УДК 681.004
В.О. Савчук, Я.В. Литвиненко канд. тех. наук доц.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ БІОМЕДИЧНОЇ ІНФОРМАЦІЇ ЕЛЕКТРОКАРДІОСИГНАЛУ ДЛЯ ЗАДАЧ ТЕЛЕМЕДИЦИНИ

V.O. Savchuk, I.V. Lytvynenko Ph.D., Assoc

ANALYSIS OF ENCRYPTION METHODS BIOMEDICAL INFORMATION FOR ISSUES OF TELEMEDICINE

Питання захисту конфіденційної інформації є дуже важливим, зокрема в телемедицині. 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. Інформація та дані, які циркулюють в медичних мережах, вимагають нових підходів для їх захисту, обробки та аналізу. До таких даних відносять медичні зображення, записи, діагностичні висновки, персональні дані та іншу конфіденційну інформацію. Такі дані треба не тільки передавати, але і зберігати, обробляти і аналізувати. Аналіз літературних джерел показує, що телемедицина в Україні розвинена на даний час досить слабо в порівнянні зі світовими аналогами, тому проблема безпеки у медичній інформатиці стає однією з найактуальніших при побудові телемедичних мереж.

В даній роботі буде розглянуто дослідження методів криптографічного захисту інформації з метою обґрунтування тих методів, які можуть бути використані для захисту інформації в задачах телемедицини.

Одним із підходів, за допомогою якого можна обмежити доступ до інформації є шифрування. На даний час відомі симетричні та асиметричні криптоалгоритми. Практичний досвід показує, що застосування конкретно визначених криптоалгоритмів не дозволяє забезпечити інтерактивний режим роботи системи, тому в сучасних криптоситемах використовуються комбінації симетричних та асиметричних алгоритмів. До таких систем належить SSL, PGP та GPG. Асиметричні алгоритми використовуються для розповсюдження ключів швидших симетричних алгоритмів. До деяких відомих, поширених алгоритмів з гарною репутацією належать: Twofish, Serpent, AES, Blowfish, CAST5, RC4 та IDEA.

Серед проведеного огляду методів криптографічного захисту інформації в програмних додатках та комп'ютерних системах слід виділити криптосистеми RSA, DSA, що являють собою схему повністю гомоморфного шифрування і дозволяють виконувати обробку зашифрованого тексту. Проведено групування алгоритмів шифрування даних на дві групи з подальшим їх аналізом та описом переваг та недоліків з метою використання для задач телемедицини.

Література

1. Дубчак Л.О. Інформаційні технології в медицині та біології / Л.О. Дубчак // Системи обробки інформації. – №4. – С.223.
2. Франчук В. М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних / В. М. Франчук. – Київ, 2012.