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 ефективності ідентифікації особи за графічним паролем

Виконав:
студент *2* курсу, групи *СТЗІАм-22-1*
Пономаренко Владислав 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)

2024 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 *Пономаренку Владиславу Олександровичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження ефективності ідентифікації особи за графічним паролем*

затверджена наказом по університету від « 03 » 11 2023 р. № 1281 Ст

2. Термін подання студентом роботи до екзаменаційної комісії *10 січня 2024 р.*

3. Вихідні дані до роботи

Тип біометричної СКУД: динамічний аналіз цифрового рукописного підпису власників мобільних пристроїв

Дослідні інформативні ознаки цифрового рукописного підпису:

1) динамічні параметри руху кінчика пальця сенсорним екраном;

2) параметри взаємодії з екраном (тиск та розмір «плями» від пальця);

3) параметри, що характеризують положення смартфону в руці користувача та коливання смартфону в просторі в процесі введення цифрового рукописного підпису

4. Перелік питань, що потрібно опрацювати в роботі

Дослідити інформативність параметрів цифрового рукописного підпису 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 цифрового рукописного підпису та обрати один з них для подальших досліджень;3) експериментально дослідити точність ідентифікації, як функцію використаних інформативних ознак цифрового рукописного підпису.

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

1. Мета та задачі кваліфікаційної роботи. А4. Ел.ф.

2. Технології поведінкової біометричної ідентифікації власників мобільних пристроїв за особливостями взаємодії з сенсорним екраном. А4. Ел.ф.

3. The MOBISIG signature database. А4. Ел.ф.

4. Результати класифікації користувачів датасету «The MOBISIG signature database». А4. Ел.ф.

5. Порівняльний аналіз результатів класифікації користувачів датасету «The MOBISIG signature database», яким відповідають найкоротші та найдовші сигнатури. А4. Ел.ф.

6. Висновки

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Аналіз сучасних методів та засобів біометричної ідентифікації власників мобільних пристроїв*	*01.09.23 – 20.09.23*	
2	*Огляд сучасних рішень та перспективних технологій в області інтеграції біометричного захисту інформації та мобільних операційних систем*	*21.09.23 – 31.10.23*	
3	*Експериментальні дослідження інформативних ознак цифрового рукописного підпису*	*01.11.23 – 31.12.23*	
4	*Перевірка роботи на антиплагіат*	*03.01.24 – 05.01.24*	
5	*Представлення кваліфікаційної роботи на кафедрі*	*10.01.2024*	

Дата видачі завдання *02 вересня 2023 р.*

Студент _____
(підпис)

Керівник роботи _____ _____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 90 с., 35 рис., 2 табл., 23 джерела, 1 додаток.

БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ, МОБІЛЬНИЙ ПРИСТРІЙ, ЦИФРОВИЙ РУКОПИСНИЙ ПІДПИС, МЕТОД ВИПАДКОВИХ ЛІСІВ,

Об’єкт дослідження – біометричні системи ідентифікації особистості.

Предмет дослідження – аутентифікація за цифровим рукописним підписом.

Метою цієї роботи є підвищення інформаційної безпеки комп’ютерних систем на основі аналізу цифрового рукописного підпису.

За допомогою бази даних «The MOBISIG signature database» та програмного забезпечення Orange проведено дослідження впливу на точність ідентифікації за цифровим рукописним підписом різних інформативних ознак: динамічних параметрів руху кінчика пальця екраном, параметрів взаємодії з екраном (тиск та розмір «плями» від пальця) та параметрів, що характеризують положення смартфону в руці користувача та коливання смартфону в просторі в процесі введення цифрового рукописного підпису.

ABSTRACT

Master thesis: 90 p., 2 tables, 35 fig., 23 sources, 1 annex.

BIOMETRIC IDENTIFICATION, SIGNATURE VERIFICATION, MOBILE AUTHENTICATION, RANDOM FORESTS.

The focus of the research is biometric identification systems of mobile devices owners.

The study subject is identification via signature dynamics.

The objective of the work is explore the possibility of using signature dynamics in mobile devices owners identification tasks.

Using the database "The MOBISIG signature database" and the Orange software, a study of the impact on the accuracy of identification by a signature of various informative features: dynamic parameters of the movement of the fingertip on the screen, parameters of interaction with the screen (pressure and size of the "spot" from the finger) and parameters characterizing the position of the smartphone in the user's hand and the vibrations of the smartphone in space during the process of entering a signature.

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;

БСКД – біометрична система контролю доступу;

ОС – операційна система.

ВСТУП

У найближчі кілька років втрачені користувачами паролі будуть вважатися проблемою минулого, адже все більше організацій використовують біометричні технології для аутентифікації. За даними компанії Gartner до 2022 року 60 % великих компаній зменшать свою залежність від паролів. Наразі співробітники Microsoft вже проходять аутентифікацію з використанням біометричних даних, а британські банки перевіряють відбитки пальців для авторизації покупок.

З 41686 інцидентів безпеки, описаних у звіті Verizon Data Breach 2019, 32 % були пов'язані з фішингом, а 29 % – з викраденими обліковими даними, а це свідчить про те, що заміна паролів на біометричні дані виправдана. Підприємствам, співробітникам і споживачам потрібен менш складний і більш безпечний спосіб аутентифікації, а використання біометрії забезпечує і те, і інше.

Хоча статичні методи біометрії здаються безпечним способом ідентифікації користувача (не можна «вкрасти» фізичні характеристики людини), в них є ряд недоліків і вони володіють різними рівнями безпеки.

Наприклад, може здатися, що немає нічого надійнішого за відбитки пальців. Проблема полягає в тому, що люди залишають свої відбитки пальців скрізь – а шахраї можуть таким чином вкрасти цей ідентифікатор. Відомий випадок, коли хакер Ян Крисслер використав доступні програми і пару знімків руки міністра оборони Німеччини Урсули фон дер Ляйєн. Основну частину з них він сам зробив звичайним фотоапаратом з відстані близько трьох метрів під час однієї з прес-конференцій. Додаткові знімки він отримав з HD-відео, на яких рука міністра була показана крупним планом з різних ракурсів. Використовуючи програму VeriFinger, хакер виконав фільтрацію і автоматичне співставлення опорних вузлів зображення. Таким способом йому вдалося отримати «цифрову копію» пальця.

В Європі співробітники поліції попереджають: якщо вам надійшов дзвінок, і людина на іншому кінці задає питання: «Ти мене чуєш?» – терміново скидайте дзвінок і нічого не кажіть аферистові. З'явилася нова схема телефонного шахрайства – зловмисник записує голос жертви (в більшості випадків відповідь на означений вище питання – «так»), а пізніше використовує цей запис у підтвердженні голосових операцій з кредитною карткою.

У серпні 2018 р. дослідники з Університету Північної Кароліни створили програмне забезпечення, здатне обдурити біометричну систему розпізнавання обличчя в смартфоні за допомогою проекції тривимірного анімаційного зображення обличчя у віртуальну реальність. Для побудови тривимірної моделі обличчя учені використовували фотографії добровольців, викладені на Facebook. Технологія дозволяє не тільки підробити зображення, але і обдурити датчики руху і глибини, якими обладнані системи безпеки.

Враховуючи вищезгадане виникла необхідність у розробці іншого біометричного підходу. Новим методом стали системи поведінкової біометрії. Ці методи базуються на ідеї використання унікальних для кожного користувача характеристик, за умови, що аутентифікація не викликає у користувача незручностей, а спеціальне обладнання з новими датчиками для цього не потрібно. Поведінка являє собою більш багатогранний спосіб аутентифікації.

Поведінкові методики передбачають збір великої кількості різноманітних даних. Наприклад, це можуть бути математичні алгоритми, які дозволяють здійснювати безперервну аутентифікацію користувача за клавіатурним почерком. Спеціальне програмне забезпечення збирає статистику поведінкових моделей користувача і формує його поведінковий патерн. Кожен раз, коли користувач працює в додатку, система порівнює його поведінку з попередніми спробами. Якщо біометричні характеристики не збігаються, то користувачеві пропонуються додаткові ступені аутентифікації. Алгоритми враховують зміни в цифровій поведінці користувача: тобто якщо людина з якихось причин стане повільніше друкувати, то система все одно повинна її розпізнати.

Поведінкову біометрію можна адаптувати для самих різних пристроїв, включаючи операційні системи для смартфонів, а не тільки певні додатки, що використовують дану технологію. Це означає, що можна забезпечити захист всього телефону. У кожної людини є лише їй притаманні особливості взаємодії зі своїми цифровими пристроями: швидкість, з якою вона друкує на клавіатурі, сила натискання на клавіші або кут, під яким вона водить пальцями по екрану смартфона. Ці моделі поведінки практично неможливо відтворити іншій людині.

Ще один плюс поведінкової біометрії – 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, це є ефективним засобом запобігання новим типам атак.

Метою цієї роботи є підвищення інформаційної безпеки мобільних пристроїв на основі аналізу цифрового рукописного підпису.

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 цифрового рукописного підпису та обрати один з них для подальших досліджень;

3) на основі обраного датасету дослідити інформативність параметрів цифрового рукописного підпису;

4) на основі проведених досліджень запропонувати сценарії використання цифрового рукописного підпису в якості біометричної технології захисту мобільних пристроїв.

1 ІНФОРМАЦІЙНА БЕЗПЕКА МОБІЛЬНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ANDROID

Згідно зі звітами рейтингового агентства Statcounter (рис. 1.1), на третій квартал 2023 року Android є найпоширенішою операційною системою (ОС) у світі з результатом 71.6 % від загальної кількості встановлених ОС, що вимагає від цієї ОС бути найбільш якісною в галузі інформаційної безпеки [1]. Однак, незважаючи на те, що компанія Google та виробники мобільних пристроїв постійно вдосконалюють систему безпеки, відкритість початкового коду і велика фрагментація платформи робить цю систему однією з найуразливіших для злочинного впливу.

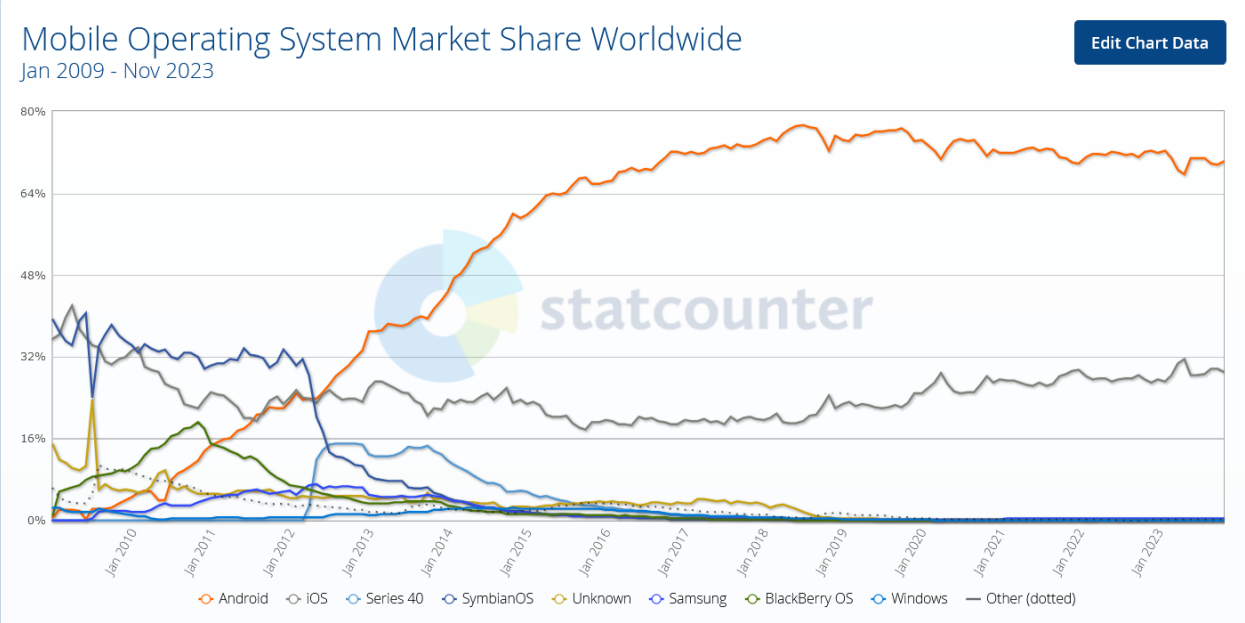


Рисунок 1.1 – Статистика часток ринку мобільних операційних систем

Головною причиною фрагментації екосистеми Android є застосована при створенні мобільних пристроїв технологія, що заснована на системі «кристал/чіп» (system on a chip, SoC). SoC полягає в інтегруванні на одному мікрочіпі центрального процесора, графічного прискорювача, радіомодуля та різної датчикової апаратури. Дана концепція дозволяє зменшити фізичний розмір пристрою, знизити енергоспоживання та підвищити продуктивність за

рахунок кращої інтеграції компонентів, але для взаємодії всієї системи потрібна розробка спеціальних драйверів. Драйвери розробляються виробниками різних чіпів на кристалі і, як правило, є пропрієтарними та унікальними для кожної моделі. В результаті, виробники мобільних пристроїв впроваджують отримані драйвери для SoC-системи у власні вироби, що призводить до залежності процедур оновлення програмного забезпечення. На рис. 1.2 наведено алгоритм виробництва мобільних пристроїв на базі Android. Через велику кількість виробників чіпсетів та мобільних пристроїв (ODM – виробник, вироби якого створюються за оригінальним проектом; OEM – виробник, деталі та обладнання якого можуть бути продані іншим виробникам) утворюється високий рівень фрагментації платформи без можливості оперативного забезпечення актуальними оновленнями мобільних пристроїв.

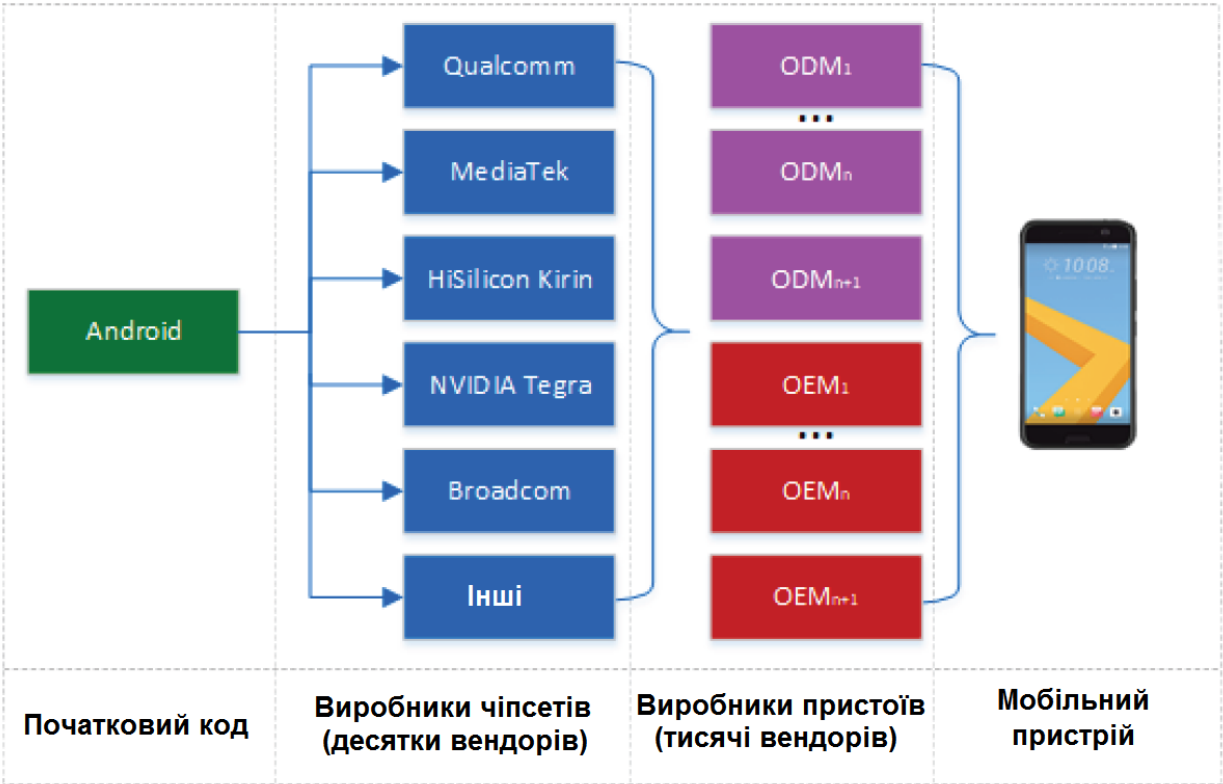


Рисунок 1.2 – Алгоритм виробництва пристроїв на ОС Android

Компанія Google для вирішення проблеми високої фрагментації пристроїв поступово робила важливі кроки. Проаналізуємо ці кроки.

1.1 Android 4.4 (KitKat, 2013)

Ще підтримується деякими розробниками додатків та, ймовірно, може вважатися відправною точкою посилення контролю над даними користувача та підвищення рівня безпеки загалом.

Робота із сертифікатами. У цій версії вперше почали приділяти увагу проблемі атаки «Людина посередині». Щоб убезпечити користувача, було вжито кілька важливих заходів, які будуть розвинені і посилені (в Android 6 і вище):

1. Попередження користувача про додавання нового довіреного сертифіката. Раніше з сертифікатами і сховищем користувача можна робити майже все, що завгодно, але з версії 4.4 Android хоча б попереджає, що встановлений сертифікат може призвести до небажаних наслідків.

2. Ускладнення перехоплення мережевого трафіку, що надсилається та отримується сервісами Google. З версії 4.4 система стежить за тим, щоб сертифікати з білого списку могли підключатися до цих сервісів.

Читання логів. Починаючи з Android 4.4, додатки користувача більше не мають доступу до системного журналу, і не можуть використовувати дозвіл «permission.READ_LOGS». Тепер цей дозвіл є тільки у системних додатків і Android Debug Bridge. За ідеєю це має захистити дані користувача, якщо вони раптом потрапляють у системний лог. Однак невідомо, як системні програми використовують цей дозвіл (тим більше, кількість системних додатків від виробника до виробника може суттєво відрізнятися).

Повноцінне використання SELinux. Система Android використовує багато функцій безпеки зі світу Unix, тому що в її основі лежить ядро Linux. Наприклад, кожен додаток у системі працює у власній «пісочниці» і не має доступу до даних інших додатків, а також не може безпосередньо звертатися до інших процесів у системі. Цей поділ реалізовано лише на рівні ядра і є класичним прикладом роботи з правами на директорії та файли в Linux. Під час встановлення програми система присвоює йому унікальні User ID (UID) та Group ID (GID), таким чином кожній програмі відповідає свій користувач.

Крім того, на рівні ядра унікальні UID та GID кожної програми використовуються для поділу доступу до ресурсів системи (пам'ять та процесорний час). Таким чином, на цьому ж рівні для кожної програми створюється своя власна «пісочниця» (Application Sandbox).

У перших версіях Android використовувався виключно механізм на основі прав користувача, без застосування додаткових заходів захисту, однак, починаючи з версії 4.4, Android використовує ще один механізм зі світу Linux – систему примусового контролю доступу – SELinux. Тепер вона працює в примусовому режимі, а не як раніше – у рекомендованому. Ця зміна переважно націлена на захист від експлойтів для підвищення привілеїв і спрямована лише на важливі та закриті частини системи, до яких у звичайного користувача не повинно бути доступу. Додатково застосовані деякі заходи щодо ускладнення атак на переповнення буфера. Для звичайних користувачів це не помітно, зате може суттєво допомогти у боротьбі зі шкідливими програмами, які намагаються отримати root-доступ або права адміністратора пристрою.

Зниження системних вимог. Google завжди усвідомлювала проблему дуже сильної фрагментації Android. Велика кількість виробників, кастомні зборки, кожен модифікує щось під себе і, як правило, виробники не поспішають оновлювати версії операційної системи через складність адаптації нових версій під внесені зміни. Такий підхід позначається на захищеності пристроїв, які тривалий час працюють без важливих оновлень безпеки.

