ІНТЕЛЕКТУАЛЬНА СИСТЕМА КРИПТОГРАФІЧНОГО ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ

Дипломний проект

122 – «Комп’ютерні науки та інформаційні технології»

Виконав: студент гр. 1КН-16сп

Підгорний В.А

Науковий керівник: Озеранський В.С.

МЕТОЮ ДОСЛІДЖЕННЯ *Є ПІДВИЩЕННЯ РІВНЯ ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ.*

ОБ'ЄКТ ДОСЛІДЖЕННЯ – ДОСЛІДЖЕННЯ Є ПРОЦЕСИ ШИФРУВАННЯ І РОЗШИФРУВАННЯ ДАНИХ.

ПРЕДМЕТ ДОСЛІДЖЕННЯ – Є ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ.

ДЛЯ ДОСЯГНЕННЯ МЕТИ НЕОБХІДНО ВИКОНАТИ НАСТУПНІ ЗАДАЧІ ПОДАЛЬШОГО ДОСЛІДЖЕННЯ :

1. Обґрунтування вибору методу шифрування цифрової інформації.
2. Розробка алгоритмів шифрування і розшифрування цифрової інформації.
3. Проектування та програмна реалізація криптографічної системи.
4. Тестування криптографічної системи.
5. Розробка інструкції користувача.

ОБҐРУНТУВАННЯ МЕТОДУ РОЗВ'ЯЗАННЯ ЗАДАЧІ КРИПТОГРАФІЧНОГО ЗАХИСТУ ЦИФРОВОЇ ІНФОРМАЦІЇ

Нейрокріптографія – розділ криптографії, що вивчає застосування стохастичних алгоритмів, зокрема, нейронні мережі, для шифрування і криптоаналізу.

Переваги нейронних мереж в криптографії:

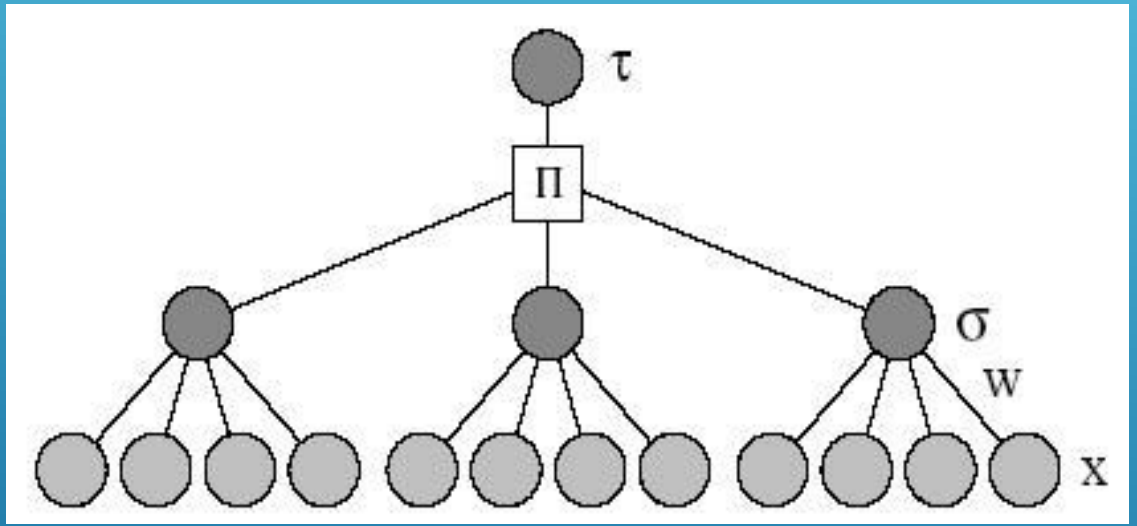
- взаємне навчання
- самонавчання
- стохастична поведінка
- низька чутливість до шуму.

Вони дозволяють вирішувати проблеми криптографії з відкритим ключем, розподілу ключів, хешування і генерації псевдовипадкових чисел.

СТРУКТУРА НЕЙРОННОЇ МЕРЕЖІ

Була обрана нейронна мережа TPM (tree parity machines) – вид багаторівневої нейронної мережі прямого поширення.

