Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

# АТЕСТАЦІЙНА РОБОТА
# Пояснювальна записка

рівень вищої освіти другий (магістерський)

Метод передачі повідомлень з використанням квантово-захищеного криптографічного алгоритму
(тема)

Виконала: Ковтун К. О.
(прізвище, ініціали)
студент 2 курсу, групи БІКСм-19-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва освітньої програми)

Керівник доц. Сєвєрінов О.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

# ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові *Ковтун Кристині Олегівні*
(прізвище, ім'я, по батькові)

1.Тема роботи *Метод передачі повідомлень з використанням квантово-захищеного криптографічного алгоритму*
затверджена наказом по університету від "22" жовтня 2020 р. № 1412Ст
2. Термін подання студентом роботи (проекту) 15.12.2020
3. Вихідні дані до роботи (проекту) статті про квантово-захищені криптоалгоритми
4. Зміст пояснювальної записки (перелік питань, що потрібно розробити)
*1. Аналіз квантово-захищених криптоалгоритмів*
*2. Обґрунтування та вибір криптоалгоритму для захищеної передачі повідомлень*
*3. Реалізація програми захищеної передачі повідомлень*
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Презентаційний матеріал у вигляді слайдів*

## КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів магістерської атестаційної роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | *Отримання завдання* | *08.09.20* | Виконано |
| 2 | *Аналіз літературних джерел за темою атестаційної роботи* | *08.09.20-30.09.20* | Виконано |
| 3 | *Аналіз квантово-захищених криптоалгоритмів* | *30.09.20-10.10.20* | Виконано |
| 4 | *Вибір та аналіз швидкодії квантово-захищеного шифру* | *10.10.20-30.11.20* | Виконано |
| 5 | *Програмна реалізація захищеного методу передачі повідомлень* | *30.11.20-30.11. 20* | Виконано |
| 6 | *Оформлення пояснювальної записки* | *30.11.20-08.12. 20* | Виконано |
| 7 | *Представлення роботи на здачу* | *08.12.20-16.12.20* | Виконано |

Дата видачі завдання 08 ___вересня____2020 р.

Студент _____
(підпис)

Керівник роботи (проекту) _____ __доц. Сєвєрінов О.В._____
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка до роботи містить 87 с., 37 рис., 21 табл., 1 дод., 18 джерел.

ДСТУ, КАЛИНА, AES, RC6, TWOFISH, MARS, НКІ, QPU, D-WAVE, БСШ, КВАНТОВИЙ КОМП’ЮТЕР.

Метою атестаційної роботи є розробка захищеного методу передачі повідомлень за допомогою квантово-захищеного шифру.

Об’єкт дослідження – криптоалгоритми, що стійкі до квантового криптоаналізу.

Предмет дослідження –.теоретичні та практичні аспекти реалізації захищеного мережного з’єднання.

Методи дослідження – методи вимірювання і порівняння, системний аналіз, методи об’єктно-орієнтованого програмування.

У роботі розглянуто стан розробки квантового комп’ютера, здійснений аналіз застосування квантового комп’ютера для криптоаналізу блокових симетричних шифрів, розглянуто сертифіковані захищені носії ключової інформації.

Основні результати – проведено аналіз швидкодії блочних симетричних шифрів, створено програмну реалізацію програмного забезпечення для захищеної передачі повідомлень.

# ABSTRACT

The explanatory note contains: 87 pages, 37 figures, 21 tables, 1 addition, 18 sources.

DSTU, KALYNA, AES, RC6, TWOFISH, MARS, CKI, QPU, D-WAVE, BSC, QUANTUM COMPUTER.

The purpose of the work is to to develop a secure method of transmitting messages using a quantum-protected cipher.

The object of this research is cryptoalgorithms that are resistant to quantum cryptanalysis.

The subject of the research is theoretical and practical aspects of implementing a secure network connection.

Research methods - methods of measurement and comparison, systems analysis, methods of object-oriented programming.

The paper considers development of the quantum computer is considered in the work, the analysis of application of the quantum computer for cryptanalysis of block symmetric ciphers is carried out, the certified protected carriers of key information.

The main results - the analysis of the speed of block symmetric ciphers, created a software implementation of software for secure messaging.

ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

| | | |
|---|---|---|
| AES | – | Advanced Encryption Standart |
| NIST | – | National Institute of Standards and Technology |
| QPU | – | Quantum processing unit |
| БСШ | – | Блоковий симетричний шифр |
| ДСТУ | – | Державний технічний стандарт України |
| НКІ | – | Носій ключової інформації |
| ОЗП | – | Оперативний запам’ятовуючий пристрій |
| ОС | – | Операційна система |
| ПЕОМ | – | Персональна електронна обчислювальна машина |
| ПЗ | – | Програмне забезпечення |
| ЦП | – | Центральний процесор |

# ВСТУП

Важливим питанням на сьогоднішній день є забезпечення захисту інформації в інформаційно-телекомунікаційних системах. Однією складовою є забезпечення конфіденційності інформації за рахунок шифрування даних.

Найбільш серйозною проблемою для криптографії є розробка квантового комп’ютеру та вдосконалення алгоритмів квантового криптоаналізу. Стійкість найбільш поширених шифрів стала під загрозу. Українські стандарти ДСТУ 7624:2014 та ДСТУ 8845:2019 забезпечують високий рівень стійкості до квантових атак.

Слід зауважити що на тему оцінки швидкодії ДСТУ 7624:2014 [12] існує безліч наукових робіт [1],[2] проте майже всі вони призначені для оцінки оптимізованих варіантів шифру або підрахунку його складності чи швидкодії на при апаратній/програмно-апаратній реалізації. Під час оцінки швидкодії криптоалгоритмів здебільшого використовуються спеціальні бібліотеки які містять потрібний шифр та спеціальні інтерфейси адже реалізація оптимізованого варіанту шифру (навіть якщо він наданий розробником шифру) потребує значних зусиль з інтеграції.

Основною задачею роботи є забезпечення конфіденційності та цілісності інформації, яка передається між клієнтськими та серверними частинами прикладних програмних систем (TCP-з’єднань).

Створюване програмне забезпечення захищеної передачі повинно забезпечувати встановлення захищеного TCP-з'єднання між клієнтом та сервером, а також шифрування даних TCP-з'єднання, які передаються між клієнтом та сервером.

Зазначені функції програмний комплекс захищеної передачі повідомлень виконує шляхом застосування механізмів криптографічного захисту інформації, яка передається між клієнтом та сервером.

Для організації ключової системи (управління ключовими даними) засобів комплексу рекомендується генерувати ключ на захищений носій ключової інформації.

Завдання магістерської роботи є проведення дослідження квантово-захищених криптоалгоритмів для подальшого використання у програмному комплексі захищеної передачі даних.

Завданням практичної направленості є програмна реалізація програмного забезпечення для захищеної передачі повідомлень.

У першому розділі наведено загальні відомості щодо створення та характеристик квантового комп’ютера та квантової захищенності блочних симтеричних шифрів.

У другому розділі розглядаються поширені блочні симетричні шифри.

У третьому розділі описано методику тестування швидкодії блочних симетричних шифрів.

У четвертому розділі наведено результати тестування швидкодії блочних симетричних шифрів.

У п’ятому розділі описано програмне забезпечення захищеної передачі повідомлень, інстуркція користувачу та огляд захищених носіїв ключової інфомації.

В тезах доповідей восьмої міжнародної науково-технічної конференції «Проблеми інформатизації» опубліковані проміжні результати магістерської роботи.

# 1 АНАЛІЗ ЗАСТОСУВАННЯ КВАНТОВИХ КОМПЮТЕРІВ В КРИПТОГРАФІЇ

## 1.1 Аналіз основних проблем створення квантового комп’ютера та розробки математичного забезпечення

Нині вирішується дві важливі проблеми – створення квантового комп’ютера та розробки і реалізації математичних методів квантового криптоаналізу. Проведемо аналіз стану їх вирішення та відповідні пропозиції.

Аналіз показує, що основна проблема у побудові квантового комп'ютера полягає в тому, що необхідно створити систему, яка б задовольняла майже несумісним таким вимогам [11]:

– кубіти (елементи квантового комп'ютера) повинні бути максимально ізольовані один від одного та від навколишнього середовища;

– можливість корельованого впливу на пару кубітів, тобто, потрібно не тільки вміти змінювати стан одного кубіту, але й ще вмикати та вимикати взаємодію між парою сусідніх кубітів;

– система кубітів повинна бути досить стабільною, щоб зберігати корельованість станів, але одночасно й легко відновлюваною для нового циклу обчислень;

– реалізовувати таку сукупність зворотних перетворень над системою кубітів, які б дозволили виконати будь-яку потрібну логічну операцію;

– під час обчислень система повинна зберігати квантові властивості, але наприкінці треба зробити вимірювання, яке б однозначно визначило стан системи і у такий спосіб звело б квантову інформацію в класичну.

Дуже важливою властивістю квантових об'єктів є можливість здійснювати паралельні операції. Так, для системи із N кубітів, що перебуває в переплутаному стан то в такій системі ефективно кодується відразу 2N чисел. Тому операція над

нею, завдяки когерентності станів різних кубітів, впливає на всі доданки в сумі і це дозволяє обробляти відразу всі 2N чисел.

На сьогодні вже існують квантові алгоритми, які дають змогу проводити атаки на такі існуючі асиметричні криптосистеми [11]:

– системи, що базуються на складності факторизації великого цілого числа (RSA);

– системи, що базуються на складності вирішення дискретного логарифму в скінченному полі Галуа (DSA) ;

– системи, що базуються на складності вирішення дискретного логарифму в групі точок еліптичної кривої (ECC) ;

– системи на базі алгебраїчних решіток (NTRU).

Усі вказані криптосистеми відносяться до класу ймовірно-стійких. А ця ймовірна стійкість як раз і визначається можливостями появи квантових комп’ютерів, і, як наслідок, вирішення задачі повного розкриття.

Значних здобутків досягла фірма D-Wave, яка стала першою компанією, що продала комерційну версію квантового комп’ютера. Так з 20 травня 2011 D-Wave Systems продає за $ 11 млн доларів квантовий комп'ютер D- Wave One з 128-кубітним чіпсетом, який виконує тільки одну задачу – дискретну оптимізацію. 25 травня 2011 Lockheed Martin підписала багаторічний контракт з D-Wave Systems, що стосується виконання складних обчислювальних завдань на квантових процесорах. Контракт також включає в себе технічне обслуговування, супутні послуги і купівлю квантового комп'ютера D- Wave One [14].

Квантовий комп'ютер – це пристрій, процеси обчислень та передачі даних у якому ґрунтуються на явищі квантової суперпозиції і квантової заплутаності. На нинішній час повноцінний квантовий комп'ютер є ще поки гіпотетичним пристроєм, можливість побудови якого пов'язана з вирішенням складних теоретичних та практичних проблем квантової фізики та складних експериментів. Дослідження в цьому напряму знаходяться на передньому краї сучасної фізики. Важливою проблемою є також обґрунтування вимог та створення мови програмування для квантового комп’ютера.

Відносно поняття «квантовий паралелізм» в обчисленні можна трактувати так: «Дані в процесі обчислень є квантовою інформацією, яка після закінчення процесу перетворюється в класичну шляхом вимірювання кінцевого стану квантового регістра з заданим числом кубітів. При цьому виграш в квантових алгоритмах досягається за рахунок того, що при застосуванні однієї квантової операції велике число коефіцієнтів суперпозиції квантових станів, які у віртуальній формі містять класичну інформацію, що перетворюється одночасно».

Вчені D-Wave опублікували статтю, в якій повідомляється, що за допомогою методу кубіто-тунельної спектроскопії ними було доведено наявність квантової когерентності і заплутаності між окремими підгрупами кубітів в процесорі під час проведення обчислень (розміром 2 і 8 елементів).

Наприкінці у грудні 2015 року фахівці компанії Google підтвердили, що згідно з їх дослідженням в комп'ютері D-Wave використовуються квантові ефекти. При цьому в «1000-кубітном» комп'ютері кубіти в дійсності організовані в кластери по 8 кубіт кожен. Якраз це і дозволило добитися в одному з алгоритмів швидкодії в 100 млн разів більше ніж у звичайному комп'ютерові [16].

В той же час програмна заява NIST або АНБ ретельно опрацьована протягом значного часу. Комітет, відповідальний за складання його, обговорює кожне речення; нічого не залишено на волю випадку або недбалого редагування. Крім того, коли попросили роз'яснити звіт в серпні 2015 року, АНБ випустило оновлену версію, яка значно не відрізняється від першої. Таким чином, ми повинні почати з передумови, що АНБ мало намір в заяві передати, що воно і зробило.

Ще незрозуміло, коли масштабовані квантові комп'ютери будуть доступні, проте в минулому році, дослідники, що працюють на побудову квантового комп'ютера підрахували, що цілком ймовірно, що квантовий комп'ютер здатний атакувати RSA-2048 в лічені години може бути побудований до 2030 року, але це вимагає закласти в бюджет близько мільярда доларів . Це серйозна довгострокова загроза для криптосистем, що в даний час стандартизована в NIST. Таким чином, перехід від 112 до 128 біт безпеки, можливо, менш актуальне, ніж перехід

від існуючих криптосистем з пост квантової криптосистемою. Цей пост-квантовий перехід викликає багато фундаментальних проблем.

Так , розробка стандартів для пост-квантової криптографії вимагає значних ресурсів для аналізу кандидата квантово-стійких схем, і зажадає значного залучення громадськості запевнити довіри в алгоритмах NIST. Інтерес в областях квантових обчислень і квантової криптографії останнім часом збільшилася, в зв'язку з розвитком квантової обчислювальної техніки і останні зміни NIST це підтверджують. Це дає можливість для взаємодії з науковою спільнотою, яка може не настати знову до практичних квантових обчислень, що є дійсно неминучим. Отже, NIST починає готуватися до переходу до квантово-стійкої криптографії.

NIST США робить наступні кроки, щоб ініціювати стандартизацію пост-квантової криптографії. У NIST планується вказати попередні критерії оцінки для квантово-наполегливих стандартів шифрування з відкритим ключем. Критерії включають безпеку та експлуатаційні вимоги. Проект критеріїв буде винесено на обговорення громадськості в 2016 році і сподіваються завершити до кінця року. У той час NIST почне приймати пропозиції щодо квантово-стійкої асиметричної криптографії, в першу чергу ЕП.

Хоча цей процес буде мати багато спільного з процесами, які привели до стандартизації AES і SHA-3, це не змагання. NIST бачить свою роль в управлінні процесом досягнення консенсусу спільноти прозорим і своєчасним чином. В ідеалі, кілька алгоритмів будуть з'являтися у міру "правильності вибору". NIST може вибрати один або більше з ЕП, що пройдуть випробовування.

Коли стандарти для квантово-стійкої криптографії з відкритим ключем стануть доступні для аналізу, NIST буде переглядати загрози квантових комп'ютерів до існуючих стандартів, що нині застосовуються, та може відкликати такі стандарти. Тому установи повинні бути готові до переходу від існуючих алгоритмів до стійких у постквантовий період вже в найближчі 6-8 років. Як показує аналіз, таких стандартизованих ЕП в даний час не існує.

Наведені вище результати аналізу стану розробки та можливості застосування квантового комп'ютера, з урахуванням [14, 16], дозволяють обґрунтувати необхідність та важливість розробки постквантової криптографії. Вирішення цієї задачі можливо при наявності моделі порушника, по суті вона зводиться до моделі квантового комп'ютера з конкретними характеристиками та можливостями по реалізації квантових алгоритмів крипто аналізу.

## 1.2 Аналіз основних загроз відносно криптографічних перетворень у постквантовий період

При побудові моделей загроз у постквантовий період, за нинішніх умов, в якості основних необхідно брати методи криптоаналізу, як основні моделі загроз, що можуть бути реалізованими на квантовому комп'ютерові при вирішенні задач криптоаналізу. Причому, усі вказані методи повинні бути орієнтовані на використання специфіки квантового комп'ютера та мову програмування на ньому.

До основних задач, які можуть бути вирішені на квантовому комп'ютерові в першу чергу необхідно віднести такі:

- квантовий алгоритм факторизації Шора [17];
- квантовий алгоритм Гровера [13];
- квантовий алгоритм Шора вирішення дискретного логарифму в скінченному полі;
- квантовий алгоритм Шора вирішення дискретного логарифму в групі точок еліптичної кривої [17];
- квантовий алгоритм криптоаналізу для перетворень в фактор кільці [11].

