УДК 004.49

П. П. Малініч[1]
І. П. Малініч[1]
Ю. О. Крижановська[2]

ФАКТОРИ ВИТОКУ КОНФІДЕНЦІЙНИХ ДАНИХ З СУЧАСНИХ HEALTHCARE-ДОДАТКІВ

[1] Вінницький національний технічний університет;
[2] Вінницький національний медичний університет ім. М. І. Пирогова

Анотація

В публікації приділено увагу проблемам кіберзахисту різних інформаційним healthcare-систем та додатків, а також як це регулюється чинним законодавством та директивами Європейського Союзу. Розглянуто та доповнено перспективи вирішення проблем кіберзахисту інформаційним healthcare-систем та додатків.

Ключові слова: кібербезпека, мобільні додатки, хмари, закон, право, персональні дані, GDPR.

Abstract

This publication pays attention to the problems of cyber protection of various healthcare IT systems and applications, as well as how it is regulated by current legislation and directives of the European Union. Prospects for solving the problems of cyber protection of healthcare IT systems and applications were considered and supplemented.

Keywords: cybersecurity, mobile apps, cloud, law, right, personal data, GDPR.

Вступ

У наш час із розвитком систем штучного інтелекту значними темпами розвивається ринок healthcare-додатків та систем. Сучасні AI-моделі незважаючи на помилки здатні більш точно виконувати діагностування, прогнозування та пошук рішень для вирішення проблемних завдань. Це часто стає корисним, особливо у випадках коли власне людських можливостей для цього недостатньо. Крім того деякі healthcare-додатки можуть поліпшити ситуацію у державах де ускладнений доступ до медицини. Однак для цього великим компаніям необхідно багато даних для тренування AI-моделей, і щоб їх отримати вони пропонують винагороду людям, які можуть ними поділитись. Багато сучасних онлайн-сервісів та мобільних додатків працюють за моделлю "персональні дані клієнта у обмін на послуги". Тобто такий підхід передбачає плату персональними даними за надані послуги чи принаймні робить послуги більш дешевими. Подібну модель використовують соціальні мережі, такі як Facebook, Instagram, TikTok та інші. Незважаючи на те що дані у healthcare інформаційних системах потребують особливого захисту, як це передбачено законодавством багатьох країн, модель "персональні дані у обмін на послуги" гарно працює і у цій сфері.

Огляд стану проблеми

Звертаючись за допомогою до лікаря, пацієнт ділиться персональними даними не лише для отримання належного рівня медичного обслуговування та психологічної підтримки, але і для одержання адекватного лікування. Хворий повідомляє таку інформацію: паспортні дані, номери телефону, адресу, майновий та сімейний стан, діагнози, результати обстежень і проведених досліджень, рецептурні призначення. Крім того, пацієнт передає дані про найближчих родичів та довірених осіб, до яких можливе звернення в разі надзвичайної ситуації [1]. Довіряючи персональну інформацію лікарю та медичним установам, хворий має право на збереження медичної таємниці, що закріплене в Основах законодавства України про охорону здоров'я (статті 39 (ч. 2, 5), 39-1, 40, 43 (ч. 1)). Умисне розголошення особистих даних пацієнта тягне за собою кримінальну відповідальність згідно зі статтею 145 Кримінального кодексу України.

Зважаючи на вищезазначене, шахраї намагаються отримати доступ до персональних даних з метою вимагання грошових виплат в обмін на нерозголошення інформації про стан пацієнта. Це призводить до несвоєчасного або неправильного лікування, втрату довіри до подальшої терапії, медичного працівника та закладу, зловживання рецептурними препаратами, фінансові втрати для установ

(штрафи, неотриманий прибуток тощо).

Зокрема 29 січня 2015 року американська компанія Anthem Blue Cross, повідомила, що шляхом зламу їхніх серверів було викрадено інформацію близько 78,8 мільйонів людей. Зловмисники отримали доступ до мережевих облікових даних щонайменше п’яти співробітників. Засобом міг бути «фішинг» – використання шахрайської електронної пошти, щоб обманним шляхом змусити будь-кого з цих співробітників розкрити його ідентифікатор мережі та пароль. Інформація, до якої було отримано доступ, включала імена, дати народження, номери соціального страхування, ідентифікаційні номери медичного закладу, домашні адреси, адреси електронної пошти, інформацію про роботу, дані про доходи. Існує думка, що ці дані було перепродано на чорному ринку. Сама ж компанія зіткнулася із колективними позовами у 2017 році, що обійшлося їй в 115 мільйонів доларів [2].