Архітектура TPM



Переваги мережі прямого поширення:

- програмні та апаратні реалізації моделі дуже прості;
- простий і швидкий алгоритм навчання;

СХЕМА АЛГОРИТМУ РОБОТИ НЕЙРОННОЇ МЕРЕЖІ

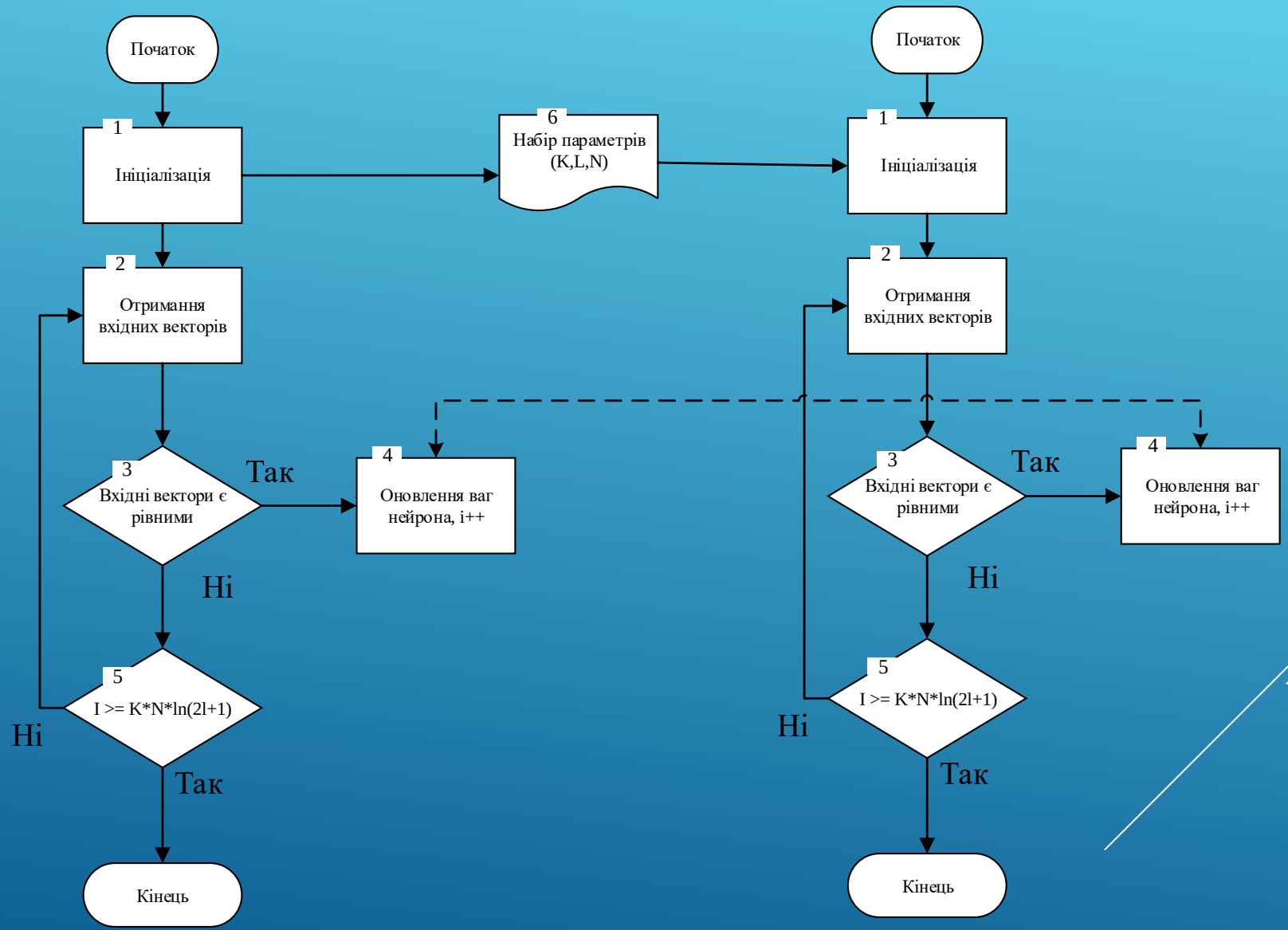
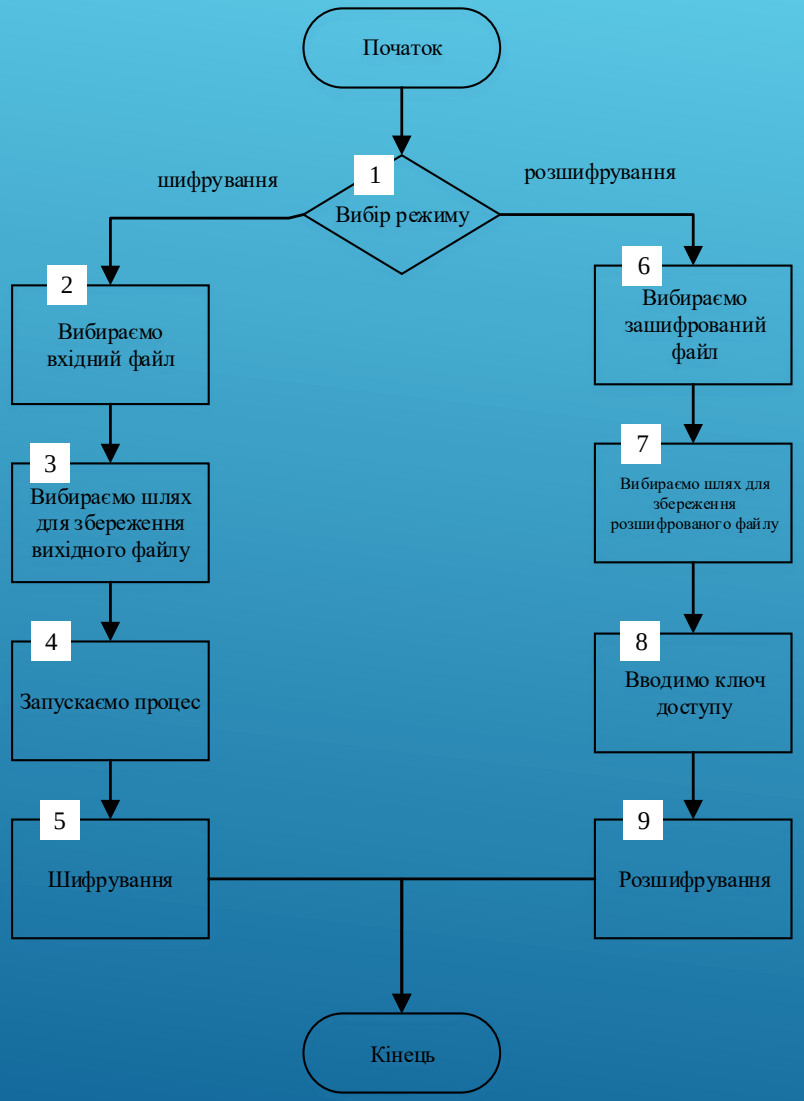
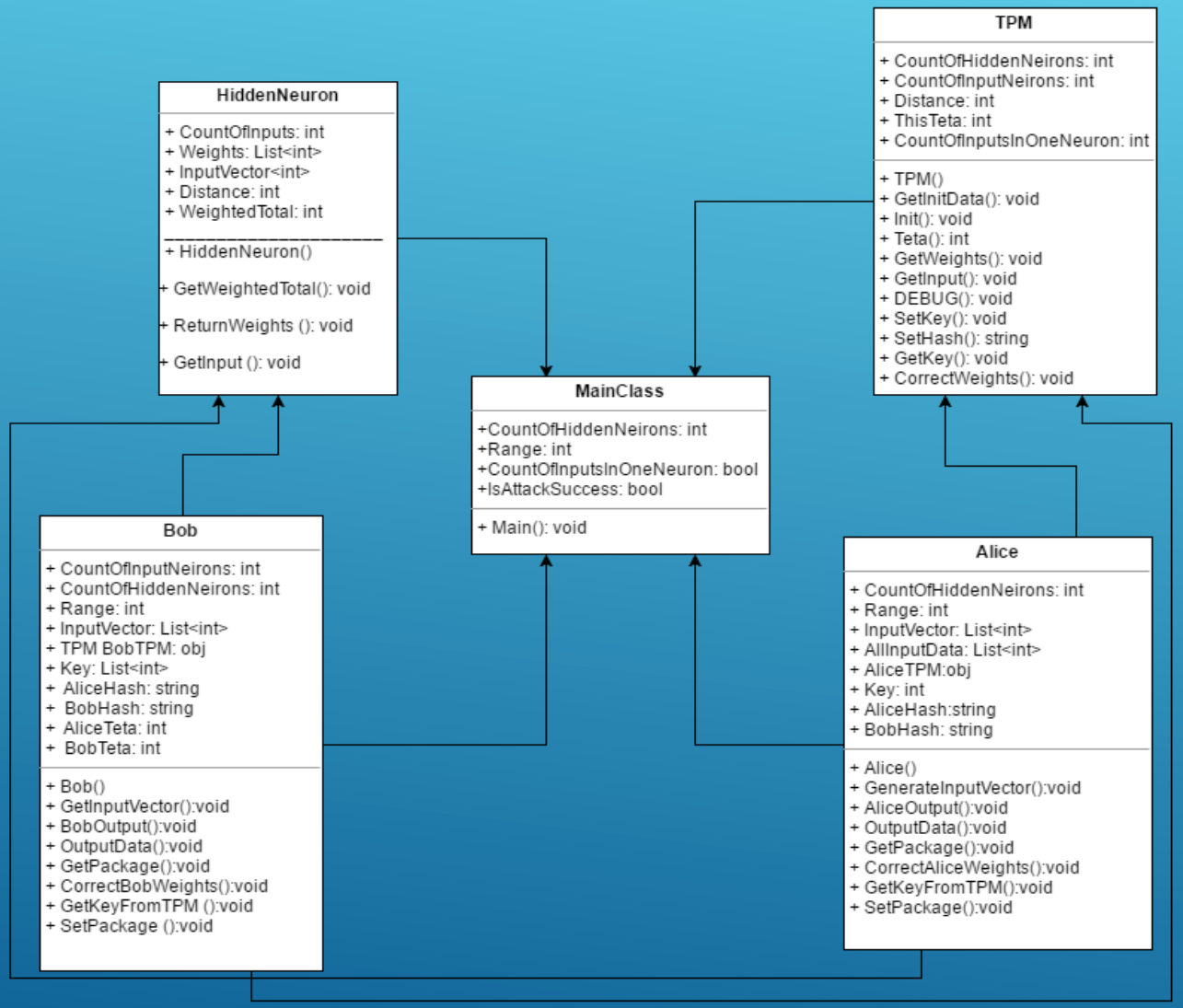


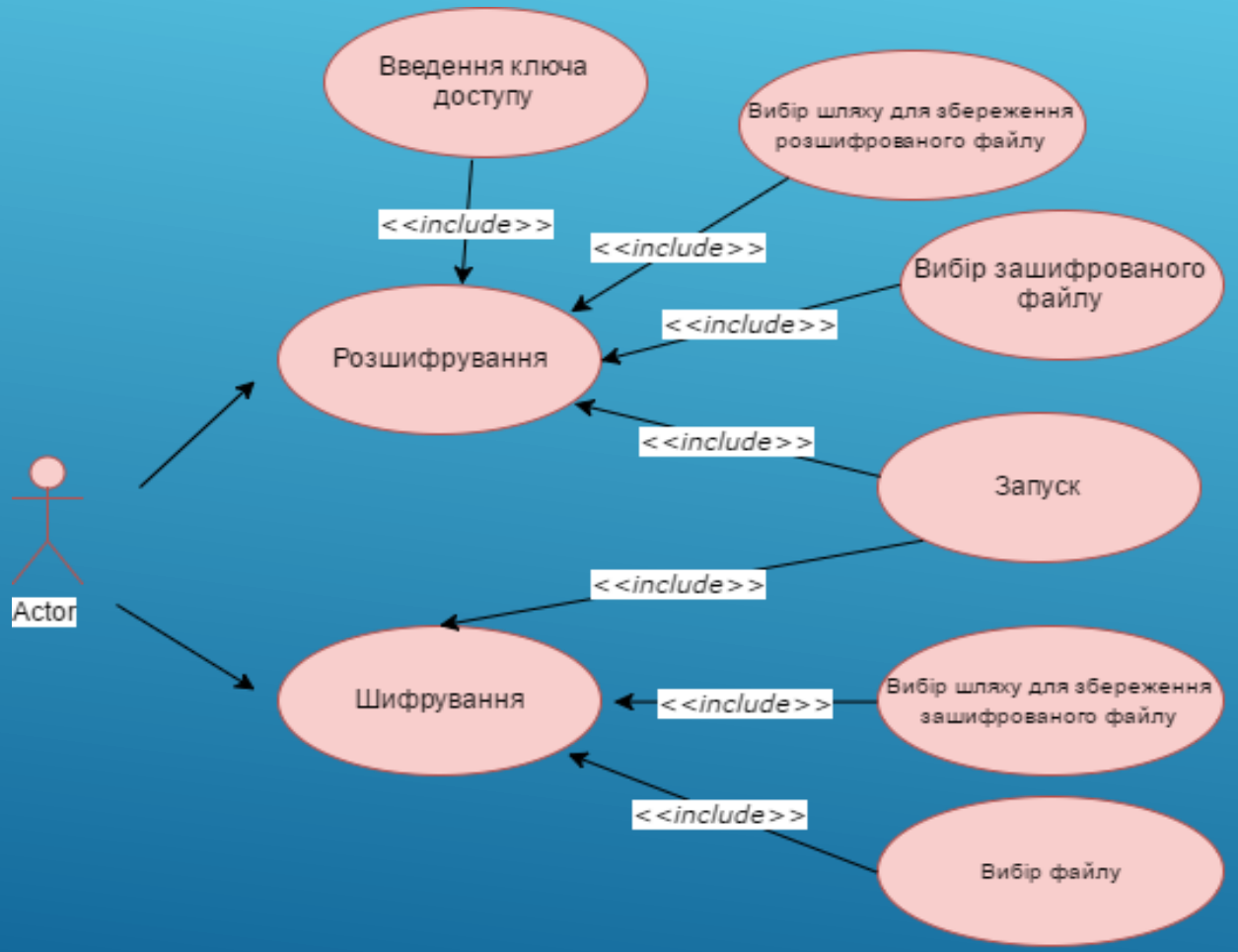
СХЕМА АЛГОРИТМУ РОБОТИ ПРОГРАМНОГО ЗАСОБУ



UML-ДІАГРАМА КЛАСІВ ПРОГРАМИ



UML- діаграма використання



ЕФЕКТИВНІСТЬ РОБОТИ ПРОГРАМИ

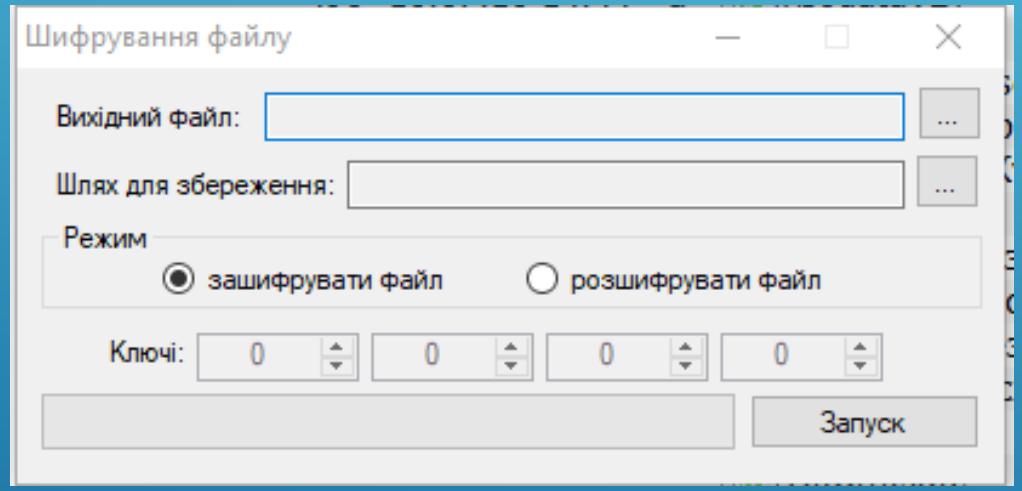
Результати тестування на швидкість обміну повідомлень

N	Середня кількість повідомлень, шт.	Середній затрачений час CPU, с
3	798,53	0,134
4	370,64	0,072
5	352,23	0,083
8	339,74	0,111
16	364,74	0,212
32	430,96	0,476
64	483,31	1,050
128	557,04	2,670
256	589,64	6,036
512	659,72	11,165
1024	720,32	24,436

Щоб зламати захист нашої системи потрібно щоб криптоаналітик перевірив всі можливі варіанти ключів, а кількість ключів при K = 3, L = 3, N = 100 дорівнює $3 \cdot 10^{253}$.

На сьогоднішній день така атака неможлива

ПРИКЛАД РОБОТИ ПРОГРАМИ



ВИСНОВКИ:

- Отже, в роботі було створено інтелектуальна система криптографічного захисту цифрової інформації.
- Мета дослідження була досягнута за рахунок збільшення рівня захисту цифрової інформації.

ДЯКУЮ ЗА УВАГУ!