Магістерська кваліфікаційна робота на тему:

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ НА ОСНОВІ ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ

Виконав студент гр. 1КН-16м Білий Ю.В.
Науковий керівник: к.т.н., доц. Колесницький О.К.

МЕТА ТА ЗАВДАННЯ ДОСЛІДЖЕННЯ

Метою дослідження магістерської кваліфікаційної роботи є спрощення процесу забезпечення секретності передачі симетричних паролей програмними засобами криптографічного захисту даних за рахунок використання нейронної мережі.

Для досягнення поставленої мети необхідно розв'язати такі завдання:

- здійснити обґрунтування доцільності розробки інформаційної технології криптографічного захисту даних на основі штучної нейронної мережі;
- здійснити аналіз методів і алгоритмів криптографічного захисту даних;
- розробити інформаційну технологію криптографічного захисту даних на основі штучної нейронної мережі;
- обґрунтувати вибір програмного інструментарію для реалізації інформаційної технології криптографічного захисту даних на основі штучної нейронної мережі;
- здійснити програмну реалізацію та тестування програмних засобів криптографічного захисту даних на основі штучної нейронної мережі.

ОБ’ЄКТ, ПРЕДМЕТ ТА МЕТОДИ ДОСЛІДЖЕННЯ

Об’єкт дослідження – процес криптографічного захисту даних з використанням нейронної мережі.

Предмет дослідження – методи та програмні засоби криптографічного захисту даних з використанням нейронної мережі та простота процесу забезпечення секретності передачі симетричних паролей.

Методи дослідження

У роботі використані наступні методи наукових досліджень:

-- системного аналізу для аналізу структури інформаційної системи,
-- симетричної криптографії
-- теорії штучних нейронних мереж для реалізації інформаційної технології криптографічного захисту даних
-- методи математичної статистики для розробки процесу захисту та обрахунків результатів експериментів із програмним засобом,
-- об’єктно-орієнтованого програмування для програмної реалізації.

НАУКОВА НОВИЗНА ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

-- знайшла подальшого розвитку інформаційна технологія криптографічного захисту даних за рахунок використання штучної нейронної мережі, що дозволило спростити процес забезпечення секретності передачі симетричних паролей;

-- удосконалено метод навчання нейронної мережі за рахунок використання правила навчання «блукань», що дозволило підвищити точність навчання нейронної мережі.

.

ПРАКТИЧНЕ ЗНАЧЕННЯ ОДЕРЖАНИХ РЕЗУЛЬТАТІВ

1. Розроблено алгоритм криптографічного захисту даних на основі штучної нейронної мережі.

2. Розроблено програмний засіб для криптографічного захисту даних на основі штучної нейронної мережі.

Розроблені алгоритми можуть бути впроваджені в начальний процес як лекція на тему «Нейромережевий метод криптографічного захисту даних» дисципліни «Нейромережеві методи обчислювального інтелекту».

ПОСТАНОВКА ЗАДАЧІ

Є дві людини і незахищений канал (наприклад, e-mail). Вони хочуть відправити деяку надсекретну інформацію один одному. Крім того, вони не можуть використовувати асиметричні алгоритми, і вони не можуть зустрітися, щоб узгодити секретний ключ для своїх повідомлень. Рішення полягає в створенні нейронних мереж, по одній для кожного з них. Потім вони повинні синхронізувати свої нейронні мережі, і синаптичні ваги нейронів цих мереж будуть утворювати секретний ключ.

АКТУАЛЬНІСТЬ ЗАДАЧІ

Ця тематика є актуальною, оскільки буде цікава для розробників, криптоаналітиків і тих користувачів, які хочуть зробити безпечним свій зв'язок.

АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

Відомі методи криптографічного захисту даних:

1) - симетричні алгоритми шифрування,
2) - асиметричні алгоритми шифрування.

Симетричне шифрування має ряд **переваг**. Одна з них — швидкість криптографічних операцій, симетричні алгоритми шифрування вимагають менше обчислень, ніж асиметричні, тобто якісні асиметричні алгоритми в сотні або в тисячі разів повільніші за якісні симетричні алгоритми.