Також під час пандемії COVID-19 в одній із приватних клінік Дніпра стався витік персональних медичних даних. Йдеться про конфіденційну інформацію працівників, пацієнтів, ПІБ, дати народження, адреси проживання, e-mail, діагнози, дані медичної картки (що становить медичну таємницю), включаючи результати аналізів, інформацію про захворювання, результати проведення ПЛР-тестів, списки хворих на COVID-19. Також у зловмисників був доступ до внесення змін у призначення ліків, редагування записів у протоколі "Надання медичної допомоги для лікування коронавірусної хвороби (COVID-19)", що могло вплинути на подальше лікування і життя людей. Витік стався внаслідок помилок конфігурації в інформаційних системах та базах даних медичного закладу, які мали доступ до мережі Інтернет. На жаль, сама клініка майже не реагувала на попередження Національного кординаційнаціного центру кібербезпеки про поширення даних. Проте недбале ставлення до збереження персональної інформації клієнтів було приводом для притягнення керівництва даного закладу до відповідальності.

Сьогодні багато компаній, які працюють з персональними даними клієнтів, можуть постраждати від дій кіберзлочинців, що у свою чергу може призвести до витоку даних та їх подальшого продажу на чорному ринку. Кіберзлочинці можуть використовувати втрачені дані для отримання грошового викупу, шантажу та заохочення до злочинного колабораціонізму. Зливи даних про здоров’я людей становлять особливу небезпеку оскільки відкривають можливості зловмисникам для маніпулювання такими людьми з метою матеріального збагачення, схилення їх до співпраці чи псування репутації.

Основа проблеми витоку даних клієнтів полягає у слабкому кіберзахисті програмних додатків, інших інформаційних систем та мереж. Іншою проблемою є людський фактор, коли співробітники, що мають доступ до даних з обмеженим доступом, передають його іншим особам чи здійснюють несанкціоноване копіювання та передачу такої інформації стороннім особам.

Багато інформаційних healthcare-систем та додатків мають схожу архітектуру (рис. 1), у ній є дві сторони: клієнта та надавача послуг. У багатьох випадках клієнт не має безпосереднього доступу до інформаційної системи і може отримати доступ до даних через кол-центр чи за допомогою звернення до співробітників рецепшину. З розвитком AI-систем у медичній сфері та різних сенсорів, що збирають дані у реальному часі присутність подібних інформаційних систем розширилась і на стороні клієнта.

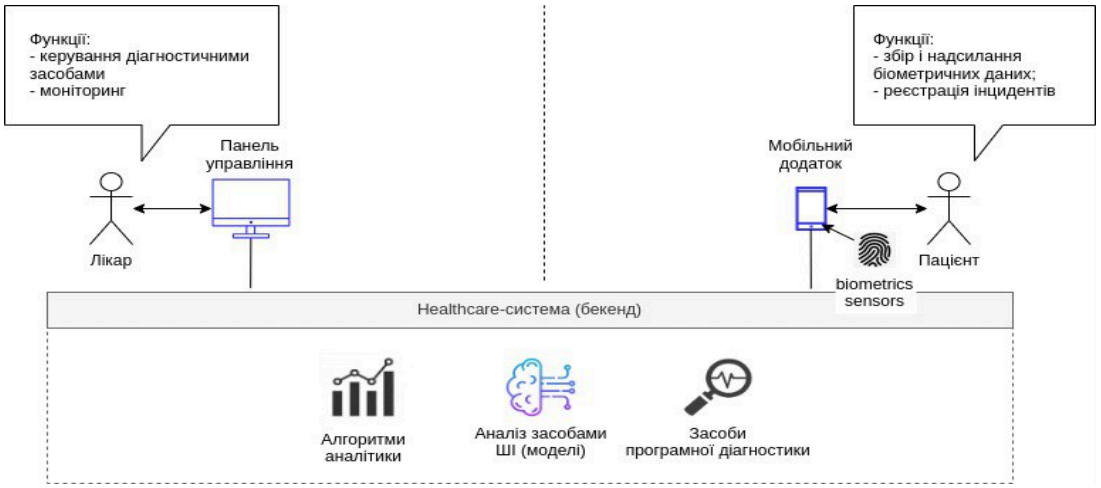

Рис. 1 – Типова архітектура сучасних healthcare-систем

У подібній архітектурі можливі як мінімум п’ять каналів витоку конфіденційної інформації: медичний персонал, сам пацієнт, програмне забезпечення на комп’ютерах та інших пристроях обох сторін, а також хмарна чи серверна інфраструктура. Витік даних може відбуватись без відома та умислу будь-якої із двох сторін, якщо має місце кіберзлочин або інфікування окремих комп’ютерів чи всієї інфраструктури шкодоносним програмним забезпеченням. Маючи навіть часткові дані про здоров’я жертви кіберзлочинці мають можливість за допомогою AI-інструментів відновити більш повну картину її здоров’я.

