Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інформаційних радіотехнологій і технічного захисту інформації*

Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти *другий (магістерський)*

Дослідження інформативних ознак сенсорного почерку власників мобільних пристроїв

Виконав:
студент *2* курсу, групи *СТЗІАм-21-1*
Кураксін Данило Олександрович

Спеціальність *125 «Кібербезпека»*
Тип програми *освітньо-професійна*
Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

Керівник *доц. Горелов Д.Ю.*

Допускається до захисту
Зав. кафедри _____ *проф. Антіпов І.Є.*
(підпис)

2022 р.

Харківський національний університет радіоелектроніки

Факультет *Інформаційних радіотехнологій і технічного захисту інформації*
Кафедра *Комп'ютерної інженерії та систем технічного захисту інформації*
Рівень вищої освіти *другий (магістерський)*
Спеціальність *125 «Кібербезпека»*
Тип програми *освітньо-професійна*
Освітня програма *«Системи технічного захисту інформації, автоматизація її обробки»*

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«___» _____ 20 _____ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Кураксіну Данилу Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження інформативних ознак сенсорного почерку власників мобільних пристроїв*

затверджена наказом по університету від « 04 » 11 2022 р. № 1446 Ст

2. Термін подання студентом роботи до екзаменаційної комісії *1 грудня 2022 р.*

3. Вихідні дані до роботи *Дослідити інформативність параметрів сенсорного почерку для задач біометричної ідентифікації власників мобільних пристроїв. Для досягнення поставленої мети необхідно розв'язати наступні задачі: 1) провести аналіз існуючих методів біометричної аутентифікації власників мобільних пристроїв, визначити особливості їх реалізації та інтеграції в мобільних операційних системах; 2) провести пошук відкритих баз даних параметрів сенсорного почерку та обрати декілька з них для подальших досліджень; 3) експериментально дослідити точність ідентифікації, як функцію використаних інформативних ознак сенсорного почерку.*

4. Перелік питань, що потрібно опрацювати в роботі
1. Аналіз безпеки даних користувача В Apple IOS та Google Android
2. Аналіз можливості, доцільності та ефективності використання сенсорного почерку для підвищення надійності захисту мобільних пристроїв
3. Експериментальні дослідження інформативних ознак сенсорного почерку почерку та порівняння отриманих результатів з системами аутентифікації за класичним клавіатурним почерком
4. Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

1. Дослідження інформативних ознак сенсорного почерку власників мобільних пристроїв. А4. Ел.ф.

2. Інформативні характеристики клавіатурного та сенсорного почерків. А4. Ел.ф.

3. The Mobikey Keystroke Dynamics Password Database. А4. Ел.ф.

4. Схема експерименту у Orange. А4. Ел.ф.

5. Результати проведених досліджень. А4. Ел.ф.

6. Висновки. А4. Ел.ф.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз сучасних методів та засобів біометричної ідентифікації власників мобільних пристроїв*	*01.09.22 – 20.09.22*	
2	*Огляд сучасних рішень та перспективних технологій в області інтеграції біометричного захисту інформації та мобільних операційних систем*	*21.09.22 – 10.10.22*	
3	*Експериментальні дослідження інформативних ознак сенсорного почерку та порівняння отриманих результатів з системами аутентифікації за клавіатурним почерком*	*11.10.22 – 30.11.22*	
4	*Перевірка роботи на антиплагіат*	*01.12.22 – 05.12.22*	
5	*Представлення кваліфікаційної роботи на кафедрі*	*10.12.2022*	

Дата видачі завдання *01 вересня 2022 р.*

Студент _____ *Кураксін Д.О.*
(підпис) (прізвище, ініціали)

Керівник роботи _____ *Горелов Д.Ю.*
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 100 с., 34 рис., 3 табл., 21 джерело, 1 додаток.

БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ, МОБІЛЬНИЙ ПРИСТРІЙ, СЕНСОРНИЙ ПОЧЕРК, МЕТОД ВИПАДКОВОГО ЛІСУ.

В роботі проаналізовано інформативні ознаки сенсорного почерку. Можна виділити три основних класи: часові параметри, параметри взаємодії з екраном (тиск та розмір «плями» від пальця) та психофізіологічні параметри, де до тиску та розміру «плями» додаються показання акселерометру та динаміка руху кінчика пальця по екрану.

Інтегральна точність мультикласової класифікації методом Random forest користувачів з датасету «The Mobikey Keystroke Dynamics Password Database» за часовими та психофізіологічними параметрами складає 94.7 %.

Мінімальна точність двійкової класифікації становить не менше 90 %. Рівень FAR становить 1.58 %. Рівень FRR становить 1.36 %.

ABSTRACT

Master thesis: 99 pages, 34 figures, 3 tables, 21 sources, 1 annex.

BIOMETRIC IDENTIFICATION, MOBILE KEYSTROKE DYNAMICS, MOBILE AUTHENTICATION, RANDOM FOREST.

In the study the informative features of mobile keystroke dynamics are analyzed. There are three main classes: time parameters, parameters of interaction with touch-screen (pressure and finger-area) and psycho-physiological parameters, where the pressure and finger-area are added to the 3D acceleration parameters and finger movement dynamics on touch screen.

The Multi-Class Classification accuracy by the Random forest method of users from the "The Mobikey Keystroke Dynamics Password Database" by time and psycho-physiological parameters is 94.7%.

The Binary Classification accuracy is not less than 90%. FAR is 1.58 %. FRR is 1.36 %.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

EER (Equal Error Rate) – коефіцієнт рівної імовірності помилок 1 і 2-го роду;

FAR (False Acceptance Rate) – помилка другого роду – випадок надання системою доступу неавторизованому користувачеві;

FRR (False Rejection Rate) – помилка першого роду – доступ заборонений користувачеві, зареєстрованому в системі;

ОС – операційна система;

ПЗ – програмне забезпечення.

ВСТУП

Безперервний розвиток комп'ютерних технологій вже де-факто призвів до майже повної залежності цивілізації від величезних обсягів даних і засобів їх обробки. Можливості програмного та апаратного забезпечення, що постійно вдосконалюються, дозволили подолати дві перешкоди на шляху до інформаційного суспільства, а саме: бар'єри технологічної / фінансової доступності та простоти / надійності використання.

Перша перешкода полягала в недостатній поширеності або повній відсутності інфраструктури для обробки даних, що призводило до високої вартості як обчислювальних пристроїв, так і супутнього програмного забезпечення. Ці обставини спочатку забезпечували відносну безпеку даних, оскільки користувачів було небагато і більшість із них належала вузьким професійним групам з високим рівнем технічної освіти. Зростання виробництва доступного за ціною апаратного забезпечення та збільшення кількості каналів зв'язку призвели до появи електронних дощок оголошень [1] з великими користувальницькими спільнотами, що унеможливило персональне відстеження дій кожного користувача та оперативну реакцію на них. У свою чергу, це призвело до перших масштабних епідемій шкідливого програмного забезпечення у вигляді примітивних вірусів і черв'яків [2]. На тому етапі розвитку загроза була обмежена другою перешкодою, що виражалася у вигляді високої складності комп'ютерних додатків, що вимагають від користувачів відповідної кваліфікації для ефективної роботи з ними, оскільки неправильне застосування могло спричинити втрату даних.

Поширення персональних комп'ютерів та розширення доступу до мережі Інтернет призвело до зростання кількості кібер-злочинів. Спочатку ці кібер-злочини були фінансово ефективні тільки при атаках на великі організації, в основному фінансові та урядові в силу винятковості можливостей з ефективної обробки великих масивів даних користувача в порівнянні з приватними

організаціями меншого масштабу. Першою шкідливою активністю, навмисне спрямованою проти рядових користувачів, були спам розсилки електронних листів. З розвитком Інтернет-банкінгу та Інтернет-торгівлі поширення набули більш небезпечні злочини, такі як крадіжка особистих даних. Це спричинило відповідь у вигляді державної кібер-поліції та приватних охоронних компаній з кібер-безпеки, які виросли з ранніх постачальників антивірусного програмного забезпечення.

На даний момент обсяги даних та кількість пристроїв їх обробки постійно зростають [3]. Пристрої з доступом до глобальної мережі перевищують за кількістю сукупне земне населення. Подібний феномен наявності величезної кількості стандартизованих вузлів зв'язку, який зазвичай називають Інтернетом речей, вважається третьою перешкодою на шляху до наступного покоління інформаційного суспільства. Основна проблема в третій перешкоді полягає в уразливості більшості пристроїв, не обладнаних через простоту і дешевизну виготовлення будь-якими значущими засобами аутентифікації вхідних з'єднань. Типи пристроїв варіюються від цифрових модулів з мережевим протоколом MQTT для передавання показань примітивних датчиків (наприклад, побутових Wi-Fi термометрів) до комп'ютерів (наприклад, Raspberry Pi) для більш складної споживчої електроніки – холодильники, пральні машини або телевізори. У силу стандартизації як машинної архітектури, і протоколів зв'язку кожен вузол може бути точкою проникнення шкідливої кибер-активності. Наприклад, відомим фактом є те, що розумні телевізори вже здатні виконувати неавторизований аудіозапис навіть без попередження користувачів [4]. Така ж активність була виявлена і в поведінці смартфонів, що виявляє акустичний патерн включення телевізора і виконує збір статистики по телеканалах. Подібний тип технології відомий як перехресне міжприладове стеження через акустичні маяки [5]. Цей механізм активно розвивається лідером відповідної індустрії SilverPush [6] та його конкурентами як Drawbridge, Flurry та Adobe.

Таким чином, сучасні технології породжують широкий діапазон різних загроз користувачам даних з безліччю векторів атаки. Отже, бажано

використовувати засоби кібербезпеки, що враховують характеристики пристроїв, сервісів і поведінки користувача.

Найпоширеніший метод ідентифікації для смартфонів на сьогоднішній день – це використання PIN-коду (персонального ідентифікаційного номера), який має обмеження, як з погляду кінцевого користувача, і з технологічного погляду. Отже, існує потреба у ненав'язливій та більш надійній методиці перевірки користувачів. Один із потенційних підходів − використання біометричних характеристик, які засновані не на знаннях користувача, а на самому користувачі. Для забезпечення додаткового рівня безпеки можна запропонувати використовувати дослідження динаміки натискання клавіш під час введення пароля або PIN-коду, що дозволяє аналізувати ритм набору тексту користувачем.

Метою цієї роботи є підвищення інформаційної безпеки мобільних пристроїв на основі аналізу сенсорного почерку.

Для досягнення поставленої мети необхідно розв’язати наступні задачі:

1) провести огляд основних методів біометричної аутентифікації, що використовуються або є перспективними до використання в мобільних пристроях.;

2) провести пошук відкритих датасетів параметрів клавіатурного почерку та обрати декілька з них для подальших досліджень;

3) на основі обраних датасетів дослідити інформативність параметрів сенсорного почерку;

4) на основі проведених досліджень запропонувати сценарії використання сенсорного почерку в якості біометричної технології захисту мобільних пристроїв.

1 АНАЛІЗ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧА В APPLE IOS ТА GOOGLE ANDROID

На даний момент світовий ринок операційних систем для мобільних пристроїв з великим відривом очолюють двоє лідерів: Google Android та Apple iOS. В процесі еволюції обидві платформи сформували свої підходи до організації безпеки даних користувача. Кожна має свої переваги та недоліки. Закрите середовище розробки iOS та оперативне реагування на вразливість створюють довіру до Apple. Але досі Apple повністю не захищає користувачів від злому та компрометації даних різними каналами.

Google за останні кілька років значно підвищила безпеку ОС Android за рахунок використання криптографічної функціональності. Але фахівці з кіберкриміналістики все ще можуть обійти захисні механізми Android та отримати доступ до даних.

Розглянемо детальніше кожну з операційних систем.

1.1 Загальні принципи безпеки та конфіденційні дані мобільних пристроїв

Практично всі дані користувача мобільних пристроїв конфіденційні: електронна пошта, повідомлення, біометрична інформація, фото- та відеоконтент, документи, розташування, паролі, історія роботи в браузері та багато іншого. Які саме дані є найбільш конфіденційними і які техніки захисту використовуються на даний момент?

Можна виділити кілька ключових технік контролю доступу до даних.

1. Безпека та ізоляція ПЗ. Сучасні операційні системи мобільних пристроїв строго розмежовують доступ додатків та доступ користувача. Наприклад, підозрілі програми не можуть отримати доступ до даних, на які немає відповідних прав. Для запуску довільного коду на пристрої необхідно зробити

обхід цього обмеження: "джейлбрейк" для iOS або отримання рут-доступу для Android.

2. Доступ за допомогою кодів та біометрії. Контроль доступу до інтерфейсу ОС найчастіше здійснюється через пароль, як правило, цифровий. Можна активувати патерн (графічний ключ – послідовність) на екрані блокування. Все частіше застосовується біометричний доступ: через розпізнавання обличчя або відбиток пальця.

3. Шифрування файлів та дисків. У разі обходу зловмисником програмних методів захисту він зіткнеться із зашифрованими даними. Це може бути як окремі файли, і розділи диска. Шифрування даних, як правило, організоване асиметрично: в обладнання вбудована одна частина ключа, а друга генерується на основі вибраного паролем користувача.

4. Безпечне апаратне забезпечення пристроїв. Останнім часом виробники впроваджують співпроцесори безпеки та їх віртуалізовані аналоги. Це захищає від програмних атак і атак на обладнання пристрою, посилюючи механізми шифрування конфіденційних даних, зокрема біометричних шаблонів.

5. Безпечне резервне копіювання та робота з хмарними системами. Нещодавно постачальники послуг почали надавати безпечну модель хмарного зберігання резервних копій даних пристрою. Сучасна система зашифрованого резервного копіювання унеможливлює прямий доступ хмарного провайдера, зловмисників або правоохоронних органів до даних користувача.

Модель загроз.

Мобільні пристрої цілком добре захищені від традиційних дистанційних атак. Однак, прямий тривалий фізичний доступ до пристрою (або його компонентів) значно полегшує роботу зловмисника або фахівця з форензики, що підвищує ризик вилучення даних.

Прямий доступ до пристрою може бути отриманий незаконно, шляхом крадіжки пристрою, або законно шляхом виконання законодавчих приписів, які можуть включати видачу паролів доступу. Це дуже тонкий момент, тому що органи влади можуть скористатися своїм службовим становищем або

невігласством користувача, що може призвести до повної компрометації пристрою. Не можна виключати і те, що зловмисник здійснить атаку методами соціальної інженерії, видаючи себе, наприклад, за того ж представника правоохоронних органів, або підробить судові документи, отримавши в результаті доступ до мобільного пристрою.

Фізичний доступ до пристрою із застосуванням інструментів кіберкриміналістики дозволяє не тільки витягти дані, але й отримати токени доступу до безпечного хмарного сховища, що знаходяться в пам'яті. Дані з пристрою та хмарного сховища, як окремо, так і разом, можуть містити різні категорії особистої інформації, створюючи серйозну загрозу порушення конфіденційності користувача.

Конфіденційні дані мобільних пристроїв.

Фахівці з кіберкриміналістики аналізують найбільш пріоритетні категорії конфіденційних даних для упіймання злочинців. Ці дані ми можемо взяти за основу:

1) IMEI, MEID / ESN та інші дані абонента мережі;

2) контакти, адресна книга, календар, нотатки тощо;

3) журнали вхідних та вихідних дзвінків;

4) SMS, MMS, миттєві повідомлення;

5) файли: аудіо, відео, документи;

6) електронна пошта;

7) активність браузера: історія, закладки;

8) GPS та геолокаційні дані;

9) соціальні мережі: облікові записи, контент;

10) SIM / UICC, провайдер, IMSI, MSISDN і т. д.

Необхідно зазначити, що цей список даних не відображає обов'язкової загрози конфіденційності користувача. Деякі дані можуть мати короткий термін актуальності, а деякі несуть інформацію про його родичів, друзів, колег. В еру повсюдного Інтернету витік навіть деяких даних зі списку може призвести до порушення конфіденційності цілої групи користувачів.

1.2 Apple iOS

У 2020 році корпорація Apple заявила, що кількість активних пристроїв по всьому світу становить понад 1 400 000 000. 48% смартфонів у США та західних країнах – iPhone під керуванням iOS. Поступове зростання кількості пристроїв Apple на світовому ринку приваблює не лише зловмисників, а й фахівців з пошуку вразливостей (багхантерів), яким компанія пропонує програми винагороди до 2 000 000 доларів США.

Розглянемо історію функцій безпеки iOS та поточні технічні аспекти захисту інформації користувачів Apple.

Огляд еволюції захисту Apple iOS.

1. Шифрування даних. Першу версію шифрування даних флеш-пам'яті при відключенні живлення було реалізовано в iOS 3 (2009 рік). Ключ шифрування не залежав від коду доступу користувача і був не потрібний для дешифрування. В iOS 8 (2014) Apple значно збільшила кількість зашифрованих даних на пристрої з використанням ключа, який генерувався на основі пароля користувача. З функцією Data Protection видалення даних відбувається разом із ключами без можливості відновлення. Однак у деяких випадках видалення даних користувачем відбувається за допомогою їх перенесення у відповідний розділ бази даних SQL на пристрої, що зберігає можливість подальшого відновлення.

2. Від кодів до біометрії. TouchID з'явився в 2013 році, а в iOS 9 (2015) було збільшено стандартну довжину цифрового пароля до шести символів. До цього паролі, що складалися із чотирьох символів, могли бути обійдені програмними експлойтами. Ємнісний датчик відбитків пальців та подальший FaceID (2017), на думку Apple, підвищили та спростили безпеку, оскільки частота, з якою обробляються біометричні дані, обмежена SEP (Secure Enclave Processor). Ефективність даних нововведень ставилася під сумнів у наукових колах.

3. SEP-архітектура та посилення апаратних компонентів пристроїв. З еволюцією iOS змінювалися апаратні компоненти пристроїв Apple. До

введення чіпа A4 (власна однокристальна розробка SoC) Apple використовувала компоненти від Samsung, LG та інших виробників (2007-2009 роки). Безпека будувалася на шифруванні завантажувальної пам'яті NOR за допомогою апаратного ключа AES (ключ UID), який керувався прискорювачем Crypto Engine.

Архітектура SEP (Secure Enclave Processor) була вперше реалізована в чіпі A7 (iPhone 5S, 2013) і дозволила виконувати функції безпеки окремо від основного процесора, на якому працюють ОС та програми. Активуючи TouchID, SEP використовує власний UID ключ для шифрування. Особливість полягає в тому, що при генерації SEP ключа навіть виробники не знають ключ UID. Починаючи з чіпа A7 відбувається послідовне посилення безпеки та продуктивності, розширення функцій SEP. Наприклад, у чіпі A12 (2020) Apple встановила захист на режим оновлення прошивки пристрою (DFU mode), як це реалізовано в режимі відновлення (recovery mode).

4. iCloud Keychain. У 2016 році анонсований iCloud Keychain, а в iOS 11 (2017) представлений CloudKit з наступним API для сторонніх розробників. Перевага полягає тут у тому, що зберігання контейнера довільних даних у хмарі організовано особливим чином: ніхто, крім користувача зі своїм Keychain, навіть сама Apple, не може дешифрувати ці дані.

Сучасний захист даних користувача iOS.

Ключові елементи захисту сформовані взаємодіями безпосередньо з пристроєм та хмарними технологіями.

1. Аутентифікація. Фізична взаємодія з пристроєм: цифровий / літерний код або біометрична автентифікація. Шести-символьний пароль активовано за замовчуванням. Підтримується вибір довших парольних буквено-цифрових фраз. Можливе повне відключення аутентифікації, що вкрай не рекомендується Apple. Спроби перебору цифрових паролів блокуються часовими інтервалами. TouchID (ємнісний датчик відбитка пальця) та FaceID (розпізнавання обличчя камерою, чутливою до глибини) застосовуються Apple для організації вищого рівня безпеки користувачів.

2. Підписування коду програм. Цифрові підписи допомагають серйозно обмежувати код, що виконується на iOS. Це досягається за рахунок безпечного завантаження (відбувається перевірка підпису, вбудованого на низькому рівні (Boot ROM), що гарантує довгостроковий захист від ініціалізації підозрілого софту) і за рахунок підпису додатка, що є наступною комбінацією: підпис, який контролюється Apple, і сертифікати з відкритим ключем для масштабування системи. Для більш спеціалізованого запуску додатків на iOS у рамках організації необхідно придбати так звані сертифікати підпису підприємства.

3. Пісочниця та аналіз коду. Для захисту від підозрілих додатків накладаються обмеження доступу до даних і API за допомогою ізольованого середовища (пісочниці). Додаток обмежується доступом до файлової системи, простору пам'яті. У підписаному маніфесті позначається дозволений доступ до системних ресурсів та служб, наприклад, служби геолокації. Програми з App Store проходять автоматичну та ручну перевірку коду. Втім, навіть за цих строгих обмежень деякі небажані програми можуть пройти перевірку та порушити конфіденційність користувача.

4. Шифрування. На той випадок, якщо зловмиснику вдасться обійти механізми безпеки через вразливості або недоліки в устаткуванні, Apple підготувала надійну систему шифрування даних пристрою Data Protection. iOS застосовує криптографічні стандарти AES, ECDH over Curve25519 та інші схвалені Національним інститутом стандартів та технологій США (NIST). Доступ до даних прив'язаний до пристрою та контролюється користувачем. Ключ для шифрування даних формується на основі комбінації обраного користувачем пароля та UID (унікальний апаратний секретний кріптоключ). Після перезавантаження пристрою потрібно відновити ключі шифрування шляхом введення встановленого пароля, далі для розблокування ключів достатньо біометричних даних.

Обхід шифрування припиняється двома шляхами: функцією отримання ключа на основі пароля та методом обмеження введень парлю із збільшенням часових інтервалів.

Apple використовує кілька класів захисту (Class key) шифрування, які розробники вільні вибирати при створенні файлів або об'єктів даних:

1) повний захист (CP) – через 10 секунд після блокування пристрою ключі шифрування видаляються;

2) захищено поки не відкрито (PUO) – зберігається відкритий ключ у пам'яті, надсилання зашифрованих файлів при заблокованому пристрої. Включається повний захист даних (CP) після того, як файл було створено та закрито;

3) захищено до першої автентифікації користувача – першого розблокування (AFU) – при введенні першого пароля ключі шифрування розшифровуються у пам'яті та залишаються там під час блокування пристрою;

4) немає захисту (NP) — якщо вимкнений пристрій, ключі шифрування зашифровані лише апаратними ключами UID. Ці ключі постійно доступні у пам'яті, коли пристрій увімкнено.

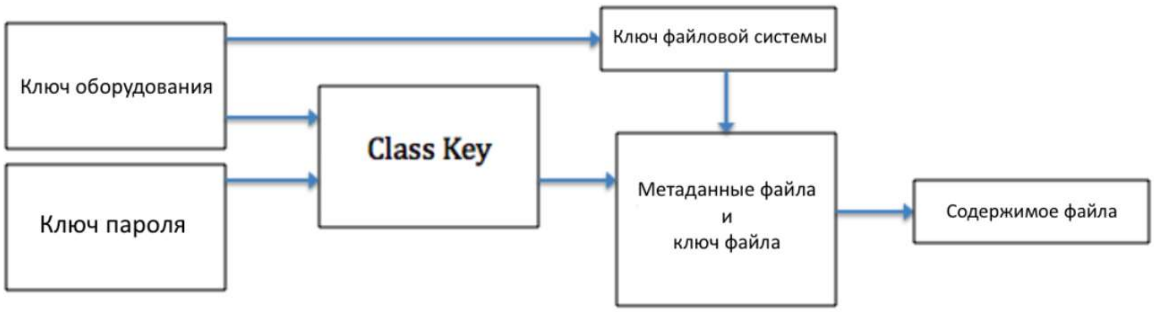


Рисунок 1.1 – Схема ієрархії ключів iOS Data Protection

5. Keychain. Це – зашифроване сховище ключів та конфіденційної інформації (логіни / паролі), яке має загальнодоступний API. Воно захищене апаратними ключами та паролем користувача. Опція Non-Migratory (NM) дозволяє дешифрувати дані лише на пристрої, де дані були зашифровані (застосовується UID).

6. Резервне копіювання. Можна виконати локально на персональному комп'ютері або в iCloud. Локальний бекап можна зашифрувати вибраним паролем, у результаті сформується структура Keybag. Ненадійний пароль матиме слабку стійкість до вибору варіантів (брутфорсу), оскільки ніяк не пов'язаний

з апаратними ключами пристрою. Тут iOS використовує 10 мільйонів ітерацій PBKDF2 підвищення стійкості до перебору. При копіюванні в Apple iCloud дані шифруються Curve25519, що дозволяє робити бекап, коли пристрій заблоковано без розкриття секретних ключів. Внаслідок того, що ключі зашифровані за допомогою iCloud Keychain, відомих Apple, виробник або зловмисник може отримати доступ до вмісту резервної копії. Тому Keychain додатково шифрує обидва типи резервної копії ключем UID для запобігання відновленню на новому пристрої.

Дані, що містяться в резервній копії iCloud: дані програм, резервні копії Apple Watch, налаштування пристрою, домашній екран та програми, iMessage, SMS та MMS, фото та відео, історія покупок у сервісах Apple, рінгтони, пароль голосової пошти.

7. iCloud та iCloud Keychain iCloud дозволяє зберігати не тільки бекапи, але й будь-які інші дані користувача, вказані для синхронізації із хмарою. Дані передаються через мережу за допомогою TLS і зберігаються в зашифрованому вигляді. Криптографічне перетворення здійснюється за допомогою 128-бітного ключа AES та ключа отриманого з пароля користувача.

iCloud Keychain дозволяє синхронізувати (з використанням асиметричного шифрування) Keychain між пристроями Apple, а у разі втрати пристрою – відновити Keychain за допомогою коду безпеки iCloud. Цей код формується з пароля користувача при включеній двофакторній аутентифікації або створюється автоматично, якщо та не включена. Застосовуючи технологію HSM (надійних апаратних модулів), Apple не має доступу до вмісту резервних копій iCloud Keychain, а при HSM-автентифікації код безпеки iCloud не передається (використовується протокол безпечного віддаленого пароля SRP). Копія зашифрованої iCloud Keychain надсилається на пристрій користувача лише після підтвердження, що кількість невдалих спроб була меншою за 10. Якщо було зафіксовано більше 10 спроб користувачеві знадобиться зареєструватися повторно для використання iCloud Keychain. Apple стверджує, що після розгортання HSM ключі підпису, необхідні для зміни програмного забезпечення,

знищуються автоматично, що обмежує корпорації доступ до даних користувачів.

8. SEP: TouchID і FaceID. Secure Enclave Processor (SEP) – співпроцесор, який використовує зашифровану пам'ять та організує роботу з автентифікації, керування ключами, шифрування та генерації випадкових чисел. Якщо ядро iOS було зламано, то SEP забезпечує шифрування за рахунок своєї автономної архітектури.

Робота аутентифікації TouchID / FaceID узгоджується за допомогою SEP.

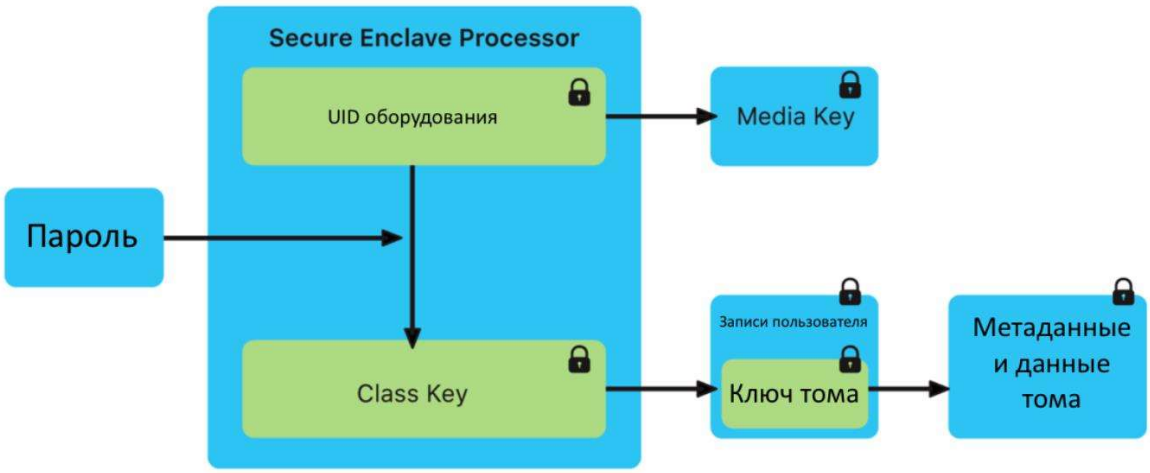


Рисунок1.2 – Схема обробки ключа Secure Enclave Processor

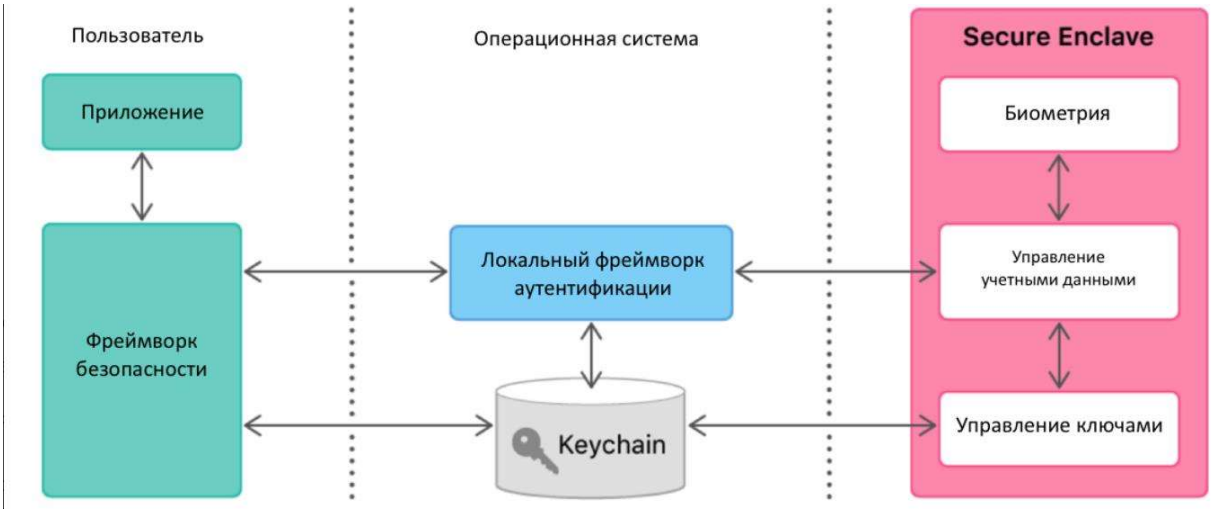


Рисунок 1.3 – Схема роботи Apple TouchID та FaceID

9. Зменшення фронту атаки. Це досягається обмеженнями шляхів введення-виведення даних для заблокованого пристрою. Для доставки експлойту

на пристрій Apple знадобиться один з цих шляхів: синхронізація даних у фоновому режимі (електронна пошта, хмарні сервіси), пуш-повідомлення, деякі мережеві повідомлення (Wi-Fi, Bluetooth, стільниковий зв'язок) і порт Lightning на пристрої.

З введенням USB Restricted операційна система iOS обмежує доступ підозрілих підключень за допомогою USB / Lightning, наприклад, інструментів форензики. iOS зупиняє роботу USB після першого підключення, якщо пристрій не був прийнятий користувачем як довірений. Відомі довірені підключення через USB / Lightning запам'ятовуються на 30 днів.

10. iMessage та FaceTime. Apple підтримує наскрізне (end-to-end) шифрування при відео- / аудіозв'язку між своїми пристроями за допомогою FaceTime. В основі лежить SRTP (безпечний транспортний протокол у режимі реального часу). iMessage застосовує схему шифрування "signcryption". Для публічних ключів використовується Apple Identity Service як довірений орган, що забезпечує справжність користувачів.

Актуальні техніки обходу захисту даних iOS.

1. Джейлбрейк та програмні експлойти. Джейлбрейк часто використовується для зняття обмежень iOS та випускається для конкретного пристрою та версії iOS. Багато інструментів форензики використовують його для доставки «корисного навантаження» у вразливий програмний компонент, як правило, через USB / Lightning. Доставка може бути здійснена через повідомлення або за допомогою спеціально підготовлених веб-сторінок. Нерідко використовується ланцюжок експлойтів. Коли контроль над ядром iOS отримано, можна отримати дані, які не були зашифровані. Наступна модифікація (патчінг) програмного ядра дозволяє запускати будь-який код у системі.

Apple дуже швидко реагує на вразливості.

Джейлбрейки checkm8 / checkra1n найбільш ефективні в 2020 році з погляду кіберкриміналістичних досліджень і дозволяють працювати з пристроями до iPhone X та будь-якої версії iOS.

Експлойти Cellebrite UFED Touch та 4PC дозволяють запускати резервне

копіювання без авторизації користувача або активувати завантажувач із кодом Cellebrite для вилучення частин файлової системи пристрою.

2. Підбір пароля. Пароль доступу до пристрою потрібний для отримання ключів дешифрування інформації класів CP та AFU.

До введення архітектури SEP обмеження на вгадування та перевірка пароля контролювалися процесором пристрою, що дозволяло проводити різні успішні атаки, які полягали у скиданні лічильника неправильно введених паролів.

На попередніх версіях iOS можна було відключити живлення пристрою для скидання лічильника, а в 2016 році була продемонстрована техніка з можливістю дзеркалування флеш-пам'яті NVRAM на iPhone 5C для забезпечення необмеженого числа введення паролів.

Обмеження на підбір у 80 мс робить атаки перебором безглуздими для складних паролів із літерами та цифрами. Для PIN-коду з 6 цифр, який використовується за замовчуванням, обмеження SEP на вгадування є основною перешкодою.

Таблиця 1.1 – Оцінка часу перебору цифрових паролів у iOS

Длина пароля	**4 цифры**	**6 цифр**	**10 цифр**
Всего вариантов	10^4 = 10 000	10^6 = 1 000 000	10^10
Всего используется	9276	997090	-
80 мс/попытка ожидание	12,37 минуты 6,19 минуты	22,16 часа 11,08 часа	~25 лет
10 мин./попытка ожидание	~70 дней ~35 дней	~20 лет ~10 лет	~200 000 лет

3. Злом SEP. Для взаємодії з SEP потрібні привілеї ядра. Джейлбрейк, ймовірно, необхідний у ланцюжку для злому SEP. При успішній атаці на SEP зловмисник або фахівець із кіберкриміналістики отримує необмежений доступ до ключів шифрування та інших функцій захисту пристрою з можливістю повністю вилучити будь-які файли.

У 2018 році компанія Grayshift представила інструмент GrayKey, який, за непідтвердженими даними, міг оминати обмеження SEP. Було представлено ряд витоків, наприклад успішне зламування пароля блокування екрану iPhone X цим же інструментом. У січні 2020 р. з'явився витік з ФБР, де говорилося, що GrayKey отримав доступ до заблокованого iPhone 11 Pro Max (iOS 13), який невразливий для checkm8, що залишає багато питань: чи це було робочим експлойтом або компрометацією безпосередньо SEP?

4. Обхід блокування екрану. Користувачі пристроїв можуть випадково виявити в інтерфейсі iOS поведінку, яка дозволяє обійти блокування екрану. Наприклад, це може бути поведінка при доступі до камери, віджету погоди або годинника. Для відтворення успішного обходу потрібна акуратність та послідовність дій. Обхід блокування може відкрити несанкціонований доступ до фотографій, контактів, iTunes. Як правило, Apple швидко закриває подібні шляхи обходу.

5. Локальне вилучення даних. Стратегія отримання даних залежить від того, в якому стані був пристрій на момент захоплення: вимкнено або включено. Під час конфіскації мобільних пристроїв Apple співробітники правоохоронних органів різних країн нерідко забирають на аналіз суміжні пристрої, наприклад MacBook або Apple TV, використовують клітину Фарадея та автономне джерело живлення для запобігання вимкненню пристрою.

Під час компрометації iOS зловмисником останнім рівнем захисту даних буде шифрування, організоване Data Protection. Тому поточні методи отримання даних без згоди (або при недоступності) користувача можуть відбуватися по одному з трьох напрямків, перерахованих далі.

1. Доступ до пристрою за допомогою ключів. Якщо ключі шифрування завантажені в пам'ять, їх можна вийняти. Наприклад, інструменти форензики Cellebrite UFED і XRY Logical дозволяють підключатися до пристроїв iOS через USB / Lightning або через Bluetooth, ініціювати резервне копіювання або переглянути файли.

2. Обхід захисних механізмів. У деяких випадках дані, недоступні

для отримання, можуть бути вилучені. Інструмент GrayKey, який успішно отримав коди доступу користувачів, є прикладом. Якщо пристрій перебуває у стані AFU (і навіть BFU), то відкрито можливість високочастотної атаки перебором пароля користувача. Успішна атака дозволить витягти всю файлову систему iOS, Keychain та вміст iCloud.

3. Альтернативні джерела даних. Тут застосовується атака на резервну копію iOS, яка зберігається на локальному комп'ютері та має порівняно слабкий захист від брутфорсу. Також використовується можливість отримання даних користувача з хмарних сервісів.

6. Вилучення даних з хмари. Все більше і більше даних мобільних пристроїв синхронізується з хмарними сервісами, що зміщує акцент на вилучення даних не з пристрою, а з хмари. Компрометація SEP може дозволити отримати Keychain, який відкриє доступ до служб iCloud, Slack, Twitter, Instagram, Facebook, Google, Uber, Dropbox. Ймовірно, ці токени зберігаються в режимі AFU, щоб підтримувати функціонування при блокуванні пристрою, але це відкриває додаткові ризики, знижуючи захист SEP, так що тут доводиться покладатися тільки на безпеку ядра iOS.

Шляхи підвищення захисту iOS.

1. Посилення захисту даних. Apple розробила якісний фреймворк для захисту даних користувача, але поки що Data Protection не використовується у максимально строгому режимі. Наприклад, токени автентифікації для хмарних сервісів схильні до ризику вилучення з пам'яті. Клас захисту в стані AFU цілком надійний, але потрібна ретельніша організація його роботи.

2. Динамічний захист даних. Може бути реалізований при взаємодії з користувачем на основі алгоритмів навчання у поєднанні з посиленням захисту класу CP. iOS прогнозує, які ключі повинні застосовуватися і коли, вчасно видаляти з пам'яті неактуальні ключі шифрування та завантажувати актуальні за необхідності.

3. Наскрізне шифрування бекапівта iCloud. Apple зберігає ключі, які можуть дешифрувати дані бекапів в iCloud. Використовуючи iCloud Keychain,

можна якісно організувати наскрізне резервне копіювання, недоступне Apple, але доступне для будь-якого довіреного пристрою користувача. Це можна застосувати і для контейнера CloudKit, що значно підвищить безпеку зберігання даних користувача в хмарі.

4. Ліквідація особливих випадків обходу шифрування. Ключ наскрізного шифрування iMessage зберігається в резервній копії iCloud, до якої Apple має доступ. Дану лазівку слід усунути шляхом перенесення ключа у контейнер CloudKit із застосуванням сценарію «end-to-end».

5. Паролі на локальні бекапи. Рекомендується підвищення складності паролів локальних бекапів для захисту від перебору. Можна реалізувати це шляхом оптимізації інтерфейсу чи навчання користувачів.

6. Посилення iCloud Keychain. Слабке місце – кластер HSM, оскільки немає прозорості шифрування з боку сервера. Тут Apple може застосувати технологію Certificate Transparency, за якої вузли перевіряють адреси та коректність HSM, публічно транслюють інформацію або діляться нею між собою.

7. Обмеження на USB-інтерфейс. Більш суворі обмеження при керуванні USB / Lightning на рівні ядра iOS можуть посилити безпеку та запобігати роботі експлойтів, наприклад checkm8.

8. Обмеження на режими DFU та JTAG. Користувачі можуть у будь-який момент перевести свій пристрій у режим DFU, і експлойти потенційно здатні використовувати цю лазівку. Тут можна організувати аутентифікацію із застосуванням криптографії.

Аналогічні рекомендації можна застосувати до режиму JTAG, який, як правило, більшості користувачів не потрібно використовувати.

9. Прозорість та функціональні протиріччя. Протиріччя у підході Apple до питання захисту даних користувача слід усунути. Наприклад, включаючи / вимикаючи опцію синхронізації даних з iCloud, користувач стикається із заплутаною політикою, з ризиком витоку даних. Це ж стосується і інтерфейсу, до налаштувань та управління iCloud за умовчанням.

10. Вплив iOS-спільнот. Величезна кількість користувачів та

популярність iOS створюють базу любителів та дослідників різного рівня. Взаємодія з цими спільнотами (не тільки на рівні багхантінгу), наприклад, за допомогою відкритого вихідного коду, допоможе не лише посилити безпеку iOS, але й почути потреби користувачів, привнести інновації.

1.3. Google Android

Android, або Android Open Source Project (AOSP) – це набір програмного забезпечення з відкритим вихідним кодом, розробленого Open Handset Alliance під керівництвом Google. Мобільні сервіси Google (GMS), що включають пропрієтарні API і програмні сервіси, значно розширюють і ускладнюють екосистему Android.

Будучи заснованою на базі Linux, Android має всі переваги та недоліки безпеки цієї операційної системи. Вразливості мобільних пристроїв під керуванням Android завжди гостро відчуваються в усьому світі через велику популярність і поширеність.

Огляд еволюції захисту Android.

1. Ізольоване середовище програми. З перших версій файлове сховище Android розділене на внутрішнє (вбудоване у пристрій) та зовнішнє (SD Card). Саме внутрішнє сховище перебуває під особливим контролем операційної системи; там програма ізолюється в пісочниці, отримуючи доступ лише до своєї власної частини сховища.

В Android 4.3 було додано SELinux (Security Enhanced Linux), який був активний для критичних системних функцій, а починаючи з Android 5.0 механізми безпеки SELinux застосовувалися вже до всієї системи. Подальший розвиток призвів до того, що в Android 9.0 кожен додаток працює в окремій «пісочниці» SELinux.

Потрібно відзначити, що починаючи з Android 7.0 суворіші обмеження вводяться і на зовнішнє сховище даних (SD Card).

2. Шифрування даних. Перші версії не застосовували жодних методів

шифрування для захисту даних користувача. В Android 4.4 введено опцію шифрування всього диска, а з Android 5.0 шифрування диска стало стандартом. Наступна еволюція Android оптимізувала роботу з шифруванням, досягнувши комбінації із шифрування метаданих (інтегрована в Android 9.0) та шифрування на основі файлів (Android 7.0), що дозволяє пристрою безпечно виконувати критично важливі системні функції без розблокування телефону.

3. Контроль цілісності. Відбувається за допомогою перевірки завантажувального коду та файлів APK (Android Package).

Перевірка завантажувального коду здійснювалася модулем dm-verity і була введена в Android 4.4. Якщо цілісність даних було порушено, користувач отримує попередження, але завантаження ОС триває. В Android 8.0 представлена нова версія завантажувача Android Verified Boot (AVB).

Перевірка установки APK-файлів з джерел, відмінних від довірених (Google Play), додана в Android 2.1. В Android 7.0 введена система підпису програми, специфічна для APK.

У 2021 році Google вимагає, щоб програми для публікації в Google Play використовували App Bundles. Остаточне складання та підписування APK перед публікацією в Google Play здійснює безпосередньо Google, що викликає протести та невдоволення багатьох розробників.

Android 4.1 вводить механізм Keymaster Hardware Abstraction Layer (HAL) для зберігання ключів лише на рівні апаратної абстракції. Keymaster TA виконує операції підпису та перевірки додатків. В Android 6.0 додано AES і HMAC, а також контроль за використанням ключів шифрування.

Введення додаткового апаратного модуля безпеки (secure element), аналогічного SEP iOS, стало звичайним явищем в останні роки. Це криптографічний модуль, що існує окремо від основного процесора і призначений для роботи виключно з секретними даними користувача. Android 9 додана функціональність StrongBox Keymaster, яка розширює можливості Keymaster TA з метою здійснення криптографічних операцій на головному процесорі пристрою.

Сучасний захист даних користувача Android.

1. Аутентифікація. Цифровий код, буквено-цифрова фраза або патерн (графічний візерунок). За деякими дослідженнями патерн-аутентифікація еквівалентна за силою цифровому паролю з двох або трьох цифр. Також підтримується біометрична автентифікація по відбитку пальця або особі користувача, що застосовується виробниками пристроїв за бажанням, тому що не потрібна Android обов'язково.

Підтримується опція Smart Lock, коли система використовує інформацію про оточення для розблокування (наприклад, коли телефон знаходиться вдома або у кишені).

2. Пісочниця для додатків. Використовується дискреційний контроль доступу (DAC) та SELinux. Файли програми в системі мають дозволи на основі ідентифікаторів користувачів Linux, тому спроба доступу програми не до своїх файлів викликає помилку.

Додатковий рівень ізоляції забезпечує SELinux. Політики SELinux дозволяють контролювати привілеї додатків суворіше. Обов'язковий контроль доступу (MAC) гарантує, що якщо процес запущений з правами суперкористувача (root), це призведе до повної компрометації системи.

3. Шифрування. Поділяється в Android на два види: повне шифрування диска та файлове шифрування.

Повне шифрування диска (з'явилося в Android 4.4) базується на модулі "dm-crypt" ядра Linux. Застосовується алгоритм AES-128 як CBC з ESSIV. Майстер-ключ шифрується ключем, який створюється з пароля користувача (цифровий код, фраза, патерн). Майстер-ключ повинен бути доступний під час завантаження ОС, щоб була можливість активувати основні функції системи. Після аутентифікації користувача майстер-ключ зберігається в пам'яті пристрою завжди, оскільки він необхідний для всіх операцій блокування доступу до розділу даних.

Файлове шифрування забезпечує більш гранульований контроль. Модуль fscrypt ядра Linux використовує алгоритм AES-256 в режимі XTS для файлів і CBC для метаданих файлів. Зашифровані файли поділяються на дві

категорії: Credential Encrypted (CE) і Device Encrypted (DE). Дані CE зашифровані з використанням ключа, отриманого з пароля користувача, тому доступ до них відкривається тільки після розблокування пристрою. Дані DE базуються на секретах безпосередньо пристрою та доступні як під час завантаження, так і після розблокування.

За замовчуванням для всіх програм застосовується CE, а DE зарезервований для певних системних програм (дзвінки, годинники, клавіатура тощо).

Поєднання шифрування на основі файлів із шифруванням метаданих дозволяє Android здійснити захист всього вмісту на пристрої. Однак зловмисник, якому вдалося отримати доступ до пам'яті пристрою (наприклад, застосувавши експлойт для компрометації ядра системи), може отримати прямий доступ до майстер-ключа та зашифрованих даних.

4. Знімний носій даних (SD-картка). Зручна функція розширення пам'яті пристрою забезпечується підтримкою карток SD. В Android 6 представлена опція сховища, що адаптується, коли система може інтегрувати SD-карту як частину свого внутрішнього сховища, застосовувати там шифрування і керувати доступом. З іншого боку, ця опція прив'язує карту SD до одного пристрою, так як ключі шифрування зберігаються безпосередньо на останньому.

5. Апаратні елементи безпеки. Безпека в сучасних пристроях під керуванням Android реалізується апаратними методами. Пристрої з архітектурою ARM використовують механізм ARM TrustZone. На відміну від Apple SEP, TrustZone використовує один процесор, а не окремий співпроцесор, що не позначається на рівні захисту. Деякі виробники встановлюють додатковий процесор безпеки: наприклад, у Samsung він є в лінійці Galaxy S, а Google вставляє чіп Titan M у пристрої лінійки Pixel. Ці модулі (secure elements) є насправді аналогами Apple SEP для операцій лише з секретними даними. Ключі Keymaster передаються в ці захищені апаратні модулі для обробки, не задіявши основний процесор.

6. Android Verified Boot (AVB). Застосовується модуль верифікації "dm-verity" для перевірки цілісності початкового завантаження системи на основі

криптографічного хеш-дерева. Якщо в міру завантаження модулів ОС одне зі значень не збігається з очікуваним, то перевірка завершується помилкою і пристрій переводиться у нефункціональний стан. Підтримується опція відкату до попередньої безпечної версії Android, яка зберігається у захищеному від несанкціонованого доступу розділі.

Розблокований завантажувач дозволяє відключити AVB і виконувати довільний код під час завантаження пристрою, що може бути корисним розробникам або користувачам, які бажають отримати рут-доступ.

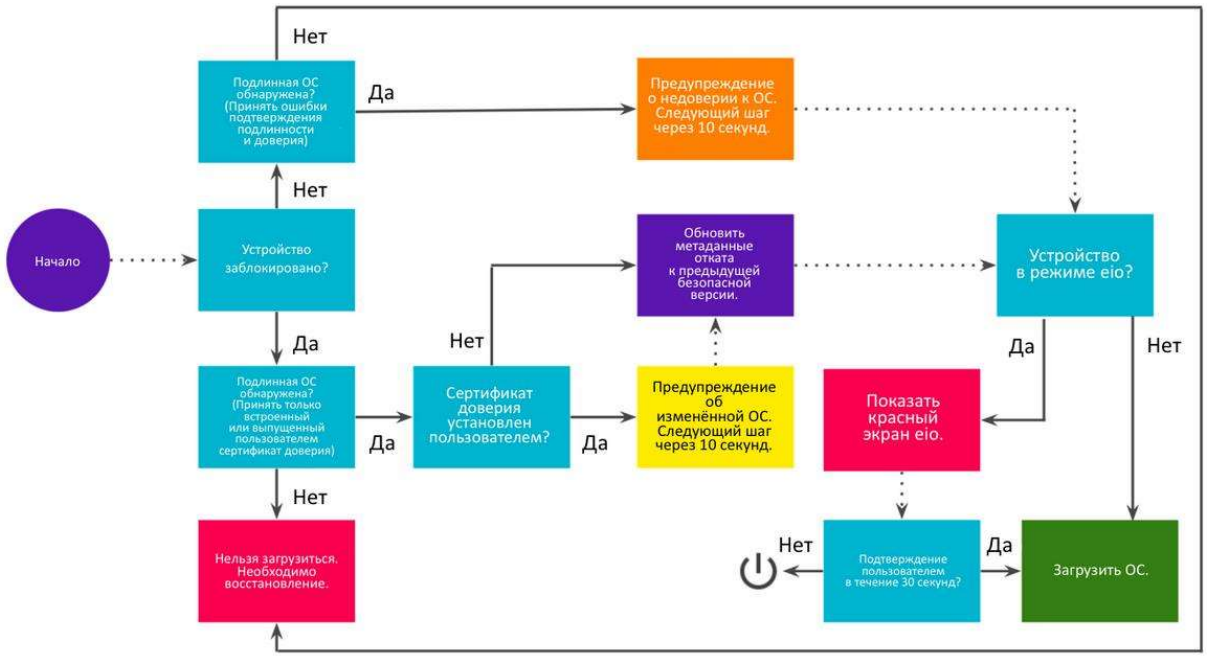


Рисунок 1.4 – Алгоритм роботи Android Verified Boot

7. Google Mobile Services (GMS). Багато функцій безпеки пов'язані з мобільними сервісами Google (GMS), такими як Drive, Gmail, Duo, Photos, Maps, Play Services. Пристрої, які пройшли сертифікацію та прийняті в GMS, позначаються як Play Protect certified.

Google використовує Google Cloud для зберігання даних та застосовує протокол TLS для зв'язку клієнта із сервером. Всі дані Google Cloud зашифровані ключами, які відомі Google. Наскрізне шифрування підтримується лише у програмі Google Duo.

Розробники програм взаємодіють з GMS через Play Services API. Слід

зазначити API SafetyNet, який по суті є службою перевірки Android-пристроїв щодо наявності рут-прав або підозрілого ПЗ.

8. Підписування APK та перевірка коду. AOSP вимагає, щоб розробник підписав створену ним програму, що запускається. Підпис (ланцюжок сертифікатів та кортежі) файлу APK відповідає відкритому ключу, що розповсюджується разом із ним. До публікації програми в Play Store здійснюється автоматична та ручна перевірка коду програми співробітниками Google.

Починаючи з версії Android 11 застосовується також модуль fs-verity – для безперервної перевірки файлів APK. Якщо телефон сертифікований GMS, то є опція встановлення програм з «невідомих джерел», наприклад, тих, які відсутні в Play Store або створені альтернативними розробниками.

9. Резервне копіювання. Організовано двома способами за допомогою GMS. Починаючи з версії Android 2.2, застосовується Android Backup Service. Програма створює резервні копії пар ключів та значень відповідно до конфігурації користувача. Ця опція не є обов'язковою і налаштовується розробником програми.

В Android 6 з'явився механізм Auto-Backup, який автоматично синхронізує дані з Google Drive. У цьому випадку налаштування розробника не потрібні, а користувачеві надається можливість відмовитися від цієї послуги.

Обидва варіанти резервного копіювання використовують Google Cloud для зберігання. GMS організує транспортування даних із пристрою у хмару.

З 2018 року підтримується наскрізне шифрування для Android Backup Service. Ключ для шифрування бекапів генерується на пристрої, для доступу до ключа застосовується класична автентифікація користувача (PIN-код, пароль або патерн). Для захисту ключа з боку Google застосовується модуль Titan HSM (входить до Google Cloud Key Vault). Titan HSM активує свій ключ тільки за умови правильної автентифікації з боку користувача пристрою. Також Titan HSM забезпечує захист від брутфорсу та контролює можливість відкату на попередні версії ПЗ.

Дані, які не належать до програм, копіюються окремо в сервіс Google

Drive за аналогією з Android Auto-Backup. Ці дані шифруються за допомогою пароля облікового запису Google або засобу автентифікації користувача на пристрої. Google має доступ до цих ключів.

Деякі виробники пропонують власні служби бекапірування. Android Debug Bridge (і ряд сторонніх інструментів) дозволяє здійснити резервне копіювання захищене паролем на локальний комп'ютер через інтерфейс USB.

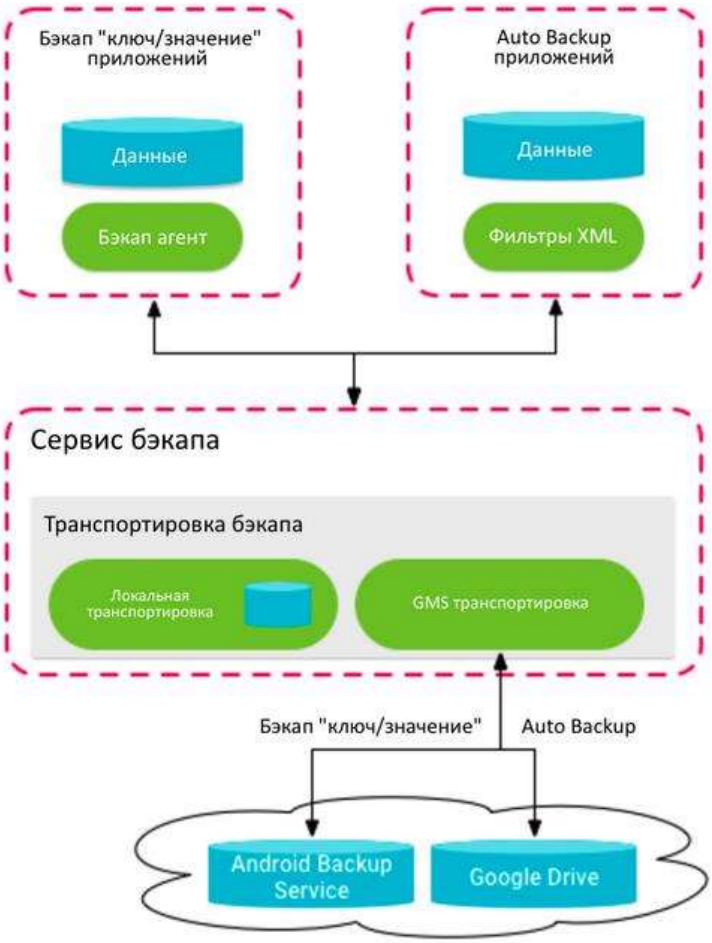


Рисунок 1.5 – Схема роботи резервного копіювання в Android

10. Повідомлення та відеозв'язок. В Android не підтримується наскрізне шифрування для обміну повідомленнями через SMS/MMS або Google Messages. Такий захист є лише у відеодзвінків у Google Duo (протокол DTLS-SRTP), які є одноранговими (без сервера-посередника, лише налаштування з'єднання маршрутизується через Google).

У групових відеочатах також підтримується наскрізне шифрування, де з

кожним із учасників відбувається парний обмін ключами.

Рисунок 1.6 – Схема встановлення безпечного з'єднання Google Duo

Техніки обходу захисту даних користувача Android.

1. Отримання рут-доступу та використання експлойтів. Отримання рут-доступу в Android аналогічно джейлбрейку на iOS – воно дозволяє модифікувати ОС під потреби користувача, оминати обмеження виробників або запускати довільний код.

Деякі пристрої відкрито підтримують рутування для цілей розробки. Для виконання цієї процедури необхідно розблокувати завантажувач. У цьому випадку всі дані користувача видаляються, оскільки система більше не довіряє завантажувачу і не може гарантувати безпеку даних. Існують експлойти, які дозволяють обходити це обмеження та отримувати доступ до даних користувача. Виробники пристроїв, у свою чергу, блокують спроби рутування. Samsung, наприклад, з 2013 року використовує Knox-bit – запрограмований електронний запобіжник, який після спрацьовування може бути замінений лише апаратно. Google SafetyNet також виявляє пристрої, на яких удалося отримати рут-доступ. За даними SafetyNet від 2017 року 5,6% пристроїв Adroid рутовані.

Отримання рут-доступу за допомогою експлойтів без загрози стирання даних користувача здійснюється за різними векторами. Наприклад, це може бути атака на ядро ОС або конкретний код пристрою (OEM або особливості SoC).

Android базується на ядрі Linux, тому багато вразливостей останньої актуальні для Android і дозволяють отримати доступ суперкористувача. Наприклад, вразливість Linux Dirty CoW лягла в основу експлойту під Android, а вразливість PingPongRoot, виявлена в ядрі Android, могла бути використана в Linux. Також постійно виявляються нові, ще невідомі (0-day) вразливості, які можуть бути використані для отримання рут-доступу, в тому числі на великій кількості пристроїв.

Атака на конкретний пристрій більш вузькоспрямована. Розглядаються особливості обладнання, прошивка компонентів, наприклад, Qualcomm EDL. При деяких маніпуляціях із пристроєм завантажується інтерфейс аварійного налагодження Qualcomm EDL, а не Android, що дозволяє зловмиснику записати необхідний код у розділ Android та отримати права суперкористувача без втрати даних. Деякі пристрої з компонентами MediaTek можна безпечно рутувати інструментом SP-Flash-Tool без розблокування завантажувача. Список таких пристроїв та вразливостей на базі ядра дуже великий через поширеність і специфіку ОС Android.

2. Альтернативні та потенційні техніки обходу захисту. Підозрілі програми, встановлені з недовірених (і навіть довірених) джерел, не завжди несуть ризик компрометації даних користувача, але зловмисник, якому вдалося запровадити такого роду програмне забезпечення, має певні переваги в обході захисних механізмів Android.

Вразливість у конкретному додатку може призвести до витоку даних, як це було, наприклад, у WhatsApp. Видалене виконання коду призводило до крадіжки архіву повідомлень програми. Режим пісочниці ефективно обмежує таку вразливість і не дозволяє скомпрометувати всю систему.

Атака на довірене апаратне та програмне забезпечення може бути

корисною в ланцюжку експлойтів. Втім, успішних атак, наприклад, на Samsung Secure Processor чи Google Titan M, зафіксовано не було. Google пропонує 1000000 доларів США за робочий експлойт для Titan M.

Брутфорс пароля та патерна обмежується механізмом Gatekeeper, який дозволяє контролювати запити за допомогою пауз між спробами. Однак можна обійти обмеження Gatekeeper шляхом компрометації архітектури TEE TrustZone і навіть повністю виключити перевірку за допомогою хитрих лазівок.

У деяких випадках Google Smart Lock дозволяє обійти блокування екрана без автентифікації користувача. Проте, коли доступ до заблокованих функцій Android або даних користувача був отриманий за допомогою обходу блокування екрана, не зафіксовано.

3. Локальне вилучення даних інструментами форензики. За допомогою Android Debug Bridge можна зробити повну резервну копію пристрою на локальну машину та отримати всі дані, але за умови, що пристрій вже розблокований або відомий PIN-код. Якщо картка SD не була прив'язана до пристрою та зашифрована, можна вийняти картку SD.

В іншому випадку для доступу до даних можна використовувати різні інструменти форензики, наприклад утиліту Autopsy з відкритим кодом. У складніших ситуаціях можна скористатися професійними сервісами від Cellebrite, Oxygenабо Magnet, які мають свої інструменти отримання даних, засновані на різних експлойтах і методиках.

4. Вилучення даних із Google Cloud. Android тісно пов'язаний із безліччю служб Google і зберігає дані в Google Cloud без наскрізного шифрування, маючи повний доступ до даних. За запитами правоохоронних органів, ця інформація може бути надана на експертизу. Винятком є сервіс Android Backup Service.

Якщо з якихось причин Google відмовляє в запиті або доступ до хмарних даних намагається отримати зловмисник, то застосовуються інструменти форензики, що дозволяють витягти з пристрою токени автентифікації для хмари.

Далі дані завантажуються з хмари у ручному режимі.

Шляхи підвищеня захисту Android.

1. Шифрування даних користувача під час блокування екрану. Після блокування екрана ключ шифрування повинен видалятися з пам'яті. Поки користувач не використовує пристрій, особисті дані будуть недоступні. Введення такої функціональної особливості в Android підвищить поточний рівень безпеки, але вимагатиме від розробників адаптувати роботу програм у фоновому режимі при заблокованому екрані. Це також обмежить ефективність вилучення даних з рутованих пристроїв за допомогою експлойтів.

2. Використання наскрізного шифрування для обміну повідомленнями та інших продуктів Google. Наскрізне шифрування в службах GMS підвищить довіру користувачів та забезпечить належну безпеку даних. З іншого боку, Google використовує машинне навчання на всіх даних користувача, до яких має доступ, для підвищення якості послуг.

3. Безпечний доступ до роботи з прошивкою. Багато експлойтів обходять захисні механізми Android використовуючи вразливості в прошивці. Можна піти апаратним шляхом і поширювати програматори прошивки із захищеними від злому компонентами, що дозволить постачальникам відстежувати виток. Другий варіант – вилючення сертифіката скомпрометованого програматора.

4. Посилення компонентів апаратної частини. Функціональність TEE TrustZone може бути посилена апаратно при використанні виділеного співпроцесора безпеки. Зменшуючи вартість пристроїв, виробники не завжди впроваджують додатковий співпроцесор для підвищення безпеки та стійкості до апаратних та програмних атак.

5. Підвищення частоти оновлення Android. Сучасні пристрої забезпечують надійний захист даних користувача. Однак величезна кількість пристроїв працює не на останній версії ОС з різних причин, що створює ризик уразливості до багатьох атак. Особливо це стосується застарілих пристроїв, які не можна встановити фінальну версію ОС. Навчання користувачів та підвищення

частоти оновлень безпеки Android допоможе знизити ризики для безпеки даних користувачів.

6. Більше переваг від відкритого коду та екосистеми. Велика популярність та охоплення ринку можуть посилити безпеку Android по багатьох напрямках. За рахунок відкритого коду розробники можуть впроваджувати покращення, які не залежать від Google. Зі свого боку Google може просувати протоколи та формувати стандарти безпеки. Єдине ядро Linux та Android вигідно обом платформам: покращення Linux відбиваються на Android і навпаки. Обидві системи допомагають одна одній своєчасно виявляти та усувати критичні вразливості, поступово підвищуючи безпеку.

1.4 Висновки до розділу.

При належному зусиллі зловмисник має високу можливість отримати доступ до конфіденційних даних користувача незалежно від використовуваної платформи. Виділимо особливості безпеки кожної з операційних систем.

Особливості безпеки Apple iOS:

1) автентифікація користувача (цифровий PIN-код, пароль, біометрія) плюс SEP;

2) підписування коду (Boot ROM та підписування додатків);

3) пісочниця та аналіз коду додатків;

4) шифрування (AES, ECDH over Curve25519, UID, Data Protection classes);

5) Keychain (API для безпечного зберігання ключів);

6) резервне копіювання (Keybag та iCloud Backup Keybag);

7) хмарний сервіс iCloud та CloudKit (API для iCloud);

8) iCloud Keychain (синхронізація та відновлення Keychain);

9) апаратне забезпечення безпеки (SEP);

10) контроль та обмеження фронту атаки (Wi-Fi, Bluetooth, пуш-повідомлення, USB/Lightning).

Особливості безпеки Google Android:

1) автентифікація користувача (цифровий PIN-код, пароль, патерн, біометрія) плюс Gatekeeper та Smart Lock;

2) пісочниця додатків (DAC+SELinux);

3) шифрування всього диска та файлів (AES-128/256, Credential Encrypted та Device Encrypted), а також SD-карти;

4) Trusted Execution Environment(TEE) та додатковий апаратний модуль безпеки (secure element);

5) Android Verified Boot;

6) резервне копіювання (Auto-Backup та Backup Service);

7) Google Mobile Services;

8) підписування додатків та аналіз коду;

9) наскрізне шифрування в Google Duo.

Незважаючи на те, що Apple ретельніше організовує шифрування файлів на пристрої і в хмарі, ніж Google, існують ситуації, коли зловмисник може отримати багато (або всі) дані користувача. Зберігання токенів аутентифікації для iCloud у режимі AFU потрібно переробити. Забезпечення наскрізного шифрування всіх даних у хмарі усуне протиріччя політиці конфіденційності Apple.

Наскрізне шифрування рекомендується і для Android GMS. Серйозніший недолік Android – це постійне зберігання ключів шифрування в пам'яті пристрою після першого розблокування. Використання аналога iOS Complete Protection значно збільшить захист даних користувача від атак зловмисників.

Користувачам мобільних пристроїв можна порекомендувати використовувати максимально складні паролі, а також біометричну автентифікацію скрізь, де рекомендується операційною системою. По можливості слід застосовувати 2FA (двофакторну автентифікацію). Корисно вивчити установки синхронізації даних з хмарними сервісами і не передавати в хмару нічого зайвого.

Рутування / джейлбрейк пристрою – це великий ризик запуску

довільного коду (у тому числі і на рівні прошивки), який може бути небезпечним та повністю скомпрометувати пристрій.

2 АНАЛІЗ МОЖЛИВОСТІ, ДОЦІЛЬНОСТІ ТА ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ СЕНСОРНОГО ПОЧЕРКУ ДЛЯ ПІДВИЩЕННЯ НАДІЙНОСТІ ЗАХИСТУ МОБІЛЬНИХ ПРИСТРОЇВ

В епоху інтелектуальних технологій кількість користувачів смартфонів зростає з кожним роком, що, у свою чергу, вимагає застосування додаткових заходів безпеки щодо інформації, що зберігається на цих пристроях. Найчастіше для обмеження доступу до мобільних телефонів використовуються або PIN-код або графічний пароль, хоча в даний час все більшого поширення набувають такі технології, як сканування відбитків пальців, використання зображення обличчя або інших біометричних характеристик. Однак слід зазначити, що найбільш поширеним на сьогоднішній день є саме PIN-код як механізм обмеження доступу до мобільних пристроїв, який не може забезпечити адекватний захист від сучасних загроз. Тому доцільно звернути увагу до інші способи ідентифікації.

Ідентифікація може бути досягнута з використанням одного із трьох підходів. Перший – використовувати те, що знає користувач (PIN-код відноситься до цієї категорії, як і пароль). Друга категорія використовує те, що є у користувача, наприклад, токен, різні карти. Нарешті, третя категорія використовує, ким є користувач. Ця категорія широко відома як біометрія, використовуються деякі індивідуальні характеристики користувача. Біометричні характеристики можна поділити на статичні та динамічні. Статичні (фізіологічні) включають такі атрибути, як сітківка ока, відбитки пальців, геометрія руки, зображення обличчя тощо.

Біометрична ідентифікація – зручний та точний метод ідентифікації. Одним із варіантів біометричної ідентифікації є аналіз натискання клавіш під час роботи з цифровими пристроями.

Підхід, що досліджується у кваліфікаційній роботі, полягає у використанні комбінації секретних знань (паролю або PIN-коду) та біометрії (аналіз

динаміки натискання клавіш при введенні парольної фрази). В даному випадку, технологія, заснована на секретних знаннях, буде використовуватися як завжди, але також аналізуватиметься ритм натискання клавіш для забезпечення додаткової перевірки.

Переваги ідентифікації користувача на основі аналізу динаміки натискання клавіш:

− унікальність: є можливість вимірювати часові дані з точністю до мікросекунд для подій натискання клавіш, щоб точно ідентифікувати користувача;

– низькі витрати на впровадження та використання: розпізнавання динаміки натискання клавіш не потребує додаткового обладнання та може бути повністю реалізовано за допомогою програмного забезпечення;

− скритність: користувач може не знати, що в деяких системах реалізовано додатковий рівень ідентифікації з використанням динаміки натискання клавіш;

− надійність: використання динаміки натискання клавіш у схемі ідентифікації пароля може підвищити її надійність.

Використання динаміки натискання клавіш на мобільних пристроях має певні особливості порівняно із звичайними клавіатурами, які використовуються у персональних комп'ютерах:

– використання меншої кількості пальців (найчастіше використовуються тільки два великі пальці та один вказівний);

– у комп'ютерних системах зі зміною клавіатури шаблон введення символів може відрізнятися, а в мобільних пристроях із сенсорним екраном це не так.

Слід зазначити, що сенсорний екран або програмна клавіатура на смартфоні має значно більше проблем для аналізу натискання клавіш порівняно з апаратною клавіатурою. Оскільки апаратні клавіатури мають більш менш усталену форму, компонування і використовуються людьми протягом значного періоду, більшість людей набагато краще знайомі і вміють поводитися з

ними, ніж з сенсорними клавіатурами. Невеликий форм-фактор смартфона, значні відмінності у розмірі клавіатури та її розкладці, а також проблеми, що виникають у деяких людей від використання програмних клавіатур через відсутність фізичного зворотного зв'язку, який вони отримували б від апаратної клавіатури, – все це може привести до разючих відмінностей роботи з сенсорними або програмними клавіатурами в порівнянні з апаратними клавіатурами.

Загальний процес систем ідентифікації на основі натискання клавіш вимагає наступних двох етапів: реєстрації (навчання) та безпосередньо ідентифікації.

На етапі навчання користувач вводить парольну фразу (у деяких випадках потрібно повторювати цю дію кілька разів). При цьому розраховуються та запам'ятовуються еталонні характеристики даного користувача (створюється еталонний шаблон користувача). На етапі ідентифікації користувач, що претендує на доступ, вводить парольну фразу, для якої розраховуються ті ж характеристики, які порівнюються з еталонними. Залежно від результату порівняння користувач або отримує доступ до пристрою, що захищається, або ні.

У процесі введення парольної фрази визначається яка клавіша була натиснута, час утримання клавіші, час, коли вона була відпущена. Так для кожного символу парольної фрази. Іноді можуть використовуватися інші характеристики: час між натисканнями двох послідовних клавіш, сила натискання на клавіші, частота помилок та інші. Ці тимчасові характеристики використовуються для створення індивідуального шаблону користувача.

Сучасні мобільні пристрої оснащені рядом сенсорів, які можуть використовуватись мобільними програмами. Так, API Android надає програмам можливість використовувати різні датчики, такі як гравітація, тиск повітря, вологість, мікрофон, камера, акселерометр, наближення, світло, гіроскоп. Основна увага приділяється датчикам руху, тобто гіроскопу та акселерометру. Акселерометр обчислює прискорення мобільних пристроїв по осях X (поперечна), Y (поздовжня) та Z (вертикальна). Програми можуть отримати доступ до значень прискорення, що оцінюється акселерометром. Гіроскоп, у свою чергу, вимірює

орієнтацію (кут) пристрою навколо кожної із трьох фізичних осей. Набір із трьох кутів, що задають орієнтацію телефону в тривимірному просторі, дозволяє визначити, де користувач натиснув на екран. Кожна клавіша має унікальну картину змін кутів за трьома осями, які можуть бути ідентифіковані. Програми можуть розраховувати значення швидкості обертання (радіан/секунду), орієнтації (кута) та вектора обертання (орієнтація пристрою як комбінація осі та кута), заданих гіроскопом. Таким чином, гіроскоп і акселерометр можуть широко використовуватися в додатках, де потрібна характеристика поведінки, наприклад, для визначення розташування або натискання клавіш на основі датчиків. В даному випадку динаміка датчика може надати дуже важливу інформацію для точного розпізнавання дій, які користувач виконує на мобільному пристрої. орієнтації (кута) та вектора обертання (орієнтація пристрою як комбінація осі та кута), заданих гіроскопом. Таким чином, гіроскоп і акселерометр можуть широко використовуватися в додатках, де потрібна характеристика поведінки, наприклад, для визначення розташування або натискання клавіш на основі датчиків. В даному випадку динаміка датчика може надати дуже важливу інформацію для точного розпізнавання дій, які користувач виконує на мобільному пристрої. орієнтації (кута) та вектора обертання (орієнтація пристрою як комбінація осі та кута), заданих гіроскопом. Таким чином, гіроскоп і акселерометр можуть широко використовуватися в додатках, де потрібна характеристика поведінки, наприклад, для визначення розташування або натискання клавіш на основі датчиків. В даному випадку динаміка датчика може надати дуже важливу інформацію для точного розпізнавання дій, які користувач виконує на мобільному пристрої.

Для реалізації процесу розпізнавання користувача системах ідентифікації використовують класифікатор, заснований одному з наступних математичних підходів: статистичні методи, нейронні мережі, методи розпізнавання образів, комбіновані.

Алгоритми, що ґрунтуються на статистиці, мають невисокі вимоги до продуктивності, що важливо для мобільної платформи. Нейросетевые

алгоритми, швидше за все, матиме високі вимоги до обробки, але у разі, показники точності ідентифікації зазвичай краще. Перевага використання нейронних мереж полягає в тому, що вони гнучкі для різних типів наборів даних. Крім того, можна одночасно розглядати велику кількість наборів даних. До того ж, нейронну мережу можна навчити спеціально для конкретного користувача.

Будь-яка біометрична ідентифікація має недолік, що полягає в тому, що деякі користувачі помилково приймаються (коефіцієнт помилкового прийняття, відомий як FAR), а деякі помилково відхиляються (хибне відхилення, відоме як FRR). Це означає, що зловмисник, який намагається отримати доступ до системи, може бути прийнятий, в той час, як дійсний користувач може бути відхилений. Для отримання кращих результатів частота помилок повинна бути якомога нижчою, а також повинна бути збалансована для особливих випадків, оскільки обидва значення не можуть дорівнювати нулю одночасно.

Іноді замість FRR та FAR оцінюється EER (рівна частота помилок). Це відбувається, коли FRR та FAR еквівалентні. Основне завдання – знайти правильне граничне значення для порівняння шаблону претендента на доступ та еталонного шаблону зареєстрованого користувача. Для деяких систем потрібний низький FAR (високий поріг), щоб зловмисник не міг проникнути до системи. Фактично це найкраще рішення для створення високозахищених систем.

На сьогоднішній день представлена достатня кількість розробок у сфері ідентифікації користувача за динамікою набору пароля або PIN-коду для мобільних пристроїв із сенсорним екраном. Однак слід зазначити, що більшість наукових праць з цієї теми є незалежними дослідженнями, кожне з яких ґрунтується на певній кількості зразків, зібраних від унікальних наборів користувачів. Дослідники збирали ці зразки за допомогою різних методів і широко варіювалися у вимірюваних даних, кількості вхідних даних, необхідних для навчання системи та ідентифікації користувачів, кількості випробуваних та різноманітності цих випробуваних, умовах тестування, мобільних пристроях. Така неоднорідність ускладнює порівняння різних досліджень. Якщо додати до цього різноманітність підходів до класифікації користувачів та

застосування цих технологій у різних галузях, завдання стає ще складнішим. Саме від вирішення цих проблем залежатиме популярність та затребуваність даної технології у користувачів мобільних пристроїв.

Щодо кількості та інформативності параметрів динаміки натискання клавіш, що використовуються при побудові системи ідентифікації, думки різних авторів також різняться. Слід зазначити, більшість авторів використовують лише дві часові характеристики: натискання (утримання) клавіші й інтервали між натисканнями двох послідовних клавіш. Деякі автори вважають, що сила натискання пальця під час набору символу є найкращим індикатором для ідентифікації користувачів у порівнянні з такими характеристиками, як час утримання та пауза між натисканнями клавіш. А деякі автори стверджують, що поєднання часових характеристик із силою натискання дає найкращі результати порівняно з їх використанням окремо.

Порівняти та оцінити результати досліджень систем ідентифікації користувачів мобільних пристроїв з динаміки набору парольної фрази за різними показниками можна за допомогою табл.2.1 [10], де вказано які інформативні параметри використовувалися; методи, що використовувалися для класифікації користувачів; різновид парольної фрази (PIN-код, довільні символи, лише цифри); довжина парольної фрази; одержані значення EER, FAR, FRR; одержана точність ідентифікації; кількість користувачів, які брали участь у експериментах; мобільні пристрої, що використовувалися в експериментах; інформацію про виправлення при наборі; зібрана кількість зразків.

Таблиця 2.1 – Порівняльний аналіз підходів до аутентифікації за сенсорним почерком

Study	Features	Classification	IT	IL	Results (in %)			
					EER	FAR	FRR	Accuracy
Dhage et al.[25]	HT,di-graphs	Mean and SD	String	10	.806			
De Mendizabal-Vazquez et al.[21]	pressure, size, latency, linear, angular acceleration	PCA and LD	PIN	4				90
Chang et al.[19]	Latency	Mean and SD	Graphical Password		12.2	11.22	12.2	
Chang et al.[19]	Pressure	Mean and SD	Graphical Password		14.6	14.54	14.6	
Chang et al.[19]	Latency, pressure	Mean and SD	Graphical Password		6.9	6.92	6.8	
Campisi et al.[31]	Latency	Mean and SD	Six different passwords	10	13			
Maiorana et al.[13]	Latency	Distance	Alphabets	10				
Huang et al.[32]	Latency, HT	Mean	abertay2011	11		7.5	5	
Tasai et al.[20]	HT/latency	Statistical	PIN	4	11.72	11.72	11.6	
Tasai et al.[20]	Time, pressure	Statistical			8.4	8.32	8.4	
Tasai et al.[20]	Time, size	Statistical			11.14	11.14	11	
Tasai et al.[20]	Time, pressure, size	Statistical			10	9.78	10	
Buchoux & Clarke[29]	Latency	Statistical	PIN			53.13	20.63	
Buchoux & Clarke[29]	Latency	Statistical	Alphanumeric			20	2.5	

Продовження таблиці 2.1

Clarke et al.[26]	HT	FF-MLP	--	--	18			
Trojahn & Ortmeier[16]	Digraph, pressure, size	J48,Kstar, MLP, RBFN, BN and NB	Any	11		2.03	2.67[!]	
Trojahn & Ortmeier[16]	x, y coordinates, pressure, size	J48,Kstar, MLP, RBFN, BN and NB	password	8		11	16	
Meng et al[24].	Touch inputs	J48, NB, Kstar, RBFN and BPNN.	--	--		7.08[&]	8.34[&]	
Meng et al.[24]	Touch inputs	PSO-RBFN	--	--		2.5	3.34	
Saevanee & Bhattarakosol[18]	Latency	PNN	Phone number	10				90
Saevanee & Bhattarakosol[18]	Pressure	PNN			1			
Karatzouni & Clarke[28]	Latency	FF-MLP	--	--	12.2	15.8	9.1	
Karatzouni & Clarke[28]	HT	FF-MLP	--	--	36.8	34.2	36.8	
Karnan & Krishnaraj[5]	HT, latency, digraph	BPNN	--	10				94.8
Jeanjaitrong & Bhattarakosol[22]	HT, latency, latency ratio, distance between buttons	BN	Graphical	4		.02	.178	82.18
Zahid et al.[23]	HT, digraph, error rate	Fuzzy	--	--		2	0	
Clarke & Furnell[29]	Latency, HT	GRNN, RBF, FF MLP	Numbers	4	8.5[%]			

Продовження таблиці 2.1

Clarke & Furnell[29]	Latency, HT	GRNN, RBF, FF MLP	Numbers	11	4.9			
Clarke & Furnell[29]	Latency, HT	GRNN, RBF, FF MLP	Numbers	Any	17.6			
Saevanee & Bhatarakosol[18]	Pressure, latency, HT	Knn	Numbers	10	1			
Trojahn et al.[12]	HT, Digraph, pressure, size	Statistical classifier using k-means	--	17		4.19	4.59	
Hwang et al.[30]	HT, latency	Artificial rhythm with cues	PIN	4	4			
Hwang et al.[30]	HT, latency	Natural rhythm without cues	PIN	4	13			
Antal et al.[14]	HT, latency, pressure, size	NB, BN, J48, KNN, SVM, RF, MLP	.tie5Roanl	10				93.04[$]
Sen & Muralidharan[27]	Pressure, HT	K*, MLP, J48, NB	Numbers (1,5,9,3)	4		14.1[#]	14.06[#]	
Giuffrida et al.[17]	accelerometer, gyroscope,	one-class SVM, NB, kNN, and the "mean algorithm".	internet and satellite	--	0.08[@]			
Giuffrida et al.[17]	n-graph				4.97			

Тут HT – час натискання клавіші, SD – стандартне відхилення, PCA – Principal Components Analysis – метод головних компонент, LDA – Linear Discriminant Analysis – лінійний дискримінантний аналіз, FF-MLP – Feed forward-MLP – нейронна мережа прямого поширення, MLP – Multilayer Perceptron – нейронна мережа, RBFN – Radial Basis Function Network – радіальна нейронна мережа, BN – Bayesian Network – Баєсова мережа, NB – Naive Bayes – наївний баєсів класифікатор, BPNN – Back Propagation Neural Network – нейронная мережа зворотного поширення, PSO – Particle Swarm Optimization – метод рою часток, PNN – Probabilistic Neural Network – ймовірнісна нейронна мережа, GRNN – Generalized Regression Neural Network – регресійна нейронна мережа, RBF – Radial Basis Function – радіальна базисна функція, SVM – Support Vector Machine – метод опорних векторів, RF – Random Forest – метод випадкових лісів, kNN – k-nearest neighbour – метод k найближчіх сусідів.

Аналіз даних в табл. 2.1 дозволяє зробити висновок, що комбінація двох факторів ідентифікації (PIN-коду/паролю та аналізу динаміки його введення) забезпечить більш високий рівень захисту пристрою від неправомірного використання нелегітимним користувачем. Навіть якщо зловмисник у будь-який спосіб дізнається PIN-код, додатковою лінією захисту буде вимога вводити його з використанням певного ритму.

Враховуючи тенденції розвитку сучасних мобільних пристроїв можна з упевненістю стверджувати, що технологія ідентифікації користувачів таких пристроїв за ритмом введення парольної фрази або PIN-коду має великий потенціал і буде затребувана завдяки наступним перевагам: простота та зручність використання з урахуванням звичних для користувача процедур введення пароля; відсутність потреби у придбанні додаткових пристроїв через використання вбудованої сенсорної клавіатури.

3 ДОСЛІДЖЕННЯ ІДЕНТИФІКАЦІЙНОГО ПОТЕНЦІАЛУ КЛАВІАТУРНОГО ПОЧЕРКУ ВЛАСНИКІВ МОБІЛЬНИХ ПРИСТРОЇВ

3.1 The MOBIKEY Keystroke Dynamics Password Database

The MOBIKEY Keystroke Dynamics Password Database було опубліковано у 2015 році [11]. З метою збору даних було розроблено та реалізовано Android-додаток для планшету Nexus 7. Користувачі повинні були ввести три різні фіксовані паролі. Використовувалися наступні паролі: легкий – kicsikutyatarka; логічний сильний – Kktsf2!2014; сильний – .tie5Roanl. Простий пароль містив лише малі літери та складався з перших трьох слів угорської приказки «Kicsi kutya tarka, se füle, se farka». Логічний сильний пароль також базується на тій самій угорській приказці, але в цьому випадку було взято перші літери слів і було використано sf2! для послідовності символів «sfsf», за якими йде рік збору даних. Логіка логічного надійного пароля була пояснена суб'єктам перед експериментом зі збору даних. Сильний пароль «.tie5Roanl» є стандартним паролем для порівняння в дослідженні динаміки натискання клавіш і також використовується у декількох датасетах з класичного клавіатурного почерку, наприклад, Keystroke Dynamics Benchmark Data Set [12].

В експерименті брали участь 54 добровольці, 5 жінок і 49 чоловіків віком 19 – 26 років. На етапі реєстрації вони зазначили свій досвід роботи з сенсорними пристроями так: 2 – недосвідчені, 6 – початківці, 17 – середні та 29 досвідчених користувачів сенсорних екранів. Серед них 4 користувача були лівшами, решта – правшами. Дані збирали в три сесії з інтервалом в один тиждень. Під час кожного сеансу учасники екмприменту вводили не менше 60 паролів, принаймні 20 паролів кожного типу. Наприкінці збору даних кожен користувач надав принаймні 60 зразків для кожного типу пароля (простий: 3323 зразки, надійний: 3303, логічний надійний: 3308). Друкарські помилки були заборонені, натомість піддослідні повинні були повторно ввести пароль. Кожен пароль потрібно було вводити однаково: однакові ключі мали бути

введені в одному порядку.

Дані в кожному з датасетів представлено у форматі Excel файлу та складаються з наступних полів (рис. 3.1):

1) holdtime1 – holdtimeN – час натискання клавіші в процесі набору парольної фрази (HT). Для паролю «kicsikutyatarka» – 15 параметрів holdtime, для паролю «Kktsf2!2014» – 13 параметрів holdtime (по дві клавіші для вводу «К» та «!»), для паролю «.tie5Roanl» – 13 параметрів holdtime (по дві клавіші для вводу «.», «5» та «R»);

2) downdown1 – downdownN – час між двома послідовними натисканнями на клавіші в процесі набору парольної фрази (DD). Для паролю «kicsikutyatarka» – 14 параметрів downdown, для паролів «Kktsf2!2014» та «.tie5Roanl» – 12 параметрів downdown;

3) updown1 – updownN – час паузи між двома послідовними натисканнями на клавіші в процесі набору парольної фрази (UD). Для паролю «kicsikutyatarka» – 14 параметрів updown, для паролів «Kktsf2!2014» та «.tie5Roanl» – 12 параметрів updown;

4) pressure1 – pressureN – тиск на екран в процесі набору парольної фрази. Для паролю «kicsikutyatarka» – 15 параметрів pressure, для паролів «Kktsf2!2014» та «.tie5Roanl» – 13 параметрів pressure;

5) fingerarea1 – fingerareaN – розмір області на сенсорному екрані від пальця користувача в процесі набору парольної фрази (FA). Для паролю «kicsikutyatarka» – 15 параметрів fingerarea, для паролів «Kktsf2!2014» та «.tie5Roanl» – 13 параметрів fingerarea;

6) meanholdtime – середнє значення часу натискання клавіш в процесі набору парольної фрази (MHT);

7) meanpressure – середнє значення тиску на екран в процесі набору парольної фрази (MP);

8) meanfingerarea – середнє значення розміру області на сенсорному екрані від пальця користувача в процесі набору парольної фрази (MFA);

9) meanxacceleration – середнє значення прискорення по вісі «X»

відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAX);

10) meanyacceleration – середнє значення прискорення по вісі «Y» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAY);

11) meanzacceleration – середнє значення прискорення по вісі «Z» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAZ);

12) totaldistance – сума відстаней (у пікселях) між двома послідовними кнопками на віртуальній клавіатурі (TD);

13) totaltime – час вводу парольної фрази (TT);

14) velocity – швидкість, обчислювалась як частка відстані та загального часу. Перед оцінкою дані були нормалізовані в діапазон [0, 1].

Таким чином, датасет для паролю «kicsikutyatarka» містить 82 інформативних параметри сенсорного почерку, а датасети для паролів «Kktsf2!2014» та «.tie5Roanl» містять по 72 інформативних параметра.

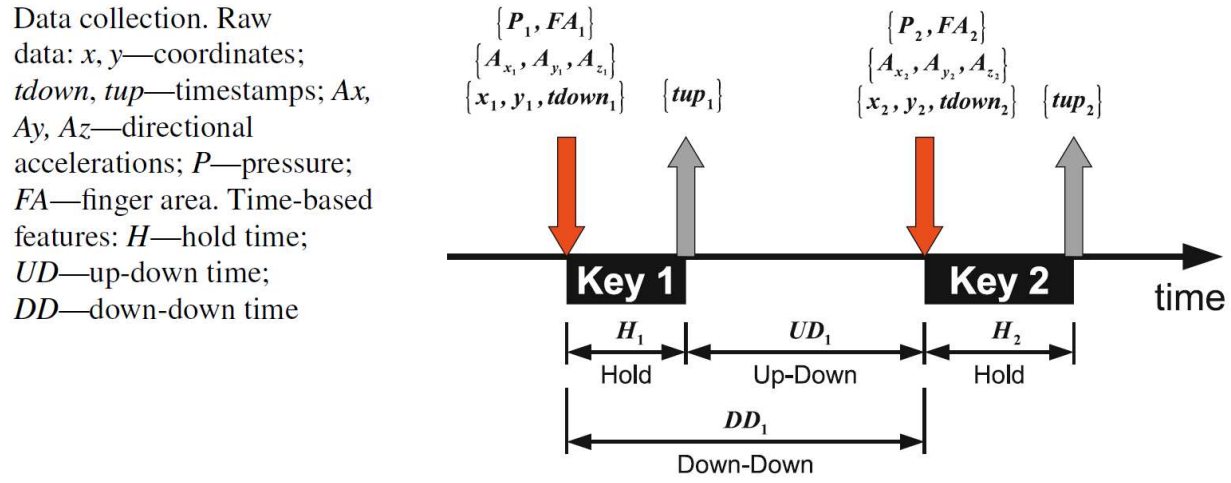


Рисунок 3.1 – Інформативні параметри сенсорного почерку у датасеті The MOBIKEY Keystroke Dynamics Password Database

3.2 Схема експерименту

Дослідження проводились у програмному середовищі Orange, що вільно розповсюджується, написано мовою Python та засновано на принципі візуального програмування для наочного доступу до алгоритмів Data mining. ПЗ Orange розроблено та підтримується Bioinformatics Laboratory of Faculty of Computer and Information Science Люблянського університету (Словенія). ПЗ Orange надає користувачеві такі основні функції [13]:

1. Завантаження даних із різних джерел (файли, веб-ресурси, бази даних) та подання їх у табличному вигляді.

2. Отримання інформації про атрибути даних (поля таблиці).

3. Побудова потоку data mining (data mining workflow).

4. Зміна даних та параметрів «на льоту» (що дозволяє відстежити зміни в режимі реального часу).

5. Візуалізація результатів за допомогою різних графіків.

6. Збереження моделі та застосування її надалі.

Orange поставляється зі своїм власним форматом даних, але може працювати з іншими форматами, наприклад, Excel (.xlsx або .xls) або CSV-файлами. Як правило, вхідними даними є таблиця із записами (об'єктами) у рядках та атрибутами даних у стовпцях. Атрибути можуть бути різного типу (безперервні, дискретні та рядкові).

Схему експерименту наведено на рис. 3.2.

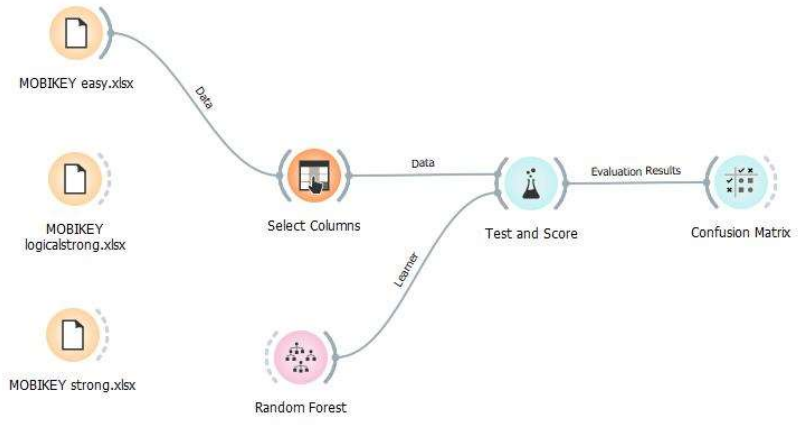


Рисунок 3.2 – Схема експерименту в Orange

3.2.1. Дослідження датасету «MOBIKEY easy».

Вихідні дані для досліджень: алгоритм класифікації Random Forest. Точність класифікації перевірялась за вбудованим у віджет «Test and Score» алгоритмом 10-fold cross-validation.

Результати мультикласової класифікації (розпізнавання) користувачів наведено на рис. 3.3. Як можна побачити інтегральна точність класифікації досить висока – 94.4 %. Отже, припущення про можливість використання сенсорного почерку для розпізнавання користувачів мобільних пристроїв є вірним.

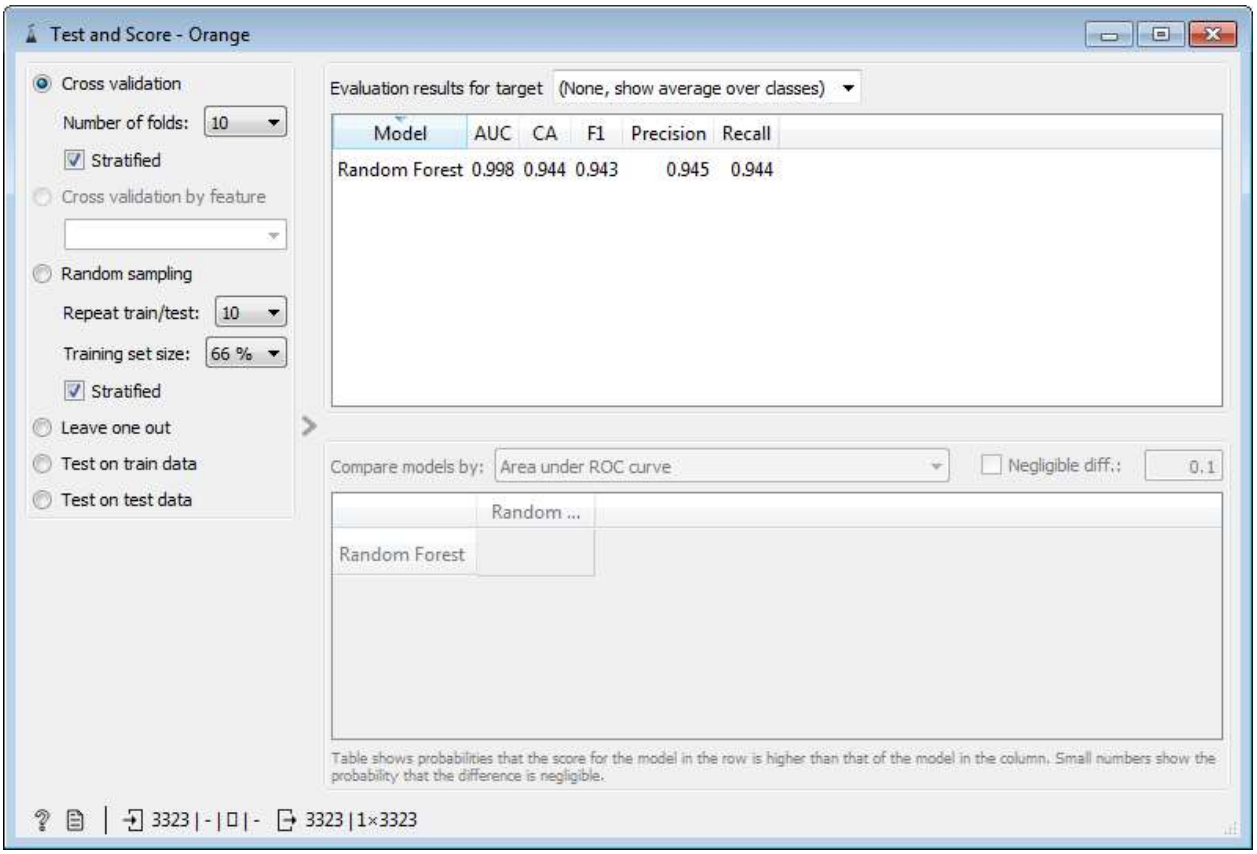


Рисунок 3.3 – Результати мультикласової класифікації користувачів датасету «MOBIKEY easy» за алгоритмом Random Forest

На рис. 3.4 наведено гістограму результатів класифікації по кожному з користувачів. Як можна побачити, мінімальне значення точності розпізнавання становить 79.4 %, максимальне – 100 %, причому кількість користувачів, для яких точність розпізнавання становить менше 90 % становить 10 осіб, тобто 18.5 % від загальної кількості користувачів. Медіана становить 96 %, тобто для половини користувачів точність розпізнавання можна вважати дуже

високою. Враховуючи, що з 54 користувачів, що брали участь в експерименті, 29, тобто майже половина, були досвідченими користувачами, можна зробити висновок, що сенсорний почерк є універсальною (можливе представлення людини однією характеристикою) і унікальною (з малою ймовірністю до смартфону можуть отримати доступ дві особи з ідентичним курсорним почерком) біометричною характеристикою. Причому, з плином часу точність розпізнавання збільшуватиметься, оскільки інформативні ознаки сенсорного почерку ставатимуть більш унікальними.

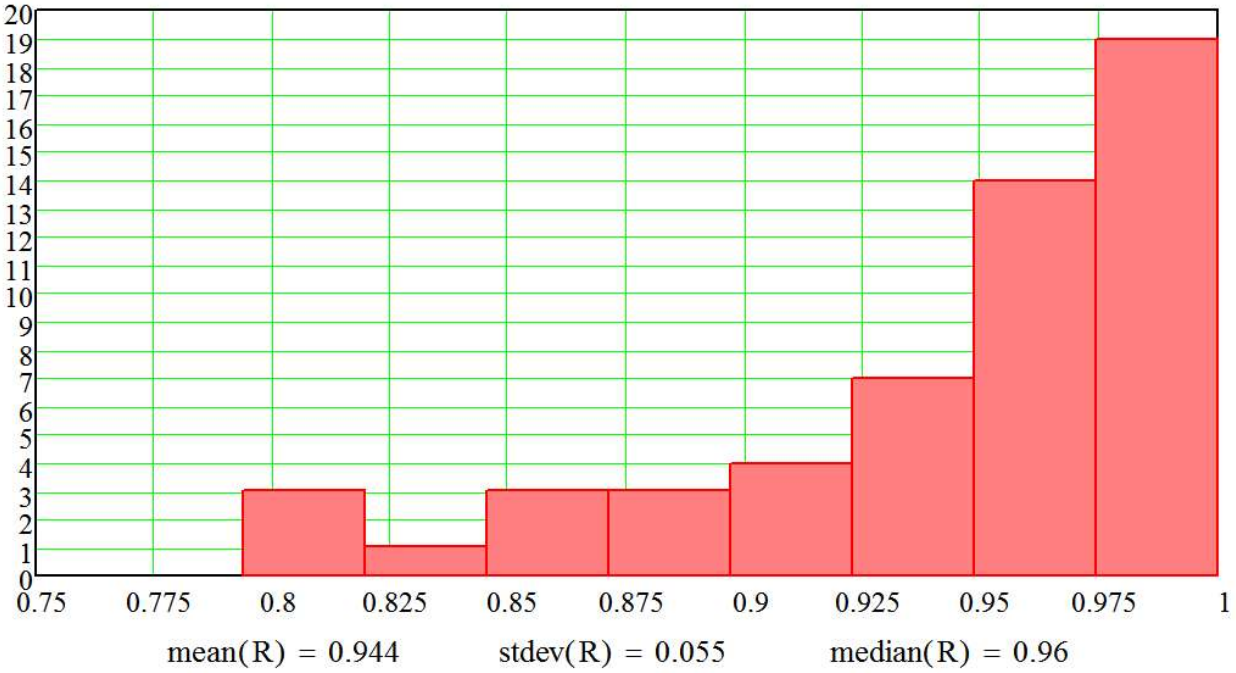


Рисунок 3.4 – Гістограма результатів мультикласової класифікації користувачів датасету «MOBIKEY easy» за алгоритмом Random Forest

3.2.2. Дослідження датасету «MOBIKEY logicalstrong».

Вихідні дані для досліджень: алгоритм класифікації Random Forest. Точність класифікації перевірялась за вбудованим у віджет «Test and Score» алгоритмом 10-fold cross-validation.

Результати мультикласової класифікації (розпізнавання) користувачів наведено на рис. 3.5. Як можна побачити інтегральна точність класифікації практично не змінилась – 94.5 %.

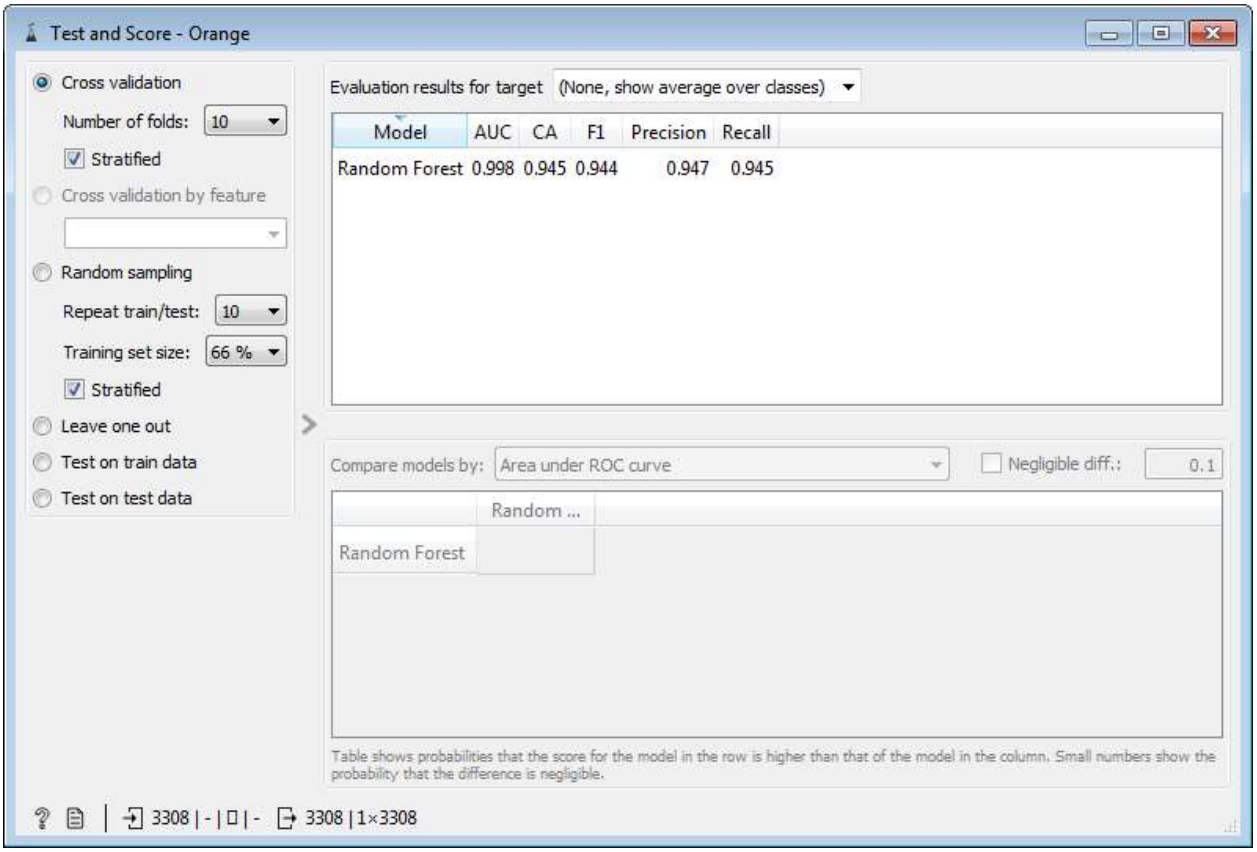


Рисунок 3.5 – Результати мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за алгоритмом Random Forest

На рис. 3.6 наведено гістограму результатів класифікації по кожному з користувачів. Як можна побачити, мінімальне значення точності розпізнавання становить 70.5 %, максимальне – 100 %, причому кількість користувачів, для яких точність розпізнавання становить менше 90 % становить 8 осіб, тобто 14.8 % від загальної кількості користувачів. Медіана становить 96.7 %, тобто точність розпізнавання для досвідчених користувачів фактично не змінилась. Отже, для досвідчених користувачів перехід до паролів, що містять великі і маленькі букви, цифри та символи не є необхідним з точки зору підвищення якості ідентифікації. Для недосвідчених користувачів подібний перехід є більш бажаним, оскільки кількість користувачів з точністю розпізнавання 90 % і більше зросла.

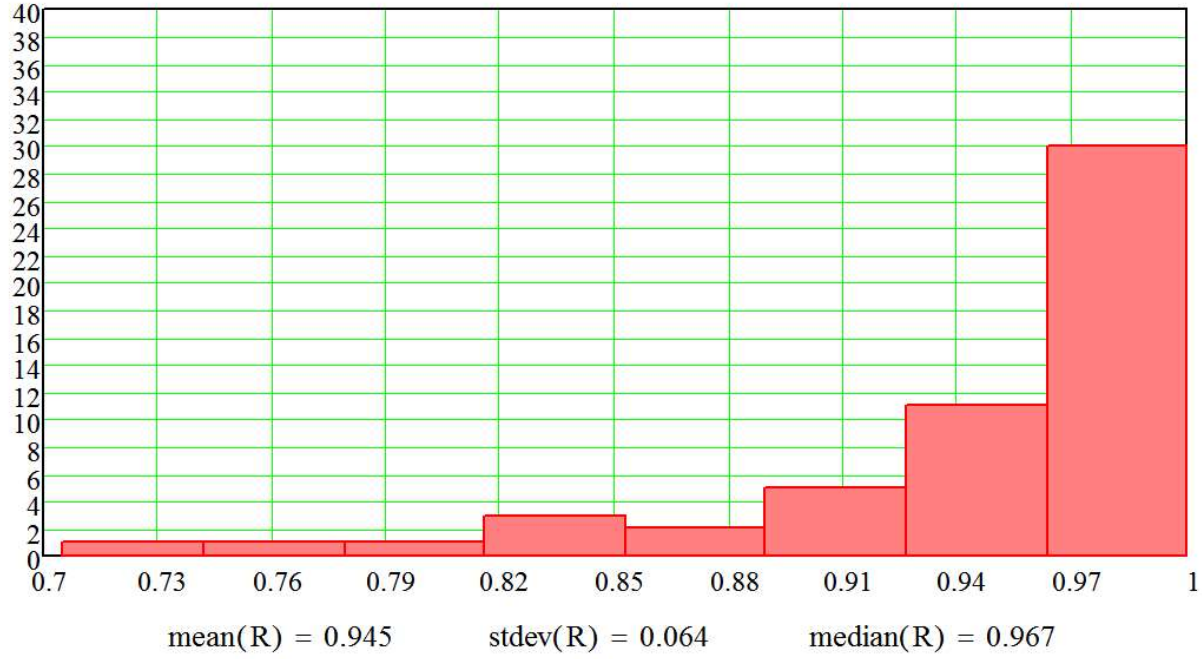


Рисунок 3.6 – Гістограма результатів мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за алгоритмом Random Forest

3.2.3. Дослідження датасету «MOBIKEY strong».

Вихідні дані для досліджень: алгоритм класифікації Random Forest. Точність класифікації перевірялась за вбудованим у віджет «Test and Score» алгоритмом 10-fold cross-validation.

Результати мультикласової класифікації (розпізнавання) користувачів наведено на рис. 3.7. Як можна побачити інтегральна точність класифікації знову практично не змінилась – 94.7 %.

На рис. 3.8 наведено гістограму результатів класифікації по кожному з користувачів. Як можна побачити, мінімальне значення точності розпізнавання становить 75 %, максимальне – 100 %, причому кількість користувачів, для яких точність розпізнавання становить менше 90 % знову становить 7 осіб, тобто 13 % від загальної кількості користувачів. Медіана становить 96.7 %, що збігається з результатами аналізу датесету «MOBIKEY logicalstrong».

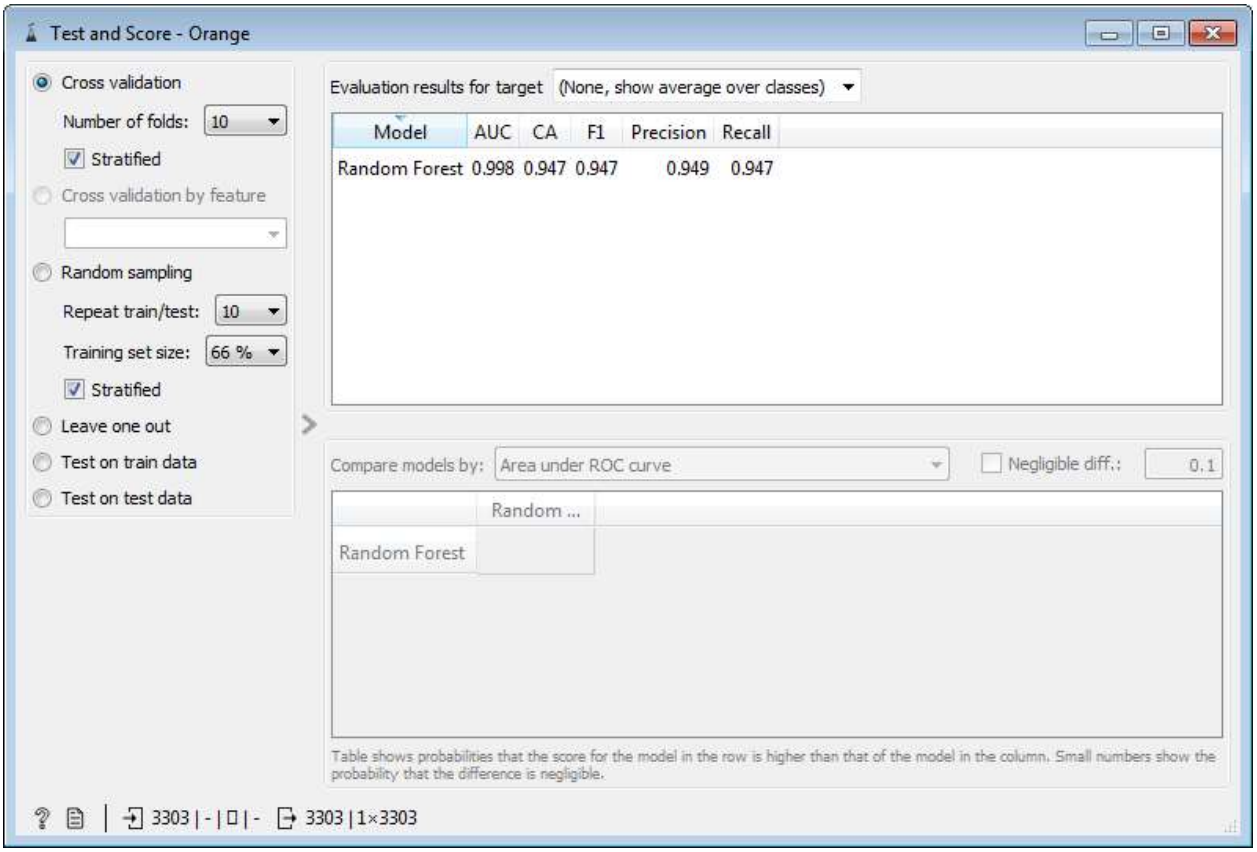


Рисунок 3.7 – Результати мультикласової класифікації користувачів датасету «MOBIKEY strong» за алгоритмом Random Forest

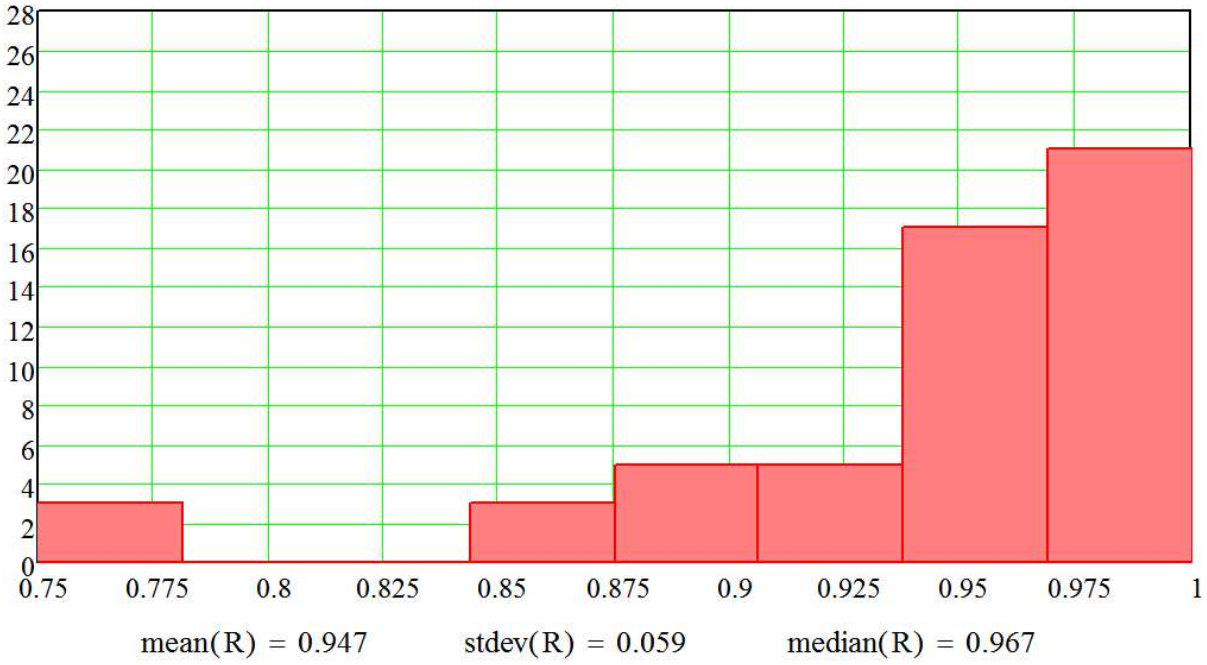


Рисунок 3.8 – Гістограма результатів мультикласової класифікації користувачів датасету «MOBIKEY strong» за алгоритмом Random Forest

Отже, враховуючи рівну довжину паролів – «Kktsf2!2014» та «.tie5Roanl» містять по 72 інформативних параметра – можна зробити висновок, що використання цифр в паролях не призводить до збільшення точності розпізнавання.

Використовуючи датасет «MOBIKEY strong» також можна провести порівняння точності розпізнавання користувача за його клавіатурним та сенсорним почерком. Для оцінки точності розпізнавання за клавіатурним почерком було використано датасет «Keystroke Dynamics Benchmark Data Set» [14], який містить часові параметри вводу парольної фрази «.tie5Roanl», яку набирали 51 користувач по 400 раз кожен. Дані в датасеті представлено у форматі Excel файлу та складаються з наступних полів: Subject – ідентифікатор користувача; sessionIndex – номер користувацької сесії (з 1 по 8); rep – порядковий номер спроби вводу паролю; H.dot, DD.dot.t, UD.dot.t, H.t, DD.t.i, UD.t.i, H.i, DD.i.e, UD.i.e, H.e, DD.e.five, UD.e.five, H.five, DD.five.Shift.r, UD.five.Shift.r, H.Shift.r, DD.Shift.r.o, UD.Shift.r.o, H.o, DD.o.a, UD.o.a, H.a, DD.a.n, UD.a.n, H.n, DD.n.l, UD.n.l, H.l, DD.l.enter, UD.l.enter, H.enter. Тут «H.A» – час натискання клавіші A, «DD.A.B» – час між натисканням клавіш A та B, «UD.A.B» – час між відпусканням клавіші A та натисканням клавіші B.

Результати мультикласової класифікації (розпізнавання) користувачів наведено на рис. 3.9. Як можна побачити інтегральна точність класифікації не змінилась – 93.4 %.

На рис. 3.10 наведено гістограму результатів класифікації по кожному з користувачів. Як можна побачити, мінімальне значення точності розпізнавання становить 74.5 %, максимальне – 100 %, причому кількість користувачів, для яких точність розпізнавання становить менше 90 % знову становить 13 осіб, тобто 25 % від загальної кількості користувачів. Медіана становить 95.5 %, що майже збігається з результатами аналізу датесетів «The MOBIKEY Keystroke Dynamics Password Database».

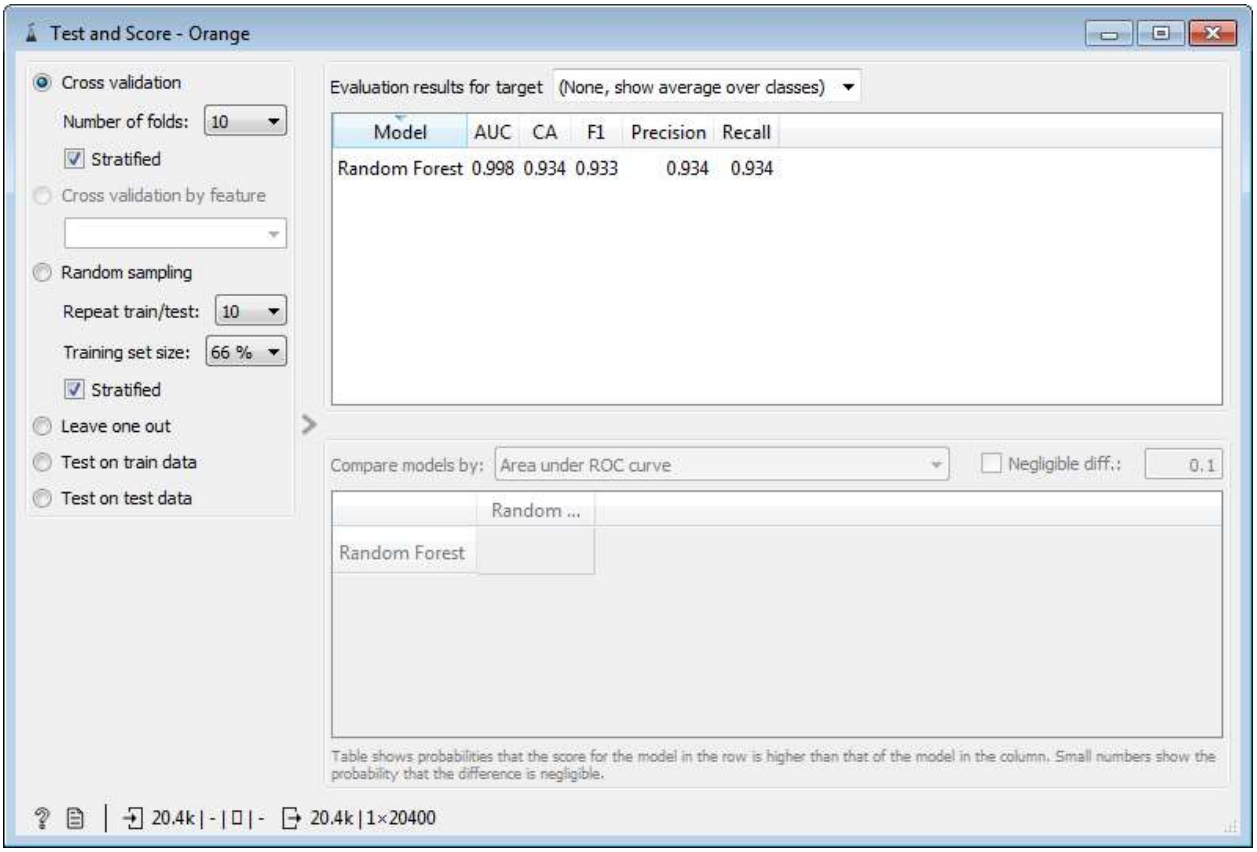


Рисунок 3.9 – Результати мультикласової класифікації користувачів датасету «Keystroke Dynamics Benchmark Data Set» за алгоритмом Random Forest

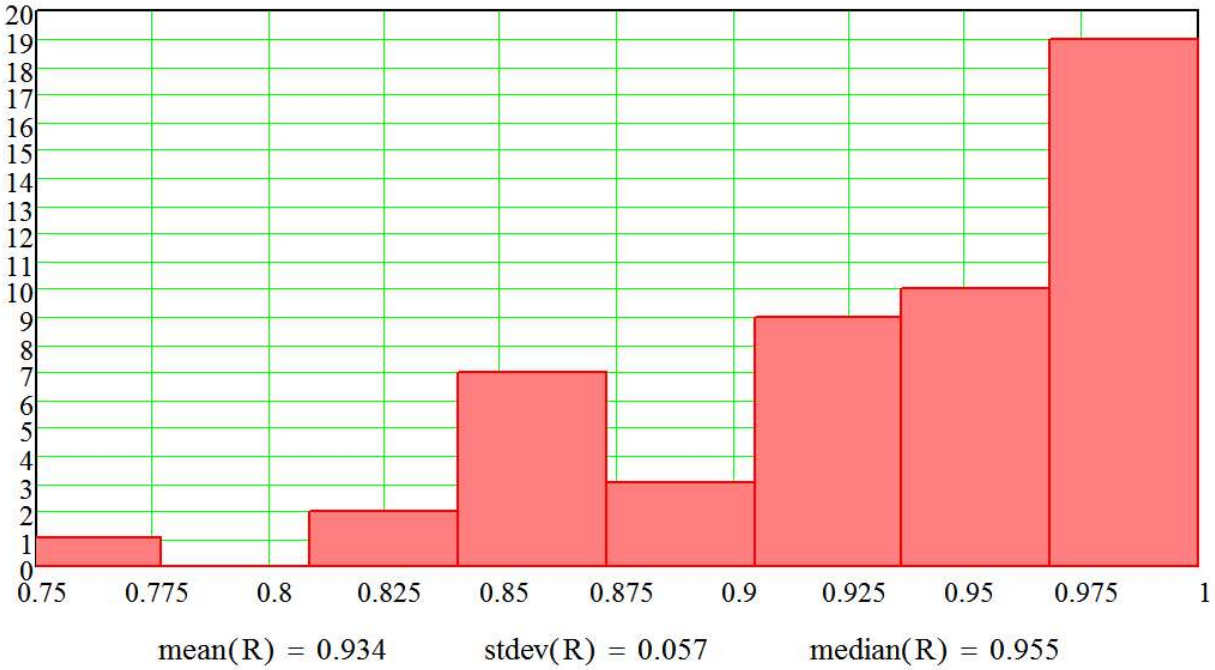


Рисунок 3.10 – Гістограма результатів мультикласової класифікації користувачів датасету «Keystroke Dynamics Benchmark Data Set» за алгоритмом Random Forest

Отже, сенсорний почерк здатен забезпечити точність ідентифікації, яка притаманна системам ідентифікації за клавіатурним почерком. Проте для забезпечення такої точності необхідно збирати більші масиви даних: пароль «.tie5Roanl» в дата сеті «MOBIKEY strong» містить 72 інформативних параметри, в той час як пароль «.tie5Roanl» в дата сеті «Keystroke Dynamics Benchmark Data Set» містить 31 інформативний параметр.

3.2.4. Результати двійкової класифікації користувачів з датасету «MOBIKEY logicalstrong».

Підвищити точність ідентифікації можна за рахунок побудови двійкової системи класифікації, тобто цільовому користувачу присвоюється клас 1, тобто «зареєстрований», а усім іншим користувачам – клас 2, тобто «зловмисник». Це можливо, оскільки на відміну від комп'ютера, де зареєстрованими користувачами можуть бути декілька людей, у мобільного пристрою завжди тільки один власник.

Для дослідження точності двійкової класифікації з датасету «MOBIKEY logicalstrong» було відібрано 9 користувачів «100», «203», «303», «503», «602», «605», «1004», «1203» та «1204», для яких точність мультикласової класифікації становила менше 95 % за всьома трьома дослідними датасетами. Отже, можна вважати, що це користувачі з найменш унікальним сенсорним почерком. Також для наочності отриманих результатів до аналізу було додано 3 користувачі «102», «302» та «1301», для яких точність мультикласової класифікації становила не менше 98 % за всьома трьома дослідними датасетами. Отже, можна вважати, що це користувачі з найбільш унікальним сенсорним почерком.

Таким чином, було проведено 66 експерименти, в яких розраховувалась точність класифікації по усіх можливих парах користувачів «100», «203», «303», «503», «602», «605», «1004», «1203», «1204», «102», «302» та «1301».

На рис. 3.11 наведено гістограму отриманих результатів. Як можна побачити, мінімальне значення точності розпізнавання становить 91.7 %,

максимальне – 100 %, причому кількість пар користувачів, для яких точність розпізнавання становить менше 95 % складає 4, тобто 6 % від загальної кількості можливих пар користувачів. А кількість пар користувачів, для яких точність розпізнавання становить менше 98 % складає 13, тобто 19.7 % від загальної кількості можливих пар користувачів. Медіана становить 100 %. Це можна пояснити практично сто відсотковою точністю класифікації у разі участі одного з користувачів з унікальним почерком. Таких пар було 30. Мінімальне значенням класифікації – 93.8 %. Останнім 29 парам відповідає точність класифікації 96.7 % і більше. Середнє значення точності класифікації – 99.5 %.

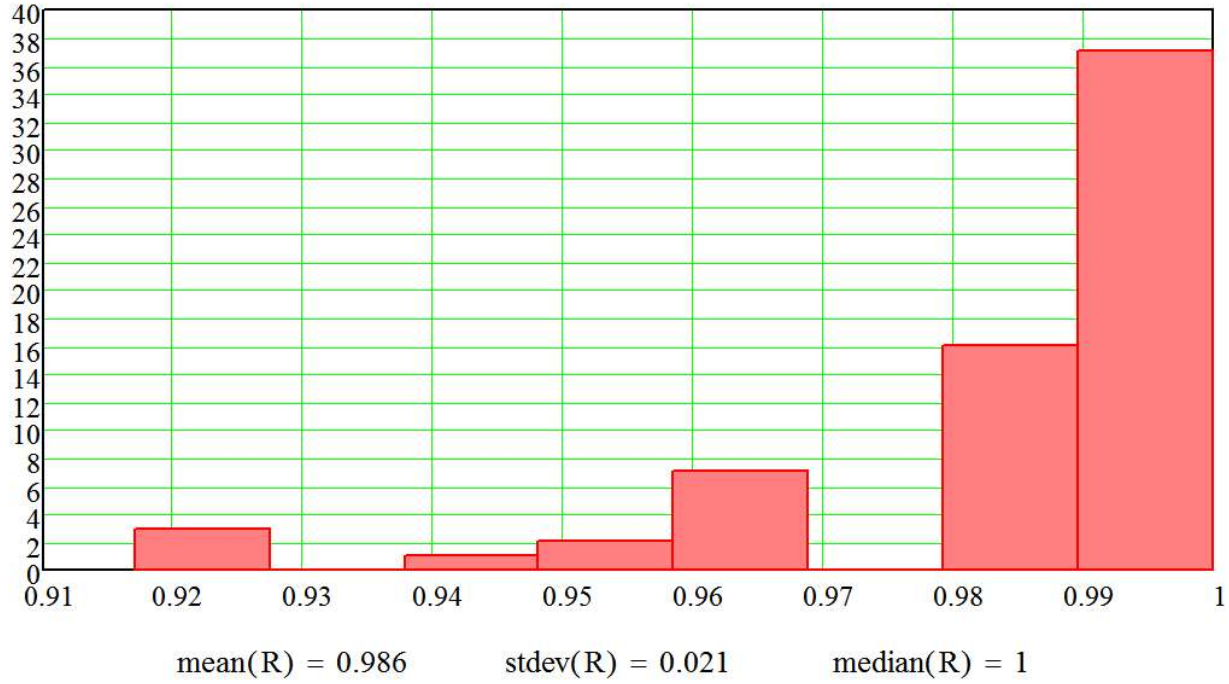


Рисунок 3.11 – Гістограма результатів двійкової класифікації
12 користувачів датасету ««MOBIKEY logicalstrong»»
за алгоритмом Random Forest

Отже, в дослідній системі ідентифікації за сенсорним почерком інтегральна (усереднена за всіма 12 користувачами) помилка FAR (випадок надання системою доступу неавторизованому користувачеві) становить 1.58 %. Враховуючи також той факт, що зловмисник апріорі має сформований сенсорний почерк, оскільки сфера його професійних навичок вимагає тривалого часу взаємодії зі смартфонами (один з пари користувачів вже має унікальний почерк),

то з плином часу значення помилки FAR буде зменшуватись, оскільки інформативні ознаки сенсорного почерку легітимного користувача також ставатимуть більш унікальними (обидва користувачі в парі мають унікальний почерк). За результатами проведених досліджень можна очікувати зменшення рівня помилки FAR до 1.2 %, тобто 12 пропусків зловмисника на 1000 спроб.

Рівень помилки FRR (доступ заборонений користувачеві, зареєстрованому в системі) за умови недосвідченого користувача може становити до 1.36 %. Якщо ж враховувати лише користувачів з унікальним почерком, то рівень помилки FRR зменшується до 0.54 %, тобто 54 недопуски верифікованого користувача на 10000 спроб.

3.2.5. Дослідження інформативності ознак сенсорного почерку користувачів з датасету «MOBIKEY logicalstrong».

Як було зазначено у п. 3.1 усі інформативні ознаки сенсорного почерку датасетів «The MOBIKEY Keystroke Dynamics Password Database» можна поділити на наступні класи:

1) часові параметри: holdtime – час натискання клавіші в процесі набору парольної фрази (HT); downdown – час між двома послідовними натисканнями на клавіші в процесі набору парольної фрази (DD); updown – час паузи між двома послідовними натисканнями на клавіші в процесі набору парольної фрази (UD);

2) параметри взаємодії з екраном: pressure – тиск на екран в процесі набору парольної фрази (P); fingerarea – розмір області на сенсорному екрані від пальця користувача в процесі набору парольної фрази (FA);

3) усереднені параметри взаємодії користувача зі смартфоном: meanholdtime – середнє значення часу натискання клавіш в процесі набору парольної фрази; mean downdown – середнє значення часу між двома послідовними натисканнями на клавіші в процесі набору парольної фрази; mean updown – середнє значення часу паузи між двома послідовними натисканнями

на клавіші в процесі набору парольної фрази; meanpressure – середнє значення тиску на екран в процесі набору парольної фрази (MP); meanfingerarea – середнє значення розміру області на сенсорному екрані від пальця користувача в процесі набору парольної фрази (MFA); meanxacceleration – середнє значення прискорення по вісі «X» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAX); meanyacceleration – середнє значення прискорення по вісі «Y» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAY); meanzacceleration – середнє значення прискорення по вісі «Z» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAZ); totaldistance – сума відстаней (у пікселях) між двома послідовними кнопками на віртуальній клавіатурі (TD); totaltime – час вводу парольної фрази (TT); velocity – швидкість, обчислювалась як частка відстані та загального часу.

На рис. 3.12 – 3.19 наведено результати мультикласової класифікації користувачів «100», «203», «303», «503», «602», «605», «1004», «1203», «1204», «102», «302» та «1301» за різними класами інформативних ознак.

Як можна побачити з рис. 3.12 – 3.19, єдиний клас інформативних ознак сенсорного почерку, що забезпечує точність класифікації вище 80 % це усереднені параметри взаємодії користувача зі смартфоном. Тут мінімальна точність класифікації – 83.3 %, максимальна – 100 %, середнє значення по 12 користувачам – 91.3 %, медіана – 91.2 %. Для класифікації за часовими параметрами маємо наступну картину: мінімальна точність класифікації – 63.9 %, максимальна – 100 %, середнє значення по 12 користувачам – 83 %, медіана – 86.1 %. Для класифікації за параметрами взаємодії з екраном маємо наступну картину: мінімальна точність класифікації – 29.5 %, максимальна – 96.8 %, середнє значення по 12 користувачам – 67.7 %, медіана – 71.1 %.

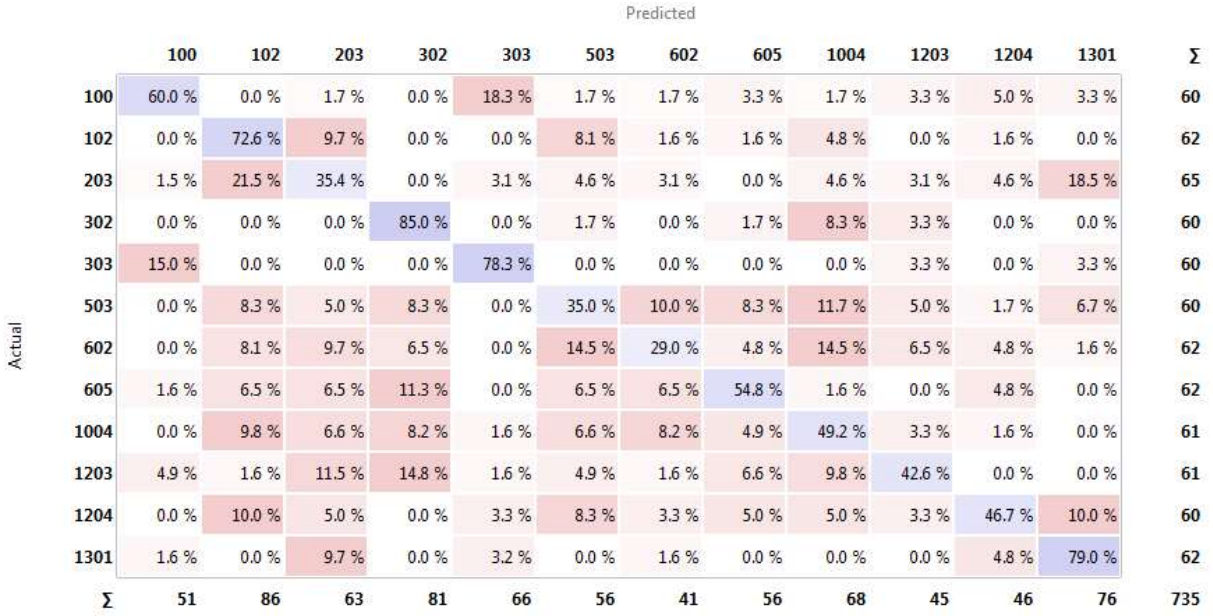


Рисунок 3.12 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 13-ма інформативними параметрами «holdtime»

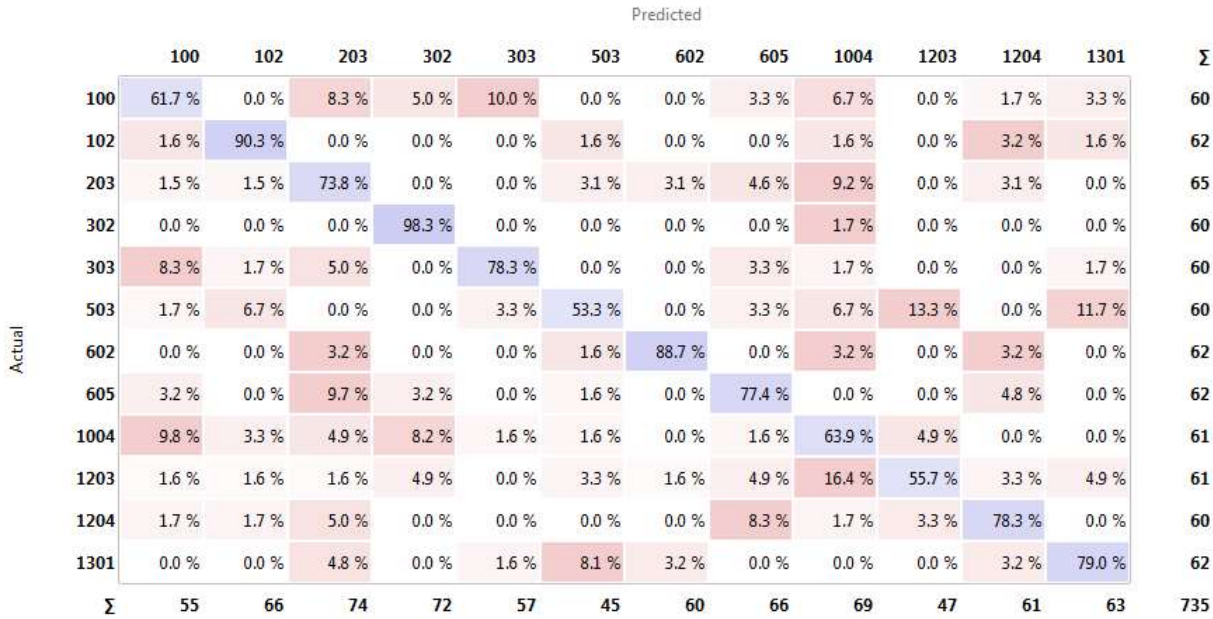
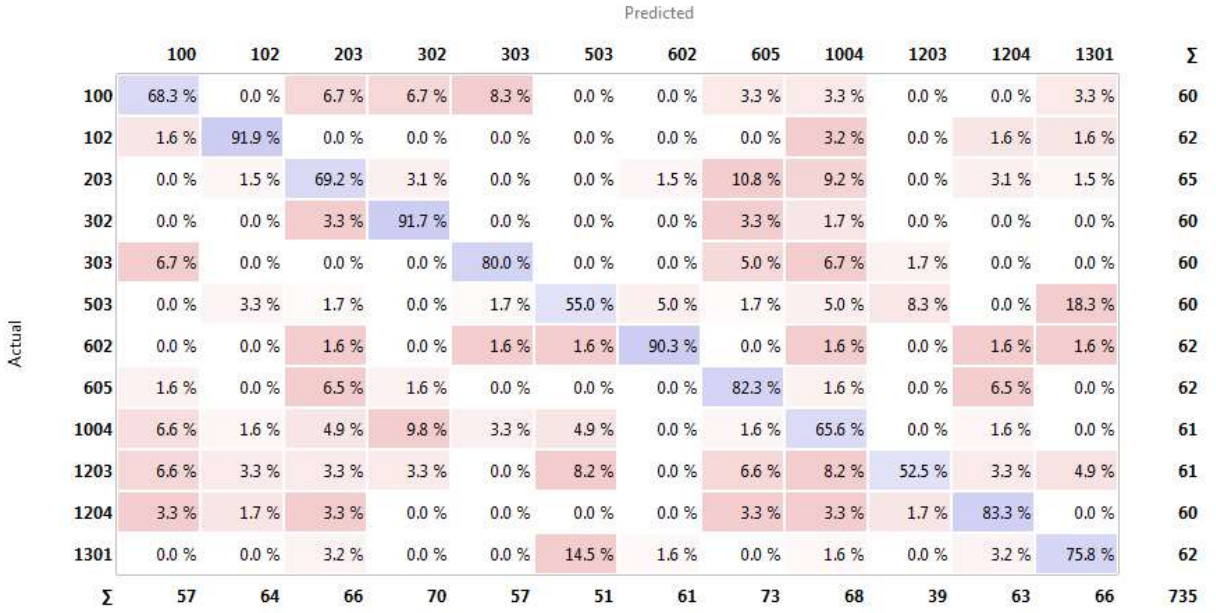


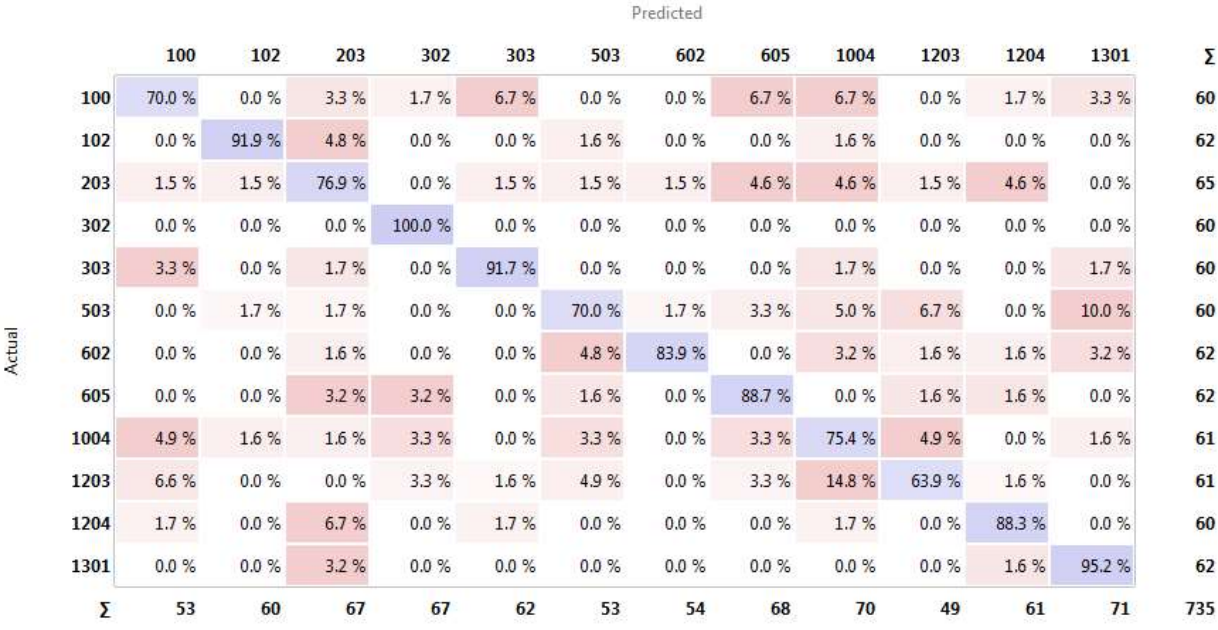
Рисунок 3.13 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 12-ма інформативними параметрами «downdown»



Predicted

Actual	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	68.3 %	0.0 %	6.7 %	6.7 %	8.3 %	0.0 %	0.0 %	3.3 %	3.3 %	0.0 %	0.0 %	3.3 %	60
102	1.6 %	91.9 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	3.2 %	0.0 %	1.6 %	1.6 %	62
203	0.0 %	1.5 %	69.2 %	3.1 %	0.0 %	0.0 %	1.5 %	10.8 %	9.2 %	0.0 %	3.1 %	1.5 %	65
302	0.0 %	0.0 %	3.3 %	91.7 %	0.0 %	0.0 %	0.0 %	3.3 %	1.7 %	0.0 %	0.0 %	0.0 %	60
303	6.7 %	0.0 %	0.0 %	0.0 %	80.0 %	0.0 %	0.0 %	5.0 %	6.7 %	1.7 %	0.0 %	0.0 %	60
503	0.0 %	3.3 %	1.7 %	0.0 %	1.7 %	55.0 %	5.0 %	1.7 %	5.0 %	8.3 %	0.0 %	18.3 %	60
602	0.0 %	0.0 %	1.6 %	0.0 %	1.6 %	1.6 %	90.3 %	0.0 %	1.6 %	0.0 %	1.6 %	1.6 %	62
605	1.6 %	0.0 %	6.5 %	1.6 %	0.0 %	0.0 %	0.0 %	82.3 %	1.6 %	0.0 %	6.5 %	0.0 %	62
1004	6.6 %	1.6 %	4.9 %	9.8 %	3.3 %	4.9 %	0.0 %	1.6 %	65.6 %	0.0 %	1.6 %	0.0 %	61
1203	6.6 %	3.3 %	3.3 %	3.3 %	0.0 %	8.2 %	0.0 %	6.6 %	8.2 %	52.5 %	3.3 %	4.9 %	61
1204	3.3 %	1.7 %	3.3 %	0.0 %	0.0 %	0.0 %	0.0 %	3.3 %	3.3 %	1.7 %	83.3 %	0.0 %	60
1301	0.0 %	0.0 %	3.2 %	0.0 %	0.0 %	14.5 %	1.6 %	0.0 %	1.6 %	0.0 %	3.2 %	75.8 %	62
Σ	57	64	66	70	57	51	61	73	68	39	63	66	735

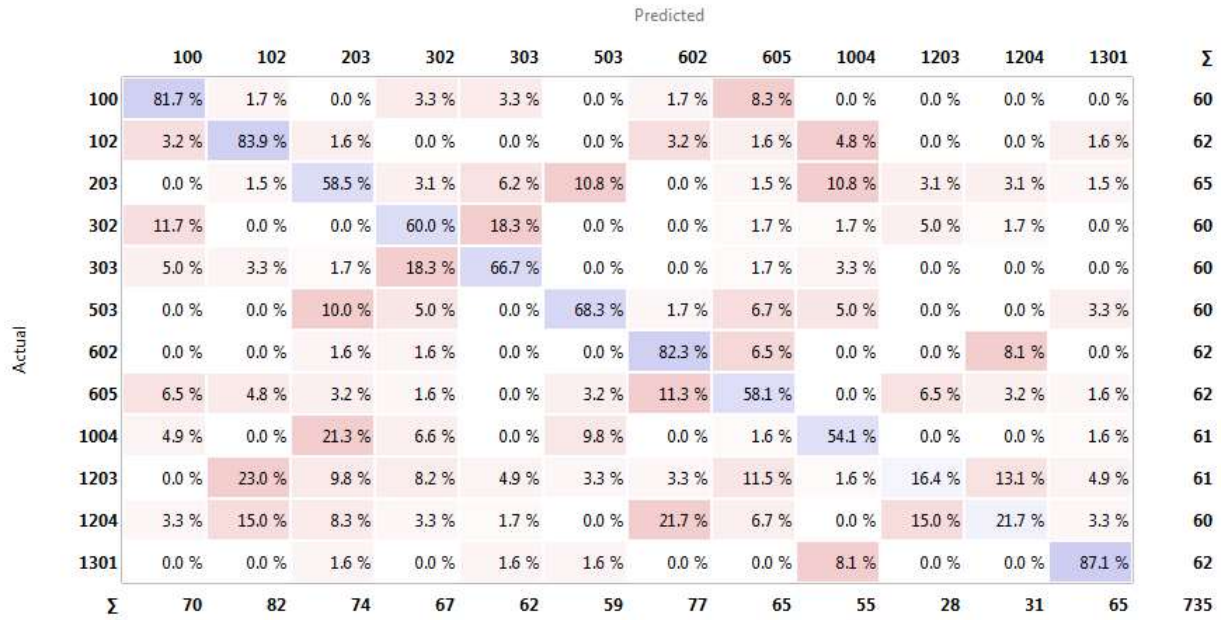
Рисунок 3.14 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 12-ма інформативними параметрами «updown»



Predicted

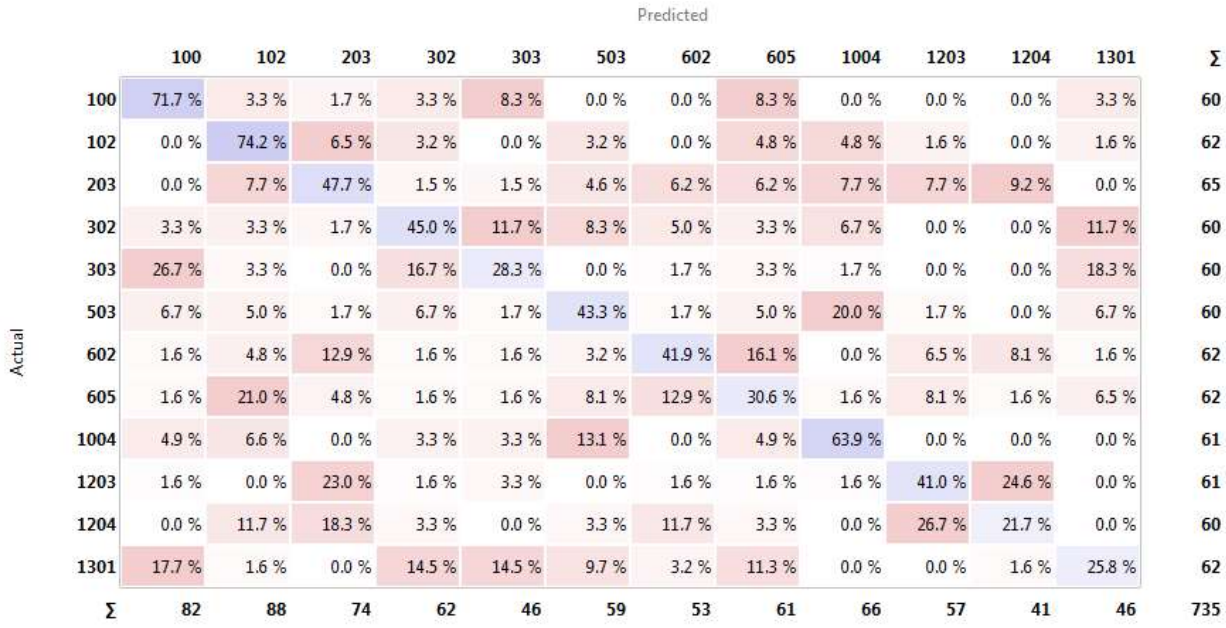
Actual	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	70.0 %	0.0 %	3.3 %	1.7 %	6.7 %	0.0 %	0.0 %	6.7 %	6.7 %	0.0 %	1.7 %	3.3 %	60
102	0.0 %	91.9 %	4.8 %	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	0.0 %	62
203	1.5 %	1.5 %	76.9 %	0.0 %	1.5 %	1.5 %	1.5 %	4.6 %	4.6 %	1.5 %	4.6 %	0.0 %	65
302	0.0 %	0.0 %	0.0 %	100.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
303	3.3 %	0.0 %	1.7 %	0.0 %	91.7 %	0.0 %	0.0 %	0.0 %	1.7 %	0.0 %	0.0 %	1.7 %	60
503	0.0 %	1.7 %	1.7 %	0.0 %	0.0 %	70.0 %	1.7 %	3.3 %	5.0 %	6.7 %	0.0 %	10.0 %	60
602	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	4.8 %	83.9 %	0.0 %	3.2 %	1.6 %	1.6 %	3.2 %	62
605	0.0 %	0.0 %	3.2 %	3.2 %	0.0 %	1.6 %	0.0 %	88.7 %	0.0 %	1.6 %	1.6 %	0.0 %	62
1004	4.9 %	1.6 %	1.6 %	3.3 %	0.0 %	3.3 %	0.0 %	3.3 %	75.4 %	4.9 %	0.0 %	1.6 %	61
1203	6.6 %	0.0 %	0.0 %	3.3 %	1.6 %	4.9 %	0.0 %	3.3 %	14.8 %	63.9 %	1.6 %	0.0 %	61
1204	1.7 %	0.0 %	6.7 %	0.0 %	1.7 %	0.0 %	0.0 %	0.0 %	1.7 %	0.0 %	88.3 %	0.0 %	60
1301	0.0 %	0.0 %	3.2 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	1.6 %	95.2 %	62
Σ	53	60	67	67	62	53	54	68	70	49	61	71	735

Рисунок 3.15 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 37-ма часовими інформативними параметрами



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	81.7 %	1.7 %	0.0 %	3.3 %	3.3 %	0.0 %	1.7 %	8.3 %	0.0 %	0.0 %	0.0 %	0.0 %	60
102	3.2 %	83.9 %	1.6 %	0.0 %	0.0 %	0.0 %	3.2 %	1.6 %	4.8 %	0.0 %	0.0 %	1.6 %	62
203	0.0 %	1.5 %	58.5 %	3.1 %	6.2 %	10.8 %	0.0 %	1.5 %	10.8 %	3.1 %	3.1 %	1.5 %	65
302	11.7 %	0.0 %	0.0 %	60.0 %	18.3 %	0.0 %	0.0 %	1.7 %	1.7 %	5.0 %	1.7 %	0.0 %	60
303	5.0 %	3.3 %	1.7 %	18.3 %	66.7 %	0.0 %	0.0 %	1.7 %	3.3 %	0.0 %	0.0 %	0.0 %	60
503	0.0 %	0.0 %	10.0 %	5.0 %	0.0 %	68.3 %	1.7 %	6.7 %	5.0 %	0.0 %	0.0 %	3.3 %	60
602	0.0 %	0.0 %	1.6 %	1.6 %	0.0 %	0.0 %	82.3 %	6.5 %	0.0 %	0.0 %	8.1 %	0.0 %	62
605	6.5 %	4.8 %	3.2 %	1.6 %	0.0 %	3.2 %	11.3 %	58.1 %	0.0 %	6.5 %	3.2 %	1.6 %	62
1004	4.9 %	0.0 %	21.3 %	6.6 %	0.0 %	9.8 %	0.0 %	1.6 %	54.1 %	0.0 %	0.0 %	1.6 %	61
1203	0.0 %	23.0 %	9.8 %	8.2 %	4.9 %	3.3 %	3.3 %	11.5 %	1.6 %	16.4 %	13.1 %	4.9 %	61
1204	3.3 %	15.0 %	8.3 %	3.3 %	1.7 %	0.0 %	21.7 %	6.7 %	0.0 %	15.0 %	21.7 %	3.3 %	60
1301	0.0 %	0.0 %	1.6 %	0.0 %	1.6 %	1.6 %	0.0 %	0.0 %	8.1 %	0.0 %	0.0 %	87.1 %	62
Σ	70	82	74	67	62	59	77	65	55	28	31	65	735

Рисунок 3.16 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 13-ма інформативним параметром «pressure»



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	71.7 %	3.3 %	1.7 %	3.3 %	8.3 %	0.0 %	0.0 %	8.3 %	0.0 %	0.0 %	0.0 %	3.3 %	60
102	0.0 %	74.2 %	6.5 %	3.2 %	0.0 %	3.2 %	0.0 %	4.8 %	4.8 %	1.6 %	0.0 %	1.6 %	62
203	0.0 %	7.7 %	47.7 %	1.5 %	1.5 %	4.6 %	6.2 %	6.2 %	7.7 %	7.7 %	9.2 %	0.0 %	65
302	3.3 %	3.3 %	1.7 %	45.0 %	11.7 %	8.3 %	5.0 %	3.3 %	6.7 %	0.0 %	0.0 %	11.7 %	60
303	26.7 %	3.3 %	0.0 %	16.7 %	28.3 %	0.0 %	1.7 %	3.3 %	1.7 %	0.0 %	0.0 %	18.3 %	60
503	6.7 %	5.0 %	1.7 %	6.7 %	1.7 %	43.3 %	1.7 %	5.0 %	20.0 %	1.7 %	0.0 %	6.7 %	60
602	1.6 %	4.8 %	12.9 %	1.6 %	1.6 %	3.2 %	41.9 %	16.1 %	0.0 %	6.5 %	8.1 %	1.6 %	62
605	1.6 %	21.0 %	4.8 %	1.6 %	1.6 %	8.1 %	12.9 %	30.6 %	1.6 %	8.1 %	1.6 %	6.5 %	62
1004	4.9 %	6.6 %	0.0 %	3.3 %	3.3 %	13.1 %	0.0 %	4.9 %	63.9 %	0.0 %	0.0 %	0.0 %	61
1203	1.6 %	0.0 %	23.0 %	1.6 %	3.3 %	0.0 %	1.6 %	1.6 %	1.6 %	41.0 %	24.6 %	0.0 %	61
1204	0.0 %	11.7 %	18.3 %	3.3 %	0.0 %	3.3 %	11.7 %	3.3 %	0.0 %	26.7 %	21.7 %	0.0 %	60
1301	17.7 %	1.6 %	0.0 %	14.5 %	14.5 %	9.7 %	3.2 %	11.3 %	0.0 %	0.0 %	1.6 %	25.8 %	62
Σ	82	88	74	62	46	59	53	61	66	57	41	46	735

Рисунок 3.17 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 13-ма інформативним параметром «fingerarea»

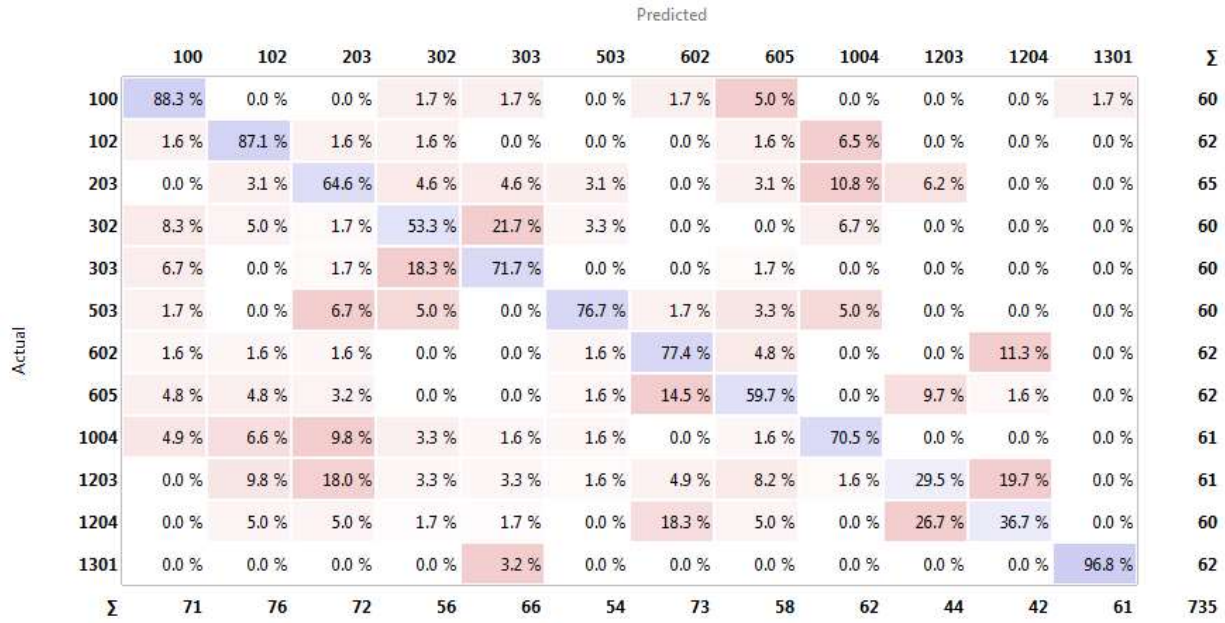


Рисунок 3.18 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за 26-ма параметрами взаємодії з екраном

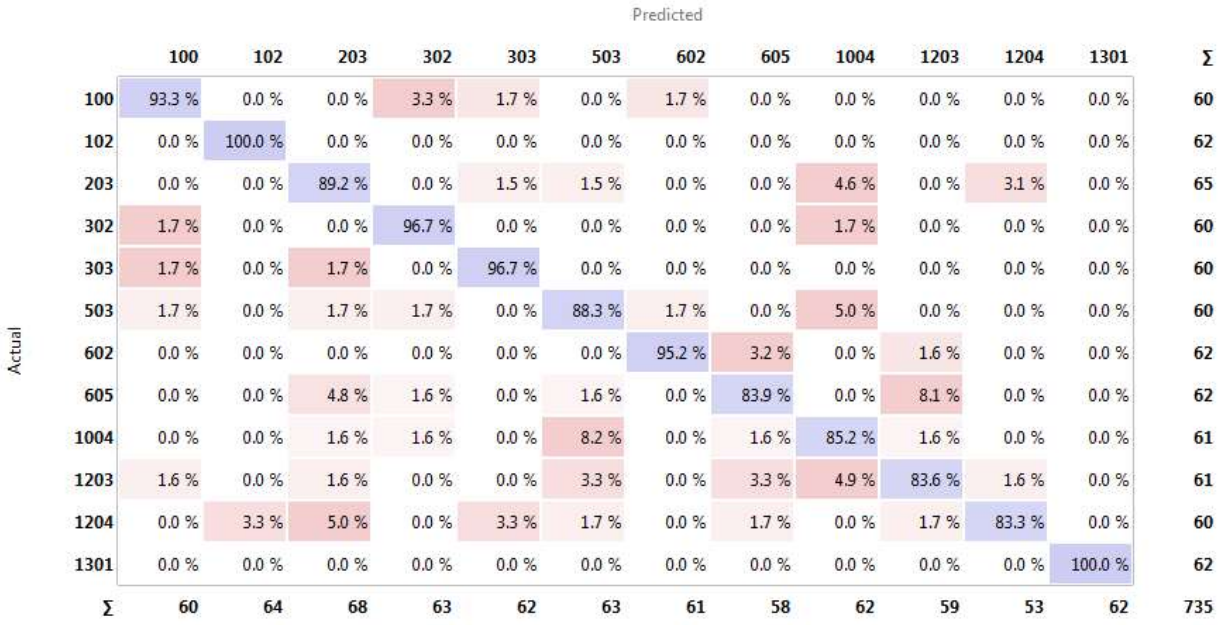


Рисунок 3.19 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за усередненими параметрами взаємодії користувача зі смартфоном

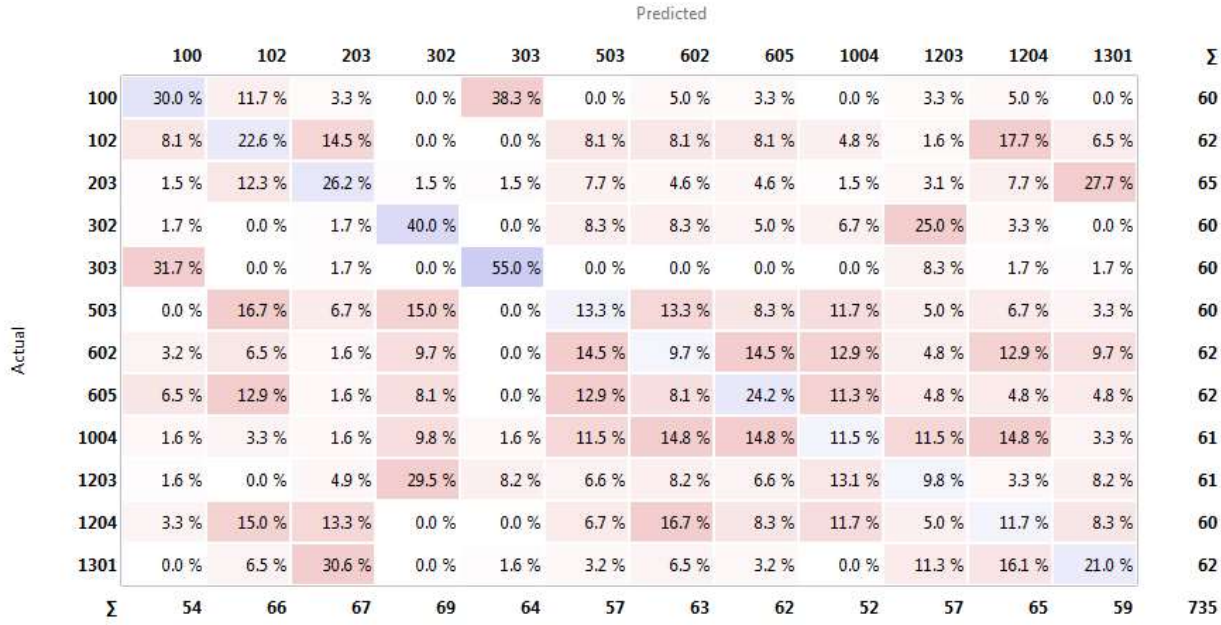
На рис. 3.20 – 3.28 наведено результати мультикласової класифікації користувачів «100», «203», «303», «503», «602», «605», «1004», «1203», «1204», «102», «302» та «1301» за кожною з інформативних ознак з класу усереднених параметрів взаємодії користувача зі смартфоном.

Як можна побачити з рис. 3.20 – 3.28, найменш інформативними є параметри «totaltime» з максимальною точністю 29 %, «meanupdown» з максимальною точністю 27.4 та «totaldistance» з максимальною точністю 20 %.

Таблиця 3.1 – Ранжування усереднених параметрів взаємодії користувача зі смартфоном за ранговими критеріями

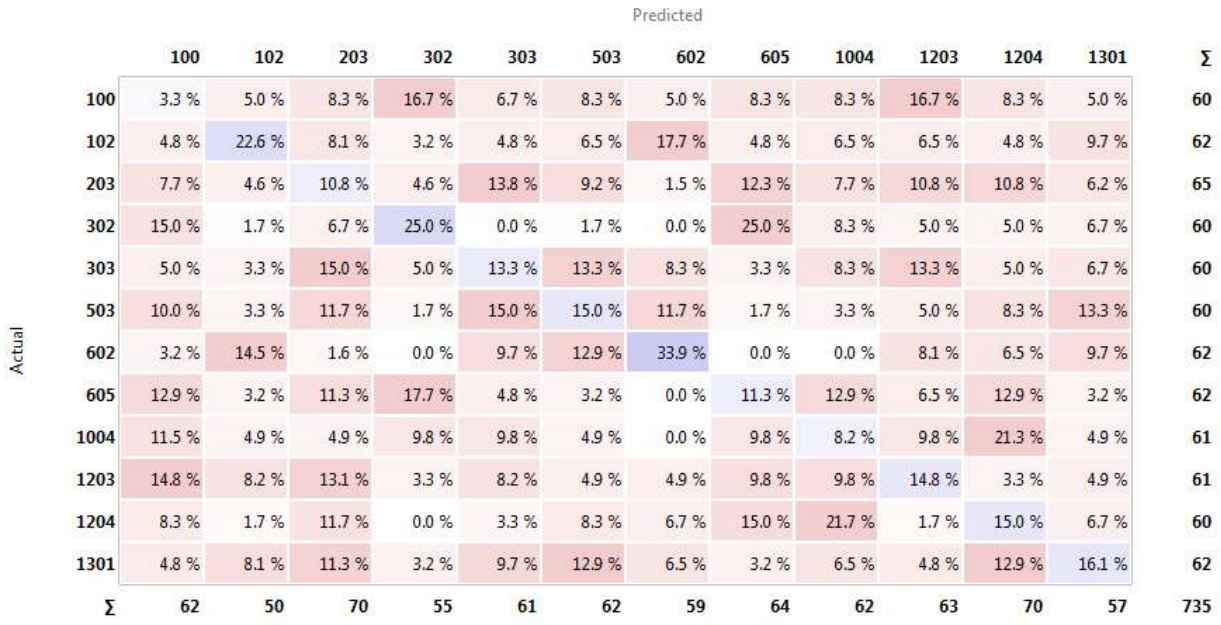
	Info. gain	**Gain ratio**	**Gini**	**ANOVA**	**χ^2**	**ReliefF**	**FCBF**	**Сумарна вага**
meanholdtime	1.000	1.000	1.000	1.000	0.940	1.000	1.000	6.940
meanfingerarea	0.777	0.777	0.834	0.553	1.000	0.385	0.806	5.131
velocity	0.653	0.653	0.636	0.745	0.809	0.597	0.707	4.801
meanzaccelaration	0.612	0.612	0.620	0.334	0.523	0.620	0.676	3.998
meanpressure	0.533	0.533	0.531	0.622	0.569	0.431	0.617	3.836
meanyaccelaration	0.596	0.596	0.603	0.256	0.416	0.698	0.000	3.165
meanxaccelaration	0.450	0.450	0.456	0.271	0.377	0.343	0.558	2.904
meanupdown	0.225	0.225	0.251	0.000	0.187	0.003	0.000	0.892
totaltime	0.176	0.176	0.186	0.029	0.203	0.000	0.000	0.771
meandowndown	0.175	0.175	0.184	0.028	0.195	0.000	0.000	0.758
totaldistance	0.000	0.000	0.000	0.076	0.000	0.103	0.273	0.453

Це підтверджує і табл. 3.1, де наведено результати пошуку найінформативніших з дослідних параметрів за допомогою інструменту «Rank» програмного середовища Orange. Цей інструмент розраховує коефіцієнт впливу кожної ознаки на формування дослідного класу. Більші коефіцієнти впливу вказують на більшу інформативність тієї чи іншої ознаки. Як можна бачити, найінформативнішими параметрами є «meanholdtime» з сумарною вагою 6.940, «meanfingerarea» з сумарною вагою 5.131, «velocity» з сумарною вагою 4.801, «meanzaccelaration» з сумарною вагою 3.998 та «meanpressure» з сумарною вагою 3.836. До малоінформативних параметрів можна віднести також «meanupdown» з сумарною вагою 0.892.



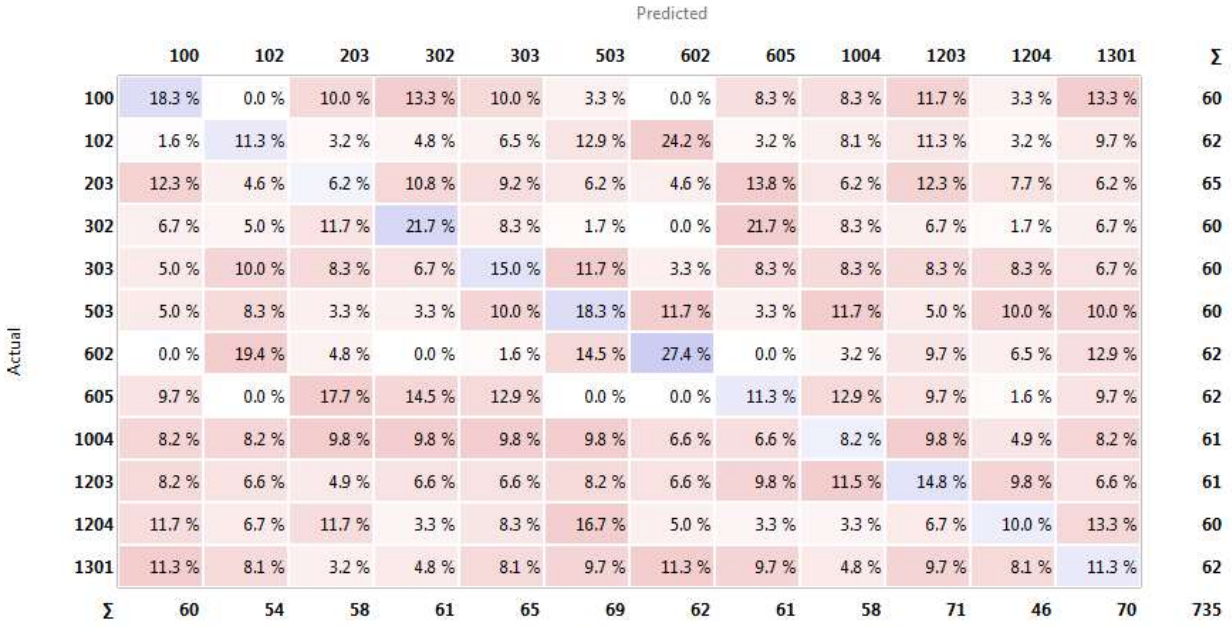
Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	30.0 %	11.7 %	3.3 %	0.0 %	38.3 %	0.0 %	5.0 %	3.3 %	0.0 %	3.3 %	5.0 %	0.0 %	60
102	8.1 %	22.6 %	14.5 %	0.0 %	0.0 %	8.1 %	8.1 %	8.1 %	4.8 %	1.6 %	17.7 %	6.5 %	62
203	1.5 %	12.3 %	26.2 %	1.5 %	1.5 %	7.7 %	4.6 %	4.6 %	1.5 %	3.1 %	7.7 %	27.7 %	65
302	1.7 %	0.0 %	1.7 %	40.0 %	0.0 %	8.3 %	8.3 %	5.0 %	6.7 %	25.0 %	3.3 %	0.0 %	60
303	31.7 %	0.0 %	1.7 %	0.0 %	55.0 %	0.0 %	0.0 %	0.0 %	0.0 %	8.3 %	1.7 %	1.7 %	60
503	0.0 %	16.7 %	6.7 %	15.0 %	0.0 %	13.3 %	13.3 %	8.3 %	11.7 %	5.0 %	6.7 %	3.3 %	60
602	3.2 %	6.5 %	1.6 %	9.7 %	0.0 %	14.5 %	9.7 %	14.5 %	12.9 %	4.8 %	12.9 %	9.7 %	62
605	6.5 %	12.9 %	1.6 %	8.1 %	0.0 %	12.9 %	8.1 %	24.2 %	11.3 %	4.8 %	4.8 %	4.8 %	62
1004	1.6 %	3.3 %	1.6 %	9.8 %	1.6 %	11.5 %	14.8 %	14.8 %	11.5 %	11.5 %	14.8 %	3.3 %	61
1203	1.6 %	0.0 %	4.9 %	29.5 %	8.2 %	6.6 %	8.2 %	6.6 %	13.1 %	9.8 %	3.3 %	8.2 %	61
1204	3.3 %	15.0 %	13.3 %	0.0 %	0.0 %	6.7 %	16.7 %	8.3 %	11.7 %	5.0 %	11.7 %	8.3 %	60
1301	0.0 %	6.5 %	30.6 %	0.0 %	1.6 %	3.2 %	6.5 %	3.2 %	0.0 %	11.3 %	16.1 %	21.0 %	62
Σ	54	66	67	69	64	57	63	62	52	57	65	59	735

Рисунок 3.20 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «meanholdtime»



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	3.3 %	5.0 %	8.3 %	16.7 %	6.7 %	8.3 %	5.0 %	8.3 %	8.3 %	16.7 %	8.3 %	5.0 %	60
102	4.8 %	22.6 %	8.1 %	3.2 %	4.8 %	6.5 %	17.7 %	4.8 %	6.5 %	6.5 %	4.8 %	9.7 %	62
203	7.7 %	4.6 %	10.8 %	4.6 %	13.8 %	9.2 %	1.5 %	12.3 %	7.7 %	10.8 %	10.8 %	6.2 %	65
302	15.0 %	1.7 %	6.7 %	25.0 %	0.0 %	1.7 %	0.0 %	25.0 %	8.3 %	5.0 %	5.0 %	6.7 %	60
303	5.0 %	3.3 %	15.0 %	5.0 %	13.3 %	13.3 %	8.3 %	3.3 %	8.3 %	13.3 %	5.0 %	6.7 %	60
503	10.0 %	3.3 %	11.7 %	1.7 %	15.0 %	15.0 %	11.7 %	1.7 %	3.3 %	5.0 %	8.3 %	13.3 %	60
602	3.2 %	14.5 %	1.6 %	0.0 %	9.7 %	12.9 %	33.9 %	0.0 %	0.0 %	8.1 %	6.5 %	9.7 %	62
605	12.9 %	3.2 %	11.3 %	17.7 %	4.8 %	3.2 %	0.0 %	11.3 %	12.9 %	6.5 %	12.9 %	3.2 %	62
1004	11.5 %	4.9 %	4.9 %	9.8 %	9.8 %	4.9 %	0.0 %	9.8 %	8.2 %	9.8 %	21.3 %	4.9 %	61
1203	14.8 %	8.2 %	13.1 %	3.3 %	8.2 %	4.9 %	4.9 %	9.8 %	9.8 %	14.8 %	3.3 %	4.9 %	61
1204	8.3 %	1.7 %	11.7 %	0.0 %	3.3 %	8.3 %	6.7 %	15.0 %	21.7 %	1.7 %	15.0 %	6.7 %	60
1301	4.8 %	8.1 %	11.3 %	3.2 %	9.7 %	12.9 %	6.5 %	3.2 %	6.5 %	4.8 %	12.9 %	16.1 %	62
Σ	62	50	70	55	61	62	59	64	62	63	70	57	735

Рисунок 3.21 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «meandowndown»

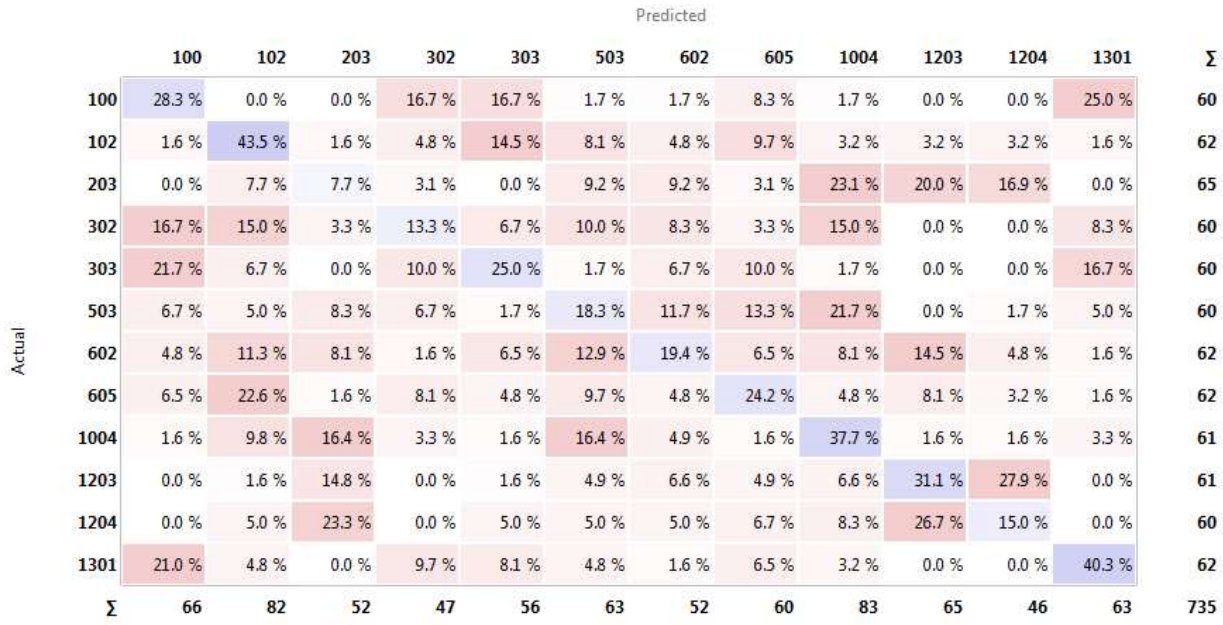


Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	18.3 %	0.0 %	10.0 %	13.3 %	10.0 %	3.3 %	0.0 %	8.3 %	8.3 %	11.7 %	3.3 %	13.3 %	60
102	1.6 %	11.3 %	3.2 %	4.8 %	6.5 %	12.9 %	24.2 %	3.2 %	8.1 %	11.3 %	3.2 %	9.7 %	62
203	12.3 %	4.6 %	6.2 %	10.8 %	9.2 %	6.2 %	4.6 %	13.8 %	6.2 %	12.3 %	7.7 %	6.2 %	65
302	6.7 %	5.0 %	11.7 %	21.7 %	8.3 %	1.7 %	0.0 %	21.7 %	8.3 %	6.7 %	1.7 %	6.7 %	60
303	5.0 %	10.0 %	8.3 %	6.7 %	15.0 %	11.7 %	3.3 %	8.3 %	8.3 %	8.3 %	8.3 %	6.7 %	60
503	5.0 %	8.3 %	3.3 %	3.3 %	10.0 %	18.3 %	11.7 %	3.3 %	11.7 %	5.0 %	10.0 %	10.0 %	60
602	0.0 %	19.4 %	4.8 %	0.0 %	1.6 %	14.5 %	27.4 %	0.0 %	3.2 %	9.7 %	6.5 %	12.9 %	62
605	9.7 %	0.0 %	17.7 %	14.5 %	12.9 %	0.0 %	0.0 %	11.3 %	12.9 %	9.7 %	1.6 %	9.7 %	62
1004	8.2 %	8.2 %	9.8 %	9.8 %	9.8 %	9.8 %	6.6 %	6.6 %	8.2 %	9.8 %	4.9 %	8.2 %	61
1203	8.2 %	6.6 %	4.9 %	6.6 %	6.6 %	8.2 %	6.6 %	9.8 %	11.5 %	14.8 %	9.8 %	6.6 %	61
1204	11.7 %	6.7 %	11.7 %	3.3 %	8.3 %	16.7 %	5.0 %	3.3 %	3.3 %	6.7 %	10.0 %	13.3 %	60
1301	11.3 %	8.1 %	3.2 %	4.8 %	8.1 %	9.7 %	11.3 %	9.7 %	4.8 %	9.7 %	8.1 %	11.3 %	62
Σ	60	54	58	61	65	69	62	61	58	71	46	70	735

Рисунок 3.22 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «meanupdown»

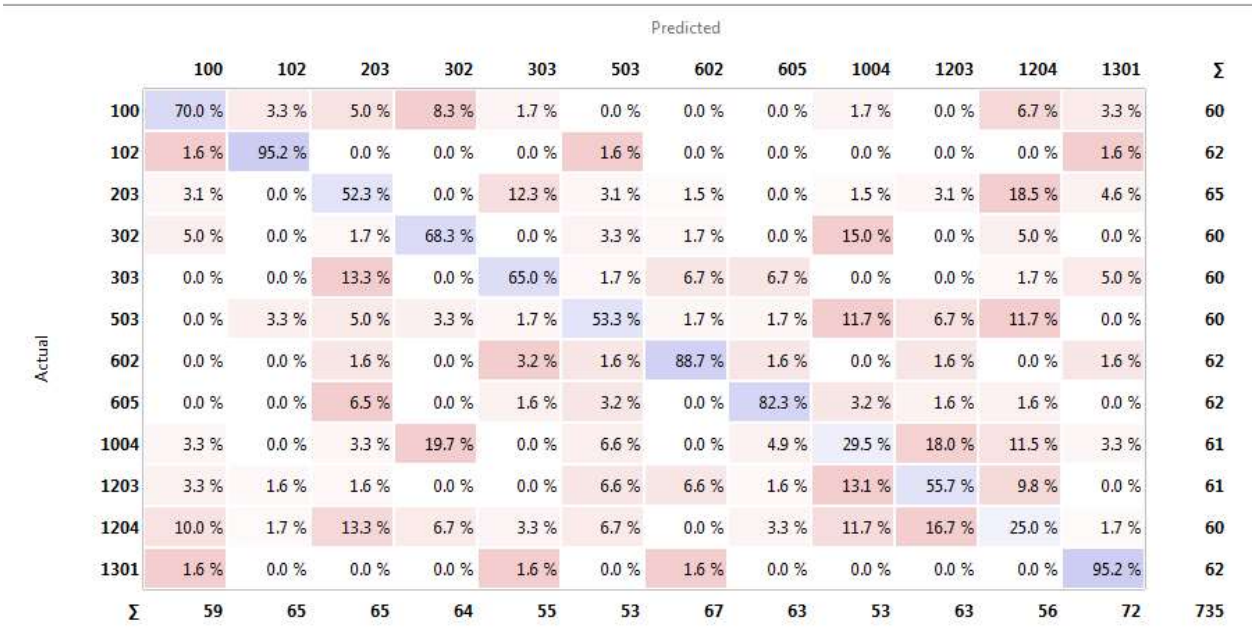
Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	35.0 %	8.3 %	0.0 %	11.7 %	1.7 %	5.0 %	18.3 %	10.0 %	5.0 %	3.3 %	1.7 %	0.0 %	60
102	6.5 %	9.7 %	16.1 %	6.5 %	6.5 %	6.5 %	3.2 %	8.1 %	8.1 %	6.5 %	11.3 %	11.3 %	62
203	0.0 %	13.8 %	13.8 %	4.6 %	12.3 %	9.2 %	1.5 %	1.5 %	21.5 %	7.7 %	9.2 %	4.6 %	65
302	16.7 %	3.3 %	6.7 %	3.3 %	11.7 %	5.0 %	15.0 %	13.3 %	3.3 %	11.7 %	10.0 %	0.0 %	60
303	3.3 %	8.3 %	10.0 %	11.7 %	16.7 %	3.3 %	5.0 %	8.3 %	5.0 %	13.3 %	15.0 %	0.0 %	60
503	1.7 %	10.0 %	16.7 %	1.7 %	3.3 %	18.3 %	8.3 %	8.3 %	15.0 %	6.7 %	3.3 %	6.7 %	60
602	25.8 %	3.2 %	1.6 %	12.9 %	9.7 %	8.1 %	6.5 %	19.4 %	4.8 %	4.8 %	3.2 %	0.0 %	62
605	11.3 %	11.3 %	1.6 %	14.5 %	9.7 %	12.9 %	8.1 %	17.7 %	3.2 %	8.1 %	1.6 %	0.0 %	62
1004	3.3 %	6.6 %	18.0 %	4.9 %	4.9 %	14.8 %	6.6 %	3.3 %	14.8 %	9.8 %	8.2 %	4.9 %	61
1203	6.6 %	3.3 %	8.2 %	6.6 %	23.0 %	6.6 %	6.6 %	9.8 %	8.2 %	9.8 %	6.6 %	4.9 %	61
1204	1.7 %	10.0 %	11.7 %	13.3 %	13.3 %	6.7 %	5.0 %	11.7 %	8.3 %	8.3 %	5.0 %	5.0 %	60
1301	0.0 %	14.5 %	3.2 %	0.0 %	0.0 %	6.5 %	0.0 %	0.0 %	8.1 %	4.8 %	3.2 %	59.7 %	62
Σ	68	63	66	56	69	63	51	68	65	58	48	60	735

Рисунок 3.23 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «meanpressure»



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	28.3 %	0.0 %	0.0 %	16.7 %	16.7 %	1.7 %	1.7 %	8.3 %	1.7 %	0.0 %	0.0 %	25.0 %	60
102	1.6 %	43.5 %	1.6 %	4.8 %	14.5 %	8.1 %	4.8 %	9.7 %	3.2 %	3.2 %	3.2 %	1.6 %	62
203	0.0 %	7.7 %	7.7 %	3.1 %	0.0 %	9.2 %	9.2 %	3.1 %	23.1 %	20.0 %	16.9 %	0.0 %	65
302	16.7 %	15.0 %	3.3 %	13.3 %	6.7 %	10.0 %	8.3 %	3.3 %	15.0 %	0.0 %	0.0 %	8.3 %	60
303	21.7 %	6.7 %	0.0 %	10.0 %	25.0 %	1.7 %	6.7 %	10.0 %	1.7 %	0.0 %	0.0 %	16.7 %	60
503	6.7 %	5.0 %	8.3 %	6.7 %	1.7 %	18.3 %	11.7 %	13.3 %	21.7 %	0.0 %	1.7 %	5.0 %	60
602	4.8 %	11.3 %	8.1 %	1.6 %	6.5 %	12.9 %	19.4 %	6.5 %	8.1 %	14.5 %	4.8 %	1.6 %	62
605	6.5 %	22.6 %	1.6 %	8.1 %	4.8 %	9.7 %	4.8 %	24.2 %	4.8 %	8.1 %	3.2 %	1.6 %	62
1004	1.6 %	9.8 %	16.4 %	3.3 %	1.6 %	16.4 %	4.9 %	1.6 %	37.7 %	1.6 %	1.6 %	3.3 %	61
1203	0.0 %	1.6 %	14.8 %	0.0 %	1.6 %	4.9 %	6.6 %	4.9 %	6.6 %	31.1 %	27.9 %	0.0 %	61
1204	0.0 %	5.0 %	23.3 %	0.0 %	5.0 %	5.0 %	5.0 %	6.7 %	8.3 %	26.7 %	15.0 %	0.0 %	60
1301	21.0 %	4.8 %	0.0 %	9.7 %	8.1 %	4.8 %	1.6 %	6.5 %	3.2 %	0.0 %	0.0 %	40.3 %	62
Σ	66	82	52	47	56	63	52	60	83	65	46	63	735

Рисунок 3.24 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «meanfingerarea»

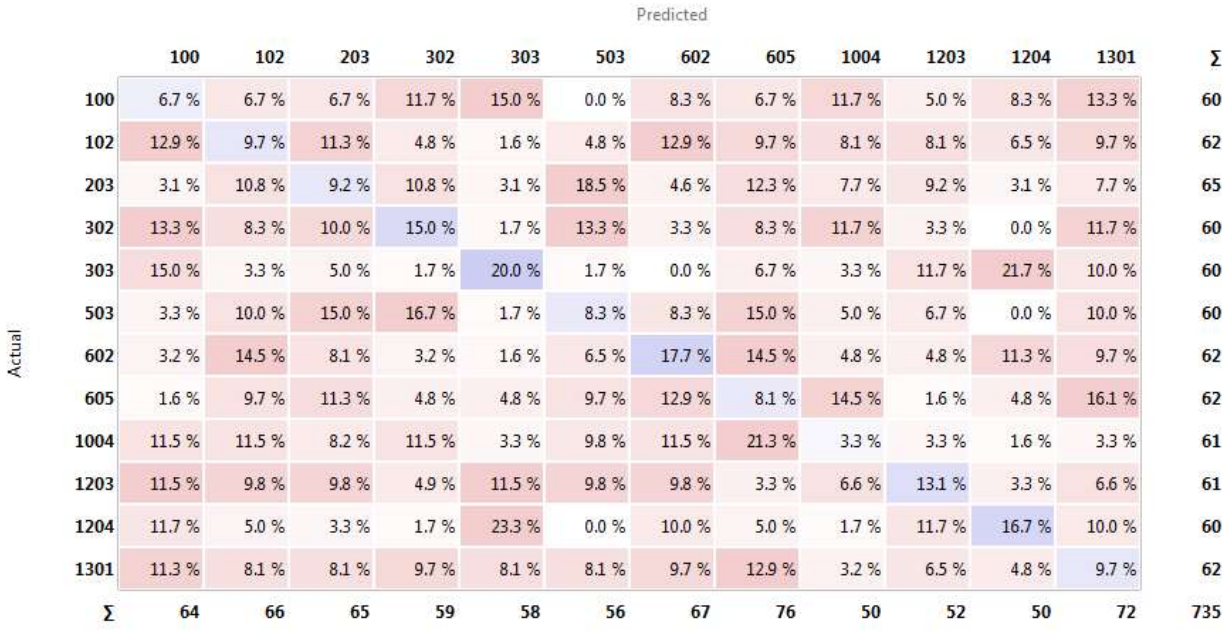


Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	70.0 %	3.3 %	5.0 %	8.3 %	1.7 %	0.0 %	0.0 %	0.0 %	1.7 %	0.0 %	6.7 %	3.3 %	60
102	1.6 %	95.2 %	0.0 %	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	1.6 %	62
203	3.1 %	0.0 %	52.3 %	0.0 %	12.3 %	3.1 %	1.5 %	0.0 %	1.5 %	3.1 %	18.5 %	4.6 %	65
302	5.0 %	0.0 %	1.7 %	68.3 %	0.0 %	3.3 %	1.7 %	0.0 %	15.0 %	0.0 %	5.0 %	0.0 %	60
303	0.0 %	0.0 %	13.3 %	0.0 %	65.0 %	1.7 %	6.7 %	6.7 %	0.0 %	0.0 %	1.7 %	5.0 %	60
503	0.0 %	3.3 %	5.0 %	3.3 %	1.7 %	53.3 %	1.7 %	1.7 %	11.7 %	6.7 %	11.7 %	0.0 %	60
602	0.0 %	0.0 %	1.6 %	0.0 %	3.2 %	1.6 %	88.7 %	1.6 %	0.0 %	1.6 %	0.0 %	1.6 %	62
605	0.0 %	0.0 %	6.5 %	0.0 %	1.6 %	3.2 %	0.0 %	82.3 %	3.2 %	1.6 %	1.6 %	0.0 %	62
1004	3.3 %	0.0 %	3.3 %	19.7 %	0.0 %	6.6 %	0.0 %	4.9 %	29.5 %	18.0 %	11.5 %	3.3 %	61
1203	3.3 %	1.6 %	1.6 %	0.0 %	0.0 %	6.6 %	6.6 %	1.6 %	13.1 %	55.7 %	9.8 %	0.0 %	61
1204	10.0 %	1.7 %	13.3 %	6.7 %	3.3 %	6.7 %	0.0 %	3.3 %	11.7 %	16.7 %	25.0 %	1.7 %	60
1301	1.6 %	0.0 %	0.0 %	0.0 %	1.6 %	0.0 %	1.6 %	0.0 %	0.0 %	0.0 %	0.0 %	95.2 %	62
Σ	59	65	65	64	55	53	67	63	53	63	56	72	735

Рисунок 3.25 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативними параметрами «meanxacceleration», «meanyacceleration» та «meanzacceleration»

Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	15.0 %	0.0 %	11.7 %	15.0 %	13.3 %	6.7 %	0.0 %	13.3 %	11.7 %	8.3 %	1.7 %	3.3 %	60
102	0.0 %	61.3 %	3.2 %	0.0 %	0.0 %	3.2 %	8.1 %	0.0 %	6.5 %	1.6 %	8.1 %	8.1 %	62
203	9.2 %	3.1 %	15.4 %	1.5 %	13.8 %	7.7 %	7.7 %	9.2 %	13.8 %	7.7 %	4.6 %	6.2 %	65
302	11.7 %	0.0 %	1.7 %	36.7 %	6.7 %	0.0 %	0.0 %	15.0 %	10.0 %	16.7 %	1.7 %	0.0 %	60
303	15.0 %	0.0 %	16.7 %	1.7 %	15.0 %	8.3 %	6.7 %	10.0 %	8.3 %	10.0 %	5.0 %	3.3 %	60
503	6.7 %	6.7 %	6.7 %	0.0 %	8.3 %	11.7 %	16.7 %	5.0 %	16.7 %	5.0 %	5.0 %	11.7 %	60
602	0.0 %	9.7 %	8.1 %	0.0 %	3.2 %	9.7 %	22.6 %	6.5 %	4.8 %	6.5 %	16.1 %	12.9 %	62
605	16.1 %	0.0 %	6.5 %	16.1 %	11.3 %	3.2 %	6.5 %	17.7 %	4.8 %	8.1 %	3.2 %	6.5 %	62
1004	9.8 %	1.6 %	9.8 %	6.6 %	9.8 %	9.8 %	4.9 %	6.6 %	13.1 %	14.8 %	9.8 %	3.3 %	61
1203	11.5 %	3.3 %	8.2 %	19.7 %	8.2 %	1.6 %	11.5 %	9.8 %	9.8 %	8.2 %	6.6 %	1.6 %	61
1204	1.7 %	10.0 %	6.7 %	1.7 %	5.0 %	8.3 %	18.3 %	3.3 %	6.7 %	8.3 %	8.3 %	21.7 %	60
1301	3.2 %	4.8 %	6.5 %	1.6 %	3.2 %	11.3 %	14.5 %	4.8 %	4.8 %	1.6 %	21.0 %	22.6 %	62
Σ	61	62	62	61	60	50	72	62	68	59	56	62	735

Рисунок 3.26 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «velocity»



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	6.7 %	6.7 %	6.7 %	11.7 %	15.0 %	0.0 %	8.3 %	6.7 %	11.7 %	5.0 %	8.3 %	13.3 %	60
102	12.9 %	9.7 %	11.3 %	4.8 %	1.6 %	4.8 %	12.9 %	9.7 %	8.1 %	8.1 %	6.5 %	9.7 %	62
203	3.1 %	10.8 %	9.2 %	10.8 %	3.1 %	18.5 %	4.6 %	12.3 %	7.7 %	9.2 %	3.1 %	7.7 %	65
302	13.3 %	8.3 %	10.0 %	15.0 %	1.7 %	13.3 %	3.3 %	8.3 %	11.7 %	3.3 %	0.0 %	11.7 %	60
303	15.0 %	3.3 %	5.0 %	1.7 %	20.0 %	1.7 %	0.0 %	6.7 %	3.3 %	11.7 %	21.7 %	10.0 %	60
503	3.3 %	10.0 %	15.0 %	16.7 %	1.7 %	8.3 %	8.3 %	15.0 %	5.0 %	6.7 %	0.0 %	10.0 %	60
602	3.2 %	14.5 %	8.1 %	3.2 %	1.6 %	6.5 %	17.7 %	14.5 %	4.8 %	4.8 %	11.3 %	9.7 %	62
605	1.6 %	9.7 %	11.3 %	4.8 %	4.8 %	9.7 %	12.9 %	8.1 %	14.5 %	1.6 %	4.8 %	16.1 %	62
1004	11.5 %	11.5 %	8.2 %	11.5 %	3.3 %	9.8 %	11.5 %	21.3 %	3.3 %	3.3 %	1.6 %	3.3 %	61
1203	11.5 %	9.8 %	9.8 %	4.9 %	11.5 %	9.8 %	9.8 %	3.3 %	6.6 %	13.1 %	3.3 %	6.6 %	61
1204	11.7 %	5.0 %	3.3 %	1.7 %	23.3 %	0.0 %	10.0 %	5.0 %	1.7 %	11.7 %	16.7 %	10.0 %	60
1301	11.3 %	8.1 %	8.1 %	9.7 %	8.1 %	8.1 %	9.7 %	12.9 %	3.2 %	6.5 %	4.8 %	9.7 %	62
Σ	64	66	65	59	58	56	67	76	50	52	50	72	735

Рисунок 3.27 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «totaldistance»

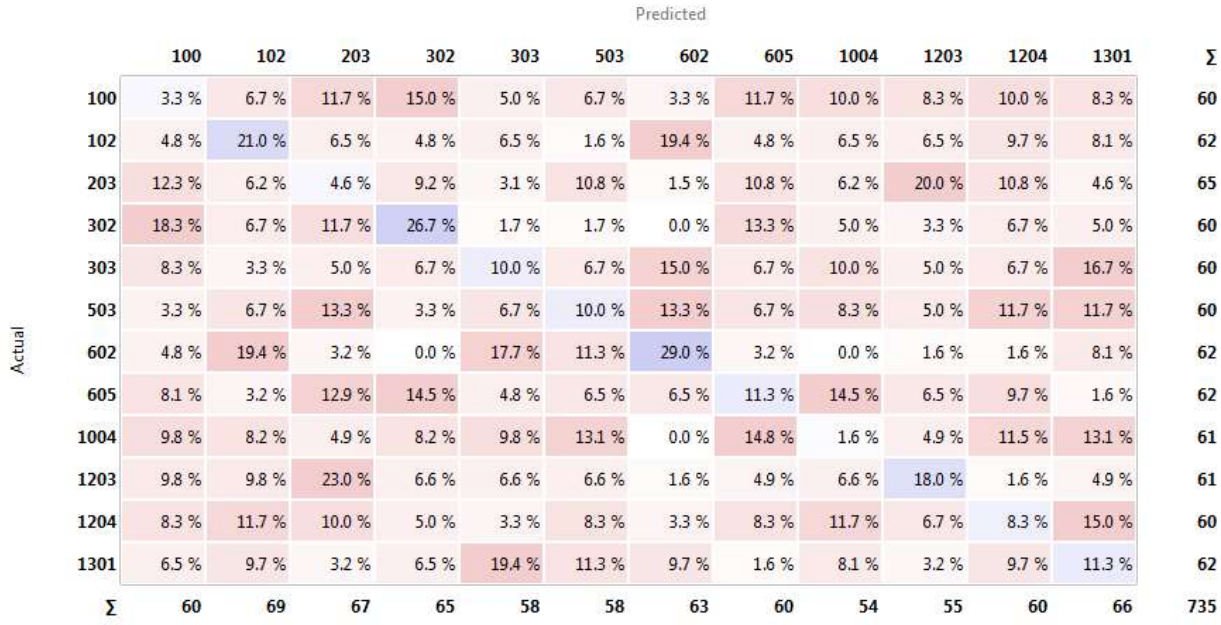
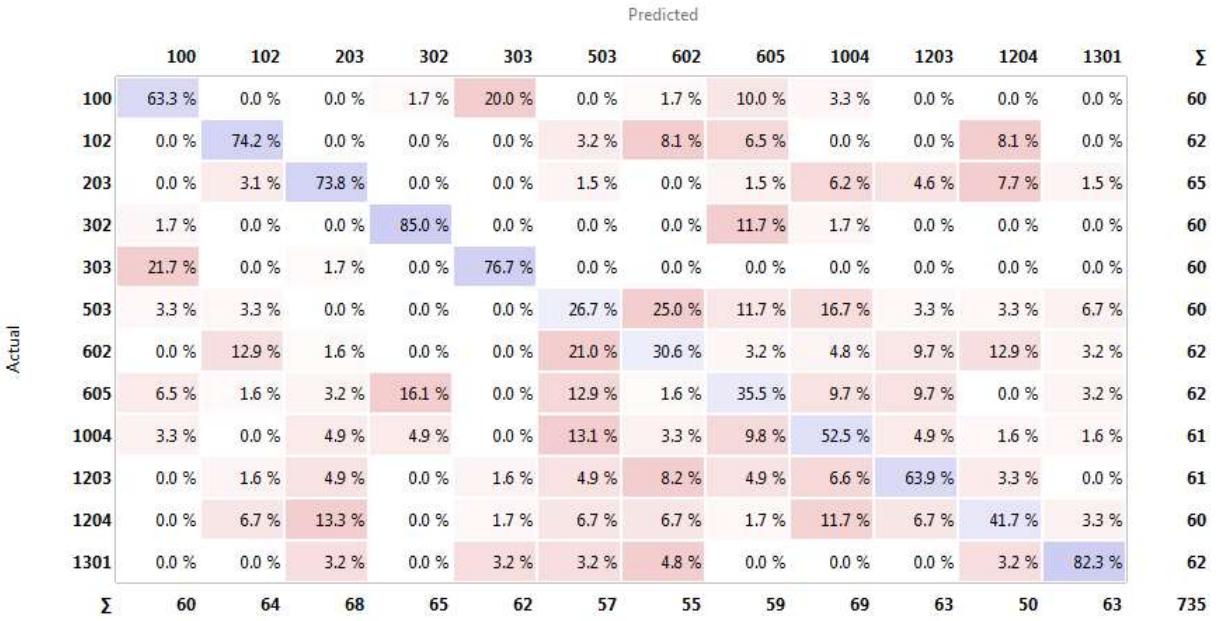


Рисунок 3.28 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативним параметром «totaltime»

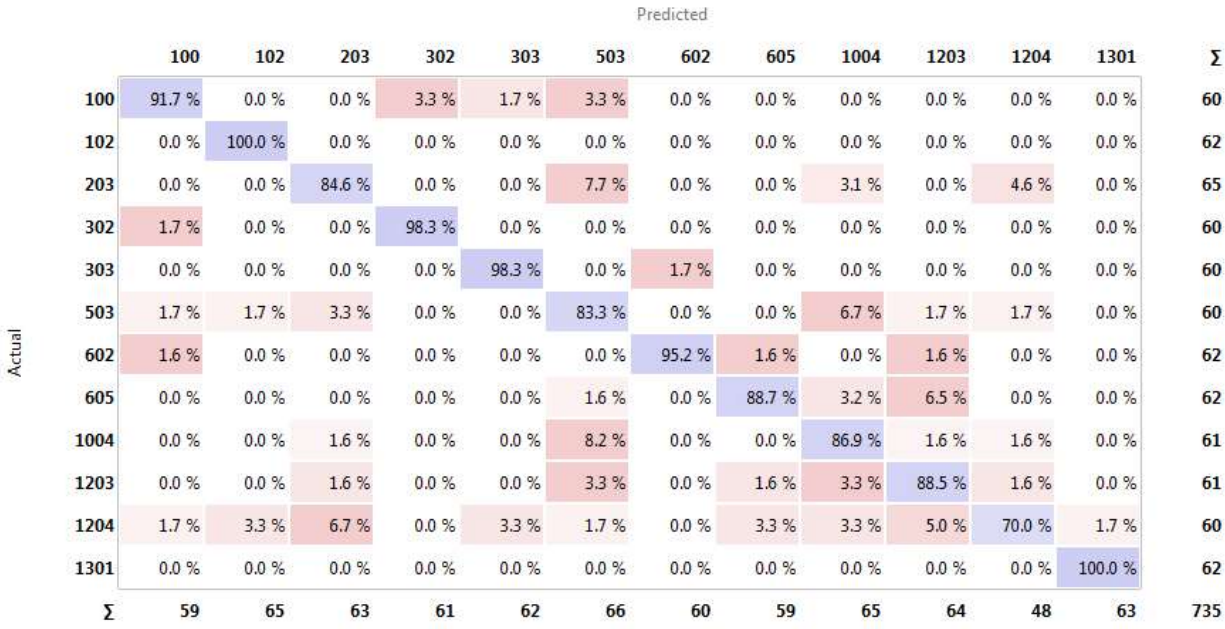
На рис. 3.27 наведено результати мультикласової класифікації користувачів «100», «203», «303», «503», «602», «605», «1004», «1203», «1204», «102», «302» та «1301» за комбінацією з п’яти найінформативних ознак з класу усереднених параметрів взаємодії користувача зі смартфоном. Як можна побачити, використання «meanholdtime», «meanfingerarea», «velocity», «meanzaccelaration» та «meanpressure» забезпечує середню точність класифікації лише 83.3 %. Додавання до цих параметрів «meanxaccelaration» та «meanyaccelaration» підвищує середню точність класифікації до 91.1 % (у порівнянні з 91.3 % при використанні усіх усереднених параметрів взаємодії користувача зі смартфоном – рис. 3.19).

Таким чином, обов’язковими інформативним параметрами при побудові системи ідентифікації за сенсорним почерком є наступні інформативні ознаки: «meanholdtime», «meanfingerarea», «velocity» «meanpressure», «meanzaccelaration», «meanxaccelaration», «meanyaccelaration».



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	63.3 %	0.0 %	0.0 %	1.7 %	20.0 %	0.0 %	1.7 %	10.0 %	3.3 %	0.0 %	0.0 %	0.0 %	60
102	0.0 %	74.2 %	0.0 %	0.0 %	0.0 %	3.2 %	8.1 %	6.5 %	0.0 %	0.0 %	8.1 %	0.0 %	62
203	0.0 %	3.1 %	73.8 %	0.0 %	0.0 %	1.5 %	0.0 %	1.5 %	6.2 %	4.6 %	7.7 %	1.5 %	65
302	1.7 %	0.0 %	0.0 %	85.0 %	0.0 %	0.0 %	0.0 %	11.7 %	1.7 %	0.0 %	0.0 %	0.0 %	60
303	21.7 %	0.0 %	1.7 %	0.0 %	76.7 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
503	3.3 %	3.3 %	0.0 %	0.0 %	0.0 %	26.7 %	25.0 %	11.7 %	16.7 %	3.3 %	3.3 %	6.7 %	60
602	0.0 %	12.9 %	1.6 %	0.0 %	0.0 %	21.0 %	30.6 %	3.2 %	4.8 %	9.7 %	12.9 %	3.2 %	62
605	6.5 %	1.6 %	3.2 %	16.1 %	0.0 %	12.9 %	1.6 %	35.5 %	9.7 %	9.7 %	0.0 %	3.2 %	62
1004	3.3 %	0.0 %	4.9 %	4.9 %	0.0 %	13.1 %	3.3 %	9.8 %	52.5 %	4.9 %	1.6 %	1.6 %	61
1203	0.0 %	1.6 %	4.9 %	0.0 %	1.6 %	4.9 %	8.2 %	4.9 %	6.6 %	63.9 %	3.3 %	0.0 %	61
1204	0.0 %	6.7 %	13.3 %	0.0 %	1.7 %	6.7 %	6.7 %	1.7 %	11.7 %	6.7 %	41.7 %	3.3 %	60
1301	0.0 %	0.0 %	3.2 %	0.0 %	3.2 %	3.2 %	4.8 %	0.0 %	0.0 %	0.0 %	3.2 %	82.3 %	62
Σ	60	64	68	65	62	57	55	59	69	63	50	63	735

Рисунок 3.27 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативними параметрами «meanholdtime», «meanfingerarea», «velocity», «meanzaccelaration» та «meanpressure»



Actual \ Predicted	100	102	203	302	303	503	602	605	1004	1203	1204	1301	Σ
100	91.7 %	0.0 %	0.0 %	3.3 %	1.7 %	3.3 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
102	0.0 %	100.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	62
203	0.0 %	0.0 %	84.6 %	0.0 %	0.0 %	7.7 %	0.0 %	0.0 %	3.1 %	0.0 %	4.6 %	0.0 %	65
302	1.7 %	0.0 %	0.0 %	98.3 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
303	0.0 %	0.0 %	0.0 %	0.0 %	98.3 %	0.0 %	1.7 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	60
503	1.7 %	1.7 %	3.3 %	0.0 %	0.0 %	83.3 %	0.0 %	0.0 %	6.7 %	1.7 %	1.7 %	0.0 %	60
602	1.6 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	95.2 %	1.6 %	0.0 %	1.6 %	0.0 %	0.0 %	62
605	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	1.6 %	0.0 %	88.7 %	3.2 %	6.5 %	0.0 %	0.0 %	62
1004	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	8.2 %	0.0 %	0.0 %	86.9 %	1.6 %	1.6 %	0.0 %	61
1203	0.0 %	0.0 %	1.6 %	0.0 %	0.0 %	3.3 %	0.0 %	1.6 %	3.3 %	88.5 %	1.6 %	0.0 %	61
1204	1.7 %	3.3 %	6.7 %	0.0 %	3.3 %	1.7 %	0.0 %	3.3 %	3.3 %	5.0 %	70.0 %	1.7 %	60
1301	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	0.0 %	100.0 %	62
Σ	59	65	63	61	62	66	60	59	65	64	48	63	735

Рисунок 3.28 – Матриця помилок мультикласової класифікації користувачів датасету «MOBIKEY logicalstrong» за інформативними параметрами «meanholdtime», «meanfingerarea», «velocity», «meanpressure», «meanzaccelaration», «meanxaccelaration», «meanyaccelaration»

3.3. Висновки до розділу.

1. Для досвідчених користувачів перехід до паролів, що містять великі і маленькі букви, цифри та символи не є необхідним з точки зору підвищення якості ідентифікації. Для недосвідчених користувачів подібний перехід є більш бажаним, оскільки кількість користувачів з точністю розпізнавання 90 % зростає зі збільшенням складності паролю.

2. Враховуючи рівну довжину паролів «Kktsf2!2014» та «.tie5Roanl» (містять по 72 інформативних параметра) та практично однакову інтегральну точність розпізнавання (середнє значення 94.7 % і медіана 96.7 %), можна зробити висновок, що використання цифр замість букв в паролях не призводить до збільшення точності розпізнавання.

3. У порівнянні з датасетом клавіатурного почерку «Keystroke Dynamics Benchmark Data Set», де містяться інформативні ознаки вводу паролю «.tie5Roanl», системи розпізнавання за сенсорним почерком можуть забезпечити точність ідентифікації, яка притаманна системам ідентифікації за клавіатурним почерком. Проте для забезпечення такої точності необхідно збирати більші масиви даних: пароль «.tie5Roanl» в дата сеті «MOBIKEY strong» містить 72 інформативних параметри, в той час як пароль «.tie5Roanl» в дата сеті «Keystroke Dynamics Benchmark Data Set» містить 31 інформативний параметр.

4. Підвищити точність ідентифікації можна за рахунок побудови двійкової системи класифікації, коли цільовому користувачу присвоюється клас 1, тобто «зареєстрований», а усім іншим користувачам – клас 2, тобто «зловмисник». Це можливо, оскільки на відміну від комп'ютера, де зареєстрованими користувачами можуть бути декілька людей, у мобільного пристрою завжди тільки один власник.

Для дослідження точності двійкової класифікації з датасету «MOBIKEY logicalstrong» було відібрано 9 користувачів «100», «203», «303», «503», «602», «605», «1004», «1203» та «1204», для яких точність мультикласової класифікації становила менше 95 % за всьома трьома дослідними датасетами. Отже,

можна вважати, що це користувачі з найменш унікальним сенсорним почерком. Також для наочності отриманих результатів до аналізу було додано 3 користувачі «102», «302» та «1301», для яких точність мультикласової класифікації становила не менше 98 % за всьома трьома дослідними датасетами. Отже, можна вважати, що це користувачі з найбільш унікальним сенсорним почерком.

Проведені експериментальні дослідження показали, що інтегральна (усереднена за всіма 12 користувачами) помилка FAR (випадок надання системою доступу неавторизованому користувачеві) становить 1.58 %. Враховуючи також той факт, що зловмисник апріорі має сформований сенсорний почерк, оскільки сфера його професійних навичок вимагає тривалого часу взаємодії зі смартфонами (один з пари користувачів вже має унікальний почерк), то з плином часу значення помилки FAR буде зменшуватись, оскільки інформативні ознаки сенсорного почерку легітимного користувача також ставатимуть більш унікальними (обидва користувачі в парі мають унікальний почерк). За результатами проведених досліджень можна очікувати зменшення рівня помилки FAR до 1.2 %, тобто 12 пропусків зловмисника на 1000 спроб.

Рівень помилки FRR (доступ заборонений користувачеві, зареєстрованому в системі) за умови недосвідченого користувача може становити до 1.36 %. Якщо ж враховувати лише користувачів з унікальним почерком, то рівень помилки FRR зменшується до 0.54 %, тобто 54 недопуски верифікованого користувача на 10000 спроб.

5. Найбільш інформативними ознаками сенсорного почерку є усереднені параметри взаємодії користувача зі смартфоном – інтегральна точність розпізнавання 91.3 %. Для класифікації за часовими параметрами інтегральна точність становить 83 %, а для класифікації за параметрами взаємодії з екраном – 67.7 %.

У якості базових ознак для побудови систем розпізнавання за сенсорним почерком слід використовувати наступні параметри: meanholdtime – середнє значення часу натискання клавіш в процесі набору парольної фрази;

meanpressure – середнє значення тиску на екран в процесі набору парольної фрази; meanfingerarea – середнє значення розміру області на сенсорному екрані від пальця користувача в процесі набору парольної фрази; meanxacceleration – середнє значення прискорення по вісі «X» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAX); meanyacceleration – середнє значення прискорення по вісі «Y» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAY); meanzacceleration – середнє значення прискорення по вісі «Z» відхилення смартфону від початкового положення в процесі вводу парольної фрази (MAZ); velocity – швидкість, обчислювалась як частка відстані та загального часу.

ВИСНОВКИ

1. Виконано огляд основних методів біометричної аутентифікації, що використовуються або є перспективними для використання в мобільних пристроях. Це розпізнавання за голосом, розпізнавання за динамічним графічним паролем, розпізнавання за тривимірним динамічним підписом, розпізнавання за геометрією долоні, розпізнавання за райдужною оболонкою ока, розпізнавання за відбитком пальця, розпізнавання за клавіатурним почерком. Використання сенсорного почерку має потенціал для застосування як додаткова міра, що підвищує загальний рівень безпеки при аутентифікації.

Крім того одним з плюсів поведінкової біометрії, до якої відноситься сенсорний почерк, є розпізнавання не тільки знайомих загроз, а й виявлення нових шахрайських схем. Оскільки цей метод заснований на характеристиках поведінки, він дозволяє розпізнавати аномальну поведінку незалежно від схеми атаки – а значить, є ефективним засобом запобігання новим, ще невідомим, типам атак.

2. У роботі проаналізовано інформативні ознаки сенсорного почерку. Можна виділити три основних класи: часові параметри, параметри взаємодії з екраном (тиск та розмір «плями» від пальця) та психофізіологічні параметри, де до тиску та розміру «плями» додаються показання акселерометру та динаміка руху кінчика пальця по екрану.

3. За даними датасету «The Mobikey Keystroke Dynamics Password Database» інтегральна точність мультикласової класифікації за сенсорним почерком становить 94.7 %. Отже, системи розпізнавання за сенсорним почерком можуть забезпечити точність ідентифікації, яка притаманна системам ідентифікації за клавіатурним почерком. Проте для забезпечення такої точності необхідно збирати більші масиви даних: пароль «.tie5Roanl» в дата сеті «MOBIKEY strong» містить 72 інформативних параметри, в той час як пароль «.tie5Roanl» в дата сеті «Keystroke Dynamics Benchmark Data Set» містить 31

інформативний параметр.

4. Для досвідчених користувачів перехід до паролів, що містять великі і маленькі букви, цифри та символи не є необхідним з точки зору підвищення якості ідентифікації. Для недосвідчених користувачів подібний перехід є більш бажаним, оскільки кількість користувачів з точністю розпізнавання 90 % зростає зі збільшенням складності паролю.

5. Точність розпізнавання за часовими параметрами сенсорного почерку становить 83 %. Таким чином, нестабільність часових параметрів сенсорного почерку обумовлює неможливість побудови аутентифікаційних систем, що враховують лише ці часові параметри.

6. Точність розпізнавання за параметрами взаємодії з екраном складає 67.7 %. Таким чином, тиск та розмір «плями» не є настільки унікальними параметрами сенсорного почерку, щоб будувати тільки за ними аутентифікаційну систему.

7. Найінформативнішими параметрами сенсорного почерку є прискорення по трьох осях координат, динаміку руху кінчика пальця по екрану та усереднений час натискання клавіш в процесі набору парольної фрази. Використання цих семи параметрів дає інтегральну точність мультикласової класифікації 91.1 %.

8. Підвищити точність ідентифікації можна за рахунок побудови двійкової системи класифікації, коли цільовому користувачу присвоюється клас 1, тобто «зареєстрований», а усім іншим користувачам – клас 2, тобто «зловмисник». Це можливо, оскільки на відміну від комп’ютера, де зареєстрованими користувачами можуть бути декілька людей, у мобільного пристрою завжди тільки один власник.

Проведені дослідження дозволяють зробити висновок про забезпечення інтегральної помилки FAR 1.58 %. Враховуючи також той факт, що зловмисник апріорі має сформований сенсорний почерк, оскільки сфера його професійних навичок вимагає тривалого часу взаємодії зі смартфонами (один з пари користувачів вже має унікальний почерк), то з плином часу значення помилки

FAR буде зменшуватись, оскільки інформативні ознаки сенсорного почерку легітимного користувача також ставатимуть більш унікальними (обидва користувачі в парі мають унікальний почерк). За результатами проведених досліджень можна очікувати зменшення рівня помилки FAR до 1.2 %, тобто 12 пропусків зловмисника на 1000 спроб.

Рівень помилки FRR (доступ заборонений користувачеві, зареєстрованому в системі) за умови недосвідченого користувача може становити до 1.36 %. Якщо ж враховувати лише користувачів з унікальним почерком, то рівень помилки FRR зменшується до 0.54 %, тобто 54 недопуски верифікованого користувача на 10000 спроб.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Аналитический центр InfoWatch. Глобальное исследование утечек корпоративной информации и конфиденциальных даннях. [Електронний ресурс] – Режим доступу: https://www.infowatch.ru/report2016. Дата звернення: 25.08.2022.

2. Исследование уязвимости мобильных устройств систем Apple и Google. [Електронний ресурс] – Режим доступу: http://cyberleninka.ru/article/n/issledovanie-uyazvimosti-mobilnyh-ustroystv-sistem-apple-i-google#ixzz4hjVQGz9w.. Дата звернення: 25.08.2022.

3. OWASP Proactive Controls 2021. [Електронний ресурс] – Режим доступу: https://owasp.org/Top10/ . Дата звернення: 25.08.2022.

4. Rovelli P. Developing a Next-generation Mobile Security Solution for Android. April 2014 School of Computer Science Reykjavík University / P. Rovelli. [Електронний ресурс] – Режим доступу: https://skemman.is/bitstream/1946/19500/1/Developing%20a%20next-generation%20Mobile%20Security%20solution%20for%20Android%20-%20Paolo%20Rovelli.pdf. Дата звернення: 25.08.2022.

5. Diasamidze S. V. Implementation of the Role Based Access Control in Application for Mobile Device on the Android OS Platform / S. V. Diasamidze, E. Yu. Kuzmenkova, D. A. Kuznetsov, A. R. Sarkisyan // Интеллектуальные технологии на транспорте, 2016, No 1. С. 21-26.

6. Barkan E., Biham E., Keller N. Instant ciphertext-only cryptanalysis of GSM encrypted communication //Journal of Cryptology. – 2008. – Т. 21. – No. 3. – С. 392-429.

7. Security Comparison between Android and iOS. [Електронний ресурс] – Режим доступу: https://www.ijert.org/research/security-comparison-between-android-and-ios-IJERTCONV5IS10021.pdf. Дата звернення: 25.08.2022.

8. Security Evaluation of IOS and Android. [Електронний ресурс] – Режим

доступу: https://dergipark.org.tr/tr/download/article-file/236943. Дата звернення: 25.08.2022.

9. Security Comparison of Android and IOS and Implementationof User Approved Security (UAS) for Android. [Електронний ресурс] – Режим доступу: https://sciresol.s3.us-east-2.amazonaws.com/IJST/Articles/2016/Issue-14/Article42.pdf. Дата звернення: 25.08.2022.

10. Baljit Singh Saini, N.K., Bhatia, K.S. Keystroke dynamics for mobile phones: a survey. [Електронний ресурс] – Режим доступу: https://sciresol.s3.us-east-2.amazonaws.com/IJST/Articles/2016/Issue-6/Article6.pdf. Дата звернення: 25.08.2022.

11. The MOBIKEY Keystroke Dynamics Password Database. [Електронний ресурс] – Режим доступу: https://www.ms.sapientia.ro/~manyi/ mobikey.html. Дата звернення: 25.08.2022.

12. Keystroke Dynamics Benchmark Data Set. [Електронний ресурс] – Режим доступу: https://www.cs.cmu.edu/~keystroke. Дата звернення: 25.08.2022.

13. Demšar, J. Orange: Data Mining Fruitful and Fun – A Historical Perspective [Text] / J. Demšar, Z. Blaž // Informatica. – 2013. – Vol. 37. – P. 55–60.

14. Keystroke Dynamics Benchmark Data Set. [Електронний ресурс] – Режим доступу: https://www.cs.cmu.edu/~keystroke Ддата звернення: 25.08.2022.

15. Alieksieiev Vasyl, Elena Sharapova, Olena Ivanova, Gorelov Denis, Synytsia Yuliia. Web-Based Application to Collect and Analyze Users Data for Keystroke Biometric Authentication. In Proceedings of the First IEEE Ukraine Conference on Electrical and Computer Engineering (UKRCON). Pages 917-922, 2017. DOI: 10.1109/UKRCON.2017.8100382

16. Vasyl Alieksieiev, Aleksey Strelnitskiy, Dmitry Gavva, Denis Gorelov, Yuliia Synytsia. Studying of keystroke dynamics statistical properties for biometric user authentication. Proceedings of 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Pages 559-563, 2018. DOI: 10.1109/TCSET.2018.8336264

17. Модифицированный метод диграфов в задаче аутентификации пользователей по клавиатурному почерку/ В.А. Алексеев, Ю.А. Синица, Д.Ю. Горелов // Журнал "Защита информации". – Киев. – 2017. – Вып. 4. – с. 252-261.

18. Сравнительный анализ перспективных технологий аутентификации пользователей ПК по клавиатурному почерку / В. А. Алексеев, Д. В. Маслий, Д. Ю. Горелов // Радиотехника: Всеукр. межвед. научн.-техн. Сб. – 2017. – Вып. 189. – С. 195-201.

19. Исследование статистических свойств клавиатурного почерка для решения задач аутентификации пользователей компьютерных сетей / Д.Ю. Горелов, В.О. Алексеев, В.М. Бублик, Д.В. Маслий // Радиотехника: Всеукр. межвед. науч.-техн. сб. – 2019. – Вып. 197. – С. 78 – 85. DOI: https://doi.org/10.30837/rt.2019.2.197.10

20. Дослідження інформативних параметрів диграфів клавіатурного почерку для задач ідентифікації користувачів комп'ютерних мереж / Д.Ю. Горелов, О.О. Іванова, О.В. Кокорін, Д.В. Маслій, О.В. Литвиненко // Радіотехніка: Всеукр. Міжвід. Наук.-техн. Зб. – 2020. – вип. 201. – с. 194 – 200. DOI: https://doi.org/10.30837/rt.2020.2.201.19

21. Исследование возможностей использования клавиатурного почерка для задач идентификации студентов в системах дистанционного образования / Д.Ю. Горелов, Е.А. Иванова, А.В Литвиненко, А.А. Довбня, Д.А. Минин // Радиотехника : Всеукр. межвед. науч.-техн. сб. 2021. Вып. 207. С. 139 – 148. DOI:10.30837/rt.2021.4.207.15