; оптимізувати діяльність працівників медичної сфери; розробити та упровадити стандарти щодо збору, обміну та зберігання медичної інформації; розробити нові пропозиції та ініціативи за результатами проведення аналізу архівних матеріалів науковцями [2].

Зважаючи на це фунціоналом МІС повинно бути передбачено не лише дотримання приватності медичних даних, але і можливість отримання відкритої інформації для статистики, аналізу та проведення різних досліджень, що обумовлює складність з питань захисту. Тобто ефективний захист інформації у МІС можливо забезпечити лише за умови взаємопов'язаного комплексного використання організаційних, програмних та технічних засобів захисту.

Виокремлюють три причини порушень інформаційної безпеки МІС – витік інформації, втрата даних та несанкціонована модифікація даних. Основними напрямами ІБ МІС є конфіденційність, цілісність, доступність [8, с. 35]. Функціоналом різних МІС передбачено майже однакові категорії даних, разом з тим зміст угод у частині щодо збору даної інформації може відрізнятися. У зв'язку із цим виникають проблеми при наданні доступу до медичних даних третім особам. Для прикладу, у положенні про медичну систему «Moniheal» визначено право розкривати певні персональні дані не тільки 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 [9]. Проте це суперечить практиці Європейського суду з прав людини. Так, у справі «Gardel v. France» ЄСПЛ наголошує на тому, що доступ до персональних даних у реєстрах можуть мати тільки ті публічні службовці, які зобов'язані зберігати конфіденційність інформації. Інші особи не мають права на доступ до таких даних. Крім того, доступ до інформації має бути наданий виключно із законних причин, таких як слідство, захист населення або державна безпека [10].

Технічна сумісність та взаємодія між медичними електронними ресурсами здійснюється відповідно до Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМУ від 25.04.2018 № 411, Порядку організації електронної інформаційної взаємодії державних електронних інформаційних ресурсів, затвердженого постановою КМУ від 10.05.2018 № 357, Положення про електронну взаємодію державних електронних інформаційних ресурсів, затвердженого постановою КМУ від 08.09.2016 № 606, з дотриманням норм Законів України «Про захист персональних даних», «Про державні фінансові гарантії медичного обслуговування населення», «Про захист інформації в інформаційно-телекомунікаційних системах».

Слід зазначити, що МІС у технічному плані різнорідні (програмна та апаратна несумісність – використання машин різних поколінь, різні мови програмування, різні організації внутрішньо машинних баз даних і т.ін.), що суттєво ускладнює їх упровадження в окремих лікувальних закладах. Зважаючи на це, Планом заходів щодо реалізації Концепції розвитку електронної охорони здоров'я (із змінами від 26.03.2024), затвердженим розпорядженням Кабінету Міністрів України від 29.09.2021 № 1175-р [11], з метою покращення ефективності розвитку ЕСОЗ передбачено: проведення інвентаризації та оцінки існуючих ІКС е-здоров'я з метою їх як оновлення, так і інтеграції до єдиного медичного інформаційного простору; гармонізацію вітчизняних стандартів з європейськими стандартами та класифікаторами, для подальшої інтеграції; створення технічних можливостей (API, спеціалізованих баз з агрегованими знеособленими даними) для доступу до знеособлених агрегованих великих даних (Big Data) в eZdorovya; розроблення концепції стратегічних напрямів розвитку кібербезпеки eZdorovya; подальше розширення функціоналу Єдиного державного веб-порталу електронних послуг «Портал Дія» та його мобільного додатка для інтероперабельності з ЕСОЗ; розвиток систем підтримки клінічних рішень, персоналізованої медицини, телемедицини, систем для обробки великих даних (Big Data), штучного інтелекту [11].

Слід зазначити, що у вересні 2024 року розпорядженням КМУ № 857-р внесено зміни до Концепції розвитку електронної охорони здоров'я від 28.12.2020 № 1671. Основними проблемними напрямами визначено: а) забезпечення сумісності інформаційних систем у сфері охорони здоров'я, а також елементів загальнонаціональної інтероперабельності та стандартів поширеного єдиного цифрового ідентифікатора особи; б) екстенсивна (покращення кількісного показника, без поліпшення якості) форма ведення медичної документації та недостатність інформації про стан здоров'я пацієнта (більша частина первинної медичної інформації зберігається у різних надавачів медичних послуг у паперовій формі) [12].

Крім того, у листопаді 2024 року Верховною Радою України прийнято за основу законопроєкт № 8153 «Про захист персональних даних» (нова редакція Закону від 2010 року), метою якого є приведення норм вітчизняного законодавства до європейських (Регламент Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних 2016/679), підвищення рівня захисту персональних даних та контролю з боку суб'єктів персональних даних за обробкою інформації. Зокрема, законопроєктом № 8153 передбачено: встановлення підстав для обробки персональних даних з деталізацією щодо форми та вимог до згоди на обробку персональних даних; заборону обробки чутливих персональних даних; встановлення обмежень на обробку персональних даних з іншою метою, ніж та, з якою вони збирались; закріплення прав суб'єктів персональних даних та встановлення обов'язків для контролера та оператора персональних даних (призначення відповідальної особи з питань захисту персональних даних; встановлення нових розмірів штрафу за порушення законодавства [13].

