

**Євтушенко Сергій Володимирович**

аспірант кафедри кібербезпеки

Національний університет «Одеська юридична академія», Одеса, Україна

ORCID: 0009-0005-6895-8156

serhiyevtushenko@gmail.com

ПРОЄКТУВАННЯ МОБІЛЬНОЇ ПЛАТФОРМИ ЗБОРУ МУЛЬТИМОДАЛЬНИХ БІОМЕТРИЧНИХ ДАНИХ КЛАВІАТУРНОГО ПОЧЕРКУ З УРАХУВАННЯМ ВИМОГ ІНТЕРПРЕТОВАНOSTІ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Анотація. Предметом дослідження є проєктування мобільної платформи збору мультимодальних біометричних даних, що поєднують клавіатурну динаміку сенсорного екрана з сигналами інерційних сенсорів смартфона, за умови, що зібраний корпус має бути придатним не лише для навчання моделей розпізнавання, а й для подальшої інтерпретації їхніх рішень. Мета роботи – сформулювати вимоги до схеми даних і протоколу збору, які впливають саме із задачі інтерпретації, розробити архітектуру платформи, що цим вимогам відповідає, та перевірити її прямим вимірюванням на пристроях різних поколінь. У статті вирішуються такі завдання: сформульовано вісім вимог до схеми даних і протоколу збору; виявлено й кількісно оцінено систематичні спотворення, яких припускається наївна реалізація збирача на стандартному полі вводу; розроблено архітектуру на основі власного методу введення, що цих спотворень уникає; обґрунтовано набір ознак з урахуванням фактичної доступності кожної ознаки на сучасних пристроях; проведено валідацію платформи на трьох смартфонах. Використано такі методи: інструментальне вимірювання характеристик підсистем введення та сенсорів Android; статистичне оброблення часових рядів клавіатурних подій із застосуванням стійких оцінок; порівняльний аналіз публічних корпусів поведінкової біометрії за єдиним набором критеріїв; аналіз залишкового витоку інформації в режимі знеособленого збору. Здобуто такі результати. Уперше кількісно оцінено систематичну розбіжність часових шкал між підсистемою введення та сенсорною підсистемою Android: на 12 сесіях трьох пристроїв зсув становив від 0,88 мс до 9,24 доби, і без його явного усунення в одинадцяти сесіях із дванадцяти жодна клавіатурна подія не потрапляє в межі власного сенсорного запису сесії, хоча зовні дані виглядають повними. Установлено, що сила натискання та площа контакту недоступні сторонній екранній клавіатурі на всіх трьох перевірених пристроях трьох поколінь Android: у 1970 подіях значення сили натискання дорівнює рівно одиниці без жодного винятку, а площа контакту подається в несумісних між пристроями одиницях, що ставить під сумнів відтворюваність частини опублікованих методів мобільної клавіатурної біометрії. Показано, що запиту частоту 200 Гц витримують усі три пристрої, а обмежувальним чинником є запит застосунку, а не апаратура. Запропоновано й перевірено режим збору з роздільною приватністю для завдань із вільним текстом та надано кількісну оцінку залишкового витоку. Висновки: вимога інтерпретованості ретроспективно накладає обмеження на етап збору даних, а наївна реалізація збирача не відмовляє й не сигналізує про помилку, а мовчки видає файли, які проходять будь-яку перевірку на повноту й при цьому непридатні для мультимодального аналізу.

Ключові слова: клавіатурний почерк; мультимодальна біометрія; інерційні сенсори; збір даних; інтерпретованість моделей; поведінкова автентифікація; мобільні пристрої.

ВСТУП

Постановка проблеми. Клавіатурний почерк – поведінкова біометрична характеристика, яка описує індивідуальні особливості набору тексту через часові інтервали між подіями натискання й відпускання клавіш. На відміну від фізіологічних характеристик, вона не потребує окремого сенсора, збирається непомітно для користувача й придатна для безперервної автентифікації протягом усього сеансу роботи, а не лише в момент входу [16], [23]. Перенесення цієї технології на смартфони природно доповнює



її другою модальністю: під час набору пристрій рухається, і акселерометр, гіроскоп та магнетометр фіксують рухові патерни, які самі по собі є індивідуальними [19].

Водночас між кількістю публікацій про моделі розпізнавання й кількістю корпусів, на яких ці моделі можна перевірити, зберігається помітний розрив. Систематичні огляди фіксують сотні робіт із клавіатурної динаміки [14], [16], [18], тоді як публічних мультимодальних корпусів, зібраних на мобільних пристроях, одиниці. Причина зрозуміла: збір біометричних даних вимагає інженерної роботи, організації сесій, згоди учасників і дотримання вимог до захисту персональних даних, а результат цієї роботи в академічній системі оцінювання важить менше, ніж нова архітектура нейронної мережі.

Проблема, якій присвячено цю статтю, полягає у тому, що наявні корпуси проєктувалися під максимізацію точності, а не під пояснення рішень. Ці дві мети ставлять до даних різні вимоги. Для навчання моделі достатньо, щоб у даних був сигнал. Для пояснення її рішення потрібно, щоб у корпусі були зафіксовані ті сторонні чинники – модель пристрою, поза, спосіб утримання, провідна рука учасника, – які модель могла використати як ярлики замість справжньої біометричної ознаки. Якщо цих чинників у даних немає, вони не зникають: вони просто стають невидимими для аналізу. Модель, навчена на такому корпусі, може демонструвати чудові показники й водночас розпізнавати не людину, а телефон, і жоден метод інтерпретації цього не виявить, бо ознаки «модель пристрою» в корпусі просто немає.

Друга частина проблеми має суто інженерну природу і, як показано нижче, виявляється лише під час реалізації. Наївно побудований збирач мобільної клавіатурної динаміки не відмовляє й не сигналізує про помилку. Він видає файли, які проходять будь-яку перевірку на повноту: усі стовпці заповнені, пропусків немає, кількість записів відповідає кількості натискань. І при цьому такі дані непридатні для мультимодального аналізу. Виявити це можна лише спеціальною перевіркою, яку не проводять, бо не знають, що її треба проводити.

Аналіз останніх досліджень і публікацій. Методи розпізнавання за клавіатурним почерком пройшли шлях від статистичних відстаней і опорних векторів [10] до рекурентних і трансформерних архітектур. Мережа TypeNet, навчена за метричним підходом на десятках тисяч користувачів, установила орієнтир для настільних клавіатур і сенсорних екранів [1]; TypeFormer переніс на цю задачу трансформерну архітектуру з механізмом уваги [20]. Порівняльні змагання на єдиній тестовій базі показали, що розрив між провідними підходами вже невеликий, і подальший приріст точності дедалі більше залежить від якості даних, а не від архітектури [22].

Мультимодальність – поєднання клавіатурної динаміки з інерційними сигналами – досліджується щонайменше з корпусу HMOG, у якому 100 учасників виконували завдання з набору тексту й читання, сидячи та йдучи, із записом акселерометра, гіроскопа й магнетометра [19]. Корпус BB-MAS охопив набір тексту, ходу й жести на настільному комп'ютері, планшеті та телефоні тих самих осіб [5]. BehavePassDB зібрано у сценарії пасивної автентифікації з окремими сесіями під різні модальності й явним поділом на навчальну та тестову частини [21]. Найбільший за кількістю учасників корпус мобільного набору зібрано в дослідженні Aalto: 37 тисяч добровольців, транскрипція речень у веб-формі [13]; він неоціненний для вивчення швидкості й помилок набору, але сенсорних даних і біометричного протоколу не містить.

Порівняння цих корпусів за єдиним набором критеріїв (табл. 1) показує, що жоден із них не покриває одночасно чотирьох умов, потрібних для інтерпретованої мультимодальної автентифікації: наявність подій натискання й відпускання окремих клавіш; безперервний запис інерційних сигналів із контрольованою й задокументованою частотою; повний набір коваріат, зокрема провідної руки та способу утримання пристрою; контраст поз при незмішаному дизайні «учасник × пристрій».

Таблиця 1

Порівняння публічних корпусів за критеріями інтерпретованого аналізу

Корпус	Учасників	Події клавіш	Інерційні сенсори	Коваріати	Контраст поз
HMOG [19]	100	так	так, 100 Гц	частково	сидячи / на ходу
BB-MAS [5]	117	так	так	частково	сидячи / на ходу
BehavePassDB [21]	81	так	так	ні	ні
Aalto mobile [13]	37 370	так	ні	вік, стать, мова	ні
Запропонована платформа	див. розділ «Обмеження»	так	так, 200 Гц, фактична частота в кожній сесії	провідна рука, утримання, поза, вік, стать, досвід	сидячи / стоячи / на ходу

Окремо слід зупинитися на ознаках, які з часом стали недоступними. Значна частина праць 2013–2018 років із мобільної клавіатурної біометрії будувала вектор ознак не лише на часових інтервалах, а й на



силі натискання та площі контакту пальця з екраном. Показовою є робота [4], у якій саме додавання цих двох величин до часових ознак дало помітний приріст точності на пристроях того часу. Наші вимірювання, наведені нижче, показують, що на сучасних пристроях сторонній екранний клавіатурі ці величини не передаються взагалі. Це означає, що відповідні методи сьогодні невідтворювані не через помилку в їхньому описі, а через зміну платформи, і що будь-який новий корпус мобільної клавіатурної біометрії має документувати фактичну доступність кожної ознаки, а не перелічувати їх за традицією.

Інтерпретованість рішень моделей у поведінковій біометрії спирається на загальні методи пояснювального штучного інтелекту – адитивні пояснення Шеплі [12] та локальні сурогатні моделі [15]. Обидва методи мають спільну властивість, вирішальну для цієї роботи: вони пояснюють рішення в термінах ознак, які подано моделі на вхід. Ознака, якої в корпусі немає, у поясненні не з'явиться ніколи, хоч би яким сильним був її вплив. Саме тому запобігання «навчанню за ярликами» – ситуації, коли модель спирається на побічну кореляцію замість цільової ознаки [9], – є не задачею етапу моделювання, а задачею етапу збору. У цьому ж напрямі рухається й ширша дискусія про те, що прозорість моделі має закладатися в постановку задачі, а не добудовуватися *post hoc* [17], та про потребу супроводжувати корпус структурованим описом умов його створення [8].

Українські дослідження в цій галузі зосереджені переважно на методах розпізнавання й на архітектурі систем автентифікації [25], [29], зокрема із застосуванням нейромережових моделей у задачах біометрії персоналу критичної інфраструктури [11] та згорткових мереж – до клавіатурних даних [24], тоді як питання проектування самого інструмента збору практично не розглядалося. Огляд стану предметної області, на який спирається ця робота, наведено в [26]; питання приватного навчання без централізованого збору біометричних шаблонів розглянуто в [27].

Мета статті. Метою статті є розроблення та експериментальна перевірка архітектури мобільної платформи збору мультимодальних біометричних даних клавіатурного почерку, схема даних і протокол якої задовольняють вимоги, що впливають із задачі подальшої інтерпретації рішень моделей машинного навчання.

Для досягнення мети розв'язано такі завдання:

- 1) сформулювати вимоги до схеми даних і протоколу збору, які впливають саме із задачі інтерпретації, а не з задачі максимізації точності;
- 2) виявити й кількісно оцінити систематичні спотворення, яких припускається наївна реалізація збирача на стандартному полі вводу мобільного застосунку;
- 3) розробити архітектуру платформи, що цих спотворень уникає, і схему даних, яка забезпечує трасовність кожної агрегованої ознаки до множини сирих подій;
- 4) обґрунтувати набір ознак з урахуванням фактичної доступності кожної з них на сучасних пристроях;
- 5) перевірити платформу прямим вимірюванням на пристроях різних поколінь і подати результати вимірювань у формі, придатній для повторення.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Робота спирається на одну тезу, яку варто сформулювати явно, бо вона визначає всю подальшу побудову: вимога інтерпретованості ретроспективно накладає обмеження на етап збору даних. Пояснити рішення моделі неможливо, якщо в корпусі не зафіксовані коваріати, здатні стати для моделі ярликами.

Розгорнемо це на конкретному прикладі, який має пряме відношення до плану експерименту. Нехай двоє учасників проходять сесії, кожен на своєму телефоні. Модель навчається розрізняти їх і досягає високої точності. Питання, чи розпізнає вона людину, чи телефон, у цьому дизайні нерозв'язне в принципі: особа й пристрій збігаються повністю, тобто конфаундовані. Ані додаткові дані, ані досконаліший метод інтерпретації тут не допоможуть – інформації, потрібної для розділення цих двох пояснень, у корпусі немає. Єдиний спосіб зробити питання розв'язним – закласти в протокол схрещений план, за якого кожен учасник проходить сесії на кожному пристрої. Це рішення ухвалюється до збору й після нього не коригується.

Те саме стосується провідної руки. Гіпотеза про те, що систематичне зміщення точки дотику від центра клавіші в один бік є наслідком того, яким пальцем і з якої руки виконано натискання, перевіряється лише тоді, коли провідну руку зафіксовано в анкеті, а зміщення дотику збережено в кожній події. Обидві величини мають потрапити в корпус одночасно; жодна з них окремо гіпотези не перевіряє.

Друга теза стосується інженерної сторони. Наївна реалізація збирача мовчки псує дані. Три вимірні приклади, які докладно розглянуто далі, полягають ось у чому: збирач, побудований на стандартному полі вводу, не отримує подій окремих клавіш і тому взагалі не вимірює час утримання – найінформативнішу ознаку клавіатурної динаміки; координати дотику, зняті з поля вводу, а не з клавіатури, є сталими, тобто



стовпці виглядають заповненими, але інформації про натискання не несуть; клавіатурні події та сенсорні відліки датуються різними годинниками, і на реальному пристрої розбіжність між ними вимірюється добами.

З цих двох тез випливають вісім вимог до платформи, які й становлять ядро запропонованого підходу.

B1. Повнота коваріат. У корпусі мають бути зафіксовані провідна рука, спосіб утримання пристрою, поза, вік, стать, досвід користування смартфоном, модель і версія операційної системи пристрою, а також фактична частота кожного сенсора в кожній сесії. Обґрунтування: кожна з цих величин є кандидатом на роль ярлика, і перевірити її вплив можна лише за наявності відповідного поля.

B2. Трасовність ознак. Кожна агрегована ознака має зводитися до визначеної множини сирих подій. Це означає, що корпус зберігає не обчислені статистики, а самі події, з порядковими номерами й мітками часу. Обґрунтування: пояснення, отримане на агрегованих ознаках, перевіряється лише поверненням до подій, з яких вони обчислені.

B3. Єдина часова шкала. Клавіатурні події та сенсорні відліки мають бути подані на одному монотонному годиннику, а застосований зсув – збережено в описі сесії, щоб перетворення можна було перевірити або скасувати під час аналізу. Обґрунтування наведено в розділі результатів: без цього мультимодальна частина корпусу непридатна, причому зовні виглядає бездоганно.

B4. Сегментація і збалансованість дизайну. Межі сесій мають бути явними, а план збору – таким, щоб учасник і пристрій не були конфаундовані. Крім того, порядок поз має чергуватися між учасниками, а перша сесія кожного учасника вважатися ознайомлювальною й не входити в аналіз.

B5. Приватність за побудовою. Знеособлення виконується на пристрої, а не після передавання. Для завдань із наперед відомим знеособленим стимулом припустимо зберігати позицію клавіші й код символу; для завдань із вільним текстом зберігається лише клас клавіші, без абсолютних координат дотику й розмірів клавіші.

B6. Відтворюваність. Схема даних версіонована; кожна сесія супроводжується описом умов запису; вивантаження містить маніфест із контрольними сумами. Обґрунтування: без цього неможливо ні перевірити цілісність переданого корпусу, ні співвіднести дані, зібрані різними версіями застосунку [8].

B7. Покриття розкладки стимулом. Фіксований текст завдання має задіювати всі клавіші, для яких збираються ознаки. Обґрунтування емпіричне і наведено нижче: попередній стимул задіював 22 літери з 32, наявних на розкладці, тобто для десяти клавіш він не передбачав жодного натискання, і жодна ознака, побудована на них, не мала б підкріплення в даних.

B8. Фіксація режиму живлення. У картку сесії записуються стан енергозбереження, тепловий стан на початку й у кінці сесії, рівень заряду та факт заряджання. Обґрунтування: просідання фактичної частоти сенсорів заднім числом неможливо пояснити, якщо ці умови не зафіксовано, а самі режими «підвищеної продуктивності» в оболонках виробників стандартного програмного інтерфейсу не мають.

Вимоги B1–B6 узагальнюють міркування, викладені вище, і частково перегукуються з практикою провідних корпусів [19], [21]. Вимоги B7 і B8 сформульовано за результатами власних вимірювань і, наскільки вдалося встановити, у літературі з мобільної клавіатурної біометрії явно не формулювалися.

МЕТОДИКА ДОСЛІДЖЕННЯ

Перша ітерація та її обмеження. Платформу розроблено у двох ітераціях, і порівняння між ними становить самостійну частину результату. Перша ітерація була типовою для швидкого прототипу: односторінковий застосунок, у якому реєстрація натискань відбувалася в обробнику зміни тексту стандартного поля вводу, сенсори опитувалися з системною сталою затримки, призначеною для оновлення інтерфейсу, а мітки часу бралися з настінного годинника. Такий прототип працює, експортує файли й на перший погляд робить саме те, чого від нього чекають.

Аудит його вихідного коду виявив вісім обмежень, з яких три мають систематичний характер і не усуваються налаштуванням. Перше: обробник зміни тексту – це подія редагування, а не подія клавіші, тому пари «натискання – відпускання» не існує в принципі, і час утримання клавіші не вимірюється. З п'яти канонічних часових ознак клавіатурної динаміки лишається одна – інтервал між послідовними натисканнями. Причина не в реалізації, а в платформі: системна екранна клавіатура Android не передає застосунку подій окремих клавіш, лише результат редагування тексту.

Друге: обробник дотиків, навішений на поле вводу, не отримує дотиків до клавіатури, бо екранна клавіатура є окремим вікном системи. Отже, координати дотику, площа контакту й сила натискання зберігають значення від останнього дотику безпосередньо до текстового поля й фактично є константами, повтореними в кожному рядку вивантаження. Це не стилістична вада, а систематично недостовірні дані: стовпці заповнені й пройдуть будь-яку перевірку на пропуски, але не несуть інформації про натискання.

Третє: сенсорні дані в такій реалізації не є часовим рядом. Обробник події сенсора лише оновлює кілька змінних поточного стану, а у вивантаженні потрапляє їхній миттєвий знімок у момент натискання клавіші. Неможливими стають вікна навколо події та будь-які статистики по них, спектральні ознаки й похідні прискорення. Уся сенсорна модальність зводиться до кількох скалярів на натискання.

Друга ітерація: архітектура. Друга ітерація перепроєктована під вимоги В1–В8. Її будову показано на рис. 1.

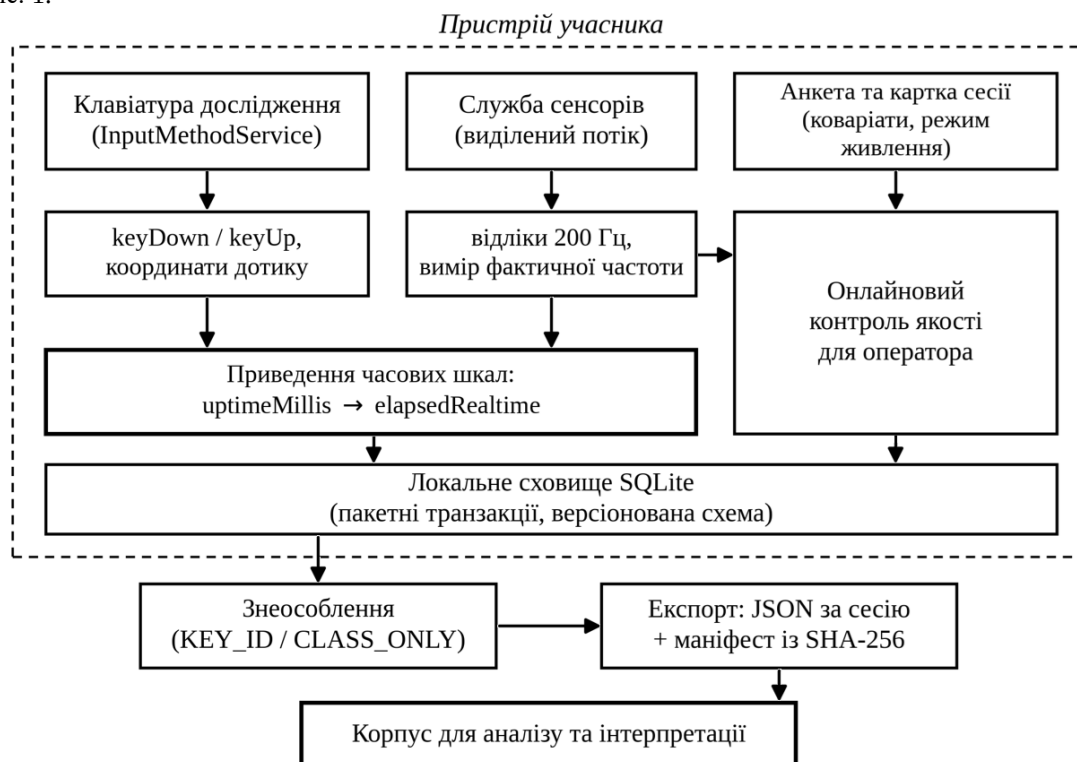


Рис. 1. Архітектура платформи збору: джерела подій, приведення часових шкал, локальне сховище, знеособлення та експорт

Ключове рішення – власна екранна клавіатура, реалізована як служба методу введення. Це єдиний надійний спосіб на платформі Android отримати одночасно момент натискання, момент відпускання й справжні координати дотику до конкретної клавіші, тобто закрити перше й друге обмеження першої ітерації. Клавіатура оголошує українську розкладку ЙЦУКЕН із 32 літерами та латинську QWERTY з цифровим рядом; перемикання між ними поза сесією виконується окремою клавішею, а під час сесії розкладку задає завдання.

Запис клавіатурних подій ведеться лише в полі вводу самого застосунку: обробник відкидає подію, якщо пакет активного редактора не збігається з власним. Навіть якщо учасник залишить клавіатуру ввімкненою після завершення дослідження, набір у сторонніх застосунках у корпус не потрапить. Це технічна реалізація обіцянки, яку дається учаснику в тексті згоди.

Сенсори записуються безперервно, на виділеному потоці, із запитом періоду 5000 мкс, що відповідає 200 Гц. Записуються акселерометр, гіроскоп, магнетометр і вектор орієнтації. Для кожного відліку зберігається не лише мітка часу самої події, а й момент виклику зворотного виклику: різниця між ними дає затримку доставки й потрібна, щоб відрізнити справжній розрив у потоці від затримки планувальника. Фактично досягнута частота вимірюється в кожній сесії й записується в її картку – на Android фактична частота майже ніколи не дорівнює запитаній.

Приведення часових шкал. Підсистема введення Android датує події за годинником, який не рахує час глибокого сну пристрою, а сенсори – за годинником, який його рахує [2], [3]. Це різні шкали, і різниця між ними дорівнює сумарній тривалості глибокого сну від останнього перезавантаження. Механізм розходження показано на рис. 2, а.

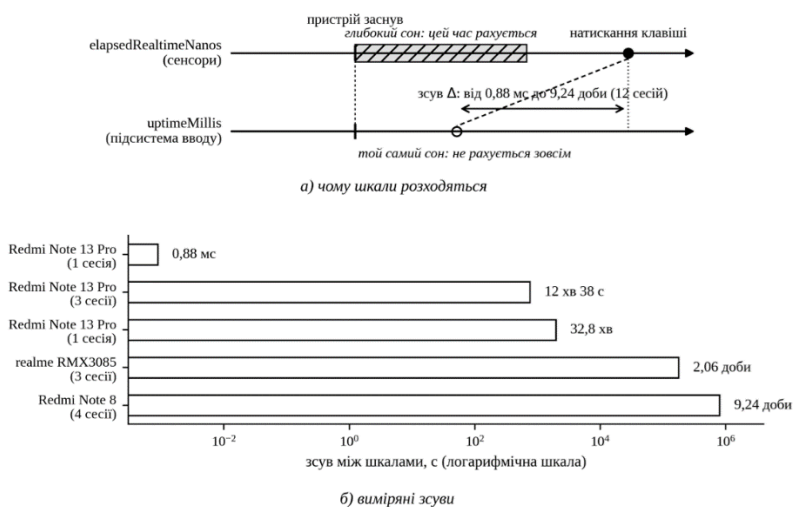


Рис. 2. Розбіжність часових шкал Android: а) механізм розходження; б) зсуви, виміряні у 12 сесіях на трьох пристроях

Зсув вимірюється один раз на початку сесії як різниця показів двох годинників, застосовується при записі кожної клавіатурної події і зберігається в полі картки сесії. Збереження зсуву є принциповим: воно дозволяє під час аналізу перевірити перетворення або скасувати його, тобто задовольняє вимогу В3 не лише за суттю, а й за перевірюваністю.

Схема даних. Схему даних побудовано за зразком BehavePassDB [21] із розширенням під вимоги В1, В2 і В8. Її наведено на рис. 3.

Дані зберігаються локально в реляційному сховищі з пакетними транзакціями по 512 відліків, що забезпечує від втрати сесії при знищенні процесу системою. Вивантаження формується як один документ на сесію плюс маніфест; події подано колонково, що і скорочує обсяг, і зберігає орієнтацію на схему BehavePassDB. Маніфест містить версію формату, версію застосунку, лічильники, опис часової шкали та контрольну суму SHA-256 кожного файлу.

Окремо слід пояснити поле зміщення точки дотику від центра клавіші, нормованого її розмірами. Це не дублювання абсолютних координат: систематичне зміщення в один бік є прямим наслідком того, яким пальцем і з якої руки виконано натискання, тому саме ця величина, а не абсолютна координата, безпосередньо пов'язана з коваріацією провідної руки й придатна для перевірки відповідної гіпотези методами інтерпретації.

Набір ознак. Набір ознак сформовано так, щоб кожна група мала явно зазначену фактичну доступність на сучасних пристроях (табл. 2). Колонка доступності – не формальність: як показано в розділі результатів, дві групи ознак, широко вживані в літературі, сьогодні недоступні взагалі.

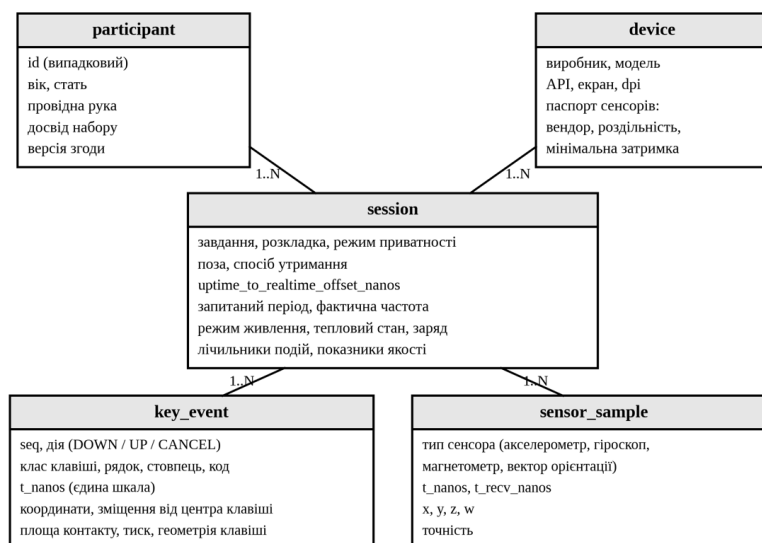


Рис. 3. Схема даних платформи



Набір ознак із зазначенням фактичної доступності

Група	Ознаки	Фактична доступність
Темпоральні	час утримання клавіші (H); інтервали між подіями у чотирьох варіантах (DD, UD, UU, DU); диграфи; швидкість набору; розподіл пауз	доступні повністю
Просторові	зміщення точки дотику від центра клавіші; нормоване її розмірами; геометрія клавіші; щільність екрана	доступні; потребують нормування на фізичний розмір при порівнянні пристроїв
Силові	сила натискання; площа контакту (велика й мала осі, розмір дотику)	недоступні на жодному з трьох перевірених пристроїв
Поведінка при виправленні	частка натискань Backspace; затримка перед виправленням; довжина серії виправлень; затримка повернення до набору	доступні повністю
Сенсорні	статистики вікна навколо події для акселерометра, гіроскопа, магнетометра; кути орієнтації; спектральні ознаки; похідна прискорення	доступні; частота фіксується в кожній сесії
Коваріати	провідна рука; спосіб утримання; поза; вік; стать; досвід; модель і версія ОС; режим живлення	доступні (анкета та картка сесії)

Поведінку при виправленні помилок винесено в окрему групу свідомо. У практиці збору поширений підхід – відкидати натискання Backspace як шум. Наведені нижче виміри показують, що це не шум, а стійка поведінкова характеристика з власною часовою структурою, і що її вилучення коштує дорого.

Протокол збору та етичні аспекти. Участь у дослідженні добровільна й починається з екрана інформованої згоди, який кожен учасник має прочитати особисто. Ім'я, контакти, місце навчання чи роботи не збираються: застосунок їх не запитує. Ідентифікатор учасника генерується випадково на пристрої й ніде не пов'язується з особою. Учасник у будь-який момент може видалити всі свої записи кнопкою відкриття згоди. Резервне копіювання даних застосунку в хмару вимкнено на рівні маніфесту.

Обробка персональних даних у дослідженні відповідає вимогам Закону України «Про захист персональних даних» [28] і принципам мінімізації даних та обмеження мети, закріпленим у Загальному регламенті про захист даних [6]. Оскільки результати збору призначені для навчання й подальшого пояснення моделей машинного навчання в задачі біометричної ідентифікації, до них застосовні також вимоги до прозорості та документування даних, передбачені Регламентом (ЄС) 2024/1689 [7].

Формулювання згоди щодо завдань із вільним текстом потребує окремої точності. Некоректно стверджувати, що відновити написане неможливо: як показано в розділі результатів, послідовність класів клавіш дозволяє відновити кількість слів і довжину кожного з них. Тому в тексті згоди зазначено, що неможливо відновити слова, а зберігається лише кількість символів у них.

План сесій побудовано за схрещеним принципом: кожен учасник проходить набір завдань на кожному пристрої, порядок пристроїв і порядок поз чергується між учасниками, перша сесія кожного учасника на кожному пристрої вважається ознайомлювальною і в аналіз не входить. Підстава для останніх двох правил емпірична й наведена нижче.

Емпірична база. Апробацію проведено на трьох смартфонах трьох поколінь Android: Xiaomi 23117RA68G (Redmi Note 13 Pro, Android 16), realme RMX3085 (Android 12) та Xiaomi Redmi Note 8 (Android 11). Виконано 12 сесій, у яких зареєстровано 1970 клавіатурних подій, що утворюють 985 повних пар «натискання – відпускання», і 349 038 сенсорних відліків. Завдання – транскрипція українського тексту (режим зі збереженням позиції клавіші) та вільний текст (режим збереження лише класу клавіші); пози – сидячи, стоячи, на ходу.

Ці сесії є технічною апробацією платформи, а не корпусом: усі вони виконані автором. Обмеження, які звідси впливають, докладно розглянуто наприкінці розділу результатів. Водночас для тих питань, яким присвячена стаття, – чи вимірює платформа те, що має вимірювати, і чи придатні одержані дані для мультимодального аналізу – обсягу апробації достатньо, бо йдеться про властивості вимірювального інструмента, а не про властивості популяції.



РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Цілісність потоку подій. Перша перевірка стосується найпростішого: чи не втрачає платформа події. У всіх 12 сесіях кількість натискань дорівнює кількості відпускань (985 і 985), порядкові номери подій утворюють неперервну послідовність без пропусків, мітки часу монотонно зростають, непарних подій і подій скасування жести немає. Жодна з 985 пар не залишилася незіставленою. Це базовий, але необхідний результат: без нього всі подальші вимірювання не мали б сенсу.

Розбіжність часових шкал. Це найважливіший результат роботи. Виміряні зсуви між шкалою підсистеми введення та шкалою сенсорної підсистеми наведено в табл. 3 і показано на рис. 2, б.

Таблиця 3

Виміряні зсуви часових шкал і наслідки їх неврахування

Пристрій	Сесій	Зсув	Подій у межах сенсорного запису після приведення шкал	Те саме без приведення
Redmi Note 13 Pro	1	0,88 мс	138 зі 138	138 зі 138
Redmi Note 13 Pro	3	758,1 с (12 хв 38 с)	428 із 428	0 із 428
Redmi Note 13 Pro	1	1965,3 с (32,8 хв)	204 із 204	0 із 204
realme RMX3085	3	2,06 доби	486 із 486	0 із 486
Redmi Note 8	4	9,23–9,24 доби	714 із 714	0 із 714
Усього	12	від 0,88 мс до 9,24 доби	1970 із 1970	138 із 1970

Зсув змінюється в діапазоні понад дев'ять порядків. Мінімальне значення 0,88 мс отримано в сесії, записаній невдовзі після перезавантаження пристрою, – саме такий випадок і створює оманливе враження, що приведення шкал непотрібне. Максимальне значення 9,24 доби відповідає пристрою, який не перезавантажувався понад тиждень і більшу частину часу перебував у глибокому сні.

Практичний наслідок сформульовано в останній колонці табл. 3. Якщо клавіатурні події залишити в їхній власній шкалі, то в одинадцяти сесіях із дванадцяти жодна клавіатурна подія не потрапляє навіть у межі сенсорного запису тієї самої сесії – усі 1832 події опиняються за межами інтервалу, у якому взагалі існують сенсорні дані. Про побудову вікон навколо натискань у такій ситуації не йдеться. При цьому файли повні, стовпці заповнені, мітки часу монотонні, і жодна автоматична перевірка якості цього не виявить: обидві шкали виглядають правдоподібно, просто вони різні.

Наскільки вдалося встановити, у літературі з мобільної мультимодальної біометрії цей ефект явно не описаний. Він і не мав би виявитися сам собою: він не спричиняє ані помилки, ані аномалії в даних, а проявляється лише як відсутність зв'язку між модальностями – тобто як негативний результат моделювання, який природно приписати слабкості сигналу, а не дефекту збору.

Фактичні частоти сенсорів проти апаратних меж. Запит 200 Гц витримали всі три пристрої (табл. 4). Розбіжність із запитаним значенням не перевищує 2,1 %, максимальний розрив у потоці акселерометра становить 4,9–5,2 мс, тобто дорівнює одному періоду; єдиний виняток – 9,47 мс в одній сесії «на ходу», що відповідає одному пропущеному відліку.

Результат суперечить очікуванню, що бюджетний пристрій 2019 року стане вузьким місцем. Навпаки: його акселерометр і гіроскоп здатні видавати 400 Гц – удвічі більше за два новіші пристрої, у яких датчики обмежені 200 Гц. Обмежувальним чинником є запит застосунку, а не апаратура. Різниця в частоті магнетометра (100 проти 50 Гц) також суто апаратна й визначається мінімальним періодом конкретної мікросхеми, а не режимом живлення чи версією системи.

Практичний висновок для протоколу: 200 Гц є правильним спільним знаменником. Підвищувати запит немає сенсу, бо два пристрої з трьох уперлися б у стелю, а аналіз усе одно зводиться до найнижчої спільної частоти. Проте сам факт, що фактична частота відрізняється від запитаної на кожному пристрої по-різному, підтверджує необхідність записувати її в кожному сесію, як того вимагає В1.

Таблиця 4

Фактичні частоти сенсорів проти апаратних меж

Пристрій	Датчик IMU	Акселерометр і гіроскоп, факт., Гц	Апаратна межа, Гц	Магнетометр, факт., Гц	Апаратна межа, Гц
Redmi Note 13 Pro	ST LSM6DSO	204,1	200	49,0–50,0	50



Пристрій	Датчик IMU	Акселерометр і гіроскоп, факт., Гц	Апаратна межа, Гц	Магнетометр, факт., Гц	Апаратна межа, Гц
realme RMX3085	InvenSense ICM4x6xx	201,3	200	50,0	50
Redmi Note 8	Bosch BMI160	198,5	400	100,0	100

Доступність ознак дотику. Результат, наведений у табл. 5, стосується не платформи, а стану самої предметної області.

Таблиця 5

Доступність ознак дотику сторонній екранній клавіатурі

Пристрій	Android	Подій	Сила натискання	Площа контакту (велика вісь)	Розмір дотику
Xiaomi 23117RA68G	16	770	1,0 – єдине значення	0,687471 – єдине значення	0,043137 – єдине значення
realme RMX3085	12	486	1,0 – єдине значення	4 рівні: 5, 11, 12, 13	= велика вісь / 255
Xiaomi Redmi Note 8	11	714	1,0 – єдине значення	1,0 – єдине значення	0,003922 – єдине значення

Сила натискання дорівнює рівно одиниці в усіх 1970 подіях на всіх трьох пристроях, без жодного винятку. Одиниця – це документоване запасне значення, яке система повертає, коли драйвер сенсорного екрана не передає застосункам цю величину. Первісна гіпотеза, що йдеться про наслідок оновлення системи, не підтвердилася: пристрій 2019 року з Android 11 поводить себе так само, як пристрій 2023 року з Android 16.

Площа контакту формально доступна, але непорівнянна між пристроями: на одному з Xiaomi це нормоване число близько 0,69, на realme – цілі значення від 5 до 13, на другому Xiaomi – стала одиниця. Одиниці вимірювання різні, і на двох із трьох пристроїв величина взагалі не змінюється. Додатково встановлено, що на двох пристроях «розмір дотику» є точно великою віссю, поділеною на 255 (розбіжність не перевищує $5 \cdot 10^{-7}$), тобто одна з двох ознак надлишкова, а на третьому пристрої ці дві величини подано в різних одиницях і такого співвідношення між ними немає.

Звідси випливає висновок, істотний для всієї предметної області. Значна частина праць 2013–2018 років із мобільної клавіатурної біометрії будувала ознаки саме на силі натискання та площі контакту й повідомляла про приріст точності від їх додавання [4]. На перевірених сучасних пристроях сторонній клавіатурі ці величини недоступні, отже, відповідні результати сьогодні невідтворювані. Формулювати це слід обережно: недоступні на жодному з трьох перевірених пристроїв – а не недоступні взагалі. Кожен додатковий пристрій коштує однієї сесії й додає одне свідчення, тому таку таблицю варто розширювати й у подальших роботах.

Що втрачає наївна реалізація. Наслідки трьох систематичних дефектів першої ітерації оцінено кількісно на тих самих даних (табл. 6).

Таблиця 6

Кількісна оцінка наслідків дефектів наївної реалізації

Дефект	Наслідок, виміряний на 12 сесіях
Реєстрація подій в обробнику зміни тексту	нуль значень часу утримання замість 985; з п'яти канонічних часових ознак лишається одна
Миттєвий знімок сенсорів у момент натискання	5910 чисел замість 349 038 відліків; вікна навколо події, спектральні ознаки та похідна прискорення неможливі
Частота опитування сенсорів ≈ 16 Гц	у вікні ± 50 мс навколо натискання медіана 2 відліки замість 20; відстань до найближчого відліку 15,5 мс (максимум 32,6) замість 1,29 мс (максимум 2,5)
Координати дотику з поля вводу, а не з клавіатури	сталі в межах сесії: стовпці заповнені, інформації про натискання не несуть
Різні часові шкали для подій і сенсорів	в 11 сесіях із 12 жодна клавіатурна подія не потрапляє в межі сенсорного запису тієї самої сесії

Третій рядок таблиці варто пояснити наочно. На рис. 4, а нижче наведено фрагмент потоку акселерометра тривалістю 3 с із накладеними моментами натискань після приведення шкал; сірі смуги відповідають інтервалам утримання клавіш. На рис. 4, б те саме вікно ± 50 мс навколо одного натискання показано у двох частотах опитування: за 200 Гц у вікно потрапляє 20 відліків, які описують форму сплеску прискорення, за приблизно 16 Гц – два відліки, розташовані фактично випадково відносно моменту натискання.

Зіставлення двох ітерацій показує, що йдеться не про різницю в якості, а про різницю в тому, які ознаки взагалі існують у даних. Наївна реалізація не дає гіршого часу утримання – вона не дає його зовсім. Це саме той тип дефекту, який найважче виявити після збору: він не залишає слідів у самих даних.

Правдоподібність вимірюваних величин. Наступне питання – чи узгоджуються одержані значення з тим, що відомо про набір тексту на сенсорному екрані. Розподіли часу утримання клавіші та інтервалів між натисканнями наведено на рис. 5.

Медіана часу утримання по сесіях коливається в межах 75,0–93,0 мс, медіана інтервалу між натисканнями – 322,7–409,5 мс. Обидва діапазони узгоджуються з опублікованими спостереженнями за набором на сенсорних екранах [13]. Стандартне відхилення часу утримання в межах сесії становить 12,3–18,1 мс, за єдиним винятком, розглянутим нижче.

Важливіший результат стосується стабільності. Для клавіш, які трапляються в усіх сесіях того самого пристрою, розкид медіан між сесіями становить 7,7 мс на Redmi Note 13 Pro (чотири сесії, 25 клавіш), 4,6 мс на realme RMX3085 (три сесії, 26 клавіш) і 4,2 мс на Redmi Note 8 (дві сесії, 26 клавіш), тоді як типове стандартне відхилення часу утримання тієї самої клавіші всередині однієї сесії дорівнює 10,1, 11,7 і 7,9 мс відповідно. Тобто те саме натискання відтворюється між сесіями точніше, ніж воно варіює всередині однієї сесії. Саме ця властивість робить величину придатною для біометрії, і саме вона зникає в реалізації, що часу утримання не вимірює.

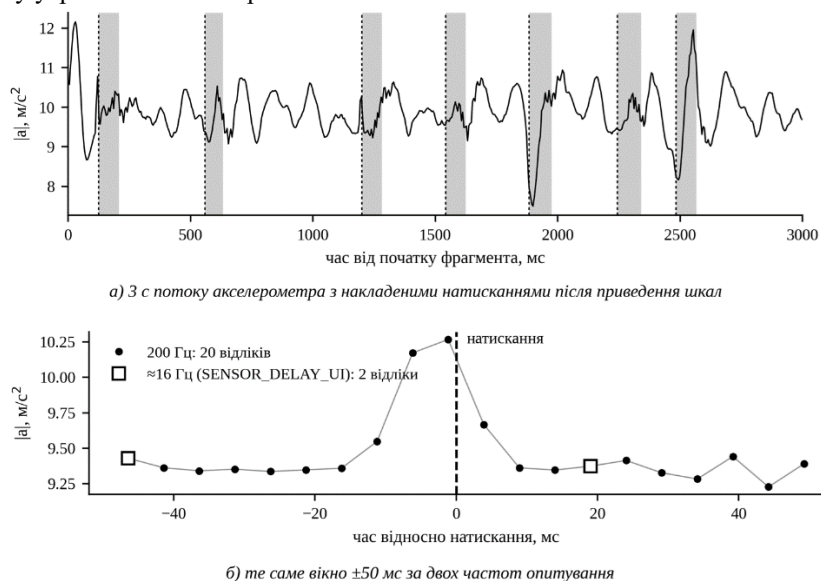


Рис. 4. Сенсорний потік і моменти натискань:

- а) фрагмент тривалістю 3 с після приведення шкал;
б) вікно ± 50 мс навколо натискання за двох частот опитування

Вплив поодиноких викидів і вибір статистик. В одній із сесій зафіксовано натискання пробілу тривалістю 1412 мс: учасник зробив паузу, не знявши палець із клавіші. Це справжня поведінка, а не збій – цілісність послідовності подій у цій сесії бездоганна. Проте один такий випадок зміщує стандартне відхилення часу утримання зі 13,3 до 147,3 мс, тобто в одинадцять разів, тоді як медіана не змінюється зовсім: 93,0 мс в обох випадках.

Звідси випливає методична вимога до етапу виділення ознак: користуватися стійкими статистиками – медіаною, усередненим середнім, міжквартильним розмахом – а не середнім і стандартним відхиленням. Паузи з утриманням клавіші слід виявляти й обробляти окремо, як самостійну поведінкову подію, а не вилучати мовчки.

Поведінка при виправленні помилок. Частка натискань Backspace у сесії коливається від 0 до 11,2 %. Це не рідкісна подія, а звичайна складова набору. Виміри показують, що виправлення має власну часову структуру.

Медіанний інтервал перед першим натисканням Backspace у серії становить 1103 мс проти 375 мс у звичайному наборі, тобто у 2,9 раза довший; окремі значення сягають 5210 мс. Усередині серії виправлень інтервали, навпаки, короткі – медіана 160 мс. Після завершення виправлення інтервал лишається підвищеним (медіана 413 мс). Тобто людина спершу помічає помилку, зупиняється, потім швидко виконує серію видалень і лише після цього повертається до звичайного темпу.

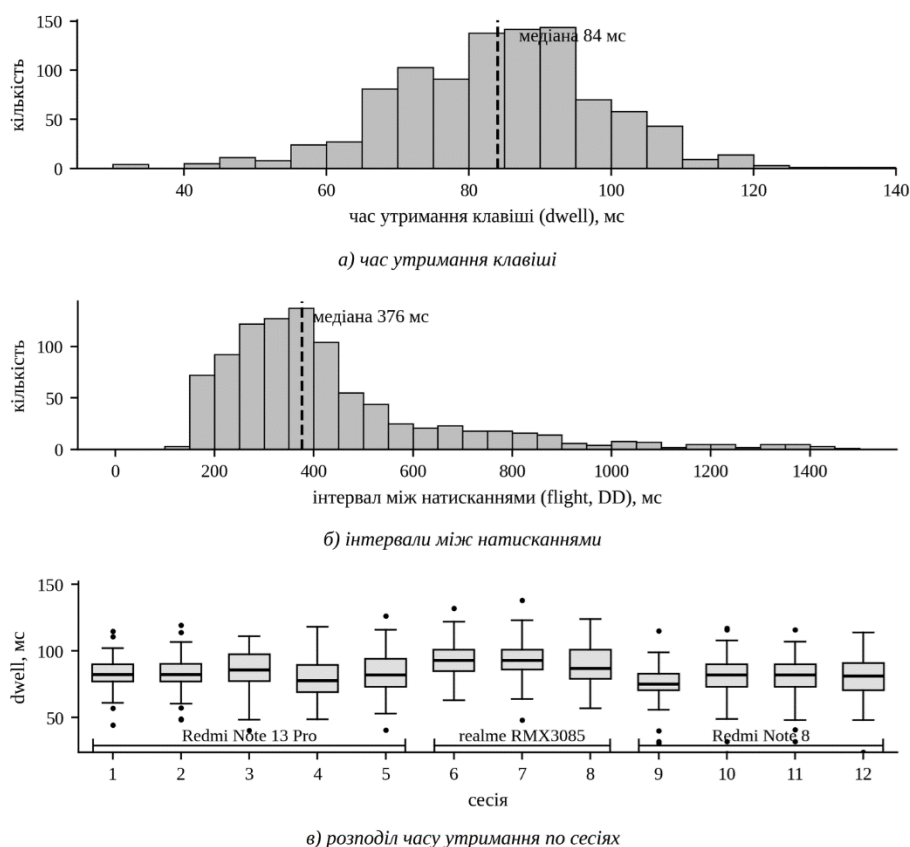


Рис. 5. Розподіли часових ознак: а) час утримання клавіші, 985 натискань; б) інтервали між натисканнями, 973 значення, з них 29 понад 1500 мс не показано; в) розподіл часу утримання по сесіях, викид 1412 мс у сесії 7 поза межами графіка

Вплив виправлень на зведені показники помірний: вилучення інтервалів, суміжних із виправленнями, зсуває медіану інтервалу між натисканнями в межах від $-7,5$ до $+11,0$ мс, тобто не більш ніж на 3 %. Але ціна такого вилучення висока – втрачається від 2,4 до 13,6 % усіх інтервалів. Справжня проблема при цьому не в зсуві середніх, а у вирівнюванні: для завдань із фіксованим текстом ознаки будуються на конкретних парах клавіш, а виправлення змінює послідовність натискань, тому в різних учасників послідовності не збігаються і зіставити диграфи безпосередньо неможливо.

Рекомендація, що впливає з цих вимірів, складається з трьох частин: ніколи не фільтрувати виправлення на етапі збору; в аналізі рахувати ознаки у двох варіантах – по всій послідовності та по ділянках без виправлень – і порівнювати їх; саму поведінку при виправленні винести в окрему групу ознак, як це зроблено в табл. 2.

Режим приватності та залишковий витік. Режим збереження лише класу клавіші перевірено на трьох сесіях вільного тексту, що містять 626 подій на двох пристроях. Приховано повністю: рядок і стовпець клавіші, код символу, абсолютні координати дотику та розміри клавіші – усі ці поля дорівнюють службовому значенню. Збережено, як і задумано: клас клавіші, час, зміщення від центра клавіші (від 81 до 118 різних значень на сесію), площа контакту й сила натискання.

Приховування абсолютних координат є принциповим і не зводиться до приховування коду символу. Геометрія клавіатури детермінована, тому за самими координатами дотику символ відновлюється майже точно – зберігати координати й приховувати код було б самообманом.

Водночас чесний аналіз показує, що залишковий витік існує. Послідовність класів клавіш дозволяє відновити структуру тексту: кількість слів і довжину кожного з них, а також розташування розділових



знаків. Для трьох перевірених сесій відновлюються ряди довжин слів для 13, 17 і 11 слів відповідно; наприклад, для однієї з них – [5, 5, 12, 5, 1, 9, 11, 1, 4, 2, 9, 4, 2, 18, 2, 4, 8]. Самі літери не відновлюються. Такий рівень захисту прийнятний для завдання, у якому учасника просять описати фільм або книгу й прямо застерігають не вказувати відомостей про себе, але формулювання згоди має його відображати точно.

Дизайн сесій: два емпіричні уроки. Перший стосується покриття розкладки. Українська розкладка застосунку містить 32 літери. Стимул, який використовувався в апробації, задіював 22 з них у типовій сесії; ще три літери трапилися лише як помилки набору, а сім – б, в, г, ж, я, є, ї – не з'явилися в даних жодного разу. Для цих семи клавіш не зібрано нічого, і жодна ознака, побудована на них, не мала б підкріплення. Стимул замінено панграмою з 89 символів, яка покриває всі 32 літери розкладки; звідси й вимога B7.

Другий урок стосується порядку сесій і виявився несподіваним. Чотири послідовні сесії з тим самим стимулом на одному пристрої дали такі медіани інтервалу між натисканнями: 377,7 мс (сидячи), 335,2 мс (сидячи), 354,0 мс (стоячи), 322,7 мс (на ходу); швидкість набору зростала монотонно – 119,1; 123,1; 137,7 і 142,7 натискання за хвилину. Паузи між трьома останніми сесіями становили 15 і 12 с. Тобто найшвидшою виявилася сесія «на ходу», яка мала б бути найповільнішою.

Пояснення просте: учасник запам'ятовує речення і далі відтворює його з пам'яті, а не читає. Ефект наочності повністю конфаундований із позою, і будь-який висновок про вплив пози на клавіатурний почерк, зроблений на такому матеріалі, був би хибним. Звідси три правила протоколу: чергувати порядок поз між учасниками; вважати першу сесію ознайомлювальною й не включати її в аналіз; не проводити всі сесії підряд без пауз. Спостереження також підкреслює вагу вимоги B4: дефект тут не в даних, а в плані експерименту, і жодна обробка після збору його не виправить.

Окремо зафіксовано, що фізичні розміри клавіш різняться між пристроями. Висота клавіатури задана в незалежних від щільності одиницях і на всіх трьох пристроях становить 9,32–9,33 мм, тоді як ширина клавіші-літери успадковується від ширини екрана: 4,68–4,72 мм на обох Xiaomi і 4,25–4,29 мм на realme, тобто на 9 % менше, зі співвідношенням сторін 0,50 проти 0,46. Та сама людина фізично працює з різними клавішами на різних телефонах, тому зіставляти нормовані зміщення дотику між пристроями без перерахунку на фізичні розміри не можна. Геометрія клавіші та щільність екрана записуються у вивантаження саме для того, щоб такий перерахунок був можливий.

Обмеження дослідження. Обмеження цієї роботи слід назвати прямо, бо вони визначають, які твердження в ній є доказовими, а які – ні.

По-перше, усі 12 сесій апробації виконано однією особою – автором. Це достатньо для тверджень про властивості вимірювального інструмента (цілісність потоку подій, зсуви часових шкал, фактичні частоти сенсорів, доступність ознак дотику), бо всі вони стосуються поведінки платформи, а не поведінки людей. Це недостатньо для будь-яких тверджень про розрізнення осіб.

По-друге, показники точності автентифікації в роботі не наводяться і не можуть бути отримані на такий вибірці. Будь-яке число такого роду, обчислене на даних однієї людини, було б беззмістовним.

По-третє, висновок про недоступність силових характеристик дотику стосується трьох перевірених пристроїв трьох поколінь Android, а не платформи Android узагалі. Розширення таблиці 5 на більшу кількість моделей є прямим і недорогим продовженням роботи.

По-четверте, внесок сенсорів руху в розрізнення осіб кількісно не оцінювався: у цій статті показано лише, що сенсорні дані записуються з контрольованою частотою й коректно суміщаються з клавіатурними подіями в часі. Оцінювання самого внеску потребує корпусу з достатньою кількістю учасників.

По-п'яте, спостереження щодо ефекту наочності отримано на послідовності сесій одного учасника й має силу методичного застереження, а не кількісної оцінки величини ефекту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі сформульовано вісім вимог до схеми даних і протоколу збору мультимодальних біометричних даних клавіатурного почерку, які впливають саме із задачі подальшої інтерпретації рішень моделей: повнота коваріат, трасовність ознак, єдина часова шкала, сегментація і збалансованість дизайну, приватність за побудовою, відтворюваність, покриття розкладки стимулом і фіксація режиму живлення. Дві останні вимоги сформульовано за результатами власних вимірювань.

Розроблено й реалізовано архітектуру платформи, що цим вимогам відповідає, і перевірено її прямим вимірюванням на трьох смартфонах трьох поколінь Android: 12 сесій, 1970 клавіатурних подій, 349 038 сенсорних відліків.

Уперше кількісно оцінено систематичну розбіжність часових шкал між підсистемою введення та сенсорною підсистемою Android. Вимірний зсув змінюється від 0,88 мс до 9,24 доби, і без його явного усунення в одинадцяти сесіях із дванадцяти жодна клавіатурна подія не потрапляє в межі власного



сенсорного запису сесії. Оскільки цей дефект не залишає жодних слідів у самих даних, він робить мультимодальний корпус непридатним непомітно для дослідника.

Установлено, що сила натискання й площа контакту недоступні сторонній екранній клавіатурі на всіх трьох перевірених пристроях: у 1970 подіях сила натискання дорівнює рівно одиниці без жодного винятку, а площа контакту подається в несумісних між пристроями одиницях. Це ставить під сумнів відтворюваність частини опублікованих методів мобільної клавіатурної біометрії й обґрунтовує потребу документувати фактичну доступність кожної ознаки в кожному новому корпусі.

Запропоновано й перевірено режим збору з роздільною приватністю, за якого для завдань із вільним текстом зберігаються часові та просторові характеристики без можливості відновлення слів; надано кількісну оцінку залишкового витоку, яка полягає у відновлюваності кількості слів і довжини кожного з них.

Показано також, що запитану частоту 200 Гц витримують усі три пристрої, причому обмежувальним чинником є запит застосунок, а не апаратура; що поведінка при виправленні помилок має власну часову структуру й має розглядатися як самостійна група ознак; що поодинокі викиди вимагають переходу до стійких статистик; і що ефект навчіння на повторюваному стимулі здатен повністю замаскувати вплив пози.

Перспективи подальших досліджень визначаються обмеженнями, названими вище. Найближчий крок – збір корпусу за схрещеним планом із достатньою кількістю учасників, що дозволить відокремити вплив особи від впливу пристрою та кількісно оцінити внесок інерційних сенсорів. Наступний – навчання й порівняння моделей на зібраному корпусі з подальшим застосуванням методів пояснювального штучного інтелекту для перевірки того, чи спирається модель на біометричні ознаки, а не на зафіксовані коваріати. Окремим напрямом лишається розширення таблиці доступності ознак дотику на більшу кількість моделей пристроїв, що дозволить перейти від твердження про три перевірені пристрої до обґрунтованого твердження про платформу загалом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Acien, A., Morales, A., Monaco, J. V., Vera-Rodriguez, R., & Fierrez, J. (2022). TypeNet: Deep learning keystroke biometrics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(1), 57–70. <https://doi.org/10.1109/TBIOM.2021.3112540>
2. Android Developers. (2026). SensorEvent. <https://developer.android.com/reference/android/hardware/SensorEvent>
3. Android Developers. (2026). SystemClock. <https://developer.android.com/reference/android/os/SystemClock>
4. Antal, M., Szabó, L. Z., & László, I. (2015). Keystroke dynamics on Android platform. *Procedia Technology*, 19, 820–826. <https://doi.org/10.1016/j.protcy.2015.02.118>
5. Belman, A. K., Wang, L., Iyengar, S. S., Sniatala, P., Wright, R., Dora, R., Baldwin, J., Jin, Z., & Phoha, V. V. (2019). Insights from BB-MAS – A large dataset for typing, gait and swipes of the same person on desktop, tablet and phone. *arXiv*. <https://doi.org/10.48550/arXiv.1912.02736>
6. European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). *Official Journal of the European Union*, L 119, 1–88.
7. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L, 2024/1689.
8. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM*, 64(12), 86–92. <https://doi.org/10.1145/3458723>
9. Geirhos, R., Jacobsen, J.-H., Michaelis, C., Zemel, R., Brendel, W., Bethge, M., & Wichmann, F. A. (2020). Shortcut learning in deep neural networks. *Nature Machine Intelligence*, 2(11), 665–673. <https://doi.org/10.1038/s42256-020-00257-z>
10. Kasprowski, P., Borowska, Z., & Harezlak, K. (2022). Biometric identification based on keystroke dynamics. *Sensors*, 22(9), 3158. <https://doi.org/10.3390/s22093158>
11. Korchenko, O., Tereikovskiy, I., Ziubina, R., Tereikovska, L., Korystin, O., Tereikovskiy, O., & Karpinskiy, V. (2025). Modular neural network model for biometric authentication of personnel in critical infrastructure facilities based on facial images. *Applied Sciences*, 15(5), 2553. <https://doi.org/10.3390/app15052553>



12. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems 30* (pp. 4765–4774). Curran Associates.
13. Palin, K., Feit, A. M., Kim, S., Kristensson, P. O., & Oulasvirta, A. (2019). How do people type on mobile devices? Observations from a study with 37,000 volunteers. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services* (pp. 1–12). ACM. <https://doi.org/10.1145/3338286.3340120>
14. Pisani, P. H., & Lorena, A. C. (2013). A systematic review on keystroke dynamics. *Journal of the Brazilian Computer Society*, 19(4), 573–587. <https://doi.org/10.1007/s13173-013-0117-7>
15. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). ACM. <https://doi.org/10.1145/2939672.2939778>
16. Roy, S., Roy, U., & Sinha, D. D. (2022). Systematic literature review on latest keystroke dynamics based models. *IEEE Access*, 10, 93569–93599. <https://doi.org/10.1109/ACCESS.2022.3197756>
17. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206–215. <https://doi.org/10.1038/s42256-019-0048-x>
18. Shadman, R., Wahab, A. A., Manno, M., Lukaszewski, M., Hou, D., & Hussain, F. (2023). Keystroke dynamics: Concepts, techniques, and applications. *arXiv*. <https://doi.org/10.48550/arXiv.2303.04605>
19. Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. S. (2016). HMOG: New behavioral biometric features for continuous authentication of smartphone users. *IEEE Transactions on Information Forensics and Security*, 11(5), 877–892. <https://doi.org/10.1109/TIFS.2015.2506542>
20. Stragapede, G., Delgado-Santos, P., Tolosana, R., Vera-Rodriguez, R., Guest, R., & Morales, A. (2024). TypeFormer: Transformers for mobile keystroke biometrics. *Neural Computing and Applications*, 36(29), 18531–18545. <https://doi.org/10.1007/s00521-024-10140-2>
21. Stragapede, G., Vera-Rodriguez, R., Tolosana, R., & Morales, A. (2023). BehavePassDB: Public database for mobile behavioral biometrics and benchmark evaluation. *Pattern Recognition*, 134, 109089. <https://doi.org/10.1016/j.patcog.2022.109089>
22. Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Damer, N., Fierrez, J., & Ortega-Garcia, J. (2023). Keystroke Verification Challenge (KVC): Biometric and fairness benchmark evaluation. *arXiv*. <https://doi.org/10.48550/arXiv.2311.06000>
23. Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. *The Scientific World Journal*, 2013, 408280. <https://doi.org/10.1155/2013/408280>
24. Terekovskiy, I., Terekovska, L., Korystin, O., Mussiraliyeva, S., & Sambetbayeva, A. (2020). User keystroke authentication and recognition of emotions based on convolutional neural network. In *Advances in Artificial Systems for Medicine and Education III* (Vol. 1126, pp. 26–35). Springer. https://doi.org/10.1007/978-3-030-39162-1_3
25. Дудикевич, В., Микитин, Г., Насилевський, В., & Фігурняк, В. (2023). До питання безпечної багатофакторної аутентифікації у веб-застосунках. *Захист інформації*, 25(2), 76–82. <https://doi.org/10.18372/2410-7840.25.17675>
26. Євтушенко, С. В. (2025). Аспекти побудови та застосування систем аналізу клавіатурного почерку для автентифікації користувачів. *Інформатика та математичні методи в моделюванні*, 15(3), 367–376. <https://doi.org/10.15276/imms.v15.no3.367>
27. Євтушенко, С. В. (2025). Про перспективи федеративного навчання для систем автентифікації на основі аналізу клавіатурного почерку. У *Матеріали LVIII Міжнародної науково-практичної конференції «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку»* (с. 173–177). Львів, Болгарія.
28. Про захист персональних даних, Закон України № 2297-VI (2010). <https://zakon.rada.gov.ua/laws/show/2297-17>
29. Касіяненко, Д. В. (2022). Автентифікація користувачів на основі аналізу клавіатурного почерку. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*, 33(72)(3), 50–55. <https://doi.org/10.32838/2663-5941/2022.3/08>

**Serhii V. Yevtushenko**

PhD student, Department of Cybersecurity
National University «Odesa Law Academy», Odesa, Ukraine
ORCID: 0009-0005-6895-8156
serhiyevtushenko@gmail.com

DESIGN OF A MOBILE PLATFORM FOR COLLECTING MULTIMODAL BIOMETRIC KEYSTROKE DYNAMICS DATA WITH REGARD TO THE INTERPRETABILITY REQUIREMENTS OF MACHINE LEARNING MODELS

Abstract. The subject of the study is the design of a mobile platform for collecting multimodal biometric data that combine touchscreen keystroke dynamics with inertial sensor signals of a smartphone, under the condition that the resulting corpus must be suitable not only for training recognition models but also for the subsequent interpretation of their decisions. The purpose of the work is to formulate the requirements for the data schema and the collection protocol that follow specifically from the interpretation task, to develop a platform architecture that satisfies these requirements, and to verify it by direct measurement on devices of different generations. The article solves the following tasks: eight requirements for the data schema and the collection protocol are formulated; the systematic distortions introduced by a naive collector implementation built on a standard text input field are identified and quantified; an architecture based on a custom input method that avoids these distortions is developed; a feature set is justified with regard to the actual availability of every feature on modern devices; the platform is validated on three smartphones. The following methods are used: instrumental measurement of the characteristics of the Android input and sensor subsystems; statistical processing of keystroke event time series using robust estimators; comparative analysis of public behavioral biometrics corpora against a unified set of criteria; analysis of residual information leakage in the de-identified collection mode. The following results were obtained. For the first time, the systematic divergence between the time bases of the Android input subsystem and the sensor subsystem has been quantified: across 12 sessions on three devices the offset ranged from 0.88 ms to 9.24 days, and without its explicit removal, in eleven sessions out of twelve not a single keystroke event falls within the boundaries of the session's own sensor recording, although the data appear complete. It is established that touch pressure and contact area are unavailable to a third-party on-screen keyboard on all three tested devices spanning three Android generations: across 1970 events the pressure value equals exactly one without a single exception, and the contact area is reported in units that are incomparable between devices, which casts doubt on the reproducibility of a part of the published mobile keystroke biometrics methods. It is shown that the requested rate of 200 Hz is sustained by all three devices, and the limiting factor is the application's request rather than the hardware. A collection mode with separable privacy for free-text tasks is proposed and verified, and a quantitative estimate of the residual leakage is provided. Conclusions: the interpretability requirement retrospectively imposes constraints on the data collection stage, while a naive collector implementation neither fails nor signals an error but silently produces files that pass any completeness check and are nevertheless unusable for multimodal analysis.

Keywords: keystroke dynamics; multimodal biometrics; inertial sensors; data collection; model interpretability; behavioral authentication; mobile devices.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Acien, A., Morales, A., Monaco, J. V., Vera-Rodriguez, R., & Fierrez, J. (2022). TypeNet: Deep learning keystroke biometrics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(1), 57–70. <https://doi.org/10.1109/TBIOM.2021.3112540>
2. Android Developers. (2026). SensorEvent. <https://developer.android.com/reference/android/hardware/SensorEvent>
3. Android Developers. (2026). SystemClock. <https://developer.android.com/reference/android/os/SystemClock>
4. Antal, M., Szabó, L. Z., & László, I. (2015). Keystroke dynamics on Android platform. *Procedia Technology*, 19, 820–826. <https://doi.org/10.1016/j.protcy.2015.02.118>



5. Belman, A. K., Wang, L., Iyengar, S. S., Sniatala, P., Wright, R., Dora, R., Baldwin, J., Jin, Z., & Phoha, V. V. (2019). Insights from BB-MAS – A large dataset for typing, gait and swipes of the same person on desktop, tablet and phone. arXiv. <https://doi.org/10.48550/arXiv.1912.02736>
6. European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.
7. European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L, 2024/1689.
8. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. Communications of the ACM, 64(12), 86–92. <https://doi.org/10.1145/3458723>
9. Geirhos, R., Jacobsen, J.-H., Michaelis, C., Zemel, R., Brendel, W., Bethge, M., & Wichmann, F. A. (2020). Shortcut learning in deep neural networks. Nature Machine Intelligence, 2(11), 665–673. <https://doi.org/10.1038/s42256-020-00257-z>
10. Kasprowski, P., Borowska, Z., & Harezlak, K. (2022). Biometric identification based on keystroke dynamics. Sensors, 22(9), 3158. <https://doi.org/10.3390/s22093158>
11. Korchenko, O., Tereikovskiy, I., Ziubina, R., Tereikovska, L., Korystin, O., Tereikovskiy, O., & Karpinskiy, V. (2025). Modular neural network model for biometric authentication of personnel in critical infrastructure facilities based on facial images. Applied Sciences, 15(5), 2553. <https://doi.org/10.3390/app15052553>
12. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In Advances in Neural Information Processing Systems 30 (pp. 4765–4774). Curran Associates.
13. Palin, K., Feit, A. M., Kim, S., Kristensson, P. O., & Oulasvirta, A. (2019). How do people type on mobile devices? Observations from a study with 37,000 volunteers. In Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services (pp. 1–12). ACM. <https://doi.org/10.1145/3338286.3340120>
14. Pisani, P. H., & Lorena, A. C. (2013). A systematic review on keystroke dynamics. Journal of the Brazilian Computer Society, 19(4), 573–587. <https://doi.org/10.1007/s13173-013-0117-7>
15. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1135–1144). ACM. <https://doi.org/10.1145/2939672.2939778>
16. Roy, S., Roy, U., & Sinha, D. D. (2022). Systematic literature review on latest keystroke dynamics based models. IEEE Access, 10, 93569–93599. <https://doi.org/10.1109/ACCESS.2022.3197756>
17. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. Nature Machine Intelligence, 1(5), 206–215. <https://doi.org/10.1038/s42256-019-0048-x>
18. Shadman, R., Wahab, A. A., Manno, M., Lukaszewski, M., Hou, D., & Hussain, F. (2023). Keystroke dynamics: Concepts, techniques, and applications. arXiv. <https://doi.org/10.48550/arXiv.2303.04605>
19. Sitová, Z., Šeděnka, J., Yang, Q., Peng, G., Zhou, G., Gasti, P., & Balagani, K. S. (2016). HMOG: New behavioral biometric features for continuous authentication of smartphone users. IEEE Transactions on Information Forensics and Security, 11(5), 877–892. <https://doi.org/10.1109/TIFS.2015.2506542>
20. Stragapede, G., Delgado-Santos, P., Tolosana, R., Vera-Rodriguez, R., Guest, R., & Morales, A. (2024). TypeFormer: Transformers for mobile keystroke biometrics. Neural Computing and Applications, 36(29), 18531–18545. <https://doi.org/10.1007/s00521-024-10140-2>
21. Stragapede, G., Vera-Rodriguez, R., Tolosana, R., & Morales, A. (2023). BehavePassDB: Public database for mobile behavioral biometrics and benchmark evaluation. Pattern Recognition, 134, 109089. <https://doi.org/10.1016/j.patcog.2022.109089>
22. Stragapede, G., Vera-Rodriguez, R., Tolosana, R., Morales, A., Damer, N., Fierrez, J., & Ortega-Garcia, J. (2023). Keystroke Verification Challenge (KVC): Biometric and fairness benchmark evaluation. arXiv. <https://doi.org/10.48550/arXiv.2311.06000>
23. Teh, P. S., Teoh, A. B. J., & Yue, S. (2013). A survey of keystroke dynamics biometrics. The Scientific World Journal, 2013, 408280. <https://doi.org/10.1155/2013/408280>
24. Tereikovskiy, I., Tereikovska, L., Korystin, O., Mussiraliyeva, S., & Sambetbayeva, A. (2020). User keystroke authentication and recognition of emotions based on convolutional neural network. In Advances in Artificial Systems for Medicine and Education III (Vol. 1126, pp. 26–35). Springer. https://doi.org/10.1007/978-3-030-39162-1_3



25. Dudykevych, V., Mykytyn, H., Nasylevskyi, V., & Fihurniak, V. (2023). Do pytan'nia bezpechnoi bahatofaktornoï avtentyfikatsii u veb-zastosunkakh. *Zakhyst informatsii*, 25(2), 76–82. <https://doi.org/10.18372/2410-7840.25.17675>
26. Yevtushenko, S. V. (2025). Aspekty pobudovy ta zastosuvannia system analizu klaviaturnoho pocherku dlia avtentyfikatsii korystuvachiv. *Informatyka ta matematychni metody v modeliuvanni*, 15(3), 367–376. <https://doi.org/10.15276/imms.v15.no3.367>
27. Yevtushenko, S. V. (2025). Pro perspektyvy federatyvnoho navchannia dlia system avtentyfikatsii na osnovi analizu klaviaturnoho pocherku. In *Materialy LVIII Mizhnarodnoi naukovo-praktychnoi konferentsii "Suchasni aspekty modernizatsii nauky: stan, problemy, tendentsii rozvytku"* (pp. 173–177). Lovech, Bulgaria.
28. Pro zakhyst personalnykh danykh, *Zakon Ukrainy* No. 2297-VI (2010). <https://zakon.rada.gov.ua/laws/show/2297-17>
29. Kasiianenko, D. V. (2022). Avtentyfikatsiia korystuvachiv na osnovi analizu klaviaturnoho pocherku. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Serii: Tekhnichni nauky*, 33(72)(3), 50–55. <https://doi.org/10.32838/2663-5941/2022.3/08>

Отримано редакцією журналу / Received: 07.06.26

Прорецензовано / Revised: 20.06.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.