УДК 004.056.5:614.2

П. Ю. Токар, д-р філос.

МЕТОДИ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ ДАНИХ ПАЦІЄНТІВ У МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ: АНАЛІТИЧНИЙ ОГЛЯД

Медичні інформаційні системи (МІС) є основою цифрової трансформації охорони здоров'я, забезпечуючи швидкий доступ до медичних даних, їх обробку та обмін між різними учасниками системи. Разом з тим використання електронних медичних записів, телемедицини та хмарних сховищ даних створює нові виклики для захисту конфіденційності пацієнтів. Кіберзагрози у сфері охорони здоров'я постійно ускладнюються, зокрема поширюються атаки типу ransomware, фішинг, несанкціонований доступ до баз даних і витоки інформації. Це обумовлює необхідність детального аналізу сучасних підходів до захисту персональних медичних даних.

У статті здійснено аналітичний огляд наукових публікацій та досліджень, присвячених методам кіберзахисту у медичних інформаційних системах. Розглянуто криптографічні методи (шифрування даних, цифрові підписи, багатофакторна автентифікація), засоби контролю доступу, методи анонімізації та псевдонімізації, технології блокчейн для збереження цілісності даних, а також інструменти машинного навчання для виявлення аномалій у мережевому трафіку. Особливу увагу приділено питанням нормативно-правового регулювання у сфері захисту персональних даних (GDPR, HIPAA) та їхньому впливу на розробку і впровадження МІС.

Аналіз літератури засвідчує, що сучасні методи забезпечення кібербезпеки у медицині мають інтегрований характер і передбачають комбінацію технічних рішень із організаційними заходами, включаючи навчання персоналу та формування культури інформаційної безпеки. Разом із тим низка проблем залишається відкритою: складність впровадження новітніх рішень у закладах охорони здоров'я з обмеженими ресурсами, потреба у стандартизації методів захисту та постійна адаптація до нових типів атак.

Стаття узагальнює сучасні підходи до захисту конфіденційності медичних даних та визначає перспективні напрями подальших досліджень у галузі кібербезпеки медицини.

Ключові слова: *кібербезпека, медичні інформаційні системи, захист даних пацієнтів, конфіденційність, криптографія, автентифікація, електронна медицина, інформаційні технології у медицині.*

Актуальність дослідження

Сфера охорони здоров'я є однією з найчутливіших до кіберзагроз, адже обробляє значні обсяги персональних даних пацієнтів, включно з інформацією про стан здоров'я, діагнози, результати лабораторних досліджень та історії хвороб [4]. У сучасних умовах цифровізації медичних послуг усе ширше впроваджуються електронні медичні картки, телемедицина, мобільні додатки для моніторингу здоров'я та хмарні сховища даних [15]. Це забезпечує

швидший доступ до інформації та підвищує ефективність роботи медичних закладів, однак водночас створює значні ризики для конфіденційності пацієнтів. Витік чи підробка таких даних може мати серйозні наслідки – від фінансових збитків до загрози життю та здоров'ю людей [5].

Зростаюча кількість атак на медичні інформаційні системи у світі підтверджує необхідність розробки та впровадження ефективних методів кіберзахисту. Серед поширених загроз виділяють атаки типу ransomware, які блокують доступ до системи з вимогою викупу, фішингові кампанії проти персоналу, несанкціонований доступ до баз даних, а також внутрішні інциденти, пов'язані з людським фактором [1]. За останні роки медичний сектор став однією з головних цілей кіберзлочинців, оскільки медичні дані мають високу цінність на «чорному ринку» та часто менш захищені, ніж у фінансовій чи оборонній сферах [10].

Особливої ваги питання кіберзахисту набуває в умовах інтеграції української системи охорони здоров'я до європейського та світового цифрового простору. Гармонізація законодавства з міжнародними стандартами, такими як GDPR та HIPAA, потребує не лише формального дотримання вимог, а й реального впровадження технологічних і організаційних рішень, що забезпечать безпеку медичних даних [9]. Водночас обмеженість ресурсів багатьох медичних закладів ускладнює швидку адаптацію до нових викликів, що робить завдання пошуку доступних і водночас ефективних методів захисту особливо актуальним [12].