Проблема криптоаналізу, на вирішення якої спрямовано метод Гровера, може бути сформульована наступним чином [13]. Нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент, що володіє деякою властивістю, яка перевіряється з поліноміальною складністю. Потрібно

знайти цей елемент з мінімально можливою складністю і, зрозуміло за менший час. Для пошуку можна скористатися математичним апаратом узагальненого «парадоксу про день народження». Детально використання цього апарату наведено та проведені відповідні дослідження в 2 та 3 розділах. Основними умовами застосування цієї моделі є випадковість та рівноймовірність здійснення запитів, тобто вхідних даних. Тому при виконанні k запитів ймовірностей успіху можна оцінити як k/N.

Вирішення цієї задачі може бути виконане з використання декількох класичних алгоритмів, в яких для підвищення ймовірності успіху процедура повторюється багатократно. Для того, щоб отримати при повторюваних квантових перетвореннях результат, що очікується, дуже важливо визначити, коли потрібно зупинитися і провести уточнення. Наприклад, використовуючи алгоритм Гровера можна знайти секретний ключ симетричного шифрування чи гешування за ітерацій, де - розмір простору ключів. В якості прикладу в таблиці 1.1 наведені оцінки стійкості симетричних криптографічних систем проти квантового криптоаналізу. Аналіз даних таблиці показує, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму Гроувера суттєво зменшується.

Зроблені попередні оцінки показують, що з використанням квантового алгоритму Шора задачу факторизації модуля N можна звести до вирішення еквівалентної проблеми, сутність етапів якої є у наступному:

– вибрати випадково й рівномірно ціле число a взаємно просте з N;

– для вибраного числа a, що є взаємно простим з N, знайти порядок r елемента a mod N.

Взаємну простоту числа та N виконати використовуючи Алгоритм Евкліда [11]. Якщо a не є взаємно простим з N, то потрібно повторно вибрати a , взаємно просте з N. Якщо a є взаємно простим з N, то порядок r елемента a mod N буде дільником числа N.

Збільшення розміру модуля перетворення і, відповідно особистого ключа, при застосуванні квантового алгоритму Шора не забезпечує необхідного

збільшення складності дискретного логарифмування в скінченному полі, як при зломі електронного цифрового підпису так і направленого шифрування. Наприклад, для модуля $P \geq 23072$ складність дискретного логарифмування в скінченному полі складає $1.4 \cdot 1031$, а з застосуванням алгоритму Шора всього $2.9 \cdot 1010$ операцій. Але, в той же час, при застосуванні квантового алгоритму проблемним є реалізація регістрів зі значним числом кубітів – не менше 9216 кубітів. Очевидно досягти такого розміру буде ще певний час проблемною задачею.

Збільшення розміру порядку базової точки при криптоаналізі з використанням квантового алгоритму не дає суттєвого збільшення криптографічної стійкості криптографічної системи на еліптичних кривих. Також показано [13], що при збільшені модуля, складність дискретного логарифмування класичними методами в групі точок еліптичної кривої зі збільшенням порядку базової точки збільшується суттєво. Але потрібно взяти до уваги, що реалізація квантового алгоритму пов’язана зі застосуванням регістрів з великою кількістю кубітів, яка необхідна для проведення квантової атаки. Наприклад для базової точки з порядком 2571 необхідно використовувати реєстр з довжиною 4016 кубітів. Вважається, що така велика кількість кубітів все певний час буде не реалізуємо.

## 1.3 Аналіз можливостей застосування квантових комп’ютерів для криптоаналізу БСШ

Існують також квантові алгоритми, що можуть використовуватися для проведення криптоаналізу симетричних криптосистем, в першу чергу блокових та потокових симетричних шифрів [3, 4, 7, 8, 9, 12]. В таких алгоритмах одна і таж процедура криптоаналізу повторюється багатократно. Але потрібно враховувати, що при мінімізації її складності повторення квантової процедури може покращувати результат деякий час, але після достатньої кількості повторень результат знову стає гіршим. Вказане можна пояснити тим, що

квантова процедура є унітарним перетворенням, в процесі якого здійснюється поворот в комплексному просторі. Таке повторне застосування квантового перетворення може наближати невідомий стан все ближче і ближче до потрібного стану, але після певного числа перетворень подальше застосування квантового перетворення може пройти повз потрібного стану і віддалить правильне рішення. Тому, для того, щоб отримати позитивний результат при повторюваних квантових перетвореннях, дуже важливо знати, коли отримане краще наближення. [174].

Показано, що одним із ефективних алгоритмів криптоаналізу симетричних криптоперетворень є алгоритм Гровера [13]. При його використанні секретний ключ симетричного крипто перетворення можна знайти виконавши (за час) $\sqrt{K}$ , де $K$ - розмір ключа. Більш детальні оцінки стійкості відомих чи перспективних блокових симетричних перетворень (шифрів) проти квантового криптоаналізу наведено в таблиці 1.1 [11].

Із аналізу таблиці 1.1 видно, що стійкість блокових симетричних перетворень (шифрів) при атаці з використанням квантового алгоритму суттєво зменшується. Наприклад БСШ DES буде повністю скомпрометований і не можливо буде вважати його стійким, так як вона буде оцінюватись значенням $2^{28}$. Навіть при використанні AES -128/128 значення секретного ключа можна буде знайти за час, приблизно $2^{64}$. А значення $2^{64}$ при нинішніх оцінках уже вважається небезпечним. Що стосується AES-256 біт, то тоді час роботи алгоритму Гровера становить $2^{128}$ , що є допустимим в наші дні.

Таблиця 1.1 – Стійкість блокових симетричних криптоперетворень проти квантового криптоаналізу при атаці на ключ та на блок повідомлення

| № п/п | Шифр | Розмір блока/ключа, біт | Кількість необхідної пам'яті для атаки на блок повідомлення/ключ, кубіт | Стійкість при атаці | |
|---|---|---|---|---|---|
| | | | | Блок повідомлення, квантових операцій | Ключ, квантових операцій |
| 1 | AES-128 | 128/128 | 128/128 | $2^{64}$ ($10^{19,2}$) | $2^{64}$ ($10^{19,2}$) |
| 2 | AES-256 | 128/256 | 128/256 | $2^{64}$ ($10^{19,2}$) | $2^{128}$ ($10^{38,4}$) |
| 3 | DES | 64/56 | 64/56 | $2^{32}$ ($10^{9,6}$) | $2^{28}$ ($10^{8,4}$) |
| 4 | TDES | 64/168 | 64/168 | $2^{32}$ ($10^{9,6}$) | $2^{134}$ ($10^{40,2}$) |
| 5 | ГОСТ-28147 | 64/256 | 64/256 | $2^{32}$ ($10^{9,6}$) | $2^{128}$ ($10^{38,4}$) |
| 6 | Калина-128 | 128/128 | 128/128 | $2^{64}$ ($10^{19,2}$) | $2^{64}$ (10 19,2) |
| 7 | Калина-256 | 256/256 | 256/256 | $2^{128}$ ($10^{38,4}$) | $2^{128}$ ($10^{38,4}$) |
| 8 | Калина-512 | 512/512 | 512/512 | $2^{256}$ ($10^{76,8}$) | $2^{256}$ ($10^{76,8}$) |
| 9 | Blowfish | 64/448 | 64/448 | $2^{32}$ ($10^{9,6}$) | $2^{224}$ ($10^{67,2}$) |

Таким чином, при появі квантового комп'ютера з певними параметрами та обчислювальною спроможністю, його застосування може привести, а скоріше всього приведе, до успішного злому ймовірно-стійких крипто перетворень, а також симетричних крипто перетворень, довжини ключів та блоків (початкових станів) яких будуть вибрані без урахування можливостей квантового криптоаналізу.

## 1.4 Квантовий алгоритм Гровера та його використання для квантового криптоаналізу симетричних криптосистем

Проблема, на вирішення якої спрямовано метод Гровера, може бути сформульована наступним чином. Нехай дана неупорядкована база даних (список) з N елементів, і нехай в ній існує один елемент, що володіє деякою властивістю, що легко перевіряється. Потрібно знайти цей елемент.

Таким чином, ми будемо формулювати проблему пошуку наступним чином в термінах експоненційно великої неупорядкованої бази даних з $N=2^n$ елементами, серед яких один елемент пронумерований спеціальним чином. Проблема полягає у тому, що необхідно знайти цей елемент. Елементарна теорія ймовірностей показує, що якщо ми переглянемо k елементів, то ми маємо ймовірність k/N знаходження необхідного нам елемента. Отже, необхідно створити O(N) запитів до бази, щоб знайти необхідний елемент з будь-якою константною (не залежної від N) ймовірністю. Алгоритм Гровера дозволяє знайти необхідний елемент з ймовірністю достатньо близькою до 1 за $O(\sqrt{N})$ кроків (більш точно, за $O(\sqrt{N})$) ітерацій виконання процедури, але за $O(\sqrt{N}\log N)$ кроків.

Існує безліч класичних алгоритмів, в яких процедура повторюється багато разів для досягнення кращого результату. Повторення квантової процедури може покращувати результат деякий час, але після достатньої кількості повторень результат знову стає гіршим. Квантова процедура це унітарне перетворення, яке здійснює поворот в комплексному просторі. Тому, в той час як повторне застосування квантового перетворення може повертати поточний стан все ближче і ближче до потрібного нам стану протягом якогось часу, подальше застосування квантового перетворення змусить стан пройти повз потрібного стану і йти все далі і далі від нього. Тому, для того, щоб отримати добрий результат при повторюваних квантових перетвореннях, дуже важливо знати, коли потрібно зупинитися [13].

З використання алгоритму Гровера ми можемо знайти секретний ключ шифрування за час $\sqrt{K}$. Детальний опис стійкості симетричних систем проти квантового криптоаналізу наведено в таблиці 1.1.

В таблиці чудово видно, що стійкість симетричних шифрів при атаці з використанням квантового алгоритму суттєво зменшується. Це означає, що DES буде повністю знищений і не можливо буде вважати його стійким, його стійкість буде дорівнювати $2^{28}$. Навіть при AES -128 можна було б знайти секретний ключ за час , приблизно $2^{64}$. А $2^{64}$ в наші дні вважається небезпечно. Що стосується AES-$2^{56}$ біт , то тоді час роботи алгоритму Гровера становить $2^{128}$ , що є допустимим в наші дні. Що стосується ГОСТ 28157-89 , вітчизняний стандарт шифрування має розмір блоку 64 біта і розмір ключа $2^{56}$ біт. При атаці на блок повідомлення , стійкість буде $2^{32}$ , а при атаці на ключ - $2^{128}$.

З використання алгоритму Гровера ми можемо знайти секретний шифрування за час √ K. Це означає , що DES буде повністю знищений і не можливо буде вважати його стійким , його стійкість буде дорівнює $2^{28}$. Навіть при AES -128 можна було б знайти секретний ключ за час , приблизно $2^{64}$. А $2^{64}$ в наші дні вважаються небезпечно. Що стосується AES -256 біт , то тоді час роботи алгоритму Гровера становить $2^{128}$ , що є допустимим в наші дні. Що стосується ГОСТ 28157-89 , вітчизняний стандарт шифрування має розмір блоку 64 біта і розмір ключа 256 біт. При атаці на блок повідомлення , стійкість буде $2^{32}$, а при атаці на ключ – $2^{128}$ .Навіть враховуючи сучасний розвиток науки техніки в області квантових обчислень і квантового криптоаналізу , а також заяв фірми D-Wave Systems про продаж своїх «квантових машин» , які не реалізують квантові ефекти , необхідні для роботи алгоритмів Шора і Гровера , сучасні криптосистеми (як симетричні так і асиметричні ) можна вважати безпечними проти квантового криптоаналізу . Але враховуючи темпи розвитку і досліджень в області квантових обчислень , сучасні криптосистеми стануть вразливими для квантових атак.

## 1.5 Технологія та специфікації квантового комп’ютера D-Wave

Замість того, щоб зберігати інформацію, використовуючи біти, представлені 0 або 1, як це роблять звичайні комп’ютери, квантові комп’ютери використовують квантові біти або кубіти для кодування інформації як 0, 1 або одночасно. Ця суперпозиція станів, поряд з квантовими ефектами заплутаності та квантового тунелювання, дозволяють квантовим комп’ютерам одночасно розглядати та маніпулювати багатьма комбінаціями бітів. Комп’ютери D-Wave [14] використовують квантовий відпал для вирішення проблем, представлених у вигляді математичних функцій (що нагадує ландшафт вершин та долин), використовуючи квантово-механічні ефекти, щоб знайти їх загальні мінімуми, відповідні оптимальним або майже оптимальним рішенням. Обчислення виконуються шляхом ініціалізації блоку квантової обробки (QPU) у основний стан відомої проблеми та відпалу системи до проблеми, яку потрібно вирішити, таким чином, щоб вона залишалася в низькоенергетичному стані протягом усього процесу. В кінці обчислення кожен кубіт закінчується як 0 або 1, концепт зображений на рисунку 1.1. Цей кінцевий стан є оптимальним або майже оптимальним рішенням проблеми, яку потрібно вирішити.

Рисунок 1.1 – Суперпозиція кубіта

У природі фізичні системи, як правило, еволюціонують у напрямку до найнижчого енергетичного стану: предмети ковзають вниз по пагорбах, гарячі речі охолоджуються тощо. Така поведінка стосується і квантових систем. Щоб уявити це, подумайте про мандрівника, який шукає найкраще рішення, знаходячи найнижчу долину в енергетичному ландшафті, яка представляє проблему. Класичні алгоритми шукають найнижчу долину, розміщуючи подорожуючого в якійсь точці ландшафту і дозволяючи цьому подорожуючому рухатися на основі місцевих варіацій. Хоча, як правило, найефективніше рухатись під гору і уникати підйому на занадто високі пагорби, такі класичні алгоритми схильні вести подорожуючих у найближчі долини, які, можливо, не є загальним мінімумом. Зазвичай потрібні численні випробування, причому багато мандрівників починають свої подорожі з різних точок. На відміну від них, квантовий відпал починається з того, що мандрівник одночасно займає безліч координат завдяки квантовому явищу суперпозиції. Ймовірність перебування в будь-якій заданій координаті плавно еволюціонує у міру відпалу, при цьому ймовірність зростає навколо координат глибоких долин. Квантове тунелювання дозволяє мандрівнику проходити через пагорби, а не змушувати їх підніматися, зменшуючи шанс потрапити в пастку в долинах, які не є загальним мінімумом. Квантове заплутування ще більше покращує результат, дозволяючи мандрівникові виявляти кореляцію між координатами, що ведуть до глибоких долин.

У фізичному корпусі системи D-Wave [14] розміщені складні кріогенні системи охолодження, екранування та введення / виводу для підтримки єдиного QPU розміром з мініатюру. Більша частина фізичного обсягу системи необхідна для розміщення холодильної системи та забезпечення легкого доступу до послуг. Хоча традиційні суперкомп'ютери генерують величезну кількість тепла і споживають величезну кількість енергії, система D-Wave споживає менше 25 кВт енергії, більша частина якої спрямована на роботу систем охолодження та інтерфейсних серверів. Щоб квантові ефекти грали роль у обчисленні, QPU вимагає екстремального, ізольованого середовища. Холодильник та шари

екранування створюють внутрішнє середовище з високим вакуумом із температурою, близькою до абсолютного нуля, яка ізольована від зовнішніх магнітних полів, вібрації та радіочастотних сигналів будь-якої форми. Суміжні шафи містять підсистеми управління та інтерфейсні сервери (зображено на рисунку 1.2), що забезпечують підключення до системи.


Рисунок 1.2 – Сервер D-Wave

QPU D-Wave [14] працює майже до абсолютного нуля. Ця надзвичайно низька температура, поряд із екранованим середовищем, яке ізолює QPU від оточення, дозволяє QPU поводитися квантовомеханічно. Системи D-Wave працюють на рівні менше 15 мілікельвінів, приблизно в 180 разів холодніше, ніж міжзоряний простір. Надзвичайно ізольоване середовище, необхідне для QPU,

ставить незвичні вимоги до конструкції, матеріалів та виробничих процесів, необхідних для різних підсистем. Підсистема вводу-виводу, яка передає інформацію в QPU і назад, відфільтровуючи всі небажані шуми, вимагає різноманітних нормальних та надпровідних матеріалів для забезпечення необхідних характеристик. Підсистема магнітного екранування забезпечує середовище з низьким рівнем поля, необхідне для QPU, використовуючи високопроникні та надпровідні матеріали для досягнення полів нижче 1 нанотесла. Це в 50 000 разів менше магнітного поля Землі.

D-Wave QPU побудований з крихітних металевих петель, кожна з яких становить один кубіт (показано на рисунку 1.3 червоним кольором).

