

ІНФОРМАЦІЙНА БЕЗПЕКА В МЕДИЧНИХ ПРИСТРОЯХ ІОТ ТА ЇХ ВПЛИВ НА ЗДОРОВ'Я ПАЦІЄНТІВ

Впровадження Інтернету речей (ІоТ) у медичній галузі відкриває широкі перспективи для підвищення якості медичних послуг та ефективного моніторингу стану здоров'я пацієнтів. Підключені медичні пристрої, такі як фітнес-трекери, безконтактні термометри, інсулінові помпи та імплантати, дозволяють збирати, аналізувати та передавати дані про стан пацієнта у режимі реального часу. Це допомагає лікарям швидко реагувати на зміни та надавати своєчасну допомогу [1-3].

Однак, незважаючи на свої переваги, використання ІоТ у медицині також несе певні ризики та виклики, пов'язані з інформаційною безпекою та конфіденційністю даних пацієнтів. Недостатній захист підключених пристроїв може призвести до витоку чутливої інформації, порушення конфіденційності або навіть впливу на коректну роботу медичних систем, що може поставити під загрозу здоров'я та безпеку пацієнтів.

Інформаційна безпека в медичних пристроях ІоТ є критично важливою, оскільки це напрямок, який відкриває безліч можливостей для поліпшення медичного обслуговування, але також несе ризики для здоров'я пацієнтів у випадку недбалого захисту даних та пристроїв [4-7]. Дослідження показує, що:

1. Загрози інформаційній безпеці медичних ІоТ-пристроїв.

Одна з основних загроз інформаційній безпеці при використанні медичних ІоТ-пристроїв – це витік конфіденційних даних пацієнтів. Через недостатнє шифрування або вразливості в системах захисту, зловмисники можуть отримати доступ до персональної інформації, історії хвороб, результатів аналізів тощо [8-10]. Це не лише порушує право на конфіденційність, а й може призвести до шахрайства або використання даних з незаконною метою.

Крім того, існує ризик кібератак на медичні ІоТ-пристрої та системи. Зловмисники можуть здійснювати спроби несанкціонованого доступу, встановлювати шкідливе програмне забезпечення або впливати на роботу пристроїв з метою порушення їх коректного функціонування [11, 12]. Це може мати критичні наслідки для здоров'я та життя пацієнтів [13].

2. Вплив кібербезпеки на фізичну безпеку пацієнтів.

Порушення кібербезпеки медичних ІоТ-пристроїв може безпосередньо вплинути на фізичну безпеку пацієнтів. Наприклад, якщо зловмисник зможе отримати доступ до інсулінової помпи або імплантату, він потенційно може змінити їх налаштування або режими роботи, що може поставити під загрозу життя пацієнта [14].

У випадку із системами моніторингу стану пацієнта, кібератака може призвести до надходження невірних даних, через що лікарі не зможуть своєчасно виявити критичні зміни в здоров'ї пацієнта та вжити необхідних заходів.

3. Аналіз існуючих стандартів безпеки.

На сьогоднішній день існують певні стандарти та вимоги до забезпечення безпеки медичних пристроїв ІоТ, такі як HIPAA (Health Insurance Portability and Accountability Act) у США та GDPR (General Data Protection Regulation) в Європейському Союзі. Однак, ці стандарти часто не встигають за швидким розвитком технологій ІоТ та потребують постійного оновлення та вдосконалення.

4. Рекомендації щодо покращення безпеки.

Для підвищення рівня інформаційної безпеки медичних ІоТ-пристроїв необхідно вжити комплексних заходів. По-перше, важливо забезпечити належне шифрування даних, що передаються між пристроями та серверами зберігання. По-друге, слід використовувати

надійні методи автентифікації та контролю доступу, щоб запобігти несанкціонованому втручанню.

Крім того, необхідно регулярно оновлювати програмне забезпечення медичних IoT-пристроїв для усунення виявлених вразливостей та своєчасно реагувати на потенційні загрози кібербезпеки. Важливо також забезпечити належне навчання медичного персоналу з питань безпеки IoT-систем та дотримання відповідних протоколів безпеки [15].

