УДК 004.49

О. В. Перестюк
М. А. Томчук

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕДИЧНИХ ДАНИХ В БАГАТОРІВНЕВІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ ЛІКУВАЛЬНОГО ЗАКЛАДУ

Вінницький національний технічний університет

Анотація

Розглянуто важливі аспекти забезпечення безпеки медичних даних в лікувальних закладах. Досліджено ризики та загрози, пов'язані з цифровими технологіями та комп'ютеризацією медичного середовища, а також приділено увагу методам та стратегіям їхнього запобігання та мінімізації. Окреслено важливість створення технічних засобів захисту, розробки політик безпеки та впровадження стандартів із захисту конфіденційності медичної інформації. Розглянуто необхідність подальшого вдосконалення технологій та політик безпеки з метою забезпечення надійного захисту медичних даних у лікувальних закладах.

Ключові слова: медичні дані, безпека, конфіденційність, комп'ютеризація, захист даних.

Abstract

Important aspects of ensuring the security of medical data in medical facilities are considered. The risks and threats associated with digital technologies and computerization of the medical environment are explored, and attention is paid to methods and strategies for their prevention and minimization. The importance of creating technical means of protection, developing security policies and implementing standards for protecting the confidentiality of medical information is outlined. Considered the need for further improvement of technologies and security policies in order to ensure reliable protection of medical data in medical institutions.

Keywords: medical data, security, privacy, computerization, data protection.

Вступ

З розвитком сучасних технологій та комп'ютеризацією лікарняних закладів збільшується важливість забезпечення безпеки медичних даних. Комп'ютерні мережі стають неодмінною складовою у сфері медичної практики, та разом з цим зростають виклики, пов'язані з безпекою та конфіденційністю інформації.

У сучасному цифровому середовищі, зростає кількість кіберзагроз та різноманітність доступних технологій ставлять під загрозу конфіденційність медичних даних. Це робить актуальним пошук ефективних стратегій та інструментів для забезпечення безпеки медичних даних у лікарняних установах.

Поява нових інформаційних технологій, таких як хмарні сервіси, мобільні додатки для збору та обробки медичної інформації, а також інтернет-підключені медичні пристрої, розширює можливості управління медичною інформацією, але одночасно створює нові вектори атак та ризики для безпеки. Тому, пошук найбільш ефективних та інноваційних підходів до забезпечення безпеки медичних даних є актуальним завданням у сучасному медичному середовищі.[1]

Аналіз сучасного стану

У сучасному медичному середовищі існують різноманітні системи та методи захисту медичних даних, які спрямовані на забезпечення конфіденційності, цілісності та доступності інформації. Однак, кожна з них має свої переваги та недоліки, які варто враховувати при їх виборі та впровадженні.

Шифрування є одним з основних методів захисту медичних даних. Цей підхід полягає у перетворенні медичної інформації у шифрований формат за допомогою спеціальних алгоритмів. Шифрування дозволяє зберігати дані у безпечному стані, що робить їх незрозумілими для несанкціонованих осіб. Однак, процес шифрування може сповільнити доступ до даних та вимагати додаткових обчислювальних ресурсів.

Для забезпечення безпеки медичних даних важливо впевнитися, що лише авторизовані користувачі мають доступ до інформації. Для цього застосовуються різноманітні методи аутентифікації, такі як

паролі, біометричні дані, картки доступу тощо. Ці методи дозволяють ідентифікувати користувачів та контролювати їхні права доступу. Однак, слабкі паролі або недостатня біометрична аутентифікація можуть стати точкою вразливості.

Системи моніторингу та аудиту безпеки дозволяють відстежувати доступ до медичної інформації, виявляти незвичайну активність та вчасно реагувати на потенційні загрози. Ці системи надають можливість аналізувати події, реєструвати витоки інформації та виявляти недоліки у захисті даних. Однак, обробка великого обсягу даних може вимагати значних ресурсів, а недостатня чутливість алгоритмів моніторингу може призвести до пропуску потенційних загроз.

Ці методи та системи є лише деякими з існуючих стратегій захисту медичних даних. Кожна з них має свої переваги та недоліки, і вибір оптимального підходу варто робити з урахуванням конкретних потреб та особливостей лікарняного закладу.[2]

Архітектура багаторівневої комп'ютерної мережі для лікувального заклад

Побудова ефективної комп'ютерної мережі для лікувального закладу є критичним елементом для забезпечення доступності, безпеки та ефективного обміну медичною інформацією. Архітектура такої мережі повинна бути ретельно спроектована з урахуванням потреб безпеки медичних даних та забезпечувати високий рівень захисту від кіберзагроз.

