МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

**БИЦЬ ТАРАС ПЕТРОВИЧ**

УДК 004.056.55

# СИСТЕМА ШИФРУВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ ТА ЇХ МЕДИЧНИХ КАРТОК

8.0501302 «Інженерія програмного забезпечення»

**Автореферат**
дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль 2017

Роботу виконано на кафедрі програмної інженерії Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

**Керівник роботи:** кандидат технічних наук, доцент,
**Михалик Дмитро Михайлович,**
Тернопільський національний технічний університет імені Івана Пулюя,

**Рецензент:** кандидат технічних наук, доцент, завідувач кафедри кібербезпеки
**Козак Руслан Орестович,**
Тернопільський національний технічний університет імені Івана Пулюя,

Захист відбудеться 22 лютого 2017 р. о $9^{.00}$ годині на засіданні екзаменаційної комісії №1 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, аудиторія 101.

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми роботи**. Використання криптографічного захисту інформації під час побудови політики безпеки медичної системи значно посилює безпеку роботи системи, але за умови, що ця система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів. Розроблювані алгоритми шифрування значно полегшують роботу із захисту даних та мінімізують ризик несанкціонованого читання. Дана розробка є актуальною здебільшого для приватних медичних закладів але й стане у нагоді для будь-якого медичного закладу, що відповідально ставиться до конфіденційності даних своїх пацієнтів.

**Мета роботи:** Розробити систему для медичних закладів з метою покращення шифрування/дешифрування даних про пацієнта (аналізи, направлення, тощо), спрощення роботи лікарів (всі аналізи в одному місці) з використанням «хмарних» технологій.

**Об'єкт, методи та джерела дослідження.** Об'єктом дослідження є процес шифрування даних, пов'язаних із пацієнтами. Предмет дослідження: методи обробки даних медичного закладу з метою побудови комп'ютерної системи, що підвищить ефективність роботи закладу. У даній дослідницькій роботі застосовуються методи шифрування AES. Засобами для цього є вхідні дані про пацієнтів та їх медичні картки, та комп'ютерні системи для виконання шифрування.

**Наукова новизна отриманих результатів:**

- досліджено способи шифрування персональних даних;
- проаналізовано існуючі системи криптоаналізу з метою вибору найоптимальнішої моделі для шифрування;
- розроблено методи та алгоритми обробки шифрування даних з метою захисту даних;
- розроблено технологію шифрування даних з метою виконання автоматизованого шифрування даних про пацієнтів;
- реалізовано методи та алгоритми у вигляді модуля програмної системи для інтеграції їх в медичну систему шифрування даних, що дозволить захищати дані про пацієнтів від несанкціонованого читання.

**Практичне значення отриманих результатів.**

Проблема складності шифрування даних існує внаслідок недосконалості методів криптоаналізу. У період розгляду проблематики не було виявлено прогресивних засобів для виконання шифрування даних про пацієнтів. Виявлено ряд проблем:

- застарілі методи шифрування даних;
- низька швидкість шифрування;
- невідповідність розшифрованих даних первинним даним;
- «вузький» погляд на процес шифрування.

За результатами виконаної роботи було розроблено систему шифрування персональних даних пацієнтів та їх медичних карток з використанням алгоритму шифрування AES. Реалізовано реальну прикладну систему шифрування даних, яка проходила тестування та чудово себе зарекомендувала в медичних закладах.

**Апробація.** Окремі результати роботи доповідались на Міжнародній науково-практичній конференції «Сучасні наукові інновації», Київ, Міжнародний центр наукових досліджень, 15-16 лютого 2017 р.

**Структура роботи.** Робота складається з розрахунково-пояснювальної записки та графічної частини. Розрахунково-пояснювальна записка складається з вступу, 5-ти частин, висновків, переліку використаних посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 100 аркушів формату А4, 2 додатки, графічна частина – 10 слайдів графічної частини.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

**У вступі** проведено огляд сучасних досягнень науки і техніки в розробці методик шифрування даних, описано загальну специфіку тематики та завдання розробки.

**В розділі «Аналітична частина»** Досліджено методики шифрування даних. Досліджено альтернтивні методи шифрування та способи дослідження, їх ефективність. Проаналізовано специфіку галузі, існуючі розробки та прикладне програмне забезпечення. Описано тематику досліджень, алгоритми та математичні моделі шифрування даних з метою захисту персональних даних пацієнтів.

**В розділі «Спеціальна частина»** Описано предметну область та специфіку шифрування персональних даних. Спроектовано архітектуру програмної системи, реалізовано і протестовано бібліотеку з набором методів та алгоритмів шифрування даних. Розроблено програмну модель системи та здійснено її тестування.

**В розділі «Обґрунтування економічної ефективності»** розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень з огляду двох підходів розробки – об'єктно-орієнтованого та процедурного. Також проаналізовано економічні складові, що виникають в ході розробки, та чинники, які впливають на виконання проекту.

**В розділі «Охорона праці та безпека в надзвичайних ситуаціях»** розглянуто питання специфіки дотримання норм та правил Охорони праці в галузі розробки ПЗ з використанням персональних комп'ютерів. Також проаналізовано вплив здорового способу життя на професійну діяльність людей. Досліджено негативний вплив іонізуючого випромінювання та дієві засоби захисту працівників від нього.

