3. Мазурець О.В. «Методи та системи штучного інтелекту», режим доступу https://msn.khnu.km.ua/course/view.php?id=4237

4. Орешков В.И. Паклин Н.Б. «Консолидация данных - ключевые понятия» режим доступу https://www.cfin.ru/itm/olap/cons.shtml

УДК 004.056.52

ВДОСКАНАЛЕННЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ У ЕЛЕКТРОННОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я «eHealth»

А.В.Овєчкін, О.В.Кручінін
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Згідно до світових тенденцій, критичні вразливості від дій зловмисників щодо витоку великої кількості інформації з обмеженим доступом зазнає сфера медичного обслуговування. Вразливості медичних систем, які використовуються у лікарнях, в купі зі зухвалими діями співробітників призводять до викрадення цілих баз з персональними даними пацієнтів, лікарів, аптек, лікарень та інших суб'єктів медичних відношень. Витрати, пов'язані з порушенням конфіденційності інформації, становлять 3,92 мільйона доларів станом на 2019 рік, а сама галузь охорони здоров'я зазнає збитки у розмірі більш ніж 400 доларів за один медичний запис пацієнта [1]. Експерти прогнозують на 2026 рік, що ринок кібербезпеки у сфері охорони здоров'я буде оцінюватися майже у 27 млрд. доларів.[2].

Це питання актуальне і для України, у зв'язку з активним впровадженням електронної системи охорони здоров'я «eHealth». Сутність системи складається в тому, що вона забезпечує обмін конфіденційною медичною інформацією, з записом та подальшим зберіганням її у центральній базі даних (ЦБД) [3].

Доступ до даних ЦБД надається користувачам через спеціально розроблені медичні інформаційні системи (МІС) – інтерфейси, які поєднують лікарні або інші медичні заклади зі сховищем даних про пацієнтів, з можливостями отримання інформації, її модифікації або наповнення новими записами [4]. Ці нововведення у діяльності медичних установ, при недбалому використані їх, можуть спровокувати створення вразливостей, які можуть бути використані кіберзлочинцями.

У медичних системах найчастіше використовують рольову модель. Вона дуже проста в початковій імплементації за рахунок того, що в медичному середовищі чітко регламентована роль кожного лікаря та співробітника лікарні, з чітко встановленими дозволами на виконанні тих чи інших операцій.

Завдання розмежування доступу за рахунок розподілу ролей лише частково вирішена у «eHealth» – існуючі ролі дуже загальні та не відповідають усім сучасним потребам щодо розмежування доступом у лікарських закладах [5]. Розширення цієї моделі зі сторони «eHealth» не гарантує гнучкості та адаптивності для кількох різних за структурою та призначенням закладів, а також у надзвичайних випадках. Наприклад, підписуючи декларацію про вибір

лікаря, що надає первину медичну допомогу, пацієнт дає згоду на обробку своєї персональної інформації не тільки обраному лікарю, але ще й будь-якім лікарям, які можуть надавати допомогу.

Тому є необхідність в розширені існуючої моделі. Вона може зініціюватися зі сторони медичного закладу та бути складовою МІС, але це збільшує вартість та складність її розробки.

Універсальним варіантом є застосування додаткової програмної системи – системи управління основними даними (УОД), з доданням рольової моделі розподілу доступом. Розробка моделі має виконуватися представниками служб безпеки та керівниками кожного закладу, що використовують ті МІС, що планують підключення її до своїх систем, разом з представниками компанії-розробника системи УОД.

Саме варіант створення уніфікованої системи, з врахуванням потреб кількох МІС та з передбаченням можливості масштабування такої системи ще на стадії її проектування є більш ефективним рішенням. Треба розуміти, що проектування однієї тільки рольової моделі розподілу доступом потребує багатограного та поглибленого вивчення принципів роботи медичного закладу, дотримання норм законодавчого права, гарантування безпеки та надійності у функціонуванні такої системи, що пов'яже великі ключові ланки одного ланцюга обміну медичною інформацією між пацієнтами, лікарями, підприємцями та іншими можливими суб'єктами медичних процесів.

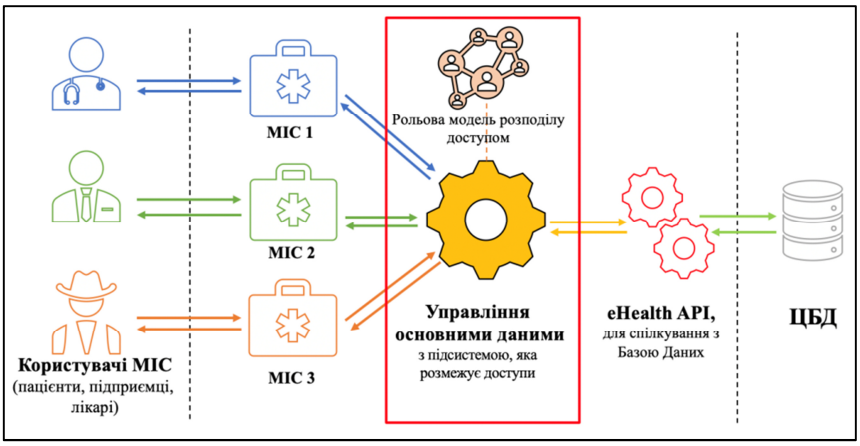

Рис 1. Структурна схема потоків даних від користувачів МІС до ЦБД з додатковою проміжною системою УОД

Механізм УОД це така сукупність інструментів та процесів обробки, яка займається збиранням та групуванням даних, як у випадках створення даних, так і в випадку запитів на їх отримання. Також вона призначена для узгодження бідь-яких систем між собою, які будуть підключені до неї [6]. У запропонованому підході головною метою такої системи є надання інформації користувачам за запитами до МІС, яка точно потребується для виконання його обов'язків відповідно до наданої йому ролі та дозволів.

Розроблятися така система може незалежно від МІС, на будь-якій мові програмування з використанням різноманітних додаткових технологій,

незалежно ні від бази даних та «eHealth API», що надає інтерфейси для роботи з базою, ні від МІС, яка розроблялася сторонніми розробниками. Її вплив на загальний процес роботи користувачів МІС з базою даних складається в тому, що наприклад, по запиту лікаря на отримання даних про пацієнта, УОД отримує увесь набір даних, потім зіставляє її з роллю користувача, що передається при запиті частіше всього через так звані «HTTP заголовки». Встановлюючи відповідності між нею та її дозволами, система відфільтровує ті дані, до яких немає дозволів у конкретній ролі, та сформовану відповідь надсилає до МІС, яка в свою чергу вже інтерпретує її для користувача.

Висновки. Таким чином, використання додаткової системи дозволяє запобігти випадкам несанкціонованого доступу до інформації. Але водночас зобов'язує її забезпечувати відповідний рівень захисту інформації, яка циркулює через УОД. Запропонована системи повинна запобігти несанкціонованому копіюванні, та спотворенню інформації, що передається через неї. Основним завданням УОД є обмеження потрапляння до МІС даних с порушенням встановлених правил розмежування доступу. В такому випадку, можна забезпечити більш високий рівень захисту інформації, та контролювати її потоки, контролюючи хто, та в якому обсязі, отримує медичні дані.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Американський університет вирішує проблеми з кібербезпекою в галузі охорони здоров'я за допомогою першої національної програми «The Daily Swig – новини кібербезпеки» : веб-сайт. URL: https://portswigger.net/daily-swig/us-university-tackles-healthcare-cybersecurity-woes-with-first-national-program (дата звернення 12.11.2019).

2. Тенденції кіберзахисту у сфері охорони здоров'я «Reports And Data» : веб-сайт. URL: https://www.globenewswire.com/news-release/2019/08/26/1906602/0/en/Healthcare-Cybersecurity-Market-To-Reach-USD-27-10-Billion-By-2026-Reports-And-Data.html (дата звернення 12.11.2019).

3. «Електрона система охорони здоров'я» : веб-сайт. URL: https://ehealth.gov.ua

4. https://ain.ua/2017/11/21/kak-razrabatyvalas-ehealth/ (дата звернення 12.11.2019).

5. Технічна документація eHealth : веб-сайт. URL: https://edenlab.atlassian.net/wiki/spaces/EH/pages/2004415/Scopes+model (дата звернення 12.11.2019).

6. Управління майстер даними. «База знань в області корпоративних сховищ даних» : веб-сайт. URL: prj-exp.ru/integration/about_mdm.php (дата звернення 12.11.2019).