

Міністерство освіти і науки України  
Український державний університет науки і технологій

Факультет «Комп'ютерні технології і системи»  
(назва факультету)

Кафедра «Електронні обчислювальні машини»  
(повна назва кафедри)

до захисту  
23.01.2023


Пояснювальна записка

до кваліфікаційної роботи  
магістра  
(ступінь вищої освіти)

на тему: Дослідження та розробка засобів біометричної ідентифікації та аутентифікації за клавіатурним почерком

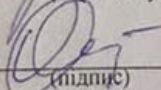
за освітньою програмою Комп'ютерна інженерія  
зі спеціальності: 123 Комп'ютерна інженерія  
(шифр і назва спеціальності)

Виконав: студент групи: КС2221

  
(підпис студента)

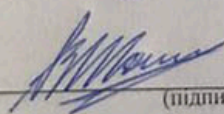
/ Данило ЯРЬОМЕНКО /  
(Ім'я ПРІЗВИЩЕ)

Керівник:

  
(підпис)

/ доцент, Денис ОСТАПЕЦЬ /  
(посада, Ім'я ПРІЗВИЩЕ)

Нормоконтролер:

  
(підпис)

/ доцент, Володимир ШАПОВАЛОВ /  
(посада, Ім'я ПРІЗВИЩЕ)

Консультанти:

\_\_\_\_\_  
(назва розділу)

\_\_\_\_\_  
(підпис)

/ \_\_\_\_\_ /  
(посада, Ім'я ПРІЗВИЩЕ)

\_\_\_\_\_  
(назва розділу)

\_\_\_\_\_  
(підпис)

/ \_\_\_\_\_ /  
(посада, Ім'я ПРІЗВИЩЕ)

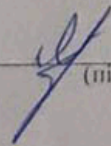
\_\_\_\_\_  
(назва розділу)

\_\_\_\_\_  
(підпис)

/ \_\_\_\_\_ /  
(посада, Ім'я ПРІЗВИЩЕ)

Засвідчую, що у цій роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент

  
(підпис)

Дніпро – 2024 рік

**Ministry of Education and Science of Ukraine  
Ukrainian State University of Science and Technologies**

Faculty «Computer technologies and systems»

(faculty)

Department «Electronic computers»

(department)

**Explanatory Note  
to Master's Thesis**

(higher education degree)

on the topic: Research and development of biometric identification and authentication means based on keyboard handwriting

in the Speciality: 123 Computer Engineering

(speciality and its code)

Done by the student of the group: KC2221

/ Danylo Yaromenko /

(name, surname)

Scientific Supervisor:

/ Associate Professor, Denis Ostapets /

(position, name, surname)

Normative controller :

/ Associate Professor, Volodymyr Shapovalov

(position, name, surname)

Supervisors

\_\_\_\_\_  
(Chapter title heading)

/ /  
(position, name, surname)

\_\_\_\_\_  
(Chapter title heading)

/ /  
(position, name, surname)

\_\_\_\_\_  
(Chapter title heading)

/ /  
(position, name, surname)

\_\_\_\_\_  
(Chapter title heading)

/ /  
(position, name, surname)

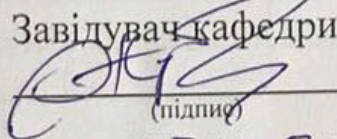
Dnipro – 2024

Міністерство освіти і науки України  
Український державний університет науки і технологій

Факультет: Комп'ютерні технології і системи  
Кафедра: ЕОМ  
Рівень вищої освіти: Другий (магістерський)  
Освітня програма: Комп'ютерна інженерія  
Спеціальність: 123 Комп'ютерна інженерія  
(шифр та назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри \_\_\_\_\_

  
(підпис)

\_\_\_\_\_ (Ім'я ПРІЗВИЩЕ)

Дата

15.11.2023

**ЗАВДАННЯ**

на кваліфікаційну роботу

магістра  
(ступінь вищої освіти)

студенту Ярьоменку Данилу Олександровичу

(Прізвище, Ім'я По батькові)

1. Тема роботи: Дослідження та розробка засобів біометричної ідентифікації та аутентифікації за клавіатурним почерком

Керівник роботи: Остапець Денис Олександрович, к.т.н., доцент

(Прізвище, Ім'я, По батькові, науковий ступінь, вчене звання)

затверджені наказом від

"21" 04 2023 р.

№ 333ст

2. Строк подання студентом роботи: 22.01.2024 р.

3. Вихідні дані до роботи: \_\_\_\_\_

Методи та алгоритми біометричної ідентифікації та аутентифікації за клавіатурним почерком

4. Зміст пояснювальної записки (перелік питань, які потрібно опрацювати):

4.1 Огляд та аналіз методів та засобів біометричної ідентифікації та аутентифікації;

4.2 Аналіз відомих методів оцінки клавіатурного почерку;

4.3 Розробка засобів ідентифікації та аутентифікації за клавіатурним почерком на базі штучної нейронної мережі;

4.4 Дослідження ефективності розроблених засобів.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):

- Характеристики біометричних методик;

- Характеристики алгоритмів розпізнавання клавіатурного почерку;

- Структура штучної нейронної мережі

- Структура даних;

- Результати дослідження.

Консультанти розділів роботи:

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав: (підпис консультанта, дата)	Завдання прийняв: (підпис студента, дата)

### КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Огляд та аналіз методів та засобів біометричної ідентифікації та аутентифікації	14.11.23	20%
2	Аналіз відомих методів оцінки клявіатурного почерку	30.11.23	20
3	Розробка засобів ідентифікації та аутентифікації за клявіатурним почерком на базі штучної нейронної мережі	21.12.23	25%
4	Дослідження ефективності розроблених засобів	16.01.24	30%
5	Реферат, вступ, висновки	19.01.24	5%
6	Подання кваліфікаційної роботи до кафедри	22.01.24	
7	Захист кваліфікаційної роботи на засіданні Екзаменаційної комісії	23.01.24	

Студент

(підпис)

Данило ЯРЬОМЕНКО

(Ім'я ПРІЗВИЩЕ)

Керівник роботи

(підпис)

Денис ОСТАПЕЦЬ

(Ім'я ПРІЗВИЩЕ)

## РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи магістра: 77 с., 37 рис., 8 табл., 1 додаток, 23 джерела.

Об'єкт розробки – засоби біометричної ідентифікації та аутентифікації за клавіатурним почерком.

Мета роботи – розробка та дослідження ефективності засобів біометричної ідентифікації та аутентифікації за клавіатурним почерком.

Представлено аналіз методів та засобів біометричної ідентифікації та аутентифікації. Проведено аналіз методів оцінки клавіатурного почерку з використанням засобів штучного інтелекту. Обрано штучну нейронну мережу як засобу біометричної ідентифікації та аутентифікації за клавіатурним почерком. Розроблено структуру нейронної мережі, проведено її налаштування, навчання та тестування. Проведено дослідження ефективності ідентифікації та аутентифікації на базі штучної нейронної мережі та класичного підходу.

Показано ефективність засобів побудованих на базі штучної нейронної мережі.

Ключові слова: БІОМЕТРИЯ, АУТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, КЛАВІАТУРНИЙ ПОЧЕРК, МАТЛАВ, ШТУЧНА НЕЙРОННА МЕРЕЖА, КЛАСИФІКАЦІЯ

## ЗМІСТ

ВСТУП .....	8
1 ОГЛЯД ТА АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ .....	9
1.1 Процедури аутентифікації та ідентифікації .....	9
1.2 Методики біометричної аутентифікації та ідентифікації .....	10
1.3 Біометрична аутентифікація та ідентифікації за клавіатурним почерком .....	13
1.4 Висновки за розділом .....	19
2 АНАЛІЗ ВІДОМИХ МЕТОДІВ ОЦІНКИ КЛАВІАТУРНОГО ПОЧЕРКУ	20
2.1 Методи оцінки клавіатурного почерку на базі ймовірнісно-статистичного підходу .....	20
2.2 Методи оцінки клавіатурного почерку з використанням засобів штучного інтелекту .....	22
2.3 Висновки за розділом .....	30
3 РОЗРОБКА ЗАСОБІВ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ НА БАЗІ ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ .....	31
3.1 Вибір середовища розробки .....	31
3.2 Вибір математичного апарату .....	32
3.3 Структура та підготовка вибірки .....	35
3.4 Експериментальне визначення найбільш ефективних параметрів нейронної мережі .....	38
3.5 Висновки за розділом .....	41
4 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ ЗАСОБІВ .....	42
4.1 Постановка задачі .....	42
4.2 Налаштування, навчання та тестування нейронної мережі .....	42
4.3 Порівняння ефективності засобів ідентифікації та аутентифікації за клавіатурним почерком .....	53
4.3.1 Режим ідентифікації .....	54

	7
4.3.2 Режим аутентифікації.....	56
4.4 Висновки за розділом .....	58
ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ .....	59
ПЕРЕЛІК ПОСИЛАНЬ.....	60
ДОДАТОК А.....	64

## ВСТУП

В умовах постійного зростання обсягу даних, процедури аутентифікації та ідентифікації стають критично важливими для забезпечення безпеки. Біометричні системи ідентифікації та аутентифікації є потенційно дієвими засобами вирішення цієї проблеми.

Незважаючи на складність їх впровадження і обмеженість у можливостях через недосконалість апаратних засобів та математичних моделей на сьогоднішній день, вони демонструють обіцяний розвиток завдяки постійному технологічному прогресу. Збільшення обчислювальної потужності, розвиток математичних моделей та використання технологій штучного інтелекту створюють передумови для значного поліпшення ефективності біометричних систем.

Засоби штучного інтелекту, як от нейронні мережі, можуть відігравати ключову роль у вдосконаленні біометричних систем, забезпечуючи високу точність і швидкість обробки даних. Розгляд засобів штучного інтелекту є важливим для подолання викликів, пов'язаних з конфіденційністю інформації в сучасному світі. Таким чином, тема робота є актуальною.

Мета роботи – розробка та дослідження ефективності засобів біометричної ідентифікації та аутентифікації за клавіатурним почерком.

Основні положення даної роботи доповідались та були схвалені на XVI та XVII Міжнародних конференціях «Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості та освіті» у 2022 та 2023 роках [1, 2], Всеукраїнській науково-технічній конференції студентів і молодих учених «Наука і сталий розвиток транспорту 2023» [3], Всеукраїнській науково-технічній конференції студентів і молодих учених «Молода Академія 2023» [4]

Робота складається із вступу, чотирьох розділів та висновків.

# 1 ОГЛЯД ТА АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ

## 1.1 Процедури аутентифікації та ідентифікації

Ідентифікація – процедура визначення користувача шляхом надання ідентифікаційних даних, як от логін, ім'я користувача, електронна пошта, номер облікового запису тощо.

Аутентифікація – це процедура перевірки та підтвердження ідентичності користувача на основі наданих їм ідентифікаційних даних. Цей процес передбачає, що користувач повинен надати додаткову інформацію, як от пароль, біометричні дані (наприклад, відбитки пальців або сканування особи), смарт-картки або інші секретні дані [5, 6].

Схема проходження користувачем процедур ідентифікації та аутентифікації наведено на рисунку 1.1.



Рисунок 1.1 – Проходження процедур ідентифікації та аутентифікації

Дані, які використовуються для підтвердження ідентичності, можна розподілити на три класи, які називають факторами аутентифікації:

- Щось, що ви знаєте (фактор знання) – це інформація, яку ви запам'ятали, як от пароль, ПІН-код або парольна фраза.
- Те, що у вас є (фактор володіння) – це предмети або пристрої, які ви маєте при собі, як от смарт-карта, картка пам'яті, смартфон або токен.
- Щось, чим ви є (біометричні дані) – це ваші фізичні особливості, як от відбиток пальця, топологія долоні, геометрія руки, рисунок райдужної оболонки/сітківки або геометрія обличчя, характер мовлення.

Система аутентифікації, що проводить процедуру аутентифікації за двома або більше факторами аутентифікації різних класів, називається багатофакторною (multi-factor authentication, MFA) і використовується в цілях підвищення рівня безпеки. Наприклад, використання ПІН-коду (щось, що ви знаєте) і цифрового підпису (те, що у вас є) для аутентифікації вважається багатофакторною аутентифікацією, тоді як використання відбитка пальця та скана обличчя – ні, оскільки ці два фактори належать до одного класу – біометричного [6-9].

Схематичне зображення факторів аутентифікації зображено на рисунку 1.2.

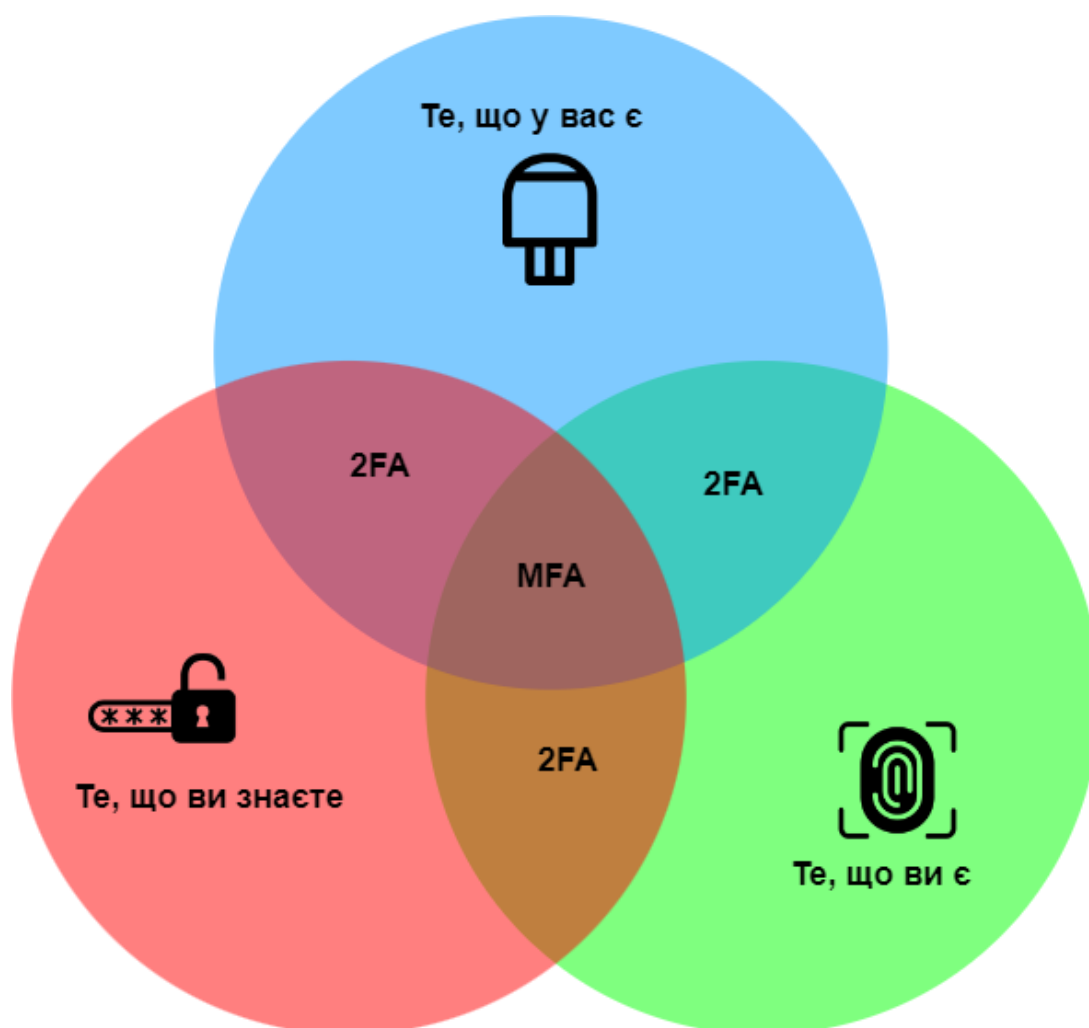


Рисунок 1.2 – Фактори аутентифікації

## 1.2 Методики біометричної аутентифікації та ідентифікації

Біометрична ідентифікація і біометрична аутентифікація – це два різні процеси, пов'язані з використанням унікальних характеристик для ідентифікації або аутентифікації користувача.

### Біометрична ідентифікація:

Мета: Визначення користувача серед існуючих профілів.

Приклади методик:

- Відбиток пальця: Система зіставляє відбиток пальця, знятий користувачем, з великою базою даних відбитків пальців і визначає, чи є відповідність.
- Розпізнавання обличчя: Аналіз особливостей обличчя (наприклад, форма очей, рота – розташування контрольних точок) для ідентифікації користувача.
- Розпізнавання голосу: Визначення користувача на основі його голосового зразка.

### Біометрична аутентифікація:

Мета: Перевірка та підтвердження ідентичності користувача.

Приклади методик:

- Сканер відбитків пальця: Користувач надає відбиток пальця, який порівнюється з попередньо збереженим відбитком для підтвердження.
- Вхід за допомогою обличчя: Система зчитує обличчя користувача та порівнює його з образом в системі для аутентифікації.
- Персональний PIN-код: Користувач вводить унікальний особистий номер (PIN) для підтвердження своєї ідентичності.

Різниця полягає в цілях використання. Біометрична ідентифікація використовується для визначення користувача серед групи. Біометрична аутентифікація застосовується для підтвердження ідентичності користувача в процесі доступу до конкретного ресурсу чи послуги.

Біометричні методики аутентифікації та ідентифікації поділяють на два класи [10]:

- статичні методики (в англійській мові середовищі «physiological», укр. фізіологічні)
- динамічні методики (в англійській мові середовищі «behavioral», укр. поведінкові)

Статичні методики ґрунтуються на фізіологічних характеристиках людини, які залишаються практично незмінними протягом життя і їх майже неможливо викрасти або підробити. Це включає в себе методики, як от аутентифікація за відбитком пальця, аутентифікація за характеристиками оболонки ока, аутентифікація за геометрією обличчя тощо.

Динамічні методики, натомість, базуються на поведінкових особливостях людини, які можуть змінюватися в залежності від її поточного стану та під впливом різних факторів. Сюди входять методики, як от аутентифікація за голосом та аутентифікація за почерком (ручним або клавіатурним) тощо.

Важливо відзначити, що статичні методики зазвичай надають вищу точність ідентифікації, але вимагають витрат на дороге обладнання, таке як сканери сітчатки ока. З іншого боку, динамічні методики є більш доступними для реалізації, але не завжди забезпечують таку саму точність, як статичні методики.

Засобами біометричної аутентифікації та ідентифікації є фізичні, анатомічні та поведінкові характеристики людини, які використовуються для підтвердження її особистості. Ось деякі засоби біометричної аутентифікації та ідентифікації:

- Контрольні точки, взяті з рисунку відбитку пальця: Використовуються сканери відбитків пальців для збору і порівняння унікальних відбитків пальців користувача;
- Контрольні точки, взяті з рисунку обличчя: Системи розпізнавання обличчя аналізують геометричні особливості обличчя і порівнюють їх зі збереженими шаблонами;
- Аудіозапис голосу: Ця методика використовує унікальні акустичні характеристики голосу особи для ідентифікації;
- Контрольні точки, взяті з рисунку радужки або сетківки: Аналізується унікальний малюнок радужки або сетківки ока для аутентифікації користувача;
- Контрольні точки, взяті з рисунку вен: Використовуються унікальні венозні структури пальців або долоні для ідентифікації;

- Профіль клавіатурного почерку: Системи аналізують специфічні риси почерку особи під час письма або підпису;
- ДНК: Аналіз ДНК зазвичай використовується, коли важлива максимальна точність (ефективність) ідентифікації особи.

Вибір конкретного засобу залежить від вимог системи і рівня безпеки, якого потрібно досягти [10, 11].

### 1.3 Біометрична аутентифікація та ідентифікації за клавіатурним почерком

Методика аутентифікації та ідентифікації за клавіатурним почерком є однією з методик біометричної аутентифікації та ідентифікації, які використовуються для визначення особистості користувача на основі його унікальних рухів під час введення тексту на клавіатурі комп'ютера. Ця методика полягає в тому, щоб виміряти та аналізувати параметри, які характеризують клавіатурний почерк користувача, до них зокрема входять:

- Час утримання клавіші (рисунок 1.3);
- Інтервали між натисканням та відпусканням клавіш:
  - 1) Інтервал між відпусканням та натисканням клавіш (рисунок 1.4);
  - 2) Інтервал між відпусканням клавіш (рисунок 1.5);
  - 3) Інтервал між натисканням клавіш (рисунок 1.6);
- Кількість помилок (рисунок 1.7);
- Сила натискання клавіші (потребує додаткових датчиків, вбудованих в клавіатуру, які вимірюють силу натискання, рисунок 1.8).

