Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студентки *Омелаєнко Анастасії Геннадіївни*

академічної групи *125м-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи побудови криптографічних конструкцій, стійких до загрози застосування квантових обчислень*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н. доц. Герасіна О.В.			
розділів:				
спеціальний	ст. викл. Войцех С.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Омелаєнко А.Г.* **академічної групи** *125м-19-1*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Методи побудови криптографічних конструкцій стійких, до загрози застосування квантових обчислень*

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.20 № 888-с

Розділ	Зміст	Термін виконання
1	Аналіз понятійної бази квантових обчислень та криптосистем	03.09.20-20.10.20
2	Методи побудови квантово-безпечних криптосистем	21.11.20-01.12.20
3	Економічне обґрунтування доцільності впровадження криптографічних конструкцій, стійких до квантових обчислень	02.12.20-09.12.20

Завдання видано _____ Герасіна О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 03.09.20

Дата подання до екзаменаційної комісії: 16.12.20

Прийнято до виконання _____ Омелаєнко А.Г.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 91 с., 16 рис., 9 табл., 4 додатки, 43 джерела.

Об’єкт досліджень: квантово-безпечна криптографія.

Метою дипломної роботи є підвищення стійкості криптографічних конструкцій в умовах використання потужних квантових обчислень.

Предмет досліджень: методи побудови квантово-безпечних криптосистем.

В першому розділі дипломної роботи проведено аналіз можливостей квантових обчислень та структур криптографічних систем. Доведена актуальність проблеми переходу на нові методи криптографічного захисту даних.

В спеціальній частині дипломної роботи проаналізовано методи побудови криптографічних конструкцій, здатних ефективно функціонувати за умови розвитку потужних квантових обчислень. Розроблені рекомендації щодо імплементації квантово-безпечних криптосистем.

В економічному розділі наведено економічне обґрунтування доцільності розробки та імплементації квантово-безпечних криптосистем.

Практична цінність роботи полягає у результатах виконаного аналізу методів побудови квантово-безпечних криптосистем.

КВАНТОВИЙ КОМП’ЮТЕР, КУБІТ, КВАНТОВИЙ ЛОГІЧНИЙ ВЕНТИЛЬ, АЛГОРИТМ ШОРА, АЛГОРИТМ ГРОВЕРА, КВАНТОВА КРИПТОГРАФІЯ, ПОСТКВАНТОВА КРИПТОГРАФІЯ

РЕФЕРАТ

Пояснительная записка: 91 с., 16 рис., 9 табл., 4 прилож., 43 источника.

Объект исследований: квантово-безопасная криптография.

Целью дипломной работы является повышение устойчивости криптографических конструкций в условиях использования мощных квантовых вычислений.

Предмет исследований: методы построения квантово-безопасных криптосистем.

В первой главе дипломной работы проведен анализ возможностей квантовых вычислений и структур криптографических систем. Доказана актуальность проблемы перехода на новые методы криптографической защиты данных.

В специальной части дипломной работы проанализированы методы построения криптографических конструкций, способных эффективно функционировать при условии развития мощных квантовых вычислений. Разработаны рекомендации по имплементации квантово-безопасных криптосистем.

В экономическом разделе приведено экономическое обоснование целесообразности разработки и имплементации квантово-безопасных криптосистем.

Практическая ценность работы заключается в результатах проведенного анализа методов построения квантово-безопасных криптосистем.

КВАНТОВЫЙ КОМПЬЮТЕР, КУБИТЫ, КВАНТОВЫЙ ЛОГИЧЕСКИЙ ВЕНТИЛЬ, АЛГОРИТМ ШОРА, АЛГОРИТМ ГРОВЕРА, КВАНТОВАЯ КРИПТОГРАФИЯ, ПОСТКВАНТОВАЯ КРИПТОГРАФИЯ

ABSTRACT

Explanatory note: 91 p., 16 fig., 9 tab, 4 applications, 43 sources.

Object of research: quantum-safe cryptography.

Purpose of degree work: increasing the stability of cryptographic structures in conditions of the use of powerful quantum computing.

Subject of research: methods for constructing quantum-safe cryptosystems.

In the first chapter, the possibilities of quantum computing and structures of cryptographic systems were analyzed. The urgency of the problem of transition to new methods of data protection is proved.

In a special part, methods of building cryptographic constructions that can function effectively under the condition of the development of powerful quantum computing are analyzed. Recommendations for the implementation of quantum-safe cryptosystems were developed.

The economic section provides an economic justification for the development and implementation of quantum-safe cryptosystems.

The practical value of the work is results of the analysis of methods for constructing quantum-safe cryptosystems.

QUANTUM COMPUTER, QUBITS, QUANTUM LOGICAL GATE, SHOR'S ALGORITHM, GROVER SEARCH ALGORITHM, QUANTUM CRYPTOGRAPHY, POST-QUANTUM CRYPTOGRAPHY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ECC – elliptic-curve cryptography (криптографія еліптичних кривих);

ПДЛЕК – проблема дискретного логарифмування у групі точок еліптичної кривої;

ПДЛ – проблема дискретного логарифмування;

ПФЧ – проблема факторизації цілих чисел;

DARPA – Defense Advanced Research Projects Agency (Агентство передових оборонниxx дослідницьких проектів);

NASA – National Aeronautics and Space Administration (Національне управління з аеронавтики і дослідження космічного простору);

DOE – United States Department of Energy (Міністерство енергетики США);

USN – United States Navy (Військово-морські сили США);

QRNG – Quantum Random Number Generator (квантовий генератор випадкових чисел);

SPV – Shortest Vector Problem (Задача знаходження найкоротшого вектора);

ISVP – (approximate) Ideal Shortest Vector Problem (Задача знаходження (приблизно) ідеального найкоротшого вектора);

SIVP – (approximate) Shortest Independent Vector Problem (Задача знаходження (приблизно) найкоротшого незалежного вектора);

CVP – Closest Vector Problem (Задача знаходження найближчого вектору).

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 АНАЛІЗ ПОНЯТІЙНОЇ БАЗИ КВАНТОВИХ ОБЧИСЛЕНЬ ТА КРИПТОСИСТЕМ 11
1.1 Квантові комп'ютери 11
1.1.2 Галузі застосування квантових комп'ютерів 11
1.1.3 Темпи розвитку квантових обчислень 12
1.1.4 Характеристика можливостей квантових комп'ютерів 14
1.1.5 Принцип роботи квантових вентилів 16
1.1.6 Вплив квантових комп'ютерів на сучасну криптографію 22
1.2 Аналіз побудови криптографічних систем 24
1.2.1 Симетричні криптосистеми 24
1.2.2 Асиметричні криптосистеми 26
1.2.3 Гібридні криптосистеми 30
1.3 Висновки. Постановка задачі 32
РОЗДІЛ 2 МЕТОДИ ПОБУДОВИ КВАНТОВО-БЕЗПЕЧНИХ КРИПТОСИСТЕМ 33
2.1 Нові підходи до побудови квантово-безпечних криптосистем 33
2.2 Квантова криптографія 35
2.2.1 Протокол BB84 36
2.3 Криптографія на основі геш-функцій 43
2.3.1 Підпис Меркле 43
2.3.2 Підпис Лампорта 45
2.4 Криптографія кодів виправлення помилок 48
2.4.1 Криптосистема McEliece 48
2.5 Криптографія на основі решіток 51
2.5.1 Криптосистема NTRU 51
2.6 Мультиваріативна криптографія 54
2.7 Криптографія ізогенії суперсингулярних еліптичних кривих 56

2.8 Рекомендації щодо імплементації квантово-безпечних криптосистем..... 58
2.9 Висновки до другого розділу 59
РОЗДІЛ 3 ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ ВПРОВАДЖЕННЯ КРИПТОГРАФІЧНИХ КОНСТРУКЦІЙ, СТІЙКИХ ДО КВАНТОВИХ ОБЧИСЛЕНЬ 60
3.1 Вступ до економічного розділу 60
3.2 Розрахунок фіксованих (капітальних) витрат 60
3.2.1 Визначення витрат на створення програмних засобів криптографічного захисту на основі постквантових криптосистем 62
3.2.1.1 Визначення трудомісткості розробки та опрацювання програмного продукту (постквантових алгоритмів) 62
3.2.2 Розрахунок витрат на створення програмного продукту 65
3.3. Розрахунок поточних (експлуатаційних) витрат 69
3.4. Оцінка можливого збитку від атаки на вузол або сегмент корпоративної мережі 74
3.4.1 Оцінка величини збитку 74
3.4.2 Загальний ефект від впровадження квантово-безпечних систем..... 78
3.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки..... 79
3.6 Висновок до економічного розділу 81
ВИСНОВКИ..... 82
ПЕРЕЛІК ПОСИЛАНЬ 83
ДОДАТОК А. Відомість матеріалів дипломної роботи..... 88
ДОДАТОК Б. Перелік документів на оптичному носії..... 89
ДОДАТОК В. Відгуки керівників розділів..... 90
ДОДАТОК Г. ВІДГУК..... 91

ВСТУП

На сьогоднішній день людство переживає активну фазу розвитку інформаційних технологій та засобів і методів їхньої реалізації. Всі сфери діяльності сучасної людини пов'язані з ІТ-технологіями, розвиток цієї галузі є найбільш актуальним. На сьогоднішній день всі найвпливовіші ІТ-корпорації світу ведуть активні дії щодо вдосконалення існуючих та розробки нових технологічних методів та пристроїв.

Однією з найбільш перспективних та багатообіцяючих галузей розвитку інформаційних технологій є створення потужного квантового комп'ютера. Такий комп'ютер спроможний перекреслити єфективність багатьох популярних на сьогодні методів криптографії.

Через це виникає потреба в принципово нових методах криптографічного захисту даних. Криптографічні методи, які не втратять своєї криптостійкості навіть за умови існування потужних квантових комп'ютерів, називаються постквантовою або квантово-безпечною криптографією.

У роботі були поставлені такі задачі :

- Проаналізувати принцип роботи квантового комп'ютера, темпи його розвитку та вплив на сучасну криптографію;
- Проаналізувати структури криптографічних систем;
- Проаналізувати методи побудови конструкцій квантово-безпечної криптографії;
- Розробити рекомендації щодо застосування квантово-безпечних криптосистем.

Метою дипломної роботи є підвищення стійкості криптографічних конструкцій в умовах використання потужних квантових обчислень.

Об'єкт досліджень: квантово-безпечна криптографія.

Предмет досліджень: методи побудови квантово-безпечних криптосистем.

Наукова новизна: розробка рекомендацій з імплементації квантово-безпечних криптосистем.

Практична цінність: результати виконаного аналізу методів побудови квантово-безпечних криптосистем.

РОЗДІЛ 1
АНАЛІЗ ПОНЯТІЙНОЇ БАЗИ КВАНТОВИХ ОБЧИСЛЕНЬ ТА КРИПТОСИСТЕМ

1.1 Квантові комп'ютери

Сучасний технологічний розвиток виходить за рамки класичної фізики, зокрема, елементарні складові звичайних комп'ютерів наблизились до атомарних розмірів, тобто до розмірів об'єктів мікросвіту, на рівні якого починають працювати закони квантової фізики. Це є одною з причин припинення дії закону Мура, який передбачав це ще у 2007 році [7]. Після відкриття існування найменших часток і принципів їхньої взаємодії, наступним етапом є створення технологій на основі цих взаємодій. Створення обчислювального пристрою (комп'ютера), який для вирішення задач макросвіту використовував би можливості мікросвіту, стало одним з головних викликів XXI сторіччя.

Квантовий комп'ютер – це обчислювальний пристрій, який для виконання своїх процесів використовує закони квантової фізики та об'єкти мікросвіту (фотони, іони, електрони).

Головні явища, які використовує квантовий комп'ютер — квантова суперпозиція та квантова заплутаність [15, 16].

Квантова суперпозиція — принцип квантової механіки, за яким елемент в один момент часу може перебувати у декількох взаємовиключних станах.

Квантова заплутаність — квантове явище, при якому декілька елементів перебувають у взаємопов'язаних між собою станах.

1.1.2 Галузі застосування квантових комп'ютерів

Квантові комп'ютери можуть бути застосовані для таких задач:

— Фінансове прогнозування;

— Економічна оптимізація;

— Моделювання хімічних реакцій (створення нових лікувальних препаратів);

— Моделювання взаємодії часток на атомарному рівні (відкриття нових фізичних явищ) (аналог адронного колайдера);

— Машинне навчання (навчання нейромереж);

— Квантові сенсори (метрологія, медицина, геодезія);

— Квантові комунікації (квантова телепортація);

— Квантова криптографія;

— Зведення експоненційно складних задач до поліноміального класу складності (факторизація великого простого числа, дискретне логарифмування).

З точки зору кібербезпеки особливу увагу привертають два останні пункти. Квантова криптографія може стати вирішенням ключової проблеми симетричної криптографії, а саме проблеми розподілу ключів. Навпаки, зведення проблеми факторизації великого простого числа у клас задач поліноміальної складності може повністю зруйнувати сучасну асиметричну криптографію та становить одну з головних загроз кібербезпеці в близькому майбутньому.

1.1.3 Темпи розвитку квантових обчислень

Ключовими, з точки кібербезпеки, є дати розробки квантового алгоритму для факторизації великих цілих чисел та вирішення проблеми дискретного логарифму Пітером Шором (Peter Williston Shor) у 1994 році та алгоритму пошуку Ловом Гровером (Lov Kumar Grover) у 1996 році.

Історія квантових обчислень бере початок з 70-х років минулого сторіччя [6]. Точкою відліку створення квантових комп'ютерів є 1998 рік, коли був представлений перший 2-кубітний і перший 3-кубітний комп'ютери та, відповідно, перша реалізація алгоритму Гровера. У 2000 році були створені 5-ти та 7-кубітні комп'ютери, а також перша реалізація частини алгоритму Шора. Наступний рік відзначився реалізацією повного алгоритму Шора - було факторизовано число 15. З 2007 року активну діяльність починає канадська

компанія D-Wave Systems, яка спеціалізується у створенні квантових комп'ютерів для комерційного використання. Саме у цьому році вона випустила перший 16-кубітний комп'ютер.

У 2018 році компанія Google заявила про створення 72-кубітного процесора Bristlecone, але подробиць щодо принципу його дії компанія не повідомила. Компанія Google вважає, що для досягнення квантової переваги необхідно задіяти 49 кубітів, не менше 40-ка з яких повинні складати обчислювальну потужність (глибину (circuit depth)), а імовірність помилки у 2-кубітному елементі повинна бути не більше ніж 0,5 %.) [17].

Найбільш успішним розробником квантових комп'ютерів є канадська компанія D-Wave Systems [8,19, 20], що у 2007 році презентувала перший у світі 16-кубітний квантовий процесор. 2011-го року D-Wave відзначилася 128-кубітним комп'ютером — D-Wave One, а вже наступного року був представлений 512-кубітний квантовий комп'ютер — D-Wave Two. Комп'ютери D-Wave наступних поколінь: 2015 рік - D-Wave 2X з 1152 кубітами; 2016 рік – комп'ютер на 2000 кубітів; та 2020 рік – 5000-кубітний квантовий комп'ютер. Остання їх розробка є доволі знаменною, тому що цей комп'ютер створений для бізнес-процесів і може бути доступним через хмарне середовище [19]. Можна констатувати факт того, що квантові обчислення вже увійшли у сферу комерційної діяльності.

Важливим буде доповнення щодо принципу роботи цих пристроїв. Комп'ютери компанії D-Wave працюють за алгоритмом квантового випалювання на відміну від класичних, які працюють на основі квантових вентилів. Саме тому ці комп'ютери не є універсальними і ефективні тільки для вузького ряду задач. На них не можливо реалізувати алгоритм Шора, що робить їх не придатними для завдань криптоаналізу. Тим не менш, проаналізувавши розвиток компанії D-Wave, яка за 13 років зробила стрибок від 16 до 5000 підконтрольних кубітів (збільшення більше ніж на 30 000 % від початкової величини), можна зробити висновки, що розвиток квантових обчислень невпинно прогресує. Можливо, що ультимативна квантова машина, яка буде здатна знищити сучасну криптографію,

працюватиме не тільки за принципом квантових вентилів, а буде складатися з декількох технологій, одною з яких будуть розробки D-Wave.

1.1.4 Характеристика можливостей квантових комп'ютерів

На відміну від класичних (лінійних) комп'ютерів, які оперують бітами, квантові комп'ютери для своїх обчислень використовують квантові біти або кубіти. Класичні комп'ютери працюють за законами класичної фізики. У класичній фізиці об'єкт у конкретний проміжок часу може перебувати тільки у одному визначеному стані. Тож біт, як складова класичної системи, може знаходитись тільки в одному стані (0 або 1) в конкретну одиницю часу. Квантові комп'ютери підпорядковуються законам квантової фізики, яка починає працювати на мікрорівні. Кубіти — це об'єкти мікрорівня (елементи атомарних розмірів). Головною відмінністю і перевагою кубітів перед бітами — здатність перших перебувати у декількох станах (0 та 1) одночасно, згідно принципу суперпозиції [16]. За принципом суперпозиції, до вимірювання квантова система перебуває у ймовірнісному стані своїх можливих значень (у кожен проміжок часу система може знаходитися в якомусь стані з деякою ймовірністю). Цей стан розраховується за формулою (1.1).

$$| \Psi \rangle = \sum_{i=0}^{n-1} k_i | i \rangle \qquad (1.1)$$

де Ψ — квантова суперпозиція, i — один з можливих станів, k — ймовірнісний коефіцієнт стану i, n — множина станів.

Квантовий світ — це ймовірнісний світ, в якому кожен об'єкт (частка) може перебувати у деякому стані з деякою імовірністю. Для позначення такої ймовірності використовують ймовірнісний коефіцієнт. Чим більше значення

ймовірнісного коефіцієнту, тим більша ймовірність того, що при вимірюванні об'єкт буде перебувати у стані, який відповідає такому коефіцієнту.

Для позначень квантових станів використовується позначення Дірака (бра-кет позначення) [20]. Зокрема, кет-нотація $| \Psi \rangle$ позначає вектор-стовпець значень k_i, що наведено в формулі (1.2).

$$\Psi = \begin{bmatrix} k \text{ першого стану} \\ . \\ . \\ . \\ k \text{ останнього стану} \end{bmatrix} \tag{1.2}$$

Вірогідністю отримання кожного стану є значення його ймовірнісного коефіцієнту в квадраті, з дотриманням умови формули (1.3).

$$\sum_{i=0}^{n-1} |k_i|^2 = 1 \tag{1.3}$$

У квантових комп'ютерах один кубіт може мати два значення. Суперпозиція кубіта описується формулою (1.4), що є еквівалентом рівняння Шредінгера (Schrödinger equation).

$$|\psi\rangle = a|0\rangle + b|1\rangle \tag{1.4}$$

де ψ — суперпозиція кубіта, a та b — ймовірнісні коефіцієнти того, що значення кубіту дорівнює 0 та 1 відповідно.

Формула (1.4) працює для одного кубіта. Квантова система, яка складається з 2-х взаємно заплутаних кубітів, може перебувати у станах $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ одночасно. Для лінійної системи можливо перебувати в один момент часу тільки в одному стані. Якщо квантовий комп'ютер може оперувати n кількістю кубітів,

то у один момент часу цей пристрій може працювати з 2^n значеннями системи, що наведено у таблиці 1.1. Така властивість квантового комп'ютера називається квантовим паралелізмом.

Таблиця 1.1 — Залежність кількості можливих значень системи в один проміжок часу від кількості задіяних елементарних інформаційних одиниць (кубітів) у квантовому комп'ютері

Одиниця часу	Кількість кубітів	Кількість значень
1	1	2
	10	1024
	100	приблизно 10^{30}
	1000	приблизно 10^{301}

1.1.5 Принцип роботи квантових вентилів

Універсальний квантовий комп'ютер — пристрій на якому можлива реалізація алгоритмів Шора та Гровера, будується на базисі технології квантових вентилів.

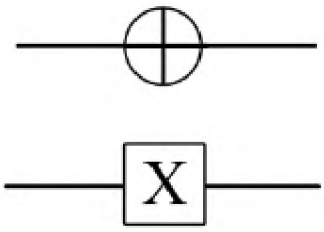
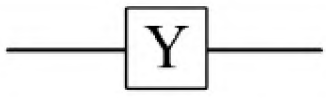
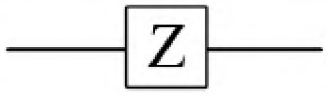
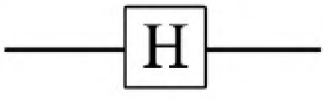
Елементарними складовими універсального квантового комп'ютера є елементарні частинки, над якими проводять унітарні (обернені) операції. Унітарні операції для квантових обчислень називаються логічними квантовими вентилями (quantum gates) [5]. З цих двох складових утворюється квантовий процесор. Так як кубіт перебуває у декількох станах одночасно, його зображають як вектор-стану. Квантовий вентиль зображають як унітарну матрицю (квадратну матрицю з комплексними елементами, множення якої на обернену до себе матрицю дає у результаті одиничну матрицю). Розмір такої матриці залежить від кількості задіяних кубітів: однокубітні вентилі позначаються як матриця 2 на 2; двохкубітні — як 4 на 4; n-кубітні — як матриця 2^n на 2^n. Взаємодія кубіту та квантового

вентиля зображується як множення вектору-стану кубіту на унітарну матрицю. Таким чином квантові обчислення зводяться до унітарних перетворень над кубітами. Для універсального квантового процесора необхідно, щоб він володів універсальним логічним блоком (набором вентилів, якими можливо реалізувати всі унітарні перетворення). Всі унітарні перетворення можливо досягти використанням однокубітних та двохкубітних вентилів [23 - 25].

Однокубітні вентилі —це логічні операції, які проводяться над одним кубітом.

До однокубітних вентилів відносяться вентилі Паулі (Pauli gate) X, Y, Z. Кожен з цих вентилів має своє зображення як унітарної матриці та схематичне позначення. Позначення вентилів Паулі наведені у таблиці 1.2.

Таблиця 1.2. — Позначення однокубітних вентилів

Назва вентилю	Відповідна унітарна матриця	Схематичне позначення
X, NOT, переключення кубіту	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	
Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	
Z, переключення фази	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	
Вентиль Адамара	$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$	

Вентиль X є еквівалентом класичному вентилю NOT. Такий вентиль, отримавши на вході кубіт з одним станом, видає на виході цей кубіт з протилежним станом (рисунок 1.1).

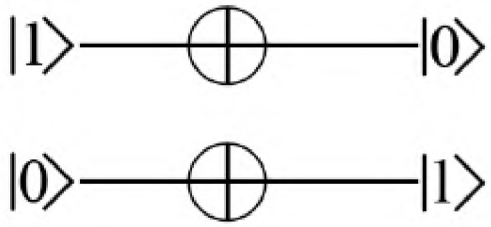


Рисунок 1.1 — Принцип дії вентиля X

Вентиль Z залишає кубіт стану |0⟩ без змін, |1⟩ конвертує у мінус |1⟩ (рисунок 1.2).

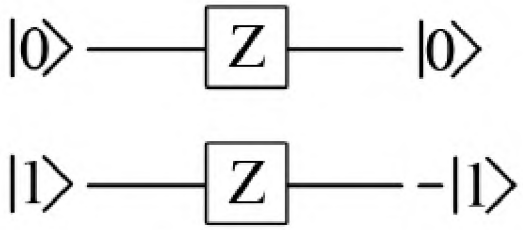


Рисунок 1.2 — Принцип дії вентиля Z

Вентиль Y є результатом множення унітарних матриць векторів X та Z. Якщо на вхід цього вентиля подати |0⟩, то на виході буде i|1⟩; якщо подати на вхід стан |1⟩, результатом буде стан мінус i|0⟩ (рисунок 1.3).

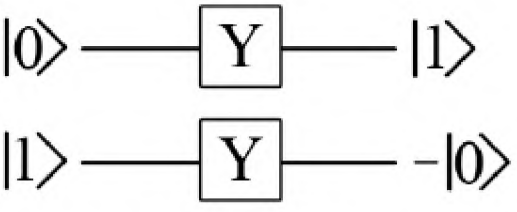


Рисунок 1.3 — Принцип дії вентиля Y

Необхідною умовою таких вентилів є їх унітарність: якщо повторно застосувати вентиль Паулі до того ж кубіту, з яким він вперше взаємодіяв, цей

кубіт повернеться до початкового стану (стану, в якому кубіт перебував до впливу вентиля) (формула (1.5)).

$$XX = YY = ZZ = I \rightarrow X^2 = Y^2 = Z^2 = I \quad (1.5)$$

де I — квантовий вентиль (одинична матриця), дія якого на кубіт не змінює стану останнього.

Вентиль Адамара (Hadamard gate) встановлює кубіт у стан суперпозиції — імовірність перебування кубіту у стані $|0\rangle$ або $|1\rangle$ стає однаковою (рисунок 1.4).

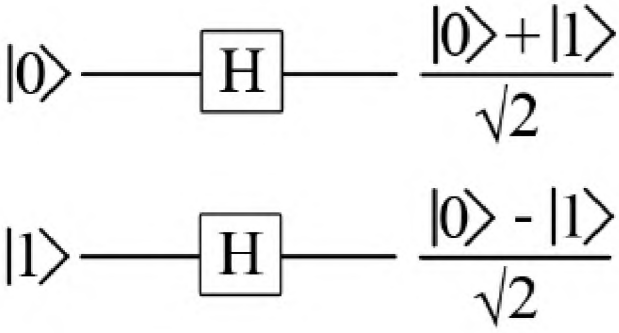


Рисунок 1.4 — Принцип дії вентиля Адамара

Двохкубітні вентилі — логічні операції, які проводяться над двома кубітами. Двохкубітні вентилі відносяться до багатокубітних — вентилів, які оперують двома та більше кубітами. Багатокубітні вентилі можуть бути керованими.

Керований вентиль — багатокубітний вентиль, на вхід якого подається мінімум один керуючий кубіт і один — керований. Такий вентиль тільки тоді виконує перетворення з керованим кубітом, якщо керуючий кубіт знаходиться у необхідному стані, інакше перетворення не відбувається. Якщо керуючий вентиль виконує перетворення керованого кубіта за умови, що стан керуючого кубіту дорівнює $|1\rangle$, то схематично такий вентиль позначається замальованим колом. Якщо для дії вентилю необхідно щоб керуючий кубіт знаходився у стані $|0\rangle$ — позначення виглядає як незамальоване коло (рисунок 1.5).

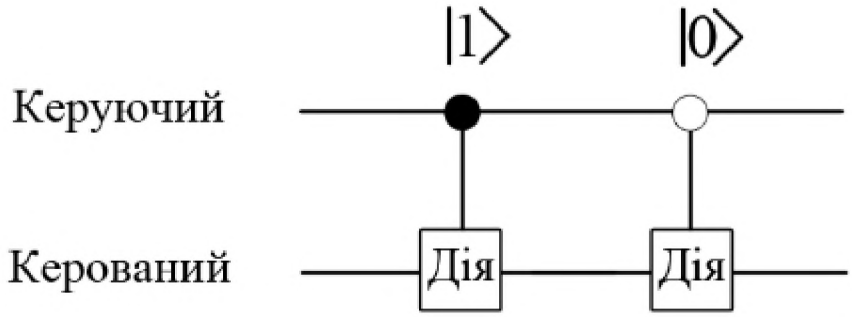


Рисунок 1.5 — Схематичне позначення керованого вентиля

Матриця для керованого вентиля формується з одиничної матриці I, яка розміщується у верхньому лівому куті та матриці дії цього вентиля, яка розміщується у нижньому правому куті. Вся інша площа матриці заповнюється нулями. Позначення багатокубітних вентилів наведено у таблиці 1.3.

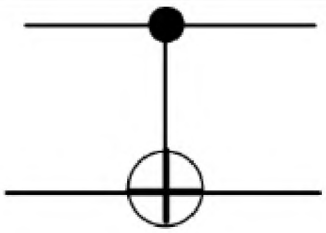
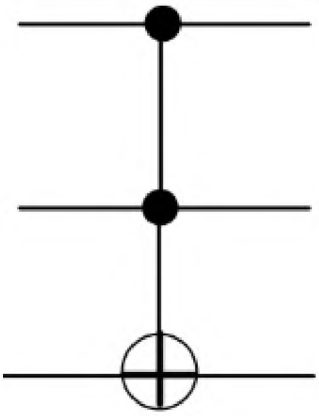
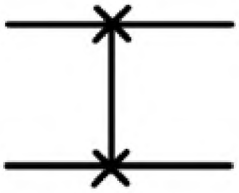
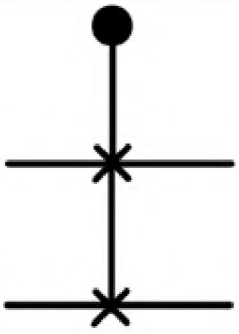
Керований вентиль CNOT змінює стан керованого вентиля на протилежний, якщо керуючий вентиль знаходиться в стані $|1\rangle$.

Вентиль Тофолі (Toffoli gate) є трьохкубітним вентилем та змінює стан третього керованого кубіту на протилежний, якщо перші два керуючих кубіта знаходяться в стані $|1\rangle$.

Вентиль SWAP не відноситься до керованих вентилів. Приймаючи на вході два кубіти, цей вентиль міняє місцями їх стани.

Вентиль Фредкіна (Fredkin gate) міняє місцями стани двох останніх кубітів, якщо перший кубіт знаходиться в стані $|1\rangle$.

Таблиця 1.3 — Позначення багатокубітних вентилів

Назва вентилю	Відповідна унітарна матриця	Схематичне позначення
CNOT	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	
CCNOT, вентиль Тофолі	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$	
SWAP	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	
CSWAP, вентиль Фредкіна	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$	

Суть використання таких вентилів полягає в заплутуванні кубітів між собою (рисунок 1.6).

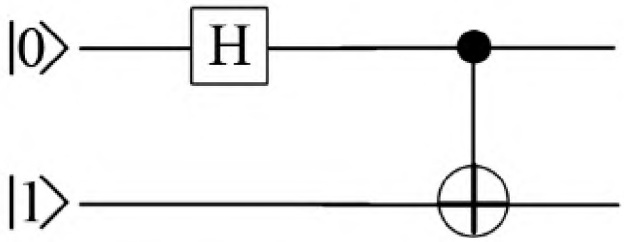


Рисунок 1.6 — Схема найпростішої квантової заплутаності

На рисунку 6 наведена схема реалізації квантової заплутаності двох кубітів: спочатку керуючий (верхній) кубіт «пройшовши» через вентиль Адамара встановлюється в стан суперпозиції (однакова імовірність при вимірюванні отримати стан $|0\rangle$ чи $|1\rangle$), а потім, в залежності від стану керуючого кубіту (який є невідомим) робиться або не робиться перетворення керованого кубіту. Таким чином, стани обох кубітів є невідомими, і самі кубіти заплутані відносно один одного.

1.1.6 Вплив квантових комп'ютерів на сучасну криптографію

Головною перевагою квантових комп'ютерів над звичайними є те, що при збільшенні квантових масивів даних кількість інформації, що у них зберігається, зростає експоненційно на відміну від звичайних масивів, які зі збільшенням своїх величин мають лінійний приріст об'єму інформації, що може у них міститися. Багатофункціональність квантових комп'ютерів: вирішення деяких експоненційно-складних математичних задач за поліноміальний час, зокрема проблеми факторизації великих чисел та дискретного логарифмування (при умові, що на ньому можна буде реалізувати алгоритм Шора), що є загрозою для сучасних асиметричних криптосистем, таких як RSA, ElGamal, DiffieHellman, еліптична криптографія (Elliptic-curve cryptography (ECC)); квадратичне зменшення часу пошуку в неупорядкованих базах даних (або ж метод грубої сили) (при можливості реалізації алгоритму Гровера), що є загрозою для симетричних криптосистем з недостатньо великим ключем шифрування;

модулювання різних наукових систем, яке не може бути створене силами лінійних (неквантових) обчислень.

Алгоритм Шора — квантовий алгоритм факторизації, реалізація якого дозволяє розкласти число N на свої прості множники виконавши $O(n^3)$ операцій (n — розмірність числа N у бітах) [5]. Алгоритм Шора здатен робити факторизацію чисел з приблизно такою ж швидкістю, як і швидкість самого шифрування цими числами. Також цей алгоритм здатен зводити задачі дискретного логарифмування до поліноміально складних, адже задачі факторизації та дискретного логарифмування є схожими. Реалізація цього алгоритму повністю знівечить ефективність сучасних асиметричних криптосистем.

Алгоритм Гровера — квантовий алгоритм пошуку в неупорядкованій базі даних. Якщо є булева функція f для n кількості змінних, то суть задачі полягає у знаходженні змінної x, для якої $f(x)$ дорівнювало б одиниці. Знайдення рішення для функції $f(x)$ є методом повного перебору. У найгіршому випадку метод повного перебору потребує перевірки 2^n можливих комбінацій. Алгоритм Гровера робить перевірку $O(\sqrt{2^n})$ разів, задіявши O(n) кубітів. У цьому алгоритмі досягається квадратичне пришвидшення вирішення задачі методом повного перебору.