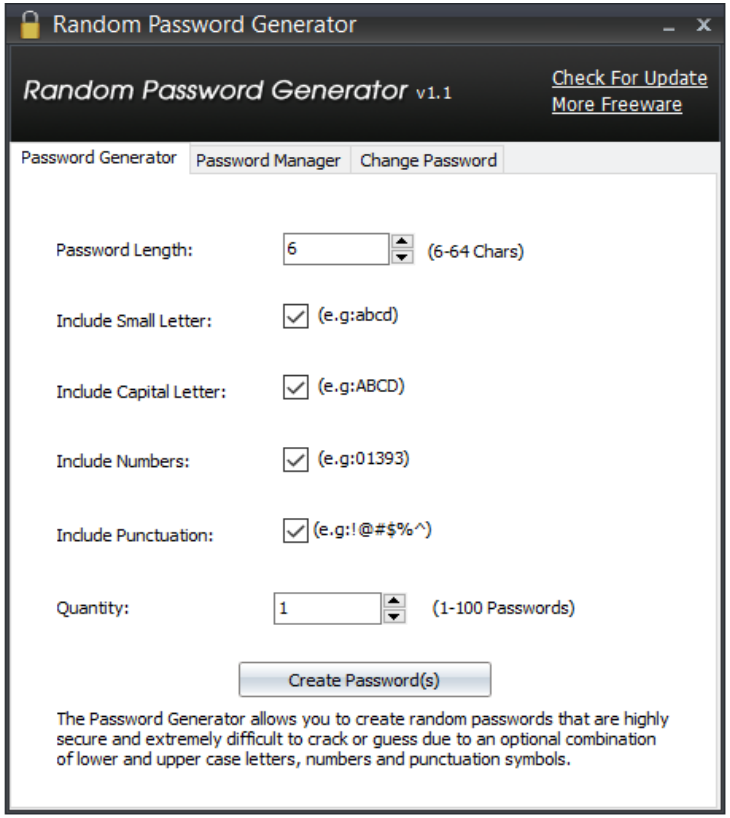
Таким чином, в нашій роботі для шифрування даних оберем симетричний алгоритм.

Але **недоліком симетричних алгоритмів** є необхідність мати секретний ключ з обох боків передачі інформації. Симетричне шифрування, може виявитися досить витратним просто через складність передачі таємного ключа. Так як ключі є предметом можливого перехоплення, їх необхідно часто змінювати та передавати по безпечних каналах передачі інформації.

Запропонована в цій роботі програма дозволяє обмінятись таємно симетричними ключами без використання безпечних каналів, особистої зустрічі чи послуг кур'єра.

ВИБІР АНАЛОГУ ДО ПРОГРАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ

Програма для генерації паролей Random Password Generator



Програма дозволяє генерувати паролі від 6 до 64 символів з використанням літер латиниці, різної символіки, форматування (великі літери або маленькі) і ін. Плюс, до простої генерації є можливість збереження і позначки цих паролів своїми коментарями. Також є можливість генерувати кілька паролів за раз за заданими умовами.

Головним недоліком програми-аналогу є те, що згенерований пароль треба передати своєму абоненту або по засекреченому каналу, або кур'єром. Це створює певні незручності та ускладнює процес передачі секретного пароля своєму абоненту.

Тому ставиться задача спрощення процесу забезпечення секретності передачі симетричних паролів програмними засобами криптографічного захисту даних.

ОБГРУНТУВАННЯ ВИБОРУ НЕЙРОННОЇ МЕРЕЖІ

Було розглянуто:

- багатошаровий персептрон,
- РБФ мережа,
- мережа Хопфілда,
- мережа Хеммінга,
- мережа Кохонена,
- АРТ мережа :