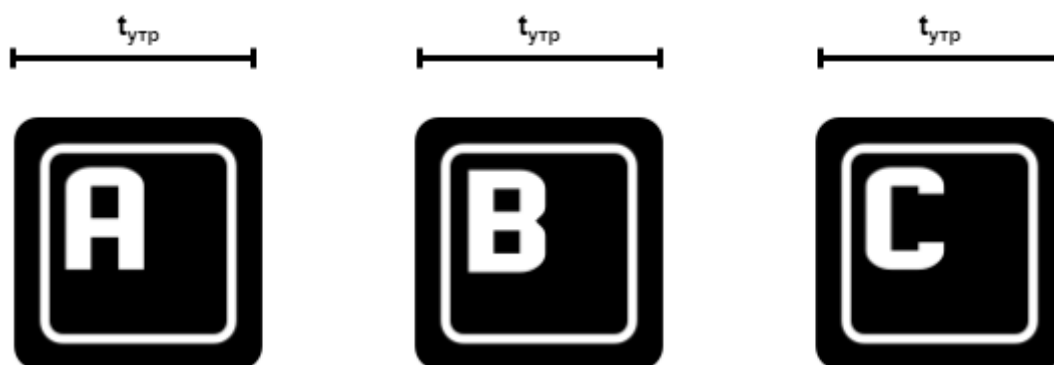


Рисунок 1.3 – Схематичне зображення представлення часу утримання клавіш



Рисунок 1.4 – Схематичне зображення представлення часових інтервалів між відпусканням і натисканням клавіш

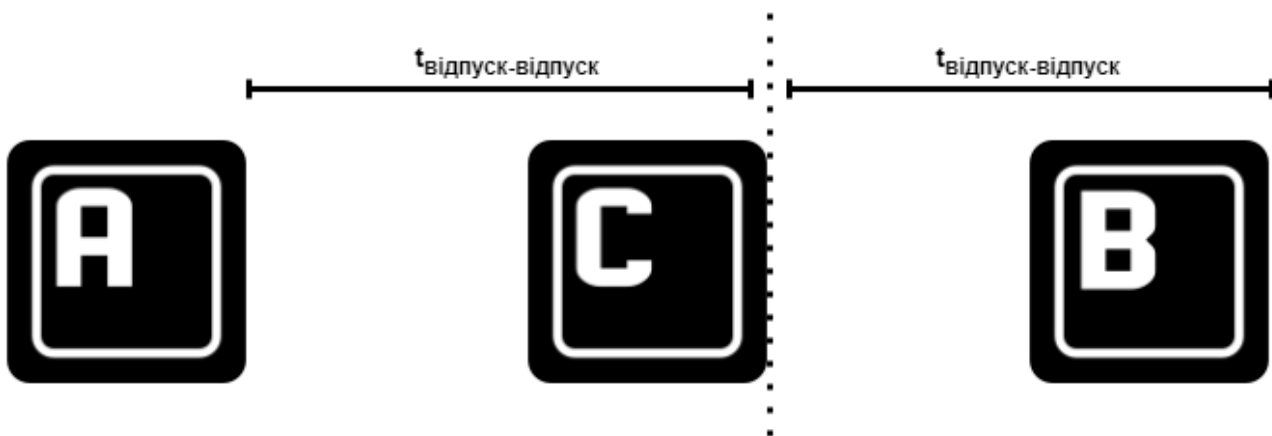


Рисунок 1.5 – Схематичне зображення представлення часових інтервалів між відпусканням клавіш

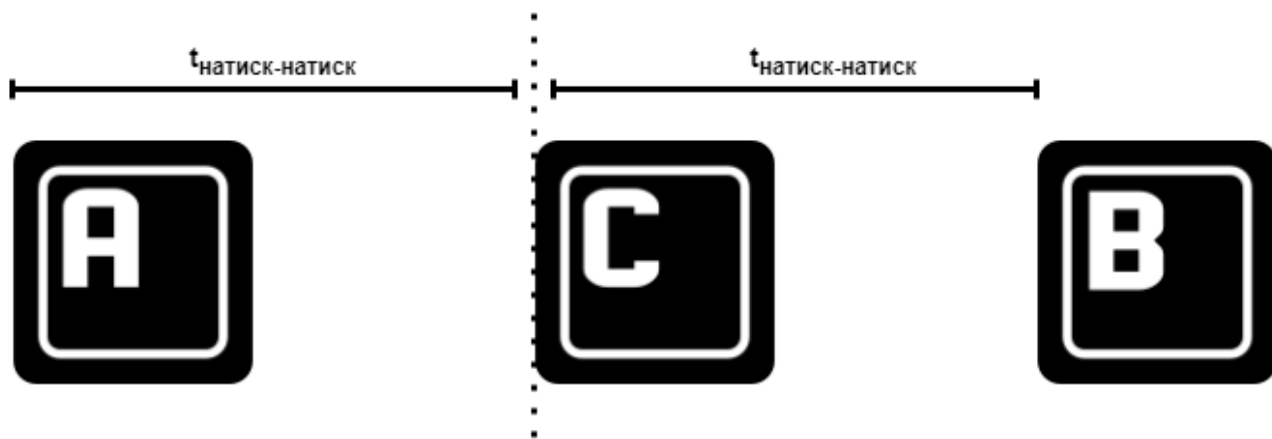


Рисунок 1.6 – Схематичне зображення представлення часових інтервалів між натисканням клавіш



Рисунок 1.7 – Схематичне зображення представлення кількості помилок

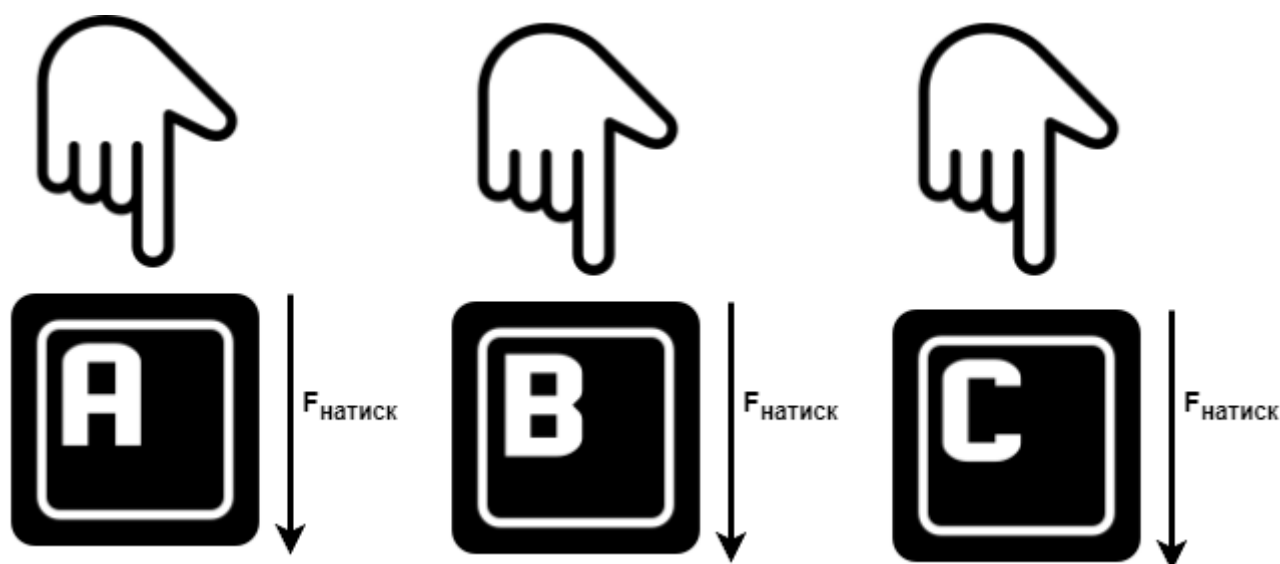


Рисунок 1.8 – Схематичне зображення представлення сили натискання клавіші

Методика розпізнавання клавіатурного почерку передбачає можливість навчання, де користувач може пройти аутентифікацію та ввести текст, щоб програма зчитала та зберегла характеристики його клавіатурного почерку. Після цього дані зберігаються у системі.

Узагальнена схема функціонування системи біометричної аутентифікації та ідентифікації за клавіатурним почерком наведено на рисунку 1.9.

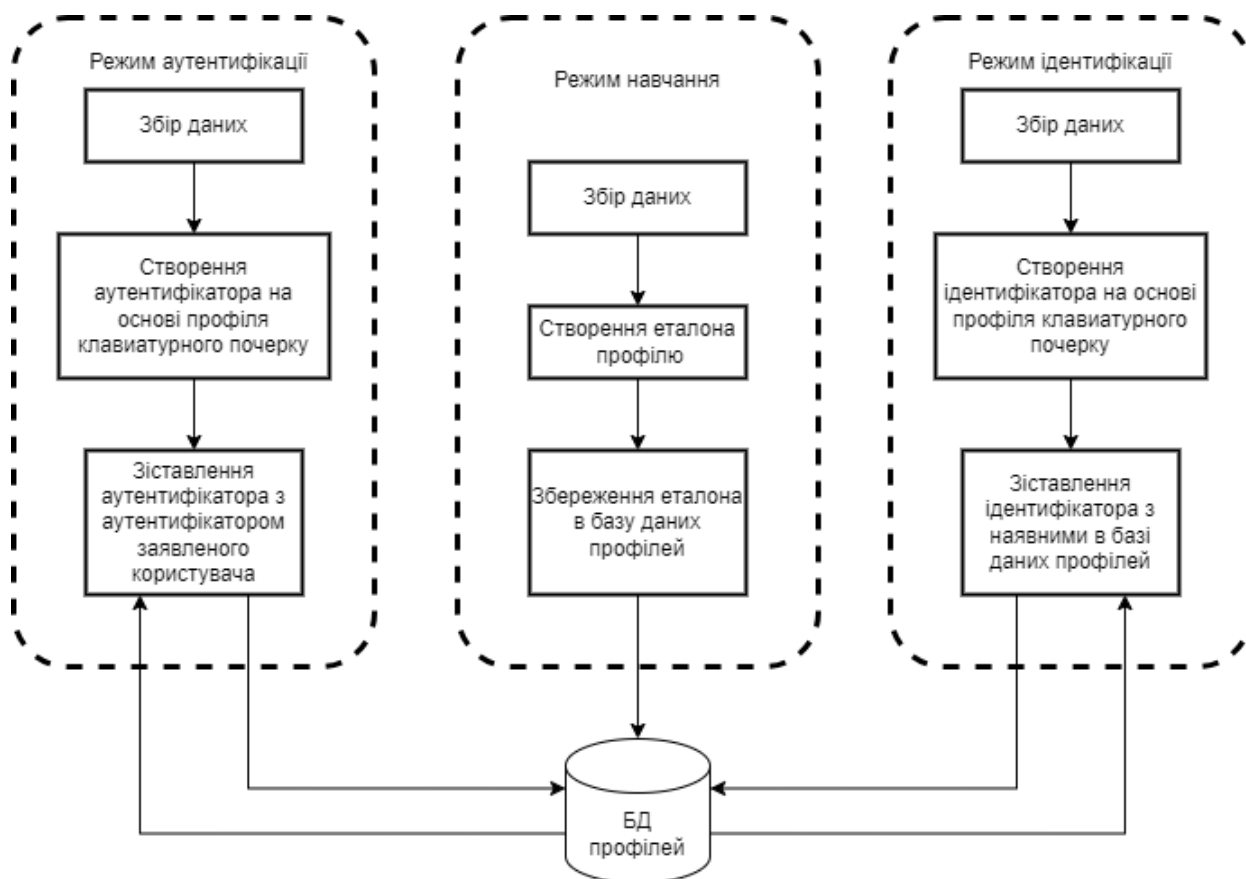


Рисунок 1.9 – Узагальнена схема функціонування системи аутентифікації та ідентифікації за клавіатурним почерком

Збір клавіатурного почерку може бути організованим трьома різними способами, описаними нижче.

Фіксація вихідних даних під час введення паролі. Цей метод швидкий, оскільки вимагає введення лише фіксованого пароля, відомого користувачу. Однак точність ідентифікації може бути низькою, особливо для коротких паролів.

Фіксація вихідних даних під час введення тексту. Цей метод дозволяє отримати більш точну інформацію про клавіатурний почерк, оскільки користувач вводить фрагменти тексту, а не лише пароль. Проте він може бути менш зручним для користувача, оскільки вимагає введення більш довгого фрагменту текстової інформації.

Прихована фіксація вихідних даних під час роботи користувача. Цей метод надає найвищу точність в розпізнаванні клавіатурного почерку, але вимагає

відносно більших обчислювальних ресурсів для постійного моніторингу. Він може бути корисним для захисту важливої інформації, але також може породжувати питання щодо конфіденційності користувачів.

Важливо враховувати, що ці методи ефективні лише у випадку, якщо у користувача є сформований клавiатурний почерк. Користувачі без сформованого клавiатурного почерку можуть мати великий розкид характеристик, що робить ідентифікацію та аутентифікацію більш складними.

Розглянемо переваги і недоліки цієї методики:

Переваги методики аутентифікації та ідентифікації за клавiатурним почерком:

- Унікальність: Кожна особа має свій унікальний клавiатурний почерк, оскільки рухи пальців і руки, швидкість та ритм натискання клавiш відрізняються від особи до особи;
- Зручність: Ця методика не вимагає додаткового обладнання, окрім стандартної клавiатури, що робить його зручним для використання в різних ситуаціях;
- Малоімовірність підробки: Важко підробити клавiатурний почерк іншої особи, оскільки він залежить від багатьох факторів, в тому числі фізичних характеристик та навичок користувача.

Недоліки методики аутентифікації та ідентифікації за клавiатурним почерком:

- Помилки аутентифікації та ідентифікації: Можливі помилки при аутентифікації та ідентифікації через зміни в клавiатурному почерку (наприклад, в разі травми, навчання новим навичкам або зміни загального стану людини відносно стану під час створення еталону);
- Залежність від умов: Якщо клавiатурна робоча обстановка змінюється (наприклад, змінюється тип клавiатури), то це може вплинути на якість ідентифікації.

У підсумку, методика аутентифікації та ідентифікації за клавiатурним почерком має свої переваги та недоліки. Він може бути використаний як один з

компонентів біометричної системи ідентифікації, але може потребувати додаткових методик для підвищення рівня безпеки та надійності, особливо в важливих сферах, як от фінанси або безпека даних.

Помилки першого і другого роду – це ключові поняття в статистиці та оцінці ефективності біометричних систем, які використовуються для аутентифікації особистості. Вони визначають, які види помилок можуть виникнути під час використання таких систем.

Помилка першого роду (False Rejection Rate, FRR) виникає, коли гіпотеза відхиляється, хоча насправді вона є істинною. Іншими словами, це помилкове спрацьовування, коли система помилково стверджує, що особа не є зареєстрованим користувачем або не має доступ до ресурсу, хоча насправді вона є зареєстрованим користувачем або має права доступу. Ця помилка створює проблеми, оскільки додаткові спроби аутентифікації можуть призвести до незручностей для користувачів і зниження зручності використання системи.

Помилка другого роду (False Acceptance Rate, FAR) виникає, коли гіпотеза приймається, хоча насправді вона є помилковою. Іншими словами, це помилкове спрацьовування, коли система помилково стверджує, що особа є зареєстрованим користувачем або має доступ до ресурсу, хоча насправді вона не є зареєстрованим користувачем або не має права доступу. Це може призвести до порушення правил безпеки системи, оскільки зловмисник отримає несанкціонований доступ [12].

Баланс між помилками першого і другого роду важливий під час проєктування біометричних систем. Цей баланс і є точністю системи і залежить від конкретних вимог і сценаріїв використання. У деяких випадках суворіші умови безпеки можуть вимагати зменшення помилки другого роду (зменшення FAR), навіть якщо це призведе до збільшення помилки другого роду (збільшення FRR), і навпаки.

Оцінка клавіатурного почерку може проводитися за допомогою двох основних підходів: ймовірно-статистичних методів і засобів штучного інтелекту.

Ймовірно-статистичні методи базуються на обчисленні математичного очікування або дистанційних метрик вибірки та подальшому порівнянні динамічних характеристик з еталоном користувача.

Вважається, що методи, які базуються на засобах штучного інтелекту, можуть забезпечити більш високу точність при оцінці клавіатурного почерку, але при цьому вони вимагають значних обчислювальних ресурсів. Також варто враховувати дві додаткові проблеми в такому підході. По-перше, навчання такої системи може займати багато часу. По-друге, неможливо надати системі навчальну вибірку для всіх можливих користувачів.

Для більш ефективного розпізнавання користувачів можна застосувати періодичне оновлення профілів клавіатурного почерку користувачів. Цей спосіб, однак, створює певні незручності, особливо – для методів, які базуються на використанні засобів штучного інтелекту. Періодичне перенавчання систем, створених за зазначеними методами може тривати доволі довго, в залежності від наявної бази даних профілів клавіатурного почерку користувачів.

#### **1.4 Висновки за розділом**

Розглянуті основні поняття біометрії, можливі характеристики клавіатурного почерку, підходи оцінки клавіатурного почерку, способи оцінки ефективності біометричних систем.

## 2 АНАЛІЗ ВІДОМИХ МЕТОДІВ ОЦІНКИ КЛАВІАТУРНОГО ПОЧЕРКУ

### 2.1 Методи оцінки клавіатурного почерку на базі ймовірнісно-статистичного підходу

В статті [13] розглядається метод оцінки почерку клавіатури як біометричної характеристики за допомогою міри Хеммінга. Параметри клавіатурного почерку, які аналізуються за допомогою цього методу включають тривалість натискання клавіш і часові інтервали між відпусканням та натисканням сусідніх клавіш. Міра Хеммінга вимірює різницю між двома рядками однакової довжини та використовується для порівняння даних користувача з біометричним еталоном. Цей еталон визначається довірчими інтервалами для часових параметрів і максимально допустимою відстанню Хеммінга. Для визначення довірчих інтервалів використовуються такі математичні показники, як середнє значення, середнє квадратичне відхилення та порогові значення для вимірювання Хеммінга.

Згідно з представленим алгоритмом в методі розпізнавання користувача за допомогою міри Хеммінга формується вектор біометричних параметрів (час утримання клавіші та часовий інтервал між відтисканням та натисканням сусідніх клавіш). Загальний вигляд набору біометричних параметрів представлено в векторі:

$$v = (\tau_1^h, \tau_1^{ud}, \tau_2^h, \tau_2^{ud}, \dots, \tau_{n-1}^h, \tau_{n-1}^{ud}, \tau_n^h) \quad (2.1)$$

Розрахунки часу утримання та часу інтервалу між відтисканням та натисканням сусідніх клавіш відбуваються за формулами:

$$\tau_i^h = T_i^{up} - T_i^{down} \quad (2.2)$$

$$\tau_i^{ud} = T_i^{down} - T_{i-1}^{up} \quad (2.3)$$

де  $\tau_i^h$  – час утримання  $i$ -ї клавіші;

$\tau^{ud}_i$  – часовий інтервал між натисканням  $i$ -ї клавіші та відпусканням  $i - 1$  клавіші;

$T^{down}$  – час натискання клавіші;

$T^{up}$  – час відтискання клавіші.

Час утримання визначається як різниця в часі між моментом натискання та відпускання  $i$ -ї клавіші.

Часовий інтервал між взаємодією з клавішами відповідає різниці між моментом натискання  $i$ -тої клавіші та моментом відтискання  $i-1$  клавіші.

Також створюється еталон біометричних характеристик. Він формується у вигляді довірчих інтервалів для певних часових параметрів та максимально допустимої відстані Хеммінга між еталонними та наданими під час аутентифікації параметрами. Загальний вигляд еталону представлено в векторі:

$$V_e = (\min(t_1), \max(t_1), \min(t_2), \max(t_2), \dots, \min(t_N), \max(t_N), E_p) \quad (2.4)$$

де  $E_p$  – поріг для міри Хеммінга для цього користувача, розрахунок порогового значення міри Хеммінга відбувається за формулою:

$$E_p = (m(E_v) + C[L, (1 - p)] \times \sigma(E_v)) \quad (2.5)$$

Розрахунок порогових значень  $\max(t_N)$  та  $\min(t_N)$  відбувається за формулами:

$$\min(t_i) = (m(t_i) - T[L, (1 - p)] \times \sigma(t_i)) \quad (2.6)$$

$$\max(t_i) = (m(t_i) + T[L, (1 - p)] \times \sigma(t_i)) \quad (2.7)$$

де  $T[L, (1-p)]$ ,  $C[L, (1-p)]$  – коефіцієнти Стюдента;

$L$  – ступінь свободи;

$p$  – ймовірність помилки першого роду;

$t_i$  –  $i$ -й часовий інтервал відповідного параметру клавіатурного почерку;

$m(t_i)$  – математичне сподівання  $i$ -го часового інтервалу;

$\sigma(t_i)$  – середнє квадратичне відхилення  $i$ -го часового інтервалу;

$m(E_v)$  – математичне сподівання міри Хеммінга для вектора користувача до еталонного;

$\sigma(E_v)$  – середнє квадратичне відхилення міри Хеммінга для вектора користувача до еталонного;

$E_p$  – порогове значення міри Хеммінга для відповідного користувача;

$E_v$  – міра Хеммінга від заданого вектора до еталона, розрахунок міри відбувається за формулою:

$$E_v = \sum_{i=1}^N e_i \quad (2.8)$$

де  $e_i$  – відстань між відповідними часовими інтервалами даного вектора та еталона, визначається за формулою:

$$e_i = \begin{cases} 0, & t_i \in [\min(t_i), \max(t_i)] \\ 1, & t_i \notin [\min(t_i), \max(t_i)] \end{cases} \quad (2.9)$$

Таким чином рішення про відповідність профіля користувача еталону приймається, якщо виконується умова:

$$E_v \leq E_p \quad (2.10)$$

Тобто міра Хеммінга профіля користувача до еталона не більше порогового значення міри Хеммінга для цього користувача.

