Захист інформації

УДК 004.78.056

Л.О. Дубчак

Тернопільський національний економічний університет, Тернопіль

НЕЧІТКА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕМЕДИЦИНІ

В статті запропоновано систему захисту інформації в телемедицині на основі нечіткої логіки, що дозволяє працювати в режимі реального часу. Виходом пропонованої нечіткої системи є криптоалгоритм шифрування даних залежно від вхідних поточних значень рівня доступу клієнта та ризику здійснення атаки під час передачі інформації. Така система захисту інформації дозволяє швидко переналаштувати систему телемедицини залежно від поточних даних, що підвищує рівень стійкості криптошифру. В статті також проведено моделювання та дослідження даної нечіткої системи захисту засобами MatLab Fuzzy Tool та Simulink.

Ключові слова: *телемедицина, нечітка логіка, нечітка система, MatLab Fuzzy Tool, Simulink.*

Вступ

Телемедицина – це галузь медицини, яка використовує телекомунікаційні та електронні інформаційні (комп'ютерні) технології для надання медичної допомоги і послуг в сфері охорони здоров'я в точці необхідності (в тих випадках, коли географічна відстань є критичним фактором) [1]. Глобальна мережа Інтернет в даному випадку є засобом зв'язку між клієнтом та комп'ютерною системою медичного закладу. Звідси випливають усі проблеми захисту інформації, що використовується в телемедицині, з точки зору інформаційної системи та мережі.

Телемедицину можна поділити на локальну (в межах одного медичного закладу) та глобальну (між різними медзакладами). Глобальна медична консультативно-діагностична система має структуру «клієнт-сервер», де в ролі клієнта виступають підсистеми консультативно-діагностичних пунктів чи центрів, а сервер виконує роль накопичувача та координаційно-технічного центру [2].

Як правило, будь-яка інформаційна система включає [2]: прикладне програмне забезпечення (ППЗ), яке відповідає за зв'язок системи з клієнтом; системи управління базами даних (СУБД); операційну систему для обслуговування ППЗ та СУБД; мережу, яка забезпечує взаємодію всіх вузлів інформаційної системи.

Найнебезпечнішими для таких інформаційних систем є несанкціонований доступ до паролів чи конфіденційної інформації, порушення прав доступу, атаки типу «відмова в обслуговуванні», «пряма» атака, віруси, сучасні атаки по побічних каналах витоку інформації.

Несанкціонований доступ полягає у підборі чи викраденні пароля або підміні IP-адреси законного користувача системи. До цього виду атак вразливі усі компоненти інформаційної системи.

Існує чотири стандартні підходи, за допомогою яких можна обмежити доступ до інформації [3]:

- контроль доступу;
- розширення парольного захисту;
- шифрування;
- використання брандмауерів.

Атака типу «відмова в обслуговуванні» полягає у створенні неправильного пакету даних чи передачі великої кількості пакетів даних по мережі з метою блокування роботи контролера домена, що зупиняє роботу комп'ютерної системи. Для захисту компонентів інформаційної системи застосовуються спеціальні програми виявлення такого типу атак чи міжмережеві екрани [4]. Комп'ютерний вірус – комп'ютерна програма, яка має здатність до прихованого саморозмноження. Одночасно зі створенням власних копій віруси можуть завдавати шкоди: знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність операційної системи комп'ютера. Розрізняють файлові, завантажувальні та макро-віруси. Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу. Для захисту від вірусів на даний час існує багато антивірусних програм, що захищає інформаційну систему від пошкодження.

Побічними каналами витоку інформації під час передачі пакетів даних по мережі є електро-магнітне випромінювання, час виконання алгоритмів шифрування та реакція системи на спеціально внесені помилки. Для протидії таким атакам використовуються, як правило, архітектурна та операційна надлишковість, тобто додаткові апаратні та програмні засоби [3, 5].

