Секція 1

МЕТОДИ ЗАХИСТУ ДАНИХ МЕДИЧНИХ КАРТОК ПАЦІЄНТІВ У BIG DATA. МЕДИЧНІ ТА ПЕРСОНАЛЬНІ ДАНІ

Луханін Б.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Землянко Г. А.

Актуальність. З кожним днем цифровізація все більше впроваджується в медичній сфері, де одна електронна база даних одразу інтегрує державну базу даних охорони здоров'я із приватними компаніями, через які люди, лікарі, аптеки та клініки мають онлайн-доступ до бази і можуть керувати записами, рецептами тощо. Проте слід пам'ятати, що збереження даних в електронному форматі завжди несе великі ризики оприлюднення даних завдяки кібератакам, навмисного розкриття лікарями/медичними сестрами чи випадкової помилки самого медичного сервісу.

Метою даної роботи є дослідження методів захисту даних медичних карток пацієнтів задля виявлення найбільш якісних та ефективних для медичних баз даних.

Основні положення. Дані, внесені до медичних карток, умовно можна поділити на: персональні дані та медичні дані. До першої категорії даних відносяться такі відомості: прізвище, ім'я, по-батькові, реєстраційний номер облікової картки платника податків, етнічне походження особи, тощо. Тому виявлені методів захисту даних медичних карток пацієнтів акцент робиться саме на захисті персональних даних.

Захист баз даних повинен бути багаторівневим.[1]. Починатися багаторівнева система безпеки повинна з контролю на рівні користувача. Захист бази даних на первинному етапі полягає в умінні розподіляти процеси, привілеї та права доступу. Загроза інформації може бути не тільки зовнішньою, але й внутрішньою [1].

Першим рівнем захисту є фізичний захист. Він включає в себе обмежене надання доступу до серверів з персональними даними, встановлення програм, які забороняють робити копії даних.[2]

Другим рівнем захисту є шифрування. Алгоритм шифрування перетворює інформацію в незрозумілі символи за допомогою математичного процесу, що навіть у разі злому системи інформація буде доступна для читання тільки авторизованим користувачам, які мають ключі шифрування [3].

Дієвим методом захисту може бути ізолювання особливо конфіденційної інформації. Особливо це може стосуватися безпосередньо персональних

даних, не включаючи медичної інформації, такий метод буде проти атак нульового дня. Навіть наявність і використання уразливості не дасть хакеру уявлення про всю структуру бази даних завдяки ізольованості, особливо цінної інформації.[1]

Третім рівнем захисту є захист IT-ресурсів. До нього належить метод управління змінами, передбачає управління внесенням змін до самої системи бази даних: злиття, редагування, тощо. Необхідно задокументувати, які зміни відбулися і чи не пошкодять вони безпечний доступ до бази даних та її додатків.

Висновки. Ведення медичних карток пацієнтів в електронному варіанті гарантують більшу надійність збереження інформації та її цілісність, але в той же час несе великі ризики опилення персональних даних у відкритому доступі. Результати дослідження показали, що захист медичних карток, в яких зберігаються персональні дані пацієнтів, має бути на трьох рівнях. Це дає контролювати: доступ до роботи із медичними картками; контроль ПЗ на комп'ютері; дозволяє підвищити захист так відокремити персональні дані від медичної інформації, контролювати потік даних та дій у базі даних.

Список літератури

1. Шифрування та захист баз даних. *iIT Distribution*. URL: https://iitd.com.ua/shifruvannja-ta-zahist-baz-danih/ (дата звернення: 15.11.2022);

2. Conceptual Model of Information Security. *Springer*. URL – https://link.springer .com/chapter/10.1007/978-3-030-66717-7_14 (дата звернення: 17.11.2022);

3. “Smart City” Technology: Conception, Security Issues and Cases. *Springer*. URL – https://link.springer.com/chapter/10.1007/978-3-030-94259-5_19 (дата звернення: 20.11.2022);

Відомості про авторів

Луханін Богдан Юрійович. Студент кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 096-875-81-12. b.lukhanin@student.csn.khai.edu

Землянко Георгій Андрійович, асистент кафедри комп’ютерних систем, мереж і кібербезпеки. g.zemlynko@csn.khai.edu