Дослідження сучасних методів підвищення кібербезпеки медичних інформаційних систем та аналіз їхньої ефективності є надзвичайно важливим для формування надійних механізмів захисту конфіденційності даних пацієнтів. Це питання має не лише технічне, а й суспільне значення, адже від рівня інформаційної безпеки залежить довіра громадян до системи охорони здоров'я та успішність її цифрової трансформації [3].

Мета дослідження

Метою роботи є аналіз та узагальнення сучасних методів захисту конфіденційності даних пацієнтів у медичних інформаційних системах з акцентом на практичні аспекти їх впровадження.

Виклад основного матеріалу

Медичні інформаційні системи сьогодні є невід'ємною складовою цифрової трансформації охорони здоров'я. Вони забезпечують збір, зберігання, обробку й передачу даних пацієнтів між різними рівнями медичних закладів, інтеграцію результатів лабораторних досліджень, електронних медичних записів, телемедичних консультацій і мобільних застосунків. З одного боку, це підвищує якість і швидкість надання послуг, з іншого – створює нові ризики, пов'язані з витоком або підробкою конфіденційних відомостей. За останні десять років кількість атак на медичний сектор у світі зросла в десятки разів. Причини цього очевидні: медичні дані мають високу цінність, оскільки містять не лише персональну інформацію, а й медичні історії, діагнози, результати обстежень, дані страхування [8]. Такі відомості можуть використовуватися для шахрайства, підробки документів, шантажу або нелегального продажу на чорному ринку. Дослідження показують, що медичні дані коштують значно дорожче за фінансові, адже вони практично не змінюються протягом життя людини [11].

Серед найпоширеніших кіберзагроз, що стосуються медичних систем, виділяють атаки типу ransomware, фішингові кампанії, несанкціонований доступ до баз даних, інсайдерські загрози, а також DDoS-атаки, які спрямовані на виведення з ладу телемедичних сервісів та реєстрів [14]. Кожен із цих сценаріїв становить небезпеку не лише для конфіденційності пацієнтів, а й для безперебійного функціонування медичних закладів. Криптографія при цьому є базовим інструментом захисту. Симетричне шифрування використовується для швидкої обробки великих масивів даних, тоді як асиметричні алгоритми забезпечують

безпечну передачу інформації через відкриті канали [6]. Цифрові підписи гарантують автентичність і цілісність медичних документів, а протоколи SSL/TLS дозволяють реалізувати захищену комунікацію між сервером і клієнтом. Однак успішність застосування криптографії залежить від належної організації управління ключами, адже компрометація ключа зводить нанівець усі переваги цих методів. Саме тому все частіше рекомендується використання апаратних модулів безпеки, які забезпечують захист ключів від зовнішнього втручання [7, 13].

Важливим напрямом захисту є контроль доступу до медичних даних, що реалізується через системи автентифікації та авторизації. Парольні системи залишаються найбільш поширеним методом, проте вони є й найбільш уразливими [9]. Багатофакторні системи автентифікації, які поєднують пароль, фізичний носій (наприклад, смартфон або токен) та біометричні характеристики, суттєво підвищують рівень безпеки. У медицині дедалі ширше застосовуються біометричні методи ідентифікації, зокрема розпізнавання відбитків пальців чи обличчя. Системи рольового управління доступом дозволяють обмежувати доступ до даних лише тими співробітниками, які мають на це законні повноваження, наприклад, лікарі конкретного відділення чи адміністратори [13].

З огляду на потребу у використанні медичних даних для наукових досліджень активно впроваджуються методи анонімізації та псевдонімізації, які дозволяють видаляти або замінювати персональні ідентифікатори, зберігаючи при цьому корисність інформації. Проте існує ризик повторної ідентифікації пацієнтів через зіставлення даних з іншими джерелами, що змушує дослідників розробляти складніші механізми, зокрема на основі диференційної приватності [1].

Важливим напрямом є використання блокчейн-технологій, які завдяки своїй децентралізованій природі та незмінності записів дозволяють забезпечити цілісність і прозорість обміну медичними даними. У таких системах будь-які зміни фіксуються в розподіленій мережі й підтверджуються учасниками, що унеможливлює приховане редагування чи підробку записів. Блокчейн активно розглядається як основа для ведення електронних медичних карток, управління згодою пацієнтів на обробку даних, а також організації телемедичних сервісів. Водночас існують обмеження, пов’язані зі складністю масштабування, високими енергетичними витратами та потребою у потужних обчислювальних ресурсах [2, 6, 12].

