УДК 681.004
Домбровська О. – ст. гр.СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ МЕТОДІВ ШИФРУВАННЯ БІОМЕДИЧНОЇ ІНФОРМАЦІЇ ДЛЯ ЗАДАЧ ТЕЛЕМЕДИЦИНИ

Науковий керівник: к.т.н. доц. Литвиненко Я. В.

Dombrovska O. M.
Ternopil Ivan Pul'uj National Technical University

RESEARCH OF ENCRYPTION METHODS BIOMEDICAL INFORMATION FOR ISSUES OF TELEMEDICINE

Supervisor: PhD, docent, Lytvynenko Y. V.

Ключові слова: шифрування, біомедичної інформація.
Keywords: encryption, biomedical information.

Темою дипломної роботи є дослідження методів шифрування біомедичної інформації для задач телемедицини. Телемедицина дає можливість надавати висококваліфіковану медичну допомогу фахівців провідних медичних центрів у віддалених районах і істотно заощувати при цьому витрати пацієнтів. Ця наука заснована на використанні комп'ютерних і телекомунікаційних технологій для обміну медичною інформацією між фахівцями з метою підвищення якості діагностики та лікування пацієнтів. Шифрування одне з них і має важливе значення для використання інформації в межах поліклініки та соціальних відносин між лікарем та пацієнтом. Метод шифрування — це формальний алгоритм, що описує порядок перетворення вихідного повідомлення в результуюче. Методи шифрування: симетричний та асиметричний. Через вади в швидкодії асиметричного методу цей метод доводиться використовувати разом з симетричним (асиметричні методи на 3 - 4 порядки повільніші).Проблемою обміну біомедичнї інформації є її незахищеність, тому було вирішено дослідити можливість шифрування. Захист забезпечить приватність відомостей про пацієнтів медичних закладів, їх аналізів та результатів обстежень, задовільнить потреби пацієнтів.

Метою дослідження є розробка економічно-обґрунтованих методів інформаційної системи шифрування для передачі біомедичної інфомації з метою задоволення потреб телемедицини, пов'язаних з мінімізацією ризику та підвищенням якості передачі. Реалізація даної мети зумовила необхідність постановки та вирішення таких завдань:

- розглянути сутність та характеристику можливих методів шифрування;
- визначити основні чинники та обгрувати вибір використання шифрів;
- розглянути основні етапи обміну інформації в межах задач телемедицини та основні завдання, що постають при отриманні даних, їх використанні та зберіганні;
- дослідити основні методичні підходи до аналізу основних задач телемедицини;
- проаналізувати інструменти мінімізації втрати біомедичної інформації;
- обґрунтувати необхідність шифрування даних.