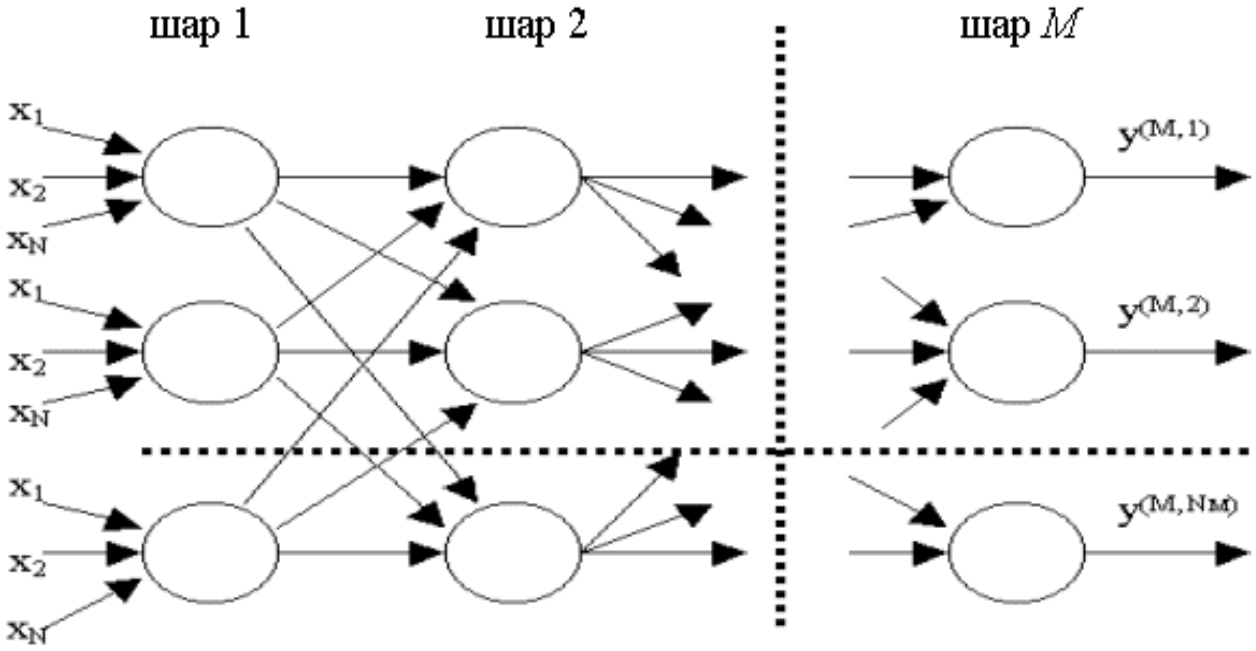
Але не кожна мережа може підійти для застосування у цій задачі. Нам потрібна така мережа, яка відноситься до категорії мереж, які навчаються «з учителем», тобто у яких є чітко визначена процедура навчання на основі навчальних прикладів (пар векторів Х-У).

Саме з цієї причини нам не підійде мережа Кохонена, оскільки вона відноситься до мереж, які навчаються «без учителя». Також нам не підійдуть нейронні мережі Хопфілда та Хеммінга, оскільки вони мають так зване «гібридне навчання», тобто в них матриця зав'язків формується не у результаті ітераційної процедури навчання, а обчислюється за формулою на основі векторів еталонних образів.

Таким чином, нам треба вибрати мережу із таких: багатошаровий персептрон, РБФ мережа, АРТ мережа

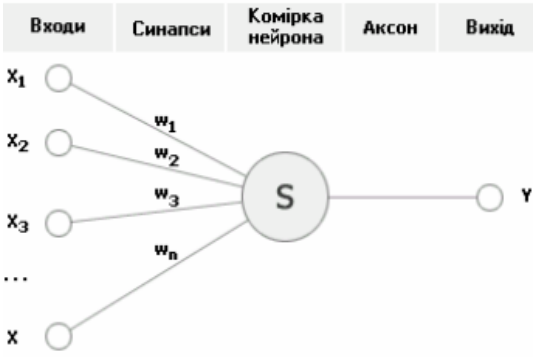
Було обрано: багатошаровий персептрон, оскільки він простіше реалізується і має простішу процедуру навчання, а значить буде швидше працювати

СТРУКТУРА БАГАТОШАРОВОГО ПЕРСЕПТРОНА



МАТЕМАТИЧНА МОДЕЛЬ БАГАТОШАРОВОГО ПЕРСЕПТРОНА

Метод зворотного поширення помилки



Структура формального нейрона

$$z = \sum_{i=0}^{N} x_i w_i , \qquad (1)$$

$$f(z) = \begin{cases} 1, z \geq \theta \\ 0, z < \theta \end{cases}$$

$$f_i^{(j)} = f\left(\sum_{t=1}^{N^{(j-1)}} f_t^{(j-1)} w_{ti}^{(j)} - \theta_i^j\right) \qquad (2)$$