Наочною ілюстрацією описаної ситуації є діаграма використання версій Android (рис. 1.3) [2]. Проблема стає особливо добре помітна в порівнянні з iOS (рис. 1.4) [3]. На діаграмі використання версій iOS яскраво виражені зубці, за якими можна однозначно визначити час виходу нової версії операційної системи. Важливо, що рання версія iOS, яка все ще використовується, це 14.6 (2019 рік). У той час, як на діаграмі Android досі можна побачити версію 5.1 (2014). І зміна має лінійний характер, без явних «переломів» після виходу нової версії. Єдина відмінність – це вихід Android 9 і вище.

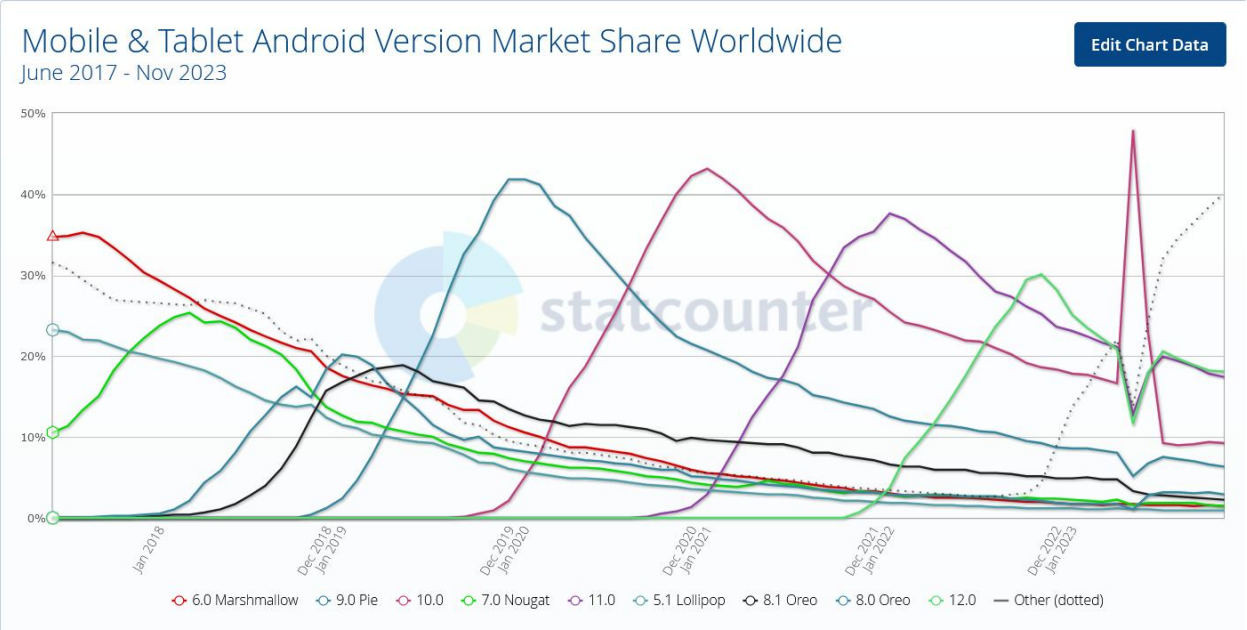


Рисунок 1.3 – Використання версій Android

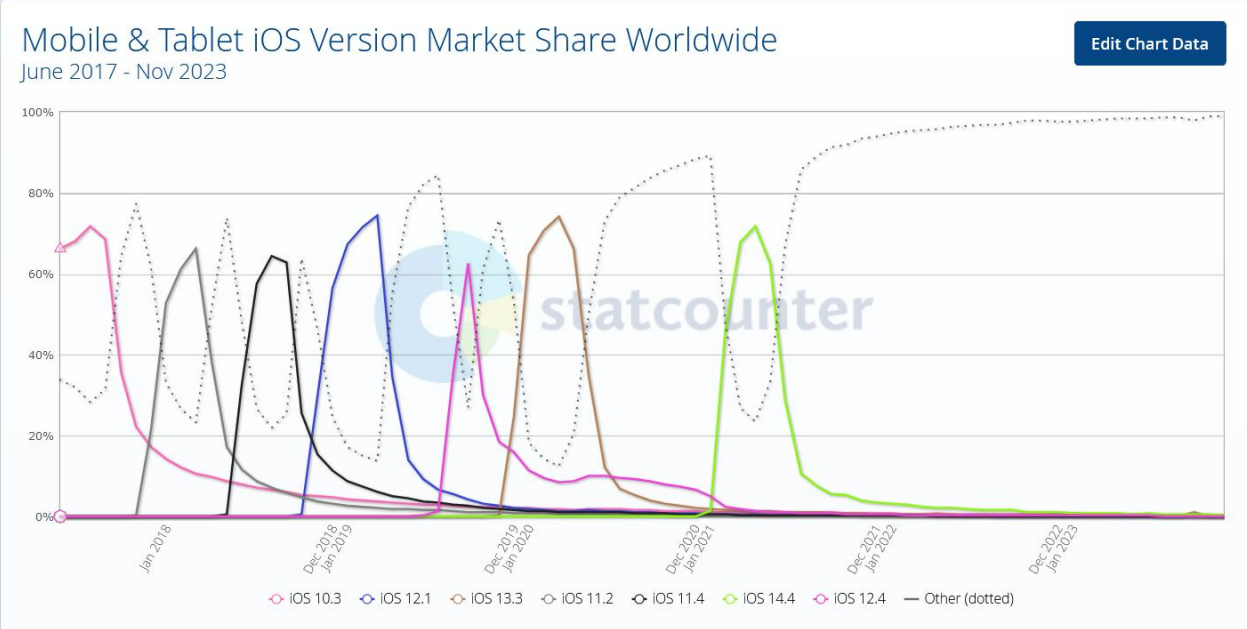


Рисунок 1.4 – Використання версій iOS

В Android 4.4 зроблено перший крок до вирішення цієї проблеми – було суттєво покращено продуктивність системи на більш слабких пристроях, щоб старі телефони могли безперешкодно оновитися на нову версію без втрати продуктивності.

1.2 Android 5 (Lollipop, 2014)

Випуск п'ятої версії Android можна назвати «проривом» у безпеці цієї операційної системи, бо саме в цій версії було закладено фундамент подальшого розвитку безпеки системи.

Посилення режиму SELinux. Android 5 продовжив справу свого попередника (Android 4) та ще більше інтегрував SELinux у захисні механізми системи. Тепер Enforcing mode (примусовий режим) обов'язковий не тільки для окремих частин системи, але й для решти, включаючи додатки користувача. Таким чином, Android 5 можна назвати першою версією, яка повноцінно використовує можливості SELinux для розмежування доступу та контролю.

Шифрування даних на пристрої. Попередні версії Android не використовували шифрування диска за замовчуванням, така опція була, але для її включення необхідно було ґрунтовно покопатися в налаштуваннях. Починаючи з п'ятої версії, Android використовує стандартне шифрування диска за допомогою класичного способуFull-Disk Encryption. Але не обійшлося і без мінусів:

1. Дані, що зберігаються на SD-карті, все ще не захищені і не зашифровані.

2. Використовується досить слабкий спосіб захисту ключа шифрування, знання якого дозволяло отримати всі дані. Цей секретний ключ був зашифрований з використанням пароля, що є рядком «default_password» і його не можна було змінити, якщо пристрій не підтримував режим Secure Startup. Цей режим дозволяв використовувати довільну фразу або цифровий код замість стандартного пароля (найчастіше використовувався код-пароль, встановлений на пристрої). Але для ввімкнення Secure Startup необхідно було вручну вибрати цей спосіб завантаження.

3. Secure Starup має один побічний ефект – введення пароля здійснювалося на ранньому етапі завантаження системи і без нього телефон навіть не приймав дзвінки.

Перші кроки в біометрії та Smart Lock. За статистикою, раніше далеко не всі користувачі встановлювали код блокування на свій телефон, аргументуючи це тим, що незручно щоразу його вводити, щоб скористатися пристроєм, наприклад, зробити фото і т.д. Щоб зробити розблокування зручнішим, Google анонсувала функцію Smart Lock, яка дозволяла розблокувати пристрій із встановленим паролем за допомогою різних Bluetooth або NFC аксесуарів. Додатково можна було включити опції розблокування в певних місцях на основі даних GPS, а також заборонити блокувати пристрій, поки він знаходиться у вас в руках (на основі даних з акселерометра). Також вперше було додано використання біометрії, а саме функцію розпізнавання обличчя.

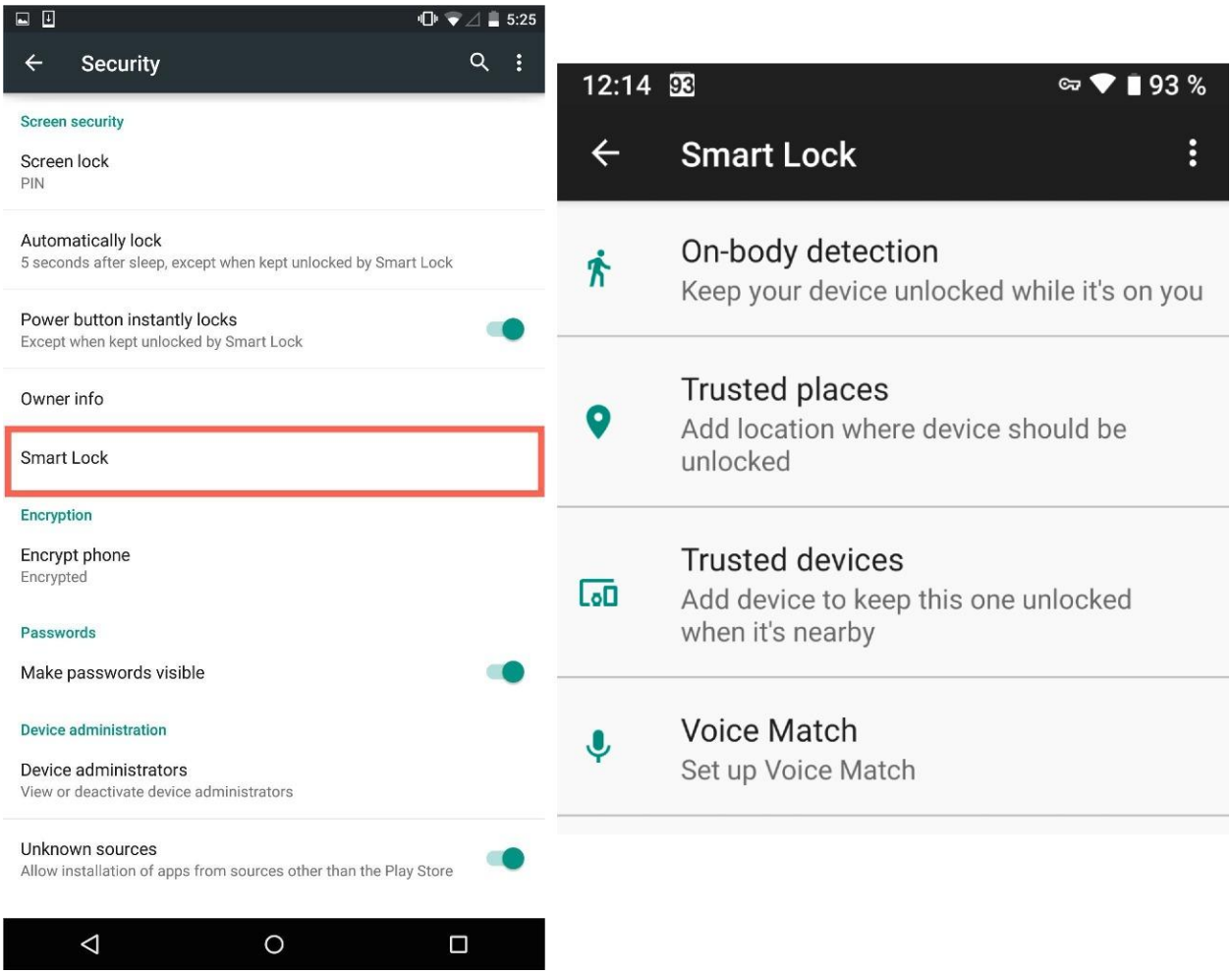


Рисунок 1.5 – Налаштування SmartLock в Android 5

Гостьовий режим. Продовжуючи тему «передачі» пристрою будь-кому, Android 5 став доступний гостьовий режим. Передаючи комусь телефон, можна було швидко перевести його в режим гостя, в якому він виглядає, як після скидання до «заводських налаштувань».

Декілька дуже корисних і потрібних функцій при втраті пристрою з'явилося в п'ятій версії Android.

Першою є доступ до телефонної книги, фотографій та повідомлень через обліковий запис Google. Тобто дані тепер синхронізувалися з хмарою і достатньо було увійти до свого облікового запису на новому телефоні, щоб відновити всю важливу інформацію з втраченого пристрою.

Друга дуже важлива функція – це можливість показати на карті місцезнаходження телефону (або його останні координати до того, як він був вимкнений), і головне – можливість віддаленого очищення пристрою.

Третя важлива функція – це захист від скидання до заводських налаштувань. Увімкнений пристрій не може виконати Factory Reset без введення аутентифікаційних даних облікового запису Google (якщо телефон вкрали, його вже не вдасться продати — він вимагатиме входу в систему).

Перехід оновлення деяких компонентів на Google Play Services. До 5 версії для оновлення Android необхідно було отримати апдейт від виробника пристрою. Тобто, ланцюжок оновлення виглядав досить складно і непередбачувано: спочатку Google дізнавалася про проблему і вирішувала її, додавала виправлення в проект AOSP, виробники пристроїв при черговому плановому оновленні забирали новий код з AOSP і компілювали його під себе, вносячи зміни, і тільки після цього він міг потрапити до кінцевого користувача.

З виходом 5-ї версії було запущено процес постачання оновлень для частини компонентів операційної системи (а саме дляWebView) через механізм оновлення Google Play. Фактично це означало, що телефон своєчасно отримуватиме всі актуальні оновлення так само, як оновлюються програми. Зручно, просто і для закриття критичних вразливостей не потрібно чекати, коли виробник випустить свій патч.

1.3 Android 6 (Marshmallow, 2015)

Після випуску 5-ї версії компанія Google продовжила додавати нові механізми безпеки, але також почала переосмислювати попередні підходи та допущені помилки. Це, напевно, перша версія Android, яка починає піклуватися про безпеку даних користувачів та доступ до цієї інформації для сторонніх програм.

Зміна логіки роботи з Permissions. Операційна система Android влаштована таким чином, що для виконання деяких операцій або доступу до ресурсів, програма повинна мати певний дозвіл. Ці дозволи поділяються на кілька рівнів: Normal та Dangerous. Їх відмінність у тому, що Dangerous-дозволи дозволяють отримувати особисту інформацію користувача або здійснювати потенційно небезпечні дії (наприклад, доступ до контактів або SMS-повідомлень). До Android 6 користувач під час встановлення програми бачив усі дозволи, які запитує програма. Спочатку йшли всі «небезпечні» дозволи, а згодом – усі інші. Маючи всю інформацію перед очима, користувач може зрозуміти, до чого буде мати доступ додаток, і прийняти рішення про його встановлення та використання.

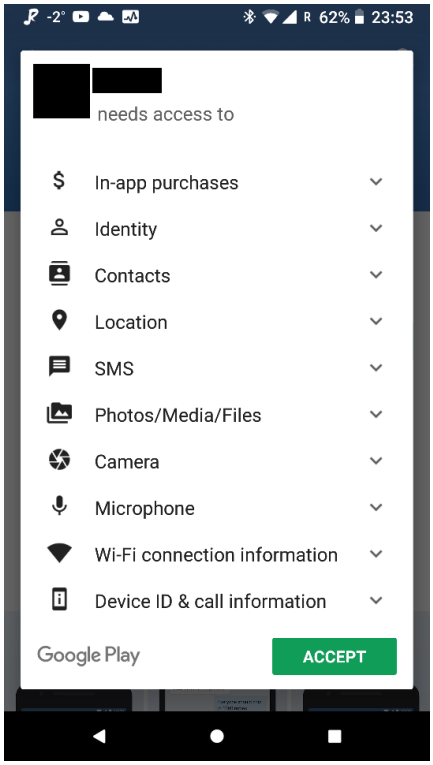


Рисунок 1.6 – Екран встановлення програми в Android 5

Починаючи з Android 6, підхід змінився: тепер при установці програми немає екрана зі списком усіх дозволів. Програма автоматично отримує всі необхідні Normal-дозволи, а Dangerous-дозволи необхідно запитувати в процесі роботи. Тобто, тепер розробнику недостатньо просто вказати, що додатку потрібен, наприклад, доступ до контактів. Щоб отримати його, необхідно явно викликати діалог підтвердження.

Доступ до апаратних ідентифікаторів. Google до версії 6 частково обмежувала права додатків на доступ до даних користувача, наприклад обмеження на читання системного журналу, але, починаючи з Android 6, це стало набувати серйозного масштабу. Зокрема, у цій версії Android MAC адреси Wi-Fi та Bluetooth адаптерів не можна отримати без спеціального та явного дозволу користувача. А зроблено це, щоб ускладнити ідентифікацію пристрою сторонніми програмами без відома користувача та співставлення цих даних з даними Wi-Fi-міток, що часто використовується для відстеження пристрою користувача та його переміщення.

Довірене завантаження. Спроби повторити ланцюжок довіреного завантаження iOS робилися Google ще у версії 4.4, але вони не були дуже успішні. Цей функціонал не був повністю опрацьований і мав необов'язковий характер. Починаючи з версії Android 6, функціоналVerified Boot, який забезпечує захист від різних модифікацій системного розділу та важливих файлів системи при завантаженні, починає активно розвиватися і стає все більш складним та підготовленим до повноцінного використання. Зокрема, у цій версії реалізовано низку криптографічних перевірок цілісності всіх частин – від завантажувача до операційної системи. Однак користувачі все ще можуть завантажити пристрій. Якщо перевірка не була пройдена – під час завантаження пристрою виникає екран, який сповіщає про модифікований завантажувач.

З версії 6 підключення USB-пристроїв тепер за замовчуванням налаштовано на режим «тільки заряджання». Щоб отримати доступ до пристрою та його вмісту, користувач повинен явно надати на це дозвіл.

Біометрія та апаратне сховище. Повноцінна можливість використову-

вати відбиток пальця для розблокування пристрою з'явилася тільки в Android 6. Також, в цій версії була представлена можливість захисту ключів шифрування, які створювалися в додатку з використанням відбитка, тобто доступ до ключа стало можливо отримати тільки після проходження користувачем процедури біометричної ідентифікації.

Це стало можливим завдяки реалізації окремого апаратного рівня зберігання інформації, яку не можна було отримати навіть за фізичного доступу до пристрою.

Можливість заборони використання http. З виходом Android 6, Google представила атрибут useCleartextTraffic як засіб захисту від випадкового використання протоколу http. При правильно виставленому прапорі застосунку в процесі роботи буде заборонено здійснювати взаємодію за протоколом http з будь-якими серверами. Це налаштування є першим кроком Google на шляху спрощення конфігурації мережевих взаємодій для програм.

Інформація про встановлене оновлення безпеки. До Android 6.0 залишалося тільки здогадуватися, чи отримував телефон оновлення безпеки та в якому стані він зараз перебуває. Але в цій версії до розділу "Про телефон" було додано інформацію про те, яке оновлення безпеки встановлено на даний момент. Теоретично, це мало змусити виробників пристроїв приділяти більш пильну увагу доставці оновлень, а користувачам дозволяло отримати повнішу інформацію про безпеку свого телефону.

Але, як показало дослідження [4], в ході якого протягом двох років експерти спостерігали за інформацією про оновлення безпеки та перевіряли актуальний стан пристроїв, багато виробників хитрують під час випуску оновлень і, хоча вони стверджують, що їхні пристрої отримали всі актуальні патчі, насправді це не так. Деякі виправлення з невідомих причин «випадають» зі списків і взагалі не доходять до користувачів. Але найцікавіше, що іноді виробники просто змінюють дату оновлення, взагалі не встановлюючи жодних патчів протягом багатьох місяців.