Що стосується створення незалежного контролюючого органу з питань захисту персональних даних (передбачено нормами ЄС), то дані норми визначено у законопроєкті № 6177 «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації» (наразі опрацьовується в комітеті). На сьогодні зазначені повноваження покладено на Уповноваженого з прав людини, проте, як зазначають експерти з кібербезпеки, він не встигає реагувати на всі випадки витоку та втрати даних [14]. У законопроєкті передбачено: здійснення Національною комісія з питань захисту персональних даних та доступу до публічної інформації контролю за дотриманням законодавства про захист персональних даних; розгляд скарг суб'єктів персональних даних щодо порушення їх прав, а також накладання штрафів на порушників; розгляд скарг на відмову в доступі до публічної інформації та видання обов'язкових для виконання рішення про надання публічної інформації.

На виконання постанови КМУ від 17.11.2021 № 1200 «Про внесення змін до Порядку функціонування електронної системи охорони здоров'я» № 411 [15], в Україні упроваджено автоматизований обмін інформацією між інформаційними ресурсами НСЗУ та Державною податковою службою через систему електронної взаємодії державних електронних інформаційних ресурсів для здійснення заходів з верифікації даних про користувачів системи електронної охорони здоров'я [16, с. 14].

Центральна база даних ЕСОЗ представляє собою інформаційно-телекомунікаційну систему, яка забезпечує можливість створення, перегляду, обміну інформацією та документами між реєстрами, державними електронними інформаційними ресурсами, електронними медичними інформаційними системами. На сьогодні до ЦБД ЕСОЗ входять наступні реєстри: пацієнтів, декларацій, суб'єктів господарювання у сфері охорони здоров'я, медичних спеціалістів, медичних працівників, договорів про медичне обслуговування населення, договорів про реімбурсацію, медичних висновків. Система

розташована на сервері дата-центру в Україні, яка має комплексну систему захисту інформації та був атестований у Державній службі спеціального зв'язку та захисту інформації. Серед ключових засобів захисту ЦБД ЕСОЗ: кваліфікований електронний підпис; алгоритми, що забезпечують цілісність даних; відокремлене зберігання медичних та персональних даних. Адміністратором ЦБД ЕСОЗ є ДП «Електронне здоров'я», до його компетенції входить: адміністрування та технічна підтримка інформації в ЕСОЗ; підключення, відключення та зупинення доступу МІС до ЦБД; тестування та підтвердження нових функціональних можливостей МІС; надання технічної підтримки МІС; надання інформаційних та консультативних послуг, а також розробка та актуалізація технічної документації.

Зазначимо, що робота у напрямі удосконалення захисту інформації у сфері охорони здоров'я наразі триває, адже повномасштабне вторгнення країни-агресора на територію України зумовили виникнення нагальних проблемних питань, які постійно потребують негайного вирішення. У першу чергу це стосується інформаційного обміну між медичними системами, адже своєчасне та якісне надання медичної допомоги як військовим, так і звичайним громадянам, які отримали травми за наслідками військової агресії, досить важливе.

З урахуванням перебування країни в умовах повномасштабної війни модернізовано напрям системи крові – автоматизовано через системи «єКров» та ЕСОЗ, що сприяє як оперативно планувати, так і в онлайн режимі моніторити запаси крові. Укладено угоду щодо доступу українських медичних закладів до ІТ-системи European Reference Networks і приєдналася до Critical Medicine Alliance, створеного ЄС з метою формування стратегічного запасу лікарських засобів. У межах реформування фармацевтичного сектору Україна отримала позитивне рішення щодо удосконалення механізмів інформаційного обміну та технічної допомоги (Technical Assistance Information Exchange – TAIEX) у сфері технічного регулювання косметики та біоцидних (дезінфекційних) засобів.

Даний напрям активно підтримується і проєктами Європейського Союзу. Яскравим прикладом є програми: «Єдиний цифровий ринок» (реалізація безпечного доступу та транскордонного обміну медичними даними, орієнтованого на пацієнта); EU4Digital (цифровий розвиток охорони здоров'я та транскордонних послуг між країнами Східного партнерства та ЄС); Twinning (удосконалення заходів щодо протидії транскордонним загрозам); продовжує участь у програмі EU4Health; Міжнародне медичне партнерство (співпраця між провідними вітчизняними та міжнародними медичними закладами – підписано 45 меморандумів про співпрацю з медзакладами 18 країн світу та співпрацю МОЗ з міністерствами охорони здоров'я 8 країн ЄС). Слушною у цьому контексті є думка В. Ляшка, який зазначає, що саме розширення співпраці та обміну позитивним досвідом є основою взаємодії у напрямі транскордонної медичної допомоги [17].