Використання квадратичного критерію якості навчання:

$$\varepsilon_i^2 = (y_i - y_i^*)^2 \qquad (3)$$

дозволяє отримати градієнтний алгоритм корекції ваг:

$$\Delta w_{ij}^{(k)} = -\gamma_{ij} \cdot \frac{\partial \varepsilon_j^2}{\partial w_{ij}^{(k)}} \qquad (4)$$

де γ_{ij} - коефіцієнт швидкості навчання.

Похибка поширюється від виходів до входів, тому спочатку обчислюються корекції ваг для вихідного шару.:

$$\frac{\partial \varepsilon_j^2}{\partial w_{ij}^{(k)}} = \frac{\partial \varepsilon_j^2}{\partial f_j^{(k)}} \cdot \frac{\partial f_j^{(k)}}{\partial z_j^{(k)}} \cdot \frac{\partial z_j^{(k)}}{\partial w_{ij}^{(k)}} \qquad (5)$$

$$\Delta w_{ij}^{(k)} = 2\varepsilon_i \gamma_{ij} \cdot \alpha f_j^{(k)} \left(1 - f_j^{(k)}\right) \cdot f_i^{(k-1)} \qquad (6)$$

Отримані складові виводимо наступним чином:

$$\delta_j^{(k)} = 2\varepsilon_j \alpha f_j^{(k)} \left(1 - f_j^{(k)}\right) \qquad (7)$$

$$\Delta w_{ij}^{(k)} = \gamma_{ij} \cdot \delta_j^{(k)} \cdot f_i^{(k-1)} \qquad (8)$$

Виділимо складову k-го шару окремо:

$$\frac{\partial \varepsilon_j^2}{\partial f_j^{(k)}} = -2\left(y_j - y_j^*\right) = -2\varepsilon_j \qquad (9)$$

$$\frac{\partial f_j^{(k)}}{\partial z_j^{(k)}} = \alpha f_j^{(k)} (1 - f_j^{(k)}) \qquad (10)$$

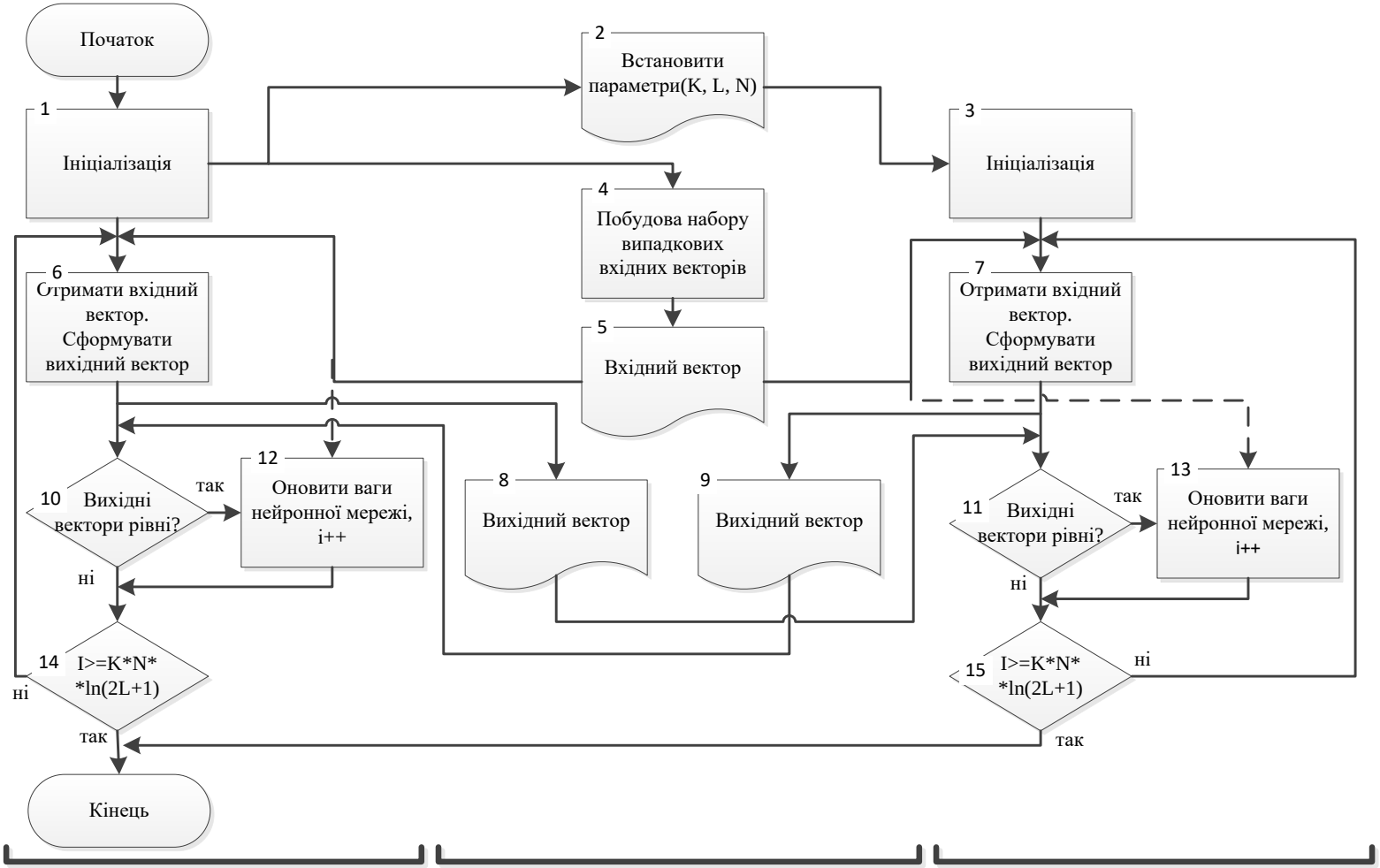
$$\frac{\partial z_j^{(k)}}{\partial w_{ij}^{(k)}} = f_i^{(k-1)} \qquad (11)$$

