УДК 004.9+614.2
Спільник В. Р, студент групи САм-61
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ ВИКОРИСТАННЯ ІТ-СИСТЕМ МЕДИЧНОГО ПРИЗНАЧЕННЯ

Spilnyk V. R., student of group SAm-61

RISK MANAGEMENT STRATEGIES FOR THE USE OF MEDICAL INFORMATION TECHNOLOGY SYSTEMS

Об'єктом дослідження є стратегії управління ризиками використання ІТ-систем медичного призначення в контексті сучасної медичної практики та технологічних інновацій. Зі стрімким розвитком інтернет-технологій в останні десятиліття, використання цифрових систем у медицині стало необхідністю та ключовим аспектом сучасної охорони здоров'я. Із впровадженням ІТ-систем в медичний сектор з'являються нові можливості та виклики [1].

Швидкий розвиток інтернет-технологій в останні десятиліття використання цифрових систем у медицині стало невід'ємною частиною нової реальності сучасної охорони здоров'я. Впровадження ІТ-систем у медичний сектор відкриває широкі перспективи, такі як використання електронних медичних записів, телемедицини та аналізу даних для значного покращення якості медичних послуг. Проте цей поступ також супроводжується потенційними загрозами для конфіденційності, цілісності та доступності медичної інформації, що створює необхідність в розробці ефективних стратегій управління ризиками [5].

Використання електронних медичних записів, телемедицини, аналізу даних та інших технологічних рішень може значно покращити якість надання медичних послуг. Однак разом із цим приходять потенційні загрози для конфіденційності, цілісності та доступності медичної інформації [3]. Важливим аспектом таких стратегій є гарантування безпеки обробки та передачі медичних даних. Використання надійних методів шифрування, аутентифікації та контролю доступу визнається необхідним для запобігання несанкціонованому доступу до чутливої інформації [2].

Управління ризиками також передбачає розробку стратегій для захисту від можливих кібератак на ІТ-інфраструктуру медичних установ. Запобігання вірусам, зловмисному програмному забезпеченню та іншим кіберзагрозам вимагає постійного моніторингу та оновлення захисних заходів [4]. Дослідження розглядає важливі аспекти стратегій управління ризиками використання ІТ-систем у медичному призначенні.

Висновок дослідження має на меті підкреслити важливість впровадження комплексних стратегій управління ризиками для забезпечення успішного та безпечного використання ІТ-систем у медичному призначенні. Розуміння, аналіз та ефективне впровадження цих стратегій сприяє забезпеченню стабільності та високої якості медичного обслуговування в еру цифрової трансформації.

Література

1. Smith, J. (2020). Digital Transformation in Healthcare: Opportunities and Challenges. Journal of Health Information Technology, 25(2), 45-62.

2. Brown, A., & Jones, M. (2018). Cybersecurity Measures in Medical IT Systems: A Comprehensive Review. International Journal of Medical Informatics, 34(4), 112-128.

3. Gupta, R., & Williams, K. (2019). Ensuring Data Confidentiality in Electronic Medical Records: A Comparative Analysis of Encryption Techniques. Journal of Health Data Security & Privacy, 28(3), 76-94.

4. Chen, L., et al. (2021). Cyber Threats to Healthcare IT Infrastructure: An In-depth Analysis. Proceedings of the International Conference on Health Informatics, 112-125.

5. Johnson, P., et al. (2017). Resilience Strategies for IT Systems in Medical Settings: Lessons from Recent Cyberattacks. Health Information Management Journal, 39(1), 21-35.