

Джаббаров Д.В.

**НАВЧАЛЬНО-ДЕМОНСТРАЦІЙНА ПРОГРАМА НА ТЕМУ
"КОДУВАННЯ-ДЕКОДУВАННЯ ІНФОРМАЦІЇ" З ДИСЦИПЛІНИ
"ЦІЛІСНІСТЬ ТА БЕЗПЕКА ІНФОРМАЦІЇ": МОДУЛІ ШИФРУВАННЯ
ТА УПРАВЛІННЯ**

Постановка завдання. В даній роботі розглянули створення та модифікації алгоритмів шифрування даних для дисципліни «Цілісність та безпека інформації». ХХІ сторіччя – це період коли Інтернет досягнув найбільшого впливу на весь світ. Зараз можна знайти практично будь-яку інформацію використовуючи пошукові системи. Кожен з нас: студентів, викладачів – має сторінки в соціальних мережах, має власну електронну пошту, користується пошуковими мережами. Безпека конфіденційної інформації наразі є найважливішим поняттям для всіх.

Навчальні заклади, медицина, військові служби, поліція, фабрики, фірми, аеропорти - всі ці структури захищають дані за допомогою різних алгоритмів шифрування. Для того щоб шифрування було надійним – потрібно використати надійний алгоритм шифрування. Алгоритмів шифрування є дуже багато.

Основними проблемою в даній роботі були вибір алгоритмів шифрування, середі та мови їх розробки. Кожен з алгоритмів мав переваги та недоліки, деякі лише недоліки в порівнянні з іншими. Середовище і мова програмування – теж, виявилось проблемою через варіативність середовищ та велику кількість мов програмування.

Результати. По критеріям доступності, надійності та застосування в сучасних проектах було вибрано наступні алгоритми шифрування: AES, RC2, RC4, Base64, SH1, MD5, SHA256, TripleDES, шифр Vigenere – всі ці алгоритми шифрування були в відкритому доступі. Для їх реалізації найкращим варіантом була середа розробки –Visual Studio, та мова програмування – С#. С# досить проста мова програмування, зручна для новачків і в ній була бібліотека для криптографії: System.Security.Cryptography. Рекомендується використовувати С# для виконання схожих завдань.

Висновки. Надійний захист інформації – це надзвичайно важливий процес в сучасному світі. Існує дуже багато різноманітних алгоритмів шифрування. Рекомендується використовувати AES, RC2, RC4, Base64, SHA256, MD5, TripleDES – через їх надійність, швидкодію і доступність. Всі алгоритми шифрування було реалізовано за допомогою Visual Studio і мови програмування С#.

Складність полягала в поєднанні всіх алгоритмів шифрування в одну програму, але цю проблему подолано, використовуючи бібліотеку System.IO. Розроблена програма буде використовуватися для викладання теми «Кодування-декодування інформації» з дисципліни «Цілісність та безпека інформації» і дозволяє забезпечити декілька лабораторних робіт.

Робота виконана під керівництвом професора кафедри ІКТіМ Купріянова О.В.