Підставивши (8) – (11) в (7) отримуємо для вихідного шару:

$$\Delta w_{ij}^{(k)} = 2\varepsilon_i \gamma_{ij} \cdot \alpha f_j^{(k)} \left(1 - f_j^{(k)}\right) \cdot f_i^{(k-1)} \qquad (12)$$

Структура інформаційної технології криптографічного захисту даних на основі нейронної мережі

АЛГОРИТМ КРИПТОГРАФІЧНОГО ЗАХИСТУ ДАНИХ

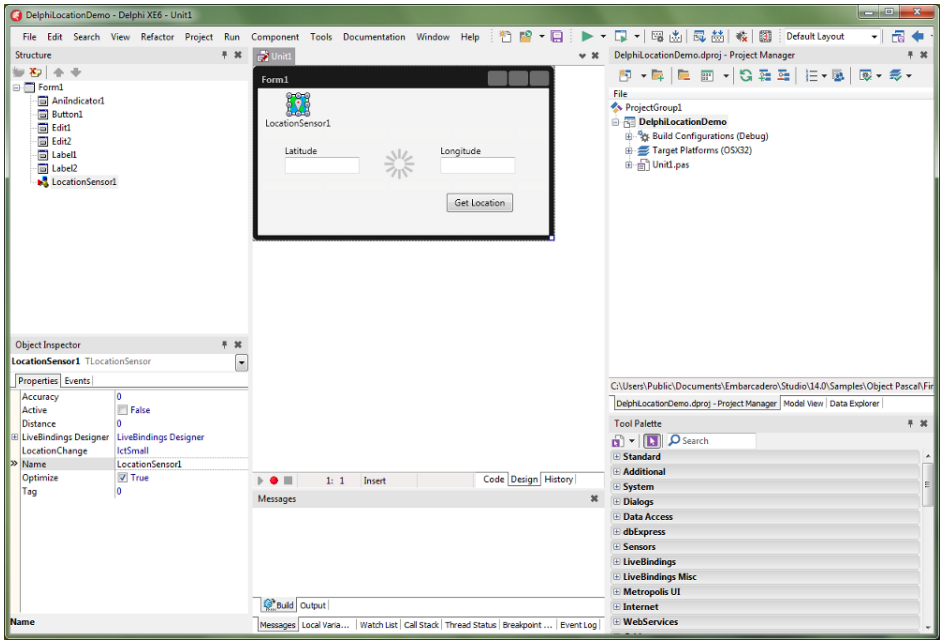


ОБГРУНТУВАННЯ ВИБОРУ МОВИ ПРОГРАМУВАННЯ

Було розглянуто такі мови програмування:

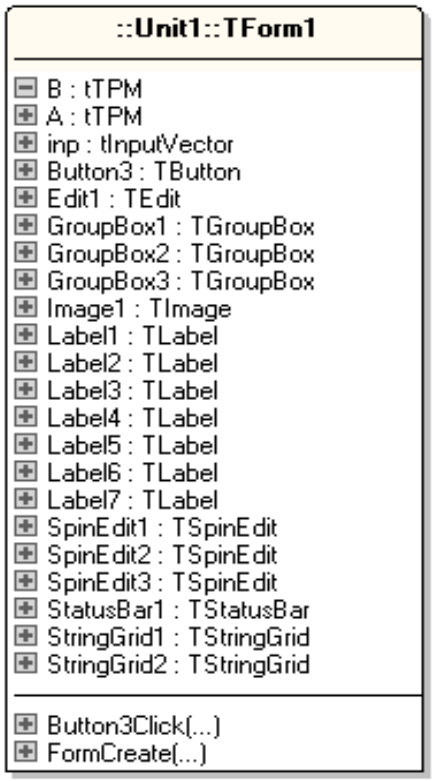
- Delphi,
- Java,
- C++,
- C#,

Для програмної реалізації була обрана мова Delphi

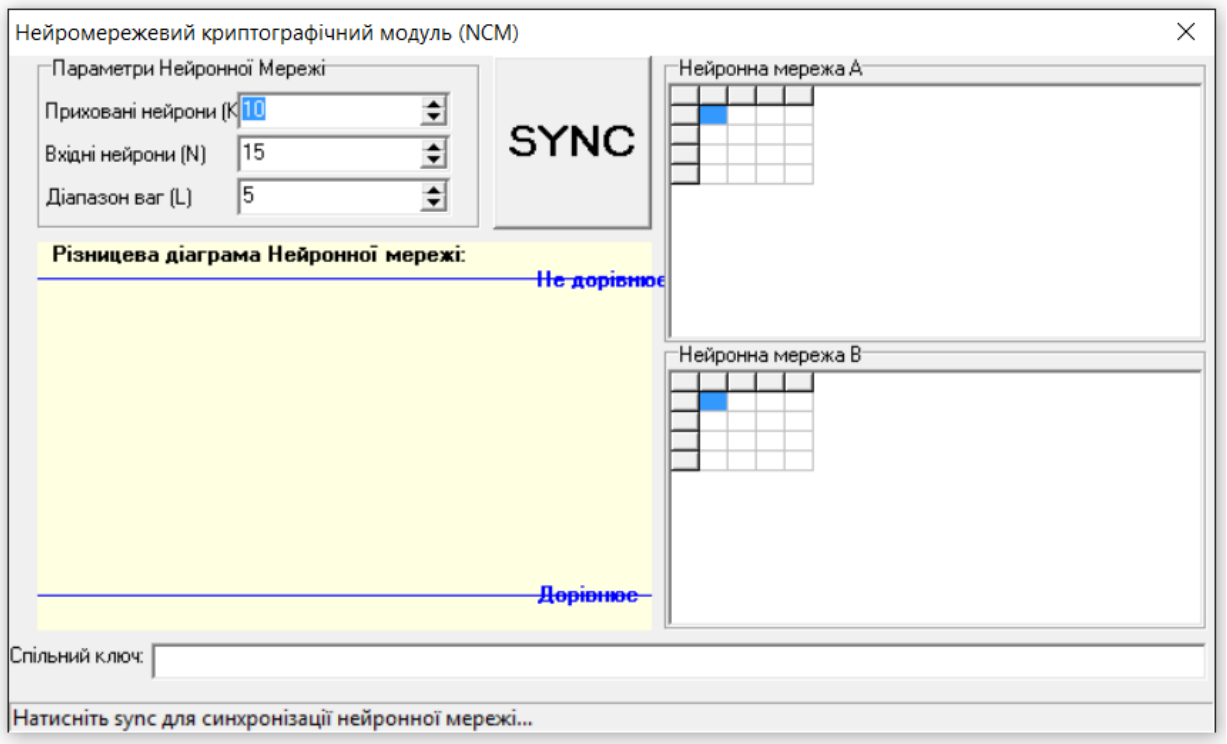


Головне вікно інтегрованого середовища Delphi

СТРУКТУРА ПРОГРАМИ