Первинний рівень мережі включає в себе пристрої, які забезпечують з'єднання на місцях надання медичних послуг, такі як реєстратури, палати, лікарські кабінети тощо. На цьому рівні розташовані медичні пристрої, які збирають та передають дані, а також робочі станції для медичного персоналу. Цей рівень мережі має бути добре захищеним від несанкціонованого доступу, оскільки на ньому зберігається найбільш чутлива медична інформація.

Мережевий рівень відповідає за передачу даних між різними підрозділами лікувального закладу, такими як лабораторії, діагностичні відділення та адміністративні підрозділи. На цьому рівні важливо забезпечити ефективне керування трафіком даних та встановити механізми захисту від зовнішніх атак.

Центральний рівень мережі включає в себе серверне обладнання та системи зберігання даних, де зосереджується основна частина медичної інформації. На цьому рівні необхідно встановити потужні механізми захисту даних, такі як регулярні резервні копії, шифрування даних та відновлення після аварій. Архітектура багаторівневої комп'ютерної мережі для лікувального закладу повинна бути гнучкою та масштабованою, забезпечуючи високий рівень безпеки медичних даних на кожному рівні. [3].

Технічні засоби захисту

Забезпечення безпеки медичних даних у лікувальних закладах вимагає використання різноманітних технічних засобів та методів, спрямованих на захист інформації від несанкціонованого доступу та зловживань. Одним з найефективніших методів захисту медичних даних є використання криптографічних методів. Це включає в себе шифрування даних за допомогою сучасних криптографічних алгоритмів, які роблять інформацію незрозумілою для неправомірного доступу. Крім того, криптографічні підписи та цифрові сертифікати використовуються для забезпечення цілісності даних та автентифікації користувачів.

Ефективна система ідентифікації користувачів є ключовим елементом захисту медичних даних. Вона включає в себе використання унікальних ідентифікаторів, паролів, біометричних даних та двофакторної аутентифікації для підтвердження ідентичності користувача перед наданням доступу до системи.

Системи моніторингу доступу до медичної інформації дозволяють відстежувати активність користувачів у системі та виявляти незвичайну чи підозрілу активність. Вони надають можливість реагувати на потенційні загрози та вчасно приймати заходи для захисту медичних даних.. [4]

Регулююча політика безпеки

Розробка та впровадження ефективної регулюючої політики безпеки є критичними етапами у захисті медичних даних у лікувальних закладах. Перший крок у створенні регулюючої політики безпеки полягає у розробці документів, які визначають правила та процедури захисту медичних

даних. Це включає в себе визначення рівнів доступу до інформації, процедур аутентифікації користувачів, правил реагування на інциденти та інші аспекти безпеки даних.

Після розробки політик безпеки вони повинні бути впроваджені у практику лікувального закладу. Це включає в себе навчання персоналу щодо правил та процедур безпеки, встановлення технічних заходів захисту даних та створення механізмів контролю виконання політик.

Важливо мати процедури реагування на інциденти, які визначають кроки, які необхідно вжити у випадку порушення безпеки даних або потенційної загрози. Це включає в себе виявлення інциденту, аналіз причин його виникнення, відновлення даних та запобігання подібним ситуаціям у майбутньому.

Регулююча політика безпеки повинна відповідати вимогам законодавства з питань конфіденційності медичної інформації. Це означає дотримання норм GDPR, HIPAA та інших регулятивних вимог щодо збереження та захисту особистих медичних даних пацієнтів.[5]

Управління ризиками

Управління ризиками є важливою складовою в забезпеченні безпеки медичних даних у лікувальних закладах. Цей процес включає аналіз потенційних загроз безпеці даних та розробку стратегій їхнього запобігання та мінімізації.

Перший крок у управлінні ризиками - це ідентифікація та аналіз потенційних загроз безпеці медичних даних. Це може включати в себе оцінку загроз зовнішніх атак, внутрішніх порушень безпеки, технічних вад і недоліків систем, природних лих або інших факторів, що можуть впливати на безпеку даних.

