

УДК 004.056.55

РОЗЛОМІЙ І.О.*, ЗАХАРОВА М.В.** , ЛЮТА М.В.***

*Черкаський національний університет імені Богдана Хмельницького

**Черкаський державний технологічний університет

***Київський національний університет технологій та дизайну

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ МЕДИЧНИХ ДАНИХ НА ОСНОВІ МОДЕЛІ РОЗМЕЖУВАННЯ ДОСТУПУ TAKE-GRANT

Мета. Розробка моделі розмежування доступу до персональних медичних даних (ПМДн) для забезпечення їх конфіденційності.

Методика. В статті розглядаються питання забезпечення захисту ПМДн при обробці в медичних інформаційних системах (МІС). Проводиться аналіз можливих загроз інформаційної безпеки в МІС. Досліджено перелік вповноважень суб'єктів над ПМДн з метою побудови моделі розмежування доступу до конфіденційної інформації.

Результати. Розглянуті особливості організації автоматизованої обробки ПМДн. Перераховані головні проблеми, пов'язані з впровадженням МІС. Приведено перелік необхідних заходів для забезпечення захисту ПМДн. Запропонована модель розмежування доступу Take-Grant.

Наукова новизна. На основі деталізованої схеми класифікації ПМДн, суб'єктів та їх вповноважень, побудовано граф надання визначених прав доступу до конкретного об'єкту, що є основою дискреційної політики безпеки МІС.

Практична значимість. Захист МІС є необхідністю, оскільки дані системи можуть значно підвищити безпеку і якість медичної допомоги, збільшити оперативність подання медичної інформації, забезпечити комфортність у роботі медичного персоналу.

Ключові слова: медична інформаційна система, персональні дані, інформаційна безпека, конфіденційність, модель Take-Grant.

Вступ. Комп'ютерні технології інтенсивно стали використовуватися в галузі охорони здоров'я. Більшість медичних установ, приватних клінік, санаторно-оздоровчих комплексів впроваджують в своїй практиці інформаційні системи [1]. Однак, це нове інформаційно-технічне середовище також створює масу нових проблем, пов'язаних з забезпеченням конфіденційності медичної інформації, а також збереженням лікарської таємниці.

Постановка завдання. Проблеми, пов'язані з організацією автоматизованої обробки і захисту ПМДн залишаються актуальними в діяльності медичних установ та закладів охорони здоров'я. Значна їх частина пов'язана із підвищенням кількості зацікавлених суб'єктів і, як наслідок, зростанням злочинності в сфері інформаційних технологій. Це суттєво ускладнює контроль доступу до конфіденційних даних. Організація обробки і захисту ПМДн медичного персоналу і пацієнтів, збереження лікарської таємниці – одне з найважливіших завдань, яке доводиться вирішувати в закладах охорони здоров'я. Актуальність проблеми захисту персональних медичних даних сьогодні не викликає сумнівів. Захист персональних медичних даних є однією з найбільш гострих проблем в інформатизації організацій медичної галузі [2].

Результати дослідження. Для обробки медичних даних використовуються медичні інформаційні системи (МІС), які передбачають наявність автоматизованого документообігу, електронних архівів медичної інформації, а також електронної історії хвороби кожного пацієнта. МІС – комплексна автоматизована інформаційна система для автоматизації

діяльності лікувально-профілактичного закладу [3]. В МІС обробляються ПМДн – відомості про стан здоров'я громадян, які відносяться до лікарської таємниці і є конфіденційними. Слід зауважити, що медицина – галузь, в якій питання збереження таємниці, конфіденційності, цілісності та достовірності ПМДн заслуговують особливої уваги. Насамперед, це пов'язано з правами людини про нерозголошення конфіденційної інформації, персональних даних [4]. Проте, завжди є суб'єкти, які зацікавлені в розсекречуванні інформації з метою використання її в корисних цілях. Одним з способів порушення інформаційної безпеки МІС є отримання несанкціонованого доступу до інформаційних ресурсів, тому при розробці системи захисту необхідно враховувати проблему розмежування доступу.

