МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
Кафедра Програмної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження методів та моделей автентифікації на основі даних про взаємодію з клавіатурою

Виконав:
студент 2 курсу групи ІПЗм-21-4
Кайдалов В.Д.
(прізвище, ініціали)

Спеціальність 121 – Інженерія програмного забезпечення

Тип програми Освітньо-наукова
Керівник доц. Голян В.В.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. Кафедри _____ проф. Дудар З.В.

2023 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Програмної інженерії

Рівень вищої освіти другий (магістерський)

Спеціальність 121 – Інженерія програмного забезпечення

Тип програми Освітньо-наукова програма

Освітня програма Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

«___»_____202_ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студента Кайдалова Вадима Дмитровича

(прізвище, ім'я, по батькові)

1. Тема роботи: «Дослідження методів та моделей автентифікації на основі даних про взаємодію з клавіатурою».

затверджена наказом університету від « 10 » квітня 202 3 р. № 340Ст

2. Термін подання роботи до екзаменаційної комісії «__»_____ 202__ р.

3. Вихідні дані до роботи: біометрична автентифікація, методи автентифікації користувачів на основі взаємодії з клавіатурою, динаміка друку, детектори аномалій, Python, NumPy, Pandas, SciPy, matplotlib, пояснювальна записка.

4. Перелік питань, що потрібно опрацювати в роботі: мета роботи, аналіз предметної області, аналіз методів автентифікації користувачів за динамікою друку, критерії їх оцінки, постановка задачі, проведення експериментів та аналіз їх результатів, формування подальших рекомендацій.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд наукової та патентної літератури	17.02.2022	виконано
2	Постановка задачі	20.02.2022	виконано
3	Розробка детекторів аномалій	07.03.2022	виконано
4	Пошук тестових даних	21.03.2022	виконано
5	Реалізація програмної системи	07.04.2023	виконано
6	Розробка плану проведення експериментальних досліджень	11.04.2023	виконано
7	Проведення експериментальних досліджень	16.04.2023	виконано
8	Аналіз отриманих результатів	17.04.2023	виконано
9	Підготовка пояснювальної записки	01.05.2023	виконано
10	Підготовка презентації та доповіді	06.05.2023	виконано
11	Перевірка на плагіат	19.05.2023	виконано
12	Нормоконтроль та рецензування	19.05.2023	виконано
13	Архівування	22.05.2023	виконано
14	Попередній захист	22.05.2023	виконано
15	Допуск до захисту у зав. кафедри	22.05.2023	виконано

Дата видачі завдання 17 січня 2022 р.

Студент _____

(підпис)

Керівник роботи _____ доц. Голян В.В.

(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ / ABSTRACT

Кваліфікаційна робота магістра містить: 61 с., 17 рис., 1 табл., 24 джер.

АВТЕНТИФІКАЦІЯ, БЕЗПЕКА, БІОМЕТРИКА, ДЕТЕКТОР АНОМАЛІЙ, ДИНАМІКА ДРУКУ, NUMPY, PANDAS, PYTHON, SCIPY.

Об’єктом дослідження є методи та моделі автентифікації на основі даних про взаємодію з клавіатурою.

Метою дослідження є розробка систем автентифікації користувачів з використанням біометричних даних про натискання клавіш клавіатури. Окрема увага приділяється дослідженню впливу розміру тренувального набору даних та вибору ознак на ефективність детекторів аномалій.

У результаті роботи було проведено аналіз існуючих алгоритмів статичної автентифікації, що використовують дані набору тексту на клавіатурі; було порівняно існуючі детектори аномалій на відкритому наборі даних та проведено додаткові випробування.

ANOMALY DETECTOR, AUTHENTICATION, BIOMETRICS, KEYSTROKE DYNAMICS, NUMPY, PANDAS, PYTHON, SECURITY, SCIPY.

The object of the research is the methods and models of authentication based on keystroke dynamics data.

The purpose of the research is to develop user authentication systems using biometric data on keystroke dynamics. Special attention is paid to investigating the impact of the size of the training dataset and feature selection on the performance of anomaly detectors.

As the result of the research, an analysis of existing algorithms for static authentication using keyboard text data was conducted, existing anomaly detectors were compared on an open dataset, and additional testing was performed.

Я, Кайдалов Вадим Дмитрович, студент групи ІПЗм-21-4, здобувач вищої освіти на другому (магістерському) рівні, кафедра Програмної інженерії, заявляю: моя кваліфікаційна робота на тему «Дослідження методів та моделей автентифікації на основі даних про взаємодію з клавіатурою», що буде представлена до ЕК для публічного захисту, виконана самостійно, в ній не містяться елементи плагіату і вона може бути опублікована в електронному архіві відкритого доступу ElArKhNURE. Всі запозичення з друкованих та електронних джерел мають відповідні посилання.

Я ознайомлений з діючим положенням «Про протидію академічному плагіату в ХНУРЕ», згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування дисциплінарних заходів.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

EER	Equal Error Rate, однаковий рівень помилок
ZMFAR	Zero-Miss False Alarm Rate, рівень помилок першого роду при відсутності помилок другого роду
ROC	Receiver Operating Characteristic, робоча характеристика приймача
SVM	Support Vector Machine, метод опорних векторів
TPR	True Positive Rate, доля помилок першого роду
FPR	False Positive Rate, доля помилок другого роду

ВСТУП

В даний час актуальною є проблема розробки методів та моделей автентифікації користувачів, що забезпечують високий рівень безпеки. Біометрична автентифікація є напрямком досліджень методів автентифікації користувачів з використанням різноманітних джерел біометричних даних, що стрімко розвивається протягом останніх років. Джерела біометричних даних можуть бути широко класифіковані на: фізіологічні, такі як відбитки пальців, малюнки райдужної оболонки ока, риси обличчя [1]; та поведінкові, такі як динаміка натискання клавіш [2], аналіз ходи та розпізнавання голосу [3][4][5].

Методи та моделі автентифікації, що використовують дані динаміки натискання клавіш, які полягають у аналізі ритму та часу набору тексту, є особливо перспективним напрямком досліджень завдяки декільком перевагам порівняно з використанням інших джерел біометричних даних. По-перше, це відносно невисока вартість та широкий доступ, оскільки дані можуть бути легко зібрані зі звичайних комп'ютерних клавіатур. Це робить їх більш доступними, ніж використання інших джерел біометричних даних, таких як сканер відбитків пальців або камери розпізнавання обличчя, які можуть бути дорогими та потребувати спеціального обладнання. По-друге, дані динаміки натискання клавіш можуть бути використані для автентифікації користувачів в реальному часі, оскільки це є континуальним процесом, який може бути відстежений протягом сеансу користувача. Інші джерела біометричних даних, такі як розпізнавання голосу або обличчя, можуть вимагати від користувача активної участі в процесі аутентифікації, що може бути незручним та знижувати ефективність роботи користувача [5].

Методи та моделі автентифікації користувачів на основі даних про взаємодію з клавіатурою в реальному часі забезпечують вищий рівень безпеки, оскільки можна виявляти аномалії у динаміці натискання клавіш під час робочої сесії користувача, без необхідності регулярних запитів на введення паролю [6]. Такий підхід дозволяє уникнути ситуації, коли зловмисник отримує доступ до комп’ютеру, на якому був введений пароль, але сесія якого не була заблокована

або призупинена, коли істинний користувач залишив свій комп’ютер без нагляду з необачності, в стресовій ситуації тощо. З іншого боку, такі методи можуть потребувати більше обчислювальної потужності та бути більш нав’язливими для користувача, оскільки їхня динаміка натискання клавіш безперервно відстежується та обробляється моделлю автентифікації, що працює у фоновому режимі на комп’ютері користувача [7][8].

Методи та моделі автентифікації з використанням динаміки введення пароля передбачають порівняння зразку даних натискання клавіш з попередньо записаним шаблоном динаміки набору конкретної фрази, зазвичай – паролю [9]. Користувач вводить свій пароль один або декілька разів під час реєстрації, і шаблон зберігається для майбутніх порівнянь при наступних входах у систему. Цей підхід може бути менш нав’язливим для користувача, оскільки їм потрібно вводити свій пароль лише один раз під час реєстрації, а подальший друк під час сесії ніяк не обробляється системою автентифікації, тому витік даних користувача через вразливість в механізмі збору даних динаміки друку під час сесії користувача стає неможливим. Такі методи також є менш витратними за ресурсами, оскільки потребують обробки даних динаміки друку тільки для одної конкретної фрази та виключно під час входу у систему [10][11].

Метою дослідження є аналіз існуючих методів та моделей автентифікації на основі даних динаміку друку під час введення конкретної фрази; визначення найперспективніших методів та моделей для подальших досліджень; визначення впливу таких параметрів цих методів та моделей, як розмір тренувального набору даних та набір ознак друку, на ефективність роботи методу чи моделі.

Об’єктом дослідження є автентифікація користувачів на основі даних динаміки друку під час введення конкретної фрази.

Предметом дослідження є методи та моделі автентифікації на основі даних про взаємодію з клавіатурою.

В якості методів дослідження були використані аналіз існуючих робіт в даному напрямку; відтворення існуючих детекторів аномалій; використання відкритого набору даних для тренування, тестування та визначення ефективності

розроблених моделей детекторів аномалій та впливу різних параметрів на отриману ефективність; формування висновків та рекомендацій щодо напрямків подальших досліджень.

В результаті роботи були отримані наступні результати:

- відтворені моделі детекторів аномалій, виявлені загальні вимоги до кожної з них;
- проведено тестування розроблених моделей детекторів аномалій на відкритому наборі даних та визначено вплив таких параметрів, як розмір тренувальних даних та набір ознак друку, на ефективність кожної з моделей;
- розроблено програмне забезпечення для випробування всіх розроблених моделей детекторів в інтерактивному режимі;
- сформовані висновки та рекомендації щодо напрямків подальших досліджень.

Тези доповіді за темою даної кваліфікаційної роботи були опубліковані в збірнику наукових праць «ΛΌГОΣ» з матеріалами III Міжнародної науково-практичної конференції «Grundlagen der modernen wissenschaftlichen Forschung» (31.03.2023; Цюріх; Швейцарська Конфедерація) [12].

1 ОГЛЯД НАУКОВОЇ ЛІТЕРАТУРИ

1.1 Загальні відомості про методи та моделі автентифікації на основі даних про взаємодію з клавіатурою

Наразі існують декілька методів використання даних динаміки друку для автентифікації користувача. За обсягом та тривалістю збору даних, ці методів можна поділити на дві категорії:

- ті, що отримують на вхід дані динаміки набору однієї конкретної фрази, наприклад, паролю;
- ті, що обробляють дані динаміки друку користувача впродовж усієї сесії користування комп'ютерною системою.

Методи, що належать до другої категорії, ще називають методами «активної» автентифікації [6][7][8]. В той час, коли методи активної автентифікації можуть забезпечити вищий рівень нагляду над безпекою сесії користувача, ці методи також потребують більше обчислювальної потужності та підвищеної відповідальності в плані своєї розробки, бо усі текстові дані, що вводяться користувачем під час роботи з комп'ютерною системою, стають більш вразливими до витоку через програмний нагляд та обробку в режимі реального часу, ніж при використанні «статичних» метод автентифікації.

З іншого боку, за поставленою задачею, методи можна поділити на дві наступні категорії:

- детектор аномалій для однокласової класифікації;
- багатокласова класифікація.

Методи багатокласової класифікації можуть застосовуватися не тільки для того, щоб заборонити доступ до комп'ютерної системи в разі невдалої спроби автентифікації, але й для того, щоб спробувати виявити особистість людини, що намагалась отримати доступ до чужої системи. Для цього необхідно провести централізований збір даних динаміки друку усіх можливих зловмисників, що на практиці може бути застосовано, наприклад, в офісному приміщенні з обмеженим

доступом, де знаходяться індивідуальні комп’ютери певної групи співробітників, що можуть мати фізичний доступ до комп’ютерів один одного.

Детектори аномалій, з іншого боку, застосовуються для визначення приналежності чергового зразка даних друку одному конкретному користувачу. Результатом опрацювання нового зразка даних друку детектором аномалій є оцінка приналежності цього зразка справжньому власнику сесії. Ця оцінка є числовим значенням, що далі порівнюється з заздалегідь встановленим пороговим значенням. Після порівняння система автентифікації приймає рішення щодо продовження або переривання користувацької сесії.

В даній роботі було досліджено саме використання детекторів аномалій для автентифікації на основі даних набору конкретної фрази.

Необроблені дані про натискання клавіш (наприклад, стан клавіші та відповідні мітки часу) не можуть бути безпосередньо використані детектором аномалій. Замість цього, з необроблених даних виділяють набір часових ознак. Ці ознаки зазвичай організовані у вектори ознак. Різні дослідники виділяють різні комбінації ознак [9]. Найбільший набір унікальних типів ознак друку, які використовуються існуючими методами, складається з наступних типів ознак:

а) DD – час, що пройшов між моментами послідовного натискання двох клавіш; дана ознака складається з:
   1) ідентифікатору клавіші, що була натиснута першою;
   2) ідентифікатору клавіші, що була натиснута другою (може дорівнювати першому при повторному натисканні);
   3) часу, що пройшов між моментами затискання цих клавіш;

б) UD – час, що пройшов між моментами відпускання однієї клавіші та затискання наступної клавіші; містить такі самі ідентифікатори, як DD;

в) H – час, що пройшов між моментами затискання однієї клавіші та відпускання тієї ж клавіші; на відміну від UD та DD, містить ідентифікатор тільки однієї клавіші.

Візуалізація визначень ознак DD, UD та H наведена на рисунку 1.1.

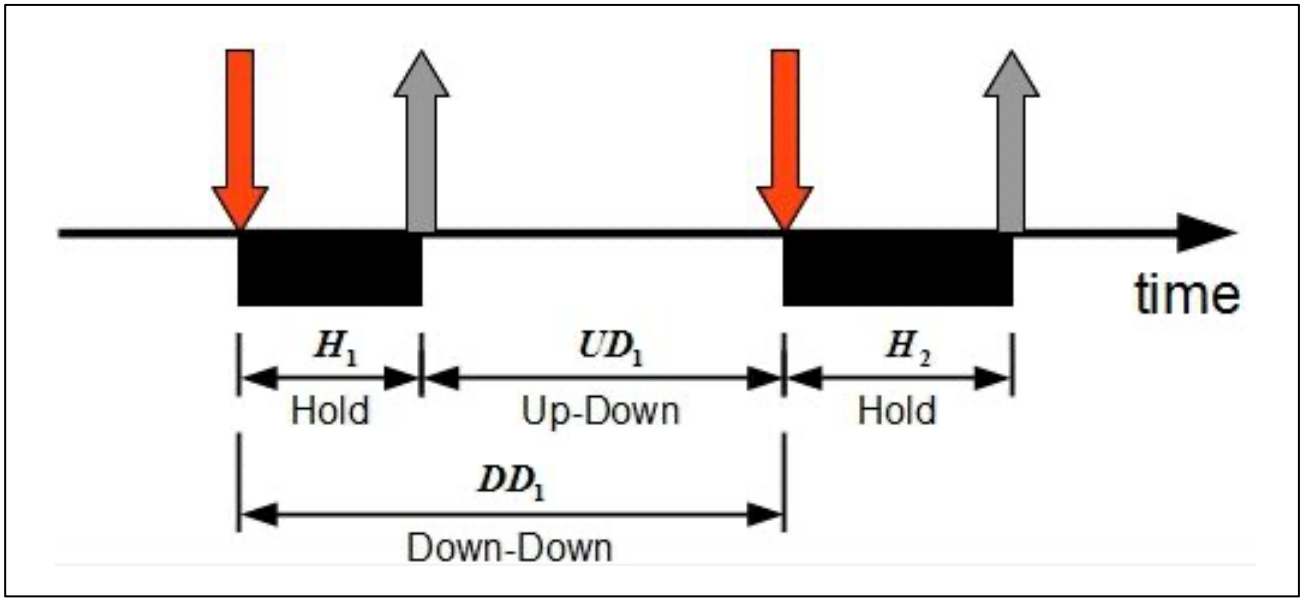

Рисунок 1.1 – Візуалізація визначень ознак DD, UD, H [13]

З попередніх досліджень в цій галузі відомо, що між деякими ознаками існує кореляція [14]. Зокрема, значення ознаки DD може бути представлена як сума відповідних значень ознак H та UD. Тим не менш, ознака DD була все одно використана під час проведення експериментів в багатьох інших роботах [9]. В даній роботі було проведено експериментальне дослідження для вивчення впливу вибору ознак друку на ефективність детекторів аномалій, деталі якого наведено в наступних розділах.

Методи, що належать до вибраних вище категорій методів автентифікації, використовують однакову конкретну фразу під час усіх спроб автентифікації, тому вектор ознак набору конкретної фрази можна представити, як вектор числових значень, де кожне числове значення відповідає тривалості часу однієї з трьох наведених вище ознак. Тип ознаки можна однозначно визначити за місцем знаходження певного значення у векторі ознак. Наприклад, для фрази з 10 символів відповідний вектор ознак, що містить всі три наведені типи ознак, буде мати 30 числових значень, кожні три з яких будуть відповідати часу натискання однієї клавіші та часу переходу до натискання наступної клавіші.

Роботу з детектором аномалій для автентифікації на основі друку можна розділити на два етапи:

– тренування детектору аномалій;
– виставлення оцінки новим зразкам даних.

Під час тренування, детектор отримує на вхід масив векторів тренувальних даних, що є даними динаміки друку під час введення істинним користувачем системи конкретної фрази. Чим більше зразків введення фрази потребує детектор аномалій для переходу до високоточного оцінювання нових зразків даних, тим гірше стає досвід користувача роботи з системою через надмірну витрати часу і зусиль. Тому важливим є дослідження впливу розміру тренувального набору даних на ефективність системи, яке, зокрема, було проведено в даній роботі.

Під час етапу виставлення оцінки новим зразкам даних, детектор, що вже пройшов етап тренування, отримує нові вектори ознак та виставляє оцінки кожному з наданих векторів.

Для прийняття рішення щодо продовження чи призупинення сесії користувача, необхідно вибрати порогове значення та порівняти його зі значенням, отриманим при оцінюванні нового зразка даних. Вибір порогового значення впливає на кількість помилок першого і другого роду. В даній роботі не розглядаються методи вибору порогового значення, але наводяться способи оцінювання ефективності детекторів аномалій, що враховують можливість встановлення різних порогових значень в тих чи інших умовах.

1.2 Огляд наукової літератури

Дослідники університету Карнегі-Меллон стали першими, хто:

– відтворили всі 11 найвідоміших на момент дослідження детекторів аномалій для автентифікації на основі даних друку, а також 3 – основаних на класичних алгоритмах детекторів аномалій;
– зібрали відносно великий набір даних від 51 користувача, ретельно описавши та обґрунтувавши спосіб збору даних;
– провели тестування розроблених детекторів аномалій задля виявлення загальних закономірностей та напрямків подальших досліджень;

– надали публічний доступ до зібраного набору даних задля подальшого використання науковим суспільством [9].

Як зазначили самі дослідники, на момент дослідження не було проведено жодного тестування усіх розроблених раніше детекторів аномалій в однакових умовах. Різні дослідники використовували різні міри ефективності детекторів аномалій та проводили тестування користуючись наборами тестових даних, що сильно відрізнялись за способом збору даних, розміром тощо.

Метою дослідників став збір такої кількості тестових даних, що мала б статистичну цінність, та подальше відтворення та тестування всіх детекторів аномалій в однакових умовах для коректного виявлення найкращих з них.

На рисунках 1.2 та 1.3 наведені таблиці порівняння робіт інших дослідників. Зокрема, в різних роботах були використані різні набори ознак даних друку; способи збору тестових даних значно відрізняються; метод вибору порогових значень для вимірювання ефективності детекторів теж не є єдиним.

	Source Study	Detector	Feature Sets				Password	
			Enter Key	Keydown-Keydown	Keyup-Keydown	Hold	Length	Reps
1	Joyce & Gupta (1990) [10]	Manhattan (filtered)	✓	✓			N/A	8
2	Bleha et al. (1990) [2]	Euclidean (normed)		✓			11–17	30
		Mahalanobis (normed)		✓			11–17	30
3	Cho et al. (2000) [4]	Nearest Neighbor (Mahalanobis)	✓		✓	✓	7	75–325
		Neural Network (auto-assoc)	✓		✓	✓	7	75–325
4	Haider et al. (2000) [8]	Fuzzy Logic		✓			7	15
		Neural Network (standard)		✓			7	15
		Outlier Count (z-score)		✓			7	15
5	Yu & Cho (2003) [21]	SVM (one-class)	✓		✓	✓	6–10	75–325
6	Araujo et al. (2004) [1]	Manhattan (scaled)		✓	✓	✓	10+	10
7	Kang et al. (2007) [11]	k-Means			✓	✓	7–10	10

Рисунок 1.2 – Порівняння існуючих робіт за наборами ознак даних [9]

В якості набору ознак друку, дослідники вибрали усі три ознаки DD, UD та H, зазначивши, що кореляція між ознаками може впливати на ефективність детекторів. Також дослідники зазначили, що дослідження впливу розміру набору тренувальних даних на ефективність детекторів є доречним можливим продовженням їхньої роботи. В їхній роботі тренування кожного детектору проводилось на наборах даних з 200 векторів ознак. Іншими словами, на практиці

це б означало, що кожному користувачу довелось би надрукувати одну й ту саму фразу 200 разів перед тим, як почати користуватись системою автентифікації. Зазначені проблеми є об'єктами дослідження в даній роботи і будуть розглянуті детальніше в наступних розділах.

	Source Study	Filtering		Testing		Results (%)		
		Users	Times	#Attempts	Updating	Threshold	Miss	False Alarm
1	Joyce & Gupta (1990) [10]		✓	1		heuristic	0.25	16.36
2	Bleha et al. (1990) [2]			1	✓	heuristic	2.8	8.1[(a)]
				1	✓	heuristic	2.8	8.1
3	Cho et al. (2000) [4]	✓	✓	1		zero-miss	0.0	19.5
		✓	✓	1		zero-miss	0.0	1.0
4	Haider et al. (2000) [8]			2		heuristic	19.	11.[(b)]
				2		heuristic	22.	20.
				2		heuristic	13.	2.
5	Yu & Cho (2003) [21]	N/A	N/A	1		zero-miss	0.0	15.78
6	Araujo et al. (2004) [1]			1	✓	heuristic	1.89	1.45
7	Kang et al. (2007) [11]	N/A	N/A	1	✓	equal-error	3.8	3.8

Рисунок 1.3 – Порівняння існуючих робіт за мірами ефективності [9]

За результатами проведеного тестування, було розраховано EER та ZMFAR для кожного з розроблених детекторів аномалій та учасника випробування. Після цього були розраховані усереднені по кількості учасникам середні значення EER та ZMFAR. Відсортовані в порядку зменшення ефективності детектори аномалій наведені на рисунку 1.4. Визначення мір ефективності EER та ZMFAR, опис їхніх переваг та недоліків наведено в наступних розділах цієї роботи.

	Detector	equal-error rate			Detector	zero-miss false-alarm rate	
1	**Manhattan (scaled)**	**0.096**	**(0.069)**	**1**	**Nearest Neighbor (Mahalanobis)**	**0.468**	**(0.272)**
2	**Nearest Neighbor (Mahalanobis)**	**0.100**	**(0.064)**	**2**	**Mahalanobis**	**0.482**	**(0.273)**
3	**Outlier Count (z-score)**	**0.102**	**(0.077)**	**3**	**Mahalanobis (normed)**	**0.482**	**(0.273)**
4	SVM (one-class)	0.102	(0.065)	**4**	**SVM (one-class)**	**0.504**	**(0.316)**
5	Mahalanobis	0.110	(0.065)	5	Manhattan (scaled)	0.601	(0.337)
6	Mahalanobis (normed)	0.110	(0.065)	6	Manhattan (filter)	0.757	(0.282)
7	Manhattan (filter)	0.136	(0.083)	7	Outlier Count (z-score)	0.782	(0.306)
8	Manhattan	0.153	(0.092)	8	Manhattan	0.843	(0.242)
9	Neural Network (auto-assoc)	0.161	(0.080)	9	Neural Network (auto-assoc)	0.859	(0.220)
10	Euclidean	0.171	(0.095)	10	Euclidean	0.875	(0.200)
11	Euclidean (normed)	0.215	(0.119)	11	Euclidean (normed)	0.911	(0.148)
12	Fuzzy Logic	0.221	(0.105)	12	Fuzzy Logic	0.935	(0.108)
13	k Means	0.372	(0.139)	13	k Means	0.989	(0.040)
14	Neural Network (standard)	0.828	(0.148)	14	Neural Network (standard)	1.000	(0.000)

Рисунок 1.4 – Результати тестування детекторів аномалій [9]

Як можна бачити, сім найгірших детекторів (місця 8-14) є однаковими для обох показників ефективності. Також є однаковою і множина семи перших детекторів для обох мір ефективності. Незважаючи на те, що порядок перших семи не є однаковим для обох показників, це спостереження свідчить про чіткий розрив між сьома детекторами, ефективність яких є вищою, і сьома, ефективність яких є значно нижчою.

Оскільки детектори аномалій були оцінені за допомогою тих самих даних, в тих же умовах та з використанням тих же процедур, можливо приписати різниці в ефективності саме детектору аномалій, а не різним експериментальним умовам.

Найкращий EER склав 0,096 і був досягнутий за допомогою детектора аномалій за Мангеттенською відстанню, описаного Араухо та ін. [9]. Детектор найближчого сусіда за відстанню Махаланобіса та детектор підрахунку викидів за z-оцінкою також були серед найкращих детекторів згідно з критерієм рівної помилки. В даній роботі вдалося відтворити значення EER для всіх вибраних детекторів, окрім SVM, що буде наведено в наступних розділах.

Найкращий показник ZMFAR становив 0,468 і був отриманий дектором аномалій найближчого сусіда (Махаланобіс), який описаний у статті Чо та ін. [9]. Класичний детектор Махаланобіса, нормований детектор Махаланобіса та детектор SVM (однокласовий) були іншими детекторами, які показали найкращі результати використовуючи показник ZFMAR. Тим не менш, в даній роботі далі буде наведено розбіжність відтворення значень даного показнику зі значеннями, отриманими в університеті Карнегі-Меллон і надано пояснення причин таких розбіжностей.

Як зазначили самі дослідники, жодна з метрик ефективності не наблизилась до необхідного рівня, щоб досягти 0,001% помилок другого роду (коли зловмисник успішно проходить автентифікацію) та 1% помилок першого роду (коли власник сесії не проходить автентифікацію), необхідних за Європейським стандартом для систем контролю доступу [15]. Дослідниками було зроблено висновок, що необхідний додатковий прогрес, перш ніж можна буде повністю покластися на динаміку натискання клавіш для контролю доступу. Тим не менш,

дані методи автентифікації вже можна використовувати в парі з введенням паролю, як метод додаткового захисту.

Оскільки, за словами дослідників, другою причиною порівняння детекторів є виявлення перспективних стратегій виявлення аномалій, які можуть посприяти прогресу в цій галузі, було додатково проведено пошук спільних стратегій серед найефективніших детекторів. Всі найефективніші детектори використовують деяку форму масштабування часових ознак (наприклад, за допомогою відстані Махаланобіса, а не евклідової відстані). Відомо, що різні ознаки часу мають різну змінність (наприклад, ознака часу затиснення клавіші H є коротшою та більш стійкою, ніж ознака часу переходу від клавіші до клавіші UD, яка є повільнішою та більш змінною). Було встановлено, що детектори, які враховують ці різниці у масштабі, демонструють кращу ефективність.

1.3 Науково-технічна задача

В дослідженні, проведеному університетом Карнегі-Меллон, за словами дослідників, довелося зробити різні компроміси (наприклад, щодо того, які ознаки включати до векторів ознак та скільки таких векторів використовувати під час тренування детекторів), що безумовно вплинули на ефективність детекторів.

Складові науково-технічна задачі даної роботи:

- опрацювання відкритого набору даних динаміки друку, наданого університетом Карнегі Меллон;
- відтворення 7 найперспективніших, за результатами попередніх досліджень, детекторів аномалій;
- відтворення умов тестування, що були описані в звіті попереднього дослідження, з метою досягнення таких самих значень EER, що і в оригінальному звіті;
- експериментальне дослідження впливу розміру тренувального набору даних та вибору ознак друку на ефективність детекторів аномалій;
- формування висновків та надання рекомендацій;

– розробка програмної системи для проведення інтерактивних випробувань усіх розроблених детекторів аномалій.

Додатково було виявлено та обґрунтовано, чому значення EER вдалося відтворити набагато точніше, ніж значення ZMFAR, та чому, у зв’язку з цим, EER можна вважати значно стабільнішою та відтворюваною мірою ефективності детекторів аномалій.

2 ОПИС ТЕОРЕТИЧНИХ ТА ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

2.1 Опис теоретичних досліджень

З огляду на результати дослідження університету Карнегі-Меллон, були обрані наступні 7 детекторів аномалій, що показали найвищі значення ефективності:

- Евклідова відстань до усередненого вектору;
- Мангеттенська відстань до усередненого вектору;
- масштабована Мангеттенська відстань до усередненого вектору;
- відстань Махаланобіса до усередненого вектору;
- найближчий сусід за відстанню Махаланобіс;
- однокласовий SVM;
- лічильник викидів за z-оцінкою.

Решта 7 детекторів аномалій, що застосовували нейронні мережі, оригінальні підходи та дещо модифіковані версії класичних детекторів аномалій, показали значно нижчу ефективність згідно з тестуванням, проведеним дослідниками в [9]. Враховуючи вихідні ресурси досліджень даної роботи, було прийнято рішення розробити і дослідити саме 7 найкращих детекторів аномалій, хоча варто зазначити, що дослідження методів, пов’язаних з нейронними мережами, може бути перспективним напрямком в даній галузі, враховуючи останні досягнення в розвитку нейромереж.

Детектори аномалій, що використовують Евклідову, Мангеттенську та Махаланобіса відстань до усередненого вектору, є класичними прикладами детекторів аномалій для широкого кола задач. Усереднений вектор ознак може бути представлений наступною формулою 1:

$$\bar{y}[i] = \frac{y_1[i] + y_2[i] + \cdots + y_n[i]}{n}, \tag{1}$$

де i – може приймати значення від 1 до кількості ознак m друку конкретної фрази;

$y_j[i]$ – значення ознаки i для вектору ознак j;

n – загальна кількість векторів ознак, що містяться в тренувальному наборі.

У детекторах аномалій, що використовують Евклідову, Мангеттенську та відстань Махаланобіса до усередненого вектору ознак, використовуються класичні визначення цих відстаней. У випадку детектора аномалій, що використовує масштабовану Мангеттенську відстань, оцінка нового зразку відбувається за наступною формулою 2:

$$\sum_{j=1}^{m} \frac{|x_j - y_j|}{a_j}, \tag{2}$$

де x_j та y_j – значення ознак j тестового та усередненого векторів відповідно;

a_j – середнє абсолютне відхилення, отримане під час тренування.

У випадку з детектором аномалій найближчого сусіда за відстанню Махаланобіса, значенням оцінки стає мінімальне значення серед значень відстаней Махаланобіса, розрахованих для всіх векторів ознак, що містяться в тренувальному набору даних. У зв’язку з необхідністю збереження усіх векторів ознак в первинному вигляді та їхньої ітеративної обробки під час етапу оцінювання нових зразків даних, цей детектор аномалій є найвибагливішим до обчислювальних ресурсів. Тим не менш, під час експериментальних досліджень ця особливість не мала значного впливу на тривалість роботи через відносно невисокий мінімальний розмір тренувальних даних, необхідного для досягнення найвищої практично можливої точності детектору.

Детектор аномалій, що використовує однокласовий SVM, на етапі тренування будує гіперплощину, що ділить вектори ознак на дві групи:

- ті , що належать до класу векторів ознак, які були згенеровані істинним власником сесії;
- решта, що не могли бути згенеровані істинним власником сесії.

На етапі оцінювання нових векторів ознак, детектор знаходить мінімальну відстань від нового вектору ознак до гіперплощини. При цьому, в класичному

вигляді значення цієї відстані є додатним, якщо новий вектор ознак належить до єдиного класу, та від'ємним – якщо не належить. У зв'язку з тим, що решта детекторів аномалій, наведених в цій роботі, повертають менші значення оцінок векторів ознак, згенерованих істинними власниками сесії, задля порівняння ефективності розроблених детекторів числове значення відстані, отримане від однокласового SVM, змінюється за знаком на протилежне.

Однокласовий SVM має відносно велику кількість параметрів, але, нажаль, дослідники не навели детальний опис налаштування цієї моделі, тому невідомі значення були обрані з урахуванням значень за замовчуванням у використаних бібліотеках [9].

Детектор аномалій, що використовує лічильник викидів за z-оцінкою, розраховує z-оцінку для значення кожної з ознак у новому векторі ознак за наступною формулою 3:

$$z_j = \frac{|x_j - y_j|}{s_j}, \tag{3}$$

де x_j та y_j – значення ознак j тестового та усередненого векторів відповідно;

s_j – середнє квадратичне відхилення, отримане під час тренування.

Значення оцінки, отримуване цим детектором, є невід'ємним цілим числом, що відповідає кількості z_j значень, що перевищили деяке встановлене порогове значення. В подальших експериментальних дослідженнях це порогове значення встановлюється в 1,96 – так само, як це було зроблено дослідниками в [9].

Оскільки деякі детектори мають параметри, які впливають на їхню ефективність, виникає питання налаштування параметрів. Оскільки не існує загальноприйнятого методу налаштування параметрів детекторів аномалій для конкретного набору даних без внесення упередженості у результати оцінки ефективності детекторів аномалій [16], було використано параметри, вказані в першоджерелах.

2.2 Метрики ефективності моделей детекторів аномалій

Для вимірювання ефективності детекторів були використані наступні міри ефективності:

- ROC-крива;
- значення EER;
- значення ZMFAR.

ROC-крива (англ. Receiver Operating Characteristic curve) - це графічне зображення, що використовується для визначення ефективності бінарного класифікатора, такого як детектор аномалій. Вона відображає залежність між часткою правильних результатів (англ. True Positive Rate, TPR) та часткою неправильних результатів (False Positive Rate, FPR) при зміні порогового значення, яке використовується для вирішення, чи вважати конкретний вектор ознак позитивним чи негативним.

TPR відображає частку вірно визначених позитивних елементів (тобто, скільки разів було правильно виявлено аномалії в тестовій вибірці), а FPR відображає частку невірно визначених негативних елементів (тобто, скільки разів зазвичай здійснено помилкову ідентифікацію звичайних користувачів як аномальних).

Чим ближче до верхнього лівого кута графік ROC-кривої, тим краще функціонує детектор аномалій. За допомогою ROC-кривої можна порівняти ефективність різних детекторів аномалій та вибрати оптимальний поріг для вирішення задачі класифікації.

Однак ROC-криві в первинному вигляді неможливо використовувати для однозначного порівняння ефективності різних детекторів, а саме – створення списку детекторів, відсортованих за ефективністю, та визначення найкращих з них. У зв’язку цим, в даній роботі також використовуються такі міри ефективності, як EER та ZMFAR.

EER – це міра ефективності детекторів аномалій. Ця міра визначається як точка на ROC-кривій, де False Acceptance Rate (FAR) – частота помилкового надання доступу до системи, тобто визначення зловмисників істинними

власниками сесії, дорівнює False Rejection Rate (FRR) – частоті помилкових відхилень, тобто відсоток спроб автентифікації користувачів, коли вони були неправильно визнані зловмисниками. Порівнюючи це з класичним визначенням ROC-кривої, можна встановити, що визначення FAR та FPR є ідентичними, а FRR дорівнює (1 – TPR).

Для розрахунку ZMFAR, порогове значення вибирається таким чином, щоб частота FPR була мінімізована з тим обмеженням, що частота TPR дорівнює одиниці. При виборі такого порогового значення детектор аномалій не допускає жодного випадку надання доступу до систему зловмиснику, при цьому мінімізуючи кількість помилок першого роду, коли справжній користувач не проходить етап автентифікації.

Рівень EER та ZMFAR – це різні показники ефективності, але обидва є показниками помилок (тобто менші значення означають менше помилок та кращу ефективність).

2.3 План проведення експериментів

Як було зазначено в розділі з огляду наукової літератури, різні дослідники вилучають різні комбінації ознак друку. Дослідники з університету Карнегі-Меллон використали всі ознаки, які використовувалися в усіх дослідженнях. Зокрема, клавіша Enter вважалась частиною пароля, роблячи 10-символьний пароль довшим на 1 натискання клавіші, а в якості ознак друку були використані ознаки DD, UD та H одночасно. Для кожного введення пароля з 10 символів було витягнуто 31 ознаку і зібрано в вектор. Час зберігається у секундах (як числа з плаваючою комою). Багато з часових ознак корелюють між собою, а деякі є лінійно залежними (тобто кожен час між натисканнями клавіш можна розкласти на суму часу утримання та часу між відпусканням та натисканням клавіші). Дослідники не трансформували дані, щоб видалити ці кореляції, незважаючи на їх негативний вплив на деякі детектори. Інші дослідники досліджували стратегії компенсації через відбір ознак [14].

Як зазначили дослідники в [9], хоча попередні дослідники проводили експерименти для вимірювання ефективності різних детекторів аномалій, порівняння цих експериментальних результатів неможливе. Занадто багато факторів відрізняються від одного оцінювання до іншого. Дослідниками було надано відкритий набір даних та відтворюваний процес для проведення тестування детекторів аномалій.

Вибір паролів для оцінки детекторів аномалій є складним завданням. З одного боку, часто більш реалістичним є дозволити користувачам обирати свої паролі. З іншого боку, збір даних ускладняється, оскільки для кожного пароля потрібні різні зразки від зловмисників. Деякі дослідники вважають, що надання можливості користувачам обирати свої паролі полегшує їхнє розрізнення [11]. Якщо це правда, то дозволити користувачам обирати свої паролі призведе до спотворення результатів експерименту, призначеного для оцінки ефективності на довільному паролі. При створенні відкритого набору даних було вирішено, що всі учасники будуть набирати однаковий пароль. Щоб створити пароль, який був би типовим і містив би достатньо символів, був використаний генератор паролів та інструмент для перевірки паролів на міцність. Було створено 10-символьний пароль, що містить літери, цифри та знаки пунктуації, та трохи його змінено, замінивши деякі знаки та регістр, щоб він краще відповідав загальній уяві про міцний пароль. Отриманий пароль має наступний вигляд: .tie5Roanl. Перевірочний інструмент на міцність оцінив цей пароль як міцний, оскільки він містить більше 7 символів, велику літеру, цифру та знак пунктуації. Найкращими з точку зору безпеки є паролі довші за 13 символів, але, згідно з попередніми дослідженнями, довжина паролю 10 є типовим значенням. Ті дослідження, де використовувалися довші рядки, частіше використовували слова та фрази з англійської мови, які легше набирати, ніж випадкові послідовності літер, цифр та знаків пунктуації.

Задля збору даних дослідниками був розроблений комп’ютерний додаток. Додаток відображає пароль на екрані з текстовим полем для введення. Щоб перейти до наступного екрану, суб’єкт повинен правильно ввести 10 символів

пароля послідовно та натиснути клавішу Enter. Якщо в послідовності виявлено будь-які помилки, суб’єкт повинен повторно ввести пароль. Суб’єкт повинен правильно ввести пароль 50 разів, щоб завершити сеанс збору даних. Кожного разу, коли суб’єкт натискає або відпускає клавішу, додаток записує подію (тобто натискання або відпускання), назву використаної клавіші та час виникнення події.

Для створення точних міток часу було використано зовнішній зразковий годинник. Було продемонстровано, що точність зразкового годинника становить ±200 мікросекунд (шляхом використання функціонального генератора для імітації натискань клавіш з фіксованим інтервалом). Звичайно, в реальних умовах суб’єкти не будуть вводити свій пароль 50 разів поспіль, і вони будуть вводити його на своїх власних комп'ютерах, а не на клавіатурі дослідників. Було вирішено пожертвувати певною кількістю реалізму задля більшої контрольованості проведення збору даних.

Для збору даних була залучена 51 особа з університету Карнегі-Меллона. Суб’єкти завершили 8 сесій збору даних (по 50 паролів у кожній), згенерувавши загалом по 400 зразків введення паролів. Вони чекали принаймні один день між сесіями, щоб відобразити деяку денну варіацію набору тексту кожним суб’єктом. Набір суб’єктів складався з 30 чоловіків та 21 жінки. Було 8 лівшів та 43 правшів. Медіана вікової групи була 31-40 років, наймолодша особа була віком 18-20 років, а найстарша – 61-70 років. Сесії суб’єктів тривали від 1,25 до 11 хвилин, медіанний час сесії становив близько 3 хвилин.

Розглянемо сценарій, в якому пароль користувача був скомпрометований зловмисником. Припускається, що користувач має досвід у наборі свого пароля, тоді як зловмисник незнайомий з ним (наприклад, вводить його вперше). Вимірюється, наскільки добре кожен з розроблених детекторів може розрізнити введення паролю зловмисником та справжнім користувачем в цьому сценарії. Один з 51 суб’єкта призначається справжнім користувачем, а решта – зловмисниками. Детектор аномалій тренується та перевіряється на здатність розпізнавати справжнього користувача та зловмисників наступним чином (згідно з [9]):

- відбувається фаза тренування детектора на векторах ознак з перших 200 повторень паролю, набраних справжнім користувачем. Детектор будує поведінкову модель друку користувача;
- запускається тестова фазу детектора на векторах ознак з решти 200 повторень, набраних справжнім користувачем. Відповідно, на основі зроблених оцінок вже можна розрахувати TPR;
- нарешті, тестова фаза детектора продовжується на векторах ознак з перших п'яти повторень, набраних кожним з 50 зловмисників. Відповідно, на основі цих оцінок можна визначити FPR.

Цей процес потім повторюється, призначаючи кожного з інших суб’єктів по черзі як дійсного користувача.

Як зазначили самі дослідники, 200 повторень може здаватись нереально великою кількістю тренувальних даних. Одначе дослідники були також стурбовані тим, що менша кількість паролів може несправедливо призвести до того, що один або декілька детекторів не будуть працювати належним чином в порівнянні з тестуваннями, проведеними в попередніх дослідженнях. Так само, непідготовленість зловмисника може здатися нереалістичною, оскільки зловмисники можуть заздалегідь практикуватись, якщо вони знають, що час введення паролю важливий. Дослідники свідомо обмежились такими умовами тестування.

В даній роботі було не тільки відтворено 11 з 14 детекторів аномалій, наведених в [9], але й було відтворене оригінальне тестування та проведене додаткове тестування для різних розмірів тренувального набору даних та різних наборів ознак друку.

В якості різних розмірів тренувального набору даних були використані наступні:

- від 5 до 50 векторів ознак з кроком 5;
- від 60 до 100 векторів ознак з кроком 10;
- від 110 до 200 векторів ознак з кроком 20.

Для тестових наборів даних було збережено співвідношення між векторами, що належать справжньому користувачеві, та векторами, що належать решті користувачів, а саме – 4 до 5. Підмножини векторів справжнього користувача формувались з усієї множини його векторів ознак, відсортованих за зростанням в хронологічному порядку, що має відповідати реальним умовам використання подібної системи автентифікації. Підмножини векторів решти користувачів були також відсортовані за складеним ключем, що складався з номеру сесії, номеру введення під час сесії та ідентифікатора користувача. Таким чином, для різних розмірів наборів даних від решти користувачів була досягнена максимальна варіативність поведінок зловмисників.

Весь процес тестування, описаний вище, був додатково повторений для зменшеного набору ознак, а саме – для UD та H. Для кожного детектору аномалій при фіксованому розмірі наборів даних та фіксованому наборі ознак друку були побудовані гістограми розподілу значень EER та ZMFAR між користувачами; а для нефіксованого розміру наборів даних – побудовані графіки впливу розміру тренувального набору даних на середні EER та ZMFAR.

Для розробки описаних вище детекторів аномалій та плану тестування була використана мова Python 3.11, та такі її пакети для роботи з векторними, табличними та багатовимірними даними, як NumPy, Pandas, SciPy. Для побудування графіків та діаграм була використана бібліотека matplotlib. Відкритий набір даних зберігався у форматі CSV.

Кожен з детекторів аномалій було розроблено у вигляді класу ООП, що успадковувався від абстрактного класу, код якого наведено на рисунку 2.2.

В якості прикладу, розглянемо клас детектору аномалій, що знаходить найближчих сусідів за відстанню Махаланобіса. Конструктор даного класу створює приватні змінні, що відповідають за збереження стану тренування, усіх векторів ознак, що знаходяться в тренувальному наборі даних, та оберненої коваріаційної матриці. Код конструктора наведено на рисунку 2.3.

```
import abc
import pandas as pd


class AbstractAnomalyDetector(
    metaclass=abc.ABCMeta
):
    @abc.abstractmethod
    def train(self, train_data: pd.DataFrame) -> None:
        """
        Train the detector using the dataset of "normal" samples.
        As soon as training is completed, the detector can be used for
        detection of anomalies in new samples.
        :param train_data: Each row is a vector of feature values.
        """
        pass

    @abc.abstractmethod
    def score(self, test_data: pd.DataFrame) -> pd.DataFrame:
        """
        Calculate anomaly scores for each sample of the provided dataset.
        The detector must be already trained before calling this method.
        :param test_data: Each row must have the same number of features as
        the test dataset's rows.
        :return: A vector of scores for each given sample. Each score value is
        implementation-specific and a threshold value must be chosen respectively.
        """
        pass
```

Рисунок 2.2 – Абстрактний клас детектору аномалій

```
import numpy as np
import pandas as pd
from scipy.spatial.distance import mahalanobis

from anomaly_detector import AbstractAnomalyDetector


class NearestNeighborMahalanobisAnomalyDetector(
    AbstractAnomalyDetector
):
    def __init__(self):
        self._is_trained: bool = False
        self._train_data: pd.DataFrame = pd.DataFrame()
        self._inv_cov_matrix: pd.DataFrame = pd.DataFrame()
```

Рисунок 2.3 – Конструктор класу детектора аномалій

Код методу класу, що відповідає за тренування детектору, створює копію тренувального набору даних, знаходить обернену коваріаційну матрицю та змінює значення змінної стану тренування, що наведено на рисунку 2.4.

```
def train(self, train_data: pd.DataFrame) -> None:
    self._train_data = train_data.copy()
    cov_matrix = train_data.cov()
    self._inv_cov_matrix = pd.DataFrame(
        # generalized inverse
        np.linalg.pinv(cov_matrix.values),
        columns=cov_matrix.columns,
        index=cov_matrix.index
    )
    self._is_trained = True
```

Рисунок 2.4 – Метод класу, що відповідає за тренування детектору

Після проведення тренування детектору, стає можливим використання його методу для розрахування оцінок для нових векторів ознак. Код методу, що знаходить відстань від нового вектору ознак до найближчого вектору з тренувального набору даних наведено на рисунку 2.5.

```
def score(self, test_data: pd.DataFrame) -> pd.DataFrame:
    if not self._is_trained:
        raise RuntimeError('detector is not trained')

    scores = []

    for _, test_row in test_data.iterrows():
        min_distance = float('inf')
        for _, train_row in self._train_data.iterrows():
            curr_distance = mahalanobis(test_row, train_row, self._inv_cov_matrix)
            min_distance = min(min_distance, curr_distance)
        scores.append(min_distance)

    return pd.DataFrame({'score': scores})
```

Рисунок 2.5 – Метод класу, що відповідає за розрахунок оцінок

Наведене використання поліморфізму дозволило прискорити розробку коду для тестування детекторів аномалій та посприяти зручності використання цього коду в інтерактивному додатку, опис якого буде наведено в наступних розділах.

2.4 Результати проведення експериментальних досліджень

Перш за все, варто відзначити досягнену точність при відтворенні базових експериментальних досліджень університету Карнегі-Меллон для 11 розроблених детекторів аномалій. Отримані значення EER та ZMFAR для тренувального набору даних з 200 векторів ознак та повного набору ознак друку наведені в таблиці 2.1.

Таблиця 2.1 – Отримані значення EER та ZMFAR

Детектор аномалій	Середній EER за [9]	Відтворений середній EER	Середній ZMFAR за [9]	Відтворений середній ZMFAR
Масштабована Мангеттенська відстань	0,096	0,098	0,601	0,559
Найближчий сусід за відстанню Махаланобіса	0,100	0,100	0,468	0,706
Лічильник викидів за z-оцінкою	0,102	0,101	0,782	0,410
Однокласовий SVM	0,102	0,119	0,504	0,766
Відстань Махаланобіса	0,110	0,110	0,482	0,742
Мангеттенська відстань	0,153	0,153	0,843	0,604
Евклідова відстань	0,171	0,171	0,875	0,736

Майже для всіх розроблених детекторів аномалій вдалося відтворити значення EER з високою точністю за результатами проведеного тестування.

Єдиним виключенням є однокласовий SVM у зв’язку з відсутністю вичерпного опису налаштувань цієї моделі в оригінальній роботі.

Окремої уваги заслуговує розбіжність в отриманих значеннях ZMFAR зі значеннями, отриманими в оригінальному дослідженні. Для пояснення причин такої розбіжності доцільним є використання ROC-кривих. ROC-криві, отриманні в результаті тестування детектору аномалій, що знаходить відстань Махаланобіса до найближчого сусіда, для суб’єкту з ідентифікатором s019 в оригінальному дослідженні та в даній роботі наведені на рисунках 2.6 і 2.7 відповідно.

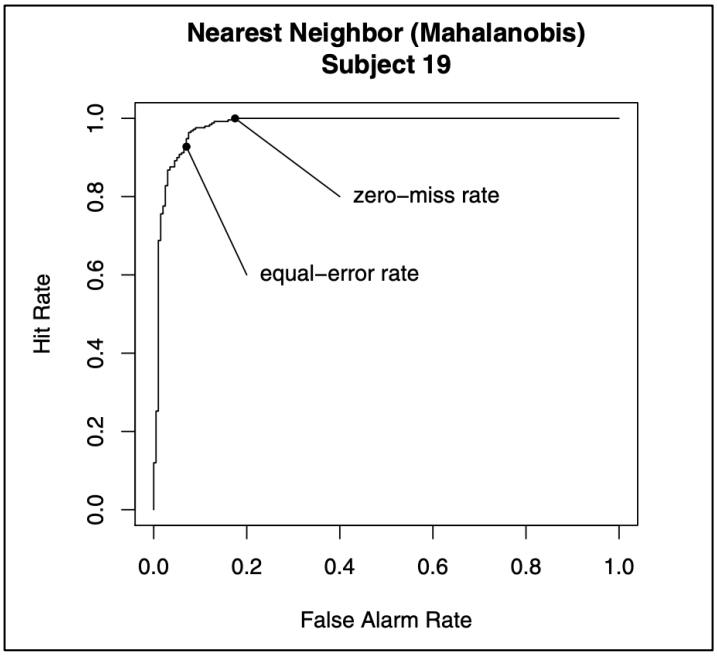

Рисунок 2.6 – ROC-крива в дослідженні [9]

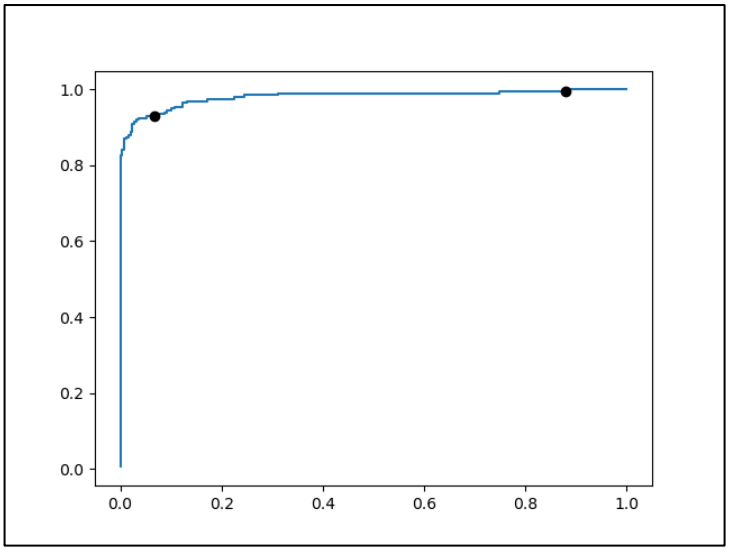

Рисунок 2.7 – ROC-крива, отримана в даній роботі

В той час, як значення EER практично співпадають, значення ZMFAR значно відрізняються. Тим не менш, значення TPR стає дуже близьким до 1 для всіх значень FPR і в роботі [9], і в даній роботі. ZMFAR є дуже вибагливим до похибок, бо присутність навіть одної помилки False Positive може призвести до дуже значного збільшення порогового значення для усунення цієї помилки і знаходження ZMFAR. Міра ефективності EER, на відміну від ZMFAR є менш вразливою до похибок та більш відтворюваною, тому, в загальному випадку, є кращою мірою для порівняння ефективності різних детекторів аномалій.

Найкращий рівень EER становив 0,096 і був отриманий детектором аномалій за масштабованою Мангеттенська відстанню. Детектор найближчого сусіда за відстанню Махаланобіса та детектор лічильнику викидів за z-оцінками були іншими детекторами, які продемонстрували високу ефективність за мірою EER.

3 АНАЛІЗ РЕЗУЛЬТАТІВ ДОСЛІДЖЕННЯ

3.1 Аналіз впливу розміру тренувального набору на ефективність моделей

Автори дослідження [9] прямо зазначили, що обраний розмір тренувального набору даних в 200 векторів ознак може здатись занадто великим для тестування детекторів аномалій в умовах, наближених до реальних. Бо система автентифікації, що для початку роботи з собою вимагає від користувачів введення конкретної фрази 200 разів поспіль, не може забезпечити високий рівень досвіду використання для користувачів. Тоді постає проблема пошуку компромісу між ефективністю детекторів аномалій та їхньою зручністю користування, бо чим більший за розміром тренувальний набір даних, тим, зазвичай, вища ефективність детектору аномалій, але нижчий рівень зручності використання.

В даній роботі було проведено експериментальне дослідження впливу розміру тренувального набору даних на ефективність розроблених детекторів аномалій. В якості різних розмірів тренувального набору даних були використані наступні:

- від 5 до 50 векторів ознак з кроком 5;
- від 60 до 100 векторів ознак з кроком 10;
- від 110 до 200 векторів ознак з кроком 20.

Для тестових наборів даних було збережено співвідношення між векторами, що належать справжньому користувачеві, та векторами, що належать решті користувачів, а саме – 4 до 5. Підмножини векторів справжнього користувача формувались з усієї множини його векторів ознак, відсортованих за зростанням в хронологічному порядку, що має відповідати реальним умовам використання подібної системи автентифікації. Підмножини векторів решти користувачів були також відсортовані за складеним ключем, що складався з номеру сесії, номеру введення під час сесії та ідентифікатора користувача. Таким чином, для різних розмірів наборів даних від решти користувачів була досягнена максимальна варіативність поведінок зловмисників.

Графік залежності середнього EER від розміру тренувальних даних для детекторів аномалій на основі Евклідової відстані та Мангеттенської відстані

наведені на рисунку 3.1.

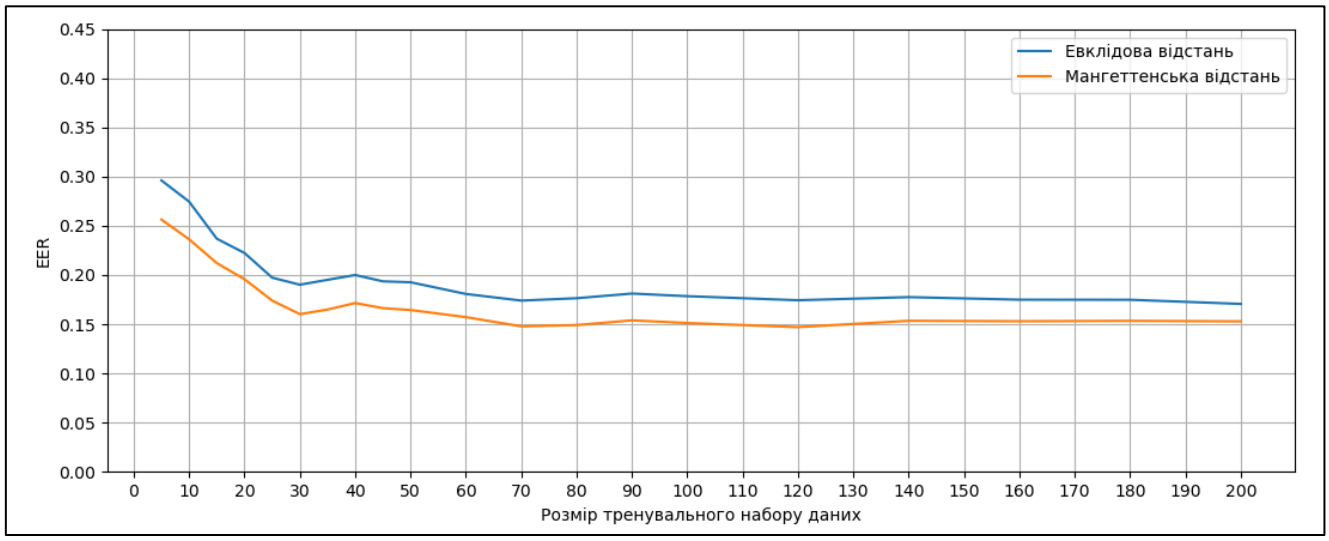

Рисунок 3.1 – Графік залежності середнього EER від розміру тренувальних даних

Після тренування на основі 70 векторів ознак, значення EER практично не змінюється для обох детекторів. Швидкість зменшення значення EER практично однакова при зміні розміру тренувальних наборів даних.

Графік залежності середнього EER від розміру тренувальних даних для детектору аномалій на основі однокласового SVM наведено на рисунку 3.2.

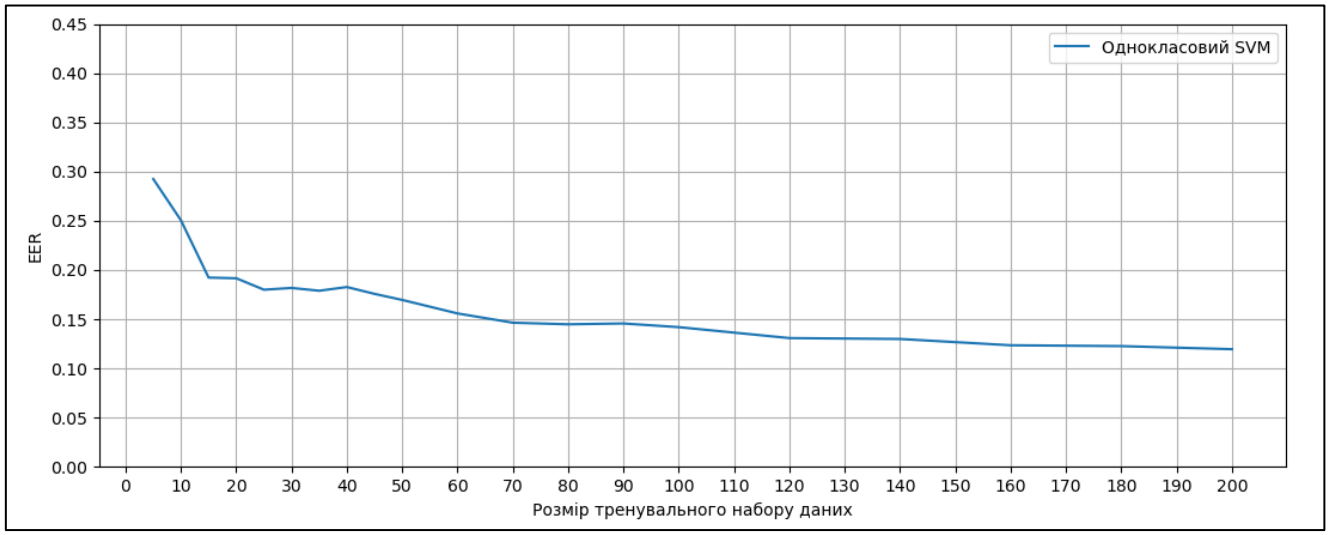

Рисунок 3.2 – Графік залежності середнього EER від розміру тренувальних даних

Судячи з отриманих значень EER для однокласового SVM, можна зробити припущення, що EER не досяг свого мінімального сталого значення. На жаль, кількості даних у вибраному наборі даних не вистачає для подальшого вивчення

цього впливу. Тим не менш, на меншій кількості даних інші детектори аномалій показують кращу ефективність, що буде наведено далі.

Графік залежності середнього EER від розміру тренувальних даних для детекторів аномалій на основі відстані Махаланобіса та найближчому сусіді за відстанню Махаланобіса наведені на рисунку 3.3.

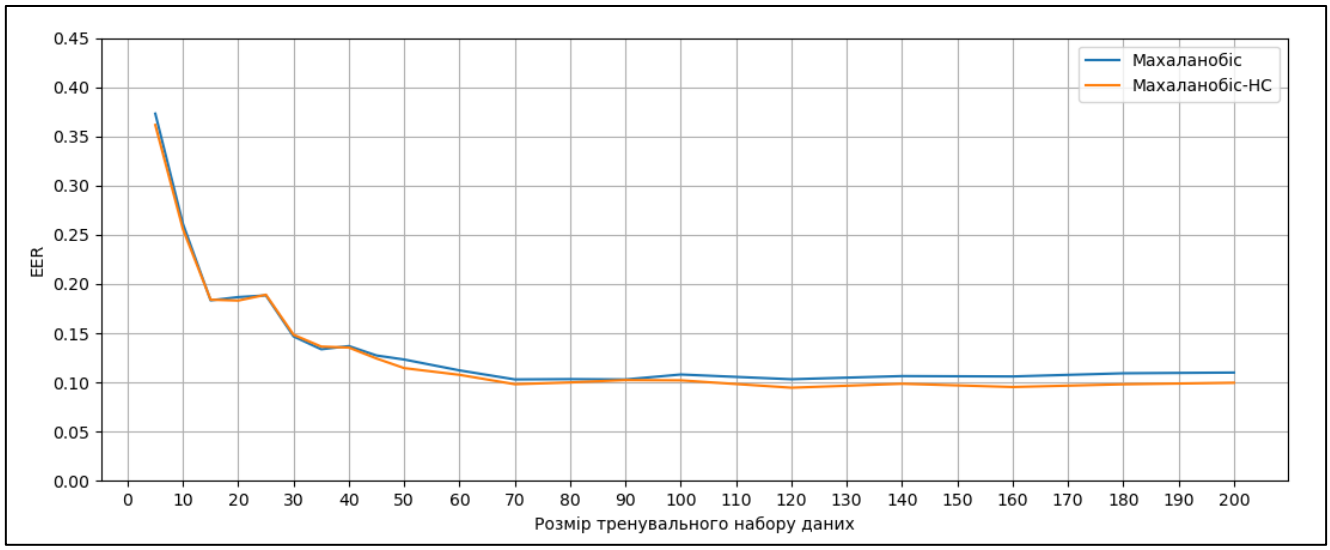

Рисунок 3.3 – Графік залежності середнього EER від розміру тренувальних даних

Практично для усіх розмірів даних детектор аномалій найближчого сусіда за відстанню Махаланобіса показує вищу ефективність, ніж його простіший варіант. Тим не менш, обидва детектори аномалій показують зависокий EER для малих розмірів даних на відміну від усіх інших розроблених детекторів аномалій. Крім того, детектор аномалій найближчого сусіда потребує значно більше ресурсів для збереження моделі друку користувача та розрахування оцінки для нового вектору ознак, ніж усі інші детектори аномалій, в той же час надаючи непропорційно мале покращення значення EER в порівнянні із своєю простішою версією.

Графік залежності середнього EER від розміру тренувальних даних для детекторів аномалій на основі масштабованої Мангеттенської відстані та лічильнику викидів за z-оцінкою наведені на рисунку 3.4.

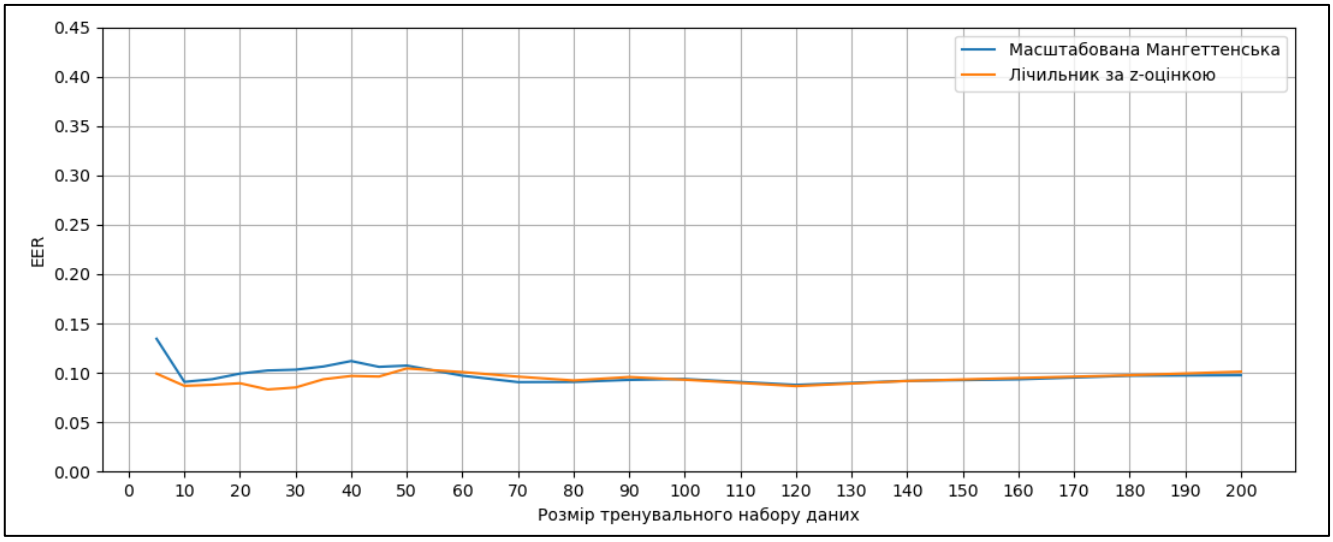

Рисунок 3.4 – Графік залежності середнього EER від розміру тренувальних даних

Дані два детектори аномалій досягли сталого мінімального значення EER при найменшій кількості векторів ознак в тренувальному наборі даних. Крім того, вони показали здібність працювати відносно точно і при малій кількості даних, при цьому лічильник викидів за z-оцінкою показав дещо кращі результати. Обидва детектори аномалій показали відносно низьку залежність від розміру тренувального набору даних і сталу ефективність. Такі результати можна пояснити вищою стійкістю даних детекторів аномалій до кореляції між ознаками друку. Було помічено, що різні ознаки друку мають різну змінність (наприклад, час утримання клавіші H має тенденцію бути швидшим і більш стійким, ніж час переходу між клавішами UD, який повільніший і має більшу змінність). Детектори, які враховують ці різниці в масштабі, демонструють кращу ефективність.

3.2 Аналіз впливу вибору ознак друку на ефективність моделей

Спираючись на попередні дослідження щодо кореляції між ознаками друку, використаними в існуючих детекторах аномалій, було проведено додаткове експериментальне дослідження впливу вибору набору ознак друку на ефективність детекторів аномалій [14]. Зокрема, з усіх векторів ознак були вилучені значення, що відповідають ознакам типу DD. Згідно із результатами

додаткового тестування було виявлено, що обидва детектори аномалій, що використовують відстань Махаланобіса, виявились стійкими до кореляції між ознаками, тому вилучення ознак типу DD практично ніяк не вплинуло на їхню ефективність. Проте для детекторів аномалій на основі масштабованої Мангеттенської відстані та лічильнику викидів за z-оцінкою вдалося досягти значного покращення ефективності за EER, що наведено на рисунках 3.5 та 3.6 відповідно.

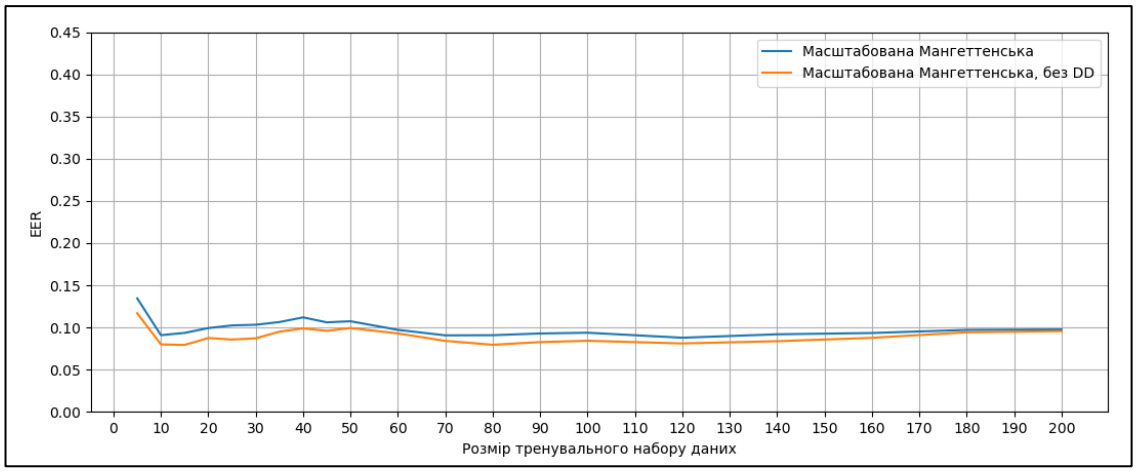

Рисунок 3.5 – Масштабована Мангеттенська відстань

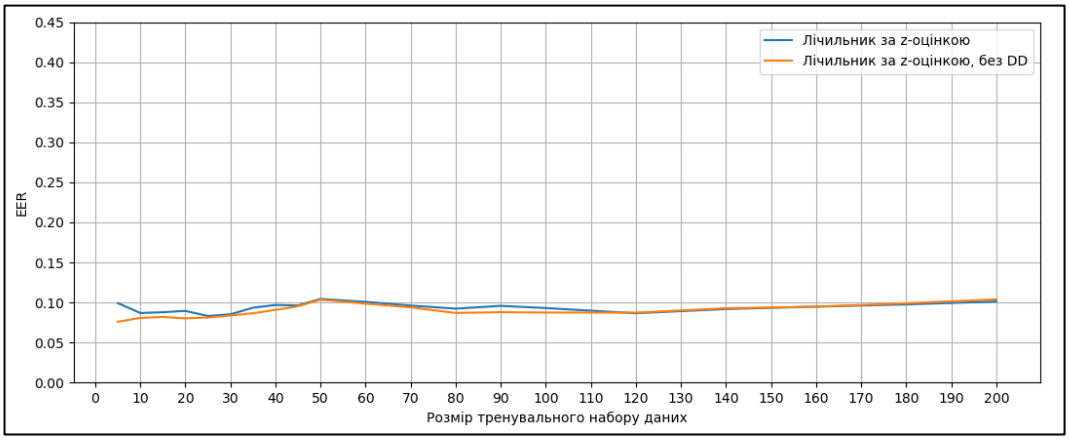

Рисунок 3.6 – Лічильник викидів за z-оцінкою

Таким чином, усунення ознаки друку типу DD дозволяє не тільки збільшити ефективність деяких детекторів аномалій, але й зменшити кількість пам’яті, необхідної для зберігання векторів ознак та моделей друку користувачів, та зменшити час, необхідний на обробку цих даних.

4 ОПИС ПРОГРАМНОЇ СИСТЕМИ

4.1 Опис використаних технологій

Інтерактивний додаток, що дозволяє проводити ручні випробування кожного з розроблених і описаних вище детекторів аномалій, був розроблений із застосуванням наступних технологій [17]:

- мова Python версії 3.11;
- пакети NumPy, Pandas, SciPy для роботи з векторами, таблицями, багатовекторними даними та алгоритмами для них;
- пакет ipywidgets для розробки інтерактивних віджетів;
- пакет Voila для розробки веб-додатків за допомогою Python без написання коду на JavaScript та HTML.

Пакет Voila в поєднанні з елементами користувацького інтерфейсу з пакету ipywidgets, дозволяє інтегрувати методи візуалізації, доступні для табличних даних з пакету Pandas, у веб-додаток без необхідності написання і, навіть, знання мов веб-програмування JavaScript та HTML.

4.2 Опис розробленої програмної системи

Запуск програмної системи відбувається через командний рядок операційної системи, в результаті веб-додаток стає доступним за адресою localhost:8866. При переході за цією адресою у веб-браузері буде відображено інтерфейс веб-додатку. Зображення користувацького інтерфейсу веб-додатку наведено на рисунку 4.1.

Серед функцій веб-додатку можна виділити наступні:

- вибір одного з 20 користувацьких профілів з різними паролями;
- відстеження подій клавіатури для створення вектору ознак друку під часу набору пароля;
- відображення вектору ознак друку UD та H;

– оцінювання нового вектору ознак друку всіма розробленими детекторами аномалій та миттєве внесення оцінок в спільну таблицю, що відображена в інтерфейсі;
– адаптивне тренування усіх детекторів аномалій з новим вектором ознак друку, що має бути врахований в подальшому тестуванні;
– можливість вимкнути адаптивне тренування при проведені випробувань з умовними зловмисниками;
– можливість збереження стану всіх детекторів аномалій у файл формату .pkl для повторного завантаження у пам’ять при наступному запуску веб-додатку.

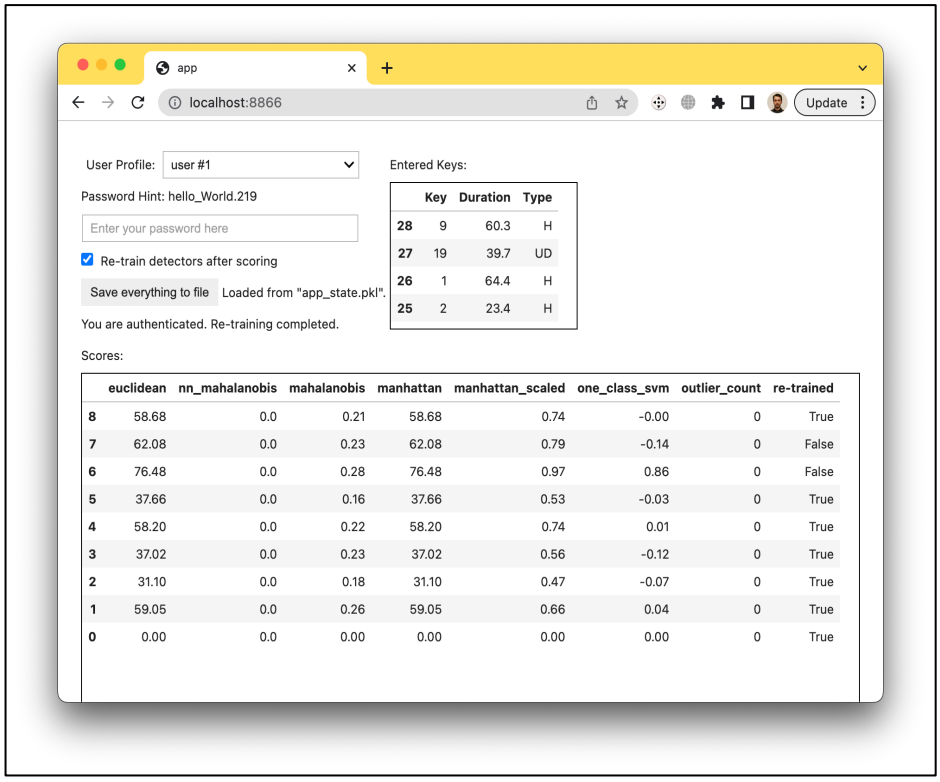

Рисунок 4.1 – Користувацький інтерфейс розробленого веб-додатку

Даний веб-додаток дозволяє зручно проводити ручне тестування будь-яких детекторів аномалій, що успадковують абстрактний клас детектору аномалій, описаного в попередніх розділах, та отримувати миттєві оцінки векторів ознак друку [18].

5 МОЖЛИВОСТІ ВПРОВАДЖЕННЯ У НАУКОВІЙ І ПРАКТИЧНІЙ ДІЯЛЬНОСТІ

Можливості впровадження методів автентифікації на основі даних динаміки друку залежать від вимог, поставлених до системи автентифікації в цілому. Наприклад, Європейський стандарт для систем контролю доступу встановлює максимальні допустимі значення для долі помилок першого роду (коли справжній користувач не пройшов автентифікацію) в 1%, а для долі помилок другого роду – 0.001% [15]. Це стосується того випадку, коли метод автентифікації на основі даних друку використовується, як єдиний фактор автентифікації, без паролю тощо. Як було наведено вище, наразі жоден детектор аномалій не може досягти таких показників ефективності, тому є необхідним подальший прогрес в цій галузі.

Тим не менш, вже відомі приклади комерційного застосування методів автентифікації на основі друку – наприклад, комерційний продукт TypingDNA [21]. Зокрема, TypingDNA пропонує рішення задачі автентифікації і на основі набору статичної фрази, і на основі аналізу набору довільних текстових даних впродовж користувацької сесії у фоновому режимі. При цьому є можливим вибір одного з трьох режимів автоматичного підбору порогового значення: «менш строгий», «середній», «більш строгий» [22]. Розробники даного ПЗ самі при цьому зазначили, що «середній» рівень строгості порогового значення є компромісом між рівнями FAR та FRR [23].

Перспективним є використання описаних методів в якості другого кроку під час двофакторної автентифікації (англ. two-factor authentication, 2FA) [24]. Зокрема, саме це і пропонує TypingDNA в рамках свого рішення задачі автентифікації на основі даних набору статичної фрази.

Серед головних переваг використання таких методів автентифікації зазначається вища швидкість взаємодії користувача з системою двофакторної автентифікації на відміну від звичайного сценарію, коли користувачу необхідно ввести код з SMS-повідомлення на телефоні тощо [19].

Технологія біометричної автентифікації за допомогою динаміки набору тексту спрощує шлях до безпечної автентифікації і в банківській справі. Зокрема, European Bank Authority (EBA) явним чином виокремлює динаміку набору тексту як елемент автентифікації з достатньо високим рівнем безпеки для практичного застосування [20].

ВИСНОВКИ

В результаті роботи були отримані наступні результати:

- проведено аналіз існуючих наукових робіт в області методів та моделей автентифікації на основі даних динаміки друку;
- відтворені моделі детекторів аномалій, виявлені загальні вимоги до кожної з них;
- розглянуто переваги і недоліки таких мір ефективності моделей детекторів аномалій, як EER та ZMFAR;
- проведено тестування розроблених моделей детекторів аномалій на відкритому наборі даних та визначено вплив таких параметрів, як розмір тренувальних даних та набір ознак друку, на ефективність кожної з моделей детекторів;
- розроблено програмне забезпечення для випробування всіх розроблених моделей детекторів в інтерактивному режимі.

Хоч застосування нейронних мереж і не призвело до отримання високих показників ефективності згідно з [9], одним з перспективних напрямків подальших досліджень в області методів та моделей автентифікації користувачів на основі даних про взаємодію з клавіатурою є повторний перегляд їх застосування для вирішення даної задачі з урахуванням усіх останніх досягнень в розвитку нейронних мереж.

З огляду на те, як просте усунення однієї ознаки друку позитивно вплинуло на ефективність частини розроблених моделей детекторів аномалій, подальше дослідження попередньої обробки тренувальних та тестових даних, а також і можливе знаходження нових ознак друку на основі існуючих є також перспективним напрямком в цій галузі.

Вибір порогового значення для моделі детектору аномалій, що пройшла етап тренування, є важливим для знаходження балансу між ефективністю моделі детектора аномалій та долею помилкових визначень справжнього користувача зловмисником, що безпосередньо впливає на зручність користування методом

автентифікації в цілому. Методи пошуку таких порогових значень для практичних застосунків даних методів автентифікації не були розглянуті в даній роботі з огляду на вихідні ресурси та пріоритетність досліджень, але також є перспективним напрямком подальшої роботи.

Вимірювання ефективності розроблених моделей детекторів аномалій допомогло зрозуміти, які з них є більш придатними до використання для малих наборів тренувальних даних, що є важливим для практичного впровадження подібних методів автентифікації, враховуючи зручність використання методів користувачами. Зокрема, це були моделі детекторів аномалій за масштабованою Мангеттенською відстанню та лічильником викидів за z-оцінкою. Проведення додаткових експериментальних досліджень зі зменшеним набором ознак (з усуненням ознак типу DD) допомогло досягти ще кращих значень ефективності для даних моделей детекторів аномалій.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. M. Teli, J. Beveridge, P. Phillips, G. Givens, D. Bolme, B. Draper. Biometric zoos: Theory and experimental evidence// International Joint Conference on Biometrics, 2011. – P. 213.

2. F. Monrose, A. Rubin. Authentication via keystroke dynamics// Proceedings of the 4th ACM Conference on Computer and Communications Security, 1997. – P. 56.

3. F. Deravi, S. P. Guness. Gaze trajectory as a biometric modality// Biosignals, 2011. – P. 341.

4. C. Shen, Z. Cai, X. Guan, Y. Du, R. A. Maxion. User authentication through mouse dynamics – IEEE Transactions on Information Forensics and Security, 2013. – P. 30.

5. K. Chen. Towards better making a decision in speaker verification// Pattern Recognition, 2003 – P. 346.

6. D. Gunetti, C. Picardi. Keystroke analysis of free text// ACM Transactions on Information Systems and Security, 2005. – P. 347.

7. T. Shimshon, R. Moskovitch, L. Rokach, Y. Elovici. Continuous verification using keystroke dynamics// International Conference on Computational Intelligence and Security, 2010. – P. 415.

8. P. Y. Wu, C. C. Fang, J. M. Chang, S. Y. Kung. Cost-effective kernel ridge regression implementation for keystroke-based active authentication system// IEEE Transactions on Cybernetics, 2016 – P. 12.

9. K. Killourhy, R. Maxion. Comparing anomaly-detection algorithms for keystroke dynamics// IEEE/IFIP International Conference on Dependable Systems Networks, 2009. – P. 134.

10. P. S. Teh, A. Teoh, S. Yue. A Survey of Keystroke Dynamics Biometrics// The Scientific World Journal, 2013. – P. 24.

11. Y. Zhong, Y. Deng. A Survey on Keystroke Dynamics Biometrics: Approaches, Advances, and Evaluations// GCSR, 2013. – P. 1-22.

12. Кайдалов В. Д., Голян В. В. Дослідження методів та моделей автентифікації на основі даних про взаємодію з клавіатурою// IV International

Scientific and Practical Conference «Grundlagen der modernen wissenschaftlichen Forschung», 2023. – P. 95–96.

13. User Verification Based on Keystroke Dynamics// Applied Machine Learning. URL: https://appliedmachinelearning.wordpress.com/2017/07/26/user-verification-based-on-keystroke-dynamics-python-code/ (дата звернення: 01.04.2023).

14. T. Wu, K. Zheng, C. Wu, X. Wang, G. Xu. User Identification by Keystroke Dynamics Based on Feature Correlation Analysis and Feature optimization// IEEE 5th International Conference on Computer and Communications, 2019. – P. 40-46.

15. CENELEC. European Standard EN 50133-1: Alarm systems. Access control systems for use in security applications. Part 1: System requirements, 2002. Standard Number EN 50133-1:1996/A1:2002, Technical Body CLC/TC 79, European Committee for Electrotechnical Standardization (CENELEC).

16. H. J. Lee, S. Cho. Retraining a keystroke dynamics-based authenticator with impostor patterns// Computers & Security, 2007. – P. 30-39.

17. Голян В.В., Бітюкова Є.І. Дослідження технологій та інструментів управління проектами// Монографія: SCIENCE, RESEARCH, DEVELOPMENT#27/ NECHNICS AND TECHNOLOGY – 2020. – 33 с.

18. Голян В.В., Кравченко О.К. Порівняння моделей життєвих циклів програмного забезпечення з метою виявлення найефективнішого// Збірник наукових праць ХНУ ПС №2 (157) – 2019. – 6 с.

19. Голян В.В., Євсєєва М.С. Методика розробки сайтів за допомогою спеціальних символів і баз даних// Сб. наук. праць за матеріалам 18-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь в XXI ст.» – 2015. – с. 193-194.

20. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2// European Banking Authority. URL: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536- 69a5- 44a5- a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20

.pdf?retry=1&_ga=2.34815457.1729804422.1683573534-601473101.1680004842 (дата звернення: 01.04.2023).

21. Replace SMS 2FA codes with better UX: Just type 4 words// TypingDNA. URL: https://www.typingdna.com/verify (дата звернення 01.04.2023).

22. V. Apukhtin, M. Shirokopetleva, V. Skovorodnikova. The Relevance of Using Message Brokers in Robust Enterprise Applications// IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2019. – P. 305-309.

23. Hramm, O., Bilous, N., Ahekian, I. Configurable Cell Segmentation Solution Using Hough Circles Transform and Watershed Algorithm. Proceedings of the International Conference on Advanced Optoelectronics and Lasers, CAOL, 2019, 2019-September, стр. 602-605, 9019493.

24. Білоус Н. В., Черненко Є. А. Проблеми та рішення локалізації об’єктів. XII Міжнародна науково-практична конференція “MODERN DIRECTIONS OF SCIENTIFIC RESEARCH DEVELOPMENT”, 18-20 травня 2022 року Чикаго, США, стр. 1-3.