На основі результатів аналізу ризиків розробляються стратегії запобігання та мінімізації ризиків. Це може включати в себе впровадження технічних засобів захисту, навчання персоналу щодо правил безпеки, створення регулярних резервних копій даних, а також впровадження процедур реагування на інциденти.

Управління ризиками є постійним процесом, який вимагає постійного моніторингу та оновлення стратегій. Це означає виявлення нових загроз та вразливостей, вдосконалення заходів захисту та адаптацію стратегій управління ризиками до змін у середовищі. [6]

Перспективи розвитку

У сфері захисту медичних даних швидко розвиваються нові технології та методи, спрямовані на покращення безпеки та конфіденційності інформації. Перспективи розвитку включають подальше поглиблення досліджень у сфері захисту медичних даних. Це охоплює проведення досліджень з виявлення та аналізу нових загроз, розробку ефективних методів захисту, а також оцінку ефективності заходів безпеки.

Однією з основних перспектив розвитку є впровадження новітніх технологій для забезпечення безпеки та конфіденційності медичних даних. Це може включати в себе використання штучного інтелекту для виявлення загроз, розробку блокчейн-технологій для забезпечення цілісності даних, а також впровадження квантової криптографії для захисту інформації.

Ще однією перспективою є розвиток стандартів та регулятивних рамок у сфері захисту медичних даних. Це дозволить стандартизувати підходи до захисту даних та забезпечити відповідність законодавству щодо конфіденційності та безпеки інформації в медичній сфері.

Перспективи розвитку у сфері захисту медичних даних є перспективними, і подальше вдосконалення технологій та методів дозволить забезпечити високий рівень безпеки та конфіденційності медичної інформації.[7]

Висновки

Було розглянуто важливі аспекти захисту медичних даних у лікувальних закладах. Зростання комп'ютеризації та цифровізації у сфері охорони здоров'я створює великі можливості для покращення надання медичних послуг, однак водночас вносить і нові виклики у сфері безпеки та конфіденційності медичних даних.

Було виявлено, що забезпечення безпеки медичних даних є критично важливим завданням для

забезпечення якості медичної допомоги та дотримання законодавства з питань конфіденційності інформації. Успішне впровадження та використання технічних засобів захисту, розробка ефективних політик безпеки, а також управління ризиками є ключовими елементами у забезпеченні безпеки медичних даних.

Важливість засобів у забезпеченні безпеки медичних даних є критичним. Постійне вдосконалення технологій та методів захисту даних є головним завданням. Створення нових стратегій та політик безпеки, а також підвищення рівня свідомості та навичок персоналу у сфері безпеки даних є першочерговою задачею. Шлях до забезпечення високого рівня безпеки та конфіденційності медичних даних та зміцнення довіри до медичної системи включає в себе спільні зусилля технічних експертів, адміністраторів мереж та медичного персоналу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Основи інформаційної безпеки: навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця : ВНТУ, 2018. – 316 с.
2. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
3. Computer Networking, a Top-Down Approach (7th Edition) / James F. Kurose Keith W. Ross – PEARSON, 2017. – 856 p. – ISBN-13: 978-0-13-359414-0.
4. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп’ютерних мережах : навч. посіб. — Кропивницький: Видавець Лисенко В. Ф., 2020. — 295 с.
5. Abouelmehdi, Karim, et al. "Big data security and privacy in healthcare: A Review." Procedia Computer Science 113 (2017): 73-80.
6. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс] – Режим доступу: www.dsszzi.gov.ua (дата звернення: 2024-05-8).
7. Oduor, Xavier Francis, and Zachary Bosire Omariba. "Application of cryptography in enhancing privacy of personal data in medical services." Int J Commun Inf Technol 3.1 (2022): 16-21.

Перестюк Олександр Вікторович — студент групи 1КІ-20б, факультет Інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, e-mail: alexandr.perestyuk@gmail.com

Томчук Микола Антонович — канд. техн. наук, доцент кафедри Обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: tomchuk@vntu.edu.ua

Oleksandr Viktorovych Perestyuk — student of group 1KI-20b, Faculty of Information Technologies, Vinnytsia National Technical University, e-mail: alexandr.perestyuk@gmail.com

Mykola Antonovych Tomchuk — Cand. Sc. (Tech), Docent of department of Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: tomchuk@vntu.edu.ua