Лише за умови ретельного планування та впровадження ефективних стратегій безпеки медичні заклади зможуть повною мірою скористатися перевагами технологій IoT, забезпечуючи при цьому захист конфіденційної інформації пацієнтів та їхню фізичну безпеку.

Отже, інформаційна безпека відіграє критично важливу роль у забезпеченні ефективного та безпечного використання медичних пристроїв IoT. Незважаючи на численні переваги, які ці інноваційні технології надають для покращення медичного обслуговування, недостатній рівень безпеки може становити серйозну загрозу для конфіденційності даних пацієнтів та їхнього здоров'я.

ЛІТЕРАТУРА

1. Лемешев М.С., Березюк О.В. Основи охорони праці для фахівців менеджменту. Навчальний посібник. Вінниця: ВНТУ, 2009. 206 с.
2. Березюк О.В. Моделювання питомих енерговитрат очищення ґрунтів полігонів твердих побутових відходів від забруднення важкими металами // Комунальне господарство міст. 2015. № 1 (120). С. 240-242.
3. Березюк О.В. Удосконалення математичної моделі концентрацій забруднювальних речовин у фільтраті полігонів твердих побутових відходів // Вісник ВПІ. 2016. № 4. С. 28-31.
4. Ткачук К.Н. та ін. Основи охорони праці: підручник. Київ: Основа, 2014. 456 с.
5. Горбатюк С.М. та ін. Лігногумат натрію як модифікатор мутагенних ефектів мітоміцину С // Матеріали І Міжнар. наук.-практ. конф. "Ліки – людині. Сучасні проблеми фармакотерапії і призначення лікарських засобів", 30-31 бер. 2017. Харків: НФУ, 2017. Т. 2. С. 97.
6. Березюк О.В. та ін. Залежність рівня бактеріологічного забруднення ґрунтів від відстані до полігону твердих побутових відходів // Наукові праці ВНТУ. 2021. № 2. 6 с.
7. Березюк О.В. та ін. Вплив наближення до полігону твердих побутових відходів на рівень мікробіологічного забруднення ґрунтових вод за загальним мікробним числом // Наукові праці Вінницького національного технічного університету. 2023. № 1. 7 с.
8. Голінько В.І., Іконніков М.Ю., Лебедев Я.Я. Охорона праці в галузі інформаційних технологій: навч. посіб. Дніпро: НГУ, 2015. 246 с.
9. Березюк О.В. та ін. Регресійна залежність показників захворюваності на хвороби органів дихання від продуктивності сміттєспалювального заводу // Наукові праці ВНТУ. 2023. № 1. 6 с.
10. Березюк О.В., Гринчак Н.М., Спрут О.В., Березюк В.О. Удосконалення математичної моделі впливу викидів дрібнодисперсного пилу на захворюваність хворобами системи кровообігу // Наукові праці ВНТУ. 2023. № 1. 7 с.
11. Закон України "Про охорону праці" від 14.10.1992 № 2694-ХІІ. [Електронний ресурс] Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2694-12>
12. Березюк О.В., Савуляк В.І. Вплив характеристик тертя на динаміку гідроприводу вивантаження твердих побутових відходів із сміттєвоза // Проблеми тертя та зношування. 2015. № 3 (68). С. 45-50.
13. Шевчук Т.І., Шкарупа В.М., Хлестова С.С. Антропогенна зміна довкілля як фактор поширення паразитарних захворювань людини // Довкілля і здоров'я: Матеріали наук.-практ. конф., 27-28 квіт. 2017 р. Тернопіль, 2017. С. 220-222.
14. IoT в охороні здоров'я: Застосування, переваги та виклики у 2023 році. [Електронний ресурс]. Режим доступу: <https://stfalcon.com/uk/blog/post/iot-in-healthcare-benefits-challenges>
15. Інтернет речей: вплив та наслідки для надання медичної допомоги. [Електронний ресурс]. Режим доступу до ресурсу: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7685921/>