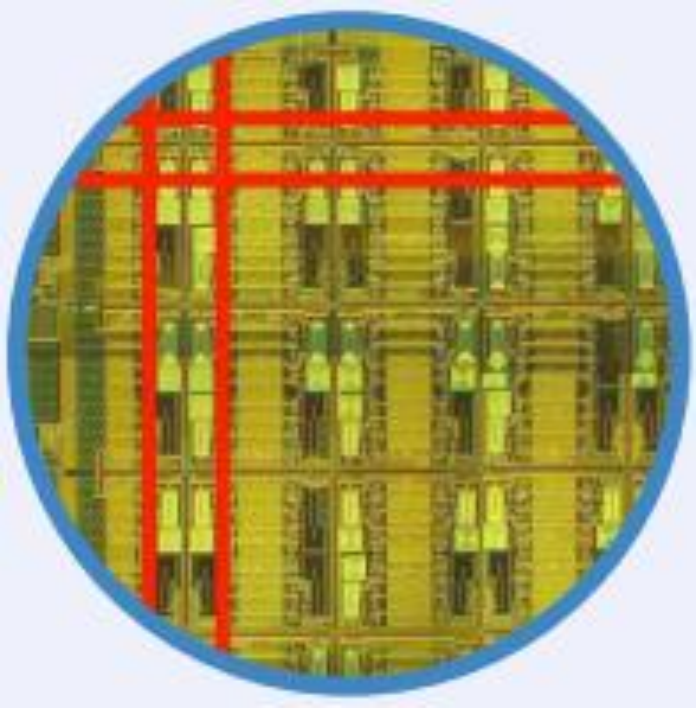

Рисунок 1.3 – Кубіти квантового комп’ютера

Починаючи з кімнатної температури у верхній частині, температура знижується на кожному рівні, як зображено на рисунку 1.4, поки не буде близькою до абсолютного нуля, де знаходиться сам QPU.

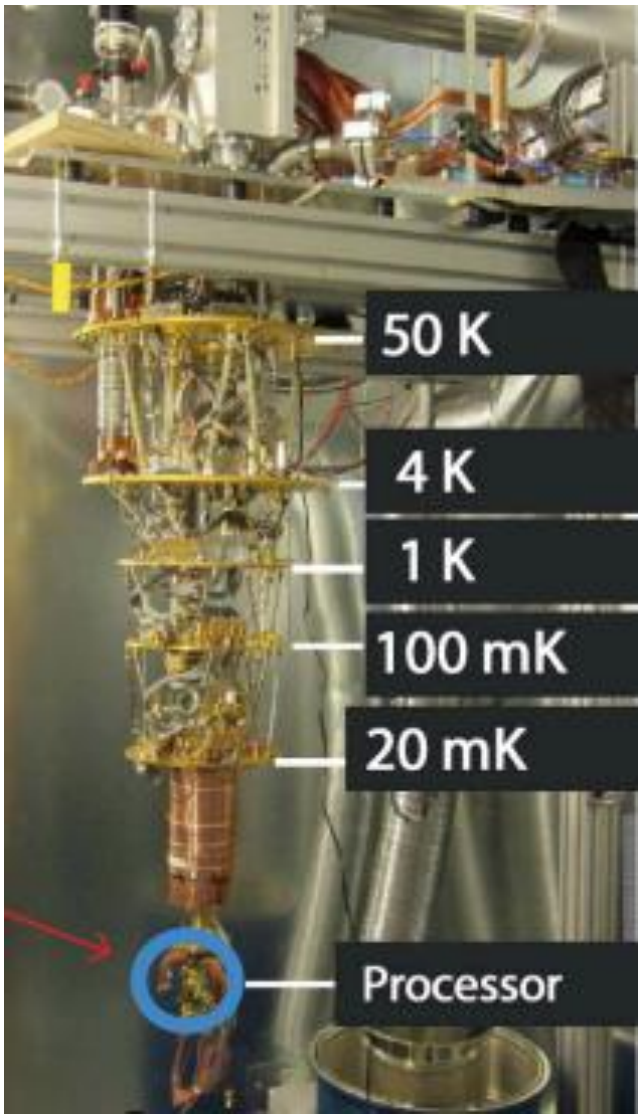


Рисунок 1.4 – Зниження температури QPU майже до абсолютного нуля

При дуже низьких температурах, близьких до абсолютного нуля, ці петлі стають надпровідниками та виявляють квантово-механічні ефекти. На рисунку 1.5 зображено квантовий процесор D-Wave.

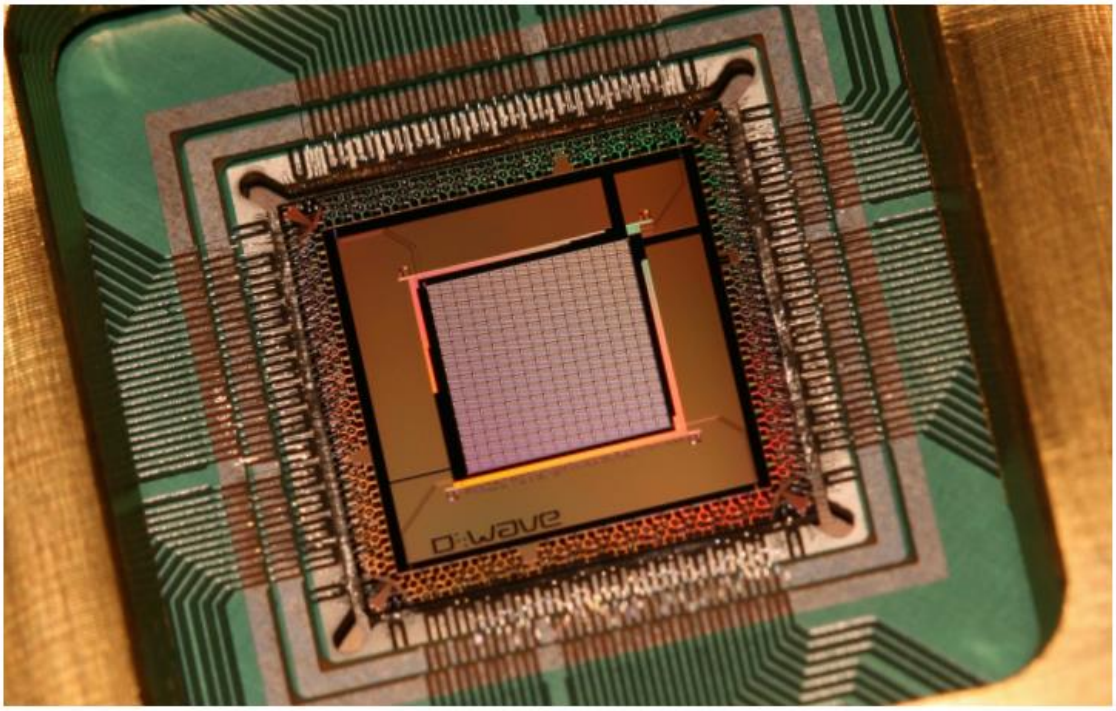


Рисунок 1.5 – Квантовий процесор D-Wave

Перебуваючи в квантовому стані, струм тече в обох напрямках одночасно, що означає, що кубіт знаходиться в суперпозиції – тобто одночасно і в стані 0, і в 1. В кінці процесу вирішення проблеми ця суперпозиція руйнується в один із двох класичних станів, 0 або 1. Перехід від одного кубіта до багатокубітного QPU вимагає взаємозв’язку кубітів для обміну інформацією. Кубіти з'єднані за допомогою муфт, які також є надпровідними петлями. Взаємозв'язок кубітів і муфт разом із схемою управління для управління магнітними полями створює інтегровану тканину програмованих квантових пристроїв. Коли QPU вирішує проблему, усі кубіти потрапляють у свої кінцеві стани, і значення, які вони мають, повертаються користувачеві у вигляді бітового рядка.

З моменту первинного впровадження системи 2000Q D-Wave представила низку вдосконалень як в апаратному, так і в програмному забезпеченні. Розроблена для пришвидшення розробки комерційних квантових додатків, квантова система Advantage створить нову апаратну та програмну платформу, яка прискорить і полегшить доставку квантових обчислювальних програм, що забезпечують переваги клієнтів для реальних додатків. Компоненти платформи

Advantage будуть виходити на ринок протягом 2020 року через постійні QPU та оновлення програмного забезпечення, які будуть доступні через Leap.

В таблицях 1.2 – 1.9 показані усі технічні та ергономічні характеристики квантового комп’ютера D-Wave.

Таблиця 1.2 – Технічні характеристики QPU

| Технічні характеристики QPU | |
|---|---|
| Кількість кубітів | 5760 |
| Кількість куплерів | 35,000+ |
| Розмір графу | P16 (Pegasus) |
| Температура кубіта | < 15 мК |

Таблиця 1.3 – Розміри

| Розміри | |
|---|---|
| Довжина | 3,0 м |
| Ширина | 2,1 м |
| Висота | 3,0 м |
| Вага | 3800 кг |

Таблиця 1.4 – Потужність

| Потужність | |
|---|---|
| Номінальна потужність | 25 кВт, максимум |
| Напруга мережі | 120/208 В, 60 Гц (стандарт)<br>230/400 В, 50 Гц (міжнародний) |
| Підключення до мережі | 3 провіда + N + PE |

Таблиця 1.5 – Охолодження

| Охолодження | |
|---|---|
| Охолоджуюча рідина | 15 кВт охолодження (4,3 холодильних тон) |

Продовження таблиці 1.5

| | |
|---|---|
| Максимальний тиск води | 6 бар |
| Максимальна температура | 25 °C @ 20,5 л/хвилина |
| Мінімальна температура | 15 °C @ 9,4 л/хвилина |
| HVAC (система управління кліматом) | 5 кВт (17,000 BTU/год) у звичайному режимі<br>12.5 кВт (43,000 BTU/год) у допоміжному режимі |

Таблиця 1.6 – Відповідність нормативним актам

| Відповідність нормативним актам | |
|---|---|
| США | UL 62368-1, FCC Part 15 part B Class A |
| Канада | CSA C22.2 NO. 62368-1:19, Industry Canada ICES-003, Class A |

Таблиця 1.7 – Екологічні вимоги

| Екологічні вимоги | |
|---|---|
| Робоча температура | 20 до 25 °C |
| Швидкість зміни температури | 1 °C в 15 хв (максимально допустима) |
| Перевезення / зберігання | –10 до 40 °C |
| Вологість (робоча) | 5 до 80% RH (без конденсації) |
| Вологість (перевезення / зберігання) | < 85% RH (без конденсації) |
| Тиск (Робочий<br>перевезення / зберігання) | 65 до 106 кПа<br>65 до 106 кПа |
| Висота над рівнем моря | 0 до 2300 м |
| Максимальна вібрація будівлі | 50 µm в секунду |

Продовження таблиці 1.7

| | |
|---|---|
| Магнітне поле навколишнього середовища | 100 μT (максимально допустима) |
| Рівень шуму | 75 дБА |

Таблиця 1.8 – Витратні матеріали

| Витратні матеріали | |
|---|---|
| Гази | Азот якості 4.8 (99.998%)<br>Гелій якості 5.0 (99.999%)<br>Використання: ~1 циліндр T-розміру кожен на рік |
| Кріогени | Рідкий азот<br>Використання: ~6 л/день |

Таблиця 1.9 – Вимоги до мережі

| Вимоги до мережі | |
|---|---|
| L2, L3 вимоги | Виділений блок L2<br>/27 внутрішніх IP-адреси |
| Швидкість Ethernet | E100 (може бути обмежена 10 Мбіт/с) |
| IP адреси | IPv4 доступний зовні; назначені |
| Фізичні зв’язки | RJ-45 GE (1000BASE-TX) |

## 1.6 Хмарні обчислення квантового комп’ютера та вартість злому

На сьогоднішній день платформа Amazon пропонує клієнтам здійснити хмарні обчислення за допомогою квантових комп’ютерів (рис. 1.6).

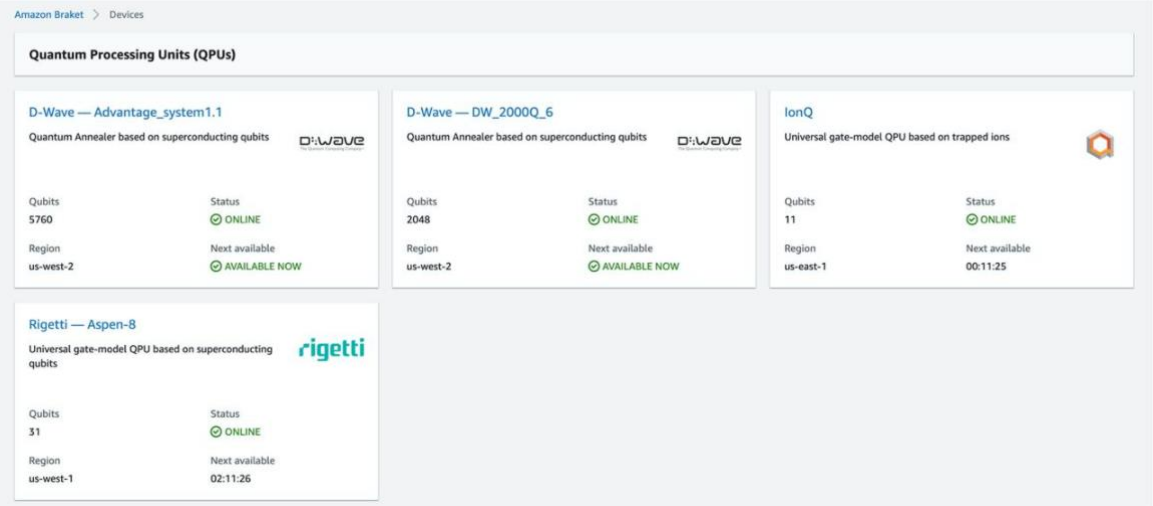


Рисунок 1.6 – Квантові комп’ютери на платформі хмарних обчислень Amazon

В таблиці 1.10 наведено характеристики наявних квантових комп’ютерів.

Таблиця 1.10 Характеристики квантових комп’ютерів

| Виробник та модель квантового компьютера | Кількість кубітів | Статус |
|---|---|---|
| D-Wave Advantage_system 1.1 | 5760 | В наявності (online) |
| D-Wave DW_2000Q_6 | 2048 | В наявності (online) |
| Rigetti Aspen-8 | 31 | В наявності (online) |
| IonQ | 11 | В наявності (online) |

З таблиці 1.10 можна побачити, що D-Wave пропонує користувачам хмарні обчислення квантового комп’ютеру з кількістю кубітів 5760.

Опис квантового комп’ютеру D-Wave наведений в п. 1.4.

Вартість однієї операції квантового комп’ютеру D-Wave Advantage_system 1.1 з кількістю кубітів 5760 дорівнює 0,30$.

Якщо припустити, що в алгоритмі Шора [17] залежність від O ідеально відповідає кількості одиничних операцій (хоча найімовірніше одна ітерація буде включати кілька операцій), то при ціні 0,3 $ отримуємо на факторизацію RSA-2048 потрібно 2,5 мільярдів доларів, а на RSA-4096 – 20 мільярдів.

В тому чи іншому випадку розвиток квантових комп’ютерів досягає того етапу, коли вже доступні функції для зламу відомих шифрів, тому розробка квантово-захищених криптоалгоритмів є актуальної задачею на сьогоднішній день, а захист інформації в інформаційно-телекомунікаційних системах повинен здійснюватися з підвищеними вимогами.

# 2 БЛОКОВІ СИМЕТРИЧНІ ШИФРИ

## 2.1 ДСТУ 7624 «Калина»

### 2.1.1 Загальні відомості

Стандарт ДСТУ 7624:2014 розроблено у співпраці Держспецзв'язку та провідних українських науковців і враховує досвід та результати проведення міжнародних і відкритого національного конкурсу криптографічних алгоритмів. Він призначений для поступової заміни міждержавного стандарту ДСТУ ГОСТ 28147:2009.

Згідно чинних змін до наказу Держспецзв'язку від 20 серпня 2012 року №1236/5/453 після 1 січня 2022 року разом з функцією гешування Купина є обов'язковим для використання при накладанні та перевірці електронного підпису за ДСТУ 4145-2002 замість криптографічного перетворення за ДСТУ ГОСТ 28147:2009.[3]

### 2.1.2 Режими роботи шифру

У стандарті описані 10 режимів роботи криптографічного алгоритму [12] (табл. 2.1).

