УДК 004.056

В. О. Клименко

В. А. Гарнага

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ДАНИХ ПАЦІЄНТІВ В МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто питання важливості забезпечення цілісності даних пацієнтів в медичних інформаційних системах. Проведено аналіз цілісності даних, загроз та методів захисту.

Ключові слова: захист медичних даних, цілісність даних, хакери, шкідливе програмне забезпечення, машинне навчання.

Abstract

This paper examines the importance of ensuring the integrity of patient data in medical information systems. An analysis of data integrity, threats, and protection methods is conducted.

Keywords: medical data protection, data integrity, hackers, malware, machine learning.

Вступ

Як відомо, цілісність є однією з основних характеристик в інформаційної безпеки [1]. Вона означає, що дані є точними, повними та достовірними. Іншими словами, гарантує те, що дані не будуть модифіковані, знищені або підроблені. Що, в свою чергу, є важливим в медичних закладах, які є об’єктами критичної інфраструктури. Адже, несанкціоноване втручання в медичні дані пацієнта може призвести до того, що лікар встановить ложний діагноз. А пацієнт мало того, що не отримає необхідного лікування, так ще й хибне лікування може значно погіршити його стан.

Метою даного дослідження є аналіз відомих методів та покращення рівня забезпечення цілісності даних пацієнтів в медичних інформаційних системах.

Аналіз цілісності даних

Для того, щоб забезпечити цілісність даних необхідно розібратися в низці питань. Наприклад, які є загрози для цілісності даних, які дані необхідно захищати, які існують методи та механізми для забезпечення цілісності даних.

Розпочнемо зі загроз цілісності даних. Загрози цілісності даних можна поділити на 3 види: навмисні й ненавмисні дії спричинені людьми та стихійні лиха. До стихійних лих відносяться: пожежі, повені, землетруси та інші. До навмисних дій можна віднести: хакерські атаки, віруси, шкідливе програмне забезпечення, несанкціонований доступ до даних (наприклад, інсайдером чи шпигуном). До ненавмисних дій відносяться: збої в роботі обладнання, збої в електропостачанні, помилки спричинені людським фактором. Все це відноситься до загроз, серед них є ті, на які можна вплинути (наприклад, якщо обмежити доступ до даних, то відповідно зменшиться ймовірність несанкціонованої модифікації даних) та ті, на які вплинути не вийде (наприклад, стихійні лиха, так як люди не навчилися їх контролювати). Тому для протидії неконтрольованим загрозам необхідно впроваджувати механізми відновлення. Наприклад, створювати резервні копії даних та зберігати їх в іншому місці.

Якщо розглядати загрози для медичного закладу, то стає зрозумілим, що ці заклади зберігають великі об'єми з даними пацієнтів, які звертаються до них по допомогу. До цих даних можна віднести як особисту інформацію (таку, як ім'я, прізвище, адреса проживання, номер телефону тощо), так і медичну інформацію (таку як, історія хвороби, результати обстежень, аналізів тощо). Раніше, до розвитку інформаційних технологій, вся ця інформація зберігалась на папері, тому якщо відбувались стихійні лиха вся ця інформація втрачалась, що в подальшому ускладнювало процес лікування хворих. Але зараз, з появою комп'ютерів, з'явилась можливість цифровізувати цю інформацію і зберігати її на фізичних носіях (компакт диски, флеш носії, жорсткі диски тощо) або в хмарних сервісах. Всі ці методи не тільки економлять використання паперу, а й надають можливість створення резервних копій та відновлення в разі втрати.

Загрози хакерських атак та методи протидії ним

З розвитком інформаційних технологій, також з'явились нові загрози. З'явились люди, які використовуючи недосконаліть розроблених систем, знаходять вразливі місця та використовують їх для корисливих цілей. Таких людей називають хакерами. Вони створюють та використовують шкідливе програмне забезпечення (віруси, хробаки, трояни та інші) та з їх допомогою мають можливість викрасти, модифікувати або взагалі видалити дані, щоб потім використати це для вимагання грошей [2].

Сфера охорони здоров'я — одна із лідерів у світі за зростанням кількості кібератак. У 2022 році на тиждень відбувалось 1 463 кібератаки, що на 74 % більше, ніж у 2021 му. Витоки даних у медичній сфері найдорожчі — у середньому вони обходились медичним закладам західних країн у 10 млн доларів США (дані CHECK POINT RESEARCH (CPR) TEAM за 2022 рік) [3].

Серед кібератак які вплинули на сферу охорони здоров'я варто виділити [4]:

- атака програми-вимагача WannaCry у травні 2017 року, яка зашифрувала дані та файли на 230 000 комп'ютерах у 150 країнах;
- атака програми-вимагача в 2018 році на обласну лікарню Хенкока в Грінфілді, США, в результаті якої лікарня заплатила викуп у розмірі чотирьох біткойнів на суму 55 000 доларів США;
- атака програми-вимагача в травні 2021 року на Управління охорони здоров'я в Ірландії, через яку були скасовані амбулаторні та медичні послуги по всій країні;
- атака в травні 2021 року, яка вивела з ладу інформаційні системи п'яти різних лікарень в Новій Зеландії;
- атака у вересні 2020 року, через яку записи пацієнтів у 400 лікарнях і медичних закладах у США і Великобританії стали недоступними, що призвело до затримки надання допомоги пацієнтам і зміни маршрутів машин швидкої допомоги.

