УДК 004.056:614.2

І. М. Лепетан

КІБЕРБЕЗПЕКА В ОХОРОНІ ЗДОРОВ'Я: ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ ПАЦІЄНТІВ В УМОВАХ ЦИФРОВІЗАЦІЇ

Вінницький національний медичний університет ім. М. І. Пирогова

Анотація. *У сучасних умовах цифровізації медичної сфери питання кібербезпеки стає критично важливим для забезпечення захисту персональних даних пацієнтів. У дослідженні розглядаються основні загрози кібербезпеці в охороні здоров'я, включаючи витоки даних, кібератаки та несанкціонований доступ. Аналізуються сучасні методи та технології захисту інформації, такі як шифрування, багатофакторна автентифікація, блокчейн та штучний інтелект. Особлива увага приділяється нормативно-правовим аспектам захисту медичних даних та міжнародним стандартам у сфері кібербезпеки. Дослідження підкреслює важливість комплексного підходу до кіберзахисту в охороні здоров'я та впровадження ефективних стратегій управління ризиками.*

Ключові слова: кібербезпека, охорона здоров'я, управління, цифровізація, медична інформація, захист даних.

Abstract. *In today's digitalized healthcare environment, cybersecurity is becoming a critical issue to ensure the protection of patients' personal data. The study examines the main threats to cybersecurity in healthcare, including data leaks, cyberattacks, and unauthorized access. Modern methods and technologies of information protection, such as encryption, multi-factor authentication, blockchain and artificial intelligence, are analyzed. Special attention is paid to the regulatory aspects of medical data protection and international standards in the field of cybersecurity. The study emphasizes the importance of a comprehensive approach to cybersecurity in healthcare and the implementation of effective risk management strategies.*

Keywords: cybersecurity, healthcare, governance, digitalization, medical information, data protection.

Цифровізація охорони здоров'я набирає стрімких обертів у всьому світі. Впровадження електронних медичних записів, систем телемедицини, хмарних рішень та Інтернету речей (IoT) значно підвищує ефективність надання медичних послуг. Однак разом із цими технологічними досягненнями виникають нові виклики, зокрема кіберзагрози, які можуть призвести до викрадення даних пацієнтів, порушення роботи медичних установ та створення загроз здоров'ю.

Цифрові технології проникають у різні аспекти охорони здоров'я, починаючи від електронних медичних карток до телемедицини та інноваційних медичних пристроїв, які можуть передавати дані в реальному часі.

Електронні медичні картки (ЕМК) – це одне з ключових досягнень цифровізації. Вони полегшують доступ до інформації про пацієнтів, що дає змогу лікарям швидко отримувати потрібні дані для лікування. Однак централізоване зберігання інформації робить ці бази вразливими для атак.

Телемедицина розширила доступ до медичних послуг, особливо в період пандемії COVID-19, коли особисті візити до лікаря були обмежені. Водночас передача медичних даних через незахищені канали може стати приводом для викрадення конфіденційної інформації.

Інтернет речей (IoT) включає в себе підключені медичні пристрої, такі як монітори серцевого ритму або пристрої для вимірювання рівня глюкози, які збирають і передають дані. Недостатній захист таких пристроїв може призвести до їхнього зламу та маніпуляцій з життєво важливими показниками.

Зазначені інструменти стають привабливими цілями для кіберзлочинців через величезні обсяги чутливої інформації. Таким чином, кібербезпека є важливим аспектом сфери охорони здоров'я, оскільки вона захищає конфіденційну медичну інформацію та запобігає втраті важливих даних.

Колектив науковців [3] пропонують під кібербезпекою у сфері охорони здоров'я розуміти важливу складову державної політики, спрямовану на контроль поточного стану інформаційних систем критичної інфраструктури, підвищення обізнаності та кіберграмотності співробітників, підготовку кваліфікованих фахівців у сфері кібербезпеки та отримання успішного світового досвіду в цій сфері. На думку вчених, важливими засобами забезпечення безпеки віддаленої підтримки пацієнтів є надійні електронні бази медичних даних, механізми реєстрації та керування доступом до медичних даних, що

передаються між пацієнтами та постачальниками медичних послуг. Водночас до забезпечення надійного захисту медичних комп'ютерних систем необхідно підходити з найбільшою ретельністю, враховуючи програмні, апаратні та організаційні аспекти [3].

Ефективний захист медичних систем та даних пацієнтів потребує комплексного підходу, який включає як технічні рішення, так і нормативно-правове регулювання.

До технічних рішень у сфері захисту медичних систем можна віднести: шифрування даних, аутентифікацію користувачів, моніторинг систем і управління доступом, оновлення програмного забезпечення та безпеку медичних пристроїв.

Шифрування даних є одним із найефективніших способів захисту інформації. Дані пацієнтів повинні бути зашифровані як під час зберігання, так і при їх передачі через мережі, щоб запобігти несанкціонованому доступу.

Аутентифікація користувачів із застосуванням багатофакторної автентифікації (MFA) може запобігти доступу до медичних систем сторонніх осіб, навіть якщо їх облікові дані були викрадені.

Моніторинг систем і управління доступом передбачає постійний нагляд за активністю в мережі та налаштування різних рівнів доступу для працівників, залежно від їхньої ролі в установі.