Одним з розповсюджених підходів до захисту інформаційних систем є використання дискреційної політики безпеки, яка володіє відносно простою реалізацією механізмів захисту інформації [5]. Основою такої політики є керування розмежуванням доступу до ресурсів МІС. Принципи дискреційної політики визначаються правилами, згідно яким розподіляються права доступу до об'єкту між ідентифікованими суб'єктами. Особливо актуальною проблема розмежування доступу є по відношенню до МІС, оскільки в ній циркулює конфіденційна інформація. Цілком логічно, що певні суб'єкти (пацієнти, лікарі) повинні мати чітко визначені права на той чи інший об'єкт. Правила розподілу прав доступу і аналіз їх впливу на МІС можна описати за допомогою моделі Take-Grant. Дана модель підтверджує чи компрометує ступінь захисту інформаційної системи і представляє її у вигляді направленого графа, в якому показані правила доступу суб'єктів до об'єкта. Формально описати модель Take-Grant можна наступним чином: представимо сукупність об'єктів, а саме ПМДн в вигляді множини $P = (p_1, p_2, \dots, p_n)$. Схематично структуру ПМДн можна зобразити наступним чином рис.1.



Рис. 1. Структура персональних медичних даних

Множину суб'єктів $S = (s_1, s_2, \dots, s_n)$ складають всі зацікавлені особи, тобто медичний персонал, пацієнти. Доступ до конфіденційної інформації може надаватися для різних цілей таких як: перегляд, редагування, копіювання, внесення змін, видалення та інших.

Взаємозв'язок суб'єктів та відповідних їм вповноважень над об'єктами і конфіденційними даними показаний на рис. 2.

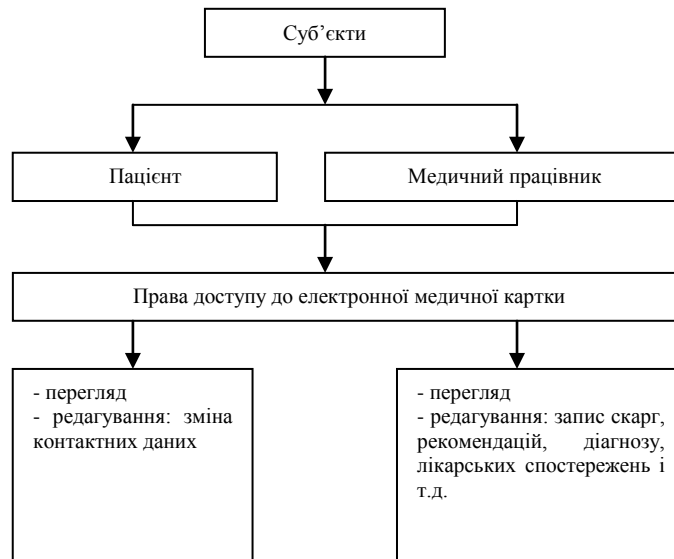


Рис. 2. Структура прав доступу суб'єктів до ПМДн

Множину прав доступу представимо у вигляді послідовності $R = (r_1, r_2, \dots, r_n) \cup (t, g)$. Згідно класичної інтерпретації моделі Take-Grant, $t(take)$ – право брати «права доступу», $g(grant)$ – право давати «права доступу» [6]. Стан системи описується графом. На рис. 3 показаний граф надання прав доступу до електронної медичної картки (ЕМК).

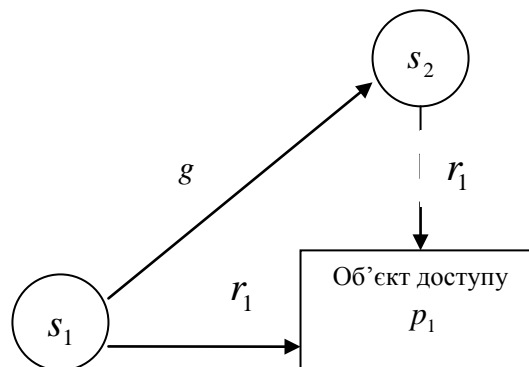


Рис. 3. Граф надання прав доступу до ЕМК

З рис. 3 видно, що об'єкт s_1 дає право доступу r_1 до об'єкту p_1 суб'єкту s_2 , де s_1 – лікар, s_2 – пацієнт, r_1 – право перегляду, p_1 – результати лікарського обстеження.

Використовуючи дану модель, можна передбачити стани, в яких буде перебувати МІС в залежності від розмежування прав доступу [7]. Тобто, модель дає можливість передбачити і проаналізувати можливі загрози інформаційної безпеки для системи. Джерелом загрози безпеки інформації може бути суб'єкт доступу, матеріальний об'єкт або фізичне явище, що є

причиною виникнення загрози безпеки інформації. Існує багато класифікацій джерел походження загроз інформаційної безпеки ПМДн.

Висновки. Проблема забезпечення захисту ПМДн ставить під загрозу інтереси і права власної недоторканості особистості. Тому системи, в яких обробляється конфіденційна інформація, повинні супроводжуватися комплексом засобів гарантування інформаційної безпеки. В роботі запропонований один з способів вирішення проблеми отримання несанкціонованого доступу до ПМДн, на прикладі моделі розмежування доступу Take-Grant. Згідно правил моделі, повноваження над об'єктом захисту можуть мати лише чітко визначені суб'єкти. Це дасть змогу забезпечити основні властивості інформації: конфіденційність, цілісність, доступність.