## **2.2 Методи оцінки клавіатурного почерку з використанням засобів штучного інтелекту**

З наявних джерел відомо про спроби використання і дослідження ефективності засобів штучного інтелекту в методах оцінки клавіатурного почерку. Деякі широко використовувані штучні нейронні мережі в методах

оцінки клавіатурного почерку: мережа радіальної базисної функції [14-15], мережа квантування навчального вектора [16-17], багат шаровий перцептрон [14, 18-20] і самоорганізуюча карта [21].

Розглянемо детальніше метод аутентифікації, запропонований в [15].

В запропонованій системі клавіатурний почерк оцінюється за такими параметрами: максимальний час утримання та затримка між натисканням, оскільки ця комбінація функцій, за словами авторів, є ефективною комбінацією. Крім того, введено новий параметр для підвищення рівня ефективності в запропонованій системі – загальний час вводу тексту. Загальний час визначається як час, потрібний особі, щоб ввести весь фрагмент тексту. Таким чином, запропонована система використовує три параметри для оцінки клавіатурного почерку, а саме максимальний час утримання клавіши, інтервал між натисканням клавіш та загальний час введення фрагмента тексту.

Запропонований засіб для оцінки клавіатурного почерку – штучна нейронна мережа радіально базисних функцій, архітектуру в загальному вигляді приведено на рисунку 2.1.

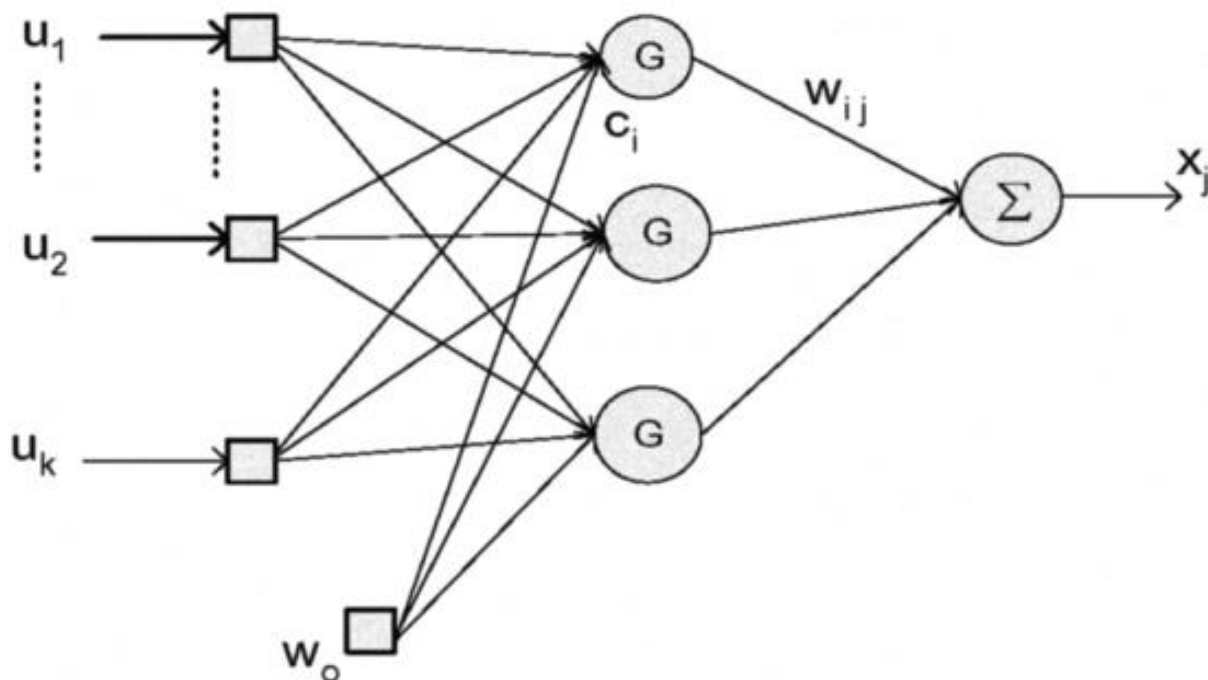


Рисунок 2.1 – Штучна нейронна мережа радіально базисних функцій

Перетворення від вихідного простору до прихованого одиничного простору є нелінійним, тоді як перетворення прихованого одиничного простору в результуючий простір  $j$  є лінійним. Математична модель RBFN може бути виражена в формулі:

$$x_j = f(u) = w_0 + \sum_{i=1}^N w_{ij} G(|u - c_i|) \quad (2.1)$$

де  $w_0$  – зміщення;

$w_{ij}$  – вага;

$u$  – вектор сигналів на вході;

$c_i$  – центр базисної функції для вузла  $i$  на прихованому шарі;

$N$  – кількість прихованих нейронів;

Підсумовуючи, кроки побудови системи аутентифікації за клавіатурними почерком наступні на базі ШНМ (штучної нейронної мережі):

- Збір даних;
- Визначення структури та параметрів ШНМ;
- Навчання ШНМ для кожної особи з використанням профілю введення та бажаного результату;
- Перевірка навченої ШНМ.

Дослідження проводили в групі з тридцяти осіб. Кожна авторизована особа повинна була ввести шість символів власного пароля 80 разів, 40 наборів використовуються для навчання, а решта використовуються для тестування даних. У кожному символі пароля включено три функції, а потім об'єднано всі три функції (максимальні сили, час затримки та загальна швидкість введення). Для прикладу було обрано пароль «avbmj2». В результаті аналізуються такі параметри:

- шість інтервалів максимального часу утримання  $a, v, b, m, j, 2$ ;
- п'ять часових інтервалів між натисканням клавіш  $a-v, v-b, b-m, m-j, j-2$ ;
- один часовий інтервал введення всього фрагменту тексту  $avbmj2$ .

В роботі [17] автори запропонували мережу квантування навчального вектору з повторним навчанням як засіб аутентифікації.

Структура функціонування системи наведено на рисунку 2.2.

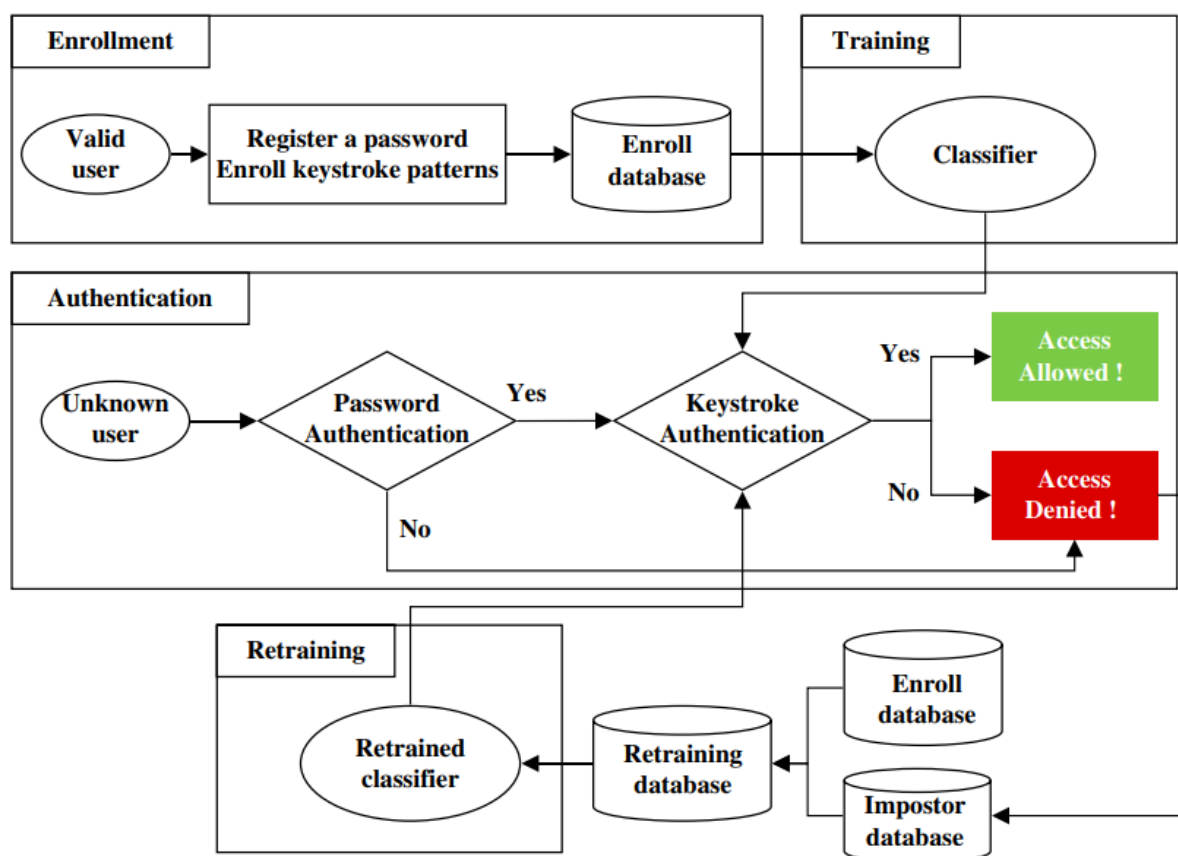


Рисунок 2.2 – Структура функціонування системи аутентифікації на базі мережі квантування навчального вектору з повторним навчанням

Спочатку кожен дійсний користувач надає свої власні шаблони натискання клавіш, створюючи базу даних реєстрації. Після створення детектора новизни з базою даних реєстрації система аутентифікації розгортається для роботи. З кількох спроб входу одні отримують доступ, а інші ні. Шаблони натискання тих, хто не отримав доступ розглядаються як нові або самозвані шаблони, які об'єднуються в базу даних перепідготовки разом із базою даних реєстрації. Детектор новизни перенавчається за допомогою бази даних перепідготовки, яка містить як шаблони реєстрації користувача, так і шаблони самозванців.

Вихідні дані для навчання склалися з двох груп:

Група А включала набори даних, які були зібрані від 21 дійсного користувача за допомогою клавіатури, підключеної до робочої станції Sun в період з 1996 по 1998 рік. Паролі цих користувачів склалися з 6 до 10 символів. Всього було створено 21 набір даних для 21 пароля. Для кожного пароля користувач надавав від 76 до 388 шаблонів для навчання та 75 для тестування. Також було зібрано 75 шаблонів від "сторонніх" осіб для кожного пароля. Оскільки передбачалося, що навчальний набір повинен бути незбалансованим, то для навчання випадково вибирали 50 шаблонів користувача та 5 шаблонів "стороннього". Тестовий набір складався з 75 шаблонів користувача та 70 шаблонів "стороннього". Всього було випадково вибрано 30 різних навчальних і тестових наборів для кожного пароля

Група Б включала набори даних, зібрані у 2005 році. Ці дані були більш реалістичними з кількох причин. Перше, ця група містила 25 дійсних користувачів, які вводили свої паролі на власних персональних комп'ютерах, а не на спільній робочій станції. Вони використовували клавіатури, з якими були знайомі. Друге, їм було запропоновано вводити інші текстові фрагменти між своїми паролями, щоб уникнути послідовного введення одного і того ж пароля. Третє, для аналізу прив'язаності до пароля кожен користувач вводив два види паролів: старий, який він використовував тривалий час, і новий, який він прийняв перед збором даних. Для кожного пароля дійсний користувач вводив його 30 разів для навчання і 24 рази для тестування, тоді як кожен із інших 24 користувачів вводив пароль один раз як "сторонній". Навчальний набір складався з 30 шаблонів користувача та трьох шаблонів "стороннього", тестовий набір – з 24 шаблонів користувача та 21 шаблону "стороннього".

В роботі [19] автори запропонували багатосаровий перцептрон з алгоритмом зворотного поширення помилки як ядро системи ідентифікації для розпізнавання осіб. Аналізували два параметри: час утримання клавіш, інтервал між відпусканням натисканням клавіш. Той самий фрагмент, введений десять разів, утворює вихідні вектори, що подаються в нейронну мережу. Учасникам дослідження пропонувалося вводити різні типи паролів: імена, довільні

фрагменти тексту, ключі програмного забезпечення, номери кредитних карток та пін-коди. Ці різноманітні введення використовувалися для перевірки ефективності аутентифікації користувачів.

Було продемонстровано, що більша кількість прихованих нейронів може бути надлишковою та погіршувати ефективність нейронної мережі, рисунок 2.3.

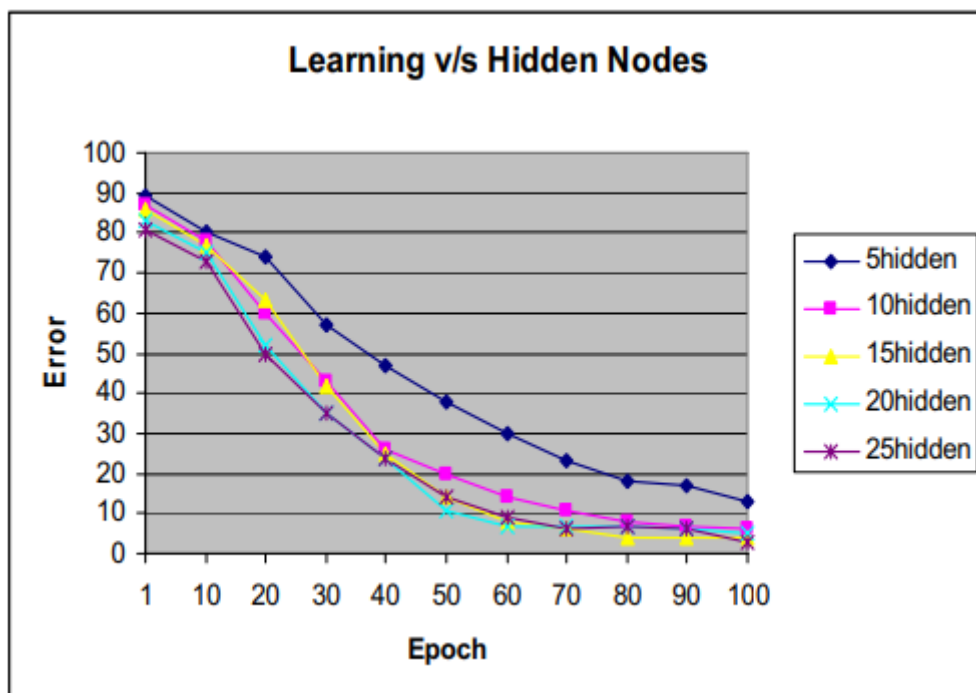


Рисунок 2.3 – Порівняння рівня похибок за епохами при різних конфігураціях ШНМ

Інформацію про представлені в роботах [14-21] штучні нейронні мережі можна звести до інформативних таблиць 2.1 – 2.5.

Таблиця 2.1 – Архітектури нейронних мереж

Назва	Опис
Радіально-базисна функція (RBF)	Використовує радіально-базисні функції як активацію, ефективна для вирішення завдань класифікації та апроксимації.
Квантування навчального вектора	Мережа, яка адаптує ваги для представлення кластерів вхідних даних. Часто використовується для завдань кластеризації.

Закінчення таблиці 2.1

Назва	Опис
Багатошаровий перцептрон (MLP)	Найбільш поширена нейронна мережа, що складається з вихідного шару, одного або декількох прихованих шарів та результуючого шару. Використовується для різних завдань, від класифікації до регресії.
Самоорганізуюча карта (SOM)	Використовується для візуалізації та інтерпретації великих даних, навчаючись без вчителя для представлення даних у двовимірному просторі.

Таблиця 2.2 – Типи навчання нейронних мереж

Тип навчання	Опис
Навчання з учителем	Передбачає наявність вчителя, який надає алгоритму приклади вхідних даних та відповідних їм правильних відповідей. Алгоритм навчається на цих даних, намагаючись мінімізувати помилку.
Навчання без вчителя	Немає явних правильних відповідей (міток). Алгоритм намагається самостійно знайти структуру в даних, наприклад, кластеризацію чи зменшення розмірності.
Навчання з підкріпленням	Модель навчається приймати рішення, ґрунтуючись на винагороді або покаранні за свої дії, без явної вказівки правильних відповідей.

Таблиця 2.3 – Алгоритми навчання нейронних мереж

Алгоритм навчання	Опис
Градiєнтний спуск	Основний алгоритм для оптимізації нейронних мереж, який прагне мінімізувати функцію втрат, налаштовуючи ваги на основі градієнта помилки.
Стохастичний градієнтний спуск (SGD)	Варіація градієнтного спуску, де оновлення ваг відбувається для кожного навчального прикладу, що часто призводить до швидшої збіжності.
Метод зворотного поширення помилки	Поширений метод навчання для багат шарових перцептронів, що включає пряме поширення вхідних даних та зворотне поширення помилки для оновлення ваг.
Алгоритми оптимізації (Adam, RMSprop тощо)	Сучасні варіанти стохастичного градієнтного спуску, які адаптують швидкість навчання для кожного параметра, покращуючи процес навчання.

Таблиця 2.4 – Функції активації в нейронних мережах

Функція активації	Опис
Сигмоїд (Логістична функція)	Перетворює вхідне значення в діапазоні (0, 1), корисна для бінарної класифікації.
Гіперболічний тангенс (tanh)	Перетворює вхідне значення в діапазоні (-1, 1), забезпечуючи сильніші градієнти, ніж сигмоїд.
ReLU (Rectified Linear Unit)	Проста функція, що повертає вхідне значення, якщо воно додатне, та нуль у протилежному випадку. Ефективна та широко використовується в глибокому навчанні.

Закінчення таблиці 2.4

<b>Функція активації</b>	<b>Опис</b>
Leaky ReLU	Варіація ReLU, що дозволяє невеликий градієнт, коли вхід менше нуля, для вирішення проблеми "вмираючих" нейронів.
Нормована експоненційна функція (softmax)	Перетворює вхідні значення в ймовірнісний розподіл, що може використовуватися для класифікації.

Таблиця 2.5 – Типи зв'язків у нейронних мережах

<b>Тип зв'язку</b>	<b>Опис</b>
Пряме поширення	Процес передачі вхідних даних через шари нейронної мережі для отримання вихідного результату.
Рекурентний	Зв'язок, що дозволяє передачу інформації від попередніх кроків до поточного стану, корисний для задач, де потрібно пам'ятати контекст.

### 2.3 Висновки за розділом

Проведено аналіз двох класів відомих методів оцінки клавiатурного почерку. Наведено найбільш поширені засоби штучного інтелекту, які використовуються для оцінки клавiатурного почерку.

## 3 РОЗРОБКА ЗАСОБІВ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ ЗА КЛАВІАТУРНИМ ПОЧЕРКОМ НА БАЗІ ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ

### 3.1 Вибір середовища розробки

Найбільш поширені інструменти розробки засобів штучного інтелекту наведено в таблиці 3.1.

Таблиця 3.1 – Інструменти розробки засобів штучного інтелекту

Інструмент	Опис	Рівень програмування	Візуальне програмування	Платний/Безкоштовний
TensorFlow	Потужна і широко використовувана платформа для глибокого навчання	Високий	Ні	Безкоштовний
PyTorch	Гнучкий та інтуїтивно зрозумілий фреймворк для глибокого навчання	Середній - високий	Ні	Безкоштовний
Keras	Високорівневий API для машинного навчання, легкий у вивченні	Низький - середній	Ні	Безкоштовний
MATLAB	Потужне середовище для числових обчислень та аналізу даних	Середній - високий	Ні	Ознайомча версія
Orange	Візуальний інструмент для аналізу даних та машинного навчання	Низький - середній	Так	Безкоштовний

TensorFlow, PyTorch і Keras, є дуже популярними і мають свої переваги, особливо у випадку, коли є необхідність працювати зі специфічними

архітектурами нейромереж або використовувати різні фреймворки машинного навчання. Вибір залежить від ваших конкретних завдань та досвіду в роботі з цими інструментами.

В свою чергу, Matlab має інтуїтивний і легкий в інтерфейс користувача, велику кількість вбудованих функцій та інструментів для роботи з нейронними мережами. Основний додаток для роботи з нейронними мережами – Neural Network Toolbox, який має готові шаблони нейронних мереж та можливості детального налаштування. Matlab може легко інтегруватися з іншими інструментами і бібліотеками для обробки даних та візуалізації, що робить його потужним інструментом для розв'язання комплексних задач. Також Matlab має велику спільноту користувачів і багато ресурсів для навчання, включаючи документацію, онлайн-курси та форуми для обміну досвідом.

Для створення засобів ідентифікації та аутентифікації за клавіатурним почерком було обрано середовище Matlab.

### **3.2 Вибір математичного апарату**

При розгляді можливих засобів штучного інтелекту для проєктування системи оцінки клавіатурного почерку було обрано штучну нейронну мережу прямого розповсюдження, яка складається з вихідного шару, прихованого шару з сигмоподібна функцією активації та результуючого шару з нормованою експоненційною функцією (softmax).

Для активації прихованого шару використовується функція гіперболічного тангенсу.

Гіперболічний тангенс - функція, яка перетворює значення сигналу на вході в діапазоні від -1 до 1, рисунок 3.1.

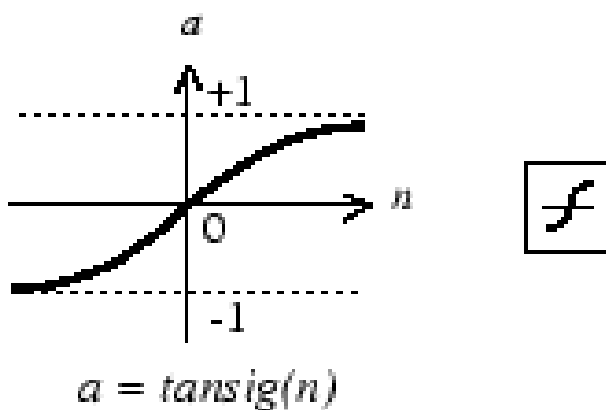


Рисунок 3.1 – Функція гіперболічного тангенсу

Значення результуючого сигналу обчислюється за формулою:

$$f(x) = \frac{1}{1+e^{-x}} \quad (3.1)$$

де  $x$  – значення сигналу на вході.

Для активації результуючого шару використовується нормована експоненційна функція:

Нормована експоненційна функція – функція, яка «стискує» вектор сигналів на вході до вектору розподілу ймовірностей зі значенням від 0 до 1, які в сумі дають одиницю, рисунок 3.2.

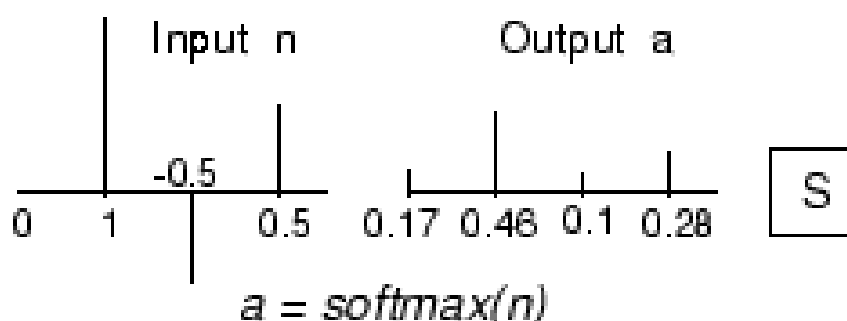


Рисунок 3.2 – Приклад перетворення вектору сигналів на вході в вектор розподілу ймовірностей в результаті

Значення результуючого сигналу обчислюється за формулою:

$$\sigma(z)_j = \frac{e^{z_j}}{\sum_{k=1}^K e^{z_k}} \quad (3.2)$$

де  $z_j$  – значення  $j$ -го сигналу на вході

$K$  – розмірність вектору сигналів на вході.

Для визначення кількості нейронів в прихованому шарі ШНМ треба визначити кількість синаптичних ваг за формулою [22]:

$$\frac{mN}{1+\log_2 N} \leq L_w \leq m \left( \frac{N}{m} + 1 \right) (n + m + 1) + m \quad (3.3)$$

де  $m$  – розмірність вектору сигналів на виході;

$n$  – розмірність вектору сигналів на вході;

$N$  – кількість елементів навчальної вибірки;

$L_w$  – кількість синаптичних ваг.

Наступний етап – обчислити кількість нейронів в прихованому шарі ШНМ за формулою:

$$L = \frac{L_w}{(n+m)} \quad (3.4)$$

де  $L$  – кількість нейронів у прихованому шарі.

Пакет прикладних програм Matlab пропонує додаток Neural Net, який має шаблони для створення нейронної мережі.

Обраний шаблон – Neural Network Pattern Recognition (нейронна мережа для розпізнавання паттернів). Шаблон цієї нейронної мережі відповідає математичному апарату, обраному в розділі. Узагальнена структура штучної нейронної мережі для розпізнавання паттернів, наведено на рисунку 3.3.

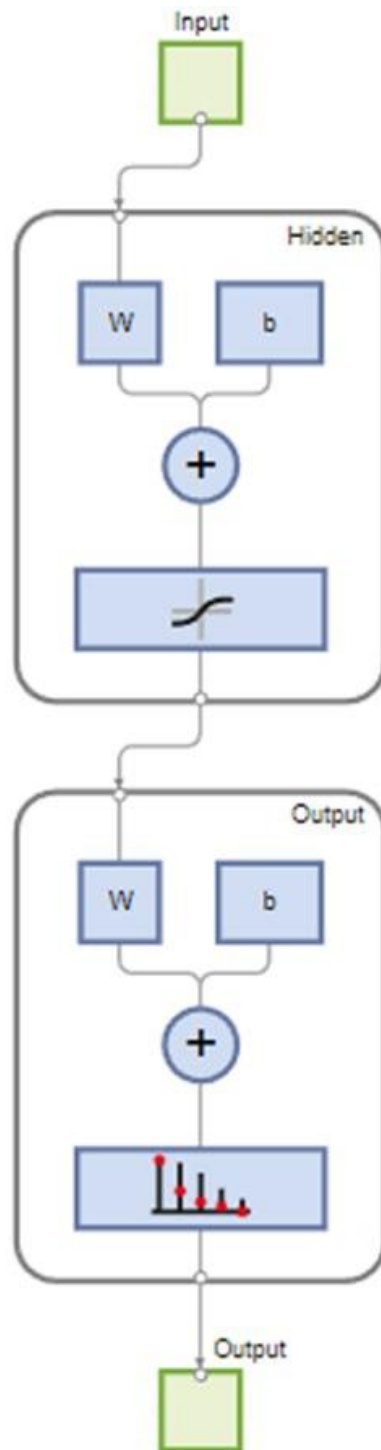


Рисунок 3.3 – Узагальнена структура штучної нейронної мережі

### 3.3 Структура та підготовка вибірки

Загальний набір даних є авторським і складається з унікальних даних десяти осіб. Для оцінки клявіатурного почерку обрані наступні параметри:

- середній час утримання клявіші;
- середній інтервал часу між відпусканням та натисканням клявіш.

Кожен користувач вводив однаковий фрагмент тексту «the quick brown fox jumps over the lazy dog». Представлений фрагмент тексту був обраний тому що містить всі маленькі літери англійського алфавіту.

В підсумку ми маємо 27 унікальних параметрів часу утримання клавіш (всі літери англійського алфавіту та пробіл) і 39 унікальних параметрів часового інтервалу між відпусканням та натисканням клавіш (t - h, h - e, e - « », « » - q, q - u, ..., o - g), тобто кожен шаблон користувача описується 66 параметрами.

При створенні шаблону, користувачі вводять ключовий фрагмент тричі, по кожному параметру підраховується середнє значення.

Кожен користувач надає 100 шаблонів клавіатурного почерку. Тобто загальний набір даних складається з 1000 шаблонів клавіатурного почерку, які мають 66000 унікальних параметрів клавіатурного почерку.

Також відповідно до вихідних даних сформовано відповідні результуючі дані, які описують відповідність вихідного шаблону тому чи іншому користувачеві.

Зміст загального набору даних наведено в додатку А.

Розподіл на навчальну, валідаційну та тестову вибірки зроблено в наступному підрозділі, оскільки є мета дослідити ефективність нейронної мережі при різних значеннях цих параметрів.

Структуру вибірки по одному на прикладі одного користувача наведено на рисунку 3.4.

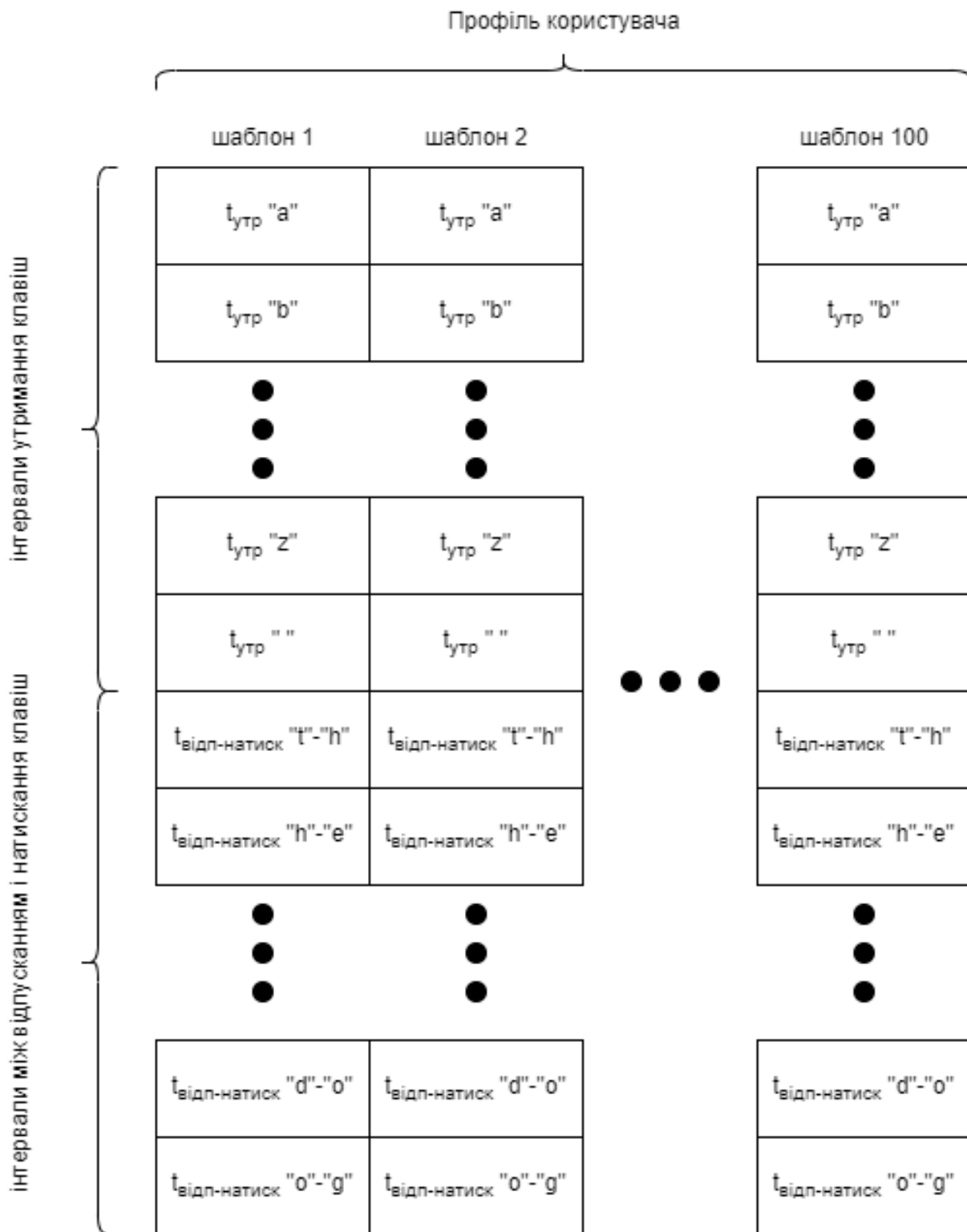


Рисунок 3.4 – Структура вибірки на прикладі одного користувача

Приклад частини вибірки загальних даних в середовищі Matlab наведено на рисунку 3.5.

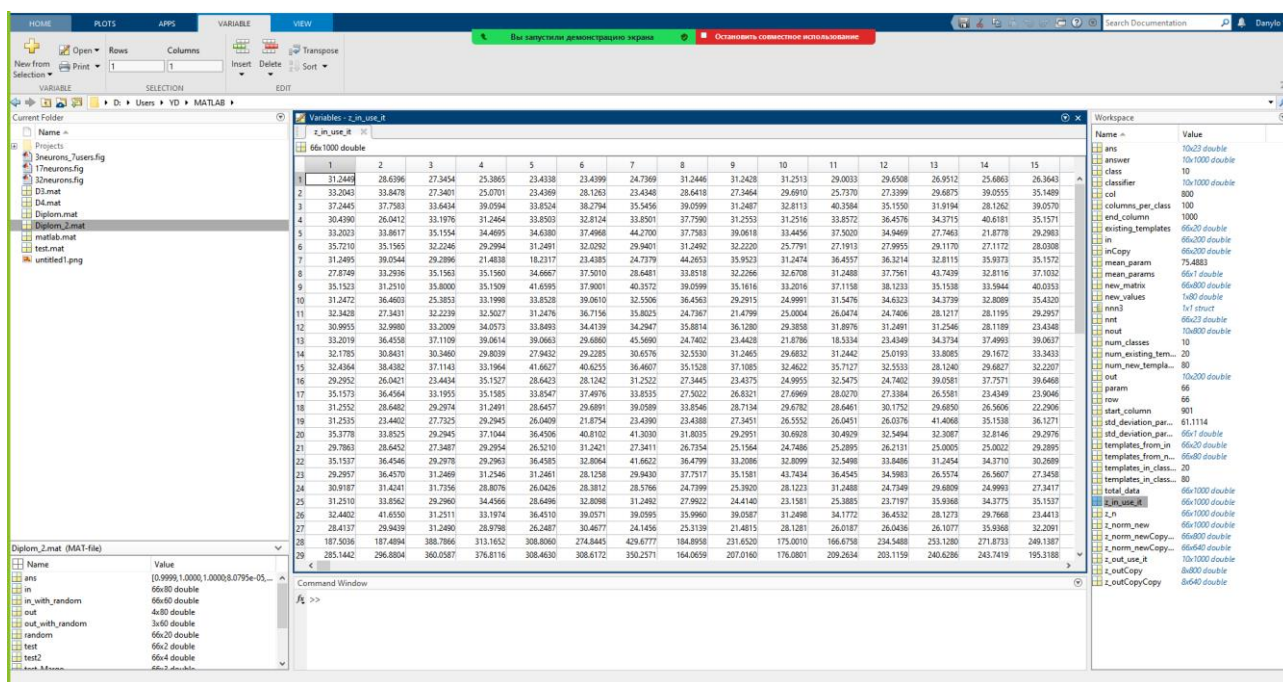


Рисунок 3.5 – Приклад частини вибірки в середовищі Matlab

### 3.4 Експериментальне визначення найбільш ефективних параметрів нейронної мережі

Проведемо дослідження залежності ефективності штучної нейронної мережі від обраних параметрів ШНМ:

- Кількість нейронів в прихованому шарі;
- Відсотки розподілу набору даних на навчальну, валідаційну та тестову вибірки.

При розподілі набору даних в таких пропорціях:

- навчальна вибірка 40%;
- валідаційна вибірка 30%;
- тестова вибірка 30%,

кількість нейронів в прихованому шарі, обчислена за (3.4), може коливатися від 2 до 103.

Проведемо дослідження ефективності ШНМ з параметрами, що задовольняють обраним умовам, результати представлені в таблиці 3.1.

Таблиця 3.1 – Результати дослідження ефективності ШНМ при розподілі вибірки 40-30-30

		Кількість нейронів в прихованому шарі								
		10	15	20	30	34	40	50	70	100
Ефективність, %	1 експ.	90,5	95	91,7	90	96	91,7	96,7	90	85
	2 експ.	96,7	98,3	96,7	78,3	98	96,7	88,3	83,3	86,7
	3 експ.	93,3	93,3	90	85	96	90	93,3	95	85

Графічне представлення порівняння ефективності ШНМ представлено на рисунку 3.6.



Рисунок 3.6 – Графік залежності ефективності ШНМ від кількості нейронів в прихованому шарі, варіант розподілу по вибірках 40-30-30

При розподілі набору даних в таких пропорціях:

- навчальна вибірка 80%;
- валідаційна вибірка 10%;
- тестова вибірка 10%,

кількість нейронів в прихованому шарі, обчислена за (3.4), може коливатися від 3 до 172.

Проведемо дослідження ефективності ШНМ з параметрами, що задовольняють обраним умовам, результати представлені в таблиці 3.2.

Таблиця 3.2 – Результати дослідження ефективності ШНМ при розподілі вибірки 80-10-10.

		Кількість нейронів в прихованому шарі								
		10	15	20	30	34	40	50	70	100
Ефективність,	1 експ.	100	100	96,7	96,7	100	96,7	100	90	93,3
	2 експ.	96,7	100	93,3	93,3	99	100	96,7	93,3	100
	3 експ.	93,3	96,7	100	93,3	99,3	96,7	96,7	96,7	93,3

Графічне представлення порівняння ефективності ШНМ представлено на рисунку 3.7.



Рисунок 3.7 – Графік залежності ефективності ШНМ від кількості нейронів в прихованому шарі, варіант розподілу по вибірках 80-10-10

Таким чином обрано параметри, при яких штучна нейронна мережа має найбільшу ефективність, а саме штучна мережа з 34 нейронами в прихованому шарі та розподілом вибірки:

- навчальна вибірка 80%;
- валідаційна вибірка 10%;
- тестова вибірка 10%.

### 3.5 Висновки за розділом

Обрано середовище розробки для створення нейронної мережі Matlab. Розроблено структуру нейронної мережі. Підготовлено набір даних для навчання та тестування нейронної мережі. Експериментальним шляхом обрано параметри штучної нейронної мережі, при яких нейронна мережа демонструє найбільшу ефективність.

## 4 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ ЗАСОБІВ

### 4.1 Постановка задачі

Налаштувати, провести навчання та тестування створеної нейронної мережі, структуру якої запропоновано в розділі 3.

Провести дослідження ефективності ідентифікації користувачів за допомогою розробленої штучної нейронної мережі.

Порівняти ефективність ідентифікації та аутентифікації розробленої штучної нейронної мережі з існуючим засобом, який базується на класичному підході [23].

### 4.2 Налаштування, навчання та тестування нейронної мережі

Перший етап налаштування штучної нейронної мережі для ідентифікації та аутентифікації користувачів – імпортування набору вихідних і результуючих даних в додаток створення нейронної мережі, вікно майстра імпорту з обраними вихідними і результуючими даними наведено на рисунку 4.1.

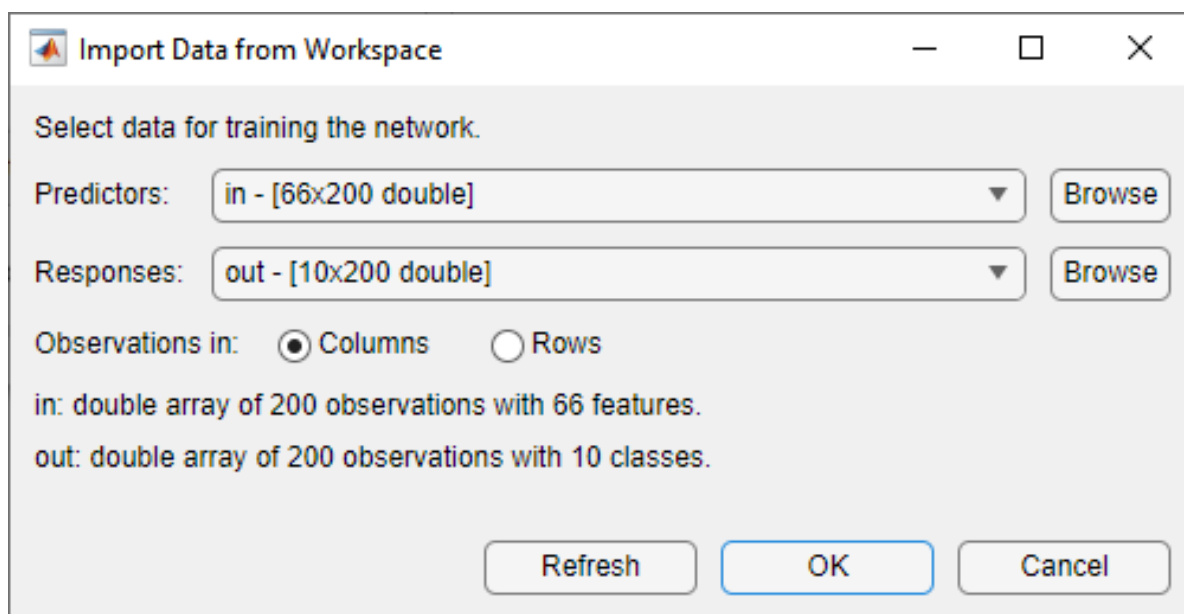


Рисунок 4.1 – Майстер імпорту вихідних та результуючих даних

Другий етап налаштування нейронної мережі:

- Обираємо бажаний відсоток розподілу даних на окремі вибірки – навчальну, валідаційну, тестову;
- Обираємо кількість нейронів в прихованому шарі

Налаштована нейронна мережа з заданими параметрами розподілу даних представлено на рисунку 4.2.

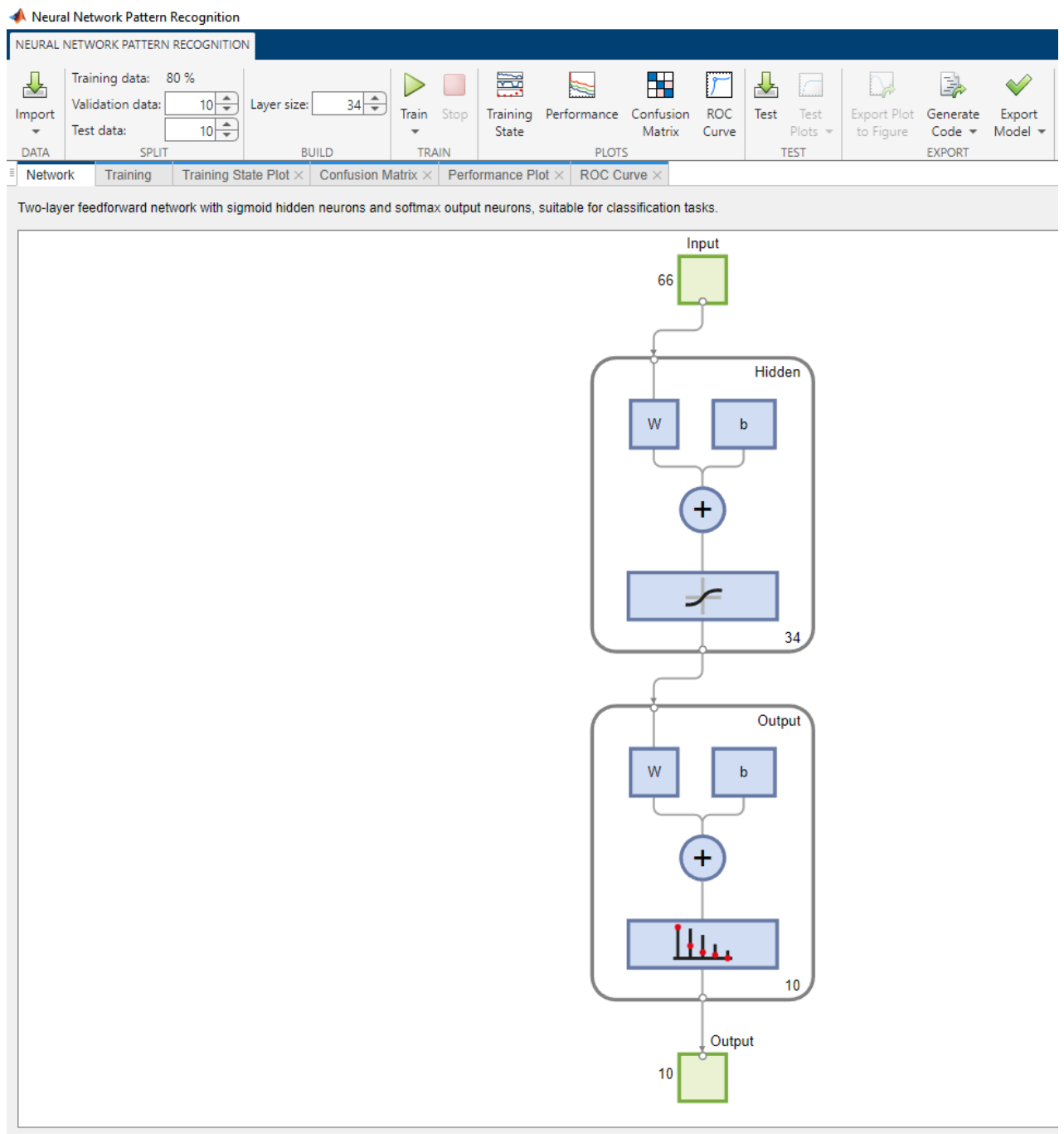


Рисунок 4.2 – Схема налаштованої нейронної мережі

Наступний етап – навчання нейронної мережі, результати навчання представлені на рисунку 4.3.

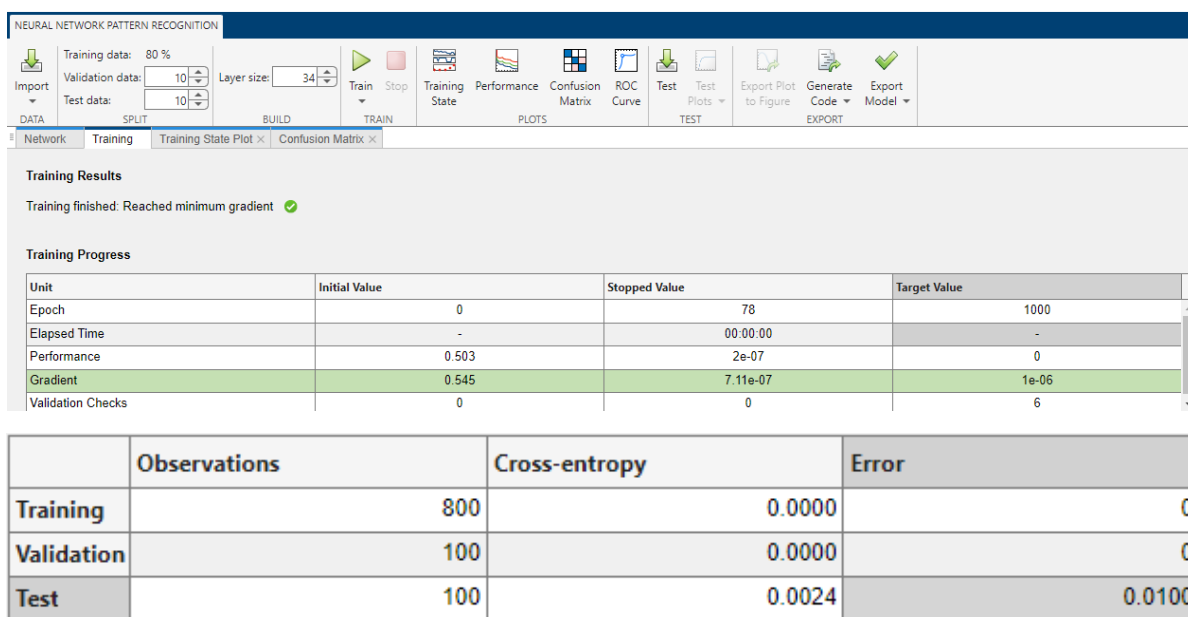


Рисунок 4.3 – Результати навчання нейронної мережі

Детальні відомості про проходження навчання представлено на рисунках 4.4 – 4.6

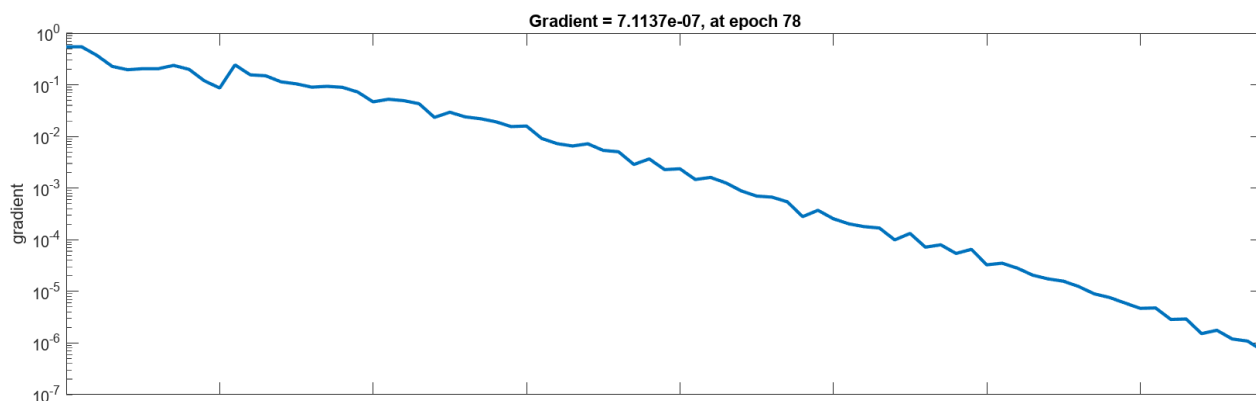


Рисунок 4.4 – Значення градієнту за епохами

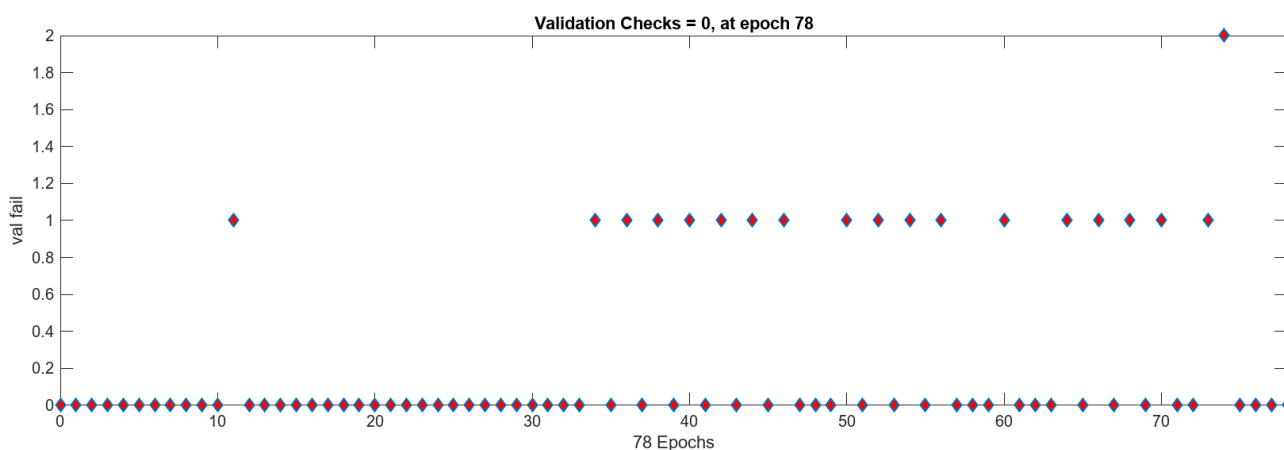


Рисунок 4.5 – Зіставлення даних з валідаційної вибірки за епохами

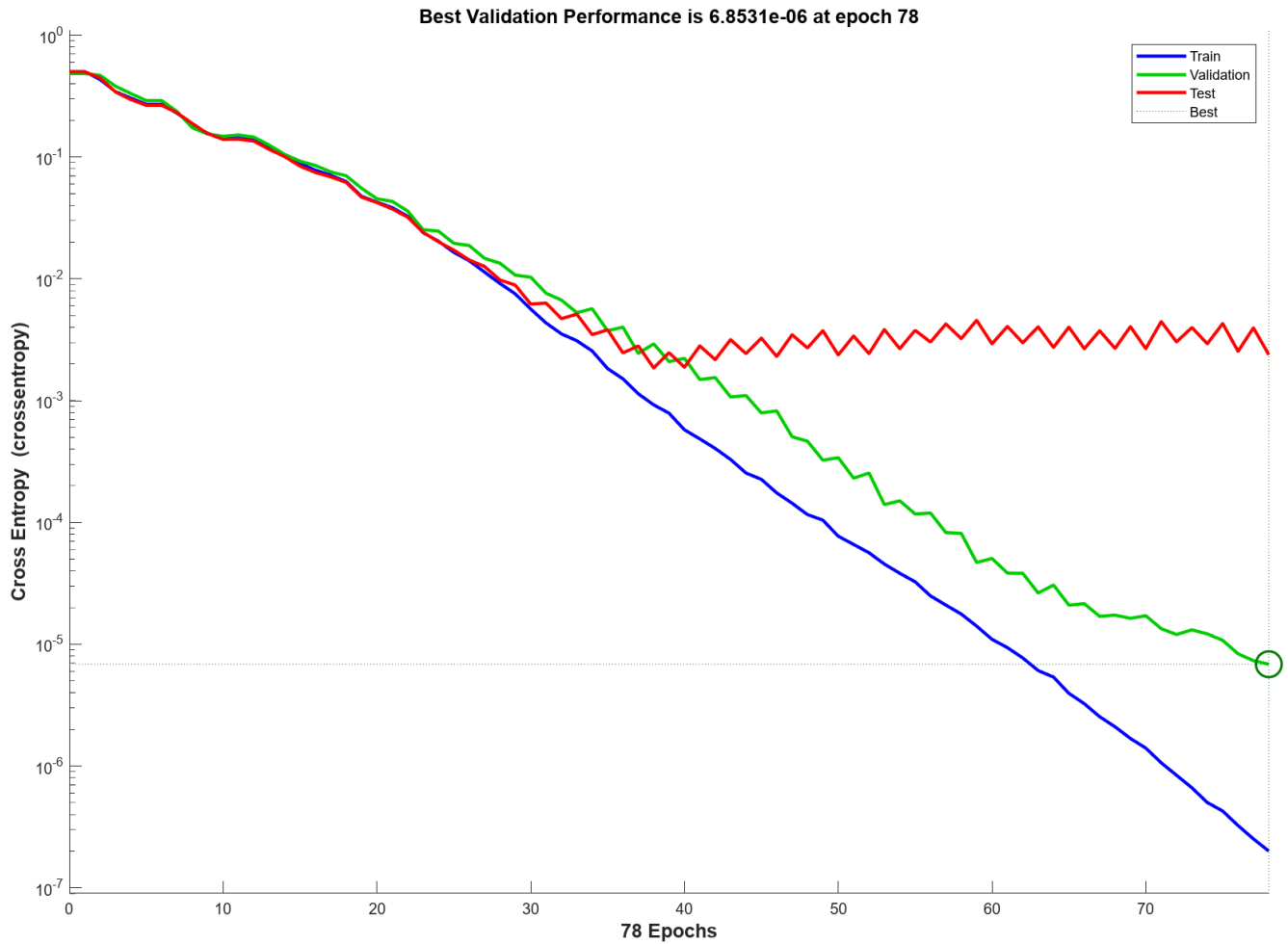


Рисунок 4.6 – Графік перехресної ентропії за епохами

Оцінка ефективності оцінки ідентифікації користувачів у вигляді матриць невідповідностей наведено на рисунках 4.7 – 4.10.

### Training Confusion Matrix

Output Class	1	84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%		
		10.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
	2	0	81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
		0.0%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	3	0	0	76	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
		0.0%	0.0%	9.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	4	0	0	0	75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
		0.0%	0.0%	0.0%	9.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	5	0	0	0	0	83	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
		0.0%	0.0%	0.0%	0.0%	10.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%
	6	0	0	0	0	0	77	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%
	0.0%	0.0%	0.0%	0.0%	0.0%	9.6%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
7	0	0	0	0	0	0	75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100%	
	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	9.4%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
8	0	0	0	0	0	0	0	84	0	0	0	0	0	0	0	0	0	0	0	0	0	100%	
	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	10.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
9	0	0	0	0	0	0	0	0	81	0	0	0	0	0	0	0	0	0	0	0	0	100%	
	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	10.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
10	0	0	0	0	0	0	0	0	0	0	84	0	0	0	0	0	0	0	0	0	0	100%	
	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	10.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
		100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	
		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	
		1	2	3	4	5	6	7	8	9	10												
		Target Class																					

Рисунок 4.7 – Матриця невідповідності навчальної вибірки



### Test Confusion Matrix

Output Class	1	2	3	4	5	6	7	8	9	10	
1	10	0	0	0	0	0	0	0	0	0	100%
2	0	9	0	0	0	0	0	0	0	0	100%
3	0	1	9	0	0	0	0	0	0	0	90.0%
4	0	0	0	15	0	0	0	0	0	0	100%
5	0	0	0	0	10	0	0	0	0	0	100%
6	0	0	0	0	0	9	0	0	0	0	100%
7	0	0	0	0	0	0	8	0	0	0	100%
8	0	0	0	0	0	0	0	8	0	0	100%
9	0	0	0	0	0	0	0	0	11	0	100%
10	0	0	0	0	0	0	0	0	0	10	100%
	100%	0.0%	100%	100%	100%	100%	100%	100%	100%	100%	9.0%
	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	1.0%
	1	2	3	4	5	6	7	8	9	10	

**Target Class**

Рисунок 4.9 – Матриця невідповідності тестової вибірки

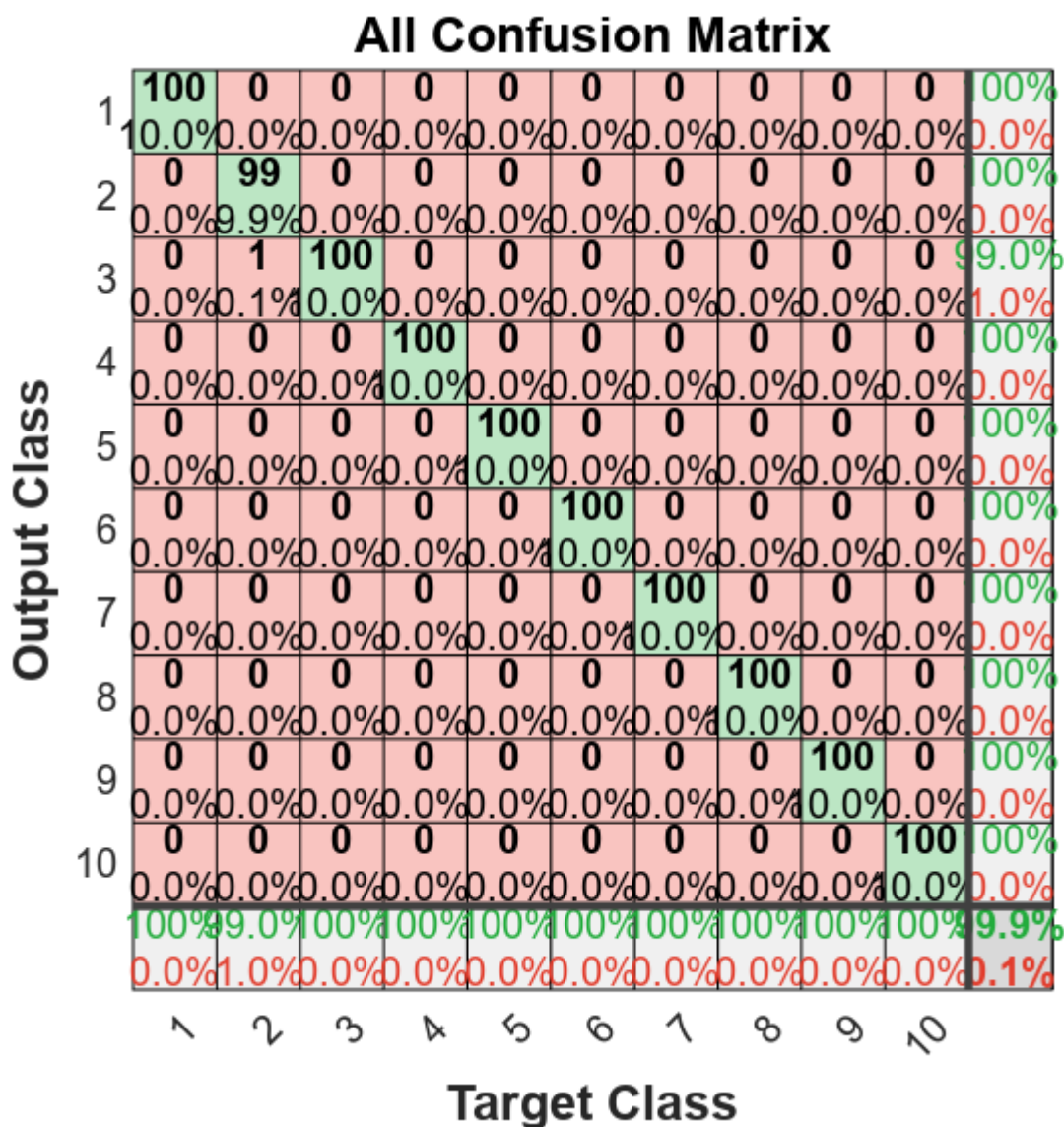


Рисунок 4.10 – Матриця невідповідності загального набору даних

Аналіз ROC-кривої (кривої похибок) можна оцінити якість класифікації. Крива залежності істинно позитивного результату від рівня хибно позитивного результату. Графік кривої похибок відповідних вибірок наведено на рисунках 4.11 – 4.14. Графік починається в точці (0,0) і закінчується в точці (1,1). Чим ближче крива ROC до верхнього лівого кута (0,1), тим краща ефективність системи.

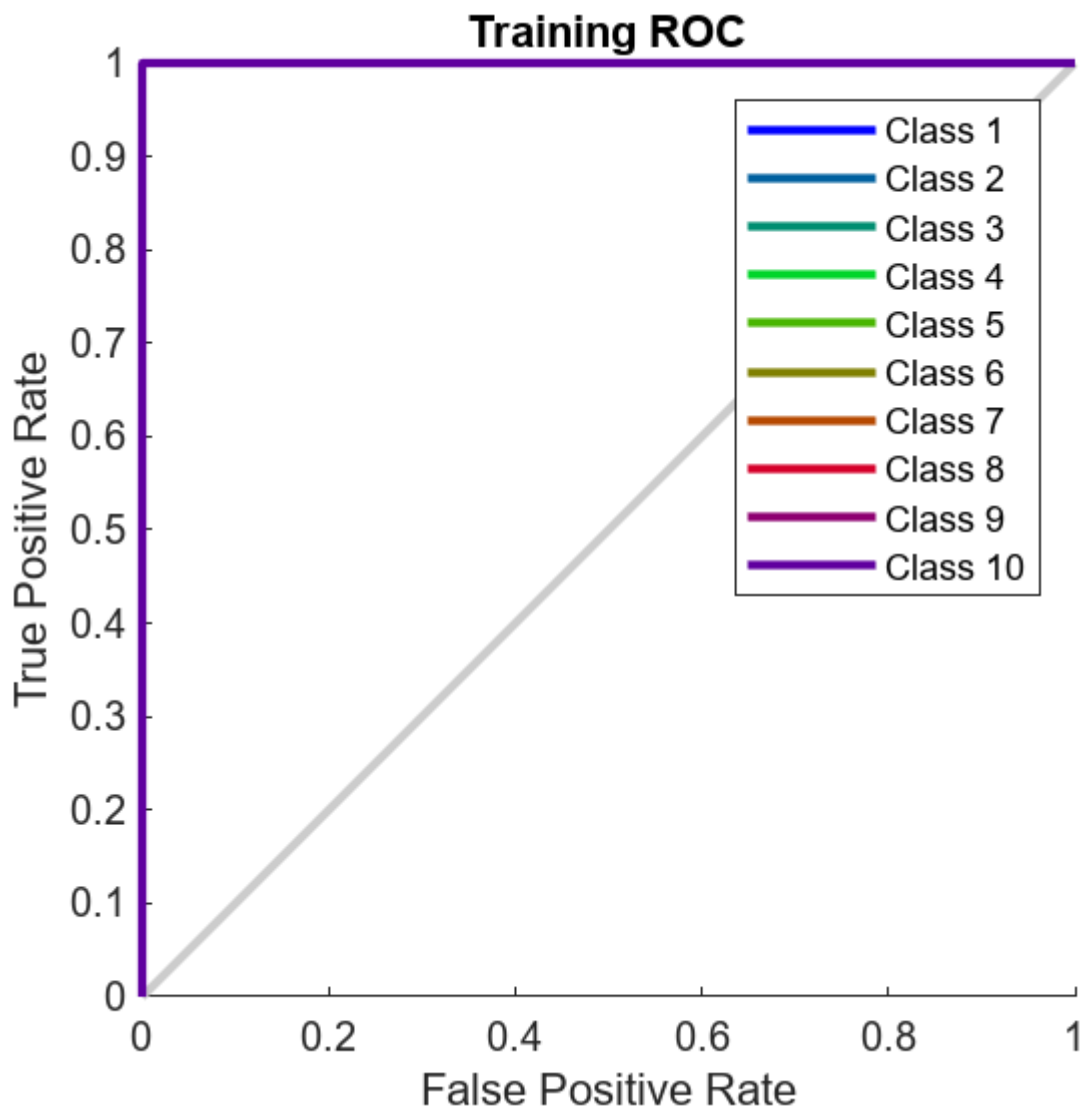


Рисунок 4.11 – Крива похибок тестової вибірки

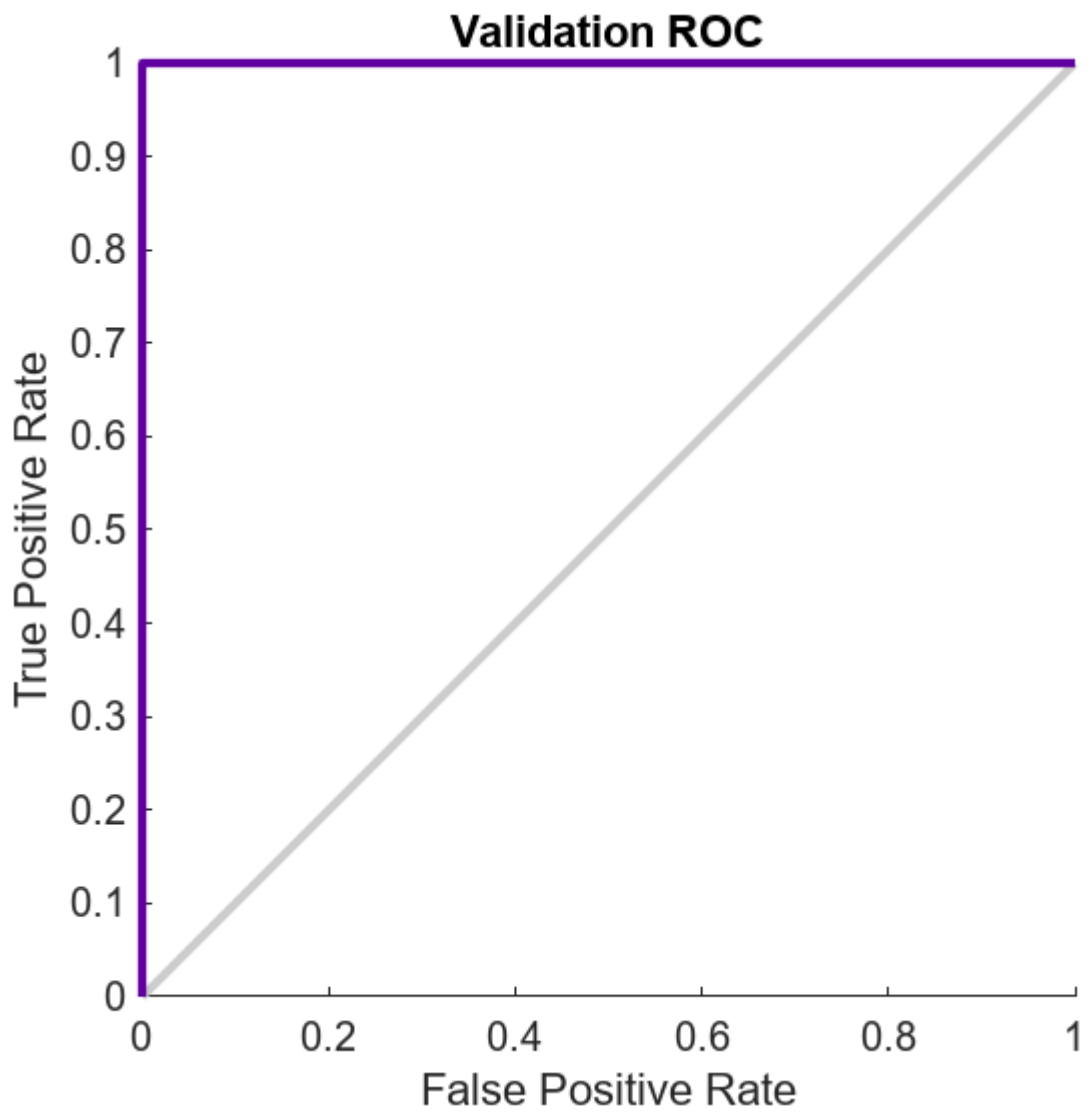


Рисунок 4.12 – Крива похибок валідаційної вибірки

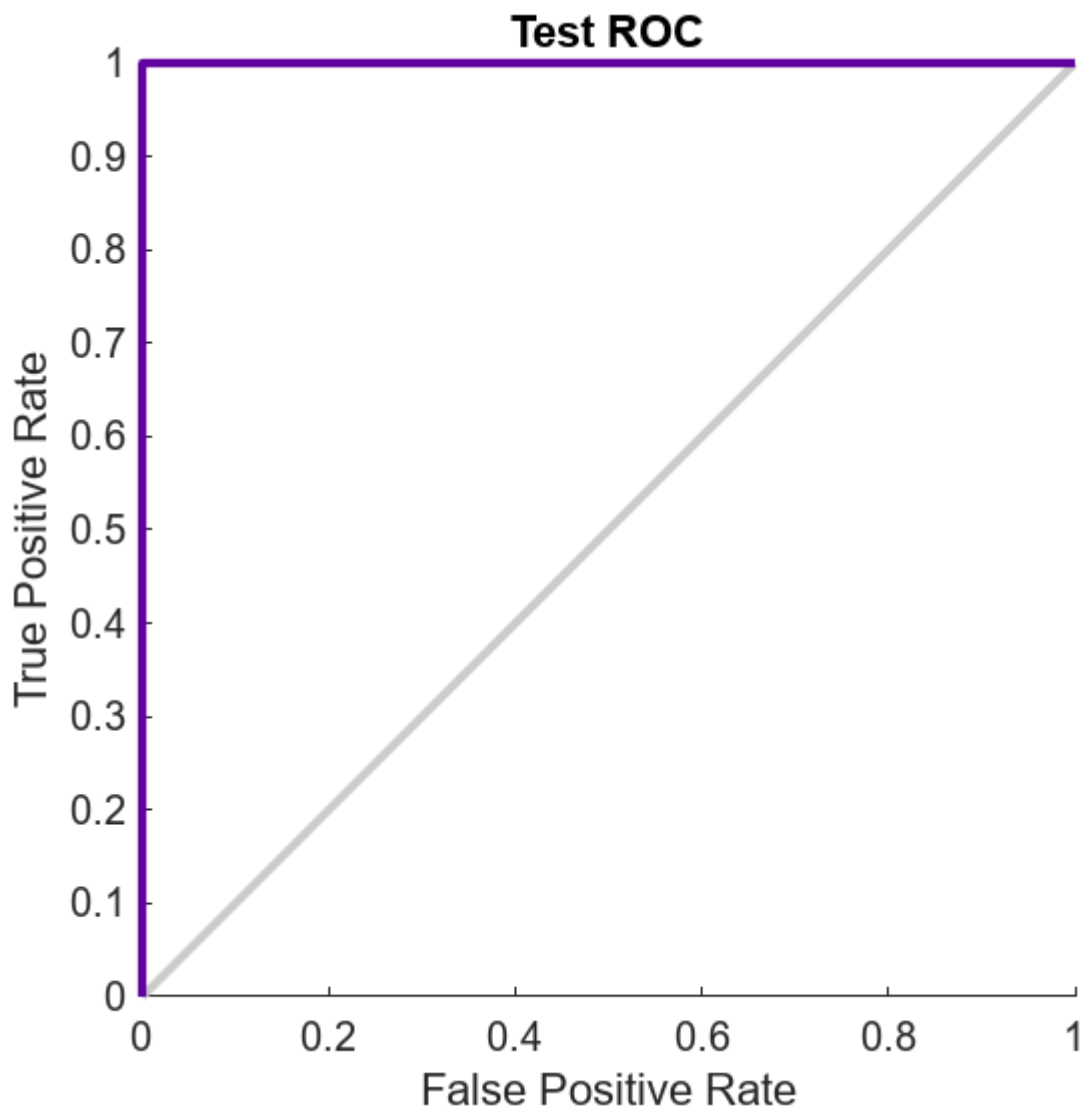


Рисунок 4.13 – Крива похибок тестової вибірки

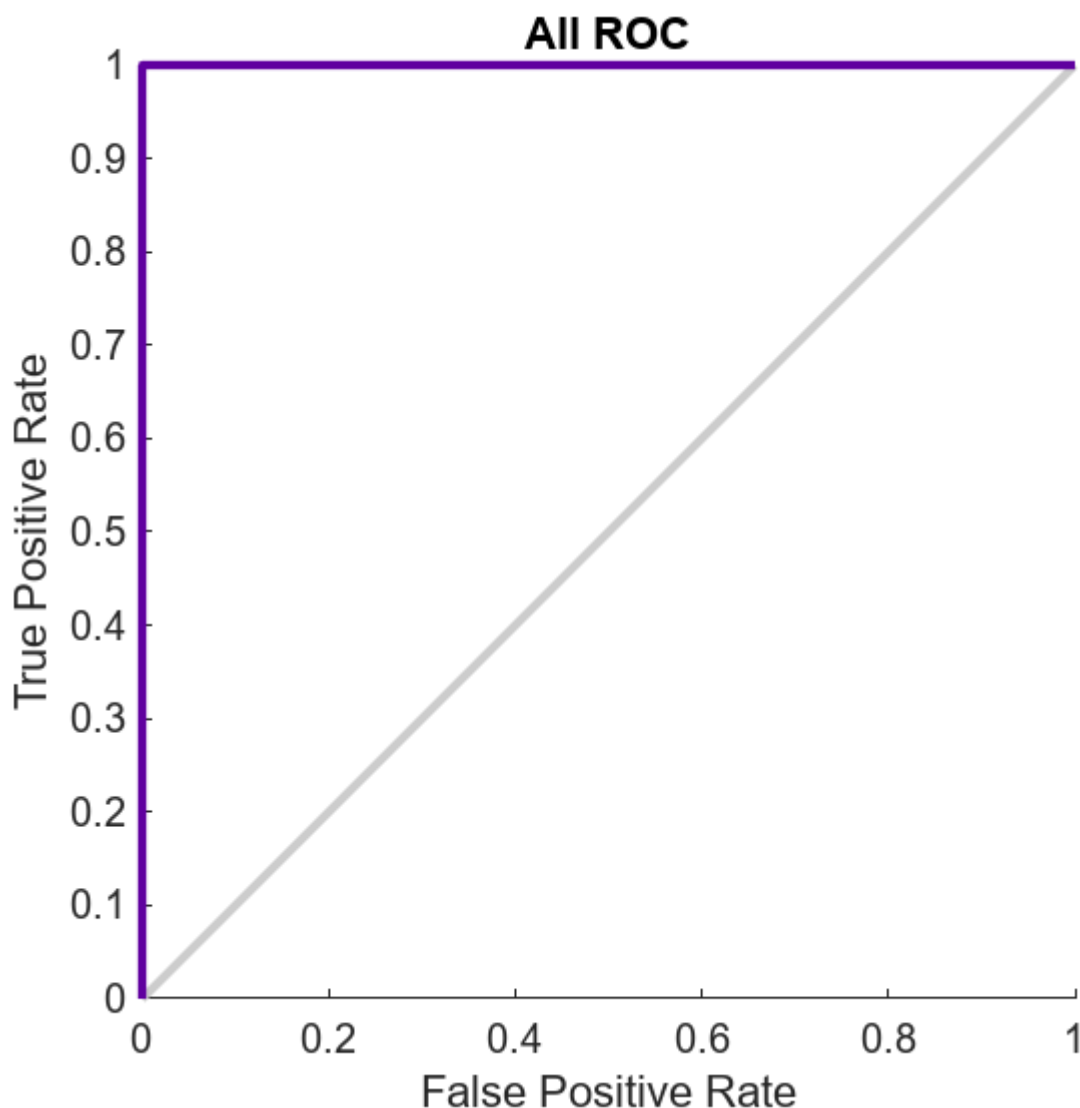


Рисунок 4.14 – Крива похибок загального набору даних

Результати дослідження створеної штучної нейронної мережі використовуються в наступному розділі для порівняння ефективності засобів ідентифікації та аутентифікації за клавіатурним почерком.

#### **4.3 Порівняння ефективності засобів ідентифікації та аутентифікації за клавіатурним почерком**

Порівняємо ефективність розробленої штучної нейронної мережі і розробленого засобу, який базується на класичному підході, представленого в роботі [23].

### 4.3.1 Режим ідентифікації

Для порівняння засобів в режимі ідентифікації, були взяті результати тестування нейронної мережі з попереднього підрозділу. Для тестування режиму ідентифікації засобу, який базується на класичному підході, була взята та сама вибірка, яка використовувалась для тестування створеної нейронної мережі в попередньому підрозділі.

Відсоток помилкових ідентифікацій, які проводились двома засобами, наведено на рисунку 4.15.

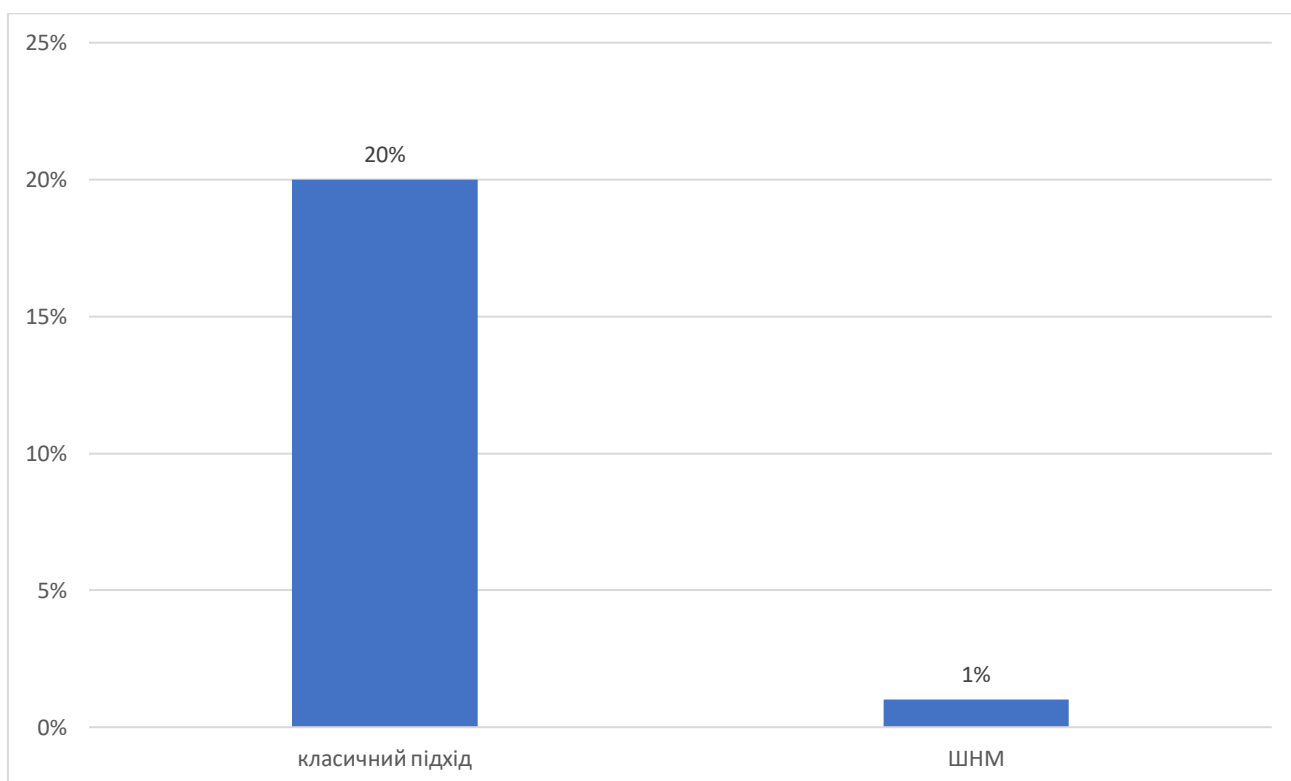


Рисунок 4.15 – Порівняння відсотку помилкових ідентифікацій за двома методами

Порівняння помилок ідентифікації по конкретних користувачах наведено на рисунку 4.16.

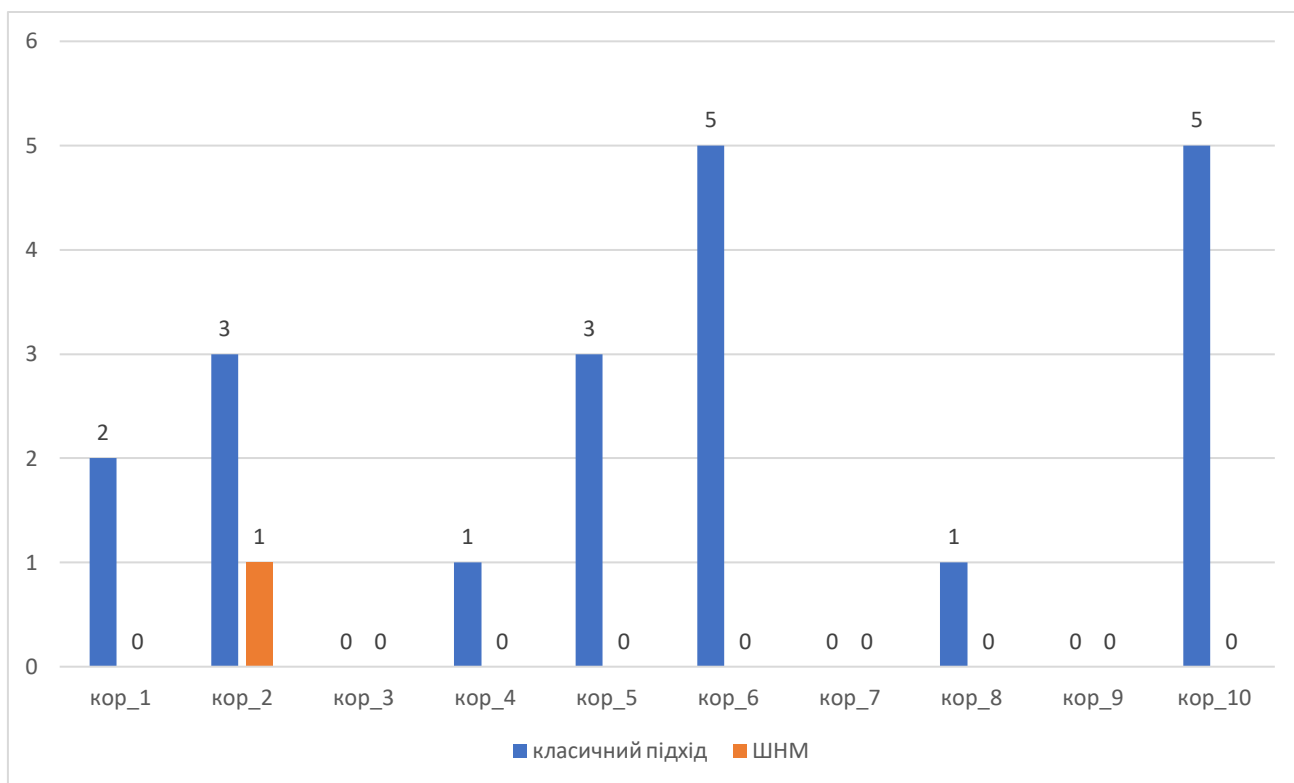


Рисунок 4.16 – Порівняння помилкових ідентифікацій користувачів за двома методами

Згідно рисунку 4.16, штучна нейронна мережа показала кращий результат. Слід зазначити, що класичний підхід базується на математичному апараті, що використовує середнє відхилення, тому для користувачів, у яких гарно сформований клавіатурний почерк (як от користувач 6 і користувач 10), дуже малі довірчі інтервали для проходження ідентифікації, тому система дуже чутливо реагує на будь які викиди часових інтервалів з довірчого діапазону.

