УДК 004.056.5

**РОЛЬОВА МОДЕЛЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТА МЕДИЧНОЇ УСТАНОВИ**

*Мірошниченко М.М., науковий керівник Ізмайлова О.В.*

Питання автоматизації документообігу в медичній галузі наразі є актуальним для нашої держави – це впровадження медичних інформаційних систем (МІС)[1] у медичні установи, електронних медичних карток пацієнтів, електронних рецептів і т.д. Нова система реалізації медичних послуг має ряд суттєвих особливостей, що ставлять підвищені вимоги до дотримання політики конфіденційності та безпеки даних.

Розв’язання питання забезпечення захисту персональних даних пацієнтів медичної установи стає ще більш актуальним в умовах запровадження електронної медичної карти, яка в ракурсі тестового режиму стартувала в Україні з 1 березня 2019 р. [2]. Застосування електронної медичної карти базується, з одного боку, на умовах забезпечення можливості для користувача будь-якої вікової категорії та з будь-яким рівнем освіти швидкого і коректного доступу до медичної картки, необхідності швидкого і своєчасного відгуку співробітників лікувального закладу, можливості переадресації електронної послуги до іншої лікувальної установи, можливості для пацієнта при одноразової реєстрації використовувати якомога більше сервісів (наприклад, взаємодія з декількома лікувальними установами різних рівнів) та, з іншого боку, на тому, що підписуючи декларацію про вибір сімейного лікаря, терапевта чи педіатра пацієнт надає право медичній установі на обробку персональних даних. Інформація медичної карти включає в себе не лише дані його ідентифікації, а й подальші різноаспектні записи з різних джерел, розголошення яких може нанести різного роду шкоди як пацієнту, так і репутації медичної установи. Все це обґрунтовує необхідність підвищеної уваги до дотримання безпеки та конфіденційності інформації, яка є запорукою формування довіри пацієнтів до даного виду взаємодії з лікувальним закладом.

 Був проведений аналіз ризиків безпеки даних медичної установи, що базувався на встановленні та оцінці видів загроз та вразливостей різних компонентів медичної карти та негативних наслідків їх реалізації. Аналіз підтвердив значущість та актуальність питання створення системи захисту даних, в розробці якої однією з центральних проблем є розвиток функціональних можливостей та удосконалення моделей, методів та механізмів підсистеми управління доступом. Аналіз особливості сучасних вимог до ведення електронної карти, потреб до конфіденційності та цілісності її даних обґрунтовує висновок про доцільність побудови системи захисту персональних даних пацієнта на основі рольової моделі розмежування доступу (з англ. Role-Based Access Control (RBAC) (рис.1).

Рольова модель (RBAC) базується на використанні формалізованих шаблонів в установі, які містять необхідні повноваження для здійснення певної діяльності. Для вирішення більшості конфіденційності та цілісності даних установи даних медичної карти пропонується визначити структуру рольових повноважень, що надаються співробітникам та зовнішнім користувачам (сімейний лікар, спеціалізований лікар, інша медична установа, медсестра, пацієнт тощо).

Основою RBAC є поняття ролі[4]. Під роллю розуміється сукупність дій і обов'язків, пов'язаних з певним видом діяльності. Системний адміністратор визначає та створює різні ролі згідно з політикою безпеки, призначає ролям відповідні повноваження, а користувачеві призначає відповідну роль.



Рис.1 Рольова модель управління доступом

Таким чином, організація управління доступом розділена до його посадових обов'язків на дві частини: призначення повноважень кожної ролі і призначення користувача на роль, що дозволяє логічно розділити користувача і права на доступ. Рольовий управління доступом значно полегшує процес адміністрування політики безпеки. Крім цього RBAC реалізує ієрархію ролей, принцип мінімальних привілеїв і принцип поділу відповідальності.

Цей підхід має такі переваги:

* Можливість побудови ієрархії ролей з успадкуванням набору прав. Це дозволяє спростити та удосконалити рольову модель.
* Просто і ефективно здійснюється надання однакових прав великій кількості користувачів – досить призначити користувачам одну роль.
* При необхідності зміни набору прав великій кількості користувачів досить змінити набір прав в ролі.
* Можливість реалізації принципу поділу повноважень (з англ. SoD – Segregation of Duties). Це значно знижує ризик надання користувачам надлишкових повноважень, наприклад, коли дві ролі не можуть бути в один момент часу призначені одному користувачеві.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. portal.ehealth.gov.ua [Електронний ресурс] «ОБРАТИ МЕДИЧНУ ІНФОРМАЦІЙНУ СИСТЕМУ». – Режим доступу: <https://portal.ehealth.gov.ua/providers.html> (дата звернення 20.03.2019)
2. moz.gov.ua [Електронний ресурс] «Як і коли почне працювати електронна медична картка в Україні». – Режим доступу: <http://moz.gov.ua/article/reform-plan/jak-i-koli-pochne-pracjuvati-elektronna-medichna-kartka-v-ukraini> (дата звернення 21.03.2019)
3. zakon.rada.gov.ua [Електронний ресурс] «Термін «Модель загроз»». – Режим доступу: <https://zakon.rada.gov.ua/laws/term/15947> (дата звернення 25.03.2019)
4. club.cnews.ru [Електронний ресурс] «Ролевая модель и метод контроля доступа». – Режим доступу: <http://club.cnews.ru/blogs/entry/rolevaya_model_i_metod_kontrolya_dostupa> (дата звернення 25.03.2019)