Список використаних джерел

1. Столбов А.П. Обработка персональных данных в здравоохранении: новые требования и проблемы / А.П. Столбов // Менеджер здравоохранения. – 2011. – №7. – С. 42–49.
2. Зыков В.Д. Обеспечение защиты информации при обработке медицинских биометрических данных / В.Д. Зыков, Р.В. Мещеряков, А.С. Романов, А.А. Шелупанов// Доклады ТУСУРа. Часть 2. – 2010. – № 2. – С. 249–252.
3. Фохт О.А. Защита персональных данных. Новое в законодательстве: тенденции, вопросы практического применения в медицинских информационных системах / О.А. Фохт, А.А. Цветков // Врач и информационные технологии. – 2013. – №5. – С. 44–51.
4. Астахова Л.В. Особенности защиты персональных данных в органах судебно-медицинской экспертизы / Л.В. Астахова, Я.А. Сапожников // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». – 2013. – № 3(13). – С. 122–127.
5. Кириенко А.Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения / А.Е. Кириенко/ /Молодой ученый. – 2012. – № 3. – С. 40–46.
6. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 452 с.
7. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Н.Т. Югов// Доклады ТУСУРа. – 2011. – № 2 (24). – С. 206– 210.

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ МЕДИЧНИХ ДАНИХ НА ОСНОВІ МОДЕЛІ РОЗМЕЖУВАННЯ ДОСТУПУ TAKE-GRANT РОЗЛОМІЙ І.А.*, ЗАХАРОВА М.В.**, ЛЮТАЯ М.В.***

*Черкаський національний університет імені Богдана Хмельницького

**Черкаський державний технологічний університет

***Київський національний університет технологій і дизайну

Мета. Розробка моделі розмежування доступу до персональних медичних даних (ПМДн) для забезпечення їх конфіденційності.

Методика. В статті розглядаються питання забезпечення захисту ПМДн при обробці в медичних інформаційних системах (МІС). Проводиться аналіз можливих загроз

інформаційної безпеки в МІС. Досліджено перелік вповноважень суб'єктів над ПМДн з метою побудови моделі розмежування доступу до конфіденційної інформації.

Результати. Розглянуті особливості організації автоматизованої обробки ПМДн. Перераховані головні проблеми, пов'язані з впровадженням МІС. Приведено перелік необхідних заходів для забезпечення захисту ПМДн. Запропонована модель розмежування доступу Take-Grant.

Наукова новизна. На основі деталізованої схеми класифікації ПМДн, суб'єктів та їх вповноважень, побудовано граф надання визначених прав доступу до конкретного об'єкту, що є основою дискреційної політики безпеки МІС.

Практична значимість. Захист МІС є необхідністю, оскільки дані системи можуть значно підвищити безпеку і якість медичної допомоги, збільшити оперативність подання медичної інформації, забезпечити комфортність у роботі медичного персоналу.

Ключові слова: медична інформаційна система, персональні дані, інформаційна безпека, конфіденційність, модель Take-Grant.

ENHANCEMENT OF EFFICIENCY OF PERSONAL MEDICAL DATA PROTECTION ON THE BASIS OF ACCESS CONTROL MODEL TAKE-GRANT

ROZLOMII I.A.*, ZAKHAROVA M.V.***, LYUTA M.V.***

*Cherkassy Bogdan Khmelnytskyi National University

**Cherkassy State Technological University

***Kiev National University of Technology and Design

Purpose. To develop the access control model to personal medical data to ensure their privacy.

Methodology. The article focuses on the issues of ensuring personal medical data protection in processing of medical information systems. Possible threats to information security in medical information systems are analyzed. Access control list to personal medical information systems to develop the access control model to confidential information is studied.

Findings. Features of automated processing of personal medical data are considered. Major problems related to the implementation of personal medical data are specified. Range of measures necessary to protect personal medical data is given. Access control model TAKE-Grant is brought forward.

Scientific novelty. On the basis of detailed classification scheme of personal medical data and access control list the graph granting certain rights to access to a particular object, basis of discretionary security policy of personal medical data, is constructed.

Practical value. Medical information systems protection is a necessity as far as these systems can significantly enhance medical assistance safety and quality, increase operational efficiency of medical data submission and maintain comfort conditions for medical staff.

Key words: medical information systems, personal data, information security, privacy, TAKE-Grant model.