Таблиця. 2.1 – Режими роботи шифру ДСТУ 7624

| Назва режиму | Позначення | Послуга безпеки яку забезпечує даний режим |
|---|---|---|
| Проста заміна (базове перетворення) | ECB | Конфіденційність |
| Гамування | CTR | Конфіденційність |
| Гамування зі зворотним зв'язком за шифротекстом | CFB | Конфіденційність |
| Вироблення імітовставки | CMAC | Конфіденційність |
| Зчеплення шифроблоків | CBC | Конфіденційність |

Продовження таблиці 2.1

| | | |
|---|---|---|
| Гамування зі зворотним зв'язком за шифрогамою | OFB | Конфіденційність |
| Вибіркове гамування із прискореним виробленням імітовставки | GCM, GMAC | Конфіденційність і цілісність (GCM), тільки цілісність (GMAC) |
| Вироблення імітовставки і гамування | CCM | Конфіденційність і цілісність |
| Індексована заміна | XTS | Конфіденційність |
| Захист ключових даних | KW | Конфіденційність і цілісність |

2.1.3 Загальні параметри шифру

Стан шифру описується матрицею 8*с елементів скінченного розширеного двійкового поля GF($2^8$) сформованого незвідним поліномом $x^8+x^4+x^3+x^2+1$.Кількість раундів та кількість рядків у матриці стану наведені у табл. 2.2.

Таблиця 2.2 – Загальні параметри шифру ДСТУ 7624

| № | Розмір блоку | Розмір ключа | Кількість раундів | Рядків у матриці стану |
|---|---|---|---|---|
| 1 | 128 | 128 | 10 | 2 |
| 2 | | 256 | 14 | |
| 3 | 256 | 256 | 14 | 4 |
| 4 | | 512 | 18 | |
| 5 | 512 | 512 | 18 | 8 |

## 2.2 AES

### 2.2.1 Загальні відомості

Advanced Encryption Standard (AES) [18], також відомий під назвою Rijndael — симетричний алгоритм блочного шифрування (розмір блока 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий як американський стандарт шифрування урядом США. Вибір припав на AES з розрахуванням на широке використання і активний аналіз алгоритму, як це було із його попередником, DES. Державний інститут стандартів і технологій (англ. National Institute of Standards and Technology, NIST) США опублікував попередню специфікацію AES 26 жовтня 2001 року, після п'ятилітньої підготовки. 26 травня 2002 року AES оголошено стандартом шифрування. Станом на 2009 рік AES є одним із найпоширеніших алгоритмів симетричного шифрування.

Підтримка прискорення AES була введена фірмою Intel в сімейство процесорів x86 починаючи з Arrandale в 2010 році, а потім на процесорах Sandy Bridge; фірмою AMD - в Bulldozer з 2011[4][5][6].

### 2.2.2 Загальні параметри шифру

AES підтримує широкий діапазон розміру блоку та ключа. AES має фіксовану довжину у 128 біт, а розмір ключа може приймати значення 128, 192 або 256 біт. Через фіксований розмір блоку AES оперує із масивом 4×4 байт, що називається станом (версії алгоритму із більшим розміром блоку мають додаткові колонки).

Для ключа 128 біт алгоритм має 10 раундів у яких послідовно виконуються операції:

- subBytes();
- shiftRows();
- mixcolumns() (у 10-му раунді пропускається);
- xorRoundKey();

Розмір ключа: 128/192/256 біт

Розмір блоку: 128 біт

Число раундів: 10/12/14

## 2.3 Twofish

### 2.3.1 Загальні відомості

Симетричний алгоритм блочного шифрування з розміром блоку 128 біт і довжиною ключа до 256 біт. Число раундів 16. Розроблено групою фахівців на чолі з Брюсом Шнайером. Був одним з п'яти фіналістів другого етапу конкурсу AES. Алгоритм розроблений на основі алгоритмів Blowfish, SAFER і Square.

Відмінними особливостями алгоритму є використання попередньо обчислюваних та залежних від ключа S-box'ів і складна схема розгортки підключення шифрування. Половина n-бітного ключа шифрування використовується як власне ключ шифрування, інша — для модифікації алгоритму (від неї залежать S-box'и) [7].

### 2.3.2 Загальні параметри шифру

Алгоритм Twofish виник в результаті спроби модифіковані алгоритм Blowfish для 128-бітового вхідного блоку. Новий алгоритм повинен був бути легко реалізованим апаратно (у тому числі використовувати таблиці меншого розміру), мати досконалішу систему розширення ключа (key schedule) і мати однозначну функцію F. В результаті, алгоритм був реалізований у вигляді змішаної мережі Фейстеля з чотирма гілками, які модифікують один одну з використанням криптоперетворень Адамара.

Довжина ключів 128, 192 і 256 біт, довжина блоку 128біт. Відсутність слабких ключів. Ефективна програмна (в першу чергу на 32-бітних процесорах) та апаратна реалізація. Гнучкість (можливість використання додаткових довжин ключа, використання в поточному шифруванні, хеш-функціях і т. д.). Простота алгоритму - для можливості його ефективного аналізу. Кількість раундів 16.

## 2.4 RC6

### 2.4.1 Загальні відомості

RC6 — симетричний блоковий криптографічний алгоритм, похідний від алгоритму RC5. Був створений Роном Рівестом, Меттом Робшау і Реєм Сіднеєм для задоволення вимог конкурсу Advanced Encryption Standard (AES). Алгоритм був одним з п'яти фіналістів конкурсу, був також представлений NESSIE і CRYPTREC. Є власницьким (пропрієтарним) алгоритмом, і запатентований RSA Security.

Є фіналістом AES, проте одна з примітивних операцій — операція множення, повільно виконується на певному обладнанні і ускладнює реалізацію шифру на ряді апаратних платформ і, що виявилося сюрпризом для авторів, на системах з архітектурою Intel IA-64 також реалізована досить погано. В даному випадку алгоритм втрачає одну зі своїх ключових переваг — високу швидкість виконання, що стало причиною для критики і однією з перепон для обрання як нового стандарту. Однак, на системах із процесором Pentium II, Pentium Pro, Pentium III, PowerPC та ARM алгоритм RC6 випереджає переможця — Rijndael [8].

### 2.4.2 Загальні параметри шифру

Варіант шифру RC6, заявлений на конкурс AES, підтримує блоки довжиною 128 біт і ключі довжиною 128, 192 і 256 біт, але сам алгоритм, як і RC5, може бути налаштований для підтримки більш широкого діапазону довжин як блоків, так і ключів (від 0 до 2040 біт). RC6 дуже схожий на RC5 за своєю структурою і також досить простий у реалізації. Кількість раундів шифру 12/14/15.

## 2.5 MARS

### 2.5.1 Загальні відомості

MARS — шифр-кандидат в AES, розроблений корпорацією IBM, яка створила у свій час DES. За заявою IBM, в алгоритм MARS вкладено 25-річний криптоаналітичний досвід фірми, і поряд з високою криптографічною стійкістю шифр допускає ефективну реалізацію навіть в таких обмежених рамках, які характерні для смарт-карт.

У розробці шифру взяв участь Дон Копперсміт, один з авторів шифру Lucifer (DES), відомий низкою статей по криптології: поліпшення структури S-блоків проти диференціального криптоаналізу, метод швидкого перемножування матриць (алгоритм Копперсміта — Винограду), криптоаналіз RSA. Крім нього в розробці алгоритму взяли участь: Керолін Барвік, Едвард Д'Евіньон, Росаріо Женаро, Шай Халеві, Чаранжіт Джутла, Стівен М. Матьяс Мол., Люк О'Коннор, Мохамед Пер'євян, Девід Саффорд, Невенко Зуніч.

За правилами конкурсу AES, учасники могли вносити незначні зміни у свої алгоритми. Скориставшись цим правилом, автори MARSa змінили процедуру розширення ключа, що дозволило знизити вимоги до енергонезалежної і оперативної пам'яті. Нижче буде надана модифікована версія алгоритму[9].

За результатами конкурсу AES, MARS вийшов у фінал, але поступився Rijndael.

### 2.5.2 Загальні параметри шифру

MARS є блочно-симетричним шифром з відкритим ключем. Розмір блоку при шифруванні 128 біта, розмір ключа може варіюватися від 128 до 448 біт включно (кратні 32 бітам). Творці прагнули поєднати в своєму алгоритмі швидкість кодування і стійкість шифру. В результаті вийшов один з самих криптостійкий алгоритм з алгоритмів, які брали участь в конкурсі AES.

Алгоритм унікальний тим, що використовував практично всі існуючі технології, застосовувані в криптоалгоритмах, а саме:

– найпростіші операції (додавання, віднімання, виключаюче або)

– підстановки з використанням таблиці замін

– фіксований циклічний зсув

– залежний від даних циклічний зсув

– множення по модулю 2 32

– ключове забілювання

– використання подвійного перемішування представляє складність для криптоаналіз а, що деякі відносять до недоліків алгоритму. У той же час на даний момент не існує будь-яких ефективних атак на алгоритм, хоча деякі ключі можуть генерувати слабкі підключі.

Розмір ключа: 128-448 біт

Розмір блоку: 128 біт

Число раундів: 32

# 3 ПОРЯДОК ТА ПРОГРАМА ДЛЯ ТЕСТУВАННЯ БСШ

## 3.1 Бібліотека Crypto++

Для тестування швидкодії була обрана популярна крипто-бібліотека Crypto++.

Crypto ++ (також відома як CryptoPP, libcrypto ++ і libcryptopp) – це безкоштовна бібліотека C ++ з відкритим вихідним кодом криптографічних алгоритмів і схем, написана китайським комп'ютерним інженером Вей Даємо. Будучи випущеною в 1995, бібліотека повністю підтримує 32-розрядні і 64-розрядні архітектури для багатьох операційних систем і платформ, таких як Android (з використанням STLport), Apple (Mac OS X і iOS), BSD, Cygwin, IBM AIX і S / 390, Linux, MinGW, Solaris, Windows,Windows Phone і Windows RT. Проект також підтримує компіляцію з використанням бібліотек різних середовищ виконання C ++ 03, C ++ 11 і C ++ 17; і безліч інших компіляторів і IDE, що включають в себе Borland Turbo C ++, Borland C ++ Builder, Clang, CodeWarrior Pro, GCC (з використанням GCC від Apple), Intel C ++ Compiler (ICC), Microsoft Visual C / C ++.

Crypto ++ зазвичай надає повні криптографічні реалізації. Наприклад, блоковий шифр Camellia, затверджений ISO / NESSIE / IETF, практично схожий з AES, хеш-функція Whirlpool, також підтверджена вищевказаними організаціями, схожа з SHA; обидва алгоритмаа включені в дану бібліотеку.

Варто додати, що бібліотека Crypto ++ іноді робить пропоновані і новітні алгоритми доступними для вивчення криптографічною спільнотою. Наприклад, VMAC, універсальний геш-базований код аутентифікації повідомлень, був доданий в ході її представлення Інженерній раді Інтернету; криві Брейнпула, запропоновані в березні 2009 року в якості інтернет-проекту в RFC 5639, були додані в Crypto ++ 5.6.0 в цьому ж місяці [10].

Список всіх алгоритмів, які підтримує бібліотека представлено в таблиці 3.1.

Таблиця 3.1 – Список алгоритмів Crypto++

| Примітив чи операція | Алгоритми чи реалізації |
|---|---|
| Генератори псевдовипадкових чисел | LCG, KDF2, Blum Blum Shub, ANSI X9.17, Mersenne Twister, RDRAND and RDSEED |
| Швидкі потокові шифри | ChaCha8/12/20, HC-128 и HC-256, Panama, Rabbit, Salsa20, SOSEMANUK, XSalsa20 |
| AES та кандидати AES | Rijndael (AES), RC6, MARS, Twofish, Serpent, CAST-256 |
| Інші блокові шифри | ARIA, Blowfish, Camellia, CHAM, HIGHT, IDEA, Kalyna (128/256/512), LEA, RC5,SEED, SHACAL-2, Simon и Speck (64/128), SIMECK, Skipjack, SM4, TEA, Threefish (256/512/1024), XTEA |
| Способи блокового шифрування | ECB, CBC, CTS, CFB, OFB, CTR |
| Режими шифрування з перевіркою достовірності | CCM, GCM, EAX |
| Схеми заповнення бокових шифрів | PKCS#5, PKCS#7, Zeros, One and zeros, W3C Padding |
| Коди автентифікації повідомлень | VMAC, HMAC, CMAC, CBC-MAC, DMAC, Two-Track-MAC |
| Криптографічна хеш-функція | BLAKE2 (BLAKE2b и BLAKE2s), Keccak, SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, и SHA-512), SHA3, Tiger, WHIRLPOOL, RIPEMD(RIPEMD-128, RIPEMD-160, RIPEMD-256, и RIPEMD-320) |

Продовження таблиці 3.1

| | |
|---|---|
| Паролезалежний KDF | PBKDF1 і PBKDF2 від PKCS #5, PBKDF від PKCS #12 appendix B |
| Криптографія з відкритим ключем | RSA, DSA, ElGamal, Nyberg-Rueppel (NR), Rabin-Williams (RW), LUC, LUCELG, DLIES (варіанти DHAES), ESIGN, curve25519 |
| Схеми заповнення для систем з відкритим ключем | PKCS#1 v2.0, OAEP, PSS, PSSR, IEEE P1363 EMSA2 і EMSA5 |
| Криптографія на еліптичних кривих | ECDSA, ECNR, ECIES, ECDH, ECMQV |

## 3.2 Загальний опис програми тестування

Програма була написана на мові програмування C++, та має назву Calyna.exe. Для роботи програми необхідна ОС Windows 10. Програма має зовнішні залежності (Crypto++). Програма здійснює шифрування, дешифрування та замір часу. Оскільки метою роботи не було написання ПЗ, параметри вибору шифру, файлу та черговість тестування змінюються безпосередньо в тілі функції main().

## 3.3 Архітектура програми для тестування

Програма складається з наступних файлів:

– main.cpp – файл з функцією входу main();

– core.h – заголовочний файл з реалізацією віртуального класу core, який описує загальні функції для тестування всіх БСШ;

– TestAES.h – заголовочний файл класу TestAES;

– TestAES.cpp – файл реалізації класу TestAES;

– Kalyna.h – заголовочний файл класу Kalyna;

– Kalyna.cpp – файл реалізації класу Kalyna;

– TestMARS.h – заголовочний файл класу TestMARS;

– TestMARS.cpp – файл реалізації класу TestMARS;

– TestRC6.h – заголовочний файл класу TestMARS;

– TestRC6.cpp – файл реалізації класу TestRC6;

– TestTwofish.h – заголовочний файл класу TestTwofish;

– TestTwofish.cpp – файл реалізації класу TestTwofish.

В програмі існують наступні класи:

– core – віртуальний клас в якому описано загальну функцію для тестування та об’явлені зміні та прототипи функцій;

– TestAES – клас для тестування БСШ AES, унаслідується від core;

– Kalyna – клас для тестування БСШ Kalyna-128, унаслідується від core;

– TestMARS – клас для тестування БСШ MARS, унаслідується від core;

– TestRC6 – клас для тестування БСШ RC6, унаслідується від core;

– TestTwofish – клас для тестування БСШ Twofish, унаслідується від core.

## 3.4 Порядок тестування

Для тестування були обрані наступні шифри Kalyna 128, AES, Twofish, RC6, MARS.

Всі шифри були протестовані на найменших параметрах ключів (MIN_KEYLENGTH), на однакових ключах та векторі ініціалізації («12345»). Для тестування створені файли розміром 64КБ, 1МБ, 4МБ, 8МБ, 16МБ. Кожний файл складався з символу «c».

Тестування здійснювалося для кожного БСШ шляхом десятикратного виміру швидкості зашифрування окремого файлу. Після тестування зашифрування для окремого файлу здійснювався перезапуск програми та наступне тестування. Перезапуск програми необхідний для зменшення впливу кешу ЦП.

Під час тестування здійснювалося й дешифрування для перевірки коректності, проте дані дешифрування не оцінювалися.

Виміру підлягали найменше, середнє та найбільше значення часу за тест.

# 4 ТЕСТУВАННЯ ШВИДКОДІЇ БСШ

## 4.1 Програмне та апаратне забезпечення тестування

Програмне та апаратне забезпечення за допомогою якого здійснювалося тестування відображено в таблиці 4.1.

