Механізм виведення інтелектуальної системи діагностики захворювань є механізмом прямого виведення висновків на основі нечітких умов в базі правил нечітких продукцій (*fuzzy forward-chaining reasoning*). Це дає можливість оперувати вхідними даними, які погано формалізовані або задані нечітко, нечітко формалізувати критерії оцінки і порівняння (використати критерії «низька», «нормальна», «підвищена» і так далі), проводити якісні оцінки вхідних даних і отриманих результатів (використання функції приналежності), проводити моделювання ІСДЗ за допомогою fuzzy-методів.

Таким чином, особливостями розробки ІСДЗ є представлення експертних даних у вигляді продукційної моделі, яка є модульною, доступною для читання, універсальною і має ефективну організацію пам'яті. Недоліки моделі усуваються за допомогою використання нечітких продукцій і лінгвістичних змінних. Крім того, використання механізму нечіткого логічного виведення дозволяє уникнути протиріччя між чіткими методами логічного виведення і нечіткими знаннями у системі.

УДК 004.056

ЗАХИСТ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ СМАРТ-КАРТАМИ В КОМП'ЮТЕРНИХ СИСТЕМАХ РОЗПІЗНАВАННЯ ПАТОЛОГІЙ ОЧНОГО ДНА

Л. В. Загоруйко, В. А. Довгалюк

В охороні здоров'я активно впроваджуються автоматизовані системи, що дозволяють зберігати інформацію в електронному вигляді. Це сприяє підвищенню ефективності інформаційного обміну між медичними установами, можливості віддаленого доступу до медичних інформаційних систем, полегшення і прискорення запису пацієнтів на прийом за допомогою електронної реєстратури. Тому можна стверджувати, що медична інформація в електронному вигляді є основою багатьох процесів в сучасній охороні здоров'я.

Однак недолік сучасних комп'ютерних систем полягає в тому, що доступ до історії хвороби для введення, зміни або видалення будь-якої інформації надається без відома самого пацієнта. В результаті подібні системи не є безпечними, оскільки в них порушуються принципи конфіденційності та цілісності інформації. Системи, які оперують такими важливими даними, як інформація про стан здоров'я людини, повинні бути надійно захищені.

Основна увага має бути направлена на забезпечення безпечного доступу до інформації, захист даних, що передаються і застосування електронних підписів. Рішенням цих проблем є використання смарт-карт лікаря і пацієнта для їх однозначної ідентифікації в єдиній базі електронних медичних карт. Застосування смарт-карт в комп'ютерних системах дозволить забезпечити безпечний доступ до інформації і надійне зберігання конфіденційних даних пацієнта. Безпека інформаційних ресурсів забезпечується криптографічними методами.

У статті представлені можливості криптографічних методів при роботі зі смарт-картами для забезпечення конфіденційності і цілісності даних пацієнтів.

Смарт-карта є пластиковою карткою, за зовнішнім виглядом ідентичною карті поліса медичного страхування. У неї вбудований чіп, що містить незалежну пам'ять і кріптопроцессор (мікрокомп'ютер, вбудований в пластикову карту). У пам'яті чіпа зберігається унікальний сертифікат користувача і інша персоніфікована інформація (наприклад, відомості про пацієнта і стан його здоров'я). Кріптопроцессор забезпечує логіку роботи карти, в тому числі генерацію ключових пар і електронного підпису.

Щоб почати роботу з комп'ютерною системою, що містить електронні історії хвороби, користувач з'єднує смарт-карту зі зчитувачем і вводить PIN-код. При цьому послідовно виконуються три пов'язаних процеси:

1) ідентифікація (процедура розпізнавання користувача за його ідентифікатором);

2) аутентифікація (процедура доказу того, що користувач насправді є тим, за кого себе видає);

3) авторизація (процедура надання користувачу певних прав доступу до ресурсів системи).

Існують два типи карт – карта пацієнта і карта лікаря. На карті пацієнта є відкрита і закрита області пам'яті. У відкритій області зберігається базова інформація (ПІБ, дата народження, група крові, найменування страхової компанії і т.п.). Ці дані повинні бути доступні будь-якому медпрацівникові для надання невідкладної допомоги пацієнту. Однак ця інформація повинна бути захищена від несанкціонованого внесення змін.

У захищеній області пам'яті зберігаються дані, необхідні для аутентифікації пацієнта, а також сертифікат відкритого ключа лікаря, який підписав цю карту. Закрита область доступна тільки медичним фахівцям за пред'явленням ними своїх смарт-карт. Інша інформація про стан здоров'я (історія хвороби) пацієнта зберігається на сервері медичного закладу і доступна відповідним фахівцям.

Другим типом смарт-карт є карта лікаря (або карта фахівця). На ній записані ПІБ фахівця, назва установи охорони здоров'я, в якому він працює, спеціалізація, персональний номер, електронний підпис. Смарт-карта лікаря дає право доступу до закритої інформації, як на карті пацієнта, так і на серверах медичних установ. Проте фахівець може отримати доступ лиш до тієї інформації, на яку він має право відповідно до своєї спеціалізації.

На смарт-карті лікаря повинні зберігатися ідентифікатор і ключова пара (ключ електронного підпису і ключ перевірки електронною підпису). Отже, дана карта повинна мати захищені області пам'яті для безпечного зберігання ключової інформації. Крім аутентифікації, смарт-карта лікаря використовується також для підписання електронних персональних медичних записів.

Література

1. Lantsberg A. V., Klaus G. Troitzch, Buldakova T. I. Development of the electronic service system of a municipal clinic (based on the analysis of foreign web resources). *Automatic Documentation and Mathematical Linguistics.* 2011. N. 2. V. 45. P. 74–80.

2. Llinás G., Rodríguez-Iñesta D. et al. Comparison of Websites from Spanish, American and British Hospitals. *Methods of Information in Medicine.* 2008. Vol. 47; Issue 2. P. 124–130.

3. Монич В. А., Кушников О. И., Алакаев Р. Р., Косоногов А. Я., Коротин Д. П., Медоваров Е. В. Электронная история болезни – важнейшее звено медицинских информационных систем. *Современные технологии в медицине.* 2010. № 3. С.73–74.

4. Kuhlisch R., Kraufmann B., Restel H. Electronic Case Records in a Box: Integrating Patient Data in Healthcare Networks. *Computer.* 2012. Vol. 45, No. 11. Pp. 34–40.

5. Aleman J. L. F., Senor Carrion I., Toval A. Personal Health Records: New Means to Safely Handle Health Data? *Computer.* 2012. Vol. 45, No. 11. Pp. 27–33.

УДК 621.3.049.76

МЕТОДИ РОЗПІЗНАВАННЯ ДИСКРЕТНОГО СИГНАЛУ В АДАПТИВНОМУ ШУМІ ДЛЯ ДВОХ КАНАЛІВ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Д. К. Ільчук

Великі об'єми інформації що передається вимагають від апаратної складової швидкості та точності в робот. З часом кількість інформації тільки збільшується. Зі збільшення об'ємів інформації стає критичним кількість помилок при передачі даних. В