Missed patches	Vendor	Samples
0 to 1	Google	Багато
	Sony	Декілька
	Samsung	Багато
	Wiko	Декілька
1 to 3	Xiaomi	Достаньо
	OnePlus	Достаньо
	Nokia	Декілька
3 to 4	HTC	Декілька
	Huawei	Достаньо
	LG	Достаньо
	Motorola	Достаньо
More than 4	TCL	Достаньо
	ZTE	Декілька

Missed patches	Chipset	Samples
< 0.5	Samsung	Багато
1.1	Qualcomm	Багато
1.9	HiSilicon	Достаньо
9.7	Mediatek	Достаньо

Рисунок 1.7 – Статистика пропущених патчів безпеки виробниками мобільних пристроїв

1.4 Android 7 (Nougat, 2016)

Розвиваючи концепцію довіреного завантаження, яке суттєво покращили в Android 6, починаючи з 7-ї версії, скомпрометовані пристрої більше не запускаються. Також додано підтримку виправлення помилок, які могли виникнути при завантаженні пристрою (це більшою мірою спрямовано на підвищення стабільності роботи системи, ніж на захист від зловмисників, але тепер теж входить у реалізацію ланцюжка довіреного завантаження у виконанні Google).

Перехід на пофайлове шифрування (FBE). В Android 5 вперше було за замовчуванням включено шифрування диска (внутрішню пам'ять пристрою), але воно мало кілька істотних недоліків. Починаючи з Android 7, з'явилася опція пофайлового шифрування даних (замість раніше використовуваного Full-Disk Encryption). Цей тип шифрування набагато більш зручний для користувача і є деяким поєднанням FDE і Secure Startup, що демонструє всі пози-

тивні сторони кожного зі способів.

Більшість даних користувача зашифровані з використанням ключа-пароля, встановленого на пристрої, а виконувані файли додатків і системні утиліти, необхідні для роботи пристрою, до першого розблокування зашифровані за допомогою апаратних ключів і доступні відразу після завантаження пристрою.

Робота з мережевими з'єднаннями. Сертифікати, які додає користувач, тепер за замовчуванням вважаються недовіреними і не можуть використовуватись для організації захищеного з'єднання. Іншими словами, навіть якщо користувач встановив сертифікат зловмисника на свій пристрій, це не дає змоги здійснити атаку "Людина посередині".

Другою дуже важливою зміною є можливість налаштування безпеки мережевої взаємодії, що дозволяє чіткіше визначати параметри з'єднань. Тепер конфігурація мережевої взаємодії – це файл XML, в якому налаштовуються параметри безпеки. Ключові можливості, які надає такий підхід:

1. Custom trust anchors – налаштування довіри центрам сертифікації (CA), яким довірятиме програма при мережній взаємодії. Наприклад, довіра до певних самопідписаних сертифікатів або обмеження набору загальнодоступних центрів сертифікації, яким довіряє програма (додані користувачем у довірені або ті CA, яким довіряє система).

2. Debug-only overrides – налаштування з'єднань спеціально для Debug-версії програми, що дозволяє розмежовувати середовища розробки та Production.

3. Cleartext traffic – більш детальне налаштування дозволів або заборони з’єднань по http для всієї програми або конкретних доменів.

4. Certificate pinning – налаштування для реалізації SSL Pinning, тобто тепер не потрібно самому відстежувати перевірку сертифіката сервера, досить просто вказати його значення в налаштуваннях і система візьме на себе всі інші рутинні операції.

1.5 Android 8 (Oreo, 2017)

Однією зі значних змін в політиці інформаційної безпеки Android стала концепція Treble. Treble – це спосіб поділу Android на дві незалежні частини, які забезпечують зв'язок із «залізом» (ядро Linux) та операційною системою Android, а також покликані вирішити проблеми фрагментації Android та доставки патчів на пристрої різних виробників. Таким чином. Google більше не залежить від виробників пристроїв щодо оновлень безпеки для внутрішніх компонентів Android. Тепер Google сама вирішує, як і коли буде оновлено телефон та які оновлення безпеки необхідно встановити.

Доступ до ідентифікаторів пристрою. В Android 6 вперше було реалізовано заборону доступу програмам до апаратних ідентифікаторів пристрою, в Android 8 цей процес продовжився. Тепер програмам заборонено отримання інформації про Android ID – унікальний ідентифікатор, який генерується при першому завантаженні пристрою (тепер для кожної програми він буде унікальним). Також серійний номер телефону не можна отримати без спеціального та явного дозволу користувача. До заборонених ідентифікаторів також потрапили час останнього завантаження та MAC-адреса Bluetooth.

В Android 8 ізолювали WebView, тепер він виконується в окремому процесі. Це означає, що за наявності вразливостей у цьому компоненті більше не вдасться отримати доступ до процесу застосунку, оскільки ізоляція реалізована з досить жорсткими умовами, рендеринг сторінки запускається в обмеженій «пісочниці» без доступу до ресурсів системи та Інтернету, тобто просто відображає контент сторінки.

Коли телефон сканує ефір на наявність точок доступу, разом із різними параметрами він надсилає і свою MAC-адресу. Якщо зібрати інформацію з кількох точок доступу, можна визначити, де і коли знаходився пристрій з певним MAC. В Android 8 додали функцію рандомізації MAC-адреси при пошуку мереж. Це важливий крок на шляху забезпечення приватності користувача – він не дозволяє відстежити реальну MAC-адресу та співставити її конкретним пристроєм.

1.6 Android 9 (Pie, 2018)

Рандомізація MAC-адреси під час підключення. В Android 8 MAC-адреси змінювалися лише при скануванні точок, доступних для підключення. Логічним продовженням стало використання випадкової адреси під час підключення до мережі. Тобто, при підключенні до різних точок доступу їм відповідатимуть різні MAC-адреси, що ускладнить ідентифікацію пристрою.

В Android 9 за замовчанням для додатків стоїть заборона використання протоколу http. Звичайно, можна його примусово відключити для всього або для певних доменів, але якщо це не зроблено, програма просто не зможе з’єднатись з сервером по небезпечному протоколу.

Приватний DNS (реалізація DNS over TLS) шифрує весь DNS-трафік, запобігаючи прослуховуванню або зміні його третьою стороною. Ця функція додає недостатній рівень безпеки та конфіденційності всім DNS-запитам, які надсилає пристрій. За замовчанням Android автоматично використовує DNS over TLS, якщо цей функціонал підтримується DNS-сервером. Але це також винесено в налаштування і може бути відключено.

В версії 9 Google реалізувала шифрування хмарних резервних копій на основі пароля користувача і тепер вони захищені від доступу зі сторони співробітників Google. Ця функціональність автоматично вмикається при дотриманні таких умов:

1. Користувач увімкнув резервне копіювання на Android 9 або вище.
2. Користувач встановив блокування екрана свого пристрою за допомогою PIN-коду, графічного ключа або пароля.

Для відновлення даних із зашифрованих резервних копій потрібно ввести PIN-код пристрою, графічного ключа або пароля.

До Android 9 можна було дати доступ до файлу всередині своєї пісочниці, встановивши йому прапор WORLD_READABLE або WORLD_WRITABLE. Це було досить поганою практикою з непередбачуваними наслідками. Починаючи з дев'ятої версії Android використання такого

підходу заборонено (додатково контролюється правилами SELinux), а для надання доступу до даних своєї програми необхідно використовувати тільки механізми IPC (міжпроцесної взаємодії), у вигляді Content Providers, які більш безпечні, підконтрольні розробникам та регулюються внутрішніми механізмами безпеки.

Заборона використання сенсорів у фоновому режимі – одна з головних security-новацій у Android 9. Тепер автоматично заборонений доступ на використання камери, мікрофона та будь-яких сенсорів додатками, які перебувають у стані Idle, тобто згорнуті та працюють у фоні.

В Android 9 доступ до приватних API заборонено. Більше того, нова версія Android виводить повідомлення у тому випадку, якщо програма використовує оголошені застарілими (deprecated) API. Це має змусити розробників перейти до використання нових API.

1.7 Android 10 (Quince Tart, 2019)

Ця система продовжує справу 9-ї версії, поступово роблячі ще жорсткішими вимоги щодо ідентифікації пристрою та доступу до різної інформації користувача.

Доданий в Android 9 механізм рандомізації MAC-адреси при підключенні добре зарекомендував себе, так що в новій 10-й версії більше не потрібно руками включати цю опцію – тепер вона включена за замовчуванням.

Якщо раніше можна було спокійно запускати Activityу фоні і, наприклад, намагатися збирати якусь інформацію (наприклад, реалізувати атаку Task Hijacking), то починаючи з 10-ї версії це заборонено. Залишається лише один варіант: попередити користувача і лише після цього запускати фонові Activity.

Ще кілька ідентифікаторів (Serial Number, IMEI, DeviceId, MEID, SIM Serial Number, Subscruber ID) перейшли до розряду заборонених до отримання звичайними програмами. З одного боку, це суттєво ускладнює життя різ-

ним додаткам, які стежать за користувачем та ідентифікують пристрій. Але, з іншого боку, легітимним додаткам стає набагато складніше визначити унікальність пристрою та «прив'язатися» до нього. Тим не менш, вбудовані програми від виробника та компанії Google, як і раніше, мають доступ до цієї інформації.

Починаючи з 10-ї версії, доступ до буфера обміну дозволено, тільки якщо програма активна і знаходиться у foreground (на передньому плані). Це зроблено з метою протидії троянам, що збирають усе, що знаходиться в буфері обміну, а потім видобувають з цих даних критично важливу інформацію, наприклад, адреса криптогаманця.

Заборона отримання інформації на екрані. Щоб захистити вміст екрана, доступ до нього в Android 10 істотно обмежений, для чого змінені відповідні дозволи (READ_FRAME_BUFFER, CAPTURE_VIDEO_OUTPUT та CAPTURE_SECURE_VIDEO_OUTPUT).

Починаючи з Android 10, ці дозволи доступні лише системним програмам. Система стежить за використанням дозволів за допомогою signature-access. Тобто використовувати дозвіл може тільки додаток, який підписаний тим же сертифікатом, що і «власник» дозволу (той додаток, який його реєструє в системі). А починаючи з Android 10, ця програма – system, тобто сама система Android. На даний момент це один із найдієвіших способів перенести різні дозволи у формат «системних», просто обмеживши до них доступ за цифровим підписом програми.

Програми, які потребують доступу до вмісту екрана пристрою, повинні використовувати спеціальний MediaProjection API, який завжди попереджає користувача про намір програми отримати доступ до екрана та вимагає його явну згоду.

1.8 Android 11 (Red Velvet Cake, 2020)

З'явився абсолютно новий механізм одноразових дозволів, які дають доступ тільки на той час, поки програма не буде закрита, і наступного разу користувачеві знову потрібно буде видати цей дозвіл. Цей функціонал працює тільки для доступу до геолокації, мікрофону та камери.

В Android 11 реалізовано функцію, що дозволяє заблокувати запит дозволів, якщо користувач двічі скасував запит. Після подвійної відмови у дозволі користувачам доведеться вручну надати їх у налаштуваннях.

Коли програма запитує дозвіл на доступ до геолокації, Android 11 спочатку видає такий дозвіл тільки для запущеної програми, а якщо геолокація необхідна і у фоновому режимі, формується окремий запит. Цей другий запит вимагає від користувачів додаткових дій замість просто натискати «Ок…, Ок…, дозволить…». Щоб увімкнути фоновий доступ до геолкації, користувачі повинні на сторінці дозволів програми вибрати для визначення місцезнаходження параметр «Дозволити весь час». Крім цього, Google також вимагає, щоб розробники додатків пояснювали, чому їх програмі в першу чергу потрібен фоновий доступ до геолокації.

Якщо було встановлено додаток, надано йому дозволи, але він не використовується протягом кількох місяців (точні часові рамки «кілька місяців» так і не визначені), дозволи будуть відкликані та можуть бути повторно включені лише вручну. Ця функція працює не з усіма програмами і не включена за замовчуванням.

Продовжуючи розвивати механізм Treble, значно покращений в Android 8, система тепер отримує всі критичні оновлення безпосередньо з Google Play. Це дуже спрощує процес оновлення та підвищує загальний рівень безпеки пристроїв, оскільки тепер оновлення системи можуть встановлюватися автоматично.

1.9 Android 12 (Snow Cone, 2021)

За аналогією з iOS під час використання камери та мікрофона у правому верхньому куті буде відображатися окремий індикатор, який повідомить користувача, що якась програма задіює вказані пристрої. Це не просто індикатор, а повноцінна область, звідки можна відразу ж «відібрати» дозволи.

Іншою не менш ваджливою особливістю стала наявність у системі «перемикача», який відключає використання мікрофона та камери для всіх програм.

Приватний дашборд – рішення, що показує, які програми запитували доступ до камери, мікрофону та геолокації за останні 24 години. Аналогічно з індикацією про активність камери і мікрофона ці дозволи можна відразу «відібрати». Більше не потрібно «ходити в налаштування», шукати там програму, розбиратися в купі меню, а достатньо натиснути пару кнопок і програма більше не зможе використовувати ті частини системи, які користувач заборонив.

У 10-й версії Android було заборонено доступ до буферу обміну. У новій версії Android механізм роботи з даними з буфера обміну ще більш вдосконалено. Тепер, коли програма намагається отримати дані з буфера обміну, користувачеві буде виведено повідомлення (toast повідомлення), що інформує, що програма «залізла» в скопійовані дані.

В Android-додатку присутні так звані компоненти, що експортуються, які можуть бути викликані іншими додатками. Щоб зробити компонент експортованим, достатньо вказати йому атрибут exported=true, але це не єдиний спосіб. Наприклад, при вказівці будь-яких intent-фільтрів компонент автоматично стає експортованим. І це не рідко призводило до проблем безпеки, коли внутрішні елементи програми були доступні для інших додатків. І 10-й версії Google оголосила атрибут exported обов'язковим до заповнення для всіх компонентів програми.

1.10 Android 13 (Tiramisu, 2022)

В Android 13 для посилення посилення безпеки зазнав змін підход до надання користувачами дозволів на доступ до ресурсів смартфону.

Починаючи з цієї версії ОС, додатку можна дозволити доступ не до всіх мультимедіа-файлів відразу, а лише до окремих типів: фото, відео, аудіо (Granular permission access). В той же час Google рекомендує розробникам ПЗ використовувати покращене рішення Photo picker, яке дозволяє користувачеві видавати додатку право на доступ взагалі до окремих зображень, звукових або відеофайлів, в той час як решта медіатеки для нього залишиться під забороною.

Крім цього, додатки в Android 13 повинні запитувати у користувача окремий дозвіл на виведення повідомлень. Без нього будь-які спроби виводу повідомлень в область повідомлень блокуватимуться.

Скорочено кількість програм, які потребують доступу до інформації про розташування користувача. Наприклад, програмам, які виконують операції сканування безпровідних мереж, тепер не потрібні повноваження, пов'язані з визначенням розташування.

Розширено можливості, націлені на підвищення конфіденційності та інформування користувача про можливі ризики. Крім попереджень про доступ додатка до буфера обміну в Android 13 при копіюванні користувачем конфіденційної інформації, такої як адреса електронної пошти, номер телефону, логін або пароль, система автоматично очищатиме історію буфера обміну через деякий час.

В Android 13 в додаток Google Messages було додано наскрізне шифрування для групових чатів.

Ще одним нововведенням став додаток-сервіс «Особиста безпека», який інтегровано у новий розділ налаштувань під назвою «Безпека та екстрені випадки». За допомогою цього сервісу ми можемо зробити такі дії:

1) налаштувати функцію екстреного дзвінка для автоматичного дзвінка до служби порятунку, надсилання СМС вибраним контактам та запису відео;

2) повідомити контакти для екстрених випадків про місце розташування користувача у разі надзвичайної ситуації;

3) якщо користувач не відчуває себе у безпеці, можна вказати час, коли смартфон перевірить, чи все гаразд з користувачем (якщо користувач не відповідає, то відбудеться відправка даних контактам, зазначених в екстрених випадках).

1.11 Android 14 (Upside Down Cake, 2023)

Repair Mode – функція, що реалізована для відповідності новим європейським законам про право на ремонт. Перевівши смартфон в режим ремонту, користувач зможе частково заблокувати смартфон перед відправкою його в сервісний центр. За допомогою Repair Mode в Android генерується тимчасовий захисний профіль, який блокує всі дані користувача, але при цьому залишає відкритою всі основні функції смартфона, щоб під час ремонту майстер мав можливість протестувати дисплей, камеру, телефонний модуль, динаміки, безпровідний модуль тощо.

Наступне нововведення – можливість приховувати конфіденційну інформацію під час запису екрана. Ця функція дозволяє користувачеві обмежити запис потрібним чином – наприклад, запис екрана для конкретного додатка, приховати системні повідомлення, повідомлення або вхідні дзвінки. Або обмежити видимість об'єктів на головному екрані, щоб у запис не потрапила якась інформація з віджету поштового клієнта чи органайзера. Якщо вибрати запис екрана з конкретного додатка і вийти з нього, Android записує чорний екран, поки користувач знову не повернеться до додатка.

Покращена функціональність можливості часткового надання повноважень для доступу лише до вибраних користувачем фотографій та відео. Як тільки додаток переходить у фоновий режим або його робота завершується, повноваження відкликаються. Аналогічний інструмент під назвою Photo Picker з'явився ще в Android 13, проте для його використання додатки повин-

ні були підтримувати сучасне API. В Android 14 система сама обмежуватиме додаткам доступ до галереї незалежно від підтримки Photo Picker.

У додатках, що працюють у фоновому режимі, тепер обов'язкова вказівка типу фонового сервісу. Під час роботи система перевіряє відповідність зазначеного типу сервісу, запитаних повноважень та API, що використовується. Наприклад, якщо додаток вказав тип фонового сервісу LOCATION, мається на увазі, що він може запросити повноваження, що стосуються лише геолокації, а ні, наприклад, мікрофону.

Додано можливості підтвердження доступу до геолокації. Так, у діалозі із запитом підтвердження доступу тепер з'явився новий розділ з інформацією про те, коли саме додаток може отримувати дані про місцезнаходження плюс подробиці, де саме можна отримати додаткові відомості про цю функцію.

У новій версії заборонено встановлення програм із SDK нижче 23. За словами розробників, це дає можливість блокувати обхід обмежень повноважень за допомогою прив'язки до старих API. Правда, ті програми, що вже встановлені, але використовують старі API, після оновлення Android все ж таки працюватимуть.

Код Android 14 повністю переписано з C/C++ на Rust. Це дозволило подолати велику кількість вразливостей, пов’язаних з помилками безпеки пам'яті за допомогою технології Memory Tagging Extension (MTE), що вже кілька років використовується в ОС Linux.

Технологія MTE допомагає знаходити у софті вразливості, пов'язані з пам'яттю. За час тестування сумісності MTE з Android співробітники Google виявили близько сотні таких багів. Технологію можна використовувати під час тестування софту або фіксувати проблеми пам'яті прямо на пристрої користувачів. Для останнього MTE має особливий енергоефективний фоновий режим. MTE – повністю апаратна технологія і наразі сумісна з чіпсетами на архітектурі ARMv8.5 та новіше. Примітно, що серія Pixel 7 несумісна із MTE, оскільки фірмовий процесор Tensor G2 побудований на ARMv8.2. Pixel 8 – перший смартфон від Google, що підтримує технологію MTE.

Android 14 містить інструменти для відключення 2G-мереж на смартфонах та планшетах. Ця можливість є доступною для корпоративних клієнтів та урядових установ, які використовують пристрої з Android Enterprise. Справа в тому, що 2G-мережі схильні до низки ризиків, коли трафік може бути перехоплений, а потім розшифрований за допомогою таких програм, як помилкові базові станції (FBS) та Stingrays.

Також у новій версії ОС усунено ризики нульового шифрування стільникового зв'язку. За словами Google, це дозволить посилити конфіденційність даних, захистивши голосовий трафік і SMS від перехоплення.

1.12 Висновки

Вбудовані функції ОС Android забезпечують безпеку багатьох дій користувача. Наприклад, вони захищають пристрої від шкідливих програм та інших загроз. Наведемо деякі з основних функцій:

1. Шифрування файлів та повне шифрування диска для захисту приватності.

2. Різні методи аутентифікації, у тому числі з використанням PIN-коду та біометричних даних, наприклад, розпізнавання обличчя або відбитка пальця.

3. Google Play Захист – вбудований антивірус для Android, який автоматично перевіряє завантажені програми на наявність шкідливого програмного забезпечення та повідомляє про необхідність видалити потенційно небезпечні програми.

4. Функція Verify Apps для блокування потенційно шкідливого програмного забезпечення.

5. Управління дозволами контролю активності додатків.

6. Автоматична перевірка паролів, які використовуються під час автозаповнення, з базами відомих скомпрометованих паролів.

7. Спам-фільтр, що попереджає про підозрілі дзвінки та повідомлення.

8. Google Safe Browsing для захисту від небезпечних сайтів та файлів.

9. Функція Smart Lock, яка розблокує пристрій лише у ситуаціях, заданих користувачем.

10. Сервіс «Знайти пристрій» для визначення координат втраченого смартфону та «Захист пристрою» для віддаленого блокування та видалення даних.

Ці вбудовані функції забезпечують високий рівень захисту пристроїв Android – це система з відкритим вихідним кодом, і зловмисникам не важко знайти «прогалини» в її безпеці і змінити код під свої потреби. Користувачів Android майже втричі більше, ніж користувачів iOS, а значить, на Android-пристроях зберігається набагато більше особистої інформації, що цікавить кіберзлочинців, які невпинно працюють над створенням додатків для злому Android. Саме тому шкідливих програм для атак на пристрої Android у 50 разів більше, ніж для атак на пристрої iOS. А оскільки Android, на відміну від інших операційних систем, допускає встановлення сторонніх додатків, у шкідливих програм набагато більше шансів потрапити на пристрої з цією ОС.

Згідно з нещодавно опублікованим звітом [5] для проведення 60 % атак, зафіксованих у листопаді 2023 року, зловмисникам знадобилося всього чотири троянці:

1) SpyAgent.JA – шкідлива програма, яка збирає особисті дані, наприклад, повідомлення та контакти користувача, надаючи доступ до камери та мікрофона зараженого пристрою. Це дозволяє зловмисникам таємно стежити за зараженими користувачами;

2) Agent.AXC – програми, які передають конфіденційні дані, такі як SMS-повідомлення, журнали дзвінків, контакти або розташування GPS;

3) Downloader.DN – перепаковані програми, взяті з Google App Store та заражені агресивним рекламним ПЗ. Деякі рекламні програми завантажують інші варіанти зловмисних програм;

4) SMSSend.AYE – шкідливе ПЗ, яке при першому запуску намагається зареєструватися в системі як SMS-застосунок за замовчуванням, запитуючи

згоду користувача. У разі успіху він збирає вхідні та вихідні повідомлення користувача та пересилає їх на командно-контрольний (C&C) сервер.

У 2022 році багато Android-пристроїв було атаковано шкідливою програмою MailBot. Це небезпечне ПЗ здатне красти паролі, фінансову інформацію та дані з криптогаманців, яке успішно ховається від усіх механізмів захисту та обходить багатофакторну автентифікацію. Воно швидко поширюється, розсилаючи SMS-повідомлення за списком контактів, що зберігаються на пристрої жертви. Не менш небезпечні й інші шкідливі програми, наприклад AlienBot, який вбудовує шкідливий код у фінансові програми, відкриваючи зловмисникам шлях до пристрою та банківських рахунків жертви, або універсальний Anubis, який краде фінансові дані, перехоплює текст, що вводиться з клавіатури, і записує звук.

Незважаючи на уразливості Android, є чимало способів, які допоможуть максимально знизити ризик кібератаки. Для цього користувачам потрібно вживати додаткових запобіжних заходів, наприклад, використовувати надійні паролі та багатофакторну автентифікацію, завантажувати програми тільки з офіційного магазину Google Play і перевіряти дозволи, що запитуються. Використовувати VPN та антивірусні програми для Android, розроблені відомою компанією, та намагатися уникати публічних мереж Wi-Fi. Це знизить ризик кібератаки та крадіжки особистих даних.

2 ПРОБЛЕМИ БІОМЕТРИЧНОЇ АВТОРИЗАЦІЇ В МОБІЛЬНІЙ ОПЕРАЦІЙНІЙ СИСТЕМІ ANDROID

Наразі мобільні пристрої надають користувачам доступ до сервісів, що вимагають виского ступеня інформаційної безпеки, серед яких мобільний банкінг, месенджери та додатки, що зберігають особисті дані. Відповідно, пройшовши у той чи інший спосіб процедуру аутентифікації, зловмисник може отримати неавторизований доступ до конфіденційних даних на мобільному пристрої: фінансової інформації, облікових даних для доступу до соціальних мереж, даних контактів у мережах мобільного зв'язку. Цього може бути достатньо для повноцінного здійснення крадіжки особистих даних. Ця загроза стає особливо актуальною в наш час, коли спостерігається значне зростання кількості кібератак, а отже, і збитків, які зазнали користувачі мобільних пристроїв. Таким чином, існує незаперечна потреба у надійному захисті персональних даних користувачів та інтелектуальної власності компаній, доступ до яких здійснюється через мобільні пристрої.

Основою більшості систем захисту є процедура аутентифікації користувача, яка полягає у перевірці належності суб'єкту доступу (користувачу) пред'явленого ним ідентифікатора та підтвердження його справжності. У багатьох мобільних додатках для аутентифікації використовуються паролі або чотири-/шестизначні PIN-коди, які є найслабше захищеним способом автентифікації: вони можуть бути втрачені, випадково показані або нелегально передані авторизованим користувачем неавторизованому. Більше того, згідно зі звітом [6] 53 % мобільних додатків, що здійснюють перевірку на стороні клієнта, використовують небезпечне зберігання аутентифікаційних даних, 29 % серверних частин мобільних додатків мають недоліки реалізації двофакторної аутентифікації, 18 % усіх додатків не обмежують кількість спроб введення даних.

Іншим широко використовуваним фактором аутентифікації є біометри-

чні характеристики: фізіологічні (відбиток пальця або долоні, сітківка та райдужна оболонка ока, геометрія обличчя тощо) та поведінкові (хода, мова, динаміка введення тексту тощо) особливості суб'єкта. Біометричні характеристики не можуть бути втрачені, вкрадені або передані третім особам.

Однак, незважаючи на всі переваги біометричних характеристик, вони також мають свої проблеми. Однією з основних проблем є неправильне розпізнавання біометричних даних. Наприклад, сканер відбитків пальців може не спрацювати, якщо палець занадто мокрий. Також можливе неправильне розпізнавання обличчя через погане освітлення або зміну зовнішнього вигляду користувача (наприклад, нові окуляри або борода). Ще однією проблемою може бути хакерська атака на систему біометричної авторизації. Зловмисники можуть спробувати підробити відбиток пальця або використовувати інші методи, щоб обійти систему та отримати доступ до приватних даних. Також деякі користувачі можуть відчувати дискомфорт від використання біометричної авторизації. Наприклад, деякі люди можуть боятися, що їхні особисті дані можуть бути вкрадені або використані без їхньої згоди.

2.1 Помилки під час сканування відбитка пальця

Біометрична авторизація за допомогою сканеру відбитка пальця є одним із найзручніших і найбезпечніших способів ідентифікації користувача в мобільному пристрої. Однак у процесі використання можуть виникати певні проблеми та помилки:

1. Слабка якість відбитка пальця. Якщо відбиток пальця недостатньо чітко або частково сканується, система може не розпізнати його і зробити помилковий висновок про неправильну ідентифікацію. Щоб уникнути такої проблеми, рекомендується сканувати відбиток із чистими та сухими пальцями, а також стежити за тим, щоб сканер був чистим та не мав пошкоджень.

2. Пошкодження або зміна відбитка пальця. Якщо відбиток пальця був пошкоджений або змінений (наприклад, через травму або інші фізичні зміни),

це може спричинити помилки під час сканування. У таких випадках рекомендується оновлення біометричних даних.

3. Проблеми з апаратною частиною. Технічні неполадки сканера відбитка пальця або неправильне його використання також можуть призвести до помилок під час авторизації. У таких ситуаціях рекомендується перевірити налаштування сканера, оновити драйвери або звернутися до сервісного центру для діагностики та ремонту.

4. Проблеми з програмним забезпеченням. Неправильне налаштування програмного забезпечення або конфлікти з іншими програмами на пристрої можуть спричинити збої та помилки під час сканування відбитка пальця. У таких випадках рекомендується оновити програму або операційну систему, очистити кеш або звернутися до сервісного центру.

Важливо пам'ятати, що помилки при скануванні відбитка пальця можуть бути результатом як технічних неполадок, так і неправильного використання або недостатньої якості відбитка. У разі виникнення проблем рекомендується перевірити та виправити зазначені вище аспекти.

2.2 *Помилки під час аутентифікації за геометрією обличчя*

1. Технічні обмеження та помилки:

1) некоректна робота у поганих умовах освітлення;

2) неправильне розпізнавання обличчя через зміни зовнішності (наприклад, із зачіскою або без окулярів);

3) помилка при розпізнаванні обличчя у разі перекриття частини обличчя якимись предметами (наприклад, час від часу поміщати обличчя під головну хустку чи шапку).

2. Недостатня швидкість та ефективність:

1) тривалий час очікування для розпізнавання обличчя, особливо в умовах низької швидкості зв'язку (у разі, якщо доданок використовує свій власний сервер, де зберігаються біометричні еталони користувачів);

2) висока ймовірність неправильного розпізнавання обличчя, що збільшує кількість повторних спроб;

3) необхідність використання високопродуктивних пристроїв для запуску та обробки даних біометричного зчитування.

3. Порушення приватності:

1) можливість несанкціонованого доступу до персональних даних в обхід біометричного зчитування;

2) зберігання та передача біометричної інформації, яка може бути використана для зловмисних цілей.

4. Альтернативні методи безпеки:

1) користувачі можуть віддавати перевагу використанню паролю або пін-коду, оскільки вони більш надійні і менш схильні до помилок;

2) можливість використання інших біометричних методів, таких як сканування відбитка пальця або розпізнавання голосу.

Таким чином, до переваг можна віднести: зручність та швидкість використання, відсутність необхідності запам'ятовування складних паролів або пін-кодів, підвищена безпека авторизації. До недоліків можна віднести: технічні обмеження та помилки, недостатня швидкість та ефективність, порушення приватності, необхідність альтернативних методів безпеки.

2.3 Проблеми сумісності з різними пристроями

Біометрична авторизація, наприклад, в мобільному банкингу може мати справу з проблемами сумісності з різними пристроями. Ось деякі з таких проблем:

1. Відсутність необхідного обладнання – не всі пристрої підтримують біометричну авторизацію, тому деяким користувачам може знадобитися використання альтернативних методів автентифікації.

2. Несумісність із певними операційними системами – різні версії операційних систем можуть мати відмінності у підтримці біометричної автори-

зації, що може призвести до несправностей.

3. Проблеми з точністю розпізнавання – багато біометричних технологій не є ідеальними і можуть мати певні помилки або помилкові спрацьовування. Це може призвести до того, що користувачі не зможуть успішно пройти авторизацію або авторизація працюватиме недостатньо надійно.

4. Відсутність стандартизації – різні пристрої біометричної авторизації можуть використовувати різні алгоритми або протоколи, що може ускладнити інтеграцію з мобільним банком.

Для вирішення проблем сумісності з різними пристроями можна використовувати такі підходи:

1. Використання альтернативних методів аутентифікації – у разі відсутності можливості використання біометричної авторизації користувачеві слід надати можливість авторизуватися за допомогою пароля або пін-коду.

2. Оновлення програмного забезпечення – регулярні оновлення мобільного банку можуть містити виправлення та покращення, які можуть вирішити проблеми сумісності з різними пристроями.

3. Тестування на різних пристроях. Перед випуском нової версії мобільного банку необхідно провести тестування на різних пристроях та операційних системах, щоб переконатися в коректній роботі біометричної авторизації.

4. Співпраця з виробниками пристроїв – банк може співпрацювати з виробниками пристроїв, щоб покращити сумісність біометричної авторизації та забезпечити її надійність.

Вирішення проблем сумісності з різними пристроями в мобільному банку потребує уважного аналізу та постійного оновлення, щоб забезпечити максимальну зручність та безпеку для користувачів.

2.4 Низька надійність системи біометричної авторизації

Розглянемо основні проблеми, з якими користувачі можуть зіткнутися під час використання цієї функції у мобільному банку та можливі шляхи вирішення.

1. Недосконаліть біометричних даних. Некоректна робота системи біометричної авторизації може бути пов'язана з недосконалістю біометричних даних, наданих користувачем. Наприклад, відбиток пальця може бути пошкоджений або дещо змінився, що ускладнює його розпізнавання. Для вирішення цієї проблеми розробники мобільного додатка повинні поліпшити алгоритми розпізнавання та збільшити кількість біометричних даних, що зберігаються в системі, для більш точної ідентифікації.

2. Шахрайські методи обходу. Однією з основних проблем системи біометричної авторизації є можливість її обходу за допомогою шахрайських методів. Наприклад, зловмисники можуть використовувати фотографію обличчя або відбитком пальця для входу до облікового запису. Для захисту від таких атак необхідно використовувати додаткові механізми безпеки, такі як другий фактор авторизації (наприклад, пароль або пін-код), які шахраям буде складніше підробити або отримати.

3. Технічні неполадки. Виникнення технічних неполадок у роботі біометричної системи авторизації також може спричинити проблеми для користувачів мобільного банку. Наприклад, сенсор відбитка пальця може бути пошкоджений або некоригований, що призводить до невдалого розпізнавання. Для вирішення цієї проблеми необхідно періодично перевіряти та підтримувати працездатність технічних компонентів системи, а також проводити оновлення та виправлення програмного забезпечення.

Усунення зазначених проблем допоможе підвищити надійність системи біометричної авторизації в мобільному банку та забезпечити безпеку даних користувачів. Однак варто зазначити, що повна непроникність системи неможлива, і тому важливо регулярно стежити за можливими оновленнями та новими методами забезпечення безпеки.

2.5 Можливість підробки біометричних даних

1. Підміна фізичних характеристик. Одним із способів підробки біометричних даних є заміна фізичних характеристик користувачів. Наприклад, відбиток пальця може бути отриманий з поверхонь, на яких користувач залишає свої сліди. Компрометація відбитка пальця може статися, коли зловмисник зміг отримати доступ до відбитка та скопіювати його. Таким чином, порушник може підробити відбиток пальця та використовувати його для несанкціонованого доступу.

2. Злам системи розпізнавання. Інший спосіб підробки біометричних даних – зламування системи розпізнавання. Зловмисники можуть використовувати різні методи, щоб обійти систему розпізнавання та отримати несанкціонований доступ до програми. Наприклад, використання простих методів, таких як фотографія обличчя, може обдурити систему розпізнавання обличчя та дозволити зловмиснику отримати доступ.

3. Використання скомпрометованого пристрою. Ще одним способом підробки біометричних даних є використання компрометованого пристрою. Якщо зловмисник отримує доступ до пристрою користувача, він може змінити або замінити біометричні дані, збережені на пристрої. Це дозволить зловмиснику отримати доступ до програми, використовуючи підроблені біометричні дані.

Для боротьби з можливістю підробки біометричних даних у мобільних програмах можуть бути застосовані наступні заходи безпеки:

1. Двофакторна аутентифікація. Додатковий шар захисту, який вимагає введення додаткового пароля або використання іншого методу аутентифікації, допоможе запобігти несанкціонованому доступу.

2. Багатофакторна аутентифікація. Використання декількох методів аутентифікації, таких як відбиток пальця та розпізнавання обличчя разом, підвищує безпеку та ускладнює процес підробки.

3. Регулярне оновлення. Постійне оновлення системи розпізнавання та біометричних даних користувача допоможе запобігти підробці даних та захи-

стити програму від злому.

4. Шифрування даних. Зберігання та передача біометричних даних повинні бути захищені за допомогою надійних алгоритмів шифрування, щоб запобігти їх несанкціонованому доступу.

Звичайно, жоден метод аутентифікації не є ідеальним і завжди існує певний рівень ризику. Однак, комбінування різних заходів безпеки може значно зменшити можливість підробки біометричних даних і забезпечити високий рівень безпеки для користувачів мобільних пристроїв.

2.6 Недостатнє навчання користувача

На жаль, багато користувачів, наприклад, мобільних банків не знають про правила та заходи, які необхідно виконати для успішної біометричної авторизації. Це може призвести до проблем з використанням цієї функції та викликати незадоволеність клієнтів.

Для вирішення проблеми з недостатнім навчанням користувачів слід зробити наступні кроки:

1. Надати детальні інструкції щодо використання функції біометричної авторизації. Інструкції мають бути зрозумілими та доступними для всіх користувачів.

2. Навчити користувачів на прикладах, як правильно налаштовувати та використовувати функцію біометричної авторизації. Це допоможе їм розбиратися з можливими проблемами та впевнено використати цю функцію.

3. Провести навчальні вебінари або семінари для користувачів, на яких розглядатимуться всі особливості роботи з біометричною авторизацією. Це дозволить користувачам поставити запитання та розібратися у проблемах, з якими вони стикаються.

Таким чином, надання достатнього навчання користувачам функції біометричної авторизації допоможе вирішити проблеми, пов'язані з недостатнім знанням клієнтами особливостей використання цієї функції.

2.7 Способи покращення результатів біометричної авторизації

1. Оновлення алгоритмів розпізнавання. Для підвищення точності та безпеки біометричної авторизації необхідно постійно оновлювати алгоритми розпізнавання відбитків пальців, обличчя чи інших біометричних даних. Важливо проводити дослідження та аналізувати нові технологічні розробки у цій галузі.

2. Багатофакторна автентифікація. Одним із способів підвищення безпеки біометричної авторизації є введення багатофакторної автентифікації. Наприклад, крім сканування відбитків пальців можна вимагати введення додаткового PIN-коду або використання голосового розпізнавання.

3. Посилений захист біометричних даних. Дуже важливо забезпечити високий рівень захисту біометричних даних користувача. Для цього необхідно використовувати сучасні алгоритми шифрування та зберігати дані в окремо захищених сховищах. Також слід передбачити можливість видалення видалення біометричних даних користувача у разі витоку інформації.

4. Навчання та підвищення обізнаності користувачів. Не завжди проблеми з біометричною авторизацією пов'язані з технічними вадами. Часто проблема полягає у неправильному використанні або нерозумінні користувачем процедури авторизації. Тому важливо проводити навчання користувачів та підвищувати їх обізнаність про можливі помилки та способи вирішення проблем.

5. Регулярне оновлення ПЗ. Безперервне оновлення програмного забезпечення мобільного банку є одним із головних способів запобігання проблемам з біометричною авторизацією. Оновлення повинні включати виправлення помилок, додавання нових функцій та оновлення алгоритмів безпеки.

2.8 Поведінкова модель введення тексту в задачі аутентифікації користувачів мобільних пристроїв

Фізіологічні характеристики (відбиток пальця чи геометрія обличчя) можуть бути підроблені. Поведінкові характеристики позбавлені цього недоліку. До таких характеристик належить динаміка введення тексту. Вона включає інформацію про швидкість набору тексту і силу натискання на клавіші (на фізичній клавіатурі або сенсорному екрані). Крім загальних переваг біометричних характеристик даний підхід має наступні переваги при реалізації на мобільних пристроях.

1. Не вимагає спеціального обладнання (сканерів), тому може бути реалізований програмно та встановлений на будь-який мобільний пристрій із сенсорним екраном та встановленим програмним забезпеченням (операційною системою), у тому числі й на пристрої, які вже знаходяться у використанні. Отже, має низькі витрати на використання.

2. Не впливає на роботу користувача з мобільним пристроєм.

3. Невідтворюваність. За допомогою програмного забезпечення можна виміряти час натискання клавіш із точністю до мікросекунд. Така точність унеможливлює штучне відтворення динаміки введення одного користувача іншим.

4. Може виконувати роль додаткового рівня захисту під час використання паролів [7, 8]. Це дозволить поєднати простоту схеми використання пароля з підвищеною надійністю біометрії. Властивість невідтворюваності динаміки введення зробить підбір чи викрадення паролю несуттєвим, оскільки є лише частиною аутентифікаційного шаблону.

5. Може забезпечувати фонову автентифікацію протягом всієї взаємодії користувача з пристроєм [9]. На особливу увагу заслуговує останній пункт. Усі існуючі системи аутентифікації базуються на автентичності тільки при вході в систему. Основна проблема таких систем полягає в тому, що вони не можуть аутентифікувати користувачів після надання доступу, що створює потенційну вразливість безпеки. Ця проблема особливо гостро постає для

мобільних пристроїв, отримати доступ до яких після здійснення входу в систему справжнім користувачем значно простіше, ніж до стаціонарних комп'ютерів. Динаміка натискань клавіш, отримана з тексту, що вільно набирається, може забезпечити безперервну автентифікацію користувача протягом усього періоду роботи з пристроєм. Проте продуктивність такого підходу значно нижча порівняно з методом, що базується на введенні фіксованого тексту.

Дослідження даних про натискання клавіш не є новою темою [10-14]. Роботи в цій галузі вже велися або для того, щоб виявити типову поведінку користувача під час роботи з системою, або для порівняння різних шаблонів поведінки. З іншого боку, вимірювання даних натискання кнопок на мобільних пристроях є відносно новою темою дослідження [15, 16].

Дослідження динаміки натискання клавіш спирається на такі характеристики: час натискання клавіші A ($PressTime_A$) в мікроссекундах, час відпускання клавіші A ($ReleaseTime_A$) в мікроссекундах, сила натискання на клавішу A ($Pressure_A$).

Виконуючи прості математичні операції над часовими мітками, можна отримати такі можливі ознаки, які є основними характеристиками, що використовуються при аналізі динаміки натискання клавіш як на фізичних [17], так і на віртуальних клавіатурах [18]:

1. Тривалість натискань користувачем клавіші «A» – $H.KeyA$.

2. Тривалість паузи між двома послідовними натисканнями клавіш «A» та «B» – $UD.KeyA.KeyB$.

3. $DD.KeyA.KeyB$ – проміжок часу між натисканням клавіші «A» і натисненням клавіші «B»;

2) $HH.KeyA.KeyB$ – проміжок часу між натисканням клавіші «A» і відпусканням клавіші «B»;

3) $UD.KeyA.KeyB$ – проміжок часу між відпусканням клавіші «A» і натисненням клавіші «B»;

4) $UU.KeyA.KeyB$ – проміжок часу між відпусканням клавіші «A» і відпусканням клавіші «B».

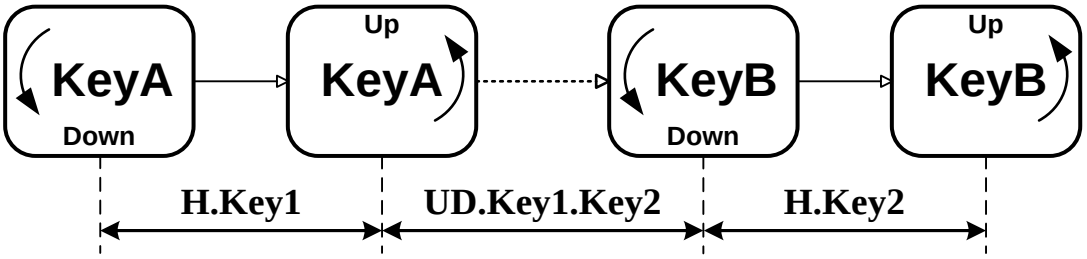


Рисунок 2.1 – Обчислення інформативних ознак
поодиноких подій клавіатури

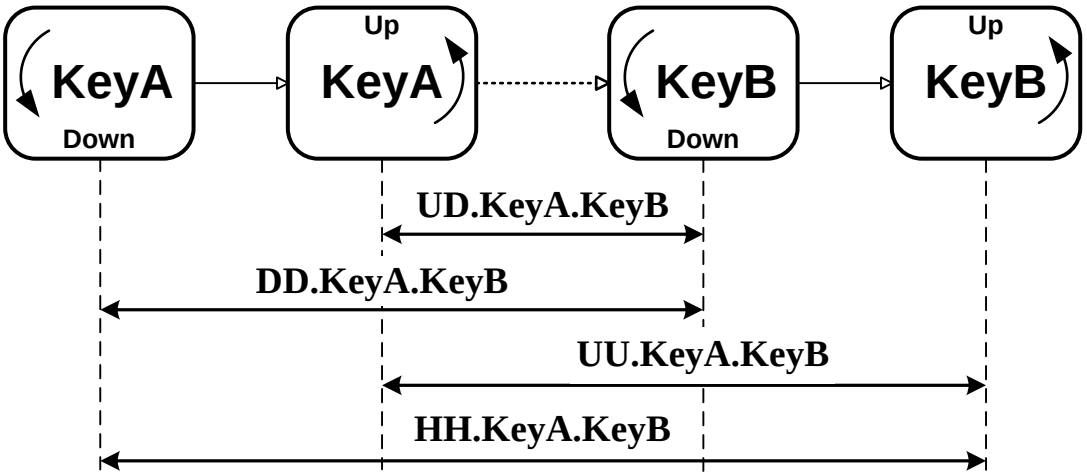


Рисунок 2.2 – Обчислення інформативних ознак диграфів клавіатури

Відмінною особливістю побудови поведінкової моделі користувача за фіксованим текстом є те, що текст (контрольне слово), що вводиться користувачем, відомий заздалегідь, що дозволяє використовувати особливості введення конкретної фрази, а не символів окремо: вимірюються ознаки, пов'язані з натисканням першої клавіші, другої та третьої і т.д. У досліджених роботах основним підходом є використання ознак $H.KeyA$ та $UD.KeyA.KeyB$. Окремим напрямом досліджень є підбір контрольного слова з оптимальним складом символів, що дозволяє найкраще диференціювати користувачів.

Для тексту, що вільно набирається, використовуваного у разі фонової аутентифікації, немає інформації ні про склад вводимих символів, ні про їх частоту. Отже, слід аналізувати введення кожного конкретного символу. Основним підходом тут є використання особливостей натискань окремих кла-

віш та пар (диграфів). Однак за такого підходу виникає проблема розмірності вектора ознак: якщо розглядати лише літери латинського алфавіту (26) та цифри (10), то розмірність вектора ознак вже біля 1400.

У ряді розглянутих робіт як альтернатива для відбору найбільш часто використовуваних диграфів застосовується розбиття всіх клавіш або диграфів на групи та обчислення зазначених вище ознак для груп в цілому, що дозволяє краще зберегти індивідуальні характеристики друку користувача. Одне з найпростіших розбиття клавіш фізичної клавіатури за розташуванням полягає у виділенні трьох областей, що не перетинаються: клавіш, набраних лівою рукою (L), клавіш, набраних правою рукою (R), і пробілу (S). Далі всі диграфи поділяються на одну з наступних восьми груп: L-L, L-R, L-S, R-L, R-R, R-S, S-L і S-R; та обчислюється середній час для кожної групи, яка використовується як одне значення ознаки.

Основними недоліками описаного вище способу отримання ознак є їх незбалансований розподіл і незалежність від користувача. По-перше, кількість натискань клавіш не розподілено рівномірно за вісьмома ознаками, що призводить до значної втрати інформації для ознаки з багатьма натисканнями клавіш і переоцінки ознаки з кількома натисканнями клавіш. По-друге, групи мають однаковий склад диграфів, що не дозволяє алгоритму автентифікації достатньо розуміти унікальну поведінку кожного користувача при введенні тексту.

Розвитком цього стало розбиття диграфів за середньої швидкості набору. Усі диграфи впорядковуються за вказаним параметром, після чого весь набір диграфів ділиться на k груп. Середній час натискання клавіші для кожної групи об'єктів використовується як окреме значення для відповідної ознаки. Основною перевагою даного підходу є те, що ознаки адаптуються до користувача. Ознаки, відокремлені для дійсного користувача, ґрунтуються на його власному розподілі швидкостей наборів диграфів та будуть добре відповідати його моделі. З іншого боку, оскільки інші користувачі мають різні стилі введення в порівнянні з дійсним, їхня відносна швидкість набору серед

ознак не буде зберігатися належним чином. Таким чином, кожен користувач матиме власну модель аутентифікації, яка залежить від його стилю друку.

Однією з основних проблем при побудові моделі користувача, здатної виявляти вторгнення, є приклади натискання клавіш зловмисником у навчальній вибірці, що призводить до необхідності використання однокласових моделей [19]. Найбільш часто використовуваними алгоритмами класифікації в роботах, присвячених дослідженню динаміки натискань клавіш, є метричні (однокласовий KNN) та ймовірнісні (однокласовий SVM, змішані гауссівські моделі, байєсовські мережі) методи. Найкращі результати досягаються під час використання однокласових класифікаторів KNN та SVM.

2.9 Розпізнавання користувачів мобільних пристроїв за динамічним графічним паролем

Графічний пароль – метод аутентифікації, коли для доступу в систему користувачеві необхідно виконати деякі операції над зображеннями, наприклад, вибрати один або кілька заздалегідь визначених об'єктів. Графічна інформація дає великі можливості для унікальності вибору пароля. Таким чином, графічні схеми паролів дають можливість зробити паролі більш зрозумілими людині при одночасному підвищенні рівня безпеки.

Найбільший недолік «звичайних» статичних графічних паролів – проблема підглядання через плече. Хоча графічні паролі важко вгадати, зловмисник, що вів спостереження кілька сеансів входу в систему, може в залежності від схеми, в кінці кінців, зрозуміти пароль. Однак цього недоліку можна уникнути, використовуючи динамічні графічні паролі.

Суть методу динамічних графічних паролів полягає в тому, що користувачеві відомий певний алгоритм і, знаючи його та свої парольні зображення, він може визначити пароль для поточної сесії. Плюси очевидні: запам'ятати алгоритм і самі зображення користувачу легше, ніж запам'ятати складний буквено-цифровий пароль, який до того ж доводиться періодично міня-

ти. При цьому навіть якщо процес аутентифікації зможуть спостерігати сторонні люди, це не знизить безпеку процесу. Кожен раз користувач буде вибирати різні зображення (вводити різні дані), що не дозволить зловмиснику побачити самі парольні зображення.

Плюсом також є те, що варіантів аутентифікації можна запропонувати безліч. Їх кількість обмежена лише фантазією розробника і складністю реалізації. Для кращого розуміння розглянемо приклади динамічної графічної аутентифікації.

Приклад 1 – «Прямі, що перетинаються». Для даного способу будуть використовуватися дві картинки. На екрані для введення пароля в довільному порядку розкидані зображення. Правильний пароль – ті з них, що знаходяться на перетині прямих, що виходять з парольних зображень. Якщо правильні зображення знаходяться на одній прямій, то пароль – самі ці зображення. Для зменшення ймовірності випадкового підбору пароля його введення необхідно зробити 3 рази. Авторизація вважається успішною, якщо користувач не допустив жодної помилки.

Спочатку зловмисник навіть не знає, скільки пральних зображеній необхідно ввести для авторизації. Звичайно, якщо він зможе тривалий час спостерігати за екраном мобільного пристрою користувача, є ймовірність вгадати такий досить-таки простий алгоритм.

Ймовірність пройти аутентифікацію, вгадавши пароль, дорівнює

$$p = \left(\frac{1}{n} \cdot \frac{1}{n-1}\right)^k, \tag{2.1}$$

де n – кількість парольних зображень, k – кількість раз, яке необхідно ввести пароль.

Приклад 2 – «Кількість клітинок». На екрані для введення пароля в довільному порядку розкидані картинки. Суть методу полягає в тому, що користувач повинен подумки порахувати найкоротший шлях між трьома парольними зображеннями і ввести отримане число в форму. Вважати «клітинки» необхідно за годинниковою стрілкою (вгору – вправо – вниз – вліво).

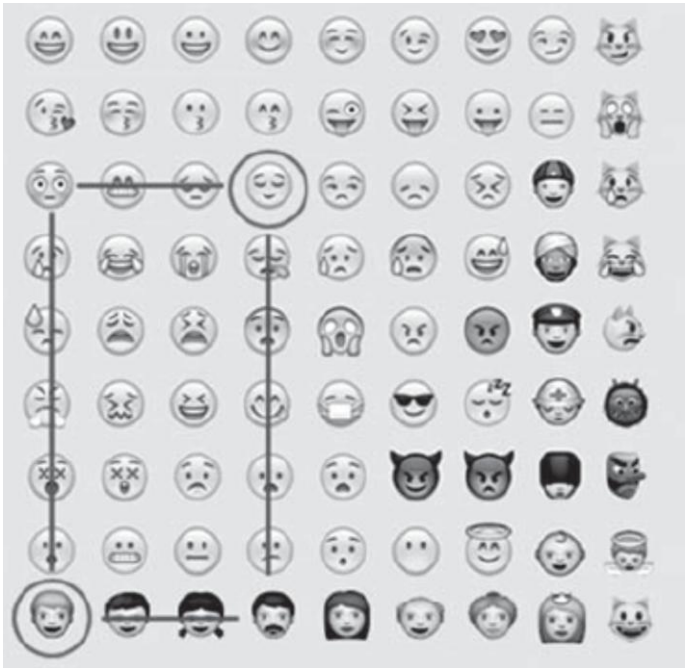


Рисунок 2.3 – Приклад реалізації алгоритму «прямі, що перетинаються»

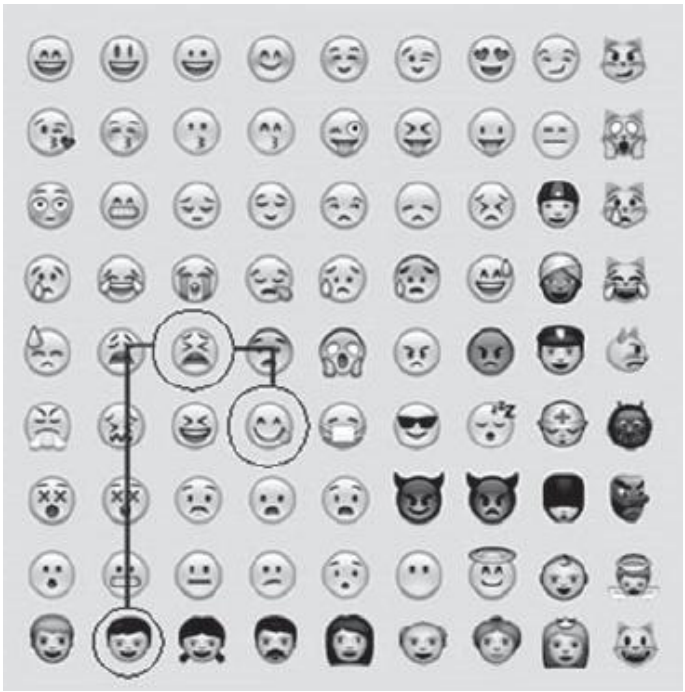


Рисунок 2.4 – Приклад реалізації алгоритму «кількість клітинок»

Для зменшення ймовірності випадкового підбору пароля його введення необхідно зробити 3 рази. Авторизація вважається успішною, якщо користувач не допустив жодної помилки.

Плюси цього методу полягають в тому, що користувачеві не потрібно

натискати на зображення, а отриманий результат завжди різний, так як картинки розташовуються в довільному порядку.

Ймовірність вгадати пароль для алгоритму «кількість клітинок» вище, ніж в першому способі, але і отримати дані про метод аутентифікації, спостерігаючи за користувачем, зловмисник не може.

Приклад 3 – «Модуль координат». Даний спосіб буде складний для користувачів, і навряд чи його раціонально використовувати в реальній системі. Є безліч зображень, з яких три парольні. Користувач повинен подумки накласти на картинку осі координат і склавши по модулю n (n – розмірність системи) координати парольних зображень обчислити поточний пароль. Колами виділені парольні зображення користувача. Їх координати відповідно: $(0;\ 2), (7;\ 5)$ і $(8;\ 5)$. Тоді координати зображення для аутентифікації: $X = (0 + 7 + 8) mod 9 = 6, Y = (2 + 5 + 5) mod 9 = 3.$

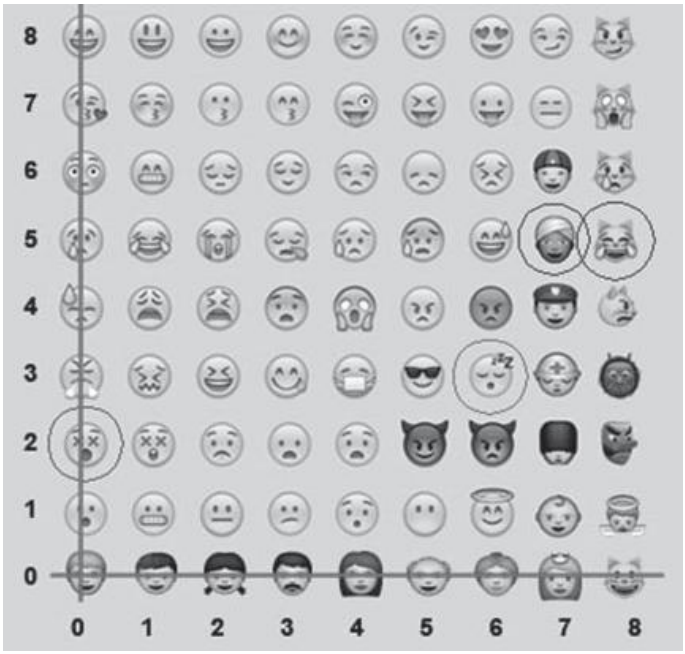


Рисунок 2.5 – Приклад реалізації алгоритму «модуль координат»

Ймовірність вгадати пароль $p = 1/n^2$ і для прикладу на рис. 2.5 дорівнює $p = \frac{1}{9^2} \approx 1.2\ \%$. У разі трикратного вводу пароля значення ймовірності становить $1.9 \cdot 10^{-4}\ \%$. Отже, вгадати такий пароль практично неможливо.

2.10 Розпізнавання користувачів мобільних пристроїв за цифровим рукописним паролем

Сучасні технології автоматизованої верифікації особистості за рукописним підписом за способами одержання зразків поділяються на дві групи: офлайнові та онлайнові. Офлайнові технології використовують для аналізу статичні («мертві») рукописи, які вже є у документах. Онлайнові технології використовують для аналізу динамічні («живі») рукописи, які аналізуються безпосередньо під час їх відтворення за допомогою спеціальних апаратно-програмних засобів. Ці дві групи технологій мають суттєві відмінності.

У першій групі технологій фактично вирішується задача порівняння зображень підпису. Застосовуються офлайнові системи у випадках, коли немає можливості контролювати процес відтворення підпису (криміналістика, виявлення авторства тощо).

У другій групі технологій підпис відтворюється на сенсорному екрані і система аналізу підпису має у своєму розпорядженні дані про параметри положення, утримання та коливання стилуса при відтворенні підпису. Обсяг інформації, що одержується при цьому, істотно перевищує той, який доступний при офлайновому аналізі. Тому автоматичні системи верифікації особистості за динамікою відтворення підпису за точністю є значно кращими за автоматичних офлайнових систем та людей-експертів.

Системи аналізу динаміки відтворення «живого» підпису в мінімальному варіанті контролюють положення кінчика стилуса в двовимірному просторі (площині екрану), тобто функції $x(t),\ y(t)$. Сучасні системи на додаток до двійки функцій $x(t),\ y(t)$ використовують ряд додаткових сенсорів, що контролюють тиск пера, просторове положення стилуса, особливості його утримання кистю руки. Найчастіше додатково контролюються тиск стилуса на планшет і кути нахилу стилуса до площини планшета. У таких пристроях фактично фіксуються напрямки п'ятивимірних векторів, взятих у еквідистантних точках часу.

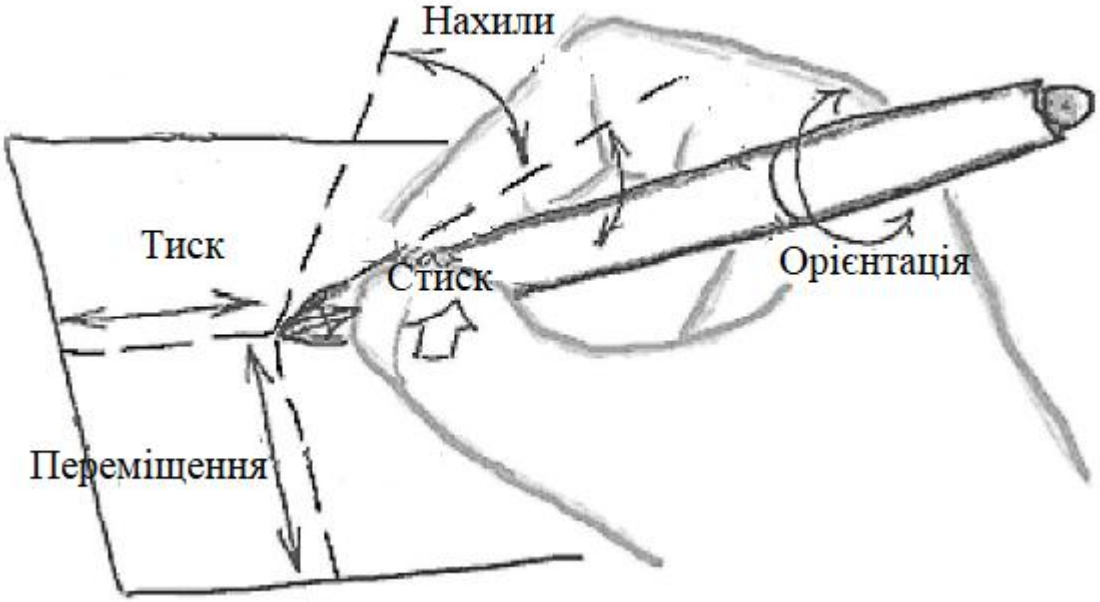


Рисунок 2.6 – Ступені свободи взаємного становища стилуса та планшета

Ймовірності помилок першого та другого роду для двовимірних систем – 10^{-2} , для тривимірних систем – 10^{-3} . Подальше збільшення мірності (числа сенсорів) призводить до нелінійно меншого приросту точності.

Додатковим засобом збільшення точності онлайнових рукописних систем є використання контролю рукописних секретних фраз (рукописного пароля). Рукописний пароль дозволяє знизити рівень помилки другого роду кілька десяткових порядків.

Найбільш поширеним способом отримання інформативних параметрів підпису є переведення часових функцій коливання стилуса в частотну область шляхом їх розкладання за ортогональним базисом Фур'є, Уолша, Хаара та ін. Коефіцієнти розкладання виконують роль інформативних параметрів підпису.

Розглянемо приклад розрахунку біометричних параметрів підпису в простій двокоординатній системі, що використовує лише дві функції коливання стилуса в площині екрану $x(t)$, $y(t)$. Функції змінюються на інтервалі часу T, який відповідає часу відтворення контрольного слова або факсиміле. В якості ортогонального базису використовуємо ряд Фур'є з кількістю членів розкладання n:

$$x(t) = a_{x0} + \sum_{j=1}^{n} a_{xj} cos\,(j\omega_0 t) + \sum_{j=1}^{n} b_{xj} sin\,(j\omega_0 t),$$

$$y(t) = a_{y0} + \sum_{j=1}^{n} a_{yj} cos\,(j\omega_0 t) + \sum_{j=1}^{n} b_{yj} sin\,(j\omega_0 t),$$

де $\omega_0 = \frac{2\pi}{T}$ основна кутова частота;

$a_{x0}, a_{y0}, a_{xj,} b_{xj}, a_{yj}, b_{yj}$- коефіцієнти розкладання.

Коефіцієнти розкладання, обчислюються за формулами

$$a_{x0} = \frac{1}{T}\int_0^T x(t)dt,$$

$$a_{y0} = \frac{1}{T}\int_0^T y(t)dt,$$

$$a_{xj} = \frac{1}{T}\int_0^T x(t)\cos(j\omega_0 t)\,dt,$$

$$b_{xj} = \frac{1}{T}\int_0^T x(t) sin\,(j\omega_0 t)dt,$$

$$a_{yj} = \frac{1}{T}\int_0^T y(t)\cos(j\omega_0 t)\,dt,$$

$$b_{yj} = \frac{1}{T}\int_0^T y(t)\sin\,(j\omega_0 t)dt.$$

Коефіцієнти розкладання $a_{x0}, a_{y0}, a_{xj,} b_{xj}, a_{yj}, b_{yj}$, обчислені для $j = \overline{1,n}$, членів розкладання, у сукупності зручно розглядати як N-мірний ($N = 4n$) вектор $V = (v_1, v_2, \dots, v_N)$, який виступає як машинна репрезентація рукописних параметрів.

У рукописних БСКД формування зразка користувача здійснюється на основі пред'явлення кількох зразків його підпису, які у загальному випадку можуть мати різний масштаб під час реєстрації та ідентифікації. Ця обстави-

на зумовлює необхідність приведення зразків підпису, що вводяться, до єдиного масштабу. Масштабування чергового введеного рукописного зразка $x_a(t), y_a(t)$ виконують відносно першого введеного зразка підпису $x_1(t), y_1(t)$:

$$x_a(t) = \mu_x \cdot x_1(t),$$
$$y_a(t) = \mu_y \cdot y_1(t),$$

де μ_x, μ_y – коефіцієнти масштабування функцій $x_a(t), y_a(t)$.

Завдяки властивості лінійності ортогональних функціоналів операцію масштабування можна реалізувати також на рівні коефіцієнтів $a_{x0}, a_{y0}, a_{xj}, b_{xj}, a_{yj}, b_{yj}$, розкладання функцій $x(t), y(t)$

$$\sqrt{\sum_{j=1}^{n}(a_{xaj}^2 + b_{xaj}^2)} = \mu_x \sqrt{\sum_{j=1}^{n}(a_{x1j}^2 + b_{x1j}^2)},$$

$$\sqrt{\sum_{j=1}^{n}(a_{yaj}^2 + b_{yaj}^2)} = \mu_x \sqrt{\sum_{j=1}^{n}(a_{y1j}^2 + b_{y1j}^2)}.$$

Практична реалізація БСКД за рукописом пов'язані з необхідністю спеціальної попередньої обробки вхідних даних, зумовленої особливостями цих даних. Для трикоординатної системи введення зразок «живого» підпису в математичному сенсі можна розглядати як систему трьох тимчасових функцій $\Psi_i = [x(t), y(t), z(t)]$, що змінюються в інтервалі $(0, T)$, та відповідає часу відтворення зразка. При цьому функції $x(t), y(t)$ відображають коливання стилуса в площині планшета, функція $z(t)$ – ступінь тиску стилуса на планшет. Після оцифрування система набуває вигляду

$$\Psi_i = \left[x(t_j), y(t_j), z(t_j)\right], \ j = \overline{1, n}, \qquad i = \overline{1, L}.$$

де n – кількість відліків у системі Ψ_i; L – кількість введених зразків.

У процесі реєстрації та контролю доступу користувач вводить кілька своїх рукописних зразків. При цьому їхній вид варіюється в досить широких межах. Одна частина варіацій (варіації першого роду) обумовлена властивими даному користувачеві природними статистичними відхиленнями в рукописному відтворенні тих самих символів і враховується в біометричному зра-

зку користувача. Інша частина варіацій (варіації другого роду) обумовлена цілісними геометричними характеристиками зразка вже після його відтворення (зрушення у площині планшета, зміни розмірностей по осях x, y, z, повороти у площині планшета). Особливістю варіацій другого роду є те, що вони не змінюють топологічних властивостей зразків як тривимірних геометричних фігур. Ці властивості залишаються постійними при деформаціях зразків, що виробляються без розривів та склеювань (при взаємно однозначних та безперервних відображеннях).

Сукупність всіх зазначених варіацій визначають помилку першого роду рукописної БСКД. Було розроблено комплекс методів попередньої обробки рукописних зразків, що дають змогу зменшити помилки першого роду за рахунок зниження впливу варіацій другого роду.

Прямий облік варіацій другого роду в еталоні користувача не доцільний, бо це значно збільшує діапазони можливих відхилень (дисперсій) по відповідних осях координат і, як наслідок, призводить до зростання помилок БСКД. Більш ефективний шлях полягає у застосуванні зворотних (компенсуючих) перетворень виявлених деформацій готових зразків на етапі їх попередньої обробки до застосування ортогональних розкладів. Для цього можна скористатися напрацьованим арсеналом методів геометричних перетворень тривимірних об'єктів.

Результатом відтворення у системі функцій $\Psi_i = \left[x(t_j), y(t_j), z(t_j)\right]$ деякого i-зразка є тривимірна фігура $\Psi_i = (x_j, y_{j,} z_j),\ j = \overline{1,n}$. Обмежимося розглядом тільки таких геометричних перетворень, які можуть бути охарактеризовані чисельними параметрами, що залежать від умов формування фігури $\Psi_i = (x_j, y_{j,} z_j)$. Суть таких геометричних перетворень у тому, що всі точки визначення фігури $\Psi_i = (x_j, y_{j,} z_j)$ зміщуються за певним законом Tr і переходять у інші точки простору:

$$\Psi_i^* = (x_j^{'}, y_j^{'}, z_j^{'}) = T_r\{\Psi_i((x_j, y_{j,} z_j)\}.$$

Характер варіацій рукописних зразків як геометричних фігур обмежу-

ється класом перетворень руху та подоби у тривимірному просторі, тому закон геометричних перетворень T_r може бути представлений у загальному вигляді

$$x_j^{'} = \rho_x\left(a_{11}x_j + a_{12}y_j + a_{13}z_j\right) + \xi_x,$$
$$y_j^{'} = \rho_y\left(a_{21}x_j + a_{22}y_j + a_{23}z_j\right) + \xi_y,$$
$$z_j^{'} = \rho_z\left(a_{31}x_j + a_{32}y_j + a_{33}z_j\right) + \xi_z.$$

де ρ_x, ρ_y, ρ_z – параметри подібності, що описують зміни масштабу фігури $\Psi_i((x_j, y_{j,} z_j)$ по осях *x*, *y*, *z*; *A* – матриця, яка задає параметри обертання фігури $\Psi_i((x_j, y_{j,} z_j)$ навколо осей координат

$$A = \begin{Vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{Vmatrix},$$

де ξ_x, ξ_y, ξ_z – параметри трансляції (паралельного перенесення початку системи координат)

У дигітайзері БСКД початкова точка відтворення рукописного зразка за допомогою програмних засобів автоматично позиціонується на початок координат, тому параметри трансляції ξ_x, ξ_y, ξ_z, можна виключити з розгляду. Обертання фігури $\Psi_i((x_j, y_{j,} z_j)$ у процесі її рукописного введення можливе лише навколо осі z. В результаті закон геометричних перетворень T_r спрощується і для правої декартової прямокутної системи координат набуває вигляду.

$$x_j^{'} = \rho_x\left(x_j \cos\alpha + y_j \sin\alpha\right),$$
$$y_j^{'} = \rho_e\left(-x_j \sin\alpha + y_j \cos\alpha\right),$$
$$z_j^{'} = \rho_z z_j.$$

У такому разі попереднє перетворення рукописних зразків з метою компенсації їх можливих деформацій зводиться до отримання коефіцієнтів ρ_x, ρ_y, ρ_z – масштабування за координатними осями та кута α – повороту зразка навколо осі z.

Перевагами таких методів попередньої обробки біометричних даних

для рукописних БСКД є їхня комплексність та універсальність. Комплексність полягає у можливості застосування єдиної методики до всієї попередньої обробки біометричних даних. Універсальність проявляється як незалежність методів попередньої обробки біометричних даних від методів отримання біометричних характеристик користувачів та їх класифікації.

Для зниження рівня помилок аутентифікації в рукописних БСКД (як і голосових) можливе застосування засекречених рукописних зразків (рукописного пароля). Рівень захисту (помилка другого роду) у цьому випадку визначатиметься двома факторами:

- здатністю системи відрізнити «свого» та «чужого» виключно за особливостями підпису;
- «секретністю» зразка підпису, що вводиться.

При спробі несанкціонованого доступу зловмиснику необхідно поєднати дві трудомісткі процедури: наслідування особливостей рукописного введення легальним користувачем та добору пароля. При довжині парольної фрази 10 символів загальний рівень захисту комп'ютерної системи стосовно використання несекретної фрази підвищується до 6 десяткових порядків.

3 ДОСЛІДЖЕННЯ ІДЕНТИФІКАЦІЙНОГО ПОТЕНЦІАЛУ ЦИФРОВОГО РУКОПИСНОГО ПІДПИСУ ВЛАСНИКІВ МОБІЛЬНИХ ПРИСТРОЇВ

3.1 The MOBISIG signature database

База даних «The MOBISIG signature database» [20-22] була опублікована у 2016 р. Датасет містить параметри вводу унікальних 83 парольних фраз. З міркувань безпеки (люди неохоче оприлюднюють свої власні підписи), учасникам експерименту було запропоновано створити підпис за даним ім'ям, перелік яких належить першим 100 найпоширенішим угорським іменам. Учасникам також було запропоновано попрактикуватися у створенні підписів шляхом вводу та видалення кількох спроб. Перші п'ять спроб видалено. База містить підписи 83 користувачів: 49 чоловіків і 34 жінки з наступним віковим розподілом: 65 користувачів віком до 25 років, 11 користувачів віком від 25 до 40 років та 7 користувачів старше 40 років.

Збір даних проводився за допомогою планшета Nexus 9 з ємнісним сенсорним екраном. Частота опитування екрану – 60 Гц. Кожна сигнатура зберігалася як послідовність дискретних значень $[x_t, y_t, t, p_t, f_{a_t}, vx_t, vy_t, ax_t, ay_t, az_t]$, де $[x_t, y_t]$ – значення координат в процесі вводу парольної фрази, t – значення часу в процесі вводу парольної фрази, $[p_t, f_{a_t}]$ – тиск і площа пальця (нормалізовані значення в інтервалі $[0,1]$) в процесі вводу парольної фрази, $[vx_t, vy_t]$ – швидкості переміщення кінчика пальця за координатами x та y відповідно в процесі вводу парольної фрази, $[ax_t, ay_t, az_t]$ – прискорення планшету в тривимірному просторі, що характеризують положення планшету в руці користувача в процесі вводу парольної фрази.

В процесі формування датасету екран планшету було розділено на дві частини (рис. 3.1): верхня частина – секція відтворення, де користувачам демонструвався анімований підпис, а нижня частина була призначена для вводу підпису. Функції анімації були доступні в обох процесах збору підписів:

справжніх і атаках-підробках. Анімація дозволяє учасникам пригадати / побачити форму та динаміку справжніх і підроблюваних підписів. Анімацію можна відтворювати будь-яку кількість раз.

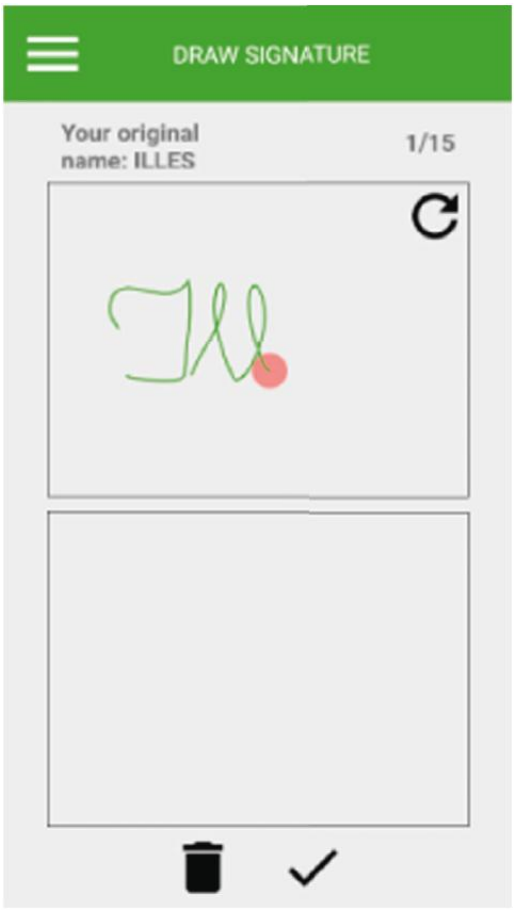


Рисунок 3.1 – Екран програми вводу цифрового рукописного підпису

Процес збору даних було розділено на три сесії з тижневою перервою між сесіями. Впродовж першої сесії кожен користувач повинен був надати 15 справжніх підписів. Впродовж другої та третьої сесії учасники повинні були надати 15 справжніх підписів і 10 підробок для двох інших користувачів (двічі по 5 підробок).

Наприкінці процесу збору даних для кожного користувача було отримано 45 справжніх підписів і 20 підробок.

Деякі з цих підписів наведено на рис. 3.2 – рис. 3.9.

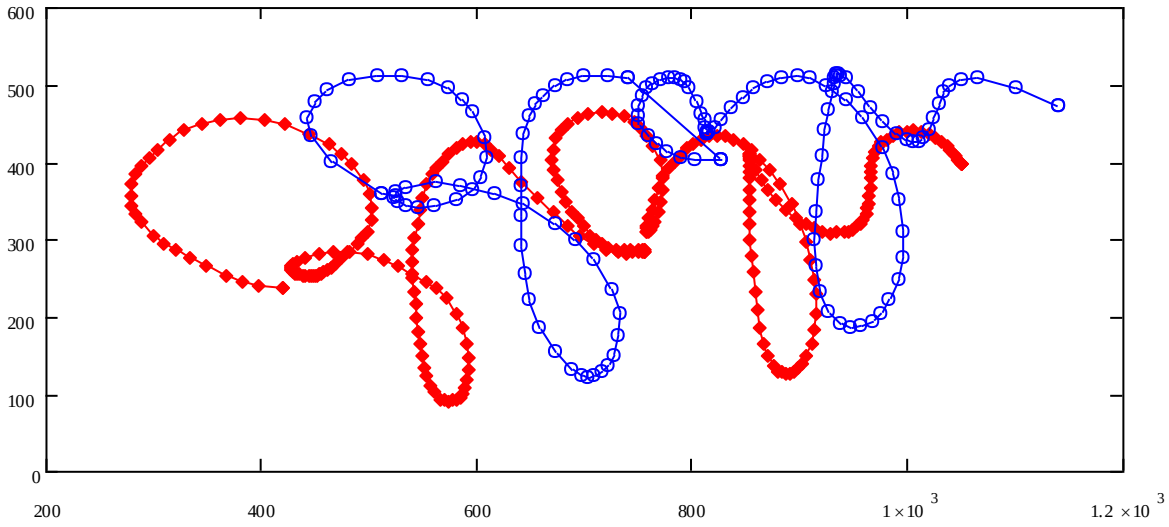


Рисунок 3.2 – Дві спроби вводу парольної фрази «OLAH» користувачем 17

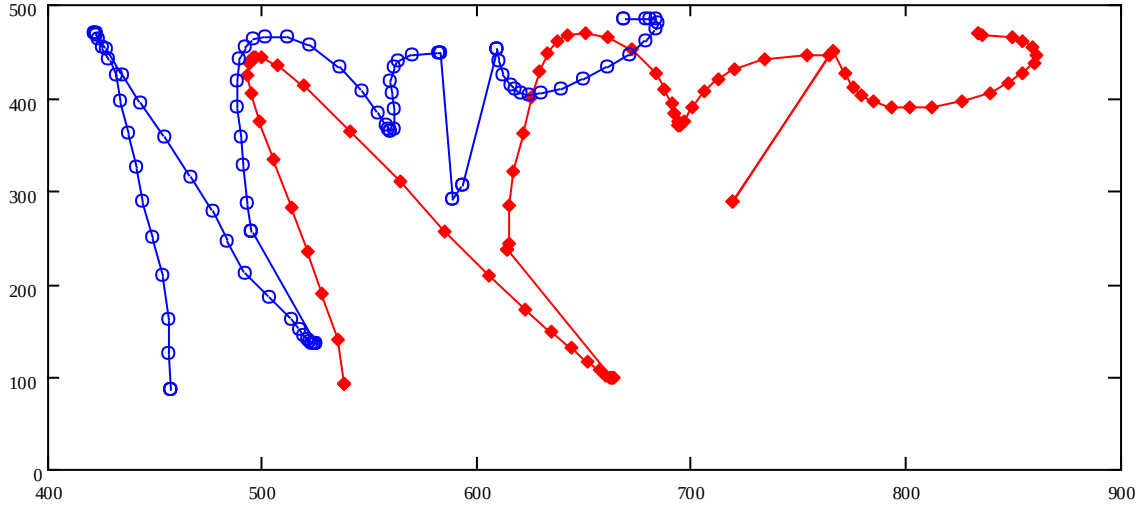


Рисунок 3.3 – Дві спроби вводу парольної фрази «KIS» користувачем 26

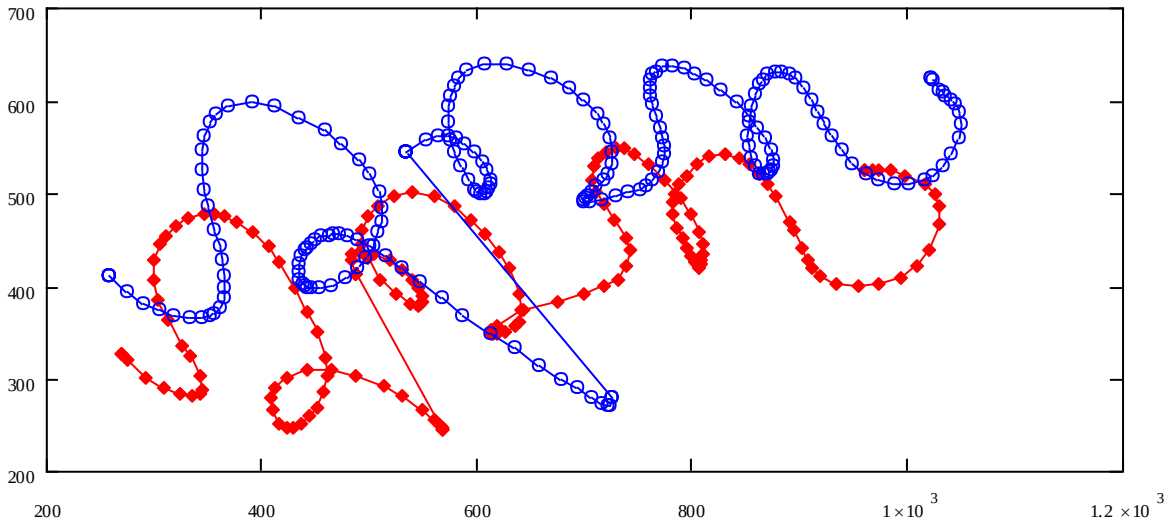


Рисунок 3.4 – Дві спроби вводу парольної фрази «VERES» користувачем 54

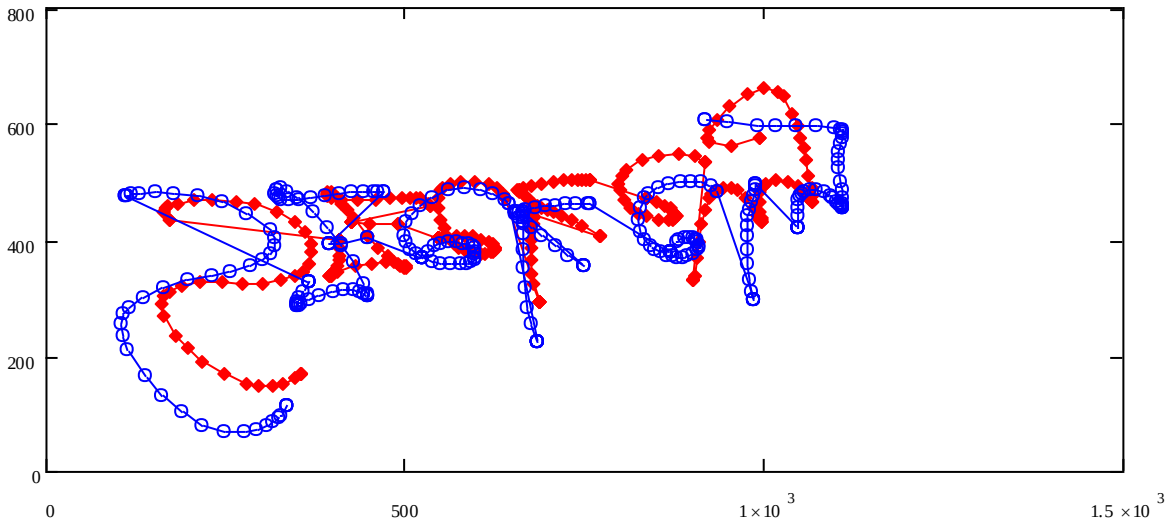


Рисунок 3.5 – Дві спроби вводу парольної фрази «SZEKLY» користувачем 75

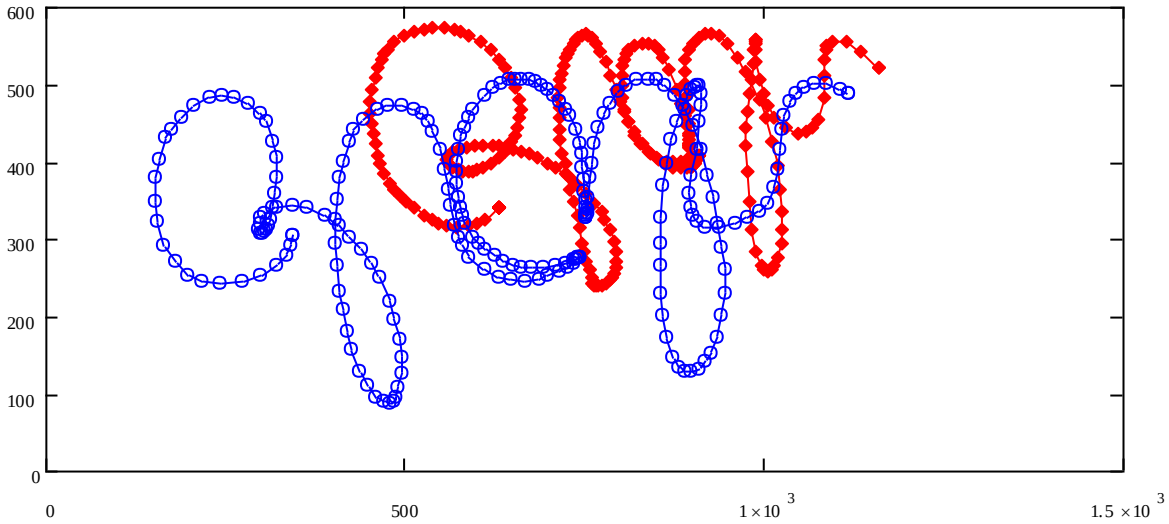


Рисунок 3.6 – Спроби підробки вводу парольної фрази «OLAH» користувачами 18 та 21

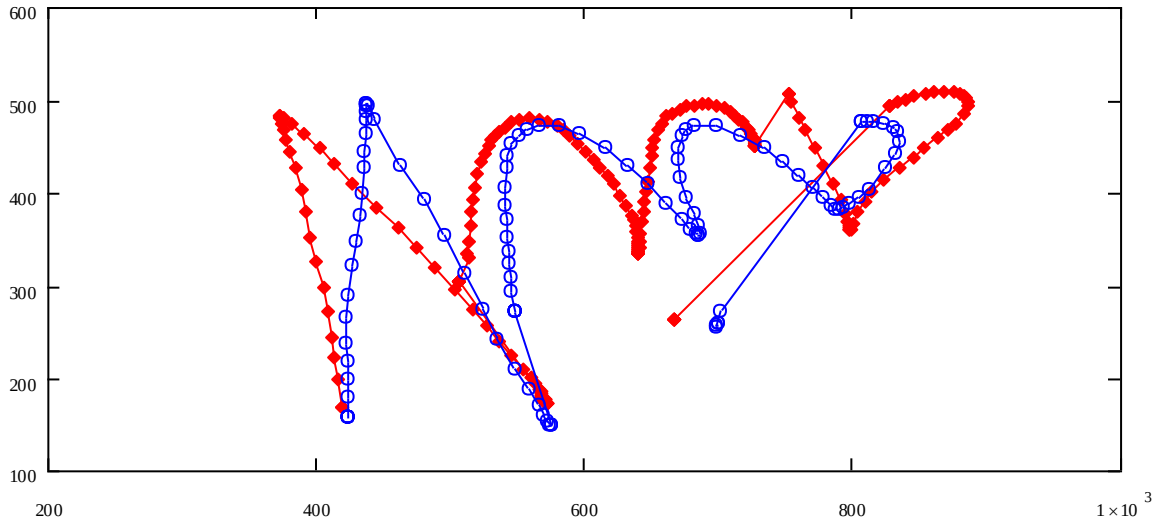


Рисунок 3.7 – Спроби підробки вводу парольної фрази «KIS» користувачами 30 та 28

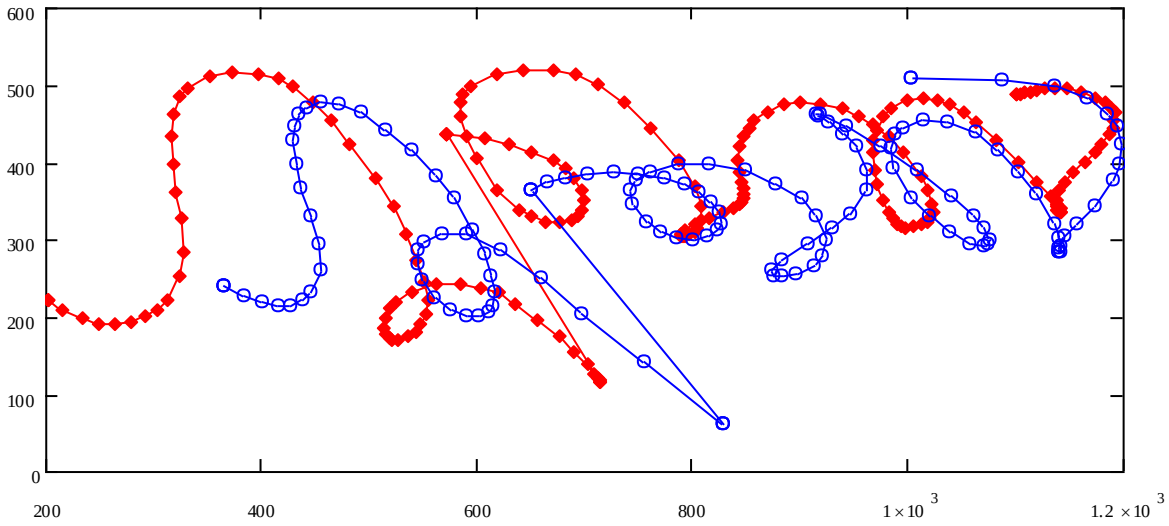


Рисунок 3.8 – Спроби підробки вводу парольної фрази «VERES» користувачами 56 та 58

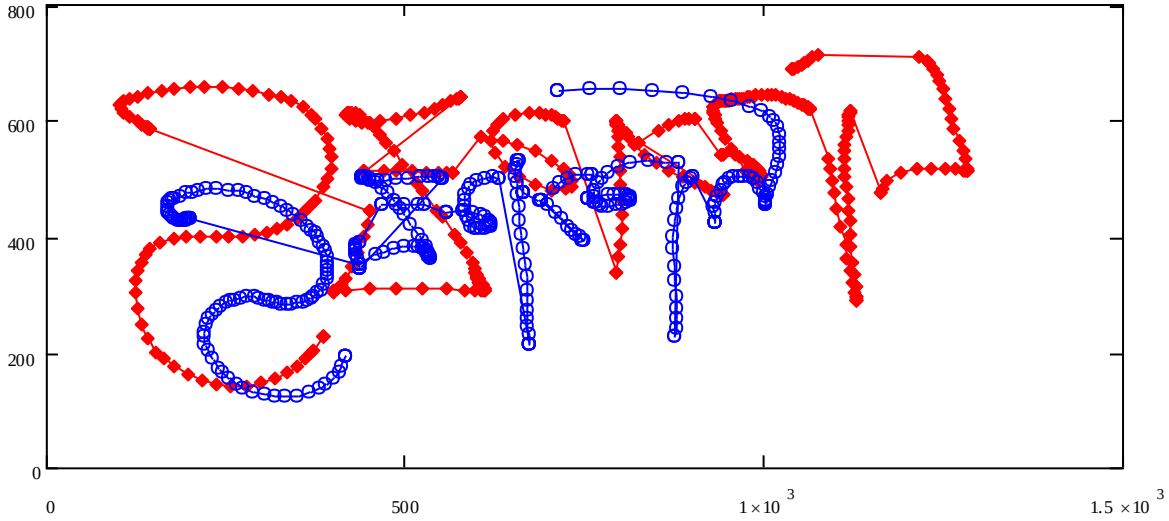


Рисунок 3.9 – Спроби підробки вводу парольної фрази «VERES» користувачами 76 та 77

3.2. Схема експерименту та результати проведених досліджень

Експериментальні дослідження проводились в пакеті Orange Data Mining. Оскільки задача ідентифікації математично є задачею класифікації, тобто задачею розбиття множини об'єктів (тестові вектори біометричних ознак) на апріорно задані класи (імена користувачів), всередині кожного з яких вони вважаються схожими один на одного, та мають приблизно однакові властивості й ознаки (вектори біометричних характеристик одного користувача дуже схожі один на одного), то в якості алгоритмів класифікації користувачів використовувався метод випадкових лісів (Random Forests).

Точність класифікації перевірялась за алгоритмом 10-fold cross-validation, у відповідності до якого дослідний набір даних розбивається на 10 однакових за розміром блоків. З 10 блоків один залишається для тестування моделі, а інші 9 блоків використовуються як тренувальний набір. Процес повторюється 10 разів, і кожен з блоків використовується один раз як тестовий набір. Наприкінці аналізу отримують 10 результатів, по одному на кожен блок, вони усереднюються і дають одну оцінку. Перевага такого способу в тому, що всі спостереження використовуються і для тренування, і для тесту-

вання моделі, і кожне спостереження використовується для тестування в точності один раз.

Кількісні параметри достовірності отриманої математичної моделі ідентифікації (класифікації) у Orange представлені наступними.

1. AUC (area under ROC) – площа, обмежена ROC-кривою (графік, що відображає співвідношення між часткою об'єктів від загальної кількості носіїв ознаки, вірно класифікованих до загальної кількості об'єктів, що не несуть ознаки, помилково класифікованих, як такі, що мають ознаку) і віссю частки помилкових позитивних класифікацій. Чим вище показник AUC, тим якісніше діє класифікатор, при цьому значення 0.5 демонструє непридатність обраного методу класифікації (відповідає звичайному вгадуванню).

2. Classification accuracy (CA) – точність класифікації, розраховується за виразом:

$$CA = \frac{TP + TN}{TP + TN + FP + FN}. \quad (3.1)$$

В (3.1) TP (True Positive) – зареєстрований суб’єкт X ідентифікований вірно і дозволено доступ; TN (True Negative) – зловмисника суб’єкта Y правильно не ідентифіковано і в доступі відмовлено; FP (False Positive) – зловмисника суб’єкта Y ідентифіковано як зареєстрованого суб’єкта X та дозволено отримати доступ; FN (False Negative) – зареєстрованого суб’єкта X ідентифіковано як зловмисника суб’єкта Y і в доступі відмовлено.

Classification accuracy – ефективна метрика якості, коли дослідник має справу із збалансованими класами. Однак, якщо кількість об’єктів одного класу значно перевищує інший, то точність покаже хороші результати, що насправді будуть неправдивими.

3. $Precision$ – точність, вказує на те, яка частка користувачів, ідентифікованих як зареєстровані, насправді є зареєстрованими. Розраховується за виразом:

$$Precision = \frac{TP}{TP + FP}. \quad (3.2)$$

4. $Recall$ – повнота, вказує на те, який відсоток дійсно зареєстрованих

користувачів система вірно ідентифікувала. Розраховується за виразом:

$$Recall = \frac{TP}{TP + FN}. \quad (3.3)$$

5. $F1$-міра. Не дуже зручно весь час звертатися до $Precision$ та $Recall$ тому кращим варіантом є використання міри, що б одночасно враховувала б обидві метрики. $F1$-міра розраховується за виразом:

$$F1 = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall}. \quad (3.4)$$

6. $Specificity$ – специфічність, визначається як відношення кількості істинно негативних класифікацій (true negative) до загальної кількості негативних класифікацій, тобто суми істинно-негативних та хибно-позитивних класифікацій:

$$Specificit = \frac{TN}{TN + FP}. \quad (3.5)$$

Оскільки традиційними показниками якості системи ідентифікації є FRR (False Reject Rate) – помилка першого роду, тобто ймовірність помилкової відмови авторизованому користувачеві (помилкова відмова «своєму») та FAR (False Accept Rate) – помилка другого роду, тобто ймовірність пропуску незареєстрованого користувача (помилковий пропуск «чужого»), то саме ними і будемо користуватись в дослідженнях:

$$FRR = 1 - Recall, \quad FAR = 1 - Specificity.$$

На рис. 3.10 та рис. 3.11 наведено гістограми значень FRR та FAR для інформативних параметрів $[x_t, y_t]$ відповідно.

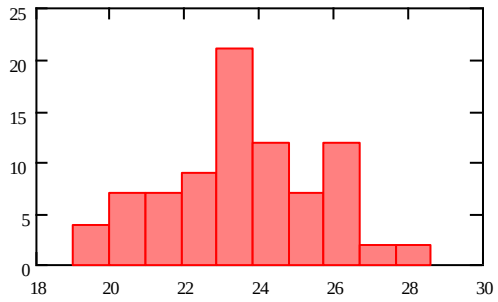


Рисунок 3.10 – Гістограма значень FRR для параметрів $[x_t, y_t]$

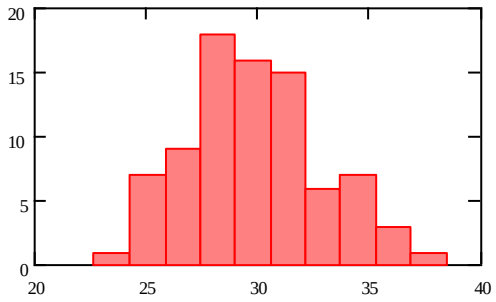


Рисунок 3.11 – Гістограма значень FAR для параметрів $[x_t, y_t]$

На рис. 3.12 та рис. 3.13 наведено гістограми значень FRR та FAR для інформативних параметрів $[p_t, f_{a_t}]$ відповідно.

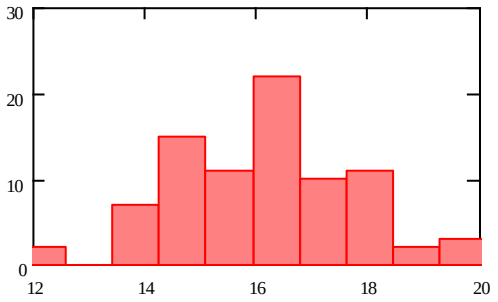


Рисунок 3.12 – Гістограма значень FRR для параметрів $[p_t, f_{a_t}]$

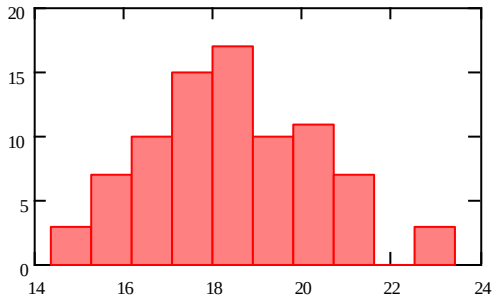


Рисунок 3.13 – Гістограма значень FAR для параметрів $[p_t, f_{a_t}]$

На рис. 3.14 та рис. 3.15 наведено гістограми значень FRR та FAR для інформативних параметрів $[x_t, y_t, p_t, f_{a_t}]$ відповідно.

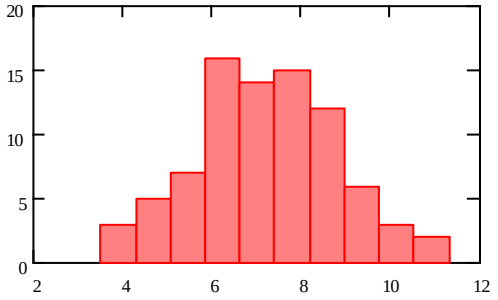


Рисунок 3.14 – Гістограма значень FRR для параметрів $[x_t, y_t, p_t, f_{a_t}]$

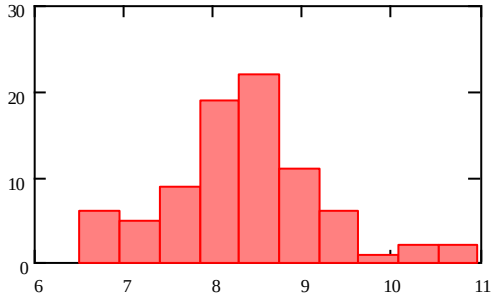


Рисунок 3.15 – Гістограма значень FAR для параметрів $[x_t, y_t, p_t, f_{a_t}]$

На рис. 3.16 та рис. 3.17 наведено гістограми значень FRR та FAR для інформативних параметрів $[vx_t, vy_t]$ відповідно.

На рис. 3.18 та рис. 3.19 наведено гістограми значень FRR та FAR для інформативних параметрів $[p_t, f_{a_t}, vx_t, vy_t]$ відповідно.

На рис. 3.20 та рис. 3.21 наведено гістограми значень FRR та FAR для інформативних параметрів $[ax_t, ay_t, az_t]$ відповідно.

На рис. 3.22 та рис. 3.23 наведено гістограми значень FRR та FAR для інформативних параметрів $[p_t, f_{a_t}, ax_t, ay_t, az_t]$ відповідно.

В табл. 3.1 наведено зведені результати точності ідентифікації користувачів в залежності від використаних інформативних ознак цифрового рукописного підпису.

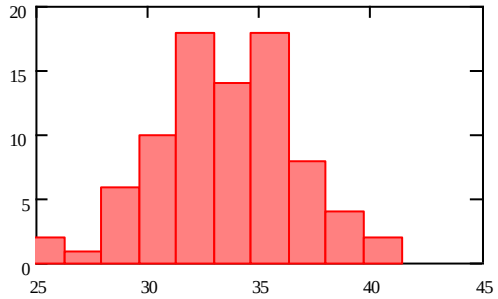


Рисунок 3.16 – Гістограма значень FRR для параметрів $[vx_t, vy_t]$

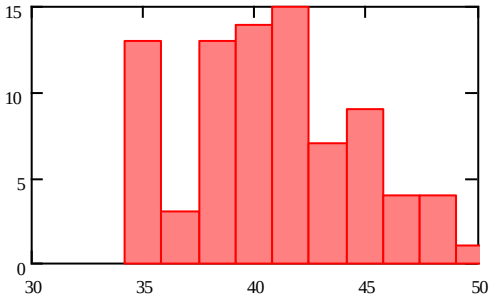


Рисунок 3.17 – Гістограма значень FAR для параметрів $[vx_t, vy_t]$

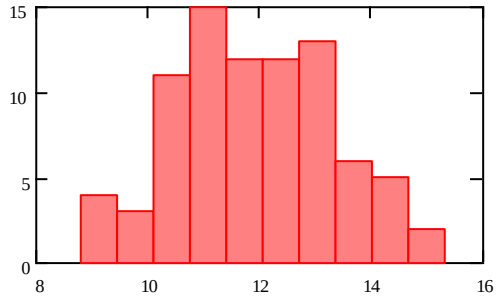


Рисунок 3.18 – Гістограма значень FRR для параметрів $[p_t, f_{a_t}, vx_t, vy_t]$

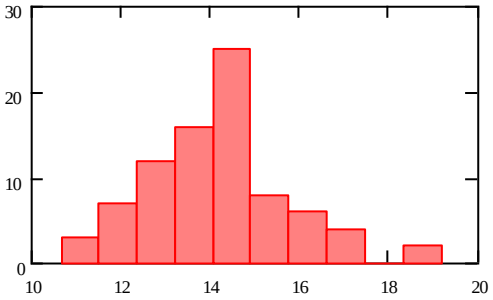


Рисунок 3.19 – Гістограма значень FAR для параметрів $[p_t, f_{a_t}, vx_t, vy_t]$

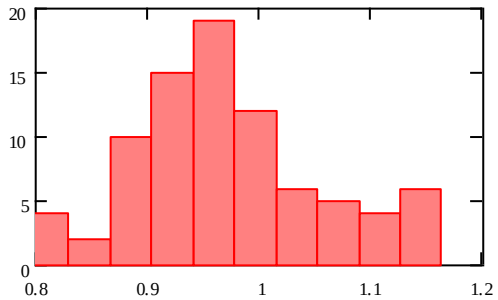


Рисунок 3.20 – Гістограма значень FRR для параметрів $[ax_t, ay_t, az_t]$

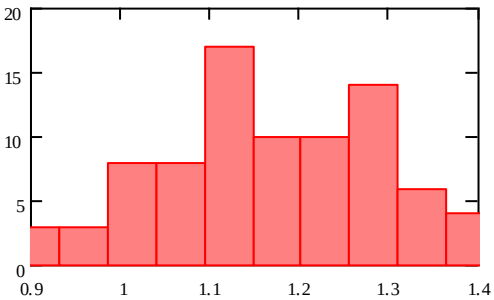


Рисунок 3.21 – Гістограма значень FAR для параметрів $[ax_t, ay_t, az_t]$

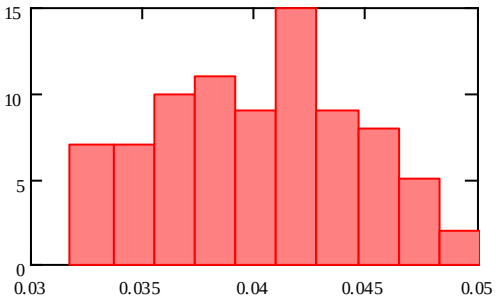


Рисунок 3.20 – Гістограма значень FRR для параметрів $[p_t, f_{a_t}, ax_t, ay_t, az_t]$

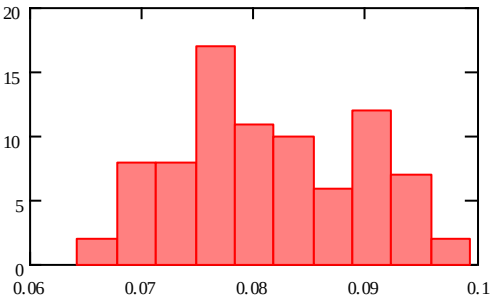


Рисунок 3.21 – Гістограма значень FAR для параметрів $[p_t, f_{a_t}, ax_t, ay_t, az_t]$

Таблиця 3.1 – Результати точності ідентифікації користувачів в залежності від використаних інформативних ознак цифрового рукописного підпису

Інформативні ознаки	False Reject Rate (помилкова відмова «своєму»), %			False Accept Rate (помилковий пропуск «чужого»), %		
	Максимальне значення	Мінімальне значення	Середнє значення	Максимальне значення	Мінімальне значення	Середнє значення
$[x_t, y_t]$	28.588	19.007	23.94	38.393	22.678	29.8
$[p_t, f_{a_t}]$	20.106	11.726	16	23.398	14.377	18.38
$[x_t, y_t, p_t, f_{a_t}]$	11.281	3.497	7.28	10.958	6.505	8.4
$[vx_t, vy_t]$	41.289	24.524	32.72	50.672	34.154	41.06
$[p_t, f_{a_t}, vx_t, vy_t]$	15.301	8.796	10.04	19.142	10.64	13.941
$[ax_t, ay_t, az_t]$	1.163	0.792	0.96	1.417	0.879	1.179
$[p_t, f_{a_t}, ax_t, ay_t, az_t]$	0.05	0.031	0.04	0.099	0.064	0.08

Як видно з табл. 3.1 жоден з параметрів, що характеризує саме динаміку відтворення рукописного підпису не забезпечує прийнятної точності. Найменша точність – 32.7 % (327 випадки на 1000 спроб) для FRR та 41.06 % (410 випадків на 1000 спроб) для FAR – відповідає швидкості переміщення кінчика пальця за координатами x та y.

Найвища точність – 16 % (160 випадки на 1000 спроб) для FRR та 18.3 % (183 випадки на 1000 спроб) для FAR – відповідає тиску і «площі плями»

від кінчика пальця в процесі вводу парольної фрази.

Варто відмітити, що подібні результати було отримано в кваліфікаційній роботі [23], що присвячено проблемі дослідження інформативних ознак клавіатурного почерку для сенсорних екранів – «За даними датасетів «MEU-Mobile KSD Data Set» (тиск на екран та за розмір «плями» від пальця в процесі вводу парольної фрази) та «The Mobikey Keystroke Dynamics Password Database» (психофізіологічні параметри) інтегральна точність мультикласової класифікації складає 53.2 % та 86.7 % відповідно. Отже тиск та розмір «плями» не є настільки унікальними параметрами «мобільного» клавіатурного почерку, щоб будувати тільки за ними аутентифікаційну систему».

Найунікальнішими параметрами введення цифрового рукописного підпису є прискорення планшету в тривимірному просторі, що характеризують положення планшету в руці користувача в процесі вводу парольної фрази – 0.96 % (10 випадків на 1000 спроб) для FRR та 1.2 % (12 випадків на 1000 спроб) для FAR.

Найвищу точність ідентифікації забезпечує комбінація тиску і «площі плями» від кінчика пальця та прискорення планшету в тривимірному просторі в процесі вводу парольної фрази – 0.04 % (4 випадки на 10000 спроб) для FRR та 0.08 % (8 випадків на 10000 спроб) для FAR. Це дуже добрий результат, що не поступається точності ідентифікації за відбитком пальця, але більш захищений від підробок.

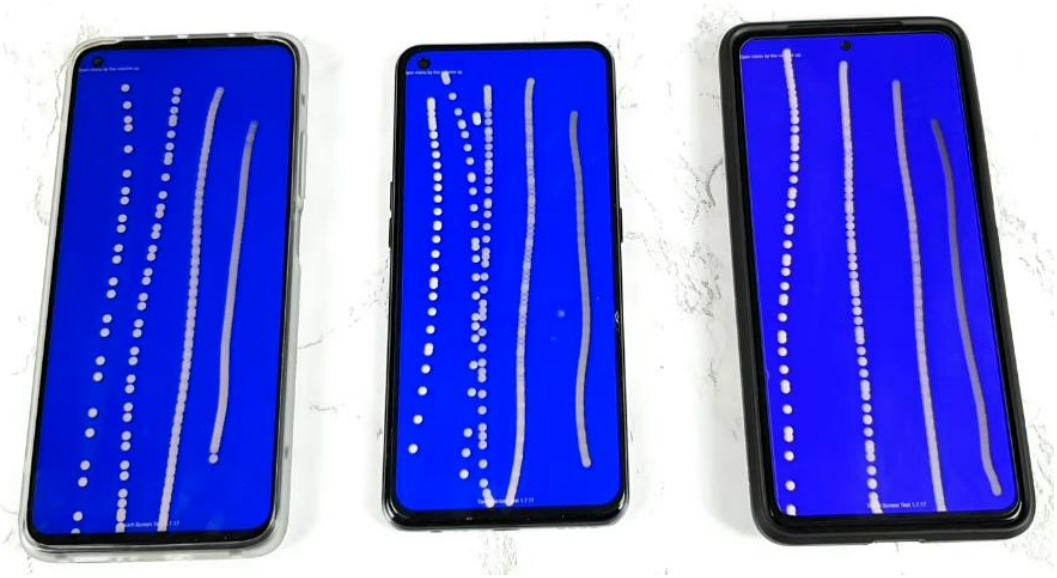
Також варто відзначити, що датасет було отримано у 2015-2016 роках на планшеті з частотою опитування екрану 60 Гц (рис. 3.22). Це призводить до того, що у випадку коротких паролів довжина послідовностей $[x_t, y_t, p_t, f_{a_t}, vx_t, vy_t, ax_t, ay_t, az_t]$ становить 50-60 відліків. Сучасні смартфони та планшети мають частоту опитування екрану 480 Гц, тобто в 8 разів більше і довжина дослідних послідовностей становила б 400-480 відліків, шо значно б підвищило точність ідентифікації.

Для підтвердження цієї тези в табл. 3.2 наведено значення FRR та FAR для двох користувачів – 19 (найкоротші інформативні послідовності) та 75

(найдовші інформативні послідовності). Як можна бачити, значення FRR та FAR для користувача 19 близькі до максимальних серед усіх користувачів. В той же час значення FRR та FAR для користувача 75, навпаки, близькі до мінімальних серед усіх користувачів.

Таблиця 3.2 – Результати точності ідентифікації користувачів 19 та 75 в залежності від використаних інформативних ознак цифрового рукописного підпису

Інформативні ознаки	False Reject Rate (помилкова відмова «своєму»), %		False Accept Rate (помилковий пропуск «чужого»), %	
	Користувач 19 / максимальне значення	Користувач 75 / мінімальне значення	Користувач 19 / максимальне значення	Користувач 75 / мінімальне значення
$[x_t, y_t]$	28.016 / 28.588	19.216 / 19.007	37.664 / 38.393	23.426 / 22.678
$[p_t, f_{a_t}]$	19.623 / 20.106	12.101 / 11.726	22.719 / 23.398	14.895 / 14.377
$[x_t, y_t, p_t, f_{a_t}]$	11.100 / 11.281	3.647 / 3.497	10.673 / 10.958	6.700 / 6.505
$[vx_t, vy_t]$	41.165 / 41.289	25.064 / 24.524	50.013 / 50.672	34.530 / 34.154
$[p_t, f_{a_t}, vx_t, vy_t]$	14.551 / 15.301	9.051 / 8.796	18.357 / 19.142	11.140 / 10.64
$[ax_t, ay_t, az_t]$	1.144 / 1.163	0.800 / 0.792	1.350 / 1.417	0.915 / 0.879
$[p_t, f_{a_t}, ax_t, ay_t, az_t]$	0.048 / 0.05	0.032 / 0.031	0.096 / 0.099	0.064 / 0.064



60 Гц 120 Гц 180 Гц

Рисунок 3.22 – Ілюстрація різних частот опитування екрану смартфону

ВИСНОВКИ

1. Виконано огляд основних методів біометричної аутентифікації, що використовуються або є перспективними для використання в мобільних пристроях. Це розпізнавання за динамічним графічним паролем, розпізнавання за тривимірним динамічним підписом, розпізнавання за відбитком пальця, розпізнавання за геометрією обличчя. Використання динамічних біометричних характеристик має потенціал для застосування як додаткова міра, що підвищує загальний рівень безпеки при аутентифікації.

2. У роботі проаналізовано інформативні ознаки цифрового рукописного підпису. Можна виділити три основних класи: динамічні параметри руху кінчика пальця екраном, параметри взаємодії з екраном (тиск та розмір «плями» від пальця) та параметри, що характеризують положення смартфону в руці користувача та коливання смартфону в просторі в процесі введення цифрового рукописного підпису.

3. За даним датасету «The MOBISIG signature database» інтегральна точність класифікації за динамічними параметрами руху кінчика пальця екраном становить 24 % (FRR) та 30 % (FAR). Таким чином, нестабільність динамічних параметрів обумовлює неможливість побудови ідентифікаційних систем, що враховують лише ці параметри.

4. За даним датасету «The MOBISIG signature database» інтегральна точність класифікації за параметрами взаємодії з екраном (тиск та розмір «плями» від пальця) становить не менше 16 % (FRR) та 18.4 % (FAR). Аналіз робіт, що присвячені вивченню проблеми мобільного клавіатурного почерку, підтверджує отриманий результат – тиск та розмір «плями» від пальця не відносяться до найінформативніших параметрів мобільного клавіатурного почерку.

6. За даними датасету «The MOBISIG signature database» найінформативнішими параметрами цифрового рукописного підпису є прискорення

планшету в тривимірному просторі, що характеризують положення планшету в руці користувача в процесі вводу парольної фрази. Використання лише цих трьох параметрів дає інтегральну точність ідентифікації 0.96 % (FRR) та 1.2 % (FAR).

7. Найвищу точність ідентифікації забезпечує комбінація тиску та розміру «плями» від пальця та прискорення планшету в тривимірному просторі в процесі вводу парольної фрази – 0.04 % (FRR) та 0.08 % (FAR). Це дуже високий результат, що не поступається точності ідентифікації за відбитком пальця, але, при цьому, цифровий рукописний підпис більш захищений від підробок.

8. Оскільки розраховані показники точності ідентифікації за цифровим рукописним підписом отримані для планшету з частотою дискретизації 60 Гц можна стверджувати про потенційну ще вищу точність, оскільки сучасні смартфони та планшети мають частоту опитування екрану до 480 Гц.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Mobile Operating System Market Share Worldwide. URL: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-200901-202311 (дата звернення: 20.10.2023).

2. Mobile & Tablet Android Version Market Share Worldwide. URL: https://gs.statcounter.com/android-version-market-share/mobile-tablet/worldwide/#monthly-201706-202311 (дата звернення: 20.10.2023).

3. Mobile & Tablet iOS Version Market Share Worldwide. URL: https://gs.statcounter.com/ios-version-market-share/mobile-tablet/worldwide/#monthly-201706-202311 (дата звернення: 20.10.2023).

4. The Android ecosystem contains a hidden patch gap. URL: https://www.srlabs.de/blog-post/android-patch-gap. Дата звернення: 20.10.2023.

5. Bitdefender Threat Debrief / December 2023. URL: https://www.bitdefender.com.au/blog/businessinsights/bitdefender-threat-debrief-december-2023/ (дата звернення: 20.10.2023).

6. Mobile Device Security. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-4.pdf (дата звернення: 20.10.2023).

7. Guven O., Akyokus S., Uysal M., Guven A. Enhanced password authentication through keystroke typing characteristics // Proc, of the IASTED Intern. Conf, on Artificial Intelligence and Appl. (AIA ’07). Honolulu: ACTA Press, 2007. P. 317-322.

8. Bar11ow N., Cukic B. Keystroke dynamics-based credential hardening systems// Handbook of Remote Biometrics. Advances in Pattern Recognition. Eds by Tistarelli M., Li S.Z., Chellappa R. London: Springer, 2009. P. 329-347.

9. F1ior E., Kowalski K. Continuous biometric user authentication in online examinations// Proc, of the 7th Intern. Conf, on Information Technology: New Generations (ITNG ’10). Las Vegas: IEEE, 2010. P. 488-492.

10. Araujo L.C.F., Sucupira L.H.R., Lizarraga M.G. et al. User authentication through typing biometrics features// IEEE Trans. Signal Process. 2005. 53. P. 851-855.

11. Kang P., Cho S. A hybrid novelty score and its use in keystroke dynamics-based user authentication// Pattern Recogn. 2009. 42. P. 3115-3127.

12. Al Sol am i E., Boyd C., Clark A., Ahmed I. User-representative feature selection for keystroke dynamics// 2011 5th Intern. Conf, on Network and System Security (NSS). Milan: IEEE, 2011. P. 229-233.

13. Alsultan A., Warwick K. Keystroke dynamics authentication: a survey of free-text methods// Int. J. Comput. Sci. Issues. 2013. 10. N 4. P. 1-10.

14. Kang P., Cho S. Keystroke dynamics-based user authentication using long and free text strings from various input devices// Inf. Sci. 2015. 308. P. 72-93.

15. A1zubaidi A., Kalita J. Authentication of smartphone users using behavioral biometrics// IEEE Communications Surveys and Tutorials. 2016. 18. N 3. P. 1998-2026.

16. Lamiche L, Bin G., Jing Y., Yu Z., Hadid A. A continuous smartphone authentication method based on gait patterns and keystroke dynamics// J. Ambient Intelligence and Humanized Computing. 2019. 10. N 11. P. 4417-4430.

17. Shimshon T., Moskovitch R., Rokach L., E1ovici Y. Clustering di-graphs for continuously verifying users according to their typing patterns// Proc, of the IEEE 26th Convention of Electrical and Electronics Engineers in Israel (IEEEI ’10). Eilat: IEEE, 2010. P. 445-449.

18. Lopes J. Keystroke recognition using Android devices. Master’s Thesis. Institute Superior Tecnico, 2015. P. 1-7.

19. Tax D.M.J. One-class classification. PhD Thesis. Delft University of Technology, 2001. P. 13-19

20. The MOBISIG on-line signature database. URL: https://www.ms.sapientia.ro/~manyi/mobisig.html (дата звернення: 20.10.2023).

21. Margit ANTAL, László Zsolt SZABÓ and Tunde TORDAI (2018), On-line Signature Verification on MOBISIG Finger Drawn Signature Corpus, 2018

22. Margit ANTAL and Andras BANDI (2017), Finger or Stylus: Their Impact on the Performance of On-line Signature Verification Systems (MACRO2017), 27-28 October, 2017 Tirgu Mures, 2017, pp. 11-22. doi: 10.1515/macro-2017-0002

23. Фесенко А.В. (2020). Дослідження ідентифікаційного потенціалу клавіатурного почерку власників мобільних пристроїв [Атестаційна робота магістра, Харківський національний університет радіоелектроніки]. Репозитарій Харківського національного університету радіоелектроніки. URL: https://openarchive.nure.ua/bitstreams/7d1ed2f6-0acf-47fd-82ac-544aa605c736/download (дата звернення: 20.10.2023).