Реалізація алгоритму Шора на великомасштабному квантовому комп'ютері здатна підірвати сучасну асиметричну криптографію, а реалізація алгоритму Гровера — поставити симетричну криптографію у жорсткі рамки. На сьогоднішній день активно використовується гібридна криптосистема, яка використовує принципи асиметричних та симетричних криптосистем. Тож немає можливості повністю відмовитися від асиметричної криптографії, використовуючи лише відкориговану симетричну. Виникає необхідність у принципово нових методах побудови криптографічних конструкцій.

1.2 Аналіз побудови криптографічних систем

Криптосистема — набір алгоритмів, якими реалізується шифрування та розшифрування інформації. Криптографічні системи поділяють на симетричні, асиметричні та гібридні.

1.2.1 Симетричні криптосистеми

В симетричних криптосистемах шифрування даних робиться тим самим ключем, що і дешифрування. Для їх реалізації потрібен один ключ [13], який обов'язково повинен знаходитися в секреті. Користувачі таких систем повинні узгодити значення секретного ключа перед початком обміну інформацією, яка буде захищатися цим ключем. Формування ключів виконується генераторами псевдовипадкових послідовностей, від якості яких залежить криптостійкість усієї системи. Якість послідовності генератора залежить від того, наскільки складно визначити значення елементу послідовності, створеної таким генератором, знаючи алгоритм формування цієї послідовності та всі попередні її елементи [10]. Якщо пристрій генерації симетричних ключів відповідає умові якості та має період повторюваності більший, ніж величини послідовностей, які він створює, то можна вважати, що такі послідовності є достатньо наближеними до випадкових. Ключі, створені з цих послідовностей можливо скомпрометувати лише методом грубої сили.

Плюси симетричних криптосистем:

— Велика швидкість шифрування та дешифрування даних;
— Малий розмір ключа;
— Висока криптостійкість.

Швидкодія симетричних алгоритмів обумовлена простотою операцій (підстановки, перестановки), які застосовуються для шифрування та дешифрування інформації.

Малий розмір ключів досягається тим, що у симетричних системах ключі є псевдовипадковими послідовностями. Якщо такі послідовності проходять всі тести на випадковість і є достатньо непередбачуваними, вони стають незалежними від математичних принципів і стають вразливими лише до повного перебору всіх можливих значень.

Через спосіб створення симетричних ключів, їх розкриття можливе лише у двох випадках:

— При перехопленні ключа під час його передачі каналом зв'язку;
— Атакою повного перебору.

На сьогоднішній день не відомі більш ефективні методи злому симетричних криптосистем, ніж атака методом грубої сили. Такий вид атаки має експоненційну залежність рівня складності від величини ключа, на який вона спрямована. При достатньому розмірі ключів симетричні криптосистеми не можуть бути зламані атакою грубої сили за адекватний проміжок часу, що характеризує високу криптостійкість таких систем.

Мінуси симетричних криптосистем:

— Потреба в наявності надійного каналу передачі даних;
— Питання взаємодовіри між користувачами зі спільним симетричним ключем;
— Експоненційна залежність кількості ключів від кількості користувачів.

Перший мінус полягає в тому, що сам ключ симетричного шифрування необхідно передати користувачам. Якщо не звертатися до послуг асиметричної криптографії, то виникає потреба в безпечному каналі передачі даних. Виконання такої умови є доволі складним завданням.

Перед користувачами зі спільним (однаковим) ключем постає питання довіри. Відсутня гарантія того, що приймальна сторона не змінить отримані дані та не звинуватить у цьому сторону-відправника. Або ж навпаки, той, хто посилає

повідомлення може надати завідомо некоректні дані і звинуватити сторону-відправника у їх модифікації. Тож робити довіру, як одну зі складових захисту, не є вірним рішенням у разі великої кількості користувачів.

У симетричних криптосистемах спостерігається експоненційне збільшення кількості ключів при лінійному збільшенні користувачів. Вже на невеликій кількості користувачів число ключів стає дуже великим. Розрахунок кількості симетричних ключів проводиться за формулою (1.6).

$$N_{ключів} = N_{користувачів} \cdot (N_{користувачів}-1) / 2 \quad (1.6)$$

де $N_{ключів}$ — кількість ключів у системі, $N_{користувачів}$ — кількість користувачів у системі.

1.2.2 Асиметричні криптосистеми

Асиметричні криптосистеми оперують двома типами ключів: закритим і відкритим. Шифрування відбувається відкритим ключем, а дешифрування робиться за допомогою закритого ключа. Якщо такі криптосистеми використовуються для електронного цифрового підпису, то засекречування інформації відбувається закритим ключем, а для її розсекречення використовується відкритий ключ. Значення закритого ключа відомо лише його власнику. Значення відкритого ключа відомо всім користувачам системи. З інформації про відкритий ключ майже неможливо віднайти дані закритого ключа. Пара асиметричних ключів формується за допомогою особливостей математичних конструкцій, вирішення яких, за сучасних обчислювальних потужностей, не може бути виконано за адекватний проміжок часу.

Особливістю асиметричних криптосистем є застосування односторонніх функцій з секретом або функцій-пасток (trapdoor function) [10,14].

Одностороння функція (one-way function) — така функція f, за якої знаючи якийсь параметр x легко обчислити f(x), але, знаючи f(x) складно знайти x.

Функція-пастка — одностороння функція, значення аргументу якої легко отримати за допомогою деяких секретних даних.

У асиметричних криптосистемах функція-пастка реалізується наступним чином: користувач P хоче надіслати повідомлення користувачу S. Для цього користувач P бере відкритий текст x (дані якими він хоче поділитися) і шифрує його за допомогою публічного ключа p, отримуючи на виході шифротекст p(x) (p(x) – це результат застосування односторонньої функції. По значеннях p(x) та p, які є відкритими, не можна знайти значення x за поліноміальний час). Отримавши шифротекст p(x), користувач S дешифрує його за допомогою свого секретного ключа s (ключ s знаходиться тільки у користувача S): s(p(x)) = x. Значення s — це секретні дані, які роблять односторонню функцію оберненою.

Асиметричні криптосистеми реалізуються на складності вирішення таких математичних задач:

— Факторизація великих цілих чисел (ПФЧ);
— Дискретне логарифмування у скінченному полі (ПДЛ);
— Дискретне логарифмування на еліптичних кривих (ПДЛЕК).

Алгоритми факторизації або розкладання на множники та дискретного логарифмування у скінченному полі мають експоненційну та субекспоненційну складність [11]. Дискретне логарифмування на еліптичних кривих є експоненційно складним [1,12].

Недоліки асиметричних криптосистем відносно симетричних:

— Повільне шифрування та дешифрування даних;
— Великий розмір ключа;
— Залежність від математичної задачі;
— Чутливість до атаки «людина посередині».

Асиметричні криптосистеми ґрунтуються на використанні деякої кількості взаємопов'язаних ключів. Такі ключі отримуються через вирішення математичних задач, складність яких залежить від величин залучених даних. Аби зашифрувати та розшифрувати дані різними ключами необхідно виконати складні математичні перетворення (функції). Здійснення таких математичних функцій потребує більше часу та обчислювальних ресурсів.

Асиметричні криптосистеми залежать від конкретних математичних задач (проблем). І хоча висока складність таких задач легко досягається за рахунок великої розмірності задіяних ключів, вже існують алгоритми субекспоненційної складності для вирішення деяких з цих проблем [11].

Атака типу «людина посередині» (Man in the middle) є доволі актуальною для асиметричних криптосистем. Вона ґрунтується на тому, що при роздачі публічного ключа зловмисник може перехопити його і замінити на свій публічний ключ. Всі повідомлення, зашифровані таким підробленим публічним ключем, будуть з легкістю розшифровані зловмисником. На сьогодні розроблені методи за допомогою яких можна мінімізувати вплив такого виду атаки (мітки часу, цифровий підпис повідомлення, протокол «тримаючись за руки») [10].

Переваги асиметричних криптосистем перед симетричними:

— Такий вид криптосистем не чутливий відносно рівня безпечності каналу передачі даних. Закритий ключ не передається, а зберігається виключно у свого власника;
— При лінійному збільшенні кількості користувачів, число ключів також має лінійний приріст. У асиметричних алгоритмах кількість задіяних ключів обчислюється за формулою (1.7).

$$N_{ключів} = 2 \cdot N_{користувачів} \quad (1.7)$$

де $N_{ключів}$ — кількість ключів у системі, $N_{користувачів}$ — кількість користувачів у системі.

На рисунку 1.7 зображено графіки залежності кількості ключів від кількості користувачів у симетричній та асиметричній криптосистемах.

Рисунок 1.7 — Залежність кількості ключів від кількості користувачів у різних криптографічних системах

У таблиці 1.4 наведені числові показники збільшення кількості ключів залежно від збільшення користувачів в різних криптосистемах.

Таблиця 1.4 — Залежність кількості ключів у різних криптосистемах від кількості користувачів

Кількість користувачів	Кількість ключів у симетричній системі	Кількість ключів у асиметричній системі
2	1	4
5	10	10
10	45	20
100	4950	200
1000	499500	2000

1.2.3 Гібридні криптосистеми

Симетричні і асиметричні криптосистеми мають свої недоліки і переваги. Асиметричні криптосистеми були створені, щоб компенсувати слабкості симетричних. Натомість, асиметрична криптографія має ряд вразливостей, які відсутні у симетричному шифруванні. Симетрична криптографія має швидку реалізацію, але потребує надійного каналу передачі, навпаки, асиметрична криптографія стійка до ненадійних каналів передачі, але є повільною і ресурсномісткою. Сучасний обмін секретними даними здійснюється з використанням обох криптосистем. Криптосистема, яка об'єднує у собі симетричну і асиметричну криптосистеми називається гібридною (змішаною) криптосистемою. У таких системах симетричні ключі використовуються для шифрування повідомлень у межах одного сеансу (для нового сеансу генерується новий симетричний ключ), а для засекречення сеансових ключів використовуються довгострокові асиметричні ключі. Схема гібридної криптосистеми зображений на рисунку 1.8.

Створення надійної криптосистеми потребує використання симетричних і асиметричних методів шифрування. Подальше розвинення криптографії можливо лише за умови удосконалення цих методів та знаходження нових, стійких до принципово нових загроз.

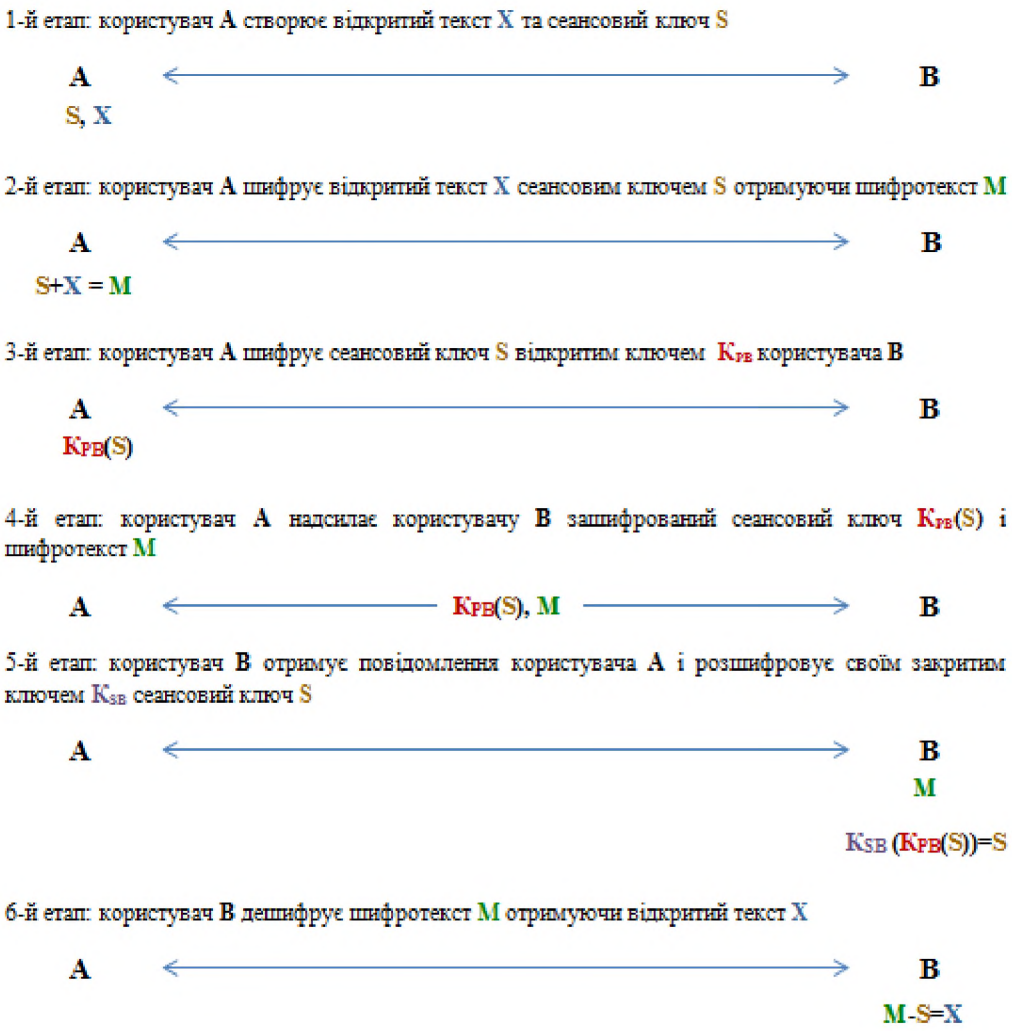


Рисунок 1.8 — Передача даних з використанням гібридної криптосистеми

1.3 Висновки. Постановка задачі

Аналіз можливостей квантових обчислень показує, що при достатній потужності ці обчислювальні технології здатні зруйнувати ефективність сучасних асиметричних криптосистем і скомпрометувати інформацію, яка захищається такими криптосистемами.

Аналіз видів криптосистем демонструє необхідність використання, як симетричних, так і асиметричних алгоритмів шифрування.

Загроза застосування потужних квантових обчислень створює потребу у нових методах побудови квантово-стійких криптографічних конструкцій.

РОЗДІЛ 2
МЕТОДИ ПОБУДОВИ КВАНТОВО-БЕЗПЕЧНИХ КРИПТОСИСТЕМ

2.1 Нові підходи до побудови квантово-безпечних криптосистем

Квантові обчислення стають дедалі популярними. Через можливість масштабування квантових комп'ютерів виникає загроза сучасній криптографії. Зашифрована інформація, яка транспортується сьогодні каналами передачі даних, може бути перехоплена і збережена до моменту, коли буде створений потужний квантовий комп'ютер здатний розшифрувати цю інформацію. Необхідно вже сьогодні починати піклуватися, щодо виникнення приладів такої обчислювальної потужності та готуватися до загрози їхнього застосування.

У 2015 році Європейський Інститут Телекомунікаційних стандартів (ETSI) запустив проект зі створення квантво-стійких криптосистем [21,41]. У 2016 Американський Інститут Стандартизації (NIST) розпочав конкурс на стандартизацію квантово-безпечних алгоритмів [39,40].

Існує декілька параметрів за якими можна визначити критичність ситуації у галузі захисту інформації [21]:

1. час секретності даних — A;

2. час, необхідний для переведення сучасних систем обміну даними на квантово-безпечний рівень — B;

3. час, що залишився до створення потужного квантового комп'ютера — C.

Якщо сума A і B менше значення C, то можна вважати, на сьогоднішній день загрози розшифрування секретних даних шляхом застосування квантових обчислень немає. У випадку, якщо сума A і B більше значення C, загроза існує. Проблема виникає в тому, що час C є достеменно невідомим. Час A для різної секретної інформації може бути різним, в залежності від важливості такої інформації (інформація для службового

користування, конфіденційна інформація, державна таємниця). Зокрема в Україні державна таємниця, в залежності від ступеня секретності, може зберігатися в секретності до 30 років, а у деяких випадках і більше (якщо державний експерт з питань таємниць приймає рішення про продовження строку секретності) [9]. Значення А секретної на сьогодні інформації, вже дорівнює, а у найгіршому випадку, перевищує час, що залишився до реалізації потужних квантових обчислень. Виникнення у майбутньому нової секретної інформації буде лише погіршувати ситуацію. Невідомим залишається значення В: відсутність стандартизованих, на міжнародному рівні, квантово-безпечних криптосистем та складність визначення періоду часу, необхідного для заміни сучасних (квантово-вразливих) криптосистем на квантово-безпечні криптосистеми. Не можна з точністю говорити про жодне значення параметрів А, В та С, але фактом є те, що технологічний розвиток з часом лише прискорюється і на сьогодні всі компанії – гіганти у сфері інформаційних технологій мають свої квантові комп'ютери і витрачають великі кошти на подальші квантові розробки. Кількість інформації, яку необхідно зберігати в таємниці, буде невпинно збільшуватися.

Реалізація алгоритму Шора на потужному квантовому комп'ютері знищіть ефективність криптографії, яка грунтується на використанні проблем факторизації великих цілих чисел та дискретного логарифмування, тобто всю сучасну асиметричну криптографію. Виникає необхідність у використанні принципово інших математичних задач як базису асиметричного шифрування.

На сьогодні відомі такі методи побудови квантово-стійких асиметричних криптосистем [12]:

— Криптографія на основі геш-функцій;

— Криптографія на основі кодів;

— Криптографія на основі решіток;

— Мультиваріативна криптографія;

— Криптографія ізогінеї суперсингулярних еліптичних кривих.

Реалізація алгоритму Гровера не зможе знищити сучасну симетричну криптографію, адже цей алгоритм має лише квадратичне прискорення. Тож симетрична криптографія на сьогодні може вважатися квантово-стійкою. Але через проблему розподілу ключів, симетрична криптографія не може використовуватися самостійно. Цю проблему вирішує асиметрична криптографія, а також квантова криптографія. Квантова криптографія вважається стійкою відносно квантових обчислень, адже грунтується не на математичних задачах, а на законах квантової фізики.

2.2 Квантова криптографія

Квантова криптографія — криптографія, яка базується на принципах квантової фізики, на відміну від звичайної криптографії, заснованої на математичних задачах. У квантовій криптографії один поляризований фотон (або інша найменша частинка) еквівалентний одному біту у звичайній криптографії.

Провідними компаніями у сфері надання послуг квантової криптографії є американська компанія MagiQ [3] та швейцарська компанія ID Quantique [22].

Послугами компанії MagiQ Technologies користуються дуже впливові організації [4], такі, як Агентство передових оборонниxx дослідницьких проектів (DARPA), Національне управління з аеронавтики і дослідження космічного простору (NASA), Міністерство енергетики США (DOE), Військово-морські сили США (USN), що говорить про перспективність квантової криптографії.

ID Quantique (IDQ) є швейцарською компанією, яка надає такі послуги у сфері квантових технологій [22], а саме: квантове шифрування, генерація

випадкових послідовностей на основі квантових явищ, розподіл квантових ключів. У 2001 році ID Quantique розробила перший у світі квантовий генератор випадкових чисел (QRNG) (високий рівень ентропії в таких генераторах досягається імовірнісною природою мікросвіту), а у 2014 генератор випадкових чисел виробництва ID Quantique став першим, який пройшов перевірку за методологією випробувань AIS31, розробленою Федеральним відомством з інформаційної безпеки Німеччини. У 2007 році технології цієї компанії були використані для захисту виборів у кантоні Женева. У 2014 компанією ID Quantique спільно з Женевським університетом встановили світовий рекорд з найдовшої відстані передачі квантових ключів — 307 кілометрів. У 2020 році компанія ID Quantique заявила про інтегрування свого генератора випадкових послідовностей у смартфон Vsmart Aris 5G.

Квантова криптографія використовує найменші частинки для передачі інформації (значення ключа) та такі принципи квантової фізики, як принцип невизначеності Гейзенберга та теорему про заборону клонування.

Принцип невизначеності Гейзенберга (Heisenberg's uncertainty principle) — принцип квантової механіки, який стверджує, що неможна одночасно з однаковою точністю встановити характеристики квантової системи (координати квантової частки та її імпульс) або, що взаємодія з квантовою системою змінює стан цієї системи.

Теорема про заборону клонування — принцип квантової механіки, який стверджує, що неможливо повністю скопіювати систему, параметри якої є невідомими.

2.2.1 Протокол BB84

Першим протоколом квантової криптографії був алгоритм BB84 [18], який був створений у 1984 році Чарльзом Беннеттом (Charles Bennett) і

Жилем Брассаром (Gilles Brassard). Цей алгоритм використовується провідними компаніями з надання послуг квантової криптографії [3,22].

Протокол BB84 — протокол передачі симетричного ключа шифрування, який використовує чотири квантові стани (поляризації) утворюючи з них два базиси: ортогональний, в якому фотон має вертикальну 0° або горизонтальну 90° поляризацію (кут коливань) та діагональний базис, в якому фотон може знаходитись в станах діагональних поляризацій 45° та 135° (таблиця 2.1).

Таблиця 2.1 — Позначення поляризації відносно базису

Ортогональний базис		Діагональний базис	
+		×	
поляризація			
↕	↔	⤡	⤢

Поляризаційні стани відображають 0 або 1 (таблиця 2.2).

Таблиця 2.2 — Встановлення поляризаційного стану відносно значення біта

1		0	
↕	⤢	↔	⤡

Для реалізації протоколу BB84 (як і будь-якого квантового алгоритму) необхідні такі технічні складові:

— Генератор елементарних частинок (для фотонів таким генератором є джерело світла);

— Поляризаційний фільтр;

— Детектор поляризації;
— Ізольований канал передачі даних (кількість «шуму» в такому каналі має бути мінімальною).

Алгоритм BB84 реалізується в декілька етапів.

Перший етап: відправник хоче передати симетричний ключ шифрування отримувачу. Для цього відправник генерує псевдовипадкову послідовність, яка складається з 0 та 1. Використовуючи генератор фотонів відправник створює послідовність фотонів довільної поляризації. В залежності від значення біту у псевдовипадковій послідовності поляризаційний фільтр задає фотонам відповідну поляризацію (таблиця 2.2). Відправник отримує послідовність відповідно поляризованих фотонів (таблиця 2.3).

Другий етап: відправник посилає свою послідовність фотонів отримувачу ізольованим каналом передачі даних. Поляризація фотонів чутлива до зовнішніх подразників, тому для квантової криптографії необхідно використовувати добре ізольовані канали передачі (рисунок 2.1).

Третій етап: Послідовність фотонів надходить до отримувача. Використовуючи поляризаційні детектори отримувач вимірює поляризацію фотонів. Отримувач не знає поляризації фотонів, тому для вимірювання поляризації він використовує детектори різних базисів (ортогонального і діагонального) у довільному порядку. Пройшовши через вірно обраний детектор, фотон не змінює поляризації. Якщо детектор вибирається некоректно (базис детектора не відповідає базису поляризації фотону), то поляризація фотону зміниться відносно базису детектора, і початкову поляризацію фотону неможливо буде встановити. Таким чином близько половини вимірювань будуть правильними (таблиця 2.4).

Четвертий етап: відправник та отримувач з'єднуються звичайним каналом зв'язку. Відправник повідомляє який базис він використав для поляризації кожного фотону, але не повідомляє як саме він поляризував

фотон. Отримувач порівнює правильну послідовність базисів з послідовністю базисів, яка використовувалася ним для детектування поляризаційних станів. Отримувач повідомляє відправнику результати порівняння. Всі неправильно детектовані фотони відкидаються. Залишені (правильно детектовані) фотони переводяться у послідовність біт. Така послідовність використовується як ключ симетричного шифрування у звичайному каналі передачі даних (таблиця 2.4).

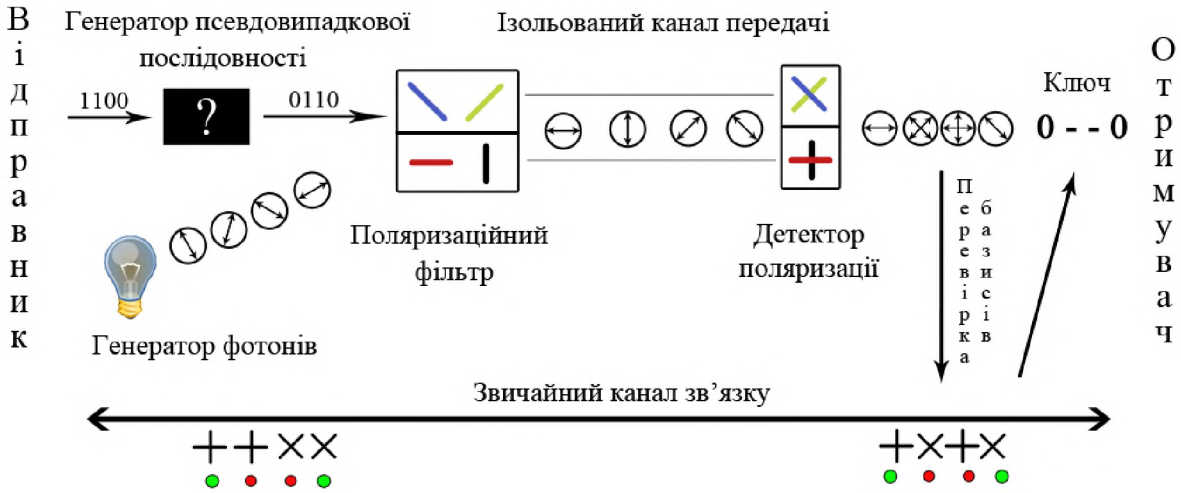


Рисунок 2.1 — Схема розподілу симетричного ключа протоколом BB84

Таблиця 2.3 — Послідовність поляризованих фотонів відправника

Початкова послідовність			
0	1	1	0
Поляризація фотонів			
↔	↕	⤢	⤡

Під час спроби перехоплення даних (послідовності фотонів) зловмисник, як і отримувач, здатен лише робити вимірювання поляризації фотонів використовуючи детектори поляризаційних станів у довільному

порядку. Таким чином зловмиснику буде відома тільки половина послідовності. Для вимірювання поляризації фотонів зловмисник буде використовувати іншу послідовність базисів детектора ніж отримувач. Дані, які отримає зловмисник будуть відмінні від даних, які дійдуть до отримувача (таблиці 2.4, 2.5).

Таблиця 2.4 — Послідовність дій на стороні отримувача

<table>
<tr><td colspan="4">Базис детектора</td></tr>
<tr><td>+</td><td>×</td><td>+</td><td>×</td></tr>
<tr><td colspan="4">Виміряна поляризація</td></tr>
<tr><td rowspan="2">↔</td><td>↗</td><td>↕</td><td rowspan="2">↘</td></tr>
<tr><td>↘</td><td>↔</td></tr>
<tr><td colspan="4">Отримана послідовність біт</td></tr>
<tr><td rowspan="2">0</td><td>1</td><td>1</td><td rowspan="2">0</td></tr>
<tr><td>0</td><td>0</td></tr>
<tr><td colspan="4">Залишені біти</td></tr>
<tr><td>0</td><td>—</td><td>—</td><td>0</td></tr>
</table>

Таблиця 2.5 — Дані отримані зловмисником

Базис детектора			
×	+	×	+
Виміряна поляризація			
			
			
Отримана послідовність біт			
1	1	1	1
0			0
Залишені біти			
—	1	1	—

Квантова криптографія гарантує, що спроба перехопити дані буде завжди виявлена. При вимірюванні поляризації фотонів зловмисник буде використовувати детектори у довільному порядку. Якщо детектор було вибрано неправильно — фотон, пройшовши через нього, змінить свою поляризацію. Це призведе до того, що після вимірювань зловмисника половина фотонів буде перебувати у іншому поляризаційному стані. Коли такі «модифіковані» фотони дійдуть до отримувача, він правильно детектує тільки четверту частину від початкової «чистої» послідовності. Коли відправник зашифрує своє повідомлення і надішле його отримувачу, той не зможе розшифрувати це повідомлення.

За теоремою про заборону клонування зловмисник не зможе скопіювати фотон. Тож зловмисник не має можливості дублювати для себе

послідовність фотонів, а потім, підслухавши по звичайному каналу зв'язку перевірку правильності обраних базисів, дешифрувати цю послідовність.

Щоб не виконувати зайвих дій з пересиланням повідомлення, яке зашифроване «некоректним» ключем (ключ відправника відмінний від ключа отримувача), виконується перевірка на надійність каналу передачі (рисунок 2.2).

Після отримання послідовності і відбору правильно виміряних значень відправник та отримувач роблять перевірку на достовірність даних, що лишилися. Відправник, який володіє правильними даними, звичайним каналом зв'язку повідомляє отримувачу деякі дані з залишеної послідовності. Якщо значення даних, що повідомив відправник, і значення даних, що є у отримувача співпали, то у процесі передачі послідовність не була модифікована. Дані, значення яких було повідомлено, відкидаються, а дані, що лишилися, використовуються як ключ для симетричного шифрування.

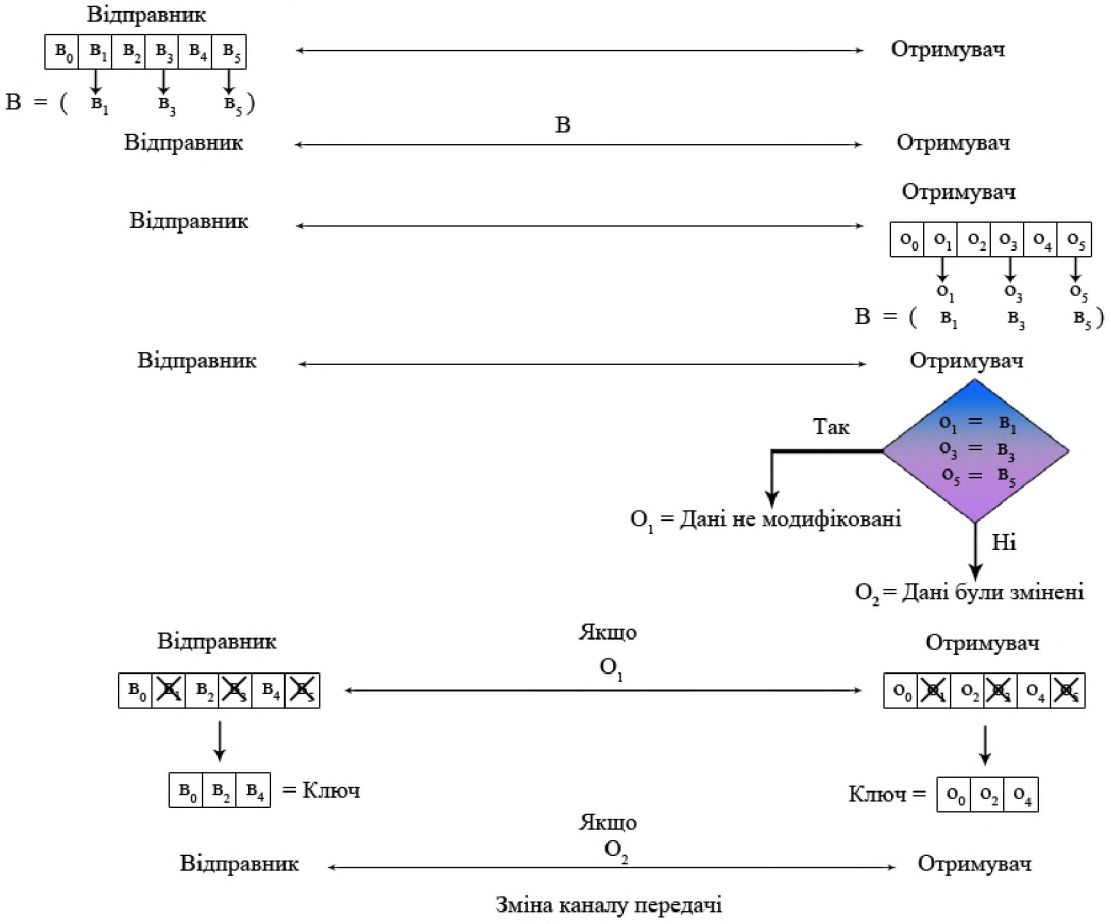


Рисунок 2.2 — Схема перевірки надійності каналу передачі

2.3 Криптографія на основі геш-функцій

2.3.1 Підпис Меркле

Підпис Меркле (Merkle signature scheme) — алгоритм многоразового підпису, який складається з якого-небудь одноразового підпису та дерева Меркле (Merkle tree).

Вперше цей алгоритм був описаний Ральфом Мерклом (Ralph Merkle) у 1979 році з використанням підпису Лампорта (Lamport signature), як одноразового підпису [26]. Дерево Меркле дозволяє за допомогою одного публічного ключа зашифрувати до 2^n різних повідомлень, де n — висота дерева, яку можна застосувати до довільної одноразової системи цифрового підпису [27].

Генерація ключів для підпису Меркле:

Створюються масиви ключів X (закритий) та Y (відкритий). Кожна пара (X_i, Y_i) — це пара закритого та секретного ключів для одноразового підпису.

Побудова дерева Мерле:

Від кожного X_i знаходиться його геш-значення $H(X_i)$, яке є елементом відкритого ключа Y_i, з яких складається початковий рівень дерева a_0. Рівень a_0 містить 2^n елементів. Наступний рівень a_1 складається з 2^{n-1} елементів. Кожен елемент наступного рівня складається з двох елементів попереднього рівня (формула 2.1).

$$a_{i,j} = H\left(a_{i-1,\, j\cdot 2} \,||\, a_{i-1,\, j\cdot 2+1}\right) \qquad (2.1)$$

де || — операція конкатенації (об’єднання), i — номер рівня, j — номер елементу.