Таблиця 4.1 – Програмне та апаратне забезпечення

| Тип | Повна назва | Характеристики |
|---|---|---|
| ОС | Windows 10 Pro | Версія 1909 |
| Середовище розробки | Visual Studio Community | Версія 16.6.30204.135 |
| Криптобібліотека | Crypto++ | Версія 8.20 |
| Допоміжні бібліотеки | Windows SDK | Версія 10.0 |
| ЦП | AMD Ryzen 5 1600 | 3.2 GHz, 6 ядер 12 потоків, кеш 576КБ/3МБ/16МБ |
| ОЗП | Kingston | 16 В, DDR-3 |

## 4.2 Результати тестування

Результати тестування яке було здійснено згідно з п.2.4 та відображено в таблицях 4.2 – 4.6

Таблиця 4.2 – Тестування швидкодії AES

| Розмір файлу(MB) | AES | | |
|---|---|---|---|
| | mix | mid | max |
| 0.064 | 0.001 | 0.001 | 0.0001 |
| 1 | 0.007 | 0.0082 | 0.009 |
| 4 | 0.033 | 0.0336 | 0.034 |

Продовження таблиці 4.2

| | | | |
|---|---|---|---|
| 8 | 0.067 | 0.0686 | 0.076 |
| 16 | 0.133 | 0.1359 | 0.138 |

Таблиця 4.3 – Тестування швидкодії Kalyna-128

| Розмір файлу(MB) | Kalyna-128 | | |
|---|---|---|---|
| | mix | mid | max |
| 0.064 | 0.038 | 0.004 | 0.043 |
| 1 | 0.069 | 0.0697 | 0.071 |
| 4 | 0.276 | 0.2784 | 0.28 |
| 8 | 0.554 | 0.5562 | 0.56 |
| 16 | 1.01 | 1.048 | 1.06 |

Таблиця 4.4 – Тестування швидкодії Twofish

| Розмір файлу(MB) | Twofish | | |
|---|---|---|---|
| | mix | mid | max |
| 0.064 | 0.0075 | 0.008 | 0.0086 |
| 1 | 0.129 | 0.1302 | 0.132 |
| 4 | 0.52 | 0.5215 | 0.524 |
| 8 | 1.032 | 1.0422 | 1.051 |
| 16 | 2.007 | 2.079 | 2.121 |

Таблиця 4.5 – Тестування швидкодії RC6

| Розмір файлу(MB) | RC6 | | |
|---|---|---|---|
| | mix | mid | max |
| 0.064 | 0.0085 | 0.009 | 0.0093 |
| 1 | 0.14 | 0.1417 | 0.1443 |
| 4 | 0.567 | 0.5687 | 0.572 |
| 8 | 1.124 | 1.1439 | 1.166 |

Продовження таблиці 4.5

| | | | |
|---|---|---|---|
| 16 | 2.235 | 2.252 | 2.361 |

Таблиця 4.6 – Тестування швидкодії MARS

| Розмір файлу(MB) | MARS | | |
|---|---|---|---|
| | mix | mid | max |
| 0.064 | 0.011 | 0.013 | 0.014 |
| 1 | 0.212 | 0.2153 | 0.219 |
| 4 | 0.85 | 0.8611 | 0.865 |
| 8 | 1.709 | 1.7268 | 1.753 |
| 16 | 3.3 | 3.44 | 3.52 |

Середні значення часу для кожного алгоритму в залежності від розміру файлу відображенні на рис 4.1.

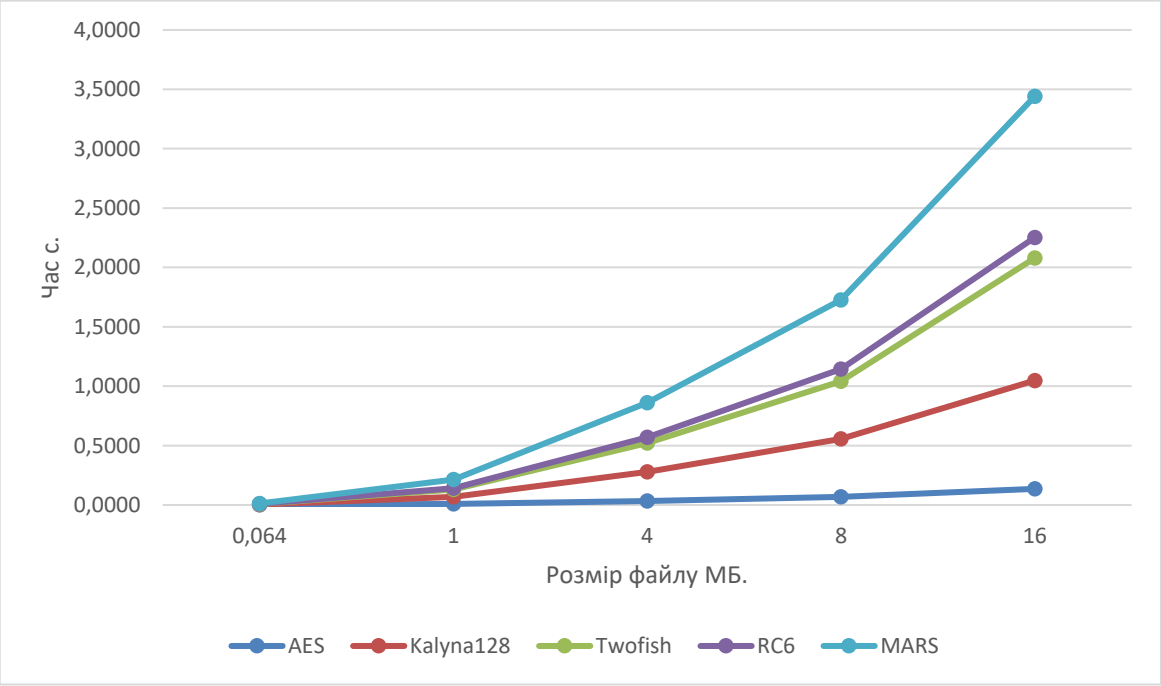


Рисунок 4.1 – Графік середніх значень швидкодії

## 4.3 Висновки та обґрунтування вибору алгоритму для реалізації захищеного з’єднання

Під час проведення досліджень була написана програма (опис програми п. 3.2) за допомогою якої було здійснено тестування (п. 3.4). Під час проведення випробувань встановлено, що БСШ AES є найшвидшим майже на всіх протестованих файлах, швидкодія більша в декілька разів(в деяких випадках до 30). Калина-128 займає друге місце, Twofish, RC6, MARS – третє, четверте та п’яте відповідно. Такі результати пояснюються тим, що сучасні процесори мають апаратну підтримку AES.

Калина випереджає аналогічні шифри в швидкодії, якщо ті не мають апаратної підтримки (як AES) та має стійкість до квантових атак завдяки підтримки ключа розміром 512 біт.

Завдяки захищеності від квантових атак шифр «Калина» було обрано для реалізації програмного забезпечення захисту IP-пакетів.

# 5 ОПИС ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ МЕРЕЖНИХ З’ЄДНАНЬ

## 5.1 Загальна інформація

Розроблене ПЗ має назву "Secure_Connect". Для функціонування ПЗ необхідна ОС Windows та встановлені бібліотеки Net Framework. ПЗ складається з виконуємого файлу "Secure_Connect.exe". Розмір файлу 30208 байт. Під час робот програма використовує 80 Мб оперативного простору та до 1% ресурсів ЦП. Програма є портативною та не потребує встановлення для запуску.

Функції програми: передача зашифрованих повідомлень між ПЕОМ.

Вихідними файлами є:

– MainWindow.xaml.cs – головний файл з реалізацію не криптографічних функцій;

– MainWindow.xaml – файл розмітки головного вікна;

– pass entr.xaml.cs – файл з реалізацію вікна введення паролю;

– pass entr.xaml – файл розмітки вікна введення паролю;

– Kalyna.cs – файл з реалізацією функцій шифрування.

Програма протестована на ПЕОМ що мають характеристики приведені в таблицях 5.1 та 5.2.

Таблиця 5.1 – Технічні характеристики клієнту ПЕОМ №1

| Компонент | Назва/характеристики |
|---|---|
| Центральний процесор | AMD Ryzen 5 1600 (3.2 GHz) |
| ОЗП | 16 GB |
| Відеоадаптер | Radeon RX 590 |
| Запам’ятовуючий пристрій | Toshiba HDWD110 |

Продовження таблиці 5.1

| | |
|---|---|
| ОС | Windows 10 build 2004 |
| Net Framework | v4.0.30319 |

Таблиця 5.2 – Технічні характеристики клієнту ПЕОМ №2

| Компонент | Назва/характеристики |
|---|---|
| Центральний процесор | Intel Core i5-8265U(1.6 GHz) |
| ОЗП | 8 GB |
| Відеоадаптер | Nvidia GeForce MX130 |
| Запам’ятовуючий пристрій | Toshiba MQ04ABF100 |
| ОС | Windows 10 build 1909 |
| Net Framework | v4.0.30319 |

## 5.2 Інструкція користувача

### 5.2.1 Запуск

Необхідно скопіювати виконуємий файл Secure_Connect.exe в будь-яку директорію та запустити його шляхом подвійного натискання лівої клавіші миші (рис 5.1).


Рисунок 5.1 – Виконуємий файл програми

Після цього відкриється головне вікно програми (рис 5.2)

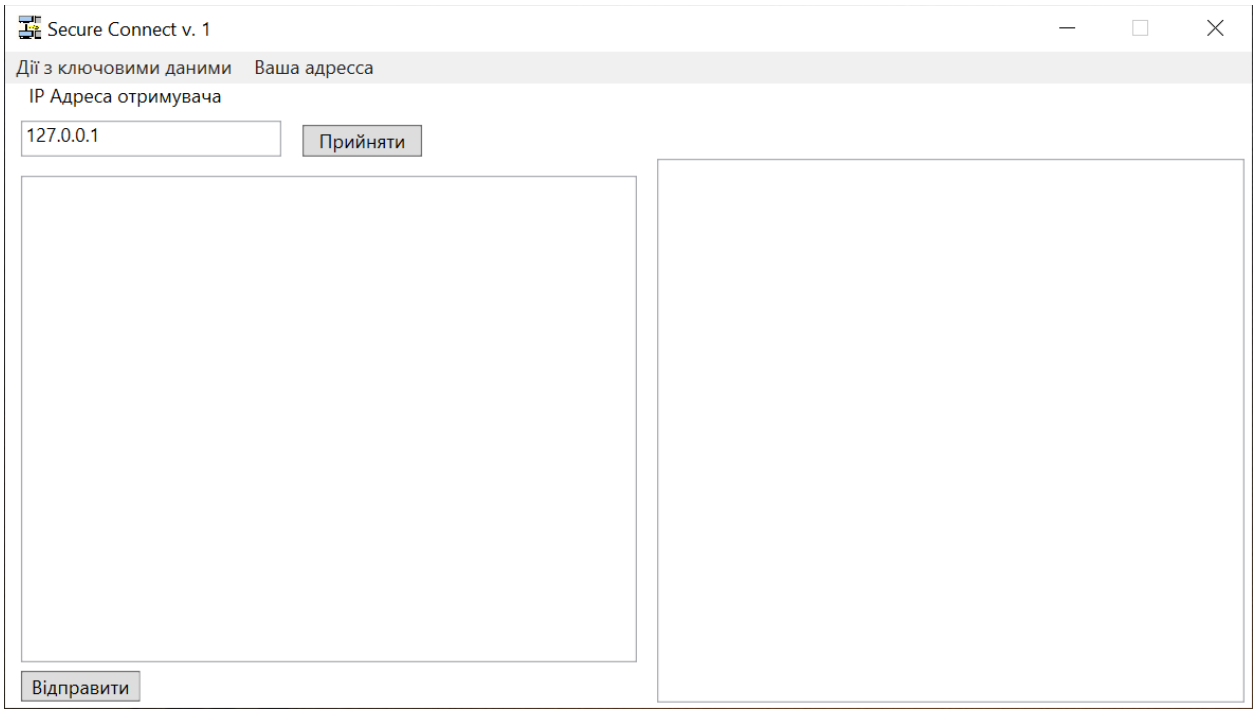


Рисунок 5.2 – головне вікно програми

### 5.2.2 Генерація ключових даних

Для генерації ключових даних слід відкрити головне меню програми та натиснути «Дії з ключовими даними» та «Згенерувати» (рис 5.3).

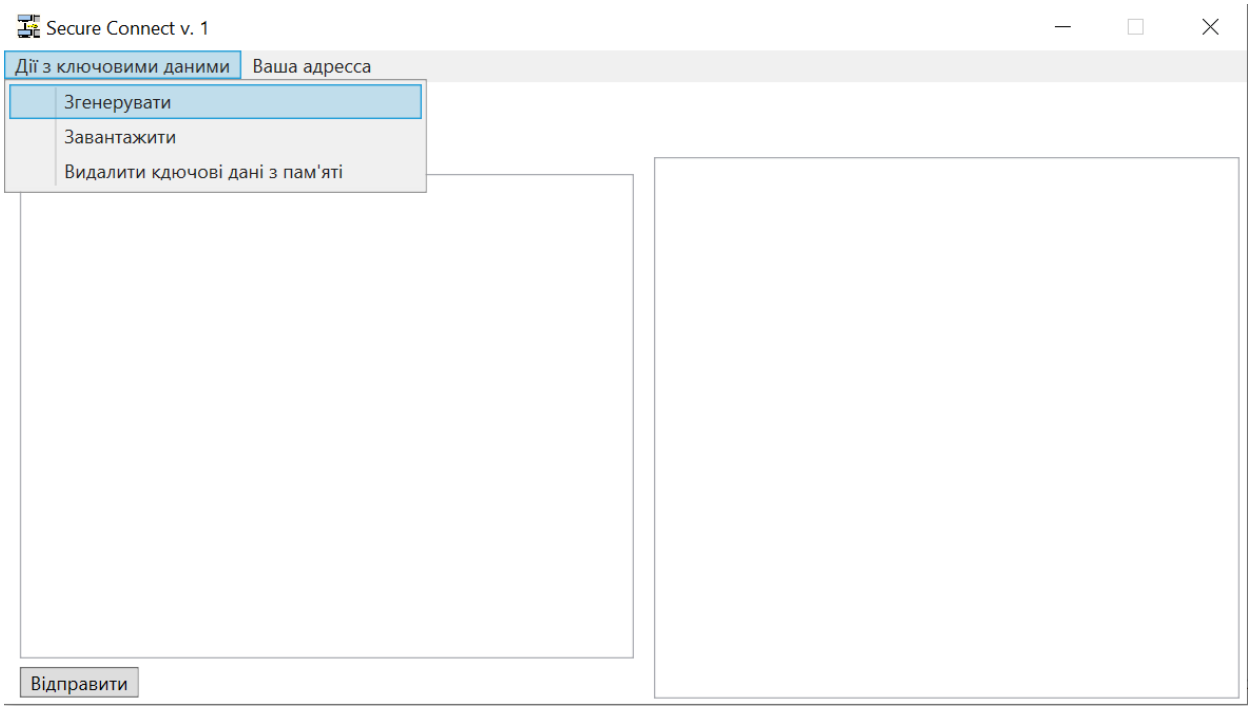


Рисунок 5.3 – «Дії з ключовими даними – Згенерувати»

Після цього з’явиться вікно в якому слід ввести вигаданий пароль до НКІ (рис 5.4).

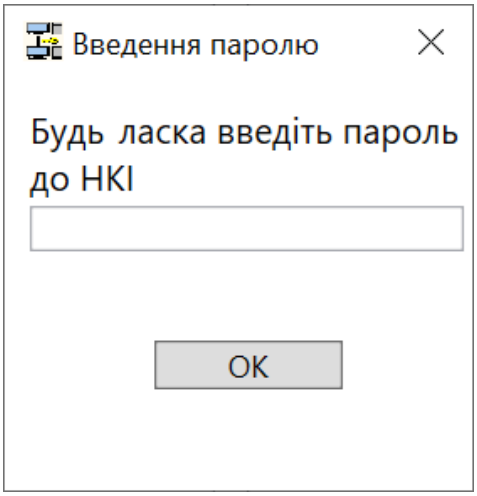


Рисунок 5.4 – Вікно введення паролю

Після введення паролю слід натиснути «ОК» (рис. 5.5).

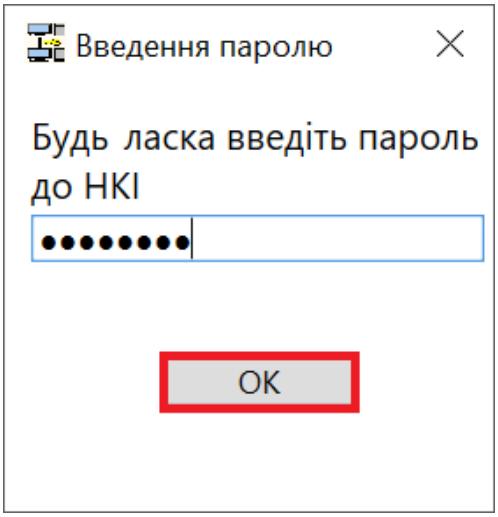


Рисунок 5.5 – Підтвердження паролю

Після підтвердження з’явиться повідомлення, яке зображено на рис. 5.6 .

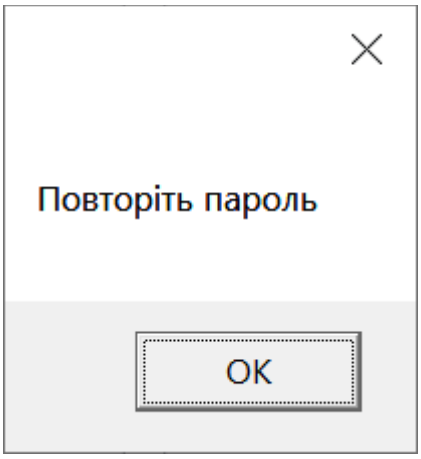


Рисунок 5.6 – Повідомлення після підтвердження паролю

Слід натиснути «ОК», та повторити введення паролю (рис. 5.4 та рис 5.5).

Якщо паролі не співпадають то з’явиться повідомлення яке зображено на рис. 5.7. Після натискання «Ок» програма перейде до початкового стану (рис 5.2).

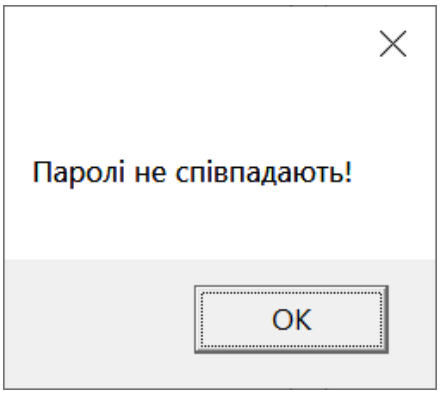


Рисунок 5.7 – Повідомлення при відмінності паролів

Якщо паролі співпадають то відкриється провідник, в якому слід вибрати директорію та дати назву файлу (рис. 5.8).

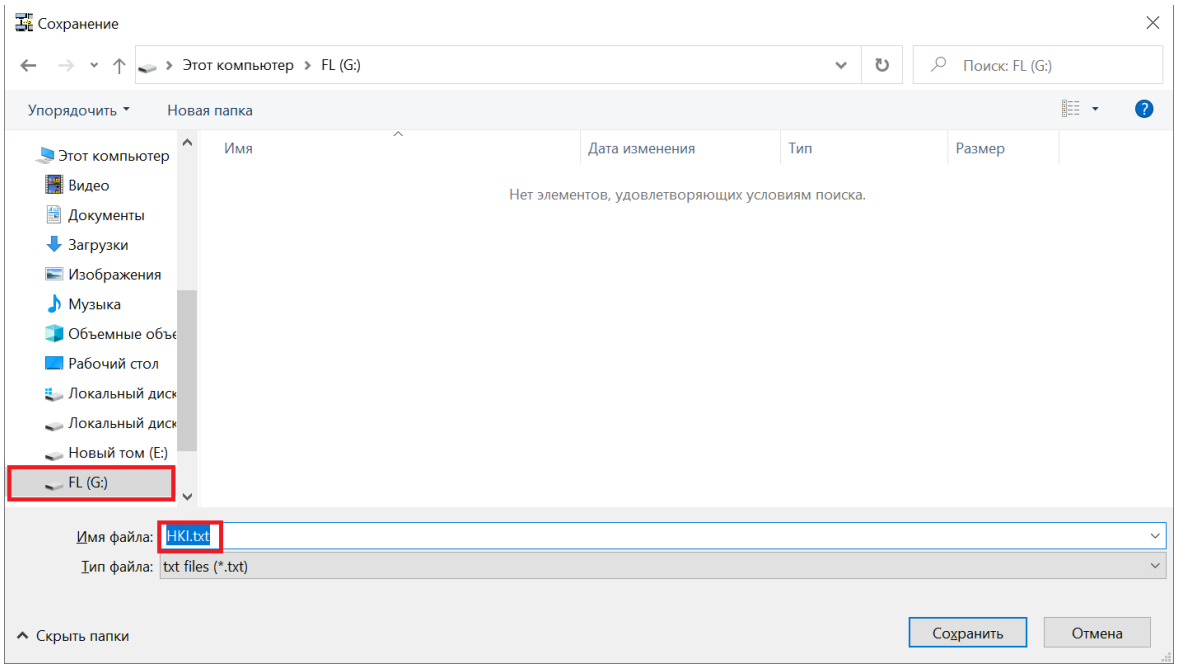


Рисунок 5.8 – Вибір директорії та назви файлу

Натиснути «Сохранить» (рис 5.9).

Примітка: в залежності від вибраної мови системи Windows дана кнопка може мати аналогічну назву на іншій мові, таку як «Зберегти» або «Save».

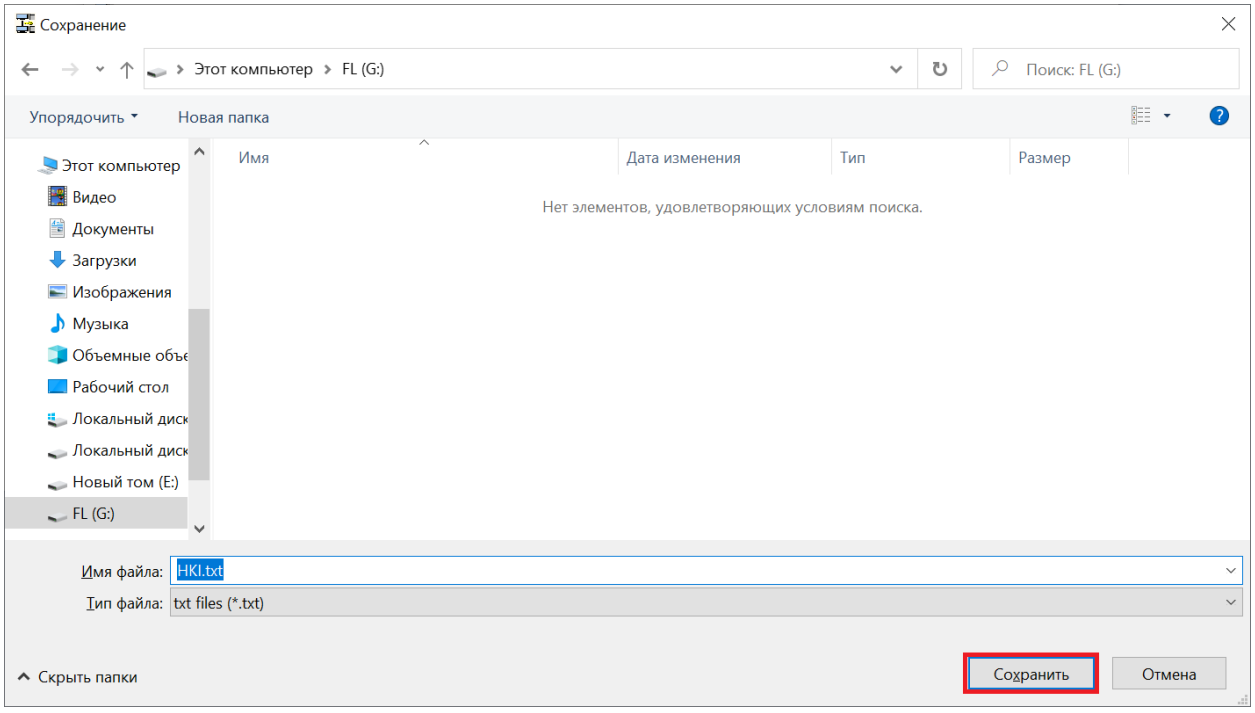


Рисунок 5.9 – Збереження HKI

Після цього НКІ буде збережено та програма повернеться до початкового стану (рис. 5.2).

НКІ має вигляд зашифрованого текстового файлу (рис. 5.10.)

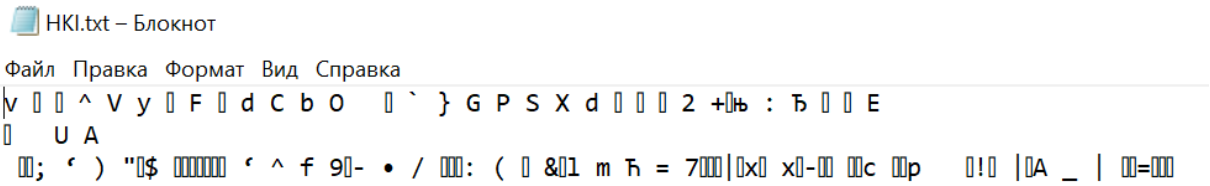


Рисунок 5.10 – Вигляд НКІ

5.2.3 Завантаження НКІ

Для прийому та відправлення повідомлень необхідно перед початком роботи завантажити НКІ. Якщо НКІ не завантажено то повідомлення не будуть приходити до користувача, та користувач не зможе відправити повідомлення. При спробі відправлення повідомлення з’явиться вікно про помилку (рис. 5.11).

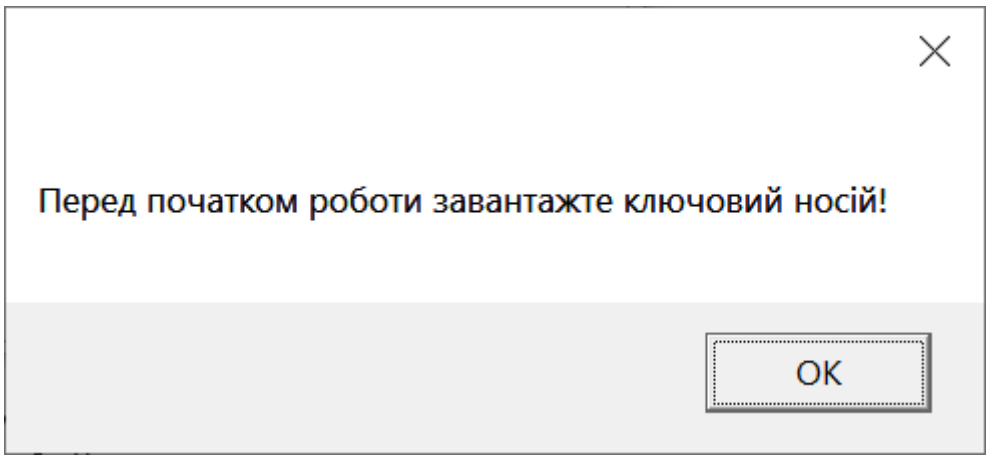


Рисунок 5.11 – Повідомлення про відсутність ключового носія

Для завантаження НКІ слід вибрати пункт «Дії з ключовими даними-Завантажити» (рис. 5.12).

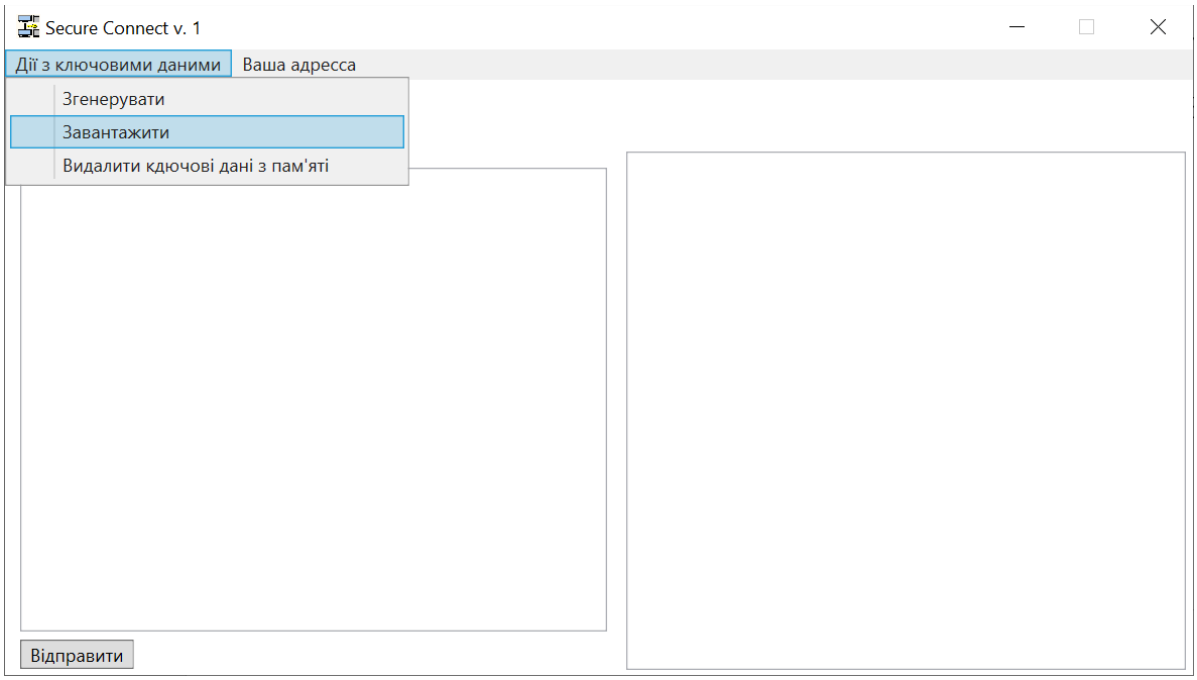


Рисунок 5.12 – Пункт «Дії з ключовими даними-Завантажити»

Після цього слід вибрати файл з НКІ та натиснути «Открыть» (рис. 5.13).

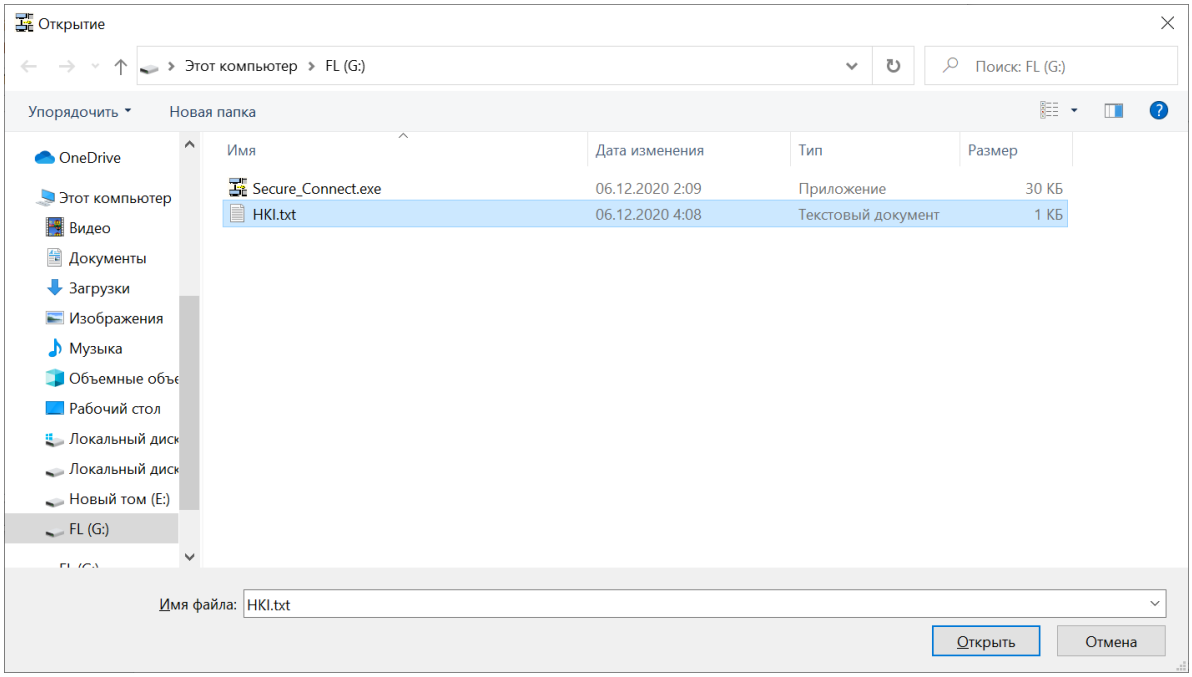


Рисунок 5.13 – Завантаження НКІ

Після цього слід ввести пароль до НКІ та натиснути «ОК» (рис 5.14).

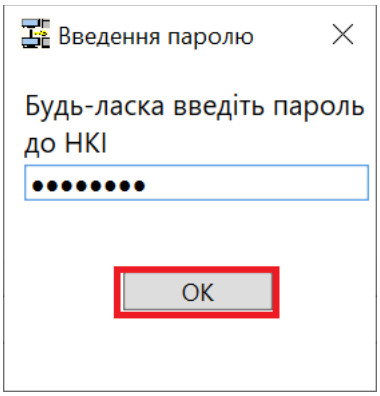


Рисунок 5.14 – Введення паролю до НКІ

Якщо пароль введено вірно то з’явиться повідомлення, яке зображено на рисунку 5.15.

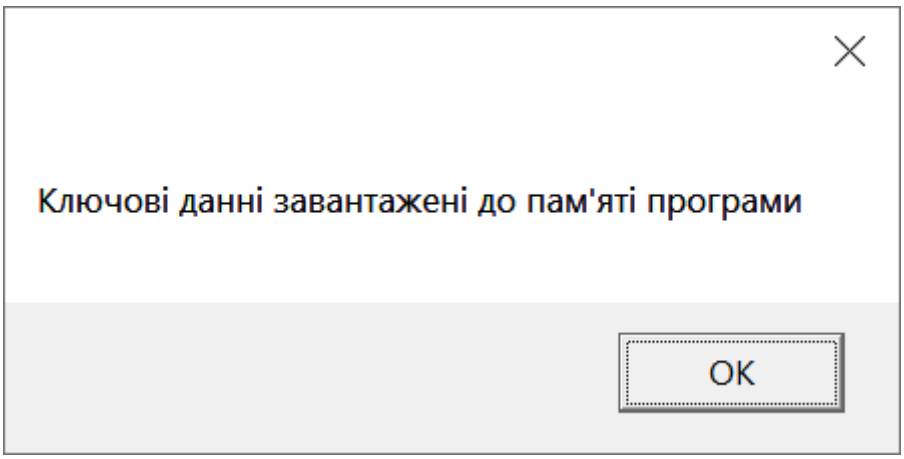


Рисунок 5.15 – повідомлення про успішне завантаження НКІ

Якщо пароль введено не вірно з’явиться повідомлення, яке зображено на рисунку 5.16.

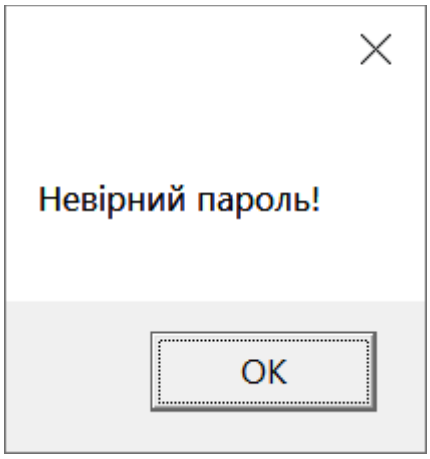


Рисунок 5.16 – Повідомлення  про невірний пароль

5.2.4 Видалення НКІ з пам’яті програми

Для видалення НКІ з пам’яті програми необхідно вибрати пункт «Дії з ключовими даними – Видалити ключові дані з пам’яті» (рис 5.17).

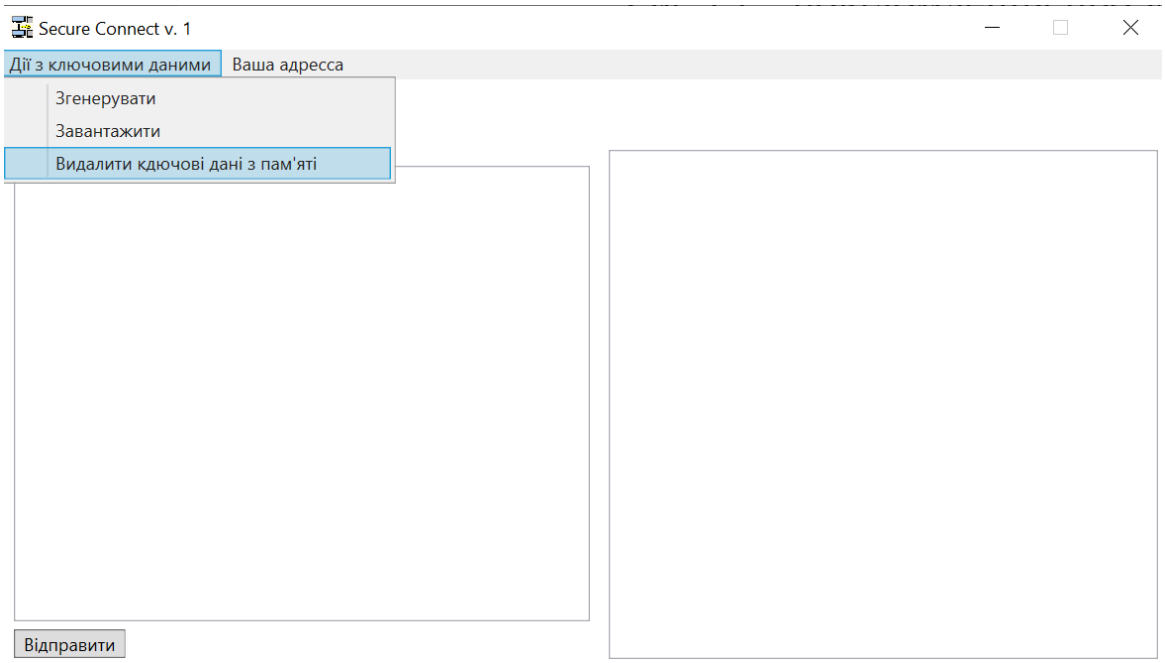


Рисунок 5.17 – Пункт «Дії з ключовими даними – Видалити ключові дані з пам’яті»

Після цього з’явиться повідомлення про видалення ключових даних (рис 5.18).

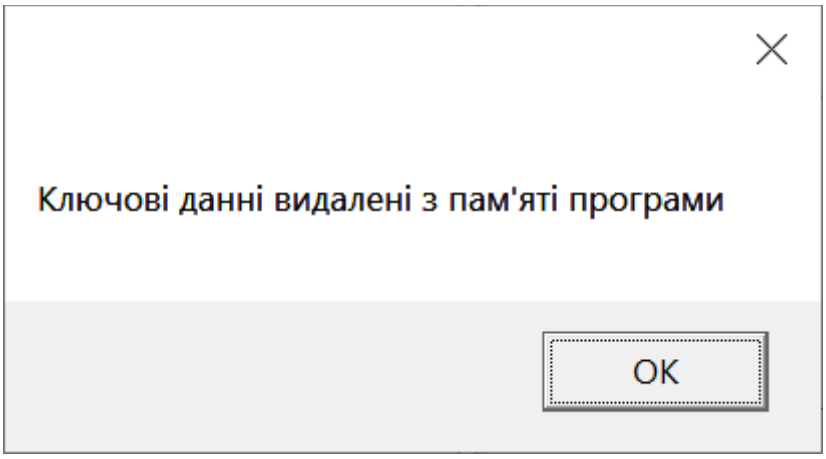


Рисунок 5.18 – Повідомлення про видалення ключових даних

5.2.5 Відправлення та отримання повідомлень

Для відправлення повідомлення необхідно завантажити НКІ (п. 5.2.3) та ввести адресу отримувача  та натиснути «Прийняти» (рис. 5.19).

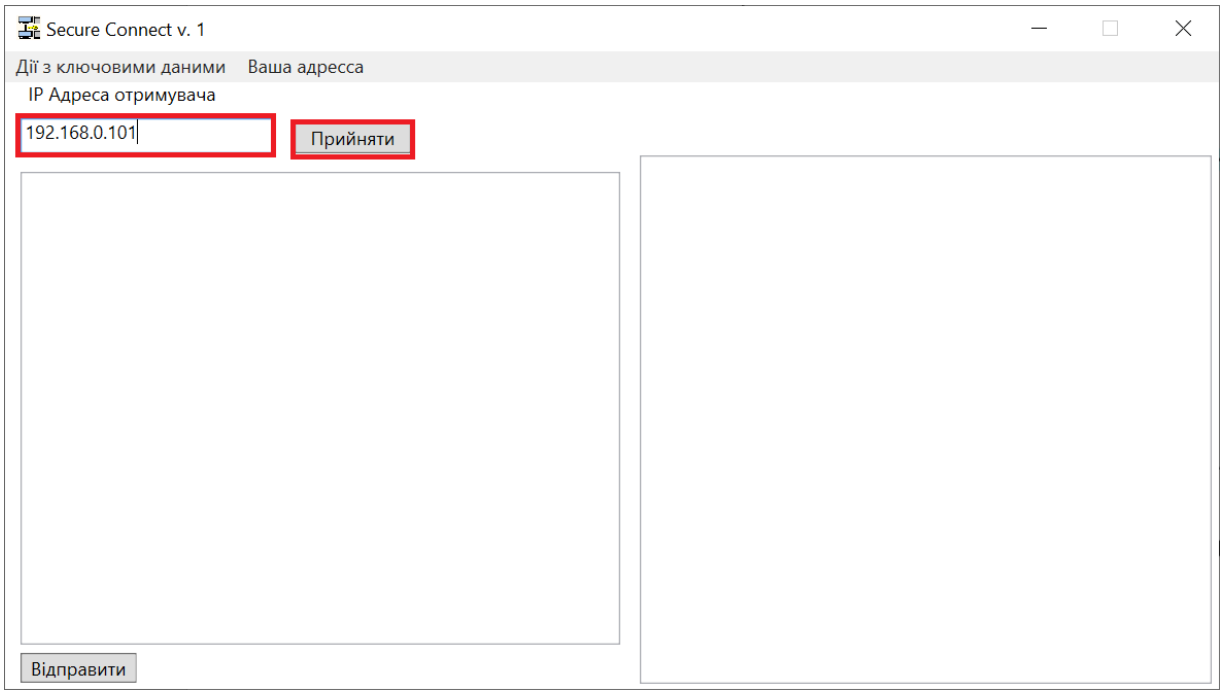


Рисунок 5.19 – Введення адреси отримувача

Після цього з’явиться повідомлення про зміну адреси отримувача (рис. 5. 20).

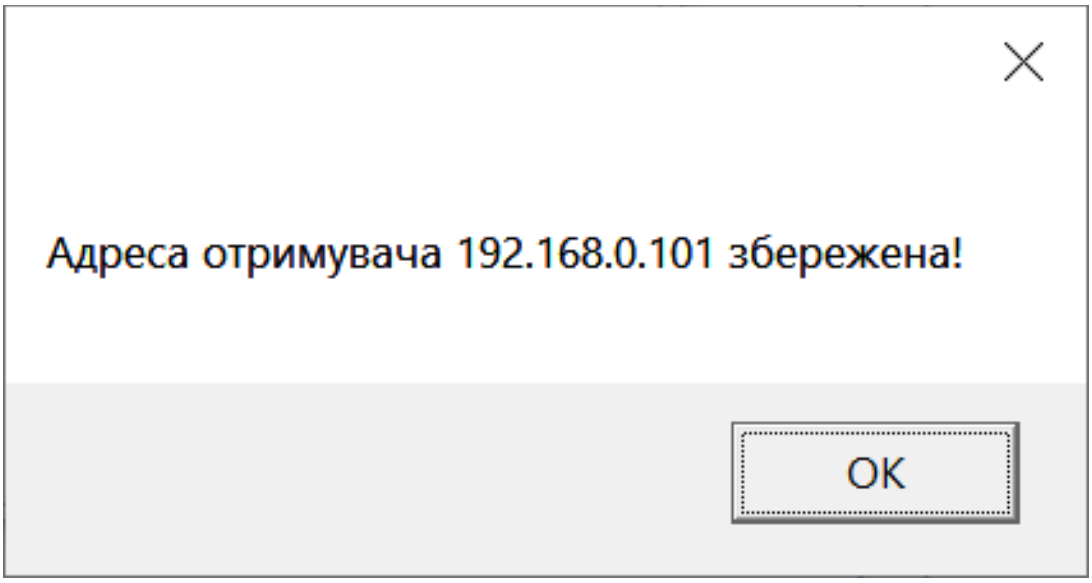


Рисунок 5.20 – Повідомлення про зміну адреси отримувача

Далі необхідно ввести повідомлення в поле, яке зображено на рисунку 5.21 та натиснути «Відправити» (рис 5.22).

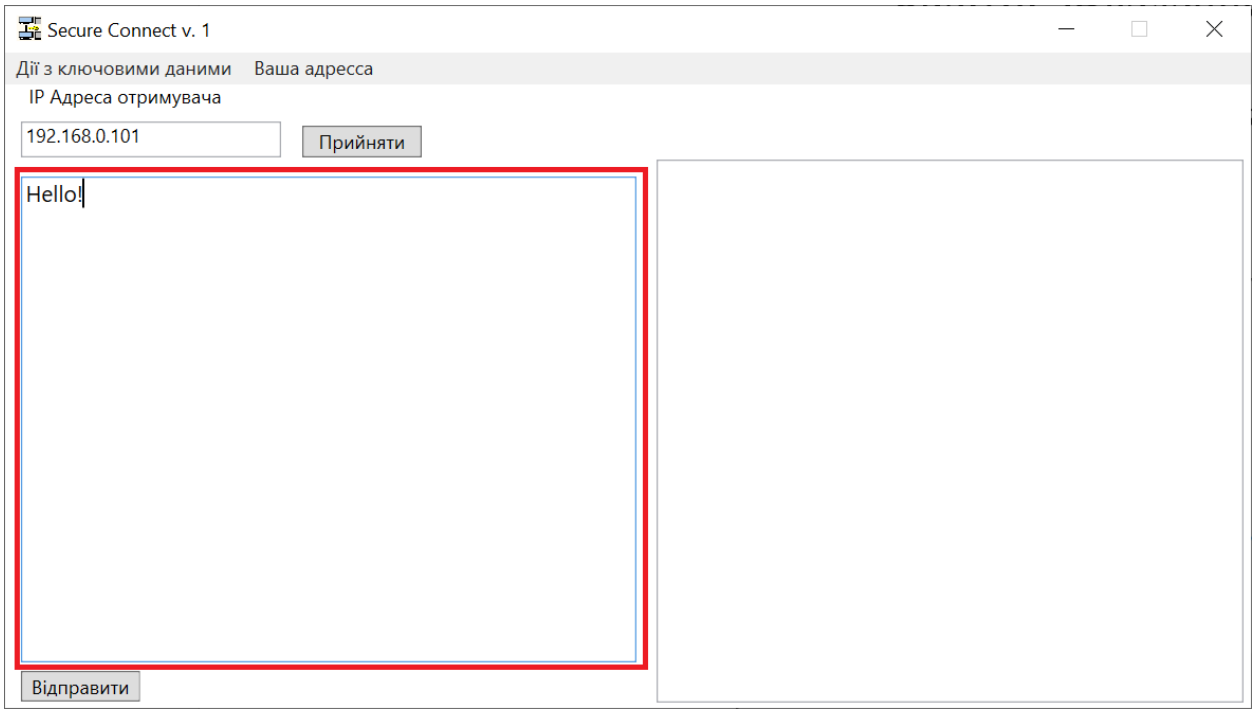


Рисунок 5.21 – Поле для відправки повідомлень

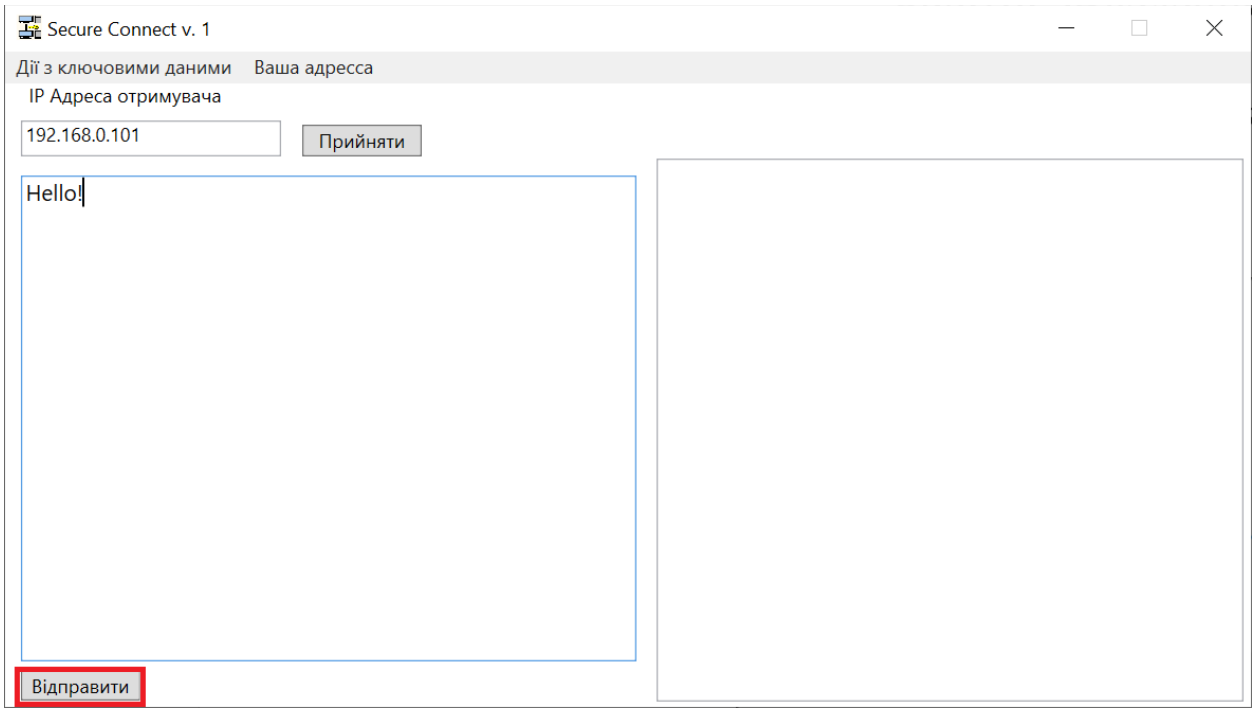


Рисунок 5.22 – Кнопка для відправлення повідомлень

Для отримання повідомлення необхідно завантажити ключовий носій (п. 5.2.3), після цього всі повідомлення будуть надходити в поле, яке зображено на рисунку 5.23.

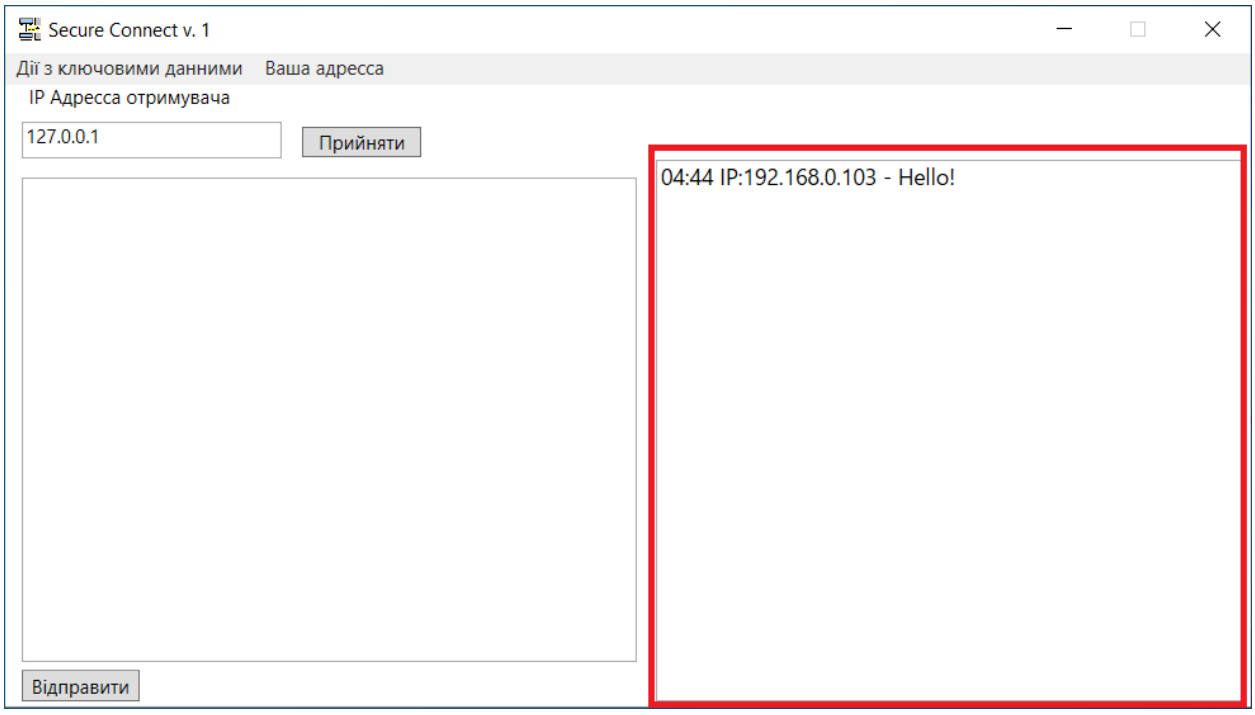


Рисунок 5.23 – поле з отриманими повідомленнями

Під час передачі по мережі, всі повідомлення будуть зашифровані й не підлягатимуть читанню (рис 5.24).

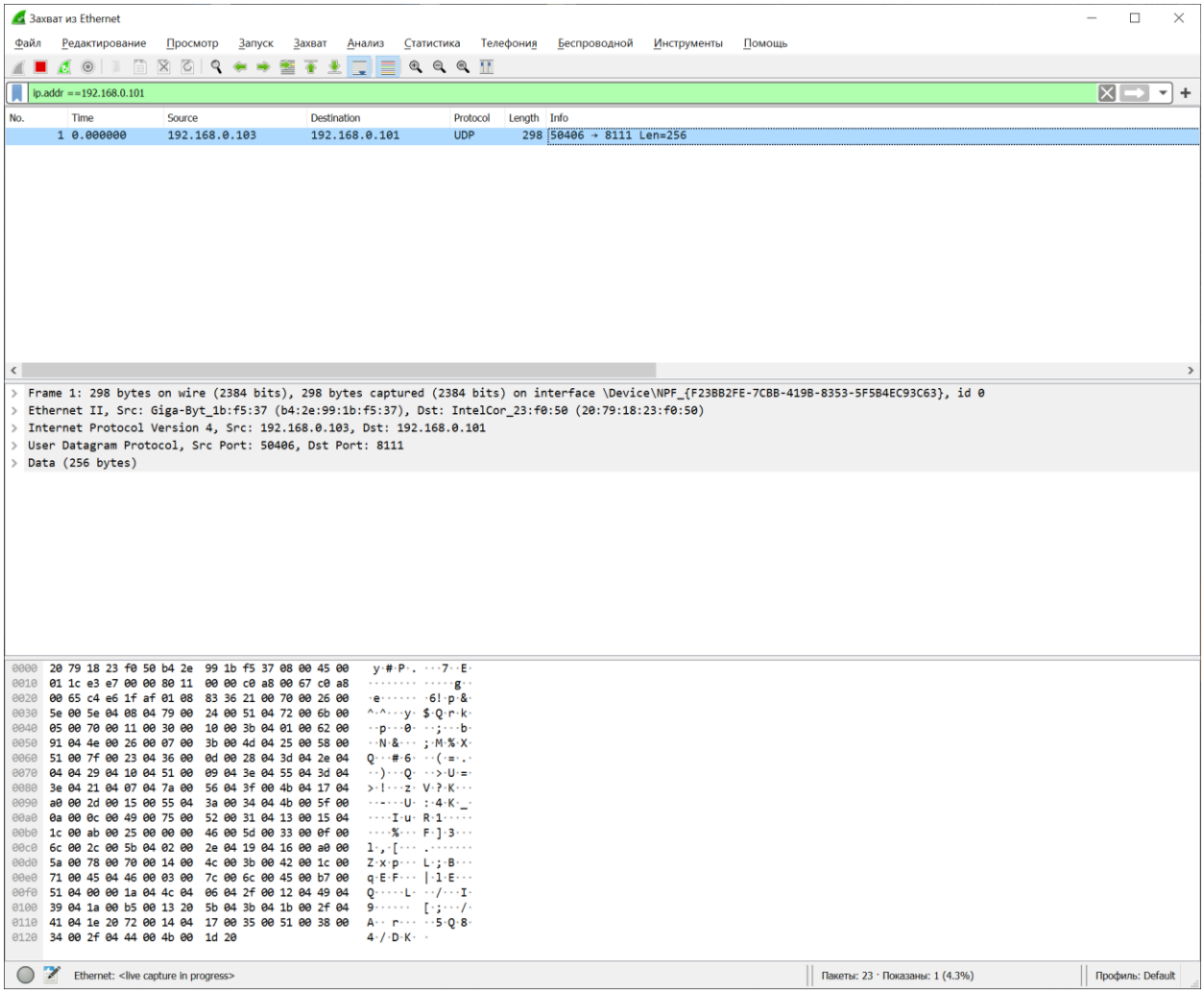


Рисунок 5.24 – Приклад пакету що передається в мережі

## 5.3 Захищені носії ключової інформації

Засіб криптографічного захисту інформації – це програмний, апаратно-програмний та апаратний засіб, призначений для криптографічного захисту інформації.

До засобів криптографічного захисту інформації належать:

– засоби, призначені для виготовлення ключових даних або документів (незалежно від виду носія ключової інформації) та управління ключовими

даними, що використовуються в засобах криптографічного захисту інформації (засоби категорії "К");

– засоби захисту від нав'язування неправдивої інформації або захисту від несанкціонованої модифікації, що реалізують алгоритми криптографічного перетворення інформації (криптоалгоритми), включаючи засоби імітозахисту та електронного цифрового підпису (засоби категорії "П");

– засоби захисту інформації від несанкціонованого доступу (у тому числі засоби розмежування доступу до ресурсів електронно-обчислювальної техніки), у яких реалізовані криптоалгоритми (засоби категорії "Р").

Залежно від способу реалізації розрізняють такі типи засобів криптографічного захисту інформації:

– програмні засоби, що функціонують у середовищі операційних систем електронно-обчислювальної техніки та взаємодіють із загальним прикладним програмним забезпеченням;

– апаратно-програмні засоби, у яких частину криптографічних функцій реалізовано в спеціальному апаратному пристрої до електронно-обчислювальної техніки, керування яким здійснюється за допомогою спеціального програмного забезпечення;

– апаратні засоби, алгоритм функціонування (включаючи криптографічні функції) яких реалізується в оптичних, механічних, мікроелектронних або інших спеціалізованих пристроях.

На даний момент в Україні затверджений перелік засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації та доступні такі захищені носії ключової інформації [15]:

1) Носій ключової інформації “Ефіт Key” UA.38782323.00001-01 (рис. 5.25)


Рисунок 5.25 – НКІ «Ефіт Кеу»

Ключовий носій має експертний висновок № 04/03/02-1257 від 12.04.2017, термін дії – до 08.10.2020. Виробник – Товариство з обмеженою відповідальністю «АЙ ТІ ІНЖИНІРІНГ».

2) Ключ електронний «Алмаз-1К» ЄААД.469535.153 (рис. 5.26).

Рисунок 5.26 – НКІ «Алмаз-1К»

Ключовий носій має експертний висновок № 04/03/02-1282 від 13.05.2019, термін дії – до 10.05.2024. Виробник – ПрАТ «Інститут інформаційних технологій».

3) Ключ електронний «SECURE TOKEN-338» (рис. 5.27)

Рисунок 5.27 – НКІ «Secure Token-338»

Ключовий носій має експертний висновок № 04/03/02-133 від 20.01.2020, термін дії – до 17.01.2025. Виробник – Товариство з обмеженою відповідальністю «АВТОР».

4) Ключ електронний «SECURE TOKEN-337Fx» АЧСА.467369.018 (рисунок 5.28).


Рисунок 5.28 – НКІ «Secure Token-337F»

Ключовий носій має експертний висновок № 04/03/02-881 від 09.04.2020, термін дії – до 07.04.2021. Виробник – Товариство з обмеженою відповідальністю «АВТОР».

5) Ключ електронний «Кристал-1» ЄААД.469535.040 (рис. 5.29).

Рисунок 5.29 – НКІ «Кристал-1»

Ключовий носій має експертний висновок № 04/03/02-934 від 16.04.2020, термін дії – до 14.04.2021. Виробник – ПрАТ «Інститут інформаційних технологій».

6) Засіб криптографічного захисту інформації «CryptoCard-337» (ТУ У 30.0-32248356-016:2011 (рис. 5.30).


Рисунок 5.30 – КЗІ «CryptoCard-337»

Засіб криптографічного захисту інформації має експертний висновок № 04/03/02-2333 від 30.06.2017, термін дії – до 27.10.2021. Виробник – Товариство з обмеженою відповідальністю «АВТОР».

# ВИСНОВКИ

Нині в криптографічному загалі широко обговорюється та досліджуються проблема створення та стандартизації перспективних криптографічних перетворень, в першу чергу для постквантового періоду. Суттєві результати досягнені в частині розроблення, стандартизації та застосування симетричних криптоперетворень. Разом з тим, продовжується розвиток та здійснюються спроби розробити більш ефективні методи криптоаналізу симетричних криптосистем – симетричних блокових перетворень, симетричних потокових перетворень та функцій гешування. Підтвердженням цьому є прийняття та застосування міжнародних стандартів ДСТУ ISO/IEC 18033-3, 18034-4, ДСТУ 7624:2014, ДСТУ 7564:2014, FIPS-197, FIPS-202 тощо.

Блоковий симетричний шифр ДСТУ 7624:2014 «Калина» має доказову квантову захищеність та відповідає вимогам сучасних криптосистем. Калина має найкращу продуктивність серед симетричних блокових шифрів (серед AES, ГОСТ-28147 та СТБ 34.101.31-2011) та підтримку 512-бітового ключа.

Використання ДСТУ 7624:2014 «Калина», в якості захисту конфіденційності при мережних з’єднаннях, дозволяє встановити шифрований канал зв’язку. Недоліком використання Калини є ймовірність успішної атаки побічними каналами.

Розроблене програмне забезпечення захищеної передачі повідомлень може бути використане для подальших досліджень властивостей криптоалгоритму при захисті IP-пакетів та в якості навчального макету.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Ефективна реалізація алгоритму блокового симетричного шифрування ДСТУ 7624:2014 («КАЛИНА») для 8/16/32-бітових вбудованих систем – Я.Р. Совин, В.І. Отенко, Є.Ф. Штефанюк, 2017. 11 стр.

2. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України – Роман Олійников, Іван Горбенко, Олександр Казимиров, Віктор Руженцев, Юрій Горбенко, 2015. 16 стр.

3. Калина (шифр) [Електронний ресурс]– Режим доступу: https://uk.wikipedia.org/wiki/Калина_(шифр)

4. Advanced Encryption Standard [Електронний ресурс]– Режим доступу: https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard

5. Расширение системы команд AES [Електронний ресурс]– Режим доступу: https://ru.wikipedia.org/wiki/Расширение_системы_команд_AES

6. Delivers Fast, Affordable Data Protection and Security [Електронний ресурс]– Режим доступу: https://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard-aes/data-protection-aes-general-technology.html

7. Twofish [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Twofish

8. RC6 [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/RC6

9. MARS [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/MARS

10. Crypto++ [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/Crypto%2B%2B.

11. Горбенко Ю.І. Побудування та аналіз систем, протоколів і засобів криптографічного захисту інформації: монографія. – Частина 1: Методи побудування та аналізу, стандартизація та застосування криптографічних систем

/ За заг. ред. д.т.н., професора І.Д. Горбенка. – Харків: Видавництво «Форт», 2015. – 960с.

12. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Чинний від 2015-07-01]. Вид. офіц. Київ, 2015. 181с.

13. Akanksha Singhal, Arko Chatterjee, Grover's Algorithm. Internship Report on Grover's Algorithm, Architecture Design and Implementation of the Quantum search algorithm (Grover's Search) DOI: 10.13140/RG.2.2.30860.95366

14. D-Wave Systems, Inc., PRACTICAL QUANTUM COMPUTING D-Wave Technology Overview [Електронний ресурс]– Режим доступу: https://www.dwavesys.com/sites/default/files/Dwave_Tech%20Overview2_F.pdf

15. Порта відкритих даних. Перелік засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації [Електронний ресурс]– Режим доступу: https://data.gov.ua/dataset/17055d98-7c52-436a-99b3-b808b323b37c/resource/9a12551c-ae0f-48d3-98e6-d3efbb557049/download/perelik-zasobiv-kzi-27-08-2020.ods

16. Yashu Swami, Amrata, Recognition of Quantum Computers vs. Classical Computers, National Electrical Engineering Conference 2011 (NEEC-2011)At: DELHI TECHNOLOGICAL UNIVERSITY, DELHI, INDIA [Електронний ресурс]– Режим- доступу: https://www.researchgate.net/publication /333561918_Recognition_of_Quantum_Computers_vs_Classical_Computers

17. Christophe Pittet, Mathematical Aspects of Shor's Algorithm [Електронний ресурс] – Режим доступу:

https://www.researchgate.net/publication/278625879_Mathematical_aspects_of_Shor's_algorithm

18. Federal Information Processing Standards Publication 197. Announcing the ADVANCED ENCRYPTION STANDARD (AES), November 2001. [Електронний ресурс] – Режим доступу:

ttps://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf