АНОТАЦІЯ

до роботи «CryptoCovid» учня I курсу Київського національного університету ім. Тараса Шевченко Каца Олександра.

# Актуальність

Людство запам’ятає 2020 рік на довго. COVID-19… Глобальна пандемія, локдаун, вже загинуло більше за п’ять мільйонів людей по всьому світу й вірус досі не відступив. Навіть зараз кожен з нас під загрозою нових хвиль розповсюдження, мутацій хвороби.

Тисячі ПЦР тестів робляться кожного дня по всіх областях України. Також відповідно до Закону «про захист персональних даних» результати аналізів – особиста інформація, тому дуже важливо, щоб було неможливе викрадення чи втрата цієї конфіденційної інформації. До речі, це ж стосується не тільки ковіду, а й ,на приклад, ракових захворювань.

В нашій країні ця галузь потребує швидкої модернізації, адже Exel або блокнот бази даних не використовують аж ніяких інструментів захисту. Тому прийшла ідея створити додаток «CryptoCovid» для шифрування/дешифрування великих об’ємів інформації.

# Мета

Метою роботи було створення нескладної для використання програми для працівників мед-лабораторій, яка дозволяла би надійно захищати особисту інформацію клієнтів.

# Процес

Розробка програмного продукту відбувалася в кілька етапів:

* вивчення відповідних бібліотек й фреймворків,
* створення інтерфейсу користувача;
* реалізація алгоритму шифрування;
* тестування й усунення багів.

Об’єктом дослідження є алгоритми шифрування, предметом дослідження – створена програма.

# Безпека

Для роботи був обраний блочний симетричний алгоритм AES-256 за його значну крипостійкість й швидкість. В США він використовується для шифрування найбільш секретних повідомлень та документів.

# Результати

У результаті проведеної роботи були досліджені різноманітні криптографічні алгоритми, серед яких: AES, Blowfish, «ГОСТ 28147-89», RC4, SEAL, RSA, Elgamal, Diffie-Hellman.

Був складений план розробки, за яким створили програми для шифрування/дешифрування інформації «CryptoCovid». При цьому використовувались IDE Android Studio, середовище розробки Eclipse та алгоритм AES через його надійність та швидкість.

# Майбутнє

План удосконалення проекту на майбутнє:

* оптимізація інтерфейсу програми
* розробка цієї програми на платформах Android та IOS
* удосконалення використаних алгоритмів й ліквідація багів
* знаходження нових шляхів застосування проекту
* популяризація програмного продукту

Вербіцький О. В. Вступ до криптології. Львів: ВНТЛ, 1998. 248 с.

Зенин О. С., Иванов М. А. Стандарт криптографической защиты – AES. Конечные поля.