Довжина кожного наступного рівня становить 2^{n-i}. Останній рівень a_n буде складатися з одного елементу. Рівень a_n називається коренем дерева і використовується як ключ верифікації підпису (рисунок 2.3).

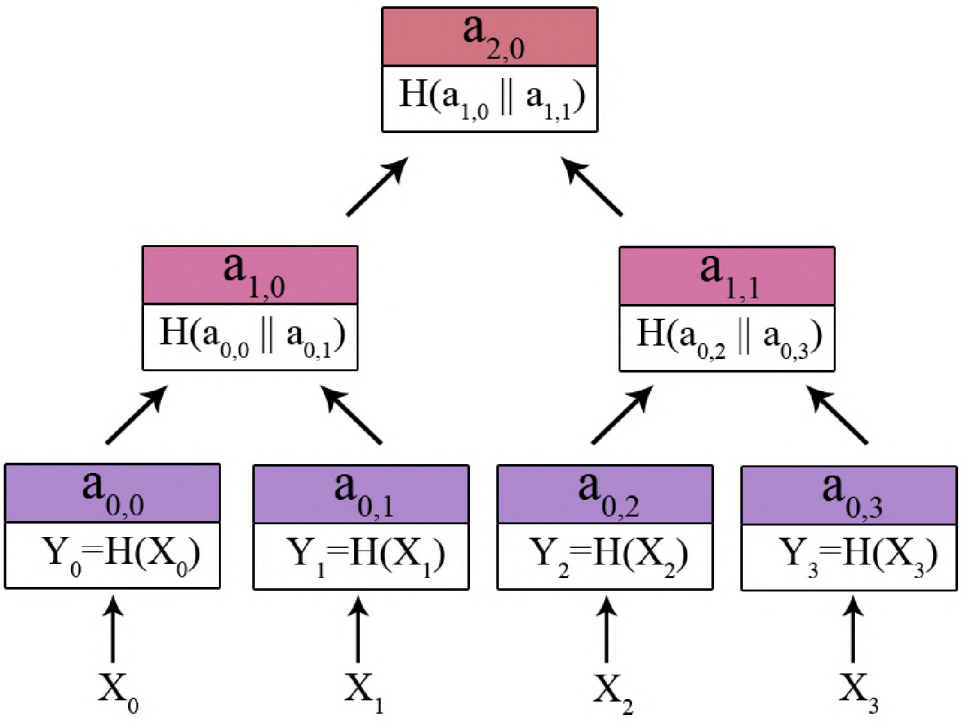


Рисунок 2.3 — Схема дерева Меркле

Процес підписування документу підписом Меркле:

Спочатку обирається закритий ключ X_i. Обчислюється одноразовий підпис Y_i, за допомогою закритого ключа X_i. Для формування підпису Меркле необхідно додати до повідомлення M відкритий ключ Y_i та всі елементи (листя) auth, які утворюють з Y_i та його наступними конкатенаціями суміжні вершини (рисунок 2.4). Підпис Меркле має вигляд: $(M, Y_i, auth_0, \dots, auth_{n-1})$.

Перевірка підпису Меркле:

В першу чергу сторона верифікації перевіряє підпис Y_i. Якщо Y_i дійсний, то починається перевірка по дереву Меркле. Геш-значення відкритого ключа Y_i конкатенують з листям $auth_0$. Геш-значення результату

конкатенації об’єднують з наступним auth. Якщо геш-значення останньої конкатенації співпало з коренем дерева Меркле — підпис дійсний.

Така конструкція є квантово-стійкою, бо її криптографічна стійкість ґрунтується на стійкості геш-функції, яка використовується.

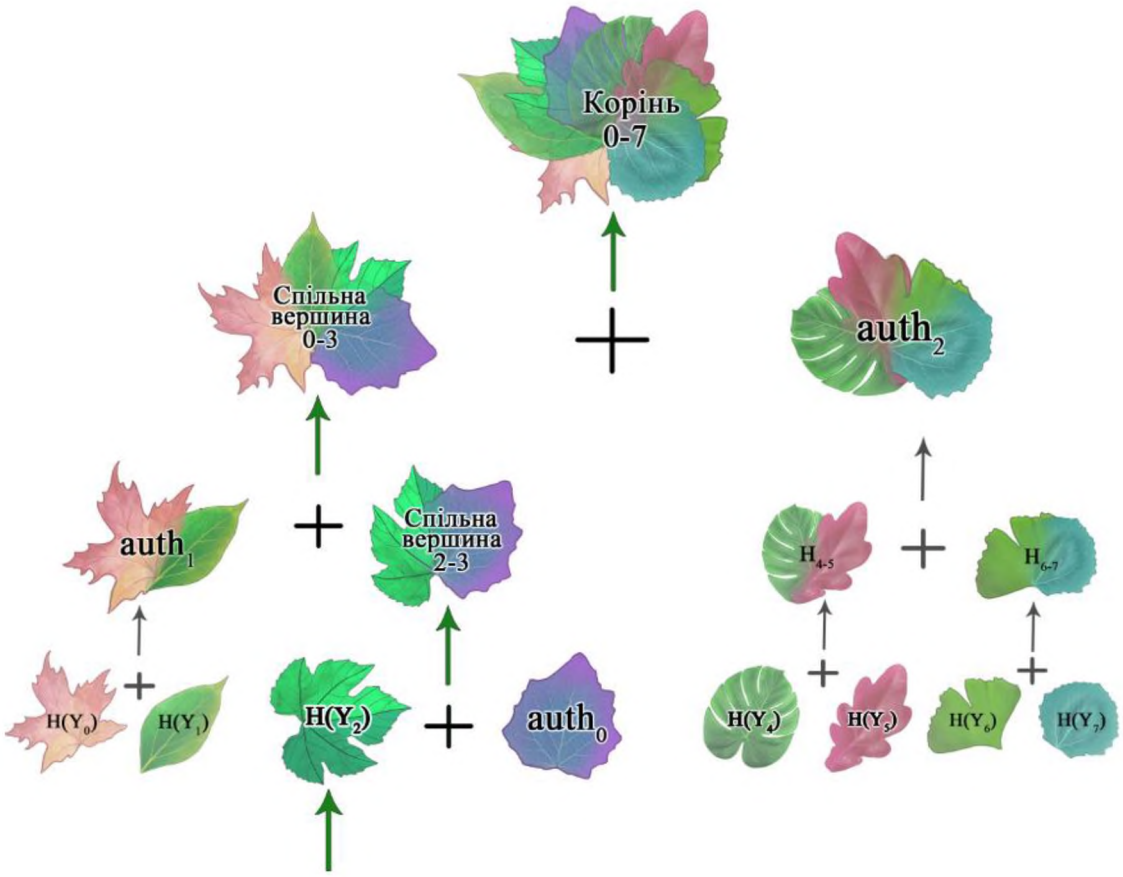


Рисунок 2.4 — Процес формування підпису Меркле

2.3.2 Підпис Лампорта

Підпис Лампорта — криптосистема створена у 1979 році Леслі Лампортом (Leslie Lamport), заснована на стійкості геш-функцій та одноразових ключах.

Генерація закритого і відкритого ключів підпису Лампорта:

Створюється n пар довільно сгенерованих чисел, де n — бітовий розмір виходу для обраної геш-функції. Всі сгенеровані числа перетворюються обраною геш-функцією. В результаті утворюються закритий ключ X —

масив пар довільно сгенерованих чисел і відкритий ключ Y — масив пар геш-значень довільних чисел.

Підпис повідомлення:

Отримується геш-значення повідомлення M. Це значення переводиться у двійкову систему. В залежності від значення біту (0 чи 1), який знаходиться на і-тому місці, до повідомлення M додають перше чи друге число з і-тої пари закритого ключа (рисунок 2.5).

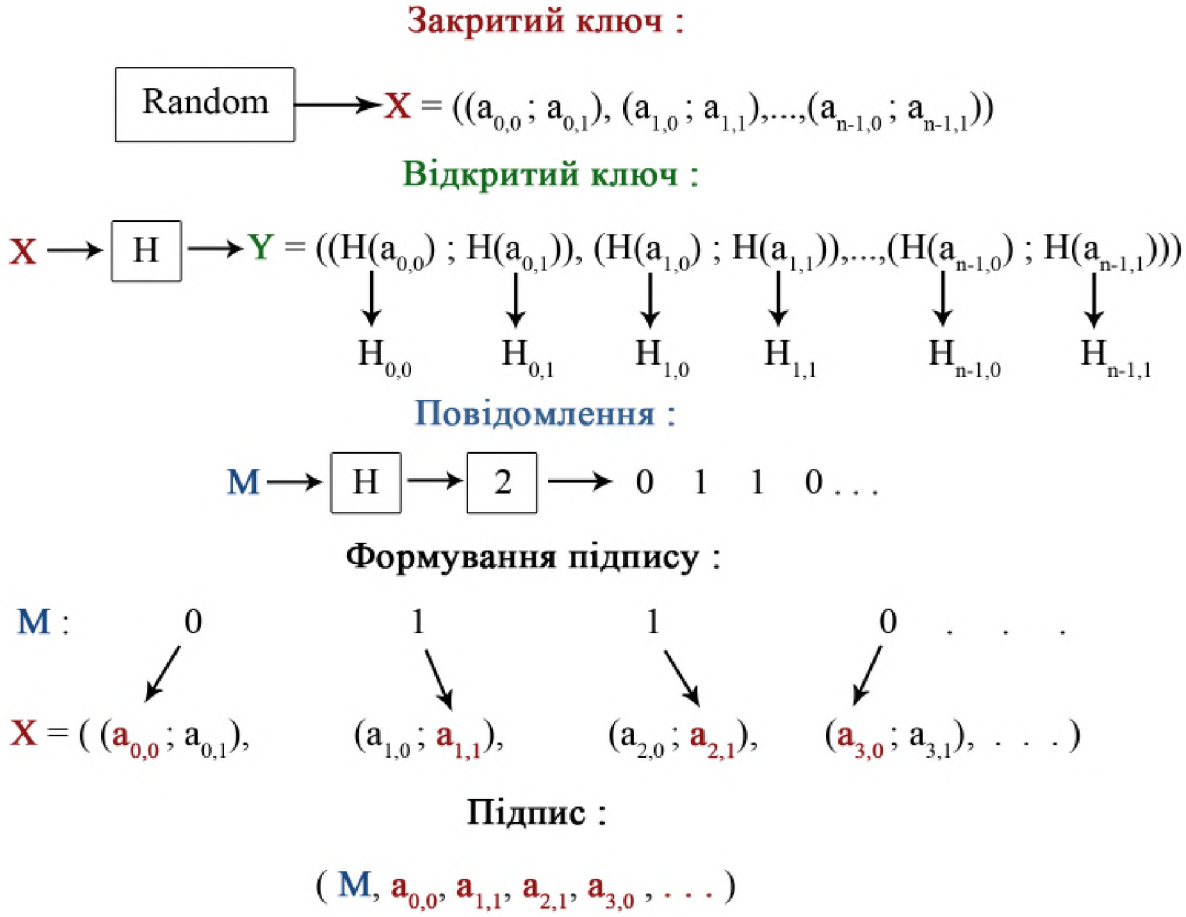


Рисунок 2.5 — Схема формування підпису Лампорта

Перевірка підпису Лампорта:

Спочатку визначається геш-значення повідомлення M. Це геш-значення переводиться у двійкову систему. Знаходиться геш-значення від і-того елементу підпису і, в залежності від значення і-того біту повідомлення (0 чи 1), геш-значення елементу підпису порівнюється з першим чи другим

значенням і-тої пари відкритого ключа Y. Якщо значення співпали — підпис дійсний (рисунок 2.6).

Плюси такого підпису:

— швидкість генерації підпису та її перевірки;
— простота реалізації;
— стійкість відносно квантових обчислень.

Мінус підпису Лампорта полягає в тому, що для кожного нового документу необхідно генерувати новий ключ. Цей мінус виправляється деревом Меркла [28].

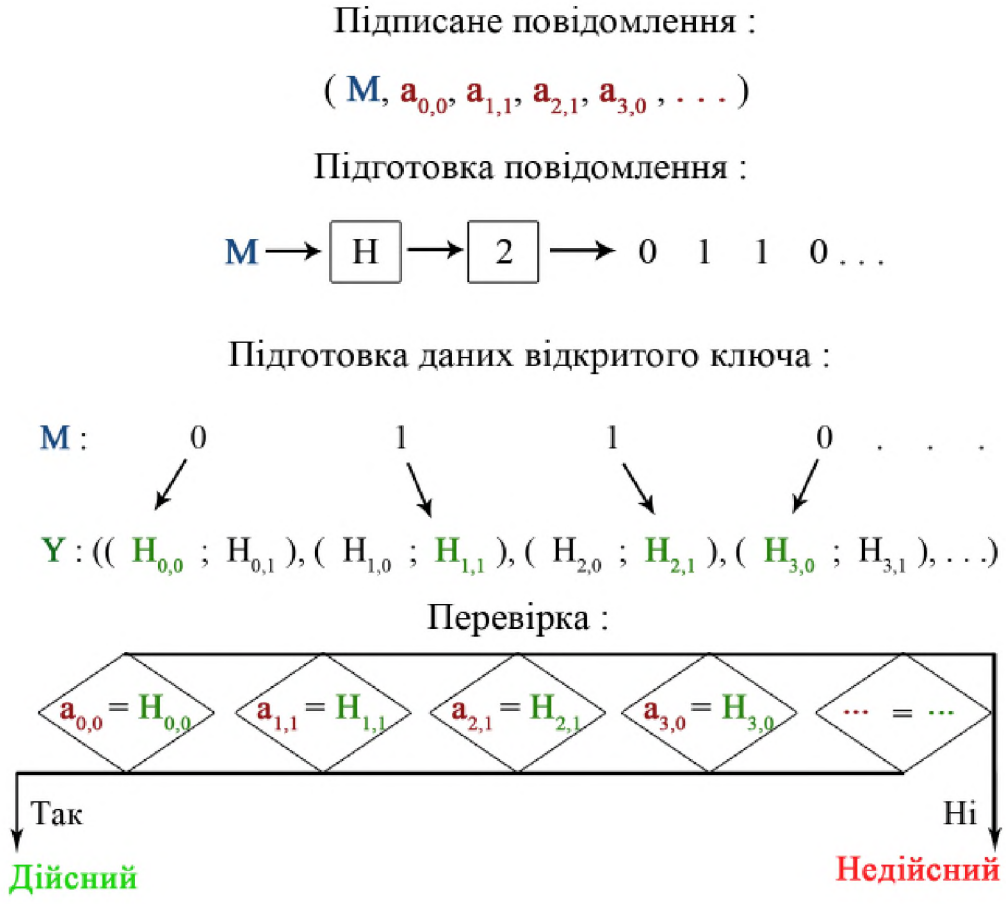


Рисунок 2.6 — Схема перевірки підпису Лампорта

2.4 Криптографія кодів виправлення помилок

Криптографія кодів використовує коди, для яких існують алгоритми швидкого виправлення помилок. Такі коди маскують під випадкові (для яких немає швидких коригуючих алгоритмів) і передають каналами зв'язку.

Найбільш відомими криптосистемами на базисі кодів є система McEliece, запропонована в 1978 році Робертом Дж. Макелісом (Robert J. McEliece) та система Нідеррайтера (Niederreiter cryptosystem), запропонована у 1986 році Гарольдом Нідеррайтером (Harald Niederreiter), яка є модифікованою версією системи McEliece.

2.4.1 Криптосистема McEliece

Криптосистема McEliece заснована на складності декодування повних лінійних кодів. Зазвичай в якості лінійного коду використовують коди Гоппа (Goppa code) [30].

Криптосистема McEliece складається з трьох етапів [29]:

1. Генерація ключів;
2. Випадкове шифрування;
3. Детерміноване розшифрування.

Текстом повідомлення є вектор довжиною k над скінченним полем GF(q).

Генерація ключів:

Обирається лінійний код C з параметрами (n, k) (рисунок 2.7), який виправляє t помилок. Для коду C обчислюється породжуюча матриця G (матриця, що складається з усіх базисних векторів лінійного коду C) розмірністю k на n.

Генерується випадкова невироджена матриця S (визначник матриці не дорівнює нулю) розмірністю k на k — для складності відновлення початкового коду.

$$C(n, k) = \{\overbrace{011...010}^{n}, \overbrace{010...001}^{n}, \ldots \overbrace{110...111}^{n}\}$$
$$2^k$$

Рисунок 2.7 — Представлення коду C, який містить 2^k кодових слів довжиною n біт.

Генерується випадкова матриця перестановки P (матриця, в якій кожен рядок і стовпець має один одиничний елемент) розмірністю n на n.

Обчислюється матриця G_{pub} розмірністю k на n, яка є добутком матриць S, G та P.

Пара (G_{pub}, t) — це відкритий ключ.

Матриці (S, G, P) — це закритий ключ.