Оновлення програмного забезпечення. Уразливості, які виявляються в медичних системах, можуть бути використані кіберзлочинцями, тому регулярне оновлення є обов'язковим для забезпечення безпеки.

Безпека медичних пристроїв. Пристрої, що підключені до мережі, повинні бути захищені від атак, оскільки злом таких пристроїв може призвести до фатальних наслідків для пацієнтів. Важливо використовувати стандарти безпеки, такі як ISO/IEC 80001-1, що регулюють управління ризиками для медичних пристроїв.

Для ефективного забезпечення захисту даних пацієнтів важливо дотримуватися міжнародних і національних стандартів. Загальний регламент захисту даних (GDPR), прийнятий у ЄС, регулює обробку та зберігання персональних даних, включно з медичною інформацією. Він вимагає забезпечення прозорості, шифрування даних та надання прав пацієнтам на контроль за їх інформацією. HIPAA (Health Insurance Portability and Accountability Act) у США встановлює вимоги до конфіденційності медичних записів і кібербезпеки у сфері охорони здоров'я.

Україна також розвиває власну законодавчу базу для кібербезпеки в охороні здоров'я. Основним законом є Закон України «Про захист персональних даних», який регулює обробку та зберігання інформації про пацієнтів [2]. Крім того, Міністерство охорони здоров'я України спільно зі Світовим Банком в рамках проєкту «Зміцнення системи охорони здоров'я та збереження життя» (HEAL Ukraine) ухвалило Угоду про позику від 22.12.22 р. №9468-UA [4], якою передбачено створити єдиний Галузевий Центр кібербезпеки в галузі охорони здоров'я, щоб забезпечити належний рівень інформаційної безпеки у цій сфері та суспільстві в цілому. Так, положеннями Угоди передбачено розвиток потенціалу, цифровізацію та підтримку інновацій, зокрема розробку основних модулів системи електронної охорони здоров'я, включаючи реєстрацію медичних працівників, портал даних пацієнтів, модулі системи електронної охорони здоров'я для груп інвалідності та реабілітації, покращення кібербезпеки даних, пов'язаних зі здоров'ям, інтеграцію цифрових систем охорони здоров'я з пов'язаними системами в сусідніх країнах і зміцнення систем електронної охорони здоров'я в усіх закладах охорони здоров'я [4].

У сучасних умовах важливо постійно вдосконалювати системи кібербезпеки в охороні здоров'я, зокрема:

1. Навчання персоналу. Медичні працівники повинні бути навчені основам кібербезпеки для уникнення фішингових атак та інших загроз.

2. Співпраця з IT-компаніями. Медичні установи повинні співпрацювати з фахівцями з кібербезпеки для моніторингу та захисту систем.

3. Оновлення законодавства. Необхідно постійно оновлювати правові норми для врахування нових викликів у сфері кібербезпеки.

Захист даних пацієнтів є ключовим аспектом кібербезпеки в умовах цифровізації охорони здоров'я. Поєднання технічних рішень, таких як шифрування та аутентифікація, із суворим регулюванням на рівні законодавства є необхідним для запобігання кіберзагрозам. Водночас важливим є навчання медичного персоналу та постійне вдосконалення систем для захисту інформації про пацієнтів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Ляшук А. Загрози і виклики для системи кібербезпеки інформаційних систем та реєстрів сфери охорони здоров'я. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2023. Вип. 6. С. 113-121.

2. Про захист персональних даних: Закон України № 2297-VI від 1 червня 2010 року. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (Дата звернення: 18.10.2024)

3. Трофименко О., Дубовий Я., Логінова Н., Прокоп Ю., Задерейко О. Питання кібербезпеки медичних комп'ютерних систем. *Захист інформації*. 2021. № 23 (1). С. 30-39.

4. Угода про позику (Проєкт «Зміцнення системи охорони здоров'я та збереження життя» (Heal Ukraine)) між Україною та Міжнародним банком реконструкції та розвитку. URL: https://zakon.rada.gov.ua/laws/ show/996_002-22#Text (дата звернення: 18.10.2024).

5. Лепетан І. М. Телемедицина як частина цифрового бренду медичних послуг. *Інформаційні технології і автоматизація – 2024:* матеріали XVII Міжнародної науково-практичної конференції. Одеса, 31 жовтня – 1 листопада 2024 року. С. 813-814.

6. Головчук Ю., Мазур Г. Цифрові технології в управлінні закладами охорони здоров'я. *Кращі практики цифровізації в ЄС та цифрова трансформація економіки України*: збірник матеріалів Міжнародної науково-практичної інтернет-конференції. Запоріжжя: видавець ФОП Мошканов В. В., 2024. С. 95-98.

Відомості про автора

Лепетан Інна Михайлівна, кандидат економічних наук, доцент, доцент кафедри менеджменту та маркетингу, Вінницький національний медичний університет ім. М.І. Пирогова, Вінниця, e-mail: lepetan_inna@i.ua

Lepetan Inna M., PhD in Economics, Associate Professor, Associate Professor of the Department of Management and Marketing, Vinnytsya National Pirogov Memorial Medical University, Vinnytsya, e-mail: lepetan_inna@i.ua