Методи забезпечення цілісності даних

Для забезпечення цілісності даних використовують різні методи. Серед них: гешування, контрольні суми, цифрові підписи, системи виявлення вторгнень, антивірусні засоби та інші [5]. Кожен з цих методів має свої переваги та недоліки. Через те, що ці методи призначені для різних цілей, часто використовуються одразу декілька методів для кращого захисту.

Гешування та контрольні суми використовуються для виявлення несанкціонованих змін у файлі, або втрат даних під час передачі. Цифрові підписи використовуються для підтвердження автентичності даних (найкращим аналогом є печатка або штамп на документі). Системи виявлення вторгнень повідомляють про втручання несанкціонованого об'єкту в інформаційну систему. Вони дозволяють вчасно реагувати на потенційні кібератаки та запобігати втратам даних. Системи типу honeypot дозволяють не тільки вчасно реагувати на кіберзагрози, а й знаходити вразливості та досліджувати методи хакерів для покращення протидії ним. Антивірусні засоби використовуються для перевірки файлів на наявність шкідливого коду, який може нашкодити системі та даним, які в ній зберігаються.

Використання машинного навчання у сфері охорони здоров'я

За останні роки все більш популярним стає використання машинного навчання і медичні заклади не є винятком. Машинне навчання дозволяє вирішувати широкий спектр задач. Спеціалісти навчають моделі, як на графічних зображеннях (знімки рентгенівські, КТ тощо), так і на текстових даних (які

включають в себе історії хвороб, результати обстежень, діагнози та плани їх лікувань). Машинне навчання використовується для допомоги лікарям з виявленням деяких видів раку на ранніх стадіях. Однією з таких моделей є Watson for Oncology (WFO) розроблена компанією IBM. Дана модель набула широкого поширення під час досліджень в Китаї [6]. Серед 182 пацієнтів, які вперше отримували протипухлинну терапію WFO надала рекомендації щодо лікування для всіх підтверджених випадків (149). 98 з підтверджених випадків отримали рекомендації, які задовільнили лікарів та після узгодження було розпочато лікування. В інших 51 випадках лікарі надали інші рекомендації, які відрізнялись від WFO.

Хоч використання машинного навчання і спрощує процес встановлення діагнозів і надання рекомендацій для лікування, але результати не завжди є задовільними, тому повністю замінити лікарів штучним інтелектом неможливо. Проте, це спрощує та пришвидшує процес лікування пацієнтів і забезпечує високу точність і достовірність результатів. Завдяки подібним моделям штучного інтелекту також стає можливим перевірка некомпетентних лікарів. Якщо лікування, яке запропонувала модель та лікування лікаря будуть часто відрізнятись, то з часом підніметься питання у чому проблема: в погано натренованій моделі, чи в некомпетентному лікарі? Тому процес впровадження систем зі штучним інтелектом створить процес, в якому лікар та модель будуть перевіряти одне одного.

Висновки

У даній роботі розглянуто питання важливості забезпечення цілісності даних, особливо в медичних закладах. Проведений аналіз загроз цілісності даних та часті хакерські атаки на заклади охорони здоров'я вказують на те, що необхідним є розробка та покращення існуючих методів захисту інформації. Адже, існуючі вразливості не тільки дозволяють хакерам збагачуватись, а й створюють проблеми для надання послуг пацієнтам, які можуть знаходитись в тяжкому стані. Також, було проаналізовано методи забезпечення цілісності даних та приклади й переваги використання штучного інтелекту в медичних закладах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Лужецькии В. А. Основи інформаційної безпеки [Текст] : навчальний посібник / В. А. Лужецькии, А. Д. Кожухівський, О. П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.
2. Каплун В.А., Майданюк В.П. Д 81 Захист операційних систем. Навчальний посібник. – Вінниця: ВНТУ, 2006. – 180 с.
3. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks. Check Point. URL: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/ (accessed: 15.11.2024).
4. Загрози кібербезпеці в галузі охорони здоров'я | ESKA Блог. *ESKA*. URL: https://eska.global/blog/zagrozi-kiberbezpeci-v-galuzi-ohoroni-zdorovya (дата звернення: 15.11.2024).
5. Євсеєв С. П. Гешування даних в інформаційних системах [Текст] : монографія / С. П. Євсеєв, О. Ю. Йохов, О. Г. Король. – Харків : Вид. ХНЕУ, 2013. – 312 с.
6. Using Artificial Intelligence (Watson for Oncology) for Treatment Recommendations Amongst Chinese Patients with Lung Cancer: Feasibility Study - PMC / C. Liu et al. *PubMed Central*. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC6231834/ (accessed: 18.11.2024).

Клименко Володимир Олександрович – студент групи 1БС-23м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vovaklim2000@gmail.com.

Гарнага Володимир Анатолійович – к., т., н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: garnaga.volodymyr@vntu.edu.ua.

Volodymyr Klymenko – Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vovaklim2000@gmail.com

Volodymyr Garnaga – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Vinnytsia. email: garnaga.volodymyr@vntu.edu.ua.