Окрему увагу приділяють застосуванню штучного інтелекту та машинного навчання для підвищення рівня кіберзахисту. Алгоритми здатні аналізувати мережевий трафік і поведінку користувачів, виявляючи аномалії, що можуть свідчити про потенційні атаки. Використання таких систем дозволяє виявляти навіть нові, раніше невідомі загрози. Водночас застосування штучного інтелекту має свої виклики: моделі вимагають якісних та великих обсягів даних для навчання, можуть містити упередженість, а також створюють додаткові ризики у разі неправильного використання [3, 8].

Технічні методи є лише однією частиною комплексного підходу. Не менш важливими є організаційні заходи, які охоплюють розробку внутрішніх політик безпеки, регулярні аудити, навчання персоналу та формування культури кібербезпеки. Практика показує, що навіть найсучасніші технічні інструменти не гарантують абсолютного захисту, якщо персонал нехтує правилами безпеки або не усвідомлює важливості їх дотримання. Саме людський фактор часто стає причиною витоку інформації, тому підвищення кіберграмотності медичних працівників і постійне оновлення їхніх знань про нові загрози є критично важливим завданням [7, 14].

Крім того, важливу роль відіграє нормативно-правове регулювання. У країнах Європейського Союзу діє Загальний регламент про захист даних (GDPR), який визначає чіткі вимоги до обробки персональних даних, включно з медичними. У США ключовим документом є HIPAA, що регламентує стандарти безпеки в медичних закладах. В Україні функціонує Закон «Про захист персональних даних», проте його положення потребують

подальшої гармонізації з європейськими стандартами. Це означає, що українські медичні установи мають впроваджувати не лише формальні, а й реальні механізми захисту даних, здатні забезпечити довіру пацієнтів та інтеграцію у міжнародний цифровий простір [5].

Перспективи розвитку кіберзахисту медицини пов'язані з подальшою інтеграцією блокчейн-рішень у національні реєстри, розвитком економічно доступних засобів багатофакторної автентифікації, ширшим використанням штучного інтелекту для моніторингу загроз, стандартизацією протоколів безпеки на міжнародному рівні та підвищенням кіберграмотності персоналу [10, 15]. Забезпечення належного рівня безпеки медичних інформаційних систем вимагає комплексного підходу, що поєднує технічні рішення, організаційні заходи та правові механізми. Лише інтеграція цих складових здатна гарантувати захист конфіденційності даних пацієнтів у сучасних умовах, коли кіберзагрози постійно ускладнюються та змінюють свою форму [4].

Висновки та перспективи подальших досліджень

Аналіз літературних джерел засвідчив, що проблема захисту конфіденційності даних пацієнтів у медичних інформаційних системах є однією з найактуальніших у сфері кібербезпеки. Сучасні підходи до забезпечення захисту мають комплексний характер і передбачають поєднання криптографічних алгоритмів, багатофакторної автентифікації, методів анонімізації та псевдонімізації даних, а також застосування інтелектуальних систем виявлення загроз. Перспективним напрямом визнано використання блокчейн-технологій для підвищення прозорості та незмінності медичних записів.

Разом з тим значні труднощі викликають фінансові та організаційні обмеження медичних закладів, низький рівень підготовки персоналу та постійна поява нових типів атак. Це зумовлює потребу у створенні економічно доступних та стандартизованих рішень, які можна було б масштабувати в умовах різних країн і систем охорони здоров'я.

Подальші дослідження доцільно зосередити на інтеграції технологій штучного інтелекту для проактивного виявлення загроз, розробці уніфікованих міжнародних стандартів кіберзахисту та удосконаленні механізмів підготовки медичного персоналу.

СПИСОК ЛІТЕРАТУРИ

1. Sharing Medical Big Data While Preserving Patient Confidentiality in Innovative Medicines Initiative: A Summary and Case Report from BigData@Heart / M. Schröder et al. *Big Data*. 2023. Т. 11, № 6. P. 399–407. DOI: 10.1089/big.2022.0178.