В свою чергу, штучна нейронна мережа може визначити більш значущі довірчі інтервали, влучання в які буде сигналізувати нейронній мережі про те, що саме це влучання більш притаманно саме цьому користувачеві. Наприклад, час утримання клавіші пробілу між користувачами, хоч і трохи, але різнитися, однак конкретний користувач приблизно однаково затримується на пробілі і має чітко виражену характеристику, яка відповідає за час утримання пробілу. Таким чином штучна нейронна мережа може виділяти чітко виражені характеристики .

### 4.3.2 Режим аутентифікації

Для перевірки ефективності аутентифікації, було створено 5 шаблонів «зловмисника», який намагається пройти процедуру аутентифікації, використовуючи особистість кожного з зареєстрованих користувачів. Шаблони додані до загальної тестової вибірки.

Графік, який демонструє показники помилок першого і другого роду засобу, що базується на класичному підході, наведено на рисунку 4.17.

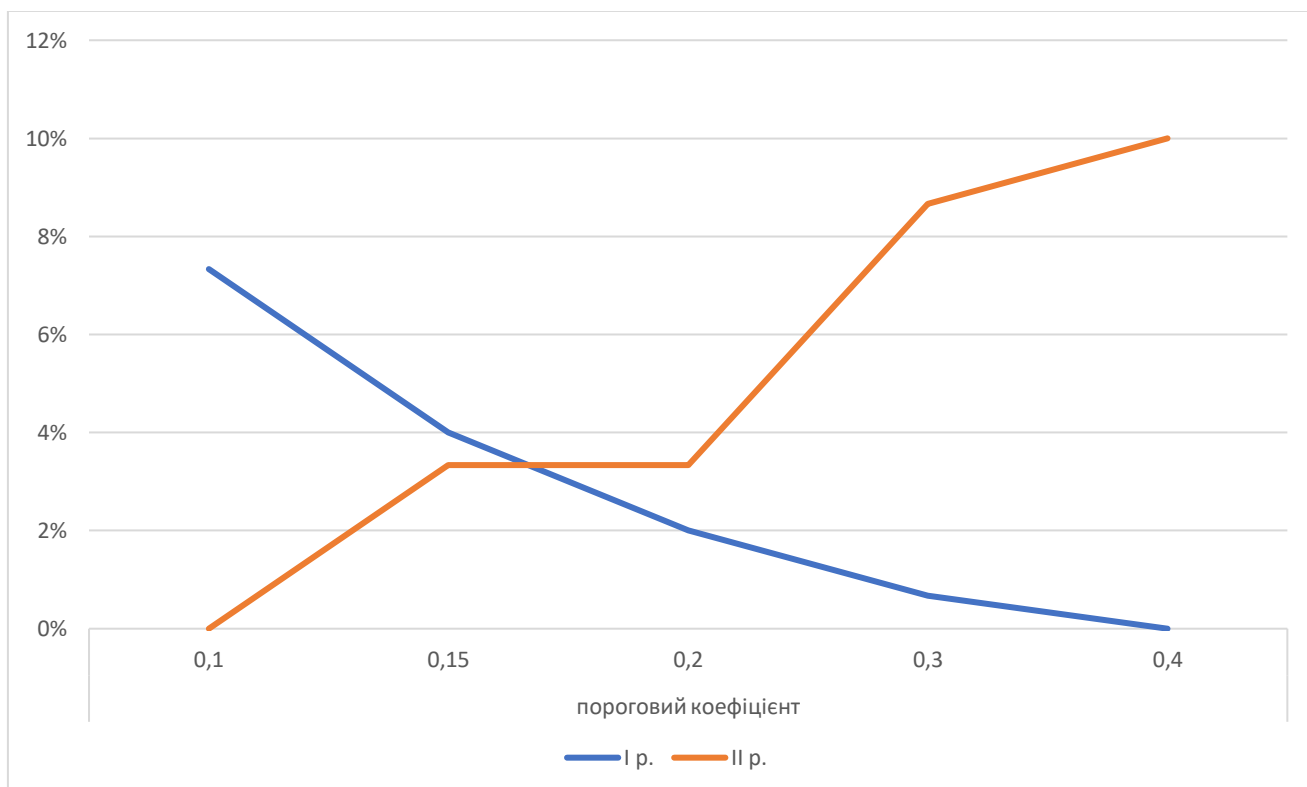


Рисунок 4.17 – Залежність показників помилок першого і другого роду засобу, що базується на класичному підході, від порогового коефіцієнту

Графік, який демонструє показники помилок першого і другого роду створеної штучної нейронної мережі, наведено на рисунку 4.18.

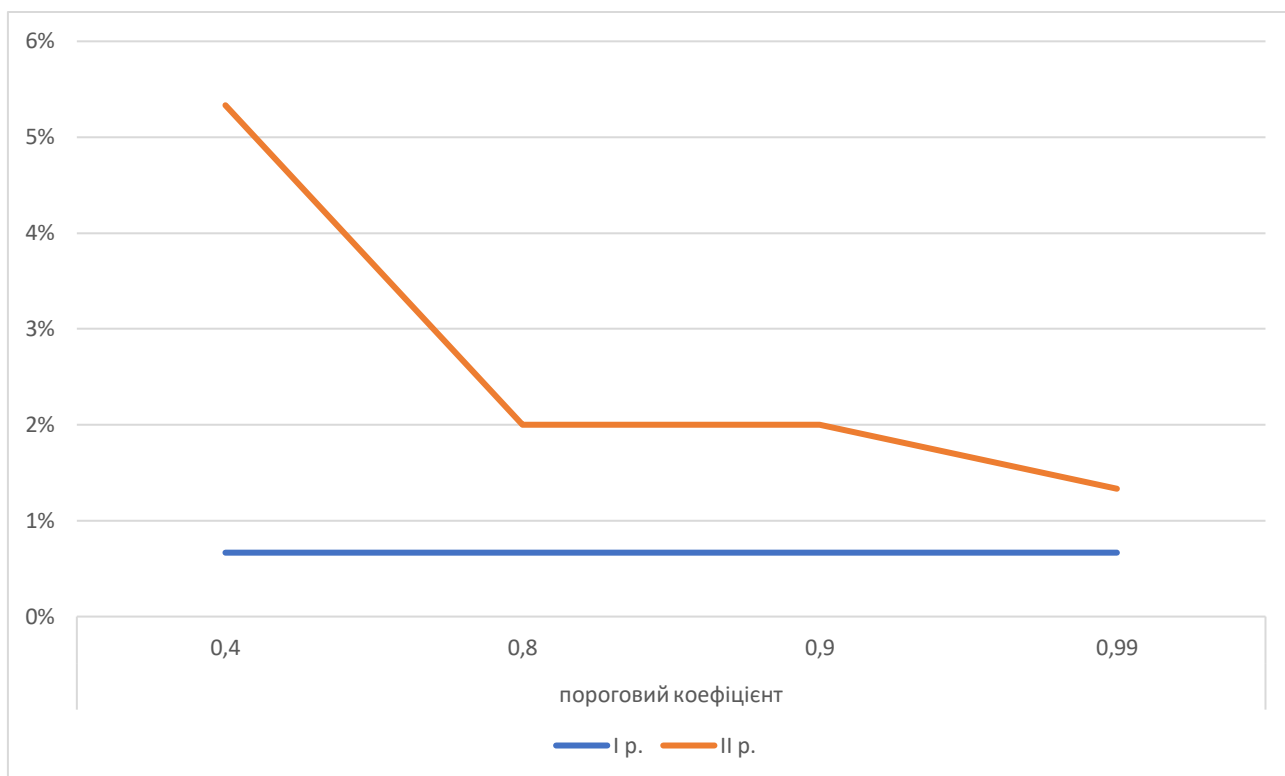


Рисунок 4.18 – Залежність показників помилок першого і другого роду створеної штучної нейронної мережі від порогового коефіцієнту

Використання низького коефіцієнту допуску не притаманно цьому засобу. Визначення точного високого коефіцієнту, який урівноважив би помилки першого і другого роду, є більш складним завданням, який потребує додаткового дослідження.

#### **4.4 Висновки за розділом**

Налаштовано штучну нейронну мережу для ідентифікації та аутентифікації за клавіатурним почерком. Проведено навчання та тестування ШНМ.

Проведено дослідження ефективності створеного засобу в порівнянні з існуючим засобом, який базується на класичному підході [23] в двох режимах: ідентифікації та аутентифікації. Розроблена штучна нейронна мережа демонструє більшу ефективність в обох режимах.

## ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

В роботі виконано розробку та дослідження ефективності засобів біометричної ідентифікації та аутентифікації за клавіатурним почерком.

Проведено огляд та аналіз методів та засобів біометричної ідентифікації та аутентифікації, характеристик клавіатурного почерку.

Розглянуто та проаналізовано методи ідентифікації та аутентифікації за клавіатурним почерком, які базуються на використанні засобів штучного інтелекту та класичному підході.

Створено авторський набір для навчання та тестування нейронної мережі.

Виконано розробку структури штучної нейронної мережі, експериментально визначено параметри, при яких штучна нейронна мережа найбільш ефективна.

Проведено налаштування, навчання та тестування створеної штучної мережі. Досліджено ефективність запропонованої штучної нейронної мережі в порівнянні з існуючим засобом, який базується на класичному підході.

Аналіз отриманих результатів показав, що штучна нейронна мережа показує більшу ефективність і можна рекомендувати використовувати механізм заснований на штучних нейронних мережах при розробці засобів ідентифікації та аутентифікації за клавіатурним почерком.

## ПЕРЕЛІК ПОСИЛАНЬ

1. Ярьоменко Д. О., Остапець Д. О. Біометрична ідентифікація та аутентифікація за клавіатурним почерком. *Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті* : Тези XVI Міжнар. науково-практ. конф., м. Дніпро, 14–15 груд. 2022 р. Дніпро, 2022. С. 156. URL: <https://ust.edu.ua/diit/documentation/news/22-12-2022-U7fd-sbornik-xvi-modern-it-conf-2022.pdf> (дата звернення: 12.01.2024).

2. Ярьоменко Д. О., Остапець Д. О. Особливості використання клавіатурного почерку для ідентифікації та автентифікації користувачів. *Сучасні інформаційні та комунікаційні технології на транспорті, в промисловості і освіті* : Тези XVII Міжнар. науково-практ. конф., м. Дніпро, 13–14 груд. 2022 р. Дніпро, 2023. С. 150. URL: <https://ust.edu.ua/diit/documentation/news/20-12-2023-hItP-sbornik-xvii-modern-it-conf-2023.pdf> (дата звернення: 12.01.2024).

3. Ярьоменко Д. О., Остапець Д. О. Ідентифікація та автентифікація користувачів на основі порівняння профілів клавіатурного почерку. *Наука і сталий розвиток транспорту 2023* : зб. тез доповідей Всеукр. наук.-техн. конференції студентів і молодих учених, м. Дніпро, 27 жовтня 2023 р : у 3 т. Дніпро, 2023. Т. 2. С. 23. URL: <https://crust.ust.edu.ua/items/3cf7404f-8735-4c84-a4fb-aacb14bbeace> (дата звернення: 12.01.2024).

4. Ярьоменко Д. О., Остапець Д. О. Комплекс біометричної ідентифікації та автентифікації за клавіатурним почерком. *Молода академія 2023* : зб. тез доповідей Всеукр. наук.-техн. конференції студентів і молодих учених, м. Дніпро, 24.05-25.05 2023 р : у 2 т. Дніпро : УДУНТ, 2023. Т. 1. С. 180-181. URL: <https://crust.ust.edu.ua/items/3cf7404f-8735-4c84-a4fb-aacb14bbeace> (дата звернення: 12.01.2024).

5. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Каб. Міністрів України від 29.03.2006 р. № 373 : станом на 21 жовт. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/373-2006-п#Text> (дата звернення: 12.01.2024).

6. Аутентифікація, авторизація та ідентифікація. *QATestLab training center*. URL: <https://training.qatestlab.com/blog/technical-articles/authentication-authorization-and-identification/> (дата звернення: 12.01.2024).
7. sp800-63-3. NIST Special Publication 800-63-3 Digital Identity Guidelines. Effective from 2020-02-02. Official edition. URL: <https://pages.nist.gov/800-63-3/sp800-63-3.html> (дата звернення: 12.01.2024).
8. Що таке MFA – багатофакторна аутентифікація?. *DATAMI*. URL: <https://datami.ua/shho-take-mfa-bagatofaktorna-autentifikatsiya/> (дата звернення: 12.01.2024).
9. Liling C., Liling W. Analysis and improvement of a multi-factor biometric authentication scheme. *Security and Communication Networks*. 2015. Т. 8, № 4. С. 617–625. URL: <https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1010> (дата звернення: 12.01.2024).
10. Захаров В. П., Рудешко В. І. Біометричні технології в ххі столітті та їх використання правоохоронними органами : Посібник. 2-ге вид. Львів : Львів. держ. ун-т внутр. справ, 2015. 492 с. URL: <https://dspace.lvduvs.edu.ua/bitstream/1234567890/6/1/Захаров%20біометричні%20технології.pdf> (дата звернення: 12.01.2024).
11. Бідюк П. І., Бондарчук В. Сучасні методи біометричної ідентифікації. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2009. № 1(18). С. 137–146. URL: <https://ela.kpi.ua/bitstream/123456789/9839/1/26.pdf> (дата звернення: 12.01.2024).
12. Handbook of Biometrics / ред.: А. К. Jain, Р. Flynn, А. А. Ross. Boston, MA : Springer US, 2008. 556 с. URL: <https://doi.org/10.1007/978-0-387-71041-9> (дата звернення: 12.01.2024).
13. Yevetskyi V., Horniichuk I. Analysis of stability of the user's keyboard handwriting characteristics in the biometric authentication systems. *Collection "Information technology and security"*. 2018. Т. 6, № 2. С. 19–28.

URL: <https://doi.org/10.20535/2411-1031.2018.6.2.153487> (дата звернення: 12.01.2024).

14. Harun N., Woo W. L., Dlay S. S. Performance of keystroke biometrics authentication system using artificial neural network (ANN) and distance classifier method. *2010 International Conference on Computer and Communication Engineering (ICCCE)*, м. Kuala Lumpur, Malaysia, 11–12 трав. 2010 р. 2010. URL: <https://doi.org/10.1109/iccce.2010.5556852> (дата звернення: 12.01.2024).

15. Sulong A., Wahyudi, Siddiqi M. U. Intelligent keystroke pressure-based typing biometrics authentication system using radial basis function network. *Its Applications (CSPA)*, м. Kuala Lumpur, Malaysia, 6–8 берез. 2009 р. 2009. URL: <https://doi.org/10.1109/cspa.2009.5069206> (дата звернення: 12.01.2024).

16. Obaidat M. S., Sadoun B. Verification of computer users using keystroke dynamics. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*. 1997. Т. 27, № 2. С. 261–269. URL: <https://doi.org/10.1109/3477.558812> (дата звернення: 12.01.2024).

17. Lee H.-j., Cho S. Retraining a keystroke dynamics-based authenticator with impostor patterns. *Computers & Security*. 2007. Т. 26, № 4. С. 300–310. URL: <https://doi.org/10.1016/j.cose.2006.11.006> (дата звернення: 12.01.2024).

18. Mantyjarvi J., Koivumaki J., Vuori P. Keystroke recognition for virtual keyboard. *IEEE International Conference on Multimedia and Expo (ICME)*, м. Lausanne, Switzerland. URL: <https://doi.org/10.1109/icme.2002.1035630> (дата звернення: 12.01.2024).

19. Pavaday N., Soyjaudah K. M. S. A comparative study of secret code variants in terms of keystroke dynamics. *2008 Third International Conference on Risks and Security of Internet and Systems (CRiSIS)*, м. Tozeur, Tunisia, 28–30 жовт. 2008 р. 2008. URL: <https://doi.org/10.1109/crisis.2008.4757473> (дата звернення: 12.01.2024).

20. Pavaday N., Soyjaudah K. M. S. Investigating performance of neural networks in authentication using keystroke dynamics. *AFRICON 2007*, м. Windhoek, South

Africa, 26–28 жовт. 2007 р. 2007.

URL: <https://doi.org/10.1109/afrcon.2007.4401575> (дата звернення: 12.01.2024).

21. Dozono H., Ito S., Nakakuni M. The Authentication System for Multi-modal Behavior Biometrics Using Concurrent Pareto Learning SOM. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2011. С. 197–204.

URL: [https://doi.org/10.1007/978-3-642-21738-8\\_26](https://doi.org/10.1007/978-3-642-21738-8_26) (дата звернення: 12.01.2024).

22. Пахомова В. М. Теорія проєктування комп'ютерних мереж : метод. рек. до виконання курс. проєкту. Дніпро : Дніпропетр. нац. ун-ту залізн. трансп. ім. акад. В. Лазар., 2020. 60 с.

URL: <https://library.ust.edu.ua/uk/catalog/book/212138> (дата звернення: 12.01.2024).

23. Ярьоменко Д. О. Розробка засобів демонстрації біометричної ідентифікації та аутентифікації за клавіатурним почерком : дипломна робота на здобуття кваліфікаційного ступеня бакалавра : спец. 125 – Кібербезпека / наук. керівник Д. О. Остапець; Укр. держ. ун-т науки і технологій. Дніпро, 2022. 60 с.

URL: <https://crust.ust.edu.ua/items/be3f5f93-67ce-4cd6-8307-af446aef3e29> (дата звернення: 12.01.2024).













466,92;911,15;89,07;4154,09;1309,70;859,42;1011,91;938,39;521,20;320,93;271,52;456,94;317,77;389,95;300,47;368,40;966,23;1613,56;3036,75;738,00;346,42;792,13;95,88;554,33;608,18;2036,75;1015,63;1719,02;903,52;1792,10;1232,81;2485,55;2022,10;1604,22;334,31;1404,43;1930,78;1340,42;1174,84;1351,38;144,4,18;574,93;1368,33;1312,09;1525,27;1891,00;15,57;1746,98;2691,87;2234,43;1291,58;1060,32;1590,13;748,35;1859,66;1389,93;2286,89;2428,74;1491,56;1164,77;1638,79;57,56;2432,15;1395,96;86;810,61;605,58;1363,39;2122,12;2132,81;773,76;874,86;1031,02;850,33;495,29;619,98;1154,01;1111,32;116,64;721,66;1295,40;1030,09;1237,34;1300,11;1115,84;402,87;778,48;1656,65;846,43;742,57;178,57;1279,81;533,17;1236,60;1074,90;786,83;61,95;287,04;1632,16;934,37;1151,32;2310,41;1109,43;148,44;177,64;93,86;72,62;85,65;83,54,32;28,41;88,48;55,60;22,9;28;280,08;55,59;49,32;37,00;41,95;106,22;73,93;144;15;181,31;97,50,332,05;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;114,31;107,07;66,00;99,97;77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;79,70;77;54;56;57;64,13;39,54;26,13;68,70;63,93;76;28;67,68;148,54;36,62;37,03;30;229,50,85;34,70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;50,59;37,02;420,76;236,49;139,82;431,03;245,26;246,26;442,11;113,83;213,37;313,41;510,40;192,97;351,88;64,45;309,67;97,23;287,39;249,20;217,44;440,60;230,89;242,88;443,29;224,04;267,13;178,37;288,22;229,04;315,04;43,49;280,00;232,30;539,62;403,54;255,97;199,80;293,58;190,99;128,49;303,70;79,70;77,54;56,57;64,13;39,54;26,37;68,70;63,93;76,28;67,68;148,54;38;62;37,03;02,50;85,34;70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;50,59;37,02;420,76;236,49;139,82;431,03;245,26;246,26;442,11;113,83;213,37;313,41;510,40;192,97;351,88;64,45;309,67;97,23;287,39;249,20;217,44;440,60;230,89;242,88;443,29;224,04;267,13;178,37;288,22;229,04;315,04;43,49;280,00;232,30;539,62;403,54;255,97;199,80;293,58;190,99;128,49;303,70;79,70;77,54;56,57;64,13;39,54;26,37;68,70;63,93;76,28;67,68;148,54;38;62;37,03;02,50;85,34;70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;50,59;37,02;420,76;236,49;139,82;431,03;245,26;246,26;442,11;113,83;213,37;313,41;510,40;192,97;351,88;64,45;309,67;97,23;287,39;249,20;217,44;440,60;230,89;242,88;443,29;224,04;267,13;178,37;288,22;229,04;315,04;43,49;280,00;232,30;539,62;403,54;255,97;199,80;293,58;190,99;128,49;303,70;79,70;77,54;56,57;64,13;39,54;26,37;68,70;63,93;76,28;67,68;148,54;38;62;37,03;02,50;85,34;70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;50,59;37,02;420,76;236,49;139,82;431,03;245,26;246,26;442,11;113,83;213,37;313,41;510,40;192,97;351,88;64,45;309,67;97,23;287,39;249,20;217,44;440,60;230,89;242,88;443,29;224,04;267,13;178,37;288,22;229,04;315,04;43,49;280,00;232,30;539,62;403,54;255,97;199,80;293,58;190,99;128,49;303,70;79,70;77,54;56,57;64,13;39,54;26,37;68,70;63,93;76,28;67,68;148,54;38;62;37,03;02,50;85,34;70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;50,59;37,02;420,76;236,49;139,82;431,03;245,26;246,26;442,11;113,83;213,37;313,41;510,40;192,97;351,88;64,45;309,67;97,23;287,39;249,20;217,44;440,60;230,89;242,88;443,29;224,04;267,13;178,37;288,22;229,04;315,04;43,49;280,00;232,30;539,62;403,54;255,97;199,80;293,58;190,99;128,49;303,70;79,70;77,54;56,57;64,13;39,54;26,37;68,70;63,93;76,28;67,68;148,54;38;62;37,03;02,50;85,34;70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;50,59;37,02;420,76;236,49;139,82;431,03;245,26;246,26;442,11;113,83;213,37;313,41;510,40;192,97;351,88;64,45;309,67;97,23;287,39;249,20;217,44;440,60;230,89;242,88;443,29;224,04;267,13;178,37;288,22;229,04;315,04;43,49;280,00;232,30;539,62;403,54;255,97;199,80;293,58;190,99;128,49;303,70;79,70;77,54;56,57;64,13;39,54;26,37;68,70;63,93;76,28;67,68;148,54;38;62;37,03;02,50;85,34;70;62,92;57,13;61,42;919,96;940,81;1555,92;963,95;1171,69;996,12;1023,76;1540,08;911,88;980,12;2052,05;963,85;987,81;1288,14;1191,90;963,98;1180,10;1255,96;971,93;980,03;219,83;249,99;191,40;166,68;184,12;203,12;506,30;438,39;479,91;428,15;358,56;181,25;196,87;156,24;218,76;144,53;193,63;229,76;192,55;116,89;562,57;233,63;233,14;294,68;200,11;183,61;235,93;322,49;288,86;233,60;280,71;260,18;203,06;174,80;192,09;346,99;158,74;288,44;255,85;149,85;97,15;65,32;71,49;67,03;148,77;208,46;82,88;188,96;93,38;96,77;97,23;89,16;81,65;89,88;87,14;73,65;72,36;83,51;302,09;214,62;1558,41;495,57;846,58;1752,30;712,72;1010,74;1352,02;399,93;357,60;246,33;270,35;320,46;307,45;222,04;968,89;1201,71;525,36;471,85;172,05;478,11;359,39;463,65;287,61;245,36;506,88;661,13;406,45;392,36;567,99;727,62;592,19;1146,42;735,88;841,11;1071,55;111,3,29;1162,50;587,97;709,74;602,86;114,31;107,07;66,00;99,77;204,56;150,26;299,09;82,08;97,86;36,31;95,52;61,43;49,02;47,00;26,99;47,23;58,25;56,01;43,56;86,66;1038,30;513,47;449,94;247,60;355,23;1115,88;823,66;177,07;163,50;164,06;353,92;352,76;1375,69;1382,51;341,22;528,29;363,55;760,13;136,72;140,62;134,35;89,33;165,58;146,16;145,76;151,03;106,46;121,17;152,75;67,14;170,28;106,60;106,54;71,27;41,61;90,24;25,61;58,08;









35,83;153,80;71,76;444,20;238,74;156,03;130,65;63,95;111,19;91,68;66,70;100,32;108,32;236,04;60,87;92,23;80,59;302,92;194,55;91,86;81,01;91,40;80,53;213,55;87,48;181,72;105,86;519,26;492,11;94,70;232,86;60,39;258,76;190,51;253,65;73,83;158,50;234,80;228,94;28,96;344,42;423,88;391,82;461,66;170,46;3
28,02;80,56;497,03;149,19;383,57;734,92;158,12;498,72;209,45;185,23;453,41;245,66;276,11;446,17;29,11;736,85;27,25;151,82;612,90;793,00;878,48;1146,66;934,69;868,12;826,06;927,37;596,71;537,81;597,90;632,27;553,17;444,00;734,33;864,13;589,94;533,27;1002,22;733,89;743,26;1042,36;809,27;984,79;812,64
;435,53;856,69;665,56;1191,88;564,98;389,41;362,18;899,66;258,00;888,40;783,32;1059,07;560,52;1133,01;216,21;409,26;121,61;75,61;56,13;88,12;113,23;68;87,95;06,96;75,26;109,58;83,62;112,52;148,18;100,44;97,96;84,66;108,41;1667,57;1300,00;687,30;1266,66;542,69;377,69;888,08;825,50;806
;56;498,30;973,08;845,31;350,55;998,71;1123,33;537,80;546,43;944,43;940,94;780,13;724,00;81,17;35;744,81;580,16;891,86;541,94;160,28;360,56;508,26;905,14;1017,23;789,85;1071,20;894,82;1104,64;514,61;830,95;683,55;1040,41;1124,45;811,26;252,45;137,11;65,25;100,10;191,93;171,69;148,50;207,87;151,94;23
4,15;256,47;117,78;73,48;136,92;215,21;184,63;58,75;41,92;137,61;240,23;101,88;291,24;44,34;95,41;131,56;257,06;217,06;249,06;76,91;31,62;82;88;42;215,05;71,94;22,96;169;62;81;71;17;13,36;53;208;49;84;41;1481,37;1889;45;2125,09;1323,30;2598,62;789,77;653,85;529,22;639,10;509,49;438,45;243,86;2
76,48;385,55;249,38;445,84;116,12;273,68;778,59;186,27;221,89;286,74;20,40;40,40;95;114,42;186,10;285,35;101,43;62,67;218,92;76,43;312,10;164,10;183,77;101,31;39,60;164,77;115,82;109,48;131,00;248,35;30,81;57,11;75,36;148,88;196,78;103,01;52,99;117,77;201,72;94,69;206,59;69;42;95;167,57;233,4
1;109,44;105,67;77,41;122,96;90,72;87,96;87,02;115,93;67,06;151,07;143,68;115,99;57,98;69,63;118,27;63,50;48,49;134,57;129,67;114,16;106,71;87,70;61,35;69,33;93,18;118,00;89,18;106,60;123,68;79,36;97,65;131,08;74,15;116,40;106,55;162,65;168,84;130,42;148,95;73,45;97,98;150,63;478,83;349,09;501,16;3
93,39;527,78;436,96;424,25;479,38;376,20;373,74;466,62;466,89;3562,70;1924,73;2269,04;1029,51;876,20;578,34;637,20;2203,73;99,47;54,74;62,48;148,20;108,83;119,26;120,57;40,49;77,21;85,09;127,40;97,18;134,82;73;83;118,57;86,16;74,69;131,18;114,26;78,71;42,65;87,75;78,33;106,67;105,94;69,13;118,98;14
6,34;162,80,70,73;88,06;87,81;81,20;79,49;127,68;118,02;72,42;108,23,80,52;132,95;421,81;101,92;346,72;12,31;783,70;943,33;185,18;1557,97;1051,61;769,72;927,83;765,94;1512,92;1048,53;562,80;502,77;845,23;1104,86;66;1936,95;810,11;741,27;2056,53;891,93;442,72;1340,20;621,13;799,54;904,72;460,33;556,31;
791,81;1414,34;254,89;177,88;500,31;565,51;1462,73;1601,89;1074,35;246,33;1090,59;2568,12;1144,68;83;1206,87;286,40;353,91;975,77;1067,47;464,03;213,38;185,29;274,36;494,29;283,65;427,61;506,49;2060,69;1596,40;1543,38;17,77;36;861,91;373,11;1162,78;2335,20;300,29;232,63;1173,26;137,02;1014,63;444,94;35,0
3;1496,10;60,75;1847,46;361,74;705,64;1240,52;970,16;1407,23;1680,95;926,23;1355,39;1418,40;1444,17;840,81;1234,11;549,15;771,35;2060,44;1541,15;1382,25;816,43;1845,31;981,15;1441,42;825,41;1491,99;231,15;956,79;1717,70;646,57;573,56;578,10;1163,12;391,50;394,84;107,36;895,14;825,33;320,67;1175,43;
0,05;738,83;117,29;717,88;467,15;137,31;454,47;1130,53;475,83;81,25;687,83;708,52;517,94;729,66;355,56;1474,93;751,98;8111,47;1001,16;474,93;990,73;198,41;52,22;410,82;869,14;240,80;57,69;234,84;303,76;543,94;286,94;16,18;48,76;51,05;94,44;13,32;41;27,77;59,53;21,69;38,19
;01,76;44;107,64;182,85;143,50
286,93;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97;354,76;175,01;181,24;167,96;165,64;167,97;167,97;158,85;177,63;296,02;45,43;62,19;64,77;84,35;68,79;33,60;69,09;24,80;550,52;35,64;77,49;83,72;97,24;55,20;68,84;74,00;93,33;94,89;56,64;84,55;147,10;65,38;36,40;48,40;34,19
;67,83;118,12;61,73;46,88;49,34;27,43;45,32;52,75;63,23;84,79;45,10;08,12;17,114,91,21,95;944,13;1100,59;2819,89;655,71;196,04;180,04;176,04;212,15;275,63;04;164,04;169,68;212,05;184,04;200,04;160,03;203,80;164,04;179,89;05;148,03;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97
;354,76;175,01;181,24;167,97;167,97;167,97;158,85;177,63;296,02;183,70;203,31;247,57;222,21;236,75;180,53;239,12;139,53;138,42;288,96;136,38;169,69;145,09;147,39;124,97;161,51;208,77;183,56;191,77;92,43;75,05;148,53;9382,01;82,82;76,44;74,56;75,00;62,92;62,33;81,77;63,84;70,76;55,61;51;64
,80;242,32;66,12;73,99;67,78;76,80;441,40;315,29;1212,35;2444,21;1404,65;2077,05;1996,48;2021,66;861,99;1774,25;1718,68;2356,58;1004,58;2162,65;3489,52;1357,74;944,16;1308,43;773,45;731,85;1797,42;2226,65;1698,95;2144,21;1463,65;79;1907,45;1237,43;71,79;791,88;589,24;723,03;596,95;282,50;319,9
9;943,83;573,35;173,46;322,49;189,13;45,43;62,19;64,77;84,35;68,79;33,60;69,09;24,80;550,52;35,64;77,49;83,72;97,24;55,20;68,84;74,00;93,33;94,89;56,64;84,55;820,37;900,22;479,71;348,37;376,95;178,91;311,81;764,79;625,93;1596,34;664,06;856,26;437,10;517,81;1149,59;1253,87;1015,22;692,80;201,94;271,1
6;290,96;125,03;152,83;58,74;48,60;245,30;43,95;29,92;11,69;9,31;20,81;55,40;25,50;71,18;130,74;73,09;59,11;125,17;27,76;76,39;154,09;52;67;127;59;300,22;484,18;97;43;224;06;263;92;447;41;309;91;312;06;383;99;337;46;335;119;33;519;88;192;94;40;65;380;59;3;77;385;87;447;58;523;54;669;01;137;10;4
47;88;285;81;152;14;570;45;160;33;475;83;243;51;567;69;147;94;484;81;129;07;451;77;140;07;540;15;241;46;147;10;65;38;36;40;48;40;34;19;67;83;118;12;61;73;46;88;49;43;45;32;75;63;23;84;79;45;10;18;27;114,91,21,95;944,13;1100,59;2819,89;655,71;196,04;180,04;176,04;212,15;275,63;04;164,04;169,68;212,05;184,04;200,04;160,03;203,80;164,04;179,89;05;148,03;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97
;354,76;175,01;181,24;167,97;167,97;167,97;158,85;177,63;296,02;183,70;203,31;247,57;222,21;236,75;180,53;239,12;139,53;138,42;288,96;136,38;169,69;145,09;147,39;124,97;161,51;208,77;183,56;191,77;92,43;75,05;148,53;9382,01;82,82;76,44;74,56;75,00;62,92;62,33;81,77;63,84;70,76;55,61;51;64
,80;242,32;66,12;73,99;67,78;76,80;441,40;315,29;1212,35;2444,21;1404,65;2077,05;1996,48;2021,66;861,99;1774,25;1718,68;2356,58;1004,58;2162,65;3489,52;1357,74;944,16;1308,43;773,45;731,85;1797,42;2226,65;1698,95;2144,21;1463,65;79;1907,45;1237,43;71,79;791,88;589,24;723,03;596,95;282,50;319,99;943,83;573,35;173,46;322,49;189,13;45,43;62,19;64,77;84,35;68,79;33,60;69,09;24,80;550,52;35,64;77,49;83,72;97,24;55,20;68,84;74,00;93,33;94,89;56,64;84,55;820,37;900,22;479,71;348,37;376,95;178,91;311,81;764,79;625,93;1596,34;664,06;856,26;437,10;517,81;1149,59;1253,87;1015,22;692,80;201,94;271,16;290,96;125,03;152,83;58,74;48,60;245,30;43,95;29,92;11,69;9,31;20,81;55,40;25,50;71,18;130,74;73,09;59,11;125,17;27,76;76,39;154,09;52;67;127;59;300,22;484,18;97;43;224;06;263;92;447;41;309;91;312;06;383;99;337;46;335;119;33;519;88;192;94;40;65;380;59;3;77;385;87;447;58;523;54;669;01;137;10;4
47;88;285;81;152;14;570;45;160;33;475;83;243;51;567;69;147;94;484;81;129;07;451;77;140;07;540;15;241;46;147;10;65;38;36;40;48;40;34;19;67;83;118;12;61;73;46;88;49;43;45;32;75;63;23;84;79;45;10;18;27;114,91,21,95;944,13;1100,59;2819,89;655,71;196,04;180,04;176,04;212,15;275,63;04;164,04;169,68;212,05;184,04;200,04;160,03;203,80;164,04;179,89;05;148,03;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97
;354,76;175,01;181,24;167,97;167,97;167,97;158,85;177,63;296,02;183,70;203,31;247,57;222,21;236,75;180,53;239,12;139,53;138,42;288,96;136,38;169,69;145,09;147,39;124,97;161,51;208,77;183,56;191,77;92,43;75,05;148,53;9382,01;82,82;76,44;74,56;75,00;62,92;62,33;81,77;63,84;70,76;55,61;51;64
,80;242,32;66,12;73,99;67,78;76,80;441,40;315,29;1212,35;2444,21;1404,65;2077,05;1996,48;2021,66;861,99;1774,25;1718,68;2356,58;1004,58;2162,65;3489,52;1357,74;944,16;1308,43;773,45;731,85;1797,42;2226,65;1698,95;2144,21;1463,65;79;1907,45;1237,43;71,79;791,88;589,24;723,03;596,95;282,50;319,99;943,83;573,35;173,46;322,49;189,13;45,43;62,19;64,77;84,35;68,79;33,60;69,09;24,80;550,52;35,64;77,49;83,72;97,24;55,20;68,84;74,00;93,33;94,89;56,64;84,55;820,37;900,22;479,71;348,37;376,95;178,91;311,81;764,79;625,93;1596,34;664,06;856,26;437,10;517,81;1149,59;1253,87;1015,22;692,80;201,94;271,16;290,96;125,03;152,83;58,74;48,60;245,30;43,95;29,92;11,69;9,31;20,81;55,40;25,50;71,18;130,74;73,09;59,11;125,17;27,76;76,39;154,09;52;67;127;59;300,22;484,18;97;43;224;06;263;92;447;41;309;91;312;06;383;99;337;46;335;119;33;519;88;192;94;40;65;380;59;3;77;385;87;447;58;523;54;669;01;137;10;4
47;88;285;81;152;14;570;45;160;33;475;83;243;51;567;69;147;94;484;81;129;07;451;77;140;07;540;15;241;46;147;10;65;38;36;40;48;40;34;19;67;83;118;12;61;73;46;88;49;43;45;32;75;63;23;84;79;45;10;18;27;114,91,21,95;944,13;1100,59;2819,89;655,71;196,04;180,04;176,04;212,15;275,63;04;164,04;169,68;212,05;184,04;200,04;160,03;203,80;164,04;179,89;05;148,03;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97
;354,76;175,01;181,24;167,97;167,97;167,97;158,85;177,63;296,02;183,70;203,31;247,57;222,21;236,75;180,53;239,12;139,53;138,42;288,96;136,38;169,69;145,09;147,39;124,97;161,51;208,77;183,56;191,77;92,43;75,05;148,53;9382,01;82,82;76,44;74,56;75,00;62,92;62,33;81,77;63,84;70,76;55,61;51;64
,80;242,32;66,12;73,99;67,78;76,80;441,40;315,29;1212,35;2444,21;1404,65;2077,05;1996,48;2021,66;861,99;1774,25;1718,68;2356,58;1004,58;2162,65;3489,52;1357,74;944,16;1308,43;773,45;731,85;1797,42;2226,65;1698,95;2144,21;1463,65;79;1907,45;1237,43;71,79;791,88;589,24;723,03;596,95;282,50;319,99;943,83;573,35;173,46;322,49;189,13;45,43;62,19;64,77;84,35;68,79;33,60;69,09;24,80;550,52;35,64;77,49;83,72;97,24;55,20;68,84;74,00;93,33;94,89;56,64;84,55;820,37;900,22;479,71;348,37;376,95;178,91;311,81;764,79;625,93;1596,34;664,06;856,26;437,10;517,81;1149,59;1253,87;1015,22;692,80;201,94;271,16;290,96;125,03;152,83;58,74;48,60;245,30;43,95;29,92;11,69;9,31;20,81;55,40;25,50;71,18;130,74;73,09;59,11;125,17;27,76;76,39;154,09;52;67;127;59;300,22;484,18;97;43;224;06;263;92;447;41;309;91;312;06;383;99;337;46;335;119;33;519;88;192;94;40;65;380;59;3;77;385;87;447;58;523;54;669;01;137;10;4
47;88;285;81;152;14;570;45;160;33;475;83;243;51;567;69;147;94;484;81;129;07;451;77;140;07;540;15;241;46;147;10;65;38;36;40;48;40;34;19;67;83;118;12;61;73;46;88;49;43;45;32;75;63;23;84;79;45;10;18;27;114,91,21,95;944,13;1100,59;2819,89;655,71;196,04;180,04;176,04;212,15;275,63;04;164,04;169,68;212,05;184,04;200,04;160,03;203,80;164,04;179,89;05;148,03;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97
;354,76;175,01;181,24;167,97;167,97;167,97;158,85;177,63;296,02;183,70;203,31;247,57;222,21;236,75;180,53;239,12;139,53;138,42;288,96;136,38;169,69;145,09;147,39;124,97;161,51;208,77;183,56;191,77;92,43;75,05;148,53;9382,01;82,82;76,44;74,56;75,00;62,92;62,33;81,77;63,84;70,76;55,61;51;64
,80;242,32;66,12;73,99;67,78;76,80;441,40;315,29;1212,35;2444,21;1404,65;2077,05;1996,48;2021,66;861,99;1774,25;1718,68;2356,58;1004,58;2162,65;3489,52;1357,74;944,16;1308,43;773,45;731,85;1797,42;2226,65;1698,95;2144,21;1463,65;79;1907,45;1237,43;71,79;791,88;589,24;723,03;596,95;282,50;319,99;943,83;573,35;173,46;322,49;189,13;45,43;62,19;64,77;84,35;68,79;33,60;69,09;24,80;550,52;35,64;77,49;83,72;97,24;55,20;68,84;74,00;93,33;94,89;56,64;84,55;820,37;900,22;479,71;348,37;376,95;178,91;311,81;764,79;625,93;1596,34;664,06;856,26;437,10;517,81;1149,59;1253,87;1015,22;692,80;201,94;271,16;290,96;125,03;152,83;58,74;48,60;245,30;43,95;29,92;11,69;9,31;20,81;55,40;25,50;71,18;130,74;73,09;59,11;125,17;27,76;76,39;154,09;52;67;127;59;300,22;484,18;97;43;224;06;263;92;447;41;309;91;312;06;383;99;337;46;335;119;33;519;88;192;94;40;65;380;59;3;77;385;87;447;58;523;54;669;01;137;10;4
47;88;285;81;152;14;570;45;160;33;475;83;243;51;567;69;147;94;484;81;129;07;451;77;140;07;540;15;241;46;147;10;65;38;36;40;48;40;34;19;67;83;118;12;61;73;46;88;49;43;45;32;75;63;23;84;79;45;10;18;27;114,91,21,95;944,13;1100,59;2819,89;655,71;196,04;180,04;176,04;212,15;275,63;04;164,04;169,68;212,05;184,04;200,04;160,03;203,80;164,04;179,89;05;148,03;255,26;251,32;250,91;281,25;309,38;1148,41;213,54;207,03;215,65;195,97
;354,76;175,01;181,24;167,97;167,97;167,97;158,85;177,63;296,02;183,70;203,31;247,57;222,21;236,75;180,53;



