

**АСПЕКТИ ПОБУДОВИ ТА ЗАСТОСУВАННЯ СИСТЕМ АНАЛІЗУ
КЛАВІАТУРНОГО ПОЧЕРКУ ДЛЯ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ**

С.В. Євтушенко

Національний університет «Одеська юридична академія»
2, Академічна вул., Одеса, 65000, Україна
Email: serhiyevtushenko@gmail.com

Предметом дослідження в статті є системи аналізу клавіатурного почерку для автентифікації користувачів з використанням методів штучного інтелекту та їх інтеграція з сенсорами мобільних пристроїв. Мета роботи – аналіз аспектів побудови та застосування систем аналізу клавіатурного почерку для автентифікації користувачів з використанням методів штучного інтелекту та дослідження перспектив їхнього розвитку для створення мультимодальних біометричних систем. У статті вирішуються такі завдання: формування моделі архітектури багаторівневих систем клавіатурної динаміки; систематизація методів штучного інтелекту для аналізу темпоральних патернів набору тексту; аналіз підходів до інтеграції гіроскопів та акселерометрів мобільних пристроїв для створення мультимодальних біометричних систем; дослідження методів інтерпретації результатів моделей глибокого навчання в контексті біометричної автентифікації. Використовуються такі методи: математичного оброблення темпоральних послідовностей клавіатурного вводу; глибокого навчання з архітектурами LSTM, CNN та Transformer; статистичного аналізу поведінкових патернів; машинного навчання з контрольованими та неконтрольованими алгоритмами; ансамблевих підходів для підвищення точності класифікації. Здобуто такі результати: сформульовано принципи побудови багаторівневої архітектури систем клавіатурного почерку; систематизовано методи штучного інтелекту для аналізу біометричних характеристик набору тексту; проаналізовано сучасні комерційні реалізації з показниками EER 0.10-0.20% для провідних систем; досліджено перспективи інтеграції сенсорів мобільних пристроїв для досягнення EER до 6.4% в мультимодальних системах. Висновки: застосування методу поєднання клавіатурної динаміки з даними гіроскопів та акселерометрів дозволяє створювати високоточні системи безперервної автентифікації з підвищеною стійкістю до атак імітації та можливістю адаптації до еволюції поведінкових патернів користувачів.

Ключові слова: клавіатурний почерк; біометрична автентифікація; штучний інтелект; глибоке навчання; мультимодальні системи.

Вступ. Клавіатурний почерк або *keystroke dynamics* представляє унікальну поведінкову біометричну технологію, яка аналізує індивідуальні особливості набору тексту для автентифікації користувачів. У сучасних умовах зростання кіберзагроз та необхідності забезпечення безперервної автентифікації користувачів, системи аналізу клавіатурного почерку набувають особливого значення як ефективний та економічно доцільний метод біометричної ідентифікації. На відміну від фізіологічних біометричних характеристик, поведінкові особливості набору тексту важче підробити або скопіювати, що робить цю технологію особливо привабливою для сучасних систем кібербезпеки.

Динаміка клавіатурного вводу відображає унікальні нейромоторні патерни кожної людини, які формуються протягом років навчання та практики набору тексту. Ці патерни включають час утримання клавіш (*dwell time*), інтервали між натисканнями (*flight time*), ритм набору та характеристики тиску. Сучасні дослідження демонструють, що інтеграція методів штучного інтелекту з аналізом клавіатурного почерку дозволяє досягати високих показників точності автентифікації при збереженні зручності використання для кінцевих користувачів.

Особливе значення набуває розвиток систем безперервної автентифікації, які здатні контролювати ідентичність користувача протягом всієї сесії роботи, що критично

важливо для захисту від атак з перехоплення сесій та внутрішніх загроз. Інтеграція сенсорів смартфонів, зокрема гіроскопів та акселерометрів, відкриває нові горизонти для мультимодальної біометричної автентифікації, що поєднує традиційний аналіз клавіатурного почерку з аналізом рухових патернів пристрою.

Теоретичні основи та класифікація систем клавіатурного почерку. Клавіатурний почерк належить до категорії поведінкових біометричних технологій, які на відміну від фізіологічних характеристик, аналізують набуті або навчені поведінкові патерни. Фундаментальною основою цієї технології є припущення, що кожна людина має унікальний стиль набору тексту, який відображає індивідуальні особливості нейромоторної координації, фізіологічних характеристик рук та пальців, а також сформованих протягом життя звичок набору тексту [1].

Історичні корені концепції клавіатурного почерку сягають XIX століття, коли телеграфісти могли розпізнавати один одного за характерним стилем передачі азбуки Морзе, відомим як "кулак відправника". Під час Другої світової війни ця техніка виявилася цінною для розрізнення дружніх операторів від ворожих на основі їхніх відмінних патернів передачі сигналів. Сучасні системи аналізу клавіатурного почерку успадкували цей принцип, адаптувавши його для цифрових клавіатур та сенсорних екранів.

Динамічні характеристики клавіатурного почерку включають декілька ключових параметрів. Час утримання клавіші (dwell time) представляє інтервал між натисканням та відпусканням окремої клавіші, відображаючи індивідуальні особливості тиску пальців та механіки набору. Час польоту (flight time) характеризує інтервали між послідовними натисканнями клавіш та має декілька варіантів вимірювання: down-down (між натисканнями двох клавіш), up-down (між відпусканням однієї клавіші та натисканням наступної), up-up (між відпусканням двох послідовних клавіш). Ці параметри формують унікальний темпоральний відбиток для кожного користувача [2].

Статистичні параметри клавіатурного почерку охоплюють широкий спектр метрик, включаючи середні значення та дисперсію часових інтервалів, аналіз розподілів ймовірностей для різних комбінацій клавіш, патерни швидкості набору та консистентності ритму. Особливе значення мають діграми (двосимвольні послідовності) та триграми (трисимвольні послідовності), які дозволяють аналізувати контекстуальні особливості набору конкретних комбінацій символів. Біометричні особливості включають глобальні характеристики (загальна швидкість набору, частота помилок, використання спеціальних клавіш) та локальні характеристики (специфічні темпоральні патерни для окремих клавіш та їх комбінацій) [3].

Сучасні системи також інтегрують аналіз патернів виправлення помилок, використання клавіш-модифікаторів (Shift, Ctrl, Alt), навігаційних клавіш та специфічних стилів капіталізації тексту. Ці розширені характеристики дозволяють створювати більш детальні та стійкі біометричні профілі користувачів, що підвищує загальну точність автентифікації та знижує ймовірність успішних атак імітації.

Архітектура та компоненти систем аналізу клавіатурного почерку. Сучасні системи аналізу клавіатурного почерку мають багаторівневу архітектуру (рис. 1), яка включає шари збору даних, попередньої обробки, екстракції ознак, класифікації та прийняття рішень. Шар збору даних забезпечує реєстрацію подій клавіатури в реальному часі з високоточними мітками часу, абстракцію від різних типів клавіатур та фільтрацію системних подій. Особливої уваги потребує забезпечення точності часових вимірювань, оскільки навіть мілісекундні відхилення можуть суттєво впливати на якість біометричних шаблонів [4].

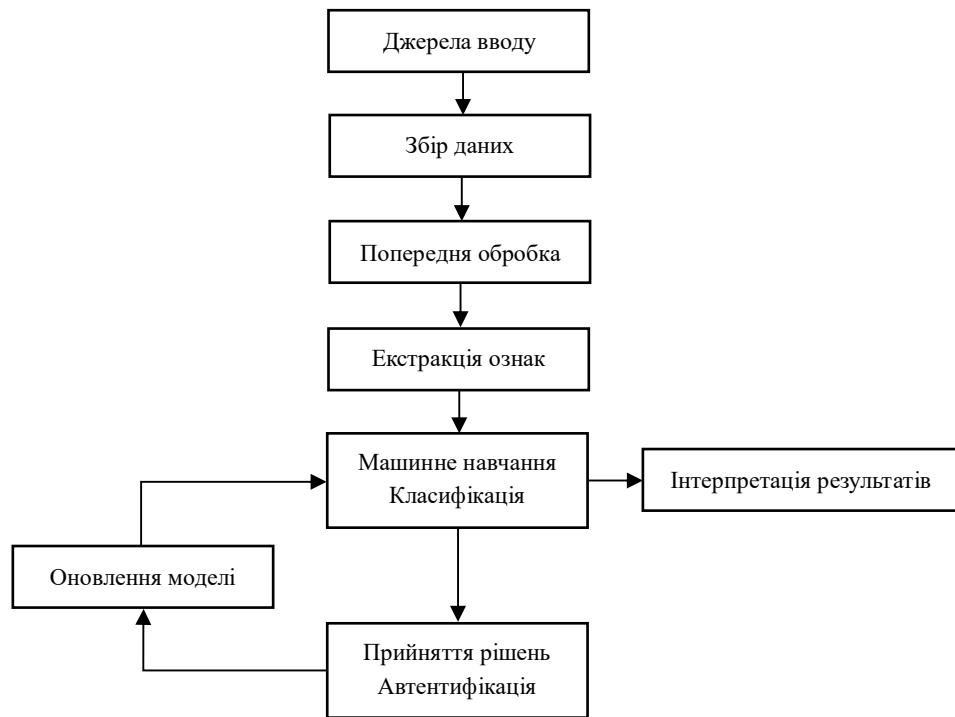


Рис. 1. Узагальнена архітектура систем аналізу клавіатурного почерку

Модуль попередньої обробки відповідає за нормалізацію часових вимірювань між різними системами, детекцію та обробку аномальних подій клавіатури, сегментацію безперервного набору на значущі фрагменти для аналізу, та оцінку якості зібраних даних. Критично важливим є врахування різних типів клавіатур, операційних систем та конфігурацій, які можуть впливати на темпоральні характеристики набору. Алгоритми нормалізації повинні компенсувати апаратні затримки та системні особливості для забезпечення кросплатформенної сумісності.

Механізм екстракції ознак включає генерацію користувацьких біометричних шаблонів, конструювання багатовимірних векторів ознак, застосування методів зменшення розмірності (PCA, LDA) та селекцію найбільш дискримінативних характеристик. Сучасні підходи використовують як традиційні статистичні методи, так і глибокі нейронні мережі для автоматичного виявлення латентних патернів у клавіатурних даних. Особливого значення набуває здатність системи адаптуватися до еволюції поведінкових патернів користувача протягом часу [5].

Система класифікації та співставлення реалізує різноманітні алгоритми машинного навчання, включаючи статистичні методи (гаусівські моделі сумішей, байєсівські класифікатори), методи на основі відстаней (евклідова, манхеттенська, махаланобіс), класичні алгоритми машинного навчання (SVM, Random Forest, Neural Networks) та сучасні архітектури глибокого навчання (LSTM, CNN, Transformer). Кожен з цих підходів має специфічні переваги та обмеження, що робить важливим вибір оптимального методу для конкретного застосування.

Модуль прийняття рішень забезпечує динамічне управління порогоми прийняття/відхилення, ймовірнісні рішення автентифікації на основі показників довіри, безперервну автентифікацію під час активного набору тексту та механізми адаптивного навчання для оновлення профілів користувачів. Особливої уваги потребує баланс між безпекою та зручністю використання, що досягається через інтелектуальне налаштування порогів на основі контексту та ризик-профілю конкретного користувача [6].

Методи штучного інтелекту в аналізі клавіатурного почерку. Інтеграція методів штучного інтелекту в системи аналізу клавіатурного почерку призвела до суттєвого покращення точності автентифікації та розширення можливостей інтерпретації

результатів. Контрольовані методи машинного навчання включають метод опорних векторів (SVM), який демонструє конкурентоспроможну продуктивність з мінімальною кількістю навчальних зразків (до 5 зразків на користувача) та показниками Equal Error Rate (EER) від 4.5% до 10.2%. Гаусівські моделі сумішей (GMM) ефективно обробляють негаусівські розподіли клавіатурних даних, особливо в конфігураціях GMM-UBM (Universal Background Model) [7].

Дерева рішень та Random Forest популярні завдяки їх інтерпретованості, непараметричній природі та толерантності до викидів. Методи на основі відстаней, такі як манхеттенська відстань, найближчі сусіди та підрахунок викидів (z-score), ідентифіковані як найефективніші детектори для виявлення злоумисників. Алгоритм k-найближчих сусідів (KNN) використовується як у контрольованому, так і неконтрольованому режимах для класифікації та детекції аномалій.

Неконтрольовані методи навчання включають алгоритми кластеризації, такі як k-means для групування користувачів та ідентифікації поведінкових патернів, k-medoids та нечіткий c-means для обробки неевклідових метрик та перекриваючих кластерних призначень. Ієрархічна кластеризація дозволяє виявляти групи користувачів зі схожими патернами набору без попередньо визначеної кількості кластерів. One-class SVM спеціально використовується для детекції викидів у клавіатурній динаміці, коли недоступні мічені дані злоумисників.

Архітектури глибокого навчання демонструють революційні результати в аналізі клавіатурного почерку. Рекурентні нейронні мережі, зокрема LSTM (Long Short-Term Memory), показують видатні результати: архітектура TypeNet досягає EER 2.2% для фізичних клавіатур та 9.2% для сенсорних екранів. Двонаправлені LSTM використовуються для захоплення як прямих, так і зворотних темпоральних залежностей у послідовностях клавіатурного вводу. GRU (Gated Recurrent Units) пропонують альтернативу LSTM з меншою кількістю параметрів, забезпечуючи швидше навчання при збереженні порівнянної продуктивності [8].

Згорткові нейронні мережі (CNN) застосовуються для аналізу клавіатурного почерку через перетворення темпоральних даних у зображеноподібні репрезентації, досягаючи EER до 4.5%. Одновимірні згортки застосовуються безпосередньо до темпоральних послідовностей клавіатурного вводу для екстракції ознак. Гібридні CNN-RNN архітектури поєднують згорткову екстракцію ознак з рекурентним моделюванням послідовностей.

Трансформерні архітектури представляють найновіші досягнення в галузі, включаючи TypeFormer як першу успішну адаптацію трансформерної архітектури для клавіатурної динаміки. Механізми self-attention дозволяють моделям фокусуватися на релевантних частинах послідовностей набору при прийнятті рішень про автентифікацію. Multi-head attention забезпечує паралельну обробку різних аспектів клавіатурних послідовностей, що веде до кращого розуміння довготривалих залежностей [9].

Ансамблеві методи та гібридні підходи демонструють синергетичні ефекти при поєднанні різних алгоритмів. Традиційні ансамблеві підходи включають Random Forest з бутстрап-семплуванням та ансамблі класифікаторів, що поєднують SVM, KNN та дерева рішень, досягаючи точності 95.65%. Буст-алгоритми, такі як AdaBoost та XGBoost, показують послідовне навчання з ваговою корекцією помилок та градієнтний бустинг з регуляризациєю відповідно. Табл. 1 містить порівняльний аналіз описаних методів штучного інтелекту.

Інтерпретація результатів штучного інтелекту в клавіатурному почерку. Пояснювальний штучний інтелект (Explainable AI) набуває критичного значення для систем біометричної автентифікації, оскільки користувачі та організації потребують розуміння логіки прийняття рішень системою. Градієнт-базовані методи включають карти сальєнтності для виділення важливих клавіатурних характеристик при прийнятті рішень про автентифікацію, Grad-CAM (Class Activation Mapping), адаптований для

аналізу клавіатурних послідовностей, та інтегровані градієнти як методи атрибуції для розуміння рішень моделі [10].

Таблиця 1.

Порівняльний аналіз методів штучного інтелекту для аналізу клавіатурного почерку

Метод	EER, %	Переваги	Недоліки	Область застосування
SVM	4.5-10.2	Мінімальна кількість навчальних зразків, стійкість до перенавчання	Чутливість до вибору ядра, складність інтерпретації	Статична автентифікація
Random Forest	5.0-8.5	Висока інтерпретованість, стійкість до викидів	Схильність до перенавчання на зашумлених даних	Аналіз важливості ознак
GMM	6.0-12.0	Ефективна обробка негаусівських розподілів	Чутливість до ініціалізації параметрів	Моделювання користувацьких профілів
LSTM	2.2-9.2	Захоплення довготривалих залежностей, адаптивність	Висока обчислювальна складність	Безперервна автентифікація
CNN	4.5-7.0	Автоматична екстракція ознак, стійкість до шуму	Втрата темпоральної інформації	Аналіз патернів набору
Transformer	1.8-5.5	Паралельна обробка, механізм уваги	Вимоги до великих наборів даних	Складні темпоральні залежності
Ансамблеві методи	3.0-6.0	Підвищена точність, стійкість	Збільшена обчислювальна складність	Критичні системи

Модель-агностичні методи включають LIME (Local Interpretable Model-agnostic Explanations) для локальних пояснень рішень щодо клавіатурних патернів, SHAP (SHapley Additive ExPlanations) для важливості ознак у патернах набору, та пермутаційну важливість для розуміння внеску ознак через контрольовані збурення. Ці методи дозволяють аналізувати, які саме аспекти клавіатурного почерку найбільше впливають на рішення про автентифікацію.

Візуалізація уваги стає особливо важливою для трансформерних архітектур, де теплові карти уваги показують, які частини клавіатурних послідовностей отримують найвищу увагу. Аналіз голів дозволяє зрозуміти патерни фокусування різних голів уваги, а темпоральні патерни уваги аналізують, як моделі зважують різні часові сегменти набору тексту.

Упередженість та етичні аспекти потребують систематичного аналізу. Метрики справедливості, такі як Skewed Impostor Ratio (SIR), використовуються для оцінки міжгрупової та внутрішньогрупової упередженості. Демографічний аналіз показує вплив статі, віку та домінуючої руки на клавіатурну автентифікацію. Мовно-специфічна упередженість виявляється при аналізі багатомовних клавіатурних патернів, де перехід між мовами може суттєво знижувати точність автентифікації [11].

Практичні виклики інтерпретації включають проблему "чорної скриньки" глибоких моделей навчання, особливо LSTM та CNN архітектур, які часто не мають інтерпретованості. Існує компроміс між продуктивністю моделі та її поясненістю, що потребує застосування post-hoc методів пояснення. Доменно-специфічні вимоги включають пояснення невдач автентифікації без розкриття вразливостей безпеки, надання зрозумілого зворотного зв'язку користувачам щодо змін у поведінці набору, та дотримання регуляторних вимог щодо поясненості біометричних систем.

Сучасні застосування та реалізації систем клавіатурного почерку. Комерційні та корпоративні системи автентифікації демонструють зрілість технології клавіатурного почерку та її готовність до широкого впровадження. Plurilock Security Inc. є провідним

комерційним постачальником з контрактами від Міністерства оборони США, здатним ідентифікувати користувачів протягом 3 секунд та 12 натискань клавіш. Компанія забезпечила контракти на \$1.3 мільйона у 2025 році серед американських комерційних клієнтів, надаючи безперервну автентифікацію через поведінкові біометрики та машинне навчання з реальними впровадженнями в лікарняних системах та корпоративних клієнтах [12].

BehavioSec, придбана LexisNexis у 2022 році, зосереджується на поведінкових біометриках для виявлення шахрайства та запобігання захопленню облікових записів, маючи сильні позиції в європейському банківському секторі з впровадженням серед мільйонів користувачів банківських додатків. TuringDNA пропонує API для біометрики набору тексту для розробників, партнерства з рішеннями управління ідентичністю для інтеграції MFA, фокусуючись на електронному навчанні та запобіганні шахрайству.

Інтеграція з багатофакторною автентифікацією демонструє суттєві переваги зменшення тертя, знижуючи вимоги OTP на 66.3% при вході та 85.8% при відновленні облікового запису, зменшуючи час автентифікації на 63.3% для входу та 78.9% для відновлення облікового запису. Користувачі віддають перевагу клавіатурній динаміці + OTP над автентифікацією лише OTP. Ризик-орієнтована автентифікація функціонує як адаптивний рівень автентифікації, підвищуючи показники ризику при відхиленні патернів набору від базової лінії та запускаючи додаткову автентифікацію при перевищенні порогів ризику [13].

Реальні сценарії впровадження охоплюють фінансові послуги для виявлення шахрайства під час процесів входу та транзакцій, запобігання захопленню облікових записів, дотримання вимог сильної автентифікації клієнтів та підвищення безпеки онлайн-банкінгу. У сфері охорони здоров'я системи використовуються для багатофакторної автентифікації в системах DHIMS 2, безперервної автентифікації медичних працівників, поєднання з біометрикою відбитків пальців для підвищеної безпеки та дотримання вимог HIPAA.

Урядові та оборонні застосування включають впровадження Міністерства оборони США, захист критичної інфраструктури, виявлення та пом'якшення внутрішніх загроз, безперервний моніторинг доступу привілейованих користувачів. В освітній сфері системи застосовуються для верифікації особи студентів на онлайн-іспитах, забезпечення академічної чесності, запобігання шахрайству в середовищах дистанційного навчання та приватної автентифікації для освітніх платформ [14].

Показники продуктивності комерційних систем як-от BehavioSec заявляють EER 0.10-0.20, інші системи повідомляють про показники точності близько 88%. Найкращі системи досягають точності понад 95% для ідентифікації користувачів, а моделі глибокого навчання показують до 82% точності для завдань ідентифікації. Фактори продуктивності включають статичну автентифікацію, придатну для верифікації входу, динамічну автентифікацію, кращу для безперервного моніторингу, мультимодальні підходи з вищою точністю при поєднанні з іншими біометриками, та якість набору даних, де продуктивність значно варіюється залежно від методів збору даних.

Майбутні напрямки досліджень. Інтеграція гіроскопів та акселерометрів з аналізом клавіатурного почерку представляє революційний напрямок розвитку мобільних біометричних систем. Останні дослідження 2025 року демонструють, що системи клавіатурної динаміки на основі сенсорів смартфонів можуть досягати EER до 6.4% при поєднанні даних акселерометра та гіроскопа з патернами клавіатурного вводу. Інтеграція даних датчиків руху знижує помилки автентифікації приблизно на 1-2% порівняно з підходами лише на основі клавіш [15].

Рух пристрою під час набору може створювати унікальні "підписи руху", які доповнюють класичні патерни клавіатурного вводу. LSTM-базовані підходи, що поєднують дані акселерометра та гіроскопа, виявляють особливий інтерес для дослідження.

Аналіз поведінки набору на сенсорному екрані порівняно з традиційною клавіатурною динамікою виявляє фундаментальні відмінності. Фізичні відмінності включають нижчі сили набору на віртуальних клавіатурах, знижену продуктивність набору порівняно з фізичними клавіатурами, вищий суб'єктивний дискомфорт у областях рук/зап'ясть та шия/плечі, різні патерни активації м'язів у згиначах та розгиначах пальців.

Аналіз орієнтації мобільного пристрою та патернів руху включає багатопозиційні моделі автентифікації, які враховують набір у сидячому положенні (найстабільніші патерни), набір під час ходьби/мобільний набір (підвищена варіабельність, що потребує адаптивних порогів) та набір у розслабленому положенні (проміжні характеристики стабільності).

Виклики збору та аналізу мобільної клавіатурної динаміки включають обмеження збору даних з обмеженнями ОС Android щодо збору фонових даних без власних реалізацій, вимоги до користувацьких клавіатур з обмеженнями доступу третіх сторін, що потребують спеціалізованих методів вводу, проблеми приватності користувачів з балансуванням безпеки з вимогами захисту даних, варіацією між пристроями з різними виробниками та розмірами екранів, що впливають на стабільність патернів. Технічні виклики охоплюють обмежені обчислювальні ресурси на мобільних платформах, оптимізацію використання батареї для безперервного моніторингу, варіації мережевого підключення, що впливають на хмарну обробку, гетерогенність апаратного забезпечення між виробниками та моделями пристроїв [16].

Виклики та перспективи розвитку. Сучасні системи аналізу клавіатурного почерку стикаються з рядом технічних та концептуальних викликів, які визначають напрямки майбутніх досліджень. Поведінкова варіабельність залишається фундаментальною проблемою, оскільки патерни набору тексту піддаються впливу втоми, настрою, фізичних станів, емоційного стану та навчальних ефектів. Ефект адаптації користувача протягом часу потребує постійного оновлення моделей, що створює компроміс між стабільністю системи та здатністю до адаптації. Залежність від пристрою проявляється у варіаціях продуктивності між різними клавіатурами, пристроями та операційними системами, що ускладнює створення універсальних біометричних профілів.

Питання масштабованості стають критичними при впровадженні систем у великих організаціях, де деградація продуктивності з ростом кількості користувачів потребує ефективних алгоритмічних рішень та оптимізації інфраструктури. Вразливості безпеки включають потенціал для replay-атак, загрози кейлогерів у скомпрометованих середовищах, потенційну витоку поведінкових даних та необхідність детекції "живості" для забезпечення людського оператора замість автоматизованого вводу [17].

Етичні та регуляторні аспекти набувають зростаючого значення з розвитком законодавства про захист персональних даних. Дотримання GDPR вимагає мінімізації даних, прозорості та права на видалення, що може конфліктувати з потребами накопичення даних для покращення точності моделей. Потенційна упередженість проти користувачів з інвалідністю потребує інклюзивного дизайну систем, а прозоре розкриття моніторингу та справедливий дизайн системи є обов'язковими для етичного впровадження.

Розширення Інтернету речей передбачає кросплатформну автентифікацію з синхронізацією клавіатурних патернів між множинними пристроями, інтеграцію розумного дому з клавіатурною поведінкою як частиною ширших поведінкових профілів, злиття з пристроями що носяться з інтеграцією даних смарт-годинників та фітнес-трекерів.

Особливо перспективний напрямок для систем клавіатурного почерку представляють федеративне навчання [18] та граничні обчислення, дозволяючи навчання моделей без централізованого збору чутливих біометричних даних.

Висновки. Системи аналізу клавіатурного почерку для автентифікації користувачів пройшли шлях від експериментальних досліджень до зрілих комерційних рішень, які

демонструють високу ефективність у реальних умовах впровадження. Інтеграція методів штучного інтелекту, зокрема глибокого навчання та трансформерних архітектур, суттєво покращила точність автентифікації, з сучасними системами, що досягають EER нижче 5% в оптимальних умовах. Особливого значення набуває здатність до безперервної автентифікації та інтеграції з багатофакторними системами безпеки. Викликає інтерес інтеграція сенсорів мобільних пристроїв, зокрема гіроскопів та акселерометрів для підвищення точності мультимодальних біометричних систем. Методи інтерпретації результатів штучного інтелекту стають критично важливими для забезпечення довіри користувачів та дотримання регуляторних вимог. Розвиток пояснювального ШІ дозволяє створювати прозорі та зрозумілі системи автентифікації, що особливо важливо для критичних застосувань у фінансовій, медичній та урядовій сферах. Майбутні дослідження фокусуються на подоланні існуючих викликів варіабельності поведінки, кросплатформної сумісності та масштабованості через розвиток адаптивних алгоритмів та федеративного навчання. Успіх технології клавіатурного почерку визначається балансом між безпекою, зручністю використання та приватністю, що досягається через інтелектуальне поєднання традиційних статистичних методів з сучасними архітектурами штучного інтелекту та всеосяжним підходом до інтерпретації результатів аналізу.

Список літератури

1. Al-Khafajiy M., et al. Biometric-Based Identity Management Framework for Personalised IoT and Cloud Computing-Based Healthcare Services. *Applied Sciences*. 2021. Vol. 11, № 4. Article 1642. DOI: <https://doi.org/10.3390/app11041642>
2. BIOSIG 2022 Conference Proceedings: 21st International Conference of the Biometrics Special Interest Group. Darmstadt, Germany, September 14-16, 2022. IEEE, 2022. DOI: <https://doi.org/10.1109/BIOSIG55365.2022>
3. BIOSIG 2023 Conference Proceedings: 22nd International Conference of the Biometrics Special Interest Group. Darmstadt, Germany, September 20-22, 2023. LNI P-339. IEEE, 2023. DOI: <https://doi.org/10.1109/BIOSIG58226.2023>
4. Buriro A., Luccio F. Mobile Biometrics: Innovations, Challenges, and Emerging Trends. *Advanced Information Networking and Applications*. AINA 2025. Lecture Notes on Data Engineering and Communications Technologies. 2025. Vol. 252. DOI: <https://doi.org/10.1007/978-3-031-57916-5>
5. A. Rahman et al., Multimodal EEG and Keystroke Dynamics Based Biometric System Using Machine Learning Algorithms. *IEEE Access*. 2021. Vol. 9, P. 94625-94643, <https://doi.org/10.1109/ACCESS.2021.3092840>
6. Korchenko O., Tereikovskiy I., Ziubina R., Tereikovska L., Korystin O., Tereikovskiy O., Karpinskiy V. Modular Neural Network Model for Biometric Authentication of Personnel in Critical Infrastructure Facilities Based on Facial Images. *Applied Sciences*. 2025. Vol. 15, № 5. Article 2553. DOI: <https://doi.org/10.3390/app15052553>
7. Mhenni A., Cherrier E., Rosenberger C., Essoukri Ben Amara N. Double serial adaptation mechanism for keystroke dynamics authentication based on a single password. *Computers & Security*. 2019. Vol. 83. P. 151–166. DOI: <https://doi.org/10.1016/j.cose.2019.02.002>
8. Migdal D., Rosenberger C. Statistical modeling of keystroke dynamics samples for the generation of synthetic datasets. *Future Generation Computer Systems*. 2019. Vol. 100. P. 907–920. DOI: <https://doi.org/10.1016/j.future.2019.04.045>
9. Monroe F., Rubin A. D. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*. 2000. Vol. 16, № 4. P. 351–359. DOI: [https://doi.org/10.1016/S0167-739X\(99\)00059-X](https://doi.org/10.1016/S0167-739X(99)00059-X)
10. Muratuly D., Denissova N., Krak Y., Apayev K. Biometric Authentication of Students to Control the Learning Process in Online Education. *Scientific Journal of Astana IT University*. 2022. Vol. 10, № 10. DOI: <http://dx.doi.org/10.37943/LYFW8581>

11. Pisani P. H., Lorena A. C. A systematic review on keystroke dynamics. *Journal of the Brazilian Computer Society*. 2013. Vol. 19, № 4. P. 573–587. DOI: <https://doi.org/10.1007/s13173-013-0117-7>
12. Rahman A., et al. Multimodal EEG and keystroke dynamics based biometric system using machine learning algorithms. *IEEE Access*. 2021. Vol. 9. P. 94625–94643. DOI: <https://doi.org/10.1109/ACCESS.2021.3092840>
13. Rahmani K., Babaie S. A. A lightweight biometric-assisted authentication approach for internet of things. *Peer-to-Peer Networking and Applications*. 2025. Vol. 18. Article 195. DOI: <https://doi.org/10.1007/s12083-025-02006-8>.
14. Roy S., Roy U., Sinha D. D. Systematic Literature Review on Latest Keystroke Dynamics Based Models. *IEEE Access*. 2022. Vol. 10. P. 93569–93599. DOI: <https://doi.org/10.1109/ACCESS.2022.3197756>
15. Sulavko A., Panfilova I., Inivatov D., Lozhnikov P., Vulfin A., Samotuga A. Biometric-Based Key Generation and User Authentication Using Voice Password Images and Neural Fuzzy Extractor. *Applied System Innovation*. 2025. Vol. 8, № 1. Article 13. DOI: <https://doi.org/10.3390/asi8010013>
16. Teh P. S., Teoh A. B. J., Yue S. A survey of keystroke dynamics biometrics. *The Scientific World Journal*. 2013. Article ID 408280. 24 p. DOI: <https://doi.org/10.1155/2013/408280>
17. Tereikovskiy I., Tereikovska L., Korystin O., Mussiraliyeva S., Sambetbayeva A. User Keystroke Authentication and Recognition of Emotions Based on Convolutional Neural Network. *Advances in Artificial Systems for Medicine and Education III. AIMEE 2019. Advances in Intelligent Systems and Computing*. 2020. Vol. 1126. P. 26–35. DOI: https://doi.org/10.1007/978-3-030-39162-1_3
18. Євтушенко С.В. Про перспективи федеративного навчання для систем автентифікації на основі аналізу клавіатурного почерку. *LVIII Міжнародна науково-практична конференція "Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку"*, м. Ловеч (Болгарія). 2025. С. 173–177

С.В. Євтушенко

**ASPECTS OF CONSTRUCTION AND APPLICATION OF KEYSTROKE
DYNAMICS ANALYSIS SYSTEMS FOR USER AUTHENTICATION**

S. V. Yevtushenko

National University "Odesa Law Academy"

2, Academic St., Odesa, 65000, Ukraine

Email: serhiyevtushenko@gmail.com

The subject of the article is keystroke dynamics analysis systems for user authentication using artificial intelligence methