Додаток А.

Комплект графічних матеріалів

# Дослідження ефективності ідентифікації особистості за клавіатурним почерком з урахуванням сили тиску на клавіші

**Актуальність роботи.** В наш час активно відбуваються процеси інформатизації суспільства. З'являється все більше веб-сервісів. Багато держав прагнуть створити електронний уряд для надання послуг громадянам. Довіра до таких веб-сервісів з боку користувачів має бути найвищою, тому в організаціях різного рівня все частіше впроваджуються біометричні системи захисту.

Статичні біометричні образи (відбиток пальця, сітківка або райдужка) не є секретними, тому їх можна скопіювати, виготовивши фізичний або цифровий муляж (для віддаленої аутентифікації). Таємні біометричні образи потенційно можуть забезпечити більш високий рівень захисту. До них належить індивідуальний клавіатурний почерк суб'єкта, що може бути кількісно описаний в процесі набору парольної фрази.

Недоліком методу аутентифікації за клавіатурним почерком є порівняно низька надійність прийнятих рішень – ймовірностей помилкової відмови у доступі (FRR) та помилкового доступу (FAR).

Кваліфікаційна робота присвячена підвищенню надійності розпізнавання суб'єктів за клавіатурним почерком за допомогою використання додаткових ознак, що характеризують динаміку набору тексту на клавіатурі, а саме сили тиску на клавіші.

# Дослідження ефективності ідентифікації особистості за клавіатурним почерком з урахуванням сили тиску на клавіші

**Метою роботи** є підвищення інформаційної безпеки комп'ютерних мереж на основі аналізу клавіатурного почерку.

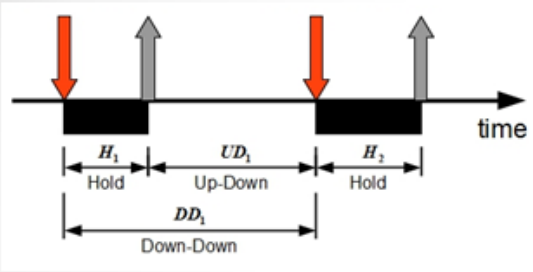
Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1) провести аналітичний огляд сучасних рішень і алгоритмів аутентифікації користувачів за клавіатурним почерком;

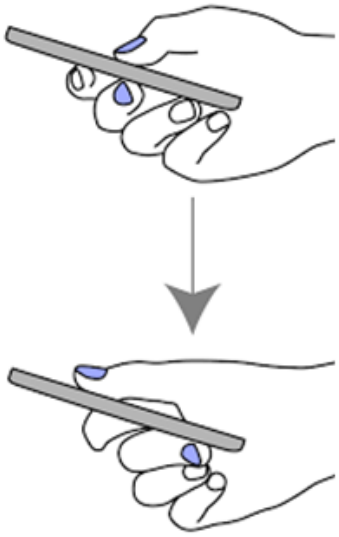
2) провести пошук відкритих датасетів клавіатурного почерку, в яких присутні дані про динаміку зміни тиску на клавіші в процесі набору текстів, та обрати один з них для подальших досліджень;

3) на основі обраного датасету провести експериментальні дослідження впливу на точність ідентифікації за клавіатурним почерком ознак динаміки зміни тиску сили на клавіші та їх комбінацій з часовими параметрами клавіатурного почерку.

# Інформативні характеристики клавіатурного та сенсорного почерків




1. Тривалість утримання клавіші (Hold-Time) на фізичній клавіатурі.
2. Тривалість паузи між відпусканням першої клавіші та натисканням другої клавіші (Up-Down-Time) на фізичній клавіатурі.
3. Час між натисканнями першої клавіші та другої клавіш (Down-Down-Time) на фізичній клавіатурі.



1. Тривалість утримання клавіші (Hold-Time) на віртуальній клавіатурі.
2. Тривалість паузи між відпусканням першої клавіші та натисканням другої клавіші (Up-Down-Time) на віртуальній клавіатурі.
3. Час між натисканнями першої клавіші та другої клавіш (Down-Down-Time) на віртуальній клавіатурі.
4. ***Тиск на екран в момент торкання пальцями екрану.***
5. ***Розмір «плями від пальця» в момент торкання пальцями екрану.***
6. ***Прискорення по трьох осях координат в момент торкання пальцями екрану.***
7. ***Загальна відстань - сума відстаней (в пікселях) між двома послідовними кнопками на віртуальній клавіатурі.***
8. ***Загальний час вводу парольної фрази.***

# Датасети параметрів клавіатурного почерку, що знаходяться у вільному доступі

1. DSL Strong Password DataSet (Dependable Systems Laboratory, Carnegie Mellon University, USA)
http://www.cs.cmu.edu/~keystroke/
2. Keystroke100 Dataset (University of Science Malaysia, Malaysia)
http://personal.ie.cuhk.edu.hk/~ccloy/downloads_keystroke100.html
3. GREYC-KeyStroke Dataset (GREYC Laboratory, University of Caen, France)
https://www.labri.fr/perso/rgiot/ressources/GREYC-KeystrokeDataset.html
4. ATVS-Keystroke DB (Universidad Autónoma de Madrid, Spain)
http://atvs.ii.uam.es/atvs/keystroke_db.html
5. LSIA Keystroke Dynamics keypress latency dataset (Laboratorio de Sistemas de Información Avanzados, Universidad de Buenos Aires, Argentina)
http://lsia.fi.uba.ar/pub/papers/kd-dataset/
6. IIITBh-keystrokes Database (International Institute of Information Technology Bhubaneswar, India)
https://github.com/aroonav/IIITBh-keystroke
7. 136 Million Keystrokes Database (Aalto University, Finland, University of Cambridge, UK)
https://userinterfaces.aalto.fi/136Mkeystrokes/
8. Queen Mary University Keystroke benchmark dataset (London, UK)
https://personal.ie.cuhk.edu.hk/~ccloy/downloads_keystroke100.html#:~:text=Keystroke100%20Dataset&text=Keystroke100%20benchmark%20dataset%20is%20a,password%20%22try4%2Dmbs%22.

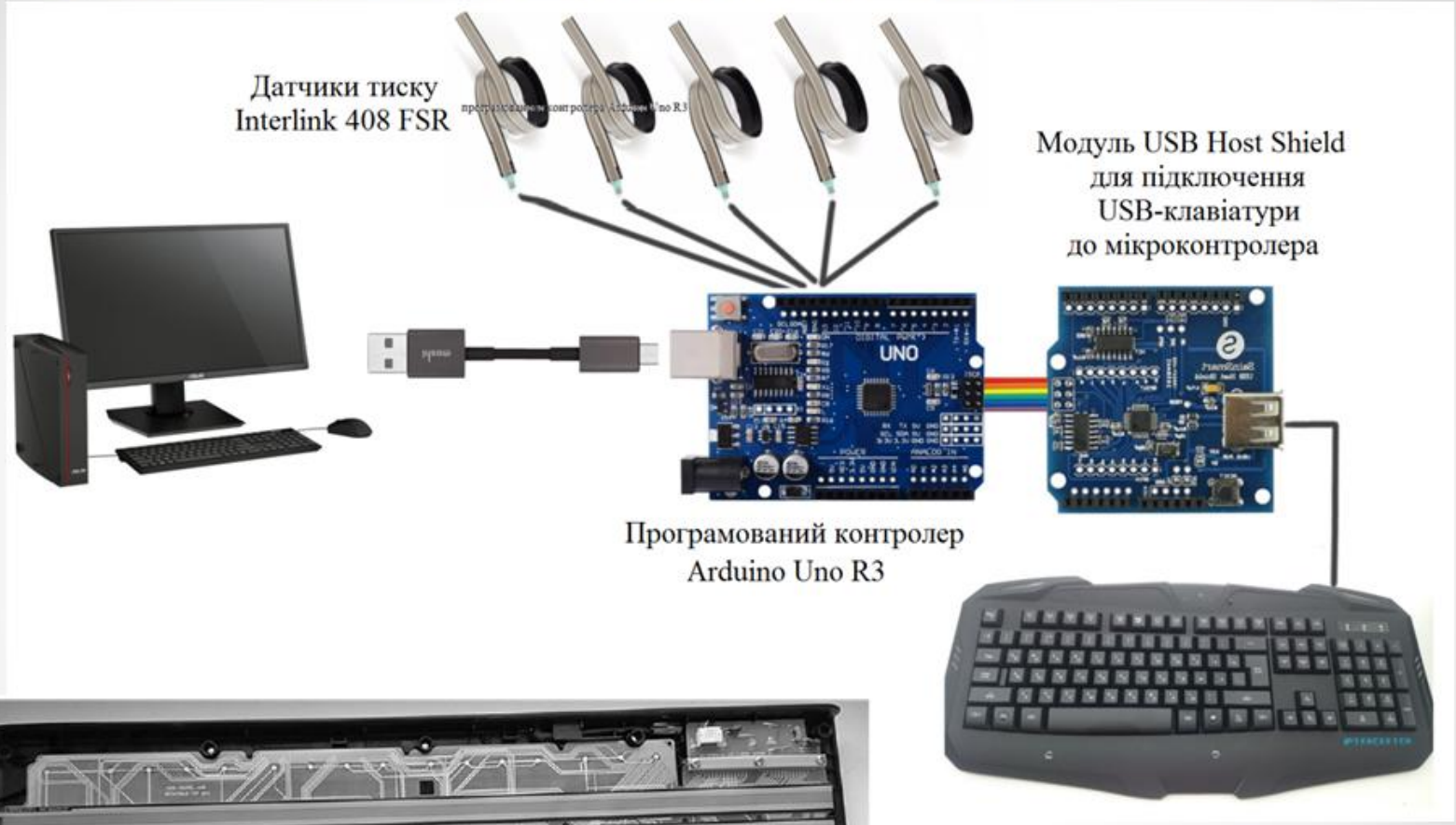
# Queen Mary University Keystroke benchmark dataset

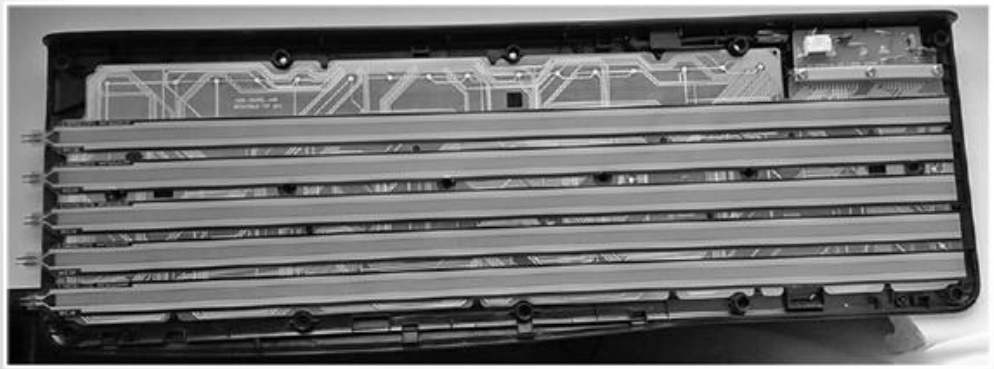
Датасет «Queen Mary University Keystroke benchmark dataset» було опубліковано у 2017 році. Датасет складається з двох датасетів.

Перший датасет містить параметри тиску користувачем на клавіші в процесі вводу паролю «.tiy4-mbs». Кількість користувачів, що брали участь в експерименті – 30 користувачів. Кількість вводів паролю – від 487 (користувач 24) до 907 (користувач 3) раз. Дані представляють файл Excel format з 11 стовпчиків. Поле «user» це ідентифікатор користувача. Останні 10 стовпчиків – параметри тиску на клавіші в процесі вводу паролю – p_k1, p_k2, p_k3, p_k4, p_k5, p_k6, p_k7, p_k8, p_k9, p_k10 (десята клавіша – enter).

Другий датасет містить часові параметри вводу паролю «.tiy4-mbsz», який набирали ті ж самі 30 користувачів. Кількість користувачів, що брали участь в експерименті – 30 користувачів. Кількість вводів паролю – 400 раз. Дані представляють файл Excel format з 32 стовпчиками. Поле «user» це ідентифікатор користувача. Останні Останні 28 стовпчик – часові параметри (в одиницях системного часу) вводу парольної фрази: H_k1, DD_k1k2, UD_k1k2, H_k2, DD_k2k3, UD_k2k3, H_k3, DD_k3k4, UD_k3k4, H_k4, DD_k4k5, UD_k4k5, H_k5, DD_k5k6, UD_k5k6, H_k6, DD_k6k7, UD_k6k7, H_k7, DD_k7k8, UD_k7k8, H_k8, DD_k8k9, UD_k8k9, H_k9, DD_k9k10, UD_k9k10, H_k10. Тут «H.kA» – час натискання клавіші A, «DD_kAkB» – час між натисканням клавіш A та B, «UD_kAkB» – час між відпусканням клавіші A та натисканням клавіші B.

# Queen Mary University Keystroke benchmark dataset

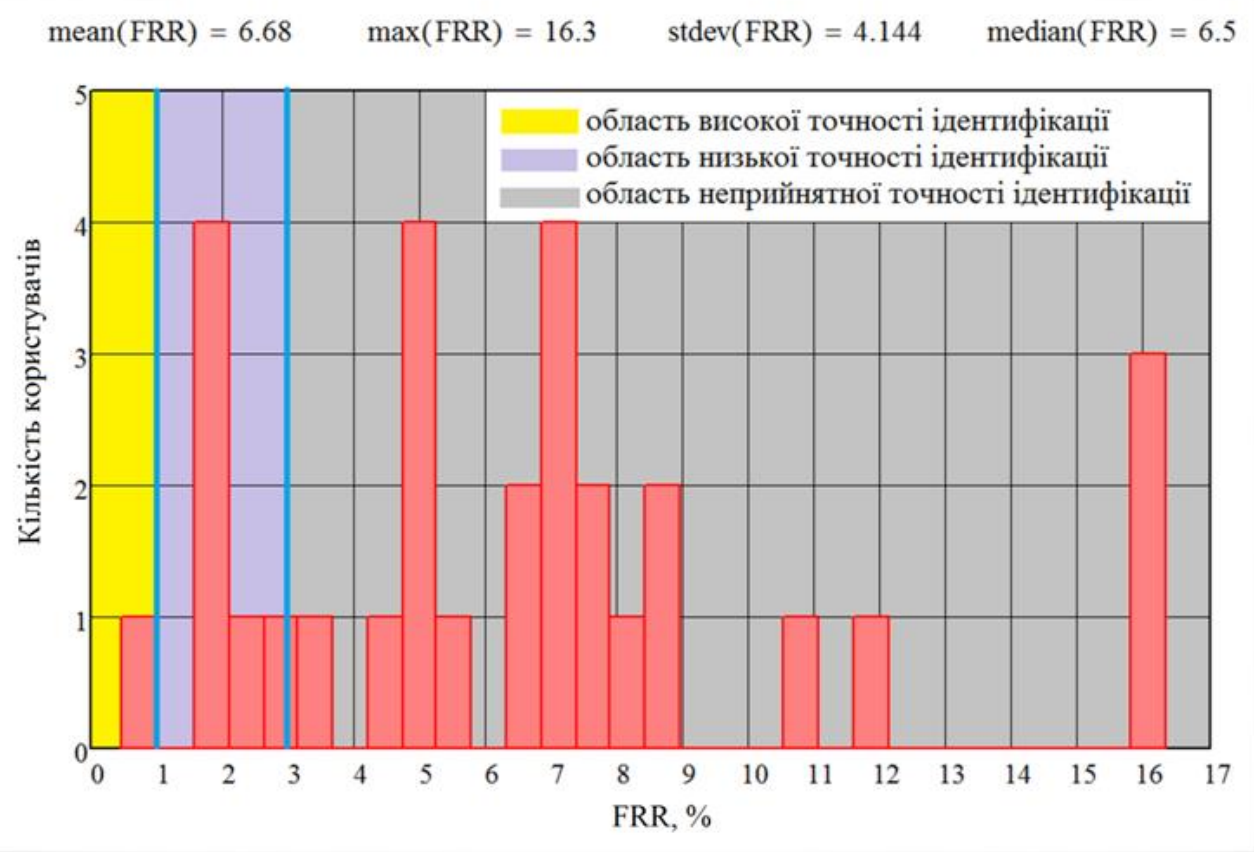


# Результати проведених досліджень

Інтегральна помилка першого роду FRR становить:
*FRR*=1-*Recall*=1-0.933=6.7%

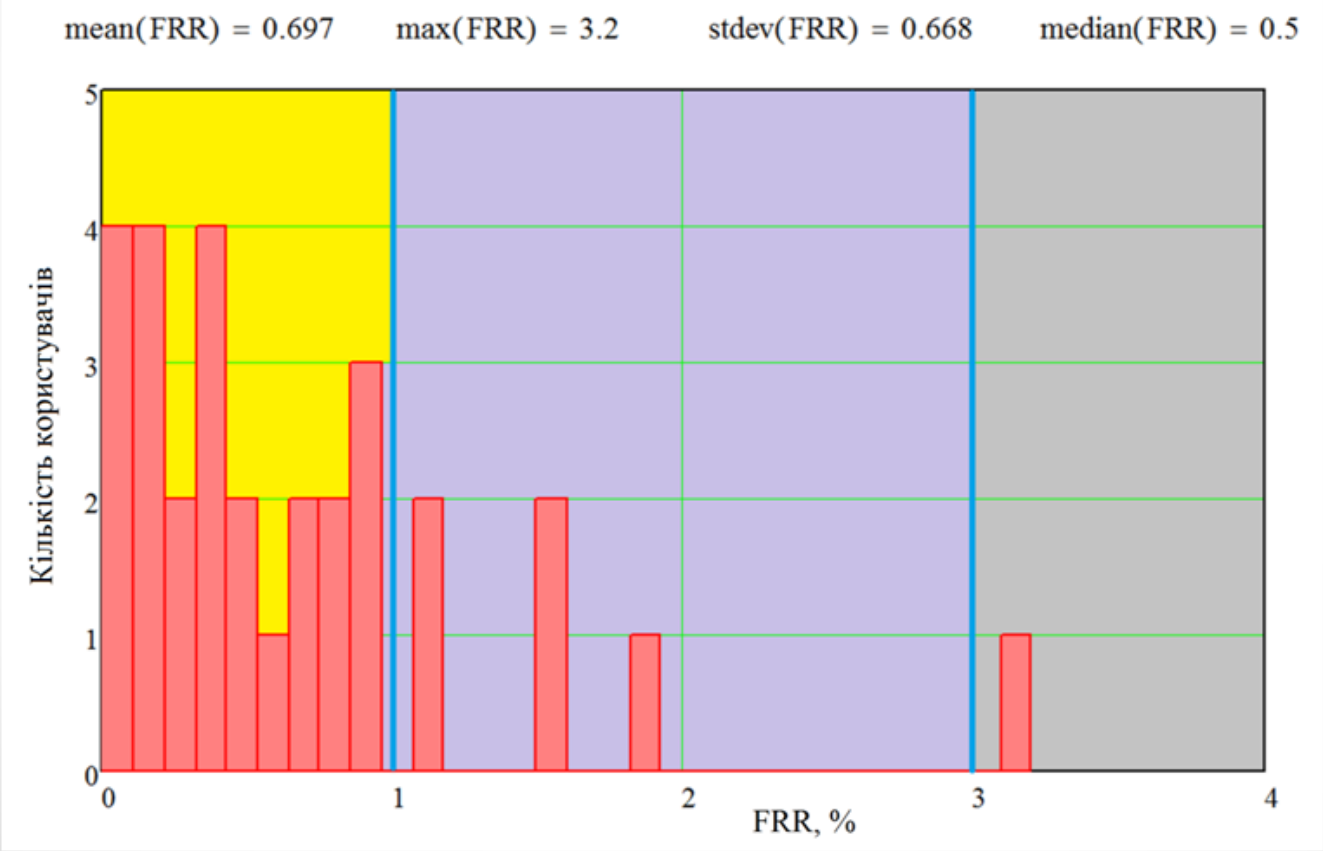
Інтегральна помилка другого роду FAR становить:
*FAR*=1-*Specificity*=1-0.998=0.2%.



# Результати проведених досліджень

Інтегральна помилка першого роду FRR становить:
*FRR*=1-*Recall*=1-0.993=0.7%

Інтегральна помилка другого роду FAR становить:
*FAR*=1-*Specificity*=1-1=0%.



# Результати проведених досліджень

Для експерименту було обрано 8 користувачів:

user26 (FRR=3.2 %, FAR=0.1 %),
user12 (FRR=1.6 %, FAR=0.1 %),
user22 (FRR=0 %, FAR=0 %),
user2 (FRR=0.5 %, FAR=0 %),
user29 (FRR=1.8 %, FAR=0.1 %),
user23 (FRR=1.6 %, FAR=0 %),
user28 (FRR=0 %, FAR=0 %),
user16 (FRR=0.5 %, FAR=0 %).

| FRR / FAR, % | | | | | | | |
|---|---|---|---|---|---|---|---|
| | user12 | user16 | user22 | user23 | user26 | user28 | user29 |
| user2 | 0.0/0.0 | 0.0/0.2 | 0.0/0.0 | 0.3/0.0 | 0.4/0.0 | 0.4/0.0 | 0.3/0.0 |
| user12 | | 0.0/0.0 | 0.0/0.3 | 0.4/0.0 | 0.0/0.0 | 0.0/0.0 | 0.0/0.0 |
| user16 | | | 0.2/0.2 | 0.2/0.0 | 0.3/0.0 | 0.0/0.0 | 0.0/0.0 |
| user22 | | | | 0.0/0.0 | 0.0/0.0 | 0.0/0.0 | 0.0/0.0 |
| user23 | | | | | 0.4/0.0 | 0.0/0.4 | 0.2/0.0 |
| user26 | | | | | | 0.0/0.4 | 0.0/0.0 |
| user28 | | | | | | | 0.4/0.0 |

# Результати проведених досліджень

| Комбінація ознак | FRR, % | FAR, % | max(FRR) | 3-й квартиль(FRR) |
|---|---|---|---|---|
| *Pressure* | 0.0 | 0.0 | 1.4 | 0.3 |
| *Pressure+ HoldTime* | 0.0 | 0.0 | 2.5 | 0.6 |
| *Pressure+ DownDownTime* | 0.0 | 0.0 | 2.2 | 0.3 |
| *Pressure+ UpDownTime* | 0.0 | 0.0 | 2.2 | 0.3 |
| *Pressure+ HoldTime+ DownDownTime* | 0.0 | 0.0 | 2.2 | 0.3 |
| *Pressure+ HoldTime+ UpDownTime* | 0.0 | 0.0 | 2.2 | 0.3 |
| *Pressure+ DownDownTime+ UpDownTime* | 0.0 | 0.0 | 2.2 | 0.3 |
| *Pressure+ HoldTime+ DownDownTime+ UpDownTime* | 0.0 | 0.0 | 2.8 | 0.3 |

# Висновки

1. Виконано огляд основних методів біометричної аутентифікації. Використання клавіатурного почерку має потенціал для застосування в комп'ютерних інформаційних системах як додаткова міра, що підвищує загальний рівень безпеки при аутентифікації. Відсутність необхідності впровадження додаткового устаткування, а також можливість тривалого збору статистики під час усього сеансу роботи користувача з клавіатурою (приховане спостереження) роблять цей підхід перспективним для практичної реалізації.

2. Проведено порівняльний аналіз сучасних систем та перспективних технологій аутентифікації користувачів комп'ютерних систем за клавіатурним почерком. Як зазначають більшість дослідників, точність аутентифікації користувачів за сенсорним почерком визначається силою тиску на екран та розміром плями від пальця. Тому актуальною є задача дослідження ідентифікаційного потенціалу клавіатурного почерку з урахуванням сили тиску на клавіші.

3. Для задач мультикласової класифікації ознаки тиску на клавіші є набагато більш інформативними, ніж часові параметри натискань на клавіші. За умови великої навчальної вибірки точність ідентифікації зловмисника може становити 100 %, а точність ідентифікації зареєстрованих користувачів – менше 1 %.

4. У випадку двокласової класифікації на основі ознак тиску на клавіші можна будувати основну систему контролю та управління доступом, бо значення помилок першого та другого родів менше 0.5 відсотка.

# Висновки

5. Ознаки тиску на клавіші є більш зачумленими, ніж часові ознаки клавіатурного почерку. Отже, актуальною є задача пошуку та фільтрації шумових даних, отриманих з датчиків тиску.

6. Комбінація ознак тиску з будь-якими часовими ознаками клавіатурного почерку також призводить до погіршення точності ідентифікації. Отже, рекомендувати використовувати ознаки тиску на клавіші в мультимодальних біометричних системах неможна. Виключення становлять випадки, коли усі модальності використовуються окремо в залежності від сценарію роботи системи (наприклад, вхід в систему за паролем та одночасно моніторинг динаміки вводу паролю на клавіатурі, а далі прихований моніторинг за користувачем в процесі роботи на основі ознак тиску на клавіші).

# Висновки

7. Враховуючи високу точність ідентифікації, ознаки тиску на клавіші в процесі роботи за клавіатурою можуть бути використані в системах виявлення потенційних внутрішніх порушників інформаційної безпеки – чим вища точність, тим точніше можна визначити діапазони зміни дослідних ознак клавіатурного почерку для кожного користувача.

Як відомо, часто внутрішніми інсайдерами є звичайні співробітники, які вимушені з тієї чи іншої причини чинити протизаконні дії. Такі інсайдери часто характеризуються високим рівнем тривожності, схильні до інтрапунітивних реакцій (самообвинувачування, похмурість, злість, незадоволення, напруженість, сердитість), чим відрізняються від справжніх злочинців.

Для такої категорії порушників можливе проактивне (на ранніх етапах) виявлення потенційних, схильних до протиправних дій осіб шляхом контролю їхньої діяльності та оцінки психоемоційного стану.

Одним з технічних індикаторів, які можуть вказувати на наявність потенційної інсайдерської загрози, може виступати клавіатурний почерк у сукупності таких показників, як сила тиску на клавіші, динаміка введення, системні друкарські помилки та використання певних літер, символів та «гарячих» клавіш. Сукупність певних значень кожного з цих показників утворює досить індивідуальну картину, що відповідає конкретній людині у певному психоемоційному стані.

| Номер документу | Позначення | Найменування | Прим. |
|---|---|---|---|
| | | *Текстові документи* | |
| 1 | | Пояснювальна записка | 81 с. |
| | | *Графічний матеріал* | |
| 2-3 | | Дослідження ефективності | 2xA4 ел.ф. |
| | | ідентифікації особистості | |
| | | за клавіатурним почерком | |
| | | з урахуванням сили тиску на клавіші | |
| 4 | | Інформативні характеристики | А4 ел.ф. |
| | | клавіатурного та сенсорного почерків | |
| 5 | | Датасети параметрів клавіатурного | А4 ел.ф. |
| | | почерку, що знаходяться | |
| | | у вільному доступі | |
| 6-7 | | Queen Mary University Keystroke | 2xA4 ел.ф. |
| | | benchmark dataset | |
| 8-11 | | Результати проведених досліджень | 4х А4 ел.ф. |
| 12-14 | | Висновки | 3х А4 ел.ф. |

| Из | Лист | № докум. | Підпис | Дата | | | | |
|---|---|---|---|---|---|---|---|---|
| Розроб. | | Зеленський | | | *Дослідження ефективності ідентифікації особи за клавіатурним почерком з урахуванням сили тиску на клавіші* | Літера | Лист | Листів |
| Перев. | | Горелов | | | | Д | | |
| | | | | | | ХНУРЕ Кафедра КРіСТЗІ | | |
| Н.контр. | | Милютченко | | | Відомість кваліфікаційної роботи магістра | | | |
| Затв. | | Антіпов | | | | | | |