**В розділі «Екологія»** досліджено та проаналізовано існуючі методології моделювання екологічних проблем, вплив моделювання на природоохоронну діяльність. Визначено роль науково-технічного прогресу в системі забезпечення якісного стану довкілля.

**У загальних висновках щодо дипломної роботи** описано результати дослідницької діяльності в ході реалізації проекту шифрування персональних даних пацієнтів та їх медичних карток. Підсумовано важливість отриманих наукових напрацювань та розроблюваних методик тестування. Також, у висновках зазначено основні якісні та кількісні характеристики, які можна отримати, користуючись розробленою технологією. Вказано використані програмні рішення для реалізації даної технології з допомогою комп'ютерного обладнання.

В додатках до пояснювальної записки наведено зразки програмного коду реалізації бібліотеки та системи шифрування. Надано зразки тестування пацієнтів з використанням розроблюваної технології. Додано диск з програмним забезпеченням, інструкцією користувача та пояснювальною запискою до розробки.

В графічній частині наведено презентаційний матеріал з поясненням розроблюваного методу шифрування даних пацієнтів та їх медичних карток з використанням комп'ютерного обладнання. Представлено результати досліджень та отрмані зразки тестування методики.

## ВИСНОВКИ

В результаті виконання дипломної роботи було розроблено алгоритми для шифрування персональних даних пацієнтів та їх медичних карток. Було використано криптографічні методи захисту інформації, а саме методи шифрування за допомогою алгоритму AES. З допомогою цього алгоритму було реалізовано можливість блокувати несанкціонований доступ до персональних даних пацієнтів.

В якості системи автоматизації процесу шифрування було спроектовано та реалізовано програмну бібліотеку, що містить набір методів та алгоритмів для дослідження характеристик шифрування. Для більш ґрунтовного підходу до дослідження та реалізації необхідних методів було розглянуто основні параметри системи, досліджено експериментальні дані та суміжні розробки, проаналізовано існуючі ефективні методи ідентифікації, переваги та недоліки кожної з них.

Даний дослідницький проект та його реалізація виконувався з метою забезпечення ефективного, точного та однозначного шифрування даних про пацієнтів. Бібліотека алгоритмів та прикладне програмне забезпечення можуть бути використані для побудови комп'ютерних моделей і візуалізації результатів, пришвидшення та забезпечення зручності виконання досліджень, порівняння результатів.

Предметна область є цікавою та надзвичайно корисною для сучасних інноваційних методик шифрування даних про пацієнтів в клініках. Програмне рішення повинно значно скоротити час та витрати на виконання захисту даних пацієнтів у галузі медицини. Розроблений метод сприяє оптимізації шифрування, а також додає свою частинку в загальний розвиток технологій в медичній галузі.

## СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Биць Т. П. Тези доповіді на Міжнародній науково-практичній конференції «Сучасні наукові інновації». – Київ, МЦНД, 2017.

# АНОТАЦІЯ

Дипломна робота на тему «Система шифрування персональних даних пацієнтів та їх медичних карток» Биця Тараса Петровича. – Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра програмної інженерії, група СПм–61 // Тернопіль, 2017.

С. – 100, рис. – 27, табл. – 5, слайдів. – 10, додат. – 2, бібліогр. – 20.

Метою дипломної роботи є дослідження та розробка технології шифрування персональних даних пацієнтів та їх медичних карток використовуючи стандарт шифрування даних AES. З допомогою цієї методики розроблено технологію захисту даних пацієнтів від несанкціонованого втручання для медичних закладів.

Методи та програмні засоби, використані при виконанні розробки системи: мова програмування C# та її бібліотеки, середовище розробки Microsoft Visual Studio, методологія гнучкої (Agile) розробки програмного забезпечення.

Результатом роботи є набір математичних моделей та комп’ютеризованих методів обробки шифрування даних з можливістю отримати якісні характеристики криптоаналізу. У вигляді модуля програмної системи реалізована бібліотека з набором алгоритмів шифрування.

Ключові слова: персональні дані, пацієнт, медична картка, діагностика, криптоаналіз, шифрування, програмна система, алгоритм, модуль, DES, AES.

# ABSTRACT

Thesis «System of encryption of personal data of patients and their medical records» by student Byts Taras Petrovych. – Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Software engineering department, group SPm-61 // Ternopil, 2017.

Pages. – 100, pictures. – 27, tables. – 5, slides – 10, add. – 2, bibl.ref. – 20.

The aim of the work is to research and develop technologies that encrypt personal data of patients and their medical records using AES encryption. With this technique designed to protect your patient data from unauthorized intervention for medical institutions.

The methods and software used in the performance of system development: C# programming language and its libraries, development environment Microsoft Visual Studio, a flexible methodology (Agile) software development.

The work is a set of mathematical models and computer processing methods of data encryption with the ability to get quality characteristics cryptanalysis. In a module software system implemented library with a set of encryption algorythms.

Keywords: personal data, patient, medical card, diagnosis, cryptanalysis, encryption, program system, algorythm, module, DES, AES.