Загалом можна визначити наступні методи захисту інформаційної системи від втрати чи викриття конфіденційної інформації [2].

Установка перешкоди – метод фізичного перешкоджання шляху зловмиснику до інформації, що

захищається, у тому числі спроб з використанням технічних засобів знімання інформації і дії на неї.

Маскування – метод захисту інформації з використанням інженерних, технічних засобів, а також шляхом криптографічного закриття інформації.

Управління доступом – метод захисту інформації за рахунок регулювання використовування всіх інформаційних ресурсів, у тому числі автоматизованої інформаційної системи підприємства. Управління доступом включає наступні функції захисту:

1) ідентифікацію користувачів, персоналу і ресурсів інформаційної системи (привласнення кожному об'єкту персонального ідентифікатора);

2) аутентифікацію (встановлення автентичності) об'єкту або суб'єкта після пред'явленому їм ідентифікатору;

3) перевірку повноважень (перевірка відповідності дня тижня, часу доби, запрошуваних ресурсів і процедур встановленому регламенту);

4) дозвіл і створення умов роботи в межах встановленого регламенту;

5) реєстрацію (протоколювання) звернень до ресурсів, що захищаються;

6) реагування (сигналізація, відключення, затримка робіт, відмова в запиті) при спробах несанкціонованих дій.

Проте, застосування всіх відомих методів захисту даних інформаційної системи не гарантує збереження цілісності даних, тому розробка нових підходів залишається актуальною задачею.

Одним із шляхів розв'язку цього завдання є застосування нечіткої логіки до побудови системи захисту інформації та її апаратної реалізації.

Нечітка система вибору алгоритму захисту інформації

Для здійснення захисту інформації в телемедицині необхідно визначити рівень доступу поточного клієнта до інформаційної системи. Крім того, варто враховувати ризик виникнення атаки через поточний канал передачі інформації, який може визначатися співвідношенням кількості звернень даного клієнта до кількості збоїв під час передачі даних через його канал.

На даний час відомі симетричні та асиметричні криптоалгоритми. Найпоширеніші серед них – симетричний DES, асиметричний RSA та на основі еліптичних кривих [5]. В загальному схема вибору алгоритму захисту інформації зображена на рис. 1. В даному випадку в якості критеріїв вибору виступають рівень доступу клієнта до інформації (access) та ризик виникнення атаки при передачі інформації поточному клієнту (risk), а підсистемою вибору є система обробки нечіткої інформації на основі механізму Мамдані. Виходом такої системи є один з криптоалгоритмів, відповідний вхідним критеріям вибору і застосовуючи який комп'ютерна система забезпечить свою оптимальну роботу.

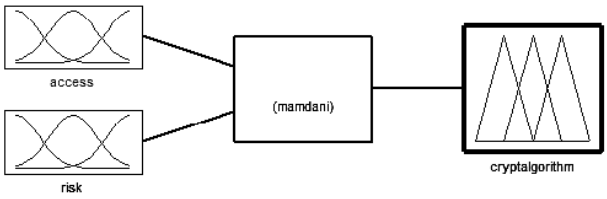


Рис. 1. Загальна схема оптимального вибору методу модулярного експоненціювання для розподілу доступу клієнтів комп'ютерної системи

В інженерних задачах застосовується, як правило, механізм нечіткого висновку Мамдані [6, 7]. В ньому використовується мінімаксна композиція нечітких множин. Даний механізм включає наступну послідовність дій [8]:

1) процедура фазифікації: визначаються степені істинності, тобто значення функцій належності для лівих частин кожного і-го правила (передумов);

2) нечіткий висновок. Спочатку визначаються мінімальний рівень "відсічення" для лівої частини кожного з правил, а потім знаходяться "усічені" функції належності висновку;

3) композиція або об'єднання отриманих "усічених" функцій, для чого використовується максимальна композиція нечітких множин;

4) дефазифікація або приведення до чіткості. Існує декілька методів дефазифікації. Наприклад, метод середнього центру або центроїдний метод. Геометричний зміст такого значення – центр ваги для кривої функції належності отриманого виходу.

Застосовуючи засіб Fuzzy Logic Toolbox середовища MATLAB 7.7.0 (R2008b), можна побудувати запропоновану нечітку систему вибору криптоалгоритму.

Значення функцій належності вхідних змінних *access* та *risk* задається трапецевидною функцією, що визначається четвіркою чисел (*a*,*b*,*c*,*d*), які позначають абсциси вершин трапеції.

Функція належності виходу *cryptoalgorithm* задається трикутною формою, яка залежить від трьох змінних (*a*,*b*,*c*) (абсциси вершин трикутника) [9] при чому в даному випадку має місце випадок симетричної трикутної функції належності, тобто (*b*-*a*)=(*c*-*b*).

Функції належності для змінних *access* та *risk*, подані на рис. 2, 3, відповідно.

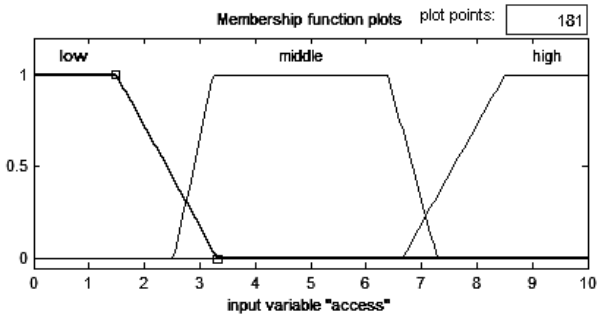


Рис. 2. Функції належності змінної *access*

Вони поділені на три інтервали кожна для точного опису змінних, зокрема, для опису рівня досту-

пу до інформації застосовується змінна *low*, що позначає низький рівень доступу (може надаватися, наприклад, новим клієнтам), *middle* - середній рівень та *high* - високий рівень доступу (може надаватися адміністратору інформаційної системи).

Для задання рівня ризику виникнення атаки пропонуються змінні *low*, *middle* та *high*, що відповідають низькому, середньому та високому рівню.

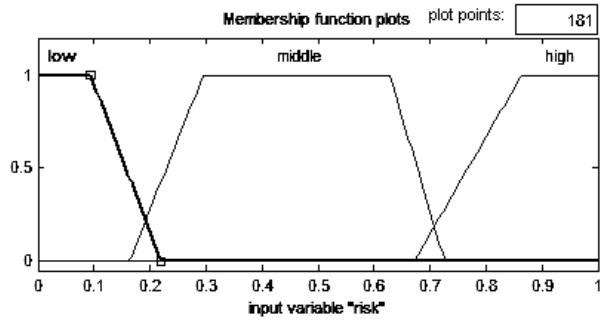


Рис. 3. Функції належності змінної *risk*

Функції належності для вихідної змінної *cryptoalgorithm* зображено на рис. 4. Вони позначаються однаковими інтервалами на осі ординат для точного визначення центру ваги, що позначає нечіткий висновок системи. *None* позначає відсутність необхідності застосування алгоритму захисту інформації (наприклад, у випадку, коли до інформаційної системи звертається адміністратор), *DES*, *RSA* та *EC* – криптоалгоритм DES, RSA та на основі еліптичних кривих, відповідно. Кожен з цих алгоритмів має свої переваги і недоліки, свій рівень стійкості та продуктивності, які описані в [5].

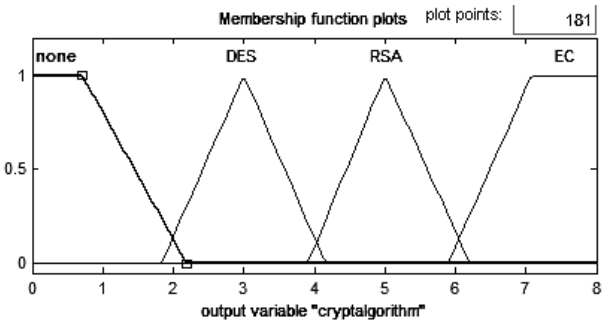


Рис. 4. Функції належності змінної *method*

База знань для побудови даної нечіткої моделі складається з правил типу «якщо - то» [9], усі вхідні змінні мають по три нечітких стани і ще один стан, коли значення вхідної змінної не задане системою. Випадок, коли значення усіх вхідних змінних не задані, на практиці неможливий, тому кількість правил нечіткого висновку досліджуваної системи $N = 4 \cdot 4 - 1 = 15$.

База правил розробленої нечіткої системи має вигляд, зображений на рис. 5.

Поверхня значень розробленої нечіткої системи вибору алгоритму захисту інформації в телемедицині зображена на рис. 6.

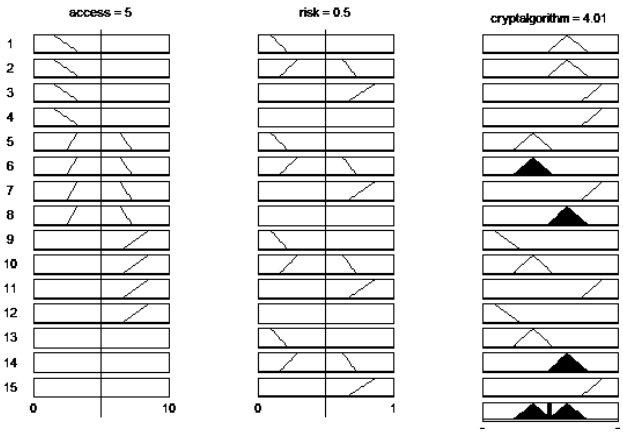


Рис. 5. База правил нечіткої системи вибору криптоалгоритму

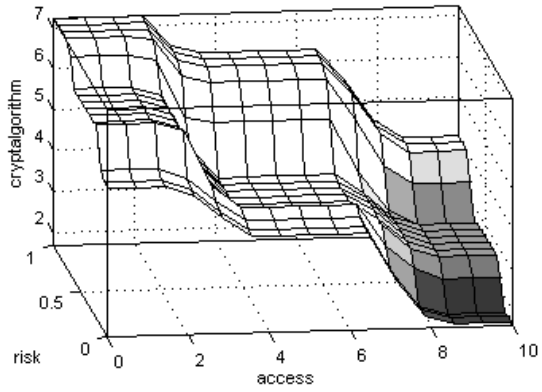


Рис. 6. Поверхня значень нечіткої системи вибору криптоалгоритму

Дослідження бази правил (рис. 5) та поверхні значень (рис. 6) запропонованої нечіткої системи показали правильність її роботи. MatLab код даної нечіткої системи має такий вигляд:

```
[System]
Name='telemedycyna'
Type='mamdani'
Version=2.0
NumInputs=2
NumOutputs=1
NumRules=15
AndMethod='min'
OrMethod='max'
ImpMethod='min'
AggMethod='max'
DefuzzMethod='centroid'
 [Input1]
Name='access'
Range=[0 10]
NumMFs=3
MF1='low':'trapmf',[-3.6 -0.4 1.49 3.32010582010582]
MF2='middle':'trapmf',[2.53 3.24 6.38888888888889 7.29]
MF3='high':'trapmf',[6.65 8.505291005291 10.4 13.6]
 [Input2]
Name='risk'
Range=[0 1]
NumMFs=3
MF1='low':'trapmf',[-0.36 -0.04 0.0939153439153439 0.22]
MF2='middle':'trapmf',[0.163 0.295 0.628306878306878 0.726]
MF3='high':'trapmf',[0.672 0.863756613756614 1.07 1.33]
 [Output1]
Name='cryptalgorithm'
Range=[0 8]
NumMFs=4
MF1='none':'trapmf',[-2.88 -0.32 0.709 2.19047619047619]
```

```
MF2='DES':'trimf',[1.83 3 4.15873015873016]
MF3='RSA':'trimf',[3.9 5 6.21]
MF4='EC':'trapmf',[5.89417989417989 7.08 8.01 8.62]
 [Rules]
1 1, 3 (1) : 1
1 2, 3 (1) : 1
1 3, 4 (1) : 1
1 0, 4 (1) : 1
2 1, 2 (1) : 1
2 2, 2 (1) : 1
2 3, 4 (1) : 1
2 0, 3 (1) : 1
3 1, 1 (1) : 1
3 2, 2 (1) : 1
3 3, 4 (1) : 1
3 0, 1 (1) : 1
0 1, 2 (1) : 1
0 2, 3 (1) : 1
0 3, 4 (1) : 1
```

Програмна реалізація дозволяє легке та економне впровадження нечіткої системи в сервер, проте, не забезпечує захисту самої розробленої системи від несанкціонованого доступу. Тому варто реалізувати дану нечітку систему апаратно. Це можна зробити засобом Simulink середовища MatLab.

Апаратна реалізація нечіткої системи захисту інформації в телемедицині

Модель нечіткої системи розподілу доступу в телемадицині, що працює за класичним механізмом Мамдані, подана на рис. 7.

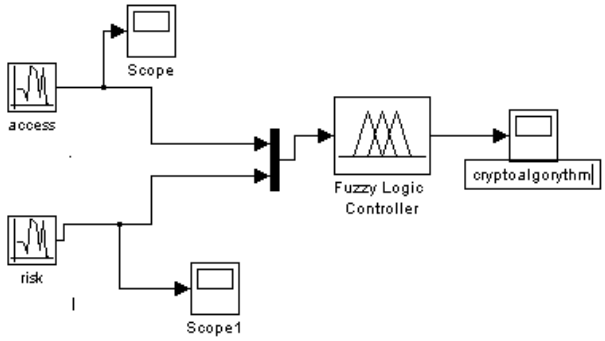


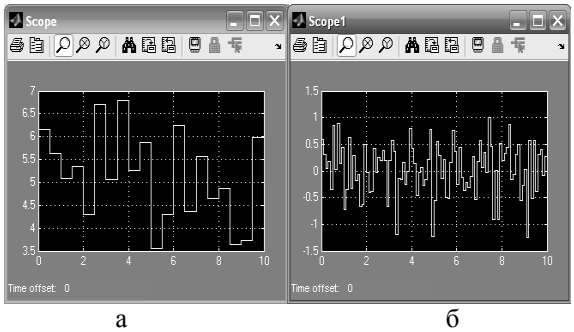
Рис. 7. Модель розробленого засобу

Входами нечіткого контролера (Fuzzy Logic Controller), який працює за механізмом Мамдані, є значення рівня доступу клієнта до інформації (access) та ризик виникнення атаки при передачі інформації поточному клієнту (risk), а виходом – значення центра ваги, який інтерпретує криптоалгоритм (cryptoalgorythm).

Загальна схема нечіткого контролера містить три блоки опису функцій належності вхідних змінних (блоки Input MF), блок опису функцій належності виходу (Output MF), виходи яких поступають на вхід 15 правил (блоки Rule 1 … 15).

Вхідні змінні задаються випадковим чином з рівномірним розподілом, що зображено на рис. 8.

Схему обчислення функцій належності вхідних та вихідної змінних, побудована системою Simulink, подано на рис. 9.



а б

Рис. 8. Рівномірно розподілене задання випадкових значень вхідних змінних: а – рівня доступу; б – ризику атаки

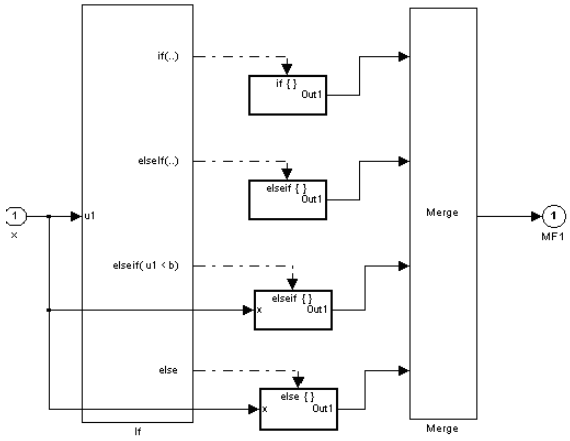


Рис. 9. Схема визначення функцій належності вхідних і вихідної змінних нечіткого контролера

Simulink опрацьовує правила з бази знань, враховуючи рейтинг, що відображається константою Weight на рис. 10.

Входами правила є значення вхідних змінних доступу та ризику атаки (вхід 1) та відповідне їм значення криптоалгоритму (вхід 2). Опрацювання цих даних відбувається за мінімальним законом (блок min). Виходами даної схеми є значення функції належності виходу *cryptoalgorythm* (вихід 1) та послідовність, що відображає інтервал задання цього виходу (вихід 2). Для здійснення висновку за механізмом Мамдані нечіткий контролер здійснює дефазифікацію, тобто знаходження центру ваги кінцевої фігури, що утворюється в результаті сумування виходів 15 правил. Схема дефазифікації, подана на рис. 11, реалізує формулу [7]:

$$r_{цв} = \sum_{j=1}^{m} r_j \mu(r_j) \Big/ \sum_{j=1}^{m} \mu(r_j),$$

де m - кількість прямокутників, на які поділено кінцеву фігуру, r_j - значення абсциси, $\mu(r_j)$ - значення ординати j-ї фігури.

У табл. 1 подано тестові значення вхідних та вихідних значень нечіткої системи вибору оптимального криптоалгоритму за механізмом Мамдані.

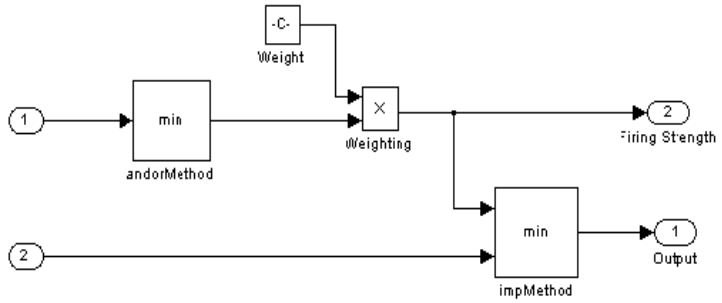


Рис. 10. Схема опрацювання вхідних нечітких значень за правилом типу «якщо - то»

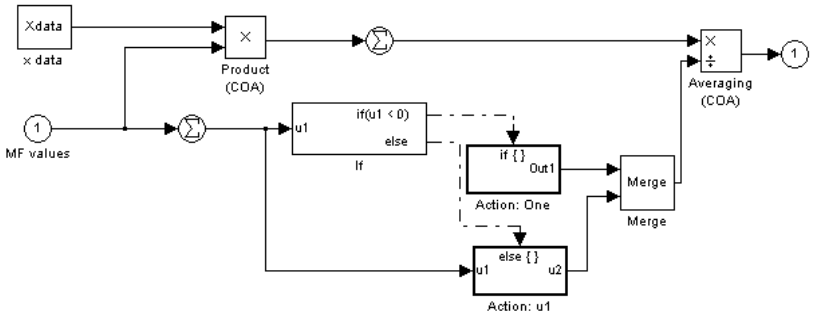


Рис. 11. Схема дефазифікації нечіткого висновку

Таблиця 1

Тестові значення змінних побудованої нечіткої системи

№п\п	Access	Risk	Cryptoalgorythm
1	5	0.5	4.01
2	6.93	0.768	5.36
3	0.6	0.5	6.29
4	8.67	0.08	1.74
5	3.81	0.941	6.31

Аналіз результатів, поданих в табл. 1, підтверджує правильність роботи розробленого засобу.