Іншим фактором ризику витоків персональних даних є розвиток квантових обчислень. Крім вагомих переваг для медицини, є і ризики розшифрування раніше переданих даних [4]. Завдяки застосуванню принципу "зберігай зараз, розшифруєш потім" (англ. *Store now, decrypt later*) та MITM-атак зловмисники можуть розшифрувати дані цілком захищених додатків, які раніше використовували нестійкі до квантового розшифрування алгоритми шифрування. Крім власне healthcare-систем це може стосуватись і месенджерів, роль яких у сучасній медицині важко недооцінити.

Подальші перспективи

У Європейському Союзі та США діють досить потужні стандарти захисту персональних даних споживачів: GDPR та HIPAA відповідно. Вони зобов'язують медичні установи приділяти значну увагу захисту персональних даних, інвестувати у даний процес та звітувати про всі можливі витоки. Нині є ряд нововведень у законодавстві України [4, 5], які наближують базу стандартів кіберзахисту до прийнятого у ЄС Загального регламенту захисту даних [6].

Висновки

На даний момент не відомо, чи стануть конфіденційні дані українців мішенню для шахраїв і чи понесуть медичні заклади відповідальність за їх втрату, особливо у час повномасштабної війни.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Чутливі дані [Електронний ресурс] // Офіційний сайт Міністерства охорони здоров'я України. – Режим доступу: https://moz.gov.ua/chutlivi-dani (дата звернення: 29.04.2024). – Назва з екрана.
2. Moffit, Robert E., and Ben Steffen. "Health care data breaches: A changing landscape." Maryland Health Care Commission (2017): 1-19.
3. Витік інформації з клініки Дніпра [Електронний ресурс] // Офіційний сайт Ради національної безпеки і оборони України. – Режим доступу: https://www.rnbo.gov.ua/ua/Diialnist/4711.html?fbclid=IwAR2wH7PZn6-AuJJjBj9vPIjg2PbDve3DXq4MPPND-y3I0RTSvVQd-9YoKCg (дата звернення: 29.04.2024). – Назва з екрана.
4. Ur Rasool R, Ahmad HF, Rafique W, Qayyum A, Qadir J, Anwar Z. Quantum Computing for Healthcare: A Review. Future Internet. 2023; 15(3):94. – Access mode: https://doi.org/10.3390/fi15030094
4. Україна. Закони. Про захист персональних даних [Текст] : Закон України : редакція від 27.04.2024 – Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 29.04.2024).
5. Україна. Закони. Основи законодавства України про охорону здоров'я [Текст] : Закон України : редакція від 19.04.2024 – Режим доступу: https://zakon.rada.gov.ua/laws/show/2801-12#Text (дата звернення: 29.04.2024).
6. General Data Protection Regulation (GDPR) [Website] // Regulation (EU) 2016/679 – EUR-Lex : 02016R0679-20160504 – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 (дата звернення: 29.04.2024).

Малініч Павло Павлович – асистент кафедри Програмного забезпечення, Вінницький національний технічний університет

Малініч Ілля Павлович – асистент кафедри Комп’ютерних наук, Вінницький національний технічний університет, e-mail: malinich@vntu.edu.ua

Юлія Олександрівна Крижановська – студентка групи 4а, медичний факультет №1, Вінницький національний медичний університет ім. М. І. Пирогова, Вінниця

Pavlo Malinich – Assistant Lecturer of Software Development department, Vinnytsia National Technical University, Vinnytsia

Illia Malinich – Assistant Lecturer of Computer Science department, Vinnytsia National Technical University, Vinnytsia, e-mail: malinich@vntu.edu.ua

Yuliia Kryzhanovska – Student of first medical faculty, Vinnytsia National Memorial Medical University of N. I. Pirogov, Vinnytsia