2. Privacy Preservation in Patient Information Exchange Systems Based on Blockchain: System Design Study / S. Lee et al. *Journal of Medical Internet Research*. 2022. Т. 24, № 3. e29108. DOI: 10.2196/29108.

3. A data flow process for confidential data and its application in a health research project / S. S. R. Crossfield et al. *PLoS ONE*. 2022. Т. 17, № 1. e0262609. DOI: 10.1371/journal.pone.0262609.

4. Privacy-protecting, reliable response data discovery using COVID-19 patient observations / J. Kim et al. *Journal of the American Medical Informatics Association.* 2021. Т. 28, № 8. P. 1765–1776. DOI: 10.1093/jamia/ocab054.

5. Effective Privacy Protection Strategies for Pregnancy and Gestation Information From Electronic Medical Records: Retrospective Study in a National Health Care Data Network in China / C. Liu et al. *Journal of Medical Internet Research*. 2024. Т. 26. e46455. DOI: 10.2196/46455.

6. Protection of confidential medical information in Ukraine: problems of legal regulation / N. Onishchenko et al. *Georgian Medical News*. 2024. № 349. P. 161–168.

7. Factors Influencing the Adoption of Advanced Cryptographic Techniques for Data Protection of Patient Medical Records / N. Lewis et al. *Healthcare Informatics Research*. 2022. Т. 28, № 2. P. 132–142. DOI: 10.4258/hir.2022.28.2.132.

8. Blockchain-based Electronic Medical Record Security Sharing Scheme / Y. Yao et al. *Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC).* 2023. P. 1–4. DOI: 10.1109/EMBC40787.2023.10340218.

9. Ethics, Integrity, and Retributions of Digital Detection Surveillance Systems for Infectious Diseases: Systematic Literature Review / I. Y. Zhao et al. *Journal of Medical Internet Research*. 2021. Т. 23, № 10. e32328. DOI: 10.2196/32328.

10. Secure Hybrid Deep Learning for MRI-Based Brain Tumor Detection in Smart Medical IoT Systems / N. G. Rezk et al. *Diagnostics (Basel)*. 2025. Т. 15, № 5. P. 639. DOI: 10.3390/diagnostics15050639.

11. Electronic Health Records Sharing Based on Consortium Blockchain / G. Wu et al. *Journal of Medical Systems*. 2024. Т. 48, № 1. P. 106. DOI: 10.1007/s10916-024-02120-9.

12. Herrero Antón de Vez H., Felez E., Cypko M. A. A methodological framework for integrating model-guided medicine and multidimensional information management systems: application in anti-aging healthcare. *International Journal of Computer Assisted Radiology and Surgery*. 2025. DOI: 10.1007/s11548-025-03337-w. URL: https://doi.org/10.1007/s11548-025-03337-w.

13. Alaqra A. S., Kane B., Fischer-Hübner S. Machine Learning-Based Analysis of Encrypted Medical Data in the Cloud: Qualitative Study of Expert Stakeholders' Perspectives. *JMIR Human Factors*. 2021. Т. 8, № 3. e21810. DOI: 10.2196/21810.

14. Feature Extraction Approach for Speaker Verification to Support Healthcare System Using Blockchain Security for Data Privacy / S. Upadhyay et al. *Computational and Mathematical Methods in Medicine*. 2022. 8717263. DOI: 10.1155/2022/8717263. URL: https://doi.org/10.1155/2022/8717263.

15. Proposal and Assessment of a De-Identification Strategy to Enhance Anonymity of the Observational Medical Outcomes Partnership Common Data Model (OMOP-CDM) in a Public Cloud-Computing Environment: Anonymization of Medical Data Using Privacy Models / S. Jeon et al. *Journal of Medical Internet Research*. 2020. Т. 22, № 11. e19597. DOI: 10.2196/19597. URL: https://doi.org/10.2196/19597.

Стаття надійшла до редакції 10.09.2025.
Стаття пройшла рецензування 23.09.2025.

Токар Петро Юрійович – студент Національного технічного університету “Харківський політехнічний інститут”, доктор філософії, асистент кафедри акушерства, гінекології та перинатології Буковинського державного медичного університету, e-mail: tokpet27@gmail.com.

Національний технічний університет “Харківський політехнічний інститут”.