Висновки

В результаті проведених досліджень розроблено нечітку систему захисту інформації в телемедицині, що може бути реалізована як програмно, так і апаратно. Дана система може легко модифікуватися відповідно до кількості та значень вхідних змінних.

Список літератури

1. Владзимирский А.В. Телемедицина [монография] / А.В. Владзимирский. – Донецк: ООО «Цифровая типография», 2011. – 437 с.

2. Лукацкий А. Атаки на информационные системы. Типы и объекты воздействия / А.Лукацкий // Электроника: Наука, Технология, Бизнес. – 2000. – №1. – С. 16-21.

3. Васильцов І.В. Атаки спеціального виду на криптопристрої та методи боротьби з ними / І.В. Васильцов / За ред. В.П. Широчина. – Кременець: Видавничий центр КОГПІ, 2009. – 264 с.

4. Дубчак Л.О. Атаки на сучасні інформаційні системи та методи захисту проти них / Л.О. Дубчак // Materiály IX mezinárodní vědecko-praktická konference «Vědecký pokrok na přelomu tysyachalety – 2013». – Praha Publishing House «Education and Science» s.r.o, 2013. - С. 3-5.

5. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; под ред. В.Ф.Шаньгина. – М.: Радио и связь, 1999. – 328 с.

6. Ross T.J. Fuzzy Logic with Engineering Applications / T.J. Ross. – McGraw-Hill Inc.(USA), 1995. – 600 p.

7. Штовба С.Д. Введение в теорию нечетких множеств и нечеткую логику / С.Д. Штовба [Електронний ресурс]. – Режим доступу до ресурсу: http://matlab.exponenta.ru/fuzzylogic/book1/.

8. Бережная М.А. Методы проектирования нечетких устройств принятия решений на основе программируемых логических интегральных микросхемах / М.А. Бережная // Технология приборостроения. – 2009. – № 2. – С. 16-23.

Надійшла до редколегії 6.05.2015

Рецензент: д-р техн. наук, проф. О.М. Березький, Тернопільський національний економічний університет, Тернопіль.

НЕЧЕТКАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕМЕДИЦИНЕ

Л.О. Дубчак

В данной статье предложена система защиты информации в телемедицине на основе нечеткой логики, позволяет работать в режиме реального времени. Выходом предлагаемой нечеткой системы является криптоалгоритм шифрования данных в зависимости от входных текущих значений уровня доступа клиента и риска осуществления атаки при передаче информации. Такая система защиты информации позволяет быстро перенастроить систему телемедицины в зависимости от текущих данных, повышает уровень устойчивости криптошифру. В статье также проведено моделирование и исследование данной нечеткой системы защиты средствами MatLab Fuzzy Tool и Simulink.

Ключевые слова: *телемедицина, нечёткая логика, нечёткая система, MatLab Fuzzy Tool, Simulink.*

FUZZY INFORMATION PROTECTION SYSTEM IN TELEMEDICINE

L.O. Dubchak

This paper proposes the information protection system in telemedicine based on fuzzy logic, which can operate in real time. The solution proposed fuzzy system is a data encryption algorithm based on the current values of the input client access and risk of making attack during transferring information. This system of information protection due to quickly reconfigure telemedicine system, based on current data, which increases resistance of crypto cipher. The article also conducted modeling and study of the fuzzy system protection with help of MatLab Fuzzy Tool and Simulink.

Keywords: *telemedicine, fuzzy logic, fuzzy system, MatLab Fuzzy Tool, Simulink.*