Висновок. З урахуванням вище викладеного, ми дійшли наступних висновків. Ефективний захист інформації у МІС можливо забезпечити лише за умови взаємопов'язаного комплексного використання організаційних, програмних та технічних засобів захисту. Основними напрямами ІБ МІС є конфіденційність, цілісність та доступність, причинами порушень інформаційної безпеки МІС є витік інформації, втрата даних та несанкціонована модифікація даних. Актуалізація проблематики захисту інформації у МІС загострилась з моменту повномасштабного вторгнення в Україну країни-агресора. З метою покращення ситуації удосконалюються правові норми у даному напрямі: внесено зміни до Концепції розвитку електронної охорони здоров'я, постанови КМУ «Про внесення змін до Порядку функціонування електронної системи охорони здоров'я»; прийнято за основу законопроєкти № 8153 та № 6177; модернізовано напрям системи крові – автоматизовано через системи «єКров» та ЕСОЗ, що сприяє як оперативно планувати, так і в онлайн режимі моніторити запаси крові; укладено угоду щодо доступу українських медичних закладів до ІТ-системи European Reference Networks та приєднання до Critical Medicine Alliance, створеного ЄС з метою формування стратегічного запасу лікарських засобів; підтримуються проєкти Європейського Союзу щодо захисту медичної інформації, що є основою як взаємодії у напрямі транскордонної медичної допомоги, так і дотриманню міжнародних стандартів у даному напрямі. Проблемним залишається питання щодо формування, з урахуванням міжнародних технічних стандартів обміну інформацією, Єдиного медичного інформаційного простору (сумісність, інтеграція, можливість передавати дані між системами як в рамках E-health, так й із суміжними галузями та сферами як на рівні України, так і на міждержавному, для подальшої інтеграції з відповідними системами в ЄС).

ЛІТЕРАТУРА

1. Стратегія національної безпеки України. URL: https://zakon.rada.gov.ua/laws/show/392/2020?find=1&text.
2. Тугарова О.К., Пономаренко І.С. 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.
3. 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.
4. 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.
5. 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.
6. Положення про захист прав та конфіденційність пацієнта: міжнар. док. від 01.10.1993. Всесвітня медична асоціація. URL: http://zakon2.rada.gov.ua/laws/show/990_056.
7. 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.
8. Радзішевська Є.Б., Висоцька О.В. Інформаційні технології в медицині. E-health /за ред. В.Г. Кнігавка. Харків: ХНМУ, 2019. 72 с.
9. 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.
10. Case «Gardel v. France» від 17.12.2009 (заява № 16428/05). URL: https://hudoc.echr.coe.int/eng#itemid:001-117288.
11. Про затвердження Плану заходів щодо реалізації Концепції розвитку електронної охорони здоров'я: розпорядження Кабінету Міністрів України від 29.09.2021 № 1175-р. URL: https://zakon.rada.gov.ua/laws/show/1175-2021-р#Text.
12. Про внесення змін до Концепції розвитку електронної охорони здоров'я: розпорядження Кабінету Міністрів України від 06.09.2024 № 857-р. URL: https://zakon.rada.gov.ua/laws/show/857-2024-р#Text.
13. Рада схвалила законопроєкт про захист персональних даних. 21.11.2024. URL: https://biz.ligazakon.net/news/232077_rada-skhvalila-zakonoprokt-pro-zakhist-personalnikh-danikh.
14. Обов'язкове інформування, контроль та великі штрафи: як новий законопроєкт змінює правила захисту персональних даних. 14.02.2024. URL: https://www.ukrinform.ua/rubric-polytics/3826649-obovazkove-informuvanna-kontrol-ta-veliki-strafi-ak-novij-zakonoproekt-zminue-pravila-zahistu-personalnih-danih.html.
15. Про внесення змін до Порядку функціонування електронної системи охорони здоров'я: постанова Кабінету Міністрів України від 17.11.2021 № 1200. URL: https://zakon.rada.gov.ua/laws/show/1200-2021-%D0%BF#Text.
16. Аналіз поточної політики розвитку електронної системи охорони здоров'я в Україні. 2022. 99 с. URL: https://amer.org.ua/wp-content/uploads/2023/01/Research_e-Health_UKR_FINAL_2022.pdf.
17. Устінов О.В. Євроінтеграція у сфері охорони здоров'я: досягнення за 2 роки. URL: com.ua/uk/novyna-255313-yevrointegratsiya-u-sferi-ohoroni-zdorov-ya-dosyagnennya-za-2-roki.