Всі користувачі системи McEliece використовують параметри n, k, t.

Випадкове шифрування:

Нехай абонент B хоче відправити повідомлення M абоненту O. Відкритим ключем абонента O є пара (G_{pub}, t).

Спочатку абонент B перетворює повідомлення M у послідовність двійкових символів довжиною k.

Абонент B генерує випадковий вектор z довжиною n з вагою Хеммінга (Hamming weight) t (число ненульових елементів).

Шифрування повідомлення M відбувається за формулою (2.2).

$$c_в = M \cdot G_{pub} + z \qquad (2.2)$$

де $c_в$ — шифротекст.

Далі $c_в$ передається каналом зв'язку абоненту О.

Детерміноване розшифрування:

Отримавши шифротекст $c_в$ абонент О обчислює обернену матрицю P^{-1} та знаходить вектор c_o за формулою (2.3).

$$c_o = c_в \cdot P^{-1} \tag{2.3}$$

Потім абонент О знаходить повідомлення М за формулою 2.4.

$$M = D \cdot c_o \cdot G^{-1} \cdot S^{-1} \tag{2.4}$$

де D — алгоритм швидкого декодування коду С, який виправляє до t кількості помилок.

У системі McEliece породжуюча матриця коду — це відкритий ключ. Шифротекст отримується шляхом маскування повідомлення (кодового слову) під випадковий код.

Суть такої криптографії полягає в тому, що за поліноміальний час неможливо декодувати псевдовипадковий код. Дані про відкритий ключ не можуть бути використані для знаходження швидкого алгоритму декодування.

Криптографія на основі кодів виправлення помилок має свої плюси та мінуси [31].

Мінуси криптографії на основі кодів:

— Великий розмір відкритого ключа;
— Шифротекст в рази більший ніж відкритий текст.

Плюси криптографії на основі кодів:

— Процеси шифрування та розшифрування реалізуються швидше деяких популярних на сьогоднішній день криптосистем;
— Квантова безпечність.

Квантова безпечність криптографії кодів виправлення помилок досягається використанням випадкових елементів (випадковий вектор z, невироджена матриця S).

2.5 Криптографія на основі решіток

Криптографія на основі решіток — асиметрична криптографія, яка будується на складності задачі теорії решіток [32].

Задачі теорії решіток:

— Задача знаходження найкоротшого вектора — SPV;
— Задача знаходження (приблизно) ідеального найкоротшого вектора — ISVP;
— Задача знаходження (приблизно) найкоротшого незалежного вектора — SIVP;
— Задача знаходження найближчого вектору — CVP.

2.5.1 Криптосистема NTRU

Криптосистема NTRU (Nth-degree TRUncated polynomial ring) — це криптосистема асиметричного шифрування, запропонована у 1996 році. У криптосистемі NTRU всі операції здійснюються у кільці усічених многочленів (кільце многочленів з визначеними операціями додавання і

множення). Криптографічна стійкість NTRU базується на складності задачі знаходження найкоротшого вектору — SPV.

Для реалізації криптосистеми NTRU використовують цілі числа N, p та q. Числа p та q — це модулі за якими виконуються визначені арифметичні операції в кільці усічених многочленів. Необхідно щоб у чисел p та q не було спільних дільників. Базовими об'єктами NTRU є многочлени порядку N-1. Криптостійкість NTRU залежить від розміру N.

Генерація ключів:

Обираються многочлени f та g з вибраного кільця усічених многочленів. Многочлен f повинен мати обернений елемент за модулем p та q. Якщо многочлен f не відповідає цій умові — такий многочлен має бути замінений.

Обчислюються обернені елементи до многочлена f за модулями p — f_p^{-1} та q — f_q^{-1}. Пара (f, f_p^{-1}) — це секретний ключ.

За формулою (2.5) розраховується відкритий ключ h.

$$h = (p \cdot f_q^{-1} \cdot g) \bmod q \qquad (2.5)$$

Шифрування:

Нехай h — відкритий ключ абонента O. Абонент B хоче відправити повідомлення M абоненту O.

Абонент B представляє повідомлення M у вигляді многочлену з коефіцієнтами по модулю p. Всі коефіцієнти многочлену повинні знаходитися в інтервалі від мінус q/2 до q/2 включно. Якщо коефіцієнти не будуть знаходитися у потрібному інтервалі, то розшифроване повідомлення

може відрізнятися від зашифрованого. Абонент B довільним чином обирає многочлен r. Шифрування повідомлення M відбувається за формулою (2.6).

$$E = (r \cdot h + M) \bmod q \tag{2.6}$$

де E — шифротекст.

Розшифрування:

Отримавши шифротекст E абонент O знаходить повідомлення M за формулою (2.7).

$$M = ((f \cdot E) \cdot f_p^{-1}) \bmod p \tag{2.7}$$

Криптосистема NTRU володіє рядом особливостей [2,33].

Мінуси NTRU:

— Шифротекст більше початкового тексту в декілька разів;
— Чутливість до обраних параметрів.

Плюси NTRU:

— Невелика кількість операцій для шифрування та розшифрування;
— Велика швидкість генерації ключів;
— Велика швидкість шифрування та розшифрування;
— Можливість використання для цифрового підпису і шифрування повідомлень;
— Квантова безпечність.

Криптосистема NTRU підходить для використання у вбудованих системах (embedded system) [34].

2.6 Мультиваріативна криптографія

Мультиваріативна криптографія — це асиметрична криптографія, яка побудована на вирішенні рівнянь, заснованих на багатомірних многочленах над скінченним полем [36].

Базовими об'єктами мультиваріативної криптографії є квадратичні поліноміальні рівняння в скінченному полі F_q (q — це кількість елементів в полі) (рисунок 2.8).

$$p_1(x_1, \ldots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij} \cdot x_i \cdot x_j + \sum_{i=1}^{n} p_i \cdot x_i + p_{01}$$

$$p_2(x_1, \ldots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij} \cdot x_i \cdot x_j + \sum_{i=1}^{n} p_i \cdot x_i + p_{02}$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$p_m(x_1, \ldots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij} \cdot x_i \cdot x_j + \sum_{i=1}^{n} p_i \cdot x_i + p_{0m}$$

Рисунок 2.8 — Базові об'єкти мультиваріативної криптографії

Безпека мультиваріативної криптографії заснована на складності вирішення проблеми MQ (MQ Problem), яка вважається NP-повною задачею.

Проблема MQ складає:

Дано m квадратичних многочленів $p_1(x)$, . . . , $p_m(x)$ з n кількістю перемінних x_1, . . . , x_n. Необхідно знайти такий вектор v, щоб виконувалась формула (2.8).

$$p_1(v) = \ldots = p_m(v) = 0 \qquad (2.8)$$

Однією з найбільш вивчених та перспективних реалізацій багатовимірної криптографії є алгоритм прихованих рівнянь поля (Hidden Field Equation, HFE), запропонований Жаком Патаріном (Jacques Patarin) у 1996 році [37]. Цей алгоритм використовує поліноми над скінченними полями різного розміру для приховування зв'язку між публічним та приватним ключами.

Приватний ключ в схемі прихованих рівнянь поля складається з приватного полінома P та двох афінних перетворень S та T, що накладаються послідовно.

Генерація публічного ключа p проводиться з використанням складових приватного ключа (S, P, T). Згенерований таким чином публічний ключ використовується для шифрування повідомлень.

Мультиваріативна криптографія володіє наступними властивостями:

— Швидкість генерації ключів та шифрування і розшифрування алгоритмів мультиваріативної криптографії здатна перевищувати швидкість деяких сучасних асиметричних криптосистем [38];
— Невибагливість до обчислювальних потужностей. Операції, які використовуються доволі прості, тому алгоритми мультиваріативної криптографії можуть бути ефективно реалізовані на таких обчислювальних пристроях, як смарт-карти і радіочастотні мітки (криптосистеми TTS та Rainbow мають гарні показники для використання їх на пристроях з обмеженими обчислювальними потужностями [29]).
— Мала величина розміру цифрового підпису (декілька сотень біт).

2.7 Криптографія ізогенії суперсингулярних еліптичних кривих

Еліптичні криві E, які використовуються в криптографії визначені на скінченному полі, разом з умовною точкою нескінченності, всі елементи якого задовольняють формулі (2.9).

$$y^2 = x^3 + ax + b \tag{2.9}$$

Параметри a та b разом з вибором початкової точки визначають криптографічну схему. Важливою характеристикою кривої є j-інваріант, що розраховується за формулою (2.10).

$$j(E) = 1728\frac{4a^3}{4a^3+27b^2} \tag{2.10}$$

Приватним ключем є ціле число k, з якого з використанням параметрів кривої та початкової точки P розраховується публічний ключ Q формулою (2.11) як результат точкової мультиплікації на кривій. Стійкість алгоритму визначається стійкістю проблеми знаходження дискретного логарифму.

$$Q = P \cdot k \tag{2.11}$$

Криптографія на еліптичних має численні переваги над поширеною криптографією на базі методу RSA як у ефективності, так і у розмірі ключа. З іншого боку, складність алгоритмів та проблема вибору безпечних кривих додають труднощів у реалізації та сумнівів у безпеці.

Разом з численними перевагами та готовністю до використання у рамках існуючої криптографічної інфраструктури, еліптична криптографія, як і криптографія на базі алгоритму RSA є квантово нестійкою, як і всі схеми, що покладаються на проблему дискретного логарифму. Незважаючи на це, виявляється можливим створення постквантової криптографічної схеми з використанням ізогенії суперсингулярних еліптичних кривих (суперсингулярної ізогенії).

Одним з напрямків використання суперсингулярної ізогенії є обмін сеансовими ключами за протоколом Діффі-Гелмана [42, 43].

Сильною стороною всіх реалізацій протоколів Діффі-Гелмана є цілковита пряма секретність (perfect forward secrecy), яка означає, що компрометація довготривалого ключа не означає компрометацію сеансових ключів і не призводить до розкриття даних з попередніх сеансів завдяки тому, що ключі для кожної сесії генеруються окремо з використанням випадкових чисел.

Ізогенія (ізоморфізм) — це окремий випадок гомоморфізму, при якому одна точка еліптичної кривої E_1 є відображенням тільки однієї точки кривої E_2.

Гомоморфізмом називається відображення точок кривої E_1 у точки іншої кривої E_2. Якщо взяти будь-які дві точки кривої E_1 (a_1; b_1) та відобразити їх у дві точки іншої еліптичної кривої E_2 (a_2; b_2), то сума точок a_1 та b_1 буде дорівнювати сумі точок a_2 та b_2.

Суперсингулярні криві мають перевагу над звичайними у швидкості обчислень, однак для постквантової криптографії визначальним є те, що ізогенія ординарних кривих не є квантово стійкою. На відміну від Діффі-Гелмана на звичайних еліптичних кривих, де використання суперсингулярних кривих робить шифрування вразливим через можливість розрахунку у цьому випадку дискретного логарифму, суперсингулярна

ізогенія безпечна щодо цього виду атак, тому що складна проблема в цьому випадку не пов'язана з дискретними логарифмами.

Криптографічна стійкість алгоритмів, що базуються на ізогенії еліптичних кривих, обумовлена обчислювальною складністю знаходження ізогенії для двох кривих.

2.8 Рекомендації щодо імплементації квантово-безпечних криптосистем

Квантова криптографія може бути використана для розподілу симетричних (сеансових) ключів шифрування. Така криптосистема є квантово-безпечною, але має дорогу та складну реалізацію. На сьогодні квантова криптографія може ефективно використовуватися установами, які працюють з державною таємницею.

Криптографія на основі геш-функцій може використовуватись для формування квантово-безпечного підпису. Але через необерненість геш-функцій не може використовуватися як система шифрування з подальшим розшифруванням даних.

Криптографія на основі кодів виправлення помилок ефективна для систем шифрування даних. До того ж, така криптографія дозволяє маскувати дані під випадкові послідовності. Цифровий підпис такими криптосистемами вважається неефективним через свою дороговизну.

Криптографія на решітках може бути ефективна як для цифрового підпису, так і для шифрування даних. Криптосистеми на основі решіток за швидкістю своєї реалізації перевищують деякі сучасні асиметричні криптосистеми. Невибагливість до обчислювальних потужностей робить такий тип криптосистем перспективним для використання у вбудованих системах.

Мультиваріативна криптографія характеризується простотою задіяних операцій та швидкодією виконуваних процесів, що робить її реалізацію ефективною на пристроях з обмеженими обчислювальними потужностями. Зокрема, швидка генерація ключів робить такий тип криптосистем перспективним для цифрового підпису.

Заміною класичного та еліптичного протоколу Діффі-Гелмана є нова версія цього протоколу на основі ізогенії суперсингулярних еліптичних кривих. Новий протокол Діффі-Гелмана володіє всіма перевагами попередніх версій, але на відміну від них, є квантово-безпечним.

2.9 Висновки до другого розділу

У другому розділі дипломної роботи проаналізовані існуючі на даний час методи побудови квантово-безпечних криптосистем.

Наведені обґрунтовані рекомендації щодо застосування квантово-безпечних криптосистем.

РОЗДІЛ 3
ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ ВПРОВАДЖЕННЯ КРИПТОГРАФІЧНИХ КОНСТРУКЦІЙ, СТІЙКИХ ДО КВАНТОВИХ ОБЧИСЛЕНЬ

3.1 Вступ

Метою економічного розділу є обґрунтування економічної доцільності розробки і впровадження криптографічних систем, стійких до загрози застосування квантових обчислень.

Для визначення ефективності необхідно виконати наступні етапи:

1. Розрахунок капітальних витрат на придбання і налагодження складових криптографічних систем або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення.
2. Розрахунок річних експлуатаційних витрат на утримання і обслуговування криптографічних систем.
3. Визначення річного економічного ефекту від впровадження криптографічних систем.
4. Визначення та аналіз показників економічної ефективності запропонованих в дипломній роботі криптографічних систем.
5. Висновок про економічну доцільність запропонованих криптографічних систем.

3.2 Розрахунок фіксованих (капітальних) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

У роботі було запропоновано два підходи до створення квантово-безпечної криптографії :

1. Квантовий розподіл ключів та симетрична криптографія;

2. Постквантова криптографія та симетрична криптографія.

Симетрична криптографія не потребує капітальних інвестицій позаяк вона вже масово використовується в інформаційних системах. Капітальні інвестиції необхідні для квантової і постквантової криптосистем.

На сьогодні існують компанії, які надають послуги квантової криптографії, тож немає потреби в розробці нових методів та алгоритмів. У підході з використанням квантової криптографії інвестування направлені на послуги аутсорсингу цих компаній та закупівлі необхідного обладнання.

Деякі методи постквантової криптографії не стандартизовані, тож у підході з використанням криптосистем такого типу інвестиції можуть бути направлені на розробку нових алгоритмів, їхню стандартизацію та введення в експлуатацію.

Капітальні витрати у підході з використанням квантової криптографії:

— Витрати на залучення компаній, які надають послуги квантової криптографії;
— Вартість первісних закупівель ліцензійного основного й додаткового програмного забезпечення;
— Витрати на закупівлю апаратного забезпечення;
— Витрати на інтеграцію криптографічних систем у вже існуючу корпоративну систему;
— Витрати на навчання технічних фахівців і обслуговуючого персоналу.

Капітальні витрати у підході з використанням постквантової криптографії:

— Вартість розробки політики функціонування криптосистеми;
— Витрати на залучення зовнішніх консультантів;
— Вартість створення ліцензійного основного й додаткового програмного забезпечення;
— Витрати на первісні закупівлі програмного забезпечення;

— Витрати на стандартизацію розроблених алгоритмів;
— Витрати на інтеграцію криптографічних систем у вже існуючу корпоративну систему;
— Витрати на навчання технічних фахівців і обслуговуючого персоналу.

3.2.1 Визначення витрат на створення програмних засобів криптографічного захисту на основі постквантових криптосистем

Для розрахунку вартості розробки і використання програмного забезпечення криптографічних систем необхідно виконати наступні етапи:

— Визначення трудомісткості розробки та опрацювання програмного забезпечення;
— Розрахунок витрат на створення програмного продукту;
— Оцінка швидкодії та надійності роботи програмного продукту.

3.2.1.1 Визначення трудомісткості розробки та опрацювання програмного продукту (постквантових алгоритмів)

Трудомісткість створення програмного забезпечення визначається тривалістю кожної робочої операції (формула (3.1)).

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д} \text{ , годин.} \qquad (3.1)$$

де ttз – тривалість складання технічного завдання на розробку програмного забезпечення;

tв – тривалість вивчення ТЗ, літературних джерел;

tа – тривалість розробки блок-схеми алгоритму;

tпр – тривалість програмування за готовою блок-схемою;

tопр – тривалість опрацювання програми на ПК;

tд – тривалість підготовки технічної документації на програмне забезпечення.