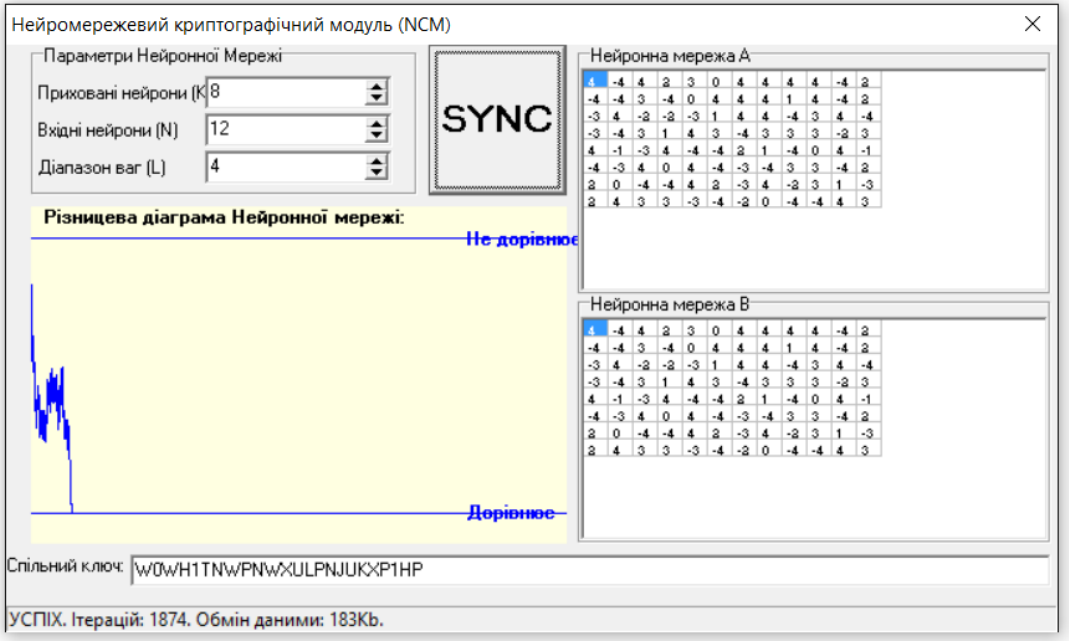


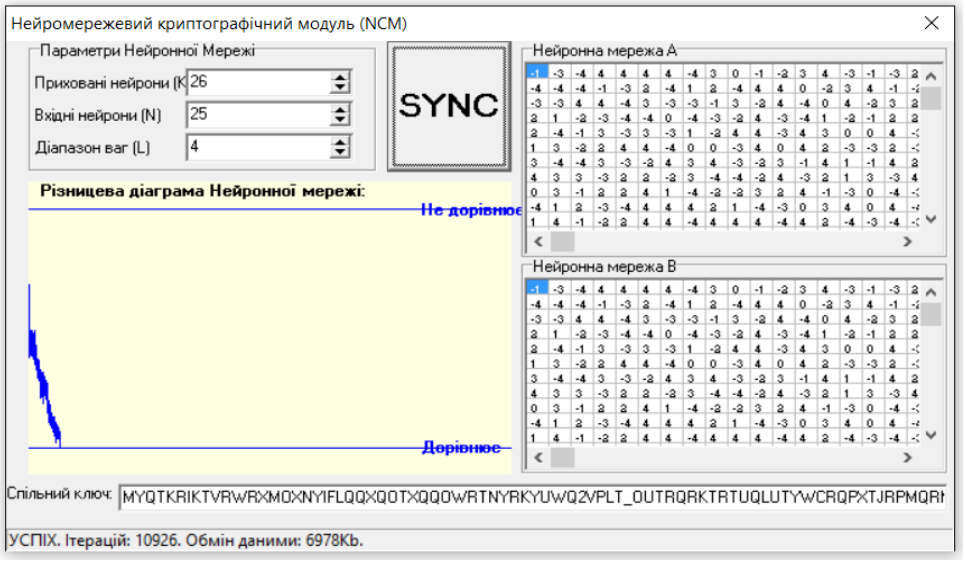
ТЕСТУВАННЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ РОБОТИ ПРОГРАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ



Початкове вікно програми криптографічного захисту даних на основі нейронної мережі

РЕЗУЛЬТУЮЧІ ВІКНА РОБОТИ ПРОГРАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ





ДОСЛІДЖЕННЯ ПАРАМЕТРІВ РОБОТИ ПРОГРАМИ КРИПТОГРАФІЧНОГО ЗАХИСТУ

Залежність довжини секретного ключа від кількості прихованих та вхідних нейронів

Кількість прихованих нейронів	5	10	15	20	25	30
Довжина секретного ключа (символів) при 10 вхідних нейронах	12	25	37	50	62	75
Довжина секретного ключа (символів) при 20 вхідних нейронах	25	50	75	100	125	150

Залежність тривалості процесу синхронізації нейронних мереж від кількості прихованих та вхідних нейронів

Кількість прихованих нейронів	5	10	15	20	25	30
Тривалість процесу синхронізації (с) при 10 вхідних нейронах	1,03	4,33	5,56	4,92	6,43	8,02
Тривалість процесу синхронізації (с) при 20 вхідних нейронах	2,10	6,04	15,03	26,02	29,52	39,25

Тестування показало надійну роботу розробленої програми, дозволило виявити важливі залежності функціональних характеристик програми від параметрів використовуваної нейронної мережі, а також довело, що поставлена в роботі мета досягнута, а саме - розроблена програма має спрощений процес забезпечення секретності передачі симетричних паролів, тобто є більш зручною у використанні, ніж програма-аналог.

ЕКОНОМІЧНА ЧАСТИНА

Було здійснено економічне обґрунтування доцільності розробки інформаційної технології криптографічного захисту даних на основі нейронної мережі.

Загальна сума витрат на виконання розробки склала 26864,37 грн.

Прогнозоване значення загальних витрат на виконання та впровадження результатів виконаної наукової роботи – 39506,42 грн.

Абсолютна ефективність вкладених інвестицій - 318805,7 грн.

Відносна (щорічна) ефективність вкладених в наукову розробку інвестицій – 109 %,

Термін окупності становить 11 місяців, що менше нормативного його значення - 3 роки, тобто фінансування розробки інформаційної технології криптографічного захисту даних на основі штучної нейронної мережі є економічно доцільним

АПРОБАЦІЯ РЕЗУЛЬТАТІВ РОБОТИ ТА ПУБЛІКАЦІЇ

Апробація результатів роботи.

Результати роботи були апробовані на IV МІЖНАРОДНІЙ НАУКОВО-ПРАКТИЧНІЙ КОНФЕРЕНЦІЇ «Інформаційні технології та взаємодії» м. Київ, 8-10 листопада 2017 року.

Публікації.

За результатами магістерської кваліфікаційної роботи опубліковано 1тези доповіді на конференції.

Висновок

В результаті виконання МКР було розроблено інформаційну технологію криптографічного захисту даних на основі нейронної мережі багатошаровий персептрон та здійснено її програмну реалізацію, яку написано мовою Delphi. Розроблена програма завдяки застосуванню процесу синхронізації двох нейронних мереж дозволяє абонентам обмінятися секретними паролями по відкритому каналу, не застосовуючи при цьому складних процедур залучення довірених кур'єрів або використання спеціального закритого каналу зв'язку. Тестування показало надійну роботу розробленої програми, дозволило виявити важливі залежності функціональних характеристик програми від параметрів нейронної мережі, а також довело, що поставлена в роботі мета досягнута, а саме - розроблена програма має спрощений процес забезпечення секретності передачі симетричних паролів, тобто є більш зручною у використанні, ніж програма-аналог.

Дякую за увагу!