УДК 004.056:614

ПРОБЛЕМИ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОХОРОНИ ЗДОРОВ'Я

Левченко А. С.
Науковий керівник – к.т.н., проф. Панфьорова І.Ю.
Харківський національний університет радіоелектроніки, каф. ІУС
м. Харків, Україна
тел.: +380984363661, email: anastasiia.levcenko@nure.ua

The article considers the critical importance of confidentiality in health care information systems. Medical information systems (MIS) allow healthcare providers to store, manage and exchange patient medical records and other confidential medical data. The article outlines the three most significant security issues, including unauthorized access to patient information, loss or theft of hardware devices, and inadequate training of medical personnel on data security. The article concludes by emphasizing the importance of confidentiality and security in MIS, and why it is crucial to ensure the protection of patients' data.

Інформаційні системи (ІС) охорони здоров'я стали критично важливими компонентами сучасного надання медичних послуг. Медичні інформаційні системи (МІС) дозволяють постачальникам медичних послуг зберігати, керувати та обмінюватися медичними записами пацієнтів та іншими конфіденційними медичними даними. Однак, зростаюча кількість електронної медичної інформації, яку зберігають МІС, породжує ризики безпеки та виклики, пов’язані з їх використанням.

Однією з найважливіших проблем безпеки в МІС є ризик несанкціонованого доступу до інформації про пацієнта. Це може статися через наявність вірусів або інші форми кібератак [1]. Ця проблема ускладнюється тим фактом, що медичні записи містять не лише особисту інформацію, але й медичні діагнози, плани лікування та інші конфіденційні дані, які можуть бути використані для крадіжки особистих даних або фінансового шахрайства.

Іншою проблемою є втрата або крадіжка пристроїв, які зберігають дані пацієнтів (ноутбуків, мобільних пристроїв) та використовуються медичними працівниками (МП) для доступу до цих даних. Якщо пристрої втрачені, то дані пацієнтів можуть потрапити в чужі руки. МП повинні вжити відповідних заходів для захисту цих пристроїв, наприклад, шифрування та захисту паролем, щоб запобігти несанкціонованому доступу до даних, що зберігаються на них [2].

Третьою проблемою є відсутність належної підготовки МП щодо безпечного поводження з даними пацієнтів. Багато МП не дотримуються найкращих практик щодо захисту конфіденційної інформації. Це призводить до випадкових порушень конфіденційності даних. Такі порушення можуть також бути шкідливими, як і навмисні порушення [3].

Наведені приклади показують, що проблеми конфіденційності та безпеки в інформаційних системах охорони здоров'я стали важливою темою обговорень в науковій спільноті. На сьогодні немає жодного ідеального рішення, яке може повністю гарантувати конфіденційність та безпеку медичної інформації. Можна визначити декілька важливих підходів та рекомендацій, які можуть допомогти зменшити ризики порушення конфіденційності та безпеки медичної інформації:

- забезпечення захисту доступу до медичної інформації (важливо, щоб тільки авторизовані користувачі мали доступ до конфіденційної медичної інформації);
- використання сильних паролів та двофакторної аутентифікації;
- використання безпечних протоколів при передачі медичної інформації (протоколи шифрування даних);
- організація безпечного зберігання медичної інформації (захищені бази даних та системи забезпечення резервного копіювання даних);
- регулярне оновлення програмного забезпечення;
- навчання медичних працівників методам взаємодії з захищеною інформацією (адже найбільша частка порушень конфіденційності трапляється завдяки користувачам ІС).

Аналіз, проведений в роботі, показав, що при проектуванні МІС необхідно використовувати технології, які забезпечать конфіденційність та безпеку даних. Вирішити проблеми конфіденційності даних в МІС можна за допомогою використання надійних систем управління базами даних (СУБД), СУБД забезпечують високий рівень захисту даних від несанкціонованого доступу, втрати або пошкодження. Серед надійних СУБД можна виділити Oracle Database, Microsoft SQL Server, IBM DB2, PostgreSQL, MySQL, MongoDB. Застосування будь-якої з цих СУБД залежить від потреб та вимог конкретної МІС. Значна роль побудови стратегії та детального планування заходів щодо забезпечення конфіденційності даних реалізується адміністратором МІС. При плануванні проєкту МІС необхідно передбачати виконання завдань із захисту даних.

Список використаних джерел:

1. Paquette, J. (2018). Preventing Cyber Attacks on Healthcare Systems: How to Protect Your Patients and Your Business» Journal of Healthcare Management, 382–383.

2. Warkentin, M. O. (2018). «Healthcare Mobile Device Security: An Exploration of Risks, Threats, and Mitigation Strategies». Health Informatics Journal, 259–269.

3. Kaya, D. (2020). «Information Security Awareness of Healthcare Professionals: A Case Study in Turkey». Health Informatics Journal, 897–906.