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті Q (формула (3.2)).

$$Q = q \cdot c \cdot (1+p), \text{ штук.} \qquad (3.2)$$

де q – очікувана кількість операторів;

c – коефіцієнт складності програмного забезпечення;

p – коефіцієнт корекції програмного забезпечення у процесі опрацювання.

Коефіцієнт складності програмного забезпечення c, що розробляється, відносно типового завдання складатиме:

$$c = 2,0$$

Корекція функціонування програмного забезпечення для криптографічних систем можлива за рахунок недостатньої дослідженості таких систем та за рахунок збільшення кола користувачів. Коефіцієнт корекції p складатиме:

$$p = 0,1$$

Очікувана кількість операторів програми q складає:

$$q = 100$$

Умовна кількість операторів у програмі складатиме:

$$Q = 100 \cdot 2,0 \cdot (1+0,1) = 220 \text{ (штук)}$$

Тривалість складання технічного завдання на розробку програмного забезпечення ttз становить:

$$t_{тз} = 100 \text{ (годин)}$$

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення технічного завдання і кваліфікації програміста оцінюється за формулою (3.3).

$$t\text{в} = \frac{Q \cdot B}{(75...85) \cdot k} \text{, годин.} \quad (3.3)$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом, k = 1,1.

Враховуючи відповідні значення коефіцієнтів, значення tв має вигляд:

$$t\text{в} = \frac{220 \cdot 1{,}5}{(75...85) \cdot 1{,}1} = 4 \text{ (години)}$$

Тривалість розробки блок-схеми алгоритму розраховується за формулою (3.4).

$$t\text{а} = \frac{220 \cdot 1{,}5}{(75...85) \cdot 1{,}1} \text{, годин.} \quad (3.4)$$

Параметр tа складатиме:

$$t\text{а} = \frac{220}{(20...25) \cdot 1{,}1} = 10 \text{ (годин)}$$

Тривалість складання програми за готовою блок-схемою tпр обчислюється за формулою (3.5).

$$t\text{пр} = \frac{Q}{(20...25) \cdot k} \text{, годин.} \quad (3.5)$$

Параметр tпр складатиме:

$$t\text{пр} = \frac{220}{(20...25)\cdot 1{,}1} = 10 \text{ (годин)}$$

Тривалість опрацювання програми на ПК tопр обчислюється за формулою (3.6).

$$t\text{опр} = \frac{1{,}5 \cdot Q}{(4...5) \cdot k} \text{, годин.} \qquad (3.6)$$

Параметр tопр складатиме:

$$t\text{опр} = \frac{1{,}5 \cdot 220}{(4...5) \cdot 1{,}1} = 75 \text{ (годин)}$$

Тривалість підготовки технічної документації на програмне забезпечення tд обчислюється за формулою (3.7).

$$t\text{д} = \frac{Q}{(15...20) \cdot k} + \frac{Q}{(15...20)} \cdot 0{,}75 \text{ , годин.} \qquad (3.7)$$

Параметр tд складатиме:

$$t\text{д} = \frac{220}{(15...20) \cdot 1{,}1} + \frac{220}{(15...20)} \cdot 0{,}75 = 24{,}3 \text{ (годин)}$$

Трудомісткість створення програмного забезпечення складатиме:

$$t = 100 + 4 + 10 + 10 + 75 + 24{,}3 = 223{,}3 \text{ (години)}$$

3.2.2 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення Ззп і вартості витрат

машинного часу, що необхідний для опрацювання програми на ПК Змч (формула (3.8)).

$$Кпз = (Ззп + Змч) \cdot N , грн. \quad (3.8)$$

де N – кількість фахівців (5).

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби і визначається за формулою (3.9).

$$Ззп = t \cdot Зпр, грн. \quad (3.9)$$

де t – загальна тривалість створення програмного забезпечення;

Зпр – середньогодинна заробітна плата програміста.

Середньогодинна заробітна платня розробника програмного забезпечення складає 250 грн/годину.

Витрати на заробітну плату виконавця Ззп складають:

$$Ззп = 223,3 \cdot 250 = 55825 (грн)$$

Вартість машинного часу для налагодження криптосистеми визначається за формулою (3.10).

$$Змч = tопр \cdot Смч + tд, грн. \quad (3.10)$$

де tопр – трудомісткість налагодження всіх необхідних операцій на ПК, годин;

tд – трудомісткість підготовки документації на ПК, годин;

Смч – вартість 1 години машинного часу ПК, грн/година.

Вартість 1 години машинного часу ПК Смч визначається за формулою (3.11).

$$Смч = Р \cdot Се + \frac{Фзал \cdot На}{Fp} + \frac{Клпз \cdot Напз}{Fp}, \text{ грн.} \quad (3.11)$$

де Р – встановлена потужність ПК, кВт (0,5);

Се – тариф на електричну енергію, грн/кВт · година (1,68);

Фзал – залишкова вартість ПК на поточний рік, грн (6000);

На – річна норма амортизації на ПК, частки одиниці (0,2);

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці (0,2);

Клпз – вартість ліцензійного програмного забезпечення, грн (5000);

Fp – річний фонд робочого часу (за 40-годинного робочого тижня Fp дорівнює 1920).

Параметр Смч складатиме:

$$Смч = 0,5 \cdot 1,68 + \frac{6000 \cdot 0,2}{1920} + \frac{5000 \cdot 0,2}{1920} = 1,985 \text{ (грн/год)}$$

Параметр Змч складатиме:

$$Змч = 75 \cdot 1,985 + 24,3 = 173,175 \text{ (грн)}$$

Параметр Кпз складатиме:

$$Кпз = (55825 + 173,175) \cdot 5 = 279\,990,875 \text{ (грн)}$$

Визначена вартість створення програмного забезпечення для імплементації криптосистем Кпз є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури для впровадження криптосистем.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта криптосистем К обчислюються за формулою (3.12).

$$К = Кпр + Кзпз + Кпз + Каз + Кнавч + Кн \quad (3.12)$$

де Кпр – вартість розробки криптосистеми та залучення для цього зовнішніх консультантів, тис. грн;

Кзпз – вартість закупівель ліцензійного основного і додаткового програмного забезпечення, тис. грн;

Кпз – вартість створення основного і додаткового програмного забезпечення, тис. грн;

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

Кн – витрати на встановлення обладнання та налагодження криптосистеми, тис. грн.

Для кожного з підходів побудови квантово-стійких криптографічних систем капітальні витрати розраховуються окремо.

Капітальні витрати у підході з використанням квантової криптографії Кк розраховуються за формулою (3.13).

$$Кк = Кпр,н + Кзпз + Каз + Кнавч \quad (3.13)$$

де Кпр,н – вартість залучення зовнішніх консультантів, встановлення обладнання та налагодження криптосистеми (аутсорсинг), тис. грн (100 000);

Кзпз – вартість закупівель ліцензійного основного і додаткового програмного забезпечення, тис. грн (100 000);

Каз – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн (500 000);

Кнавч – витрати на навчання технічних фахівців, тис. грн (20 000).

Параметр Кк складатиме:

Кк = 100 000 + 100 000 + 500 000 + 20 000 = 720 000 (тис. грн)

Капітальні витрати у підході з використанням постквантової криптографії Кп розраховуються за формулою (3.14).

$$Кп = Кзпз + Кпз + Кнавч + Кн \quad (3.14)$$

де Кзпз – вартість закупівель ліцензійного основного і додаткового програмного забезпечення для розробки і тестування криптоалгоритмів, тис. грн (10 000);

Кпз – вартість розробки постквантових алгоритмів, тис. грн (280 000);

Кнавч – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн (20 000);

Кн – витрати на стандартизацію криптосистеми, тис. грн (60 000).

Параметр Кп складатиме:

Кп = 10 000 + 280 000 + 20 000 + 60 000 = 370 000 (тис. грн)

3.3. Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

До поточних витрат відносять наступні витрати:

— Вартість відновлення і модернізації криптосистеми (Св);

— Витрати на керування криптосистемою в цілому (Ск);

— Витрати, викликані активністю користувачів криптосистеми (Сак).

До витрат Ск можна віднести:

— Навчання адміністративного персоналу й кінцевих користувачів;

— Амортизаційні відрахування від вартості обладнання та програмного забезпечення;

— Заробітна плата обслуговуючого персоналу;

— Аутсорсинг;

— Навчальні курси і сертифікація обслуговуючого персоналу;

— Технічне і організаційне адміністрування і сервіс.

До витрат Ск можна віднести:

— Пряма допомога і додаткові настроювання;

— Формальне навчання;

— Розробка додатків;

— Робота з даними;

— Неформальне навчання;

— Futz-фактор (обсяг витрат, пов'язаних з наслідками некомпетентних дій користувача).

Річні поточні (експлуатаційні) витрати на функціонування криптосистеми С обчислюються за формулою (3.15).

$$C = Св + Ск + Сак, \text{ тис. грн.} \qquad (3.15)$$

Витрати на відновлення і модернізацію криптосистеми Св та витрати викликані активністю користувачів квантової криптосистеми Сак покладаються на компанію з аутсорсингу.

Для квантової криптосистем річні витрати С можуть бути обчислені із значення витрат Ск.

Витрати на керування криптосистемою Ск обчислюються за формулою (3.16).

$$Ск = Сн + Са + Сз + Се + Со + Стос, грн. \quad (3.16)$$

де Сн – витрати на навчання адміністративного персоналу і кінцевих користувачів;

Са – річний фонд амортизаційних відрахувань;

Сз – річний фонд заробітної плати інженерно-технічного персоналу;

Се – вартість електроенергії за рік;

Со – витрати на залучення сторонніх організацій;

Стос – витрати на технічне і організаційне адміністрування та сервіс.

Значення параметрів для підходу з використанням квантової криптографії:

Сн = 20 000 (грн/рік)

Са = $\frac{720\ 000}{20\ років}$ = 36 000 = 5 % від капітальних затрат = 0,05 (20 років – запланований час експлуатації криптосистеми)

Значення параметру Сз обчислюється за формулою (3.17).

$$Сз = Зосн + Здод, грн. \quad (3.17)$$

де Зосн, Здод – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова — в розмірі 8-10% від основної заробітної плати. Якщо заробітна плата обчислюється для декількох працівників — місячний посадовий оклад помножується на кількість задіяних працівників.

Значення параметрів для квантової криптосистеми:

Основна заробітна плата працівників – 30 000 грн;

Кількість основних працівників – 5 чоловік;

$$Зосн = 30\,000 \cdot 5 \cdot 12 = 1\,800\,000 \text{ (грн/рік)}$$

Додаткова заробітна плата – 3 000 грн;

Кількість додаткових працівників – 3 чоловік;

$$Здод = 3\,000 \cdot 3 \cdot 12 = 108\,000 \text{ (грн/рік)}$$

Параметр Сз складає:

$$Сз = 1\,800\,000 + 108\,000 = 1\,908\,000 \text{ (грн)}$$

Вартість електроенергії, що споживається апаратурою квантової криптосистеми протягом року Се обчислюється за формулою (3.18).

$$Се = Р \cdot Fр \cdot Це, \text{ грн.} \qquad (3.18)$$

де Р – встановлена потужність апаратури квантової криптосистеми, кВт (1,6);

Fр – річний фонд робочого часу криптосистеми (8757 год/рік (365 днів на 24 годин, з урахуванням часу простою – 3 години/рік);

Це – тариф на електроенергію, грн/кВт на годину (1,68).

Параметр Се складає:

$$Се = 1{,}6 \cdot 8757 \cdot 1{,}68 = 23\,539 \text{ (грн)}$$

Параметр Со для квантової криптосистеми складає 50 000 (грн/рік) (40 000 (грн/рік) на послуги аутсорсингу, 10 000 (грн/рік) на навчання працівників).

Витрати Стос визначаються у відсотках від вартості капітальних витрат:

$$Стос = 21\,600 \text{ (грн)}$$

Витрати на керування квантовою криптосистемою Ск складають:

$$Ск = 20\,000 + 0{,}05 + 1\,908\,000 + 23\,539 + 50\,000 + 21\,600 = 2\,023\,139{,}05 \text{ (грн)}$$

Річні поточні (експлуатаційні) витрати С на квантову криптосистему складають:

$$С = 2\ 023\ 139,\ 05\ (грн)$$

Значення параметрів для підходу з використанням постквантової криптографії:

Сн = 20 000 (грн/рік)

Са = $\frac{370\ 000}{20\ років}$ = 18 500 = 5 % від капітальних затрат = 0,05 (20 років – запланований час експлуатації криптосистеми)

Основна заробітна плата працівників – 30 000 грн;

Кількість основних працівників – 3 чоловік;

$$Зосн = 60\ 000 \cdot 3 \cdot 12 = 1\ 080\ 000\ (грн/рік)$$

Параметр Сз складає:

$$Сз = 1\ 080\ 000\ (грн)$$

Встановлена потужність апаратури постквантової криптосистеми Р, кВт (0,5);

Річний фонд робочого часу криптосистеми Fр (8757 год/рік (365 днів на 24 годин, з урахуванням часу простою – 3 години/рік);

Тариф на електроенергію Це, грн/кВт на годину (1,68).

Параметр Се складає:

$$Се = 0,5 \cdot 8757 \cdot 1,68 = 7\ 355\ (грн)$$

Параметр Со для постквантової криптосистеми складає 10 000 (грн/рік).

Витрати Стос складають 11 100 (грн).

Витрати на керування постквантовою криптосистемою Ск складають:

$$Ск = 20\ 000 + 0,05 + 1\ 080\ 000 + 7\ 355 + 10\ 000 = 1\ 117\ 355\ (грн)$$

Витрати на відновлення і модернізацію постквантової криптосистеми Св та витрати викликані активністю користувачів квантової криптосистеми Сак не відносяться до поточних витрат, адже на етапі розробки

постквантових алгоритмів повинні враховуватися можливі навантаження і атаки на систему. Модернізація постквантової криптосистеми потребує нової стандартизації, що відноситься до етапу розробки (капітальні витрати).

Річні поточні (експлуатаційні) витрати С для постквантової криптосистеми складають:

$$C = 1\ 117\ 355 \text{ (грн)}.$$

3.4 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

3.4.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

- $t_п$ – час простою вузла корпоративної мережі, у годинах;
- $t_в$ – час, необхідний для відновлення системи, у годинах;
- $t_{ві}$ – час відновлення інформації, у годинах;
- $З_0$ – заробітна платня обслуговуючого персоналу;
- $З_с$ – заробітна платня співробітників атакованого вузла;
- $Ч_0$ – чисельність обслуговуючого персоналу;
- $Ч_с$ – чисельність співробітників атакованого вузла;
- О – обсяг продажів атакованого вузла, у грн.;
- П – вартість доопрацювання, модифікації програмного забезпечення чи апаратного устаткування;
- I – число атакованих вузлів;

  N – середнє число атак на рік.

Втрати від простою атакованого вузла можна визначити за формулою (3.19).

$$U = Пп + Пв + V, \quad (3.19)$$

де Пп – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв – вартість відновлення працездатності вузла або сегмента корпоративної мережі, грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки і розраховуються за формулою (3.20).

$$Пп = \frac{\sum Зс}{F} \cdot tп, \quad (3.20)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 годин).

Весь обмін електронною інформацією здійснюється з використанням криптосистем. Якщо криптосистема буде несправна — вся електронна інформація буде скомпрометована. Це призведе до зупинки всіх робочих процесів компанії, і задіяння всієї робочої сили на відновлення криптосистеми.

При кількості працівників компанії — 100 осіб, та середній заробітній платні у 25000 грн, число витрат на оплату робочого часу при зламу криптосистеми складатимуть:

$$Пп = \frac{2\ 500\ 000}{176} = 14\ 204,\ 54\ (грн)$$

Витрати на відновлення працездатності системи Пв обчислюються за формулою (3.21).

$$Пв = Пви + Ппв + Пзч, \quad (3.21)$$

де Пви – витрати на повторне введення інформації, грн;

Ппв – витрати на відновлення системи, грн;

Пзч – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників компанії Зс, які зайняті введенням втраченої інформації, з урахуванням необхідного для цього часу tві (формула (3.22)).

$$Пви = \frac{\sum Зс}{F} \cdot tві, \quad (3.22)$$

Показник Пви складає:

$$Пви = \frac{2\ 500\ 000 \cdot 20}{176} = 284\ 091 \text{ (грн)}$$

Витрати Ппв визначаються часом відновлення після атаки tв і розміром середньогодинної заробітної плати персоналу (формула (3.23)).

$$Ппв = \frac{\sum Зо}{F} \cdot tв, \quad (3.23)$$

Витрати Ппв для постквантової криптосистеми складають:

$$Ппв = \frac{250 \cdot 5 \cdot 20}{176} = 142 \text{ (грн)}$$

Витрати Ппв для квантової криптосистеми покладаються на аутсорсинг.

Витрати на заміну обладнання Ппз квантової криптографії покладаються на компанію з аутсорсингу.

Параметр Пв для квантової криптосистеми складає:

$$Пв = 284\ 091 + 142 = 284\ 233\ (грн)$$

Параметр Пв для постквантової криптосистеми складає:

$$Пв = 284\ 091\ (грн)$$

Витрати на заміну обладнання Ппз постквантової криптографії не становлять нових витрат, позаяк постквантові криптосистеми можуть бути реалізовані без закупівлі нового обладнання.

Витрати V визначаються із середньогодинного обсягу продажів і сумарного часу простою системи (формула (3.24)).

$$V = \frac{О}{Fr} \cdot (tп + tв + tви), \qquad (3.24)$$

де Fr – річний фонд часу роботи компанії (становить близько 2080 годин).

Для розрахунку обсягу продажів компанії використовується формула (3.25).

$$О = (Пт + Пб) \cdot Пкт\ , \qquad (3.25)$$

де Пт – вартість проведення транзакції, грн (10 000);

Пб – сума яку отримує банк за кожну транзакцію, % (10);

Пкт - кількість транзакцій оброблених у момент часу, од./хв (100).

Параметр О складає:

$$О = (10\ 000 + 1\ 000) \cdot (100 \cdot 60) = (10\ 000 + 1\ 000) \cdot 6\ 000 = 66\ 000\ 000\ (грн)$$

Параметр V складає (20 годин – час простою системи):

$$V = \frac{66\ 000\ 000}{2080} \cdot 20 = 634\ 615\ (грн)$$

Параметр U для квантової криптосистеми складає:

$$U = 14\,204 + 284\,233 + 634\,615 = 933\,052 \text{ (грн)}$$

Параметр U для постквантової криптосистеми складає:

$$U = 14\,204 + 284\,091 + 634\,615 = 932\,910 \text{ (грн)}$$

Загальний збиток B обчислюється за формулою (3.26).

$$B = \sum i \sum n\, U, \tag{3.26}$$

Параметр B для квантової системи становить:

$$B = 5 \cdot 20 \cdot 933\,052 = 93\,305\,200 \text{ (грн)}$$

Параметр B для постквантової системи становить:

$$B = 5 \cdot 20 \cdot 932\,910 = 93\,291\,000 \text{ (грн)}$$

3.4.2 Загальний ефект від впровадження квантово-безпечних систем

Загальний ефект від впровадження квантово-безпечних криптосистем визначається з урахуванням ризиків порушення інформаційної безпеки і обчислюється за формулою (3.27).

$$E = B \cdot R - C, \tag{3.27}$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію комплексу, тис. грн.

Параметр E для квантової криптографії складає:

$$E = 93\,305\,200 \cdot 0{,}2 - 2\,023\,139 = 16\,637\,901 \text{ (грн)}$$

Параметр E для постквантової криптографії складає:

$$E = 93\ 291\ 000 \cdot 0{,}2 - 1\ 117\ 355 = 17\ 540\ 845 \text{ (грн)}$$

3.5. Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності впровадження рекомендацій, здійснюється на основі визначення та аналізу наступних показників:

а) коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

б) термін окупності капітальних інвестицій То.

Ключовою перевагою показника ТСО є те, що він дозволяє зробити висновки про доцільність реалізації проекту в області інформаційної безпеки на підставі оцінки одних тільки витрат.

Показник сукупної вартості володіння (ТСО) використовується, якщо величину відверненого збитку від атаки на вузол або сегмент компанії важко або неможливо визначити у вартісній формі.

У цьому випадку необхідно порівняти сукупну вартість володіння, розраховану для двох варіантів проектного рішення щодо створення або удосконалення системи інформаційної безпеки, і вибрати варіант із найменшою з них.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі (формула (3.28)).

$$\text{ROSI} = \frac{E}{K}, \quad \text{частки одиниці,} \tag{3.28}$$

де Е – загальний ефект від впровадження квантово-безпечної криптосистеми, тис. грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Показник ROSI для квантової криптосистеми складає:

$$\text{ROSI} = \frac{16\,637\,901}{720\,000} = 23{,}1$$

Показник ROSI для постквантової криптосистеми складає:

$$\text{ROSI} = \frac{17\,540\,845}{370\,000} = 47{,}4$$

Порівнюючи показники ROSI для квантової і постквантової криптосистем, можна зробити висновки, що постквантова криптосистема є економічно вигіднішою. Надалі буде використовуватися показник ROSI для постквантової криптосистеми.

Потужність квантових обчислень буде спрямована на великі компанії, вартість інформації яких, перевищує вартість реалізації квантової атаки. Такі компанії спроможні провести перекваліфікацію криптосистем за власний рахунок.

Проект визнається економічно доцільним, якщо значення ROSI перевищує величину бажаної норми прибутковості альтернативних варіантів вкладення коштів з урахуванням інфляції (формула (3.29)).

$$\text{ROSI} > \frac{N\text{деп} - N\text{інф}}{100}, \qquad (3.29)$$

де Nкр – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, % (20);

Nінф – річний рівень інфляції, % (4,1).

Результат нерівності становить:

$$47{,}4 > 0{,}159$$

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження постквантових криптосистем і обчислюється за формулою (3.30).

$$\text{То} = \frac{\text{Е}}{\text{К}} = \frac{1}{ROSI}\text{, років,} \qquad (3.30)$$

Показник То для постквантової криптосистеми складає:

$$\text{То} = \frac{1}{47{,}4} = 0{,}021 \text{ (років)}$$

(за умови створення потужних квантових комп'ютерів)

3.6 Висновок до економічного розділу

В результаті розрахунку витрат на реалізацію квантово-безпечних криптографічних конструкцій, було виявлено, що постквантова криптографія є економічно вигіднішою ніж квантова криптографія. Розмір капітальних витрат на постквантову криптографію становить 370 000 (грн), а щорічні експлуатаційні витрати — 1 117 355 (грн).

Коефіцієнт повернення інвестицій ROSI демонструє, що одна гривня капітальних інвестицій приносить 47,4 (грн) додаткового прибутку.

Загальний ефект від впровадження постквантової криптосистеми визначається з урахуванням ризиків порушення інформаційної безпеки і становить 17 540 845 (грн).

За умови, що потужні квантові комп'ютери будуть реалізовані, застосування конструкцій постквантової криптографії допоможе запобігти збиткам у розмірі до 93 291 000 (грн/рік) та окупиться за 0,021 рік.

ВИСНОВКИ

У дипломній роботі були розроблені рекомендації щодо застосування квантово-безпечних криптосистем. В ході розв'язання поставлених у дипломній роботі задач були отримані наступні наукові та практичні результати:

1. Проведено аналіз наукових розробок, публікацій, літератури та обґрунтована необхідність розробки та імплементації квантово-безпечних криптосистем;
2. Проаналізовані методи побудови квантово-безпечних криптосистем;
3. Розроблені рекомендації щодо застосування квантово-безпечних криптосистем;
4. Обґрунтована економічна доцільність імплементації квантово-безпечних криптосистем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Полторак В.П., Голков В.Б. Порівняльний аналіз систем електронного цифрового підпису та особливості їх реалізації на еліптичних кривих. 2013. URL: http://it-visnyk.kpi.ua/wp-content/uploads/2014/07/58_13.pdf.

2. Stefan Heyse. Post quantum cryptography: implementing alternative public key schemes on embedded devices. 2013. URL: https://www.emsec.ruhr-uni-bochum.de/media/attachments/files/2014/03/thesis-stefan-heyse.pdf .

3. MagiQ QPN. Ultimate Cryptography Solution for Network Security. [Електронний ресурс]. URL: https://www.magiqtech.com/solutions/network-security.

4. MagiQ Technologies, Inc. [Електронний ресурс]. 2020. URL: https://en.wikipedia.org/wiki/MagiQ_Technologies,_Inc.

5. National Academies of Sciences, Engineering, and Medicine 2018. Quantum Computing: Progress and Prospects. URL: http://cs.brown.edu/courses/csci1800/sources/2018_NAE_QuantumComputing_ProgressAndProspects.pdf.

6. С.А. Дуплий, И.И. Шаповал. Топологические методы в квантовых вычислениях. Национальный научный центр — Харьковский Физико-Технический Институт. 2007.

7. Закон Мура [Електронний ресурс]. 2020. URL: https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%BE%D0%BD_%D0%9C%D1%83%D1%80%D0%B0.

8. D-Wave Systems [Електронний ресурс]. 2020. URL: https://uk.wikipedia.org/wiki/D-Wave_Systems#cite_note-MITreview-8.

9. Закон України «Про державну таємницю» № 3856-XII від 21.01.94: Стаття 13. Строк дії рішення про віднесення інформації до державної таємниці [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

10. Брюс Шнайер. Прикладная криптография. 2-е издание. 2016. 610 с.

11. О. Н. Василенко. Теоретико-числовые алгоритмы в криптографии. 2003. URL: http://www.dut.edu.ua/uploads/l_1108_51986491.pdf.

12. Ю.І. Горбенко, Р.С. Ганзя. Аналіз стійкості постквантових криптосистем. 2014. URL: https://openarchive.nure.ua/bitstream/document/4837/1/268-274.pdf.

13. Ключ (криптография) [Електронний ресурс]. 2020. URL: https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F).

14. Ю. А. Тарнавський. Технології захисту інформації. 2018. URL: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf.

15. Amir Fruchtman and Iris Choi. Technical Roadmap for Fault-Tolerant Quantum Computing. University of Oxford. 2016. URL: https://nqit.ox.ac.uk/sites/www.nqit.ox.ac.uk/files/2016-11/NQIT%20Technical%20Roadmap.pdf.

16. Принцип суперпозиції (квантова механіка). [Електронний ресурс]. 2020. URL:https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF_%D1%81%D1%83%D0%BF%D0%B5%D1%80%D0%BF%D0%BE%D0%B7%D0%B8%D1%86%D1%96%D1%97_(%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D0%B0_%D0%BC%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%BA%D0%B0).

17. A Preview of Bristlecone, Google's New Quantum Processor. [Електронний ресурс]. 2018. URL: https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html.

18. Саймон Сингх. Книга шифров. 2006. URL: http://www.vixri.com/d/Singx%20Sajmon%20_Kniga%20shifrov.pdf.

19. D-Wave Systems. [Електронний ресурс].URL: https://www.dwavesys.com/.

20. О. П. Кобушкін. Квантова механіка. 2016. URL: https://ela.kpi.ua/bitstream/123456789/18348/1/Kvantova_mexanika_Kobushkin.pdf.

21. ETSI (European Telecommunications Standards Institute). Quantum Safe Cryptography and Security. [Електронний ресурс]. 2015. URL: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

22. ID Quantique. [Електронний ресурс]. 2020. URL: https://www.idquantique.com/.

23. Карлаш Г.Ю. Квантові інформаційні системи. Київський національний університет імені Тараса Шевченка. 2018. URL: http://rex.knu.ua/wp/wp-content/uploads/2018/05/QIS_Karlash.pdf.

24. Quantum Circuits. [Електронний ресурс]. 2020. URL: https://docs.microsoft.com/en-us/quantum/concepts/circuits?view=qsharp-preview.

25. Квантовый логический вентиль - Quantum logic gate. [Електронний ресурс]. 2020. URL: https://ru.qaz.wiki/wiki/Quantum_logic_gate.

26. Ralph Charles Merkle. Secrecy, authentication, and Public key systems. 1979. URL: http://www.merkle.com/papers/Thesis1979.pdf.

27. Ю. И. Воронин. Система электронной подписи. 2017. URL: https://core.ac.uk/download/pdf/217189939.pdf.

28. Nigel P. Smart. Cryptography and Coding. 2005. URL: https://www.researchgate.net/profile/Gerard_Cohen/publication/220963109_A_Trellis-Based_Bound_on_21Separating_Codes/links/00b4952b0b8b1399d5000000.pdf#page=105.

29. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen. Post-Quantum Cryptography. 2009. URL: https://www.researchgate.net/profile/Nicolas_Sendrier/publication/226115302_CodeBased_Cryptography/links/540d62d50cf2df04e7549388/Code-Based-Cryptography.pdf.

30. Suanne Au, Christina Eubanks-Turner, Jennifer Everson. The McEliece Cryptosystem. 2003. URL: http://www.math.unl.edu/~s-jeverso2/McElieceProject.pdf.

31. Применение помехоустойчивых кодов в криптографии. [Електронний ресурс] .2015. URL: http://cryptowiki.net/index.php?title=%D0%9F%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE%D0%BC%D0%B5%D1%85%D0%BE%D1%83%D1%81%D1%82%D0%BE%D0%B9%D1%87%D0%B8%D0%B2%D1%8B%D1%85_%D0%BA%D0%BE%

D0%B4%D0%BE%D0%B2_%D0%B2_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D0%B8.

32. Криптография на решётках. [Електронний ресурс]. 2020. URL: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F_%D0%BD%D0%B0_%D1%80%D0%B5%D1%88%D1%91%D1%82%D0%BA%D0%B0%D1%85.

33. Priit Karu, Jonne Loikkanen. Practical Comparison of Fast Public-key Cryptosystems. 2001. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.5694&rep=rep1&type=pdf.

34. Быстрые криптосистемы с открытым ключом. [Електронний ресурс]. 2019.URL: https://ru.wikipedia.org/wiki/%D0%91%D1%8B%D1%81%D1%82%D1%80%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC.

35. Jintai Ding. Current State of Multivariate Cryptography. 2017. URL: https://www.researchgate.net/publication/319170467_Current_State_of_Multivariate_Cryptography.

36. Jintai Ding, Bo-Yin Yang. Multivariate Public Key Cryptography. 2009. URL: https://www.iis.sinica.edu.tw/papers/byyang/12734-F.pdf.

37. J. Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms. 1996. URL: http://www.minrank.org/hfe.pdf.

38. Anna Inn-Tung Chen, Ming-Shing Chen, Tien-Ren Chen, Chen-Mou Cheng, Jintai Ding, Eric Li-Hsiang Kuo, Frost Yu-Shuang Lee, Bo-Yin Yang. SSE Implementation of Multivariate PKCs on Modern x86 CPUs. 2009. URL: https://link.springer.com/chapter/10.1007/978-3-642-04138-9_3.

39. NIST. Post-Quantum Cryptography. Round 3 Submissions. [Електронний ресурс]. 2020. URL: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions.

40. PQCrypto 2016. [Електронний ресурс]. 2016. URL: https://pqcrypto 2016.jp/.

41. ETSI launches Quantum Safe Cryptography specification group. [Електронний ресурс]. 2015. URL: https://www.etsi.org/newsroom/news/947-2015-03-news-etsi-launches-quantum-safe-cryptography-specification-group.

42. L. d. Feo, D. Jao, J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. 2011. URL: https://eprint.iacr.org/2011/506.pdf.

43. Craig Costello, Patrick Longa, Michael Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. URL:https://www.researchgate.net/profile/Patrick_Longa/publication/301749413_Efficient_Algorithms_for_Supersingular_Isogeny_DiffieHellman/links/57994b7708aed51475e8915b/Efficient-Algorithms-for-Supersingular-Isogeny-Diffie-Hellman.pdf.

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	22	
6	А4	2 Розділ	27	
7	А4	3 Розділ	22	
8	А4	Висновки	1	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.docx

2 Завдання.docx

3 Реферат.docx

4 Список умовних скорочень.docx

5 Зміст.docx

6 Вступ.docx

7 Розділ 1.docx

8 Розділ 2.docx

9 Розділ 3.docx

10 Висновки.docx

11 Перелік посилань.docx

12 Додаток А.docx

13 Додаток Б.docx

14 Додаток В.docx

15 Додаток Г.docx

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Методи побудови криптографічних конструкцій, стійких до загрози застосування квантових обчислень

студентки групи 125м-19-1
Омелаєнко Анастасії Геннадіївни

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 91 сторінці та містить 16 рисунків, 9 таблиць, 43 джерела та 4 додатка.

Актуальність теми полягає в необхідності підвищення рівня криптографічної захищеності інформації від загрози застосування квантових обчислень.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Авторка показала достатній рівень володіння теоретичними положеннями з обраної теми та здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було розглянуто можливості квантових обчислень та загрози, що вони становлять для інформаційної безпеки. Було розглянуто види криптосистем, проаналізовано їх переваги та недоліки. Був проведений ґрунтовний аналіз методів побудови квантово-безпечних криптографічних систем та наведені рекомендації щодо їх застосування.

Робота написана грамотною мовою, оформлена у відповідності до діючих вимог і містить необхідний ілюстрований матеріал. Авторка добре знає проблему та уміє вирішувати практичні завдання.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог “Положення про систему виявлення та запобігання плагіату”.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а її авторка Омелаєнко А.Г. заслуговує на оцінку «_____».

Керівник дипломної роботи,
к.т.н. доц. Герасіна О.В.

Керівник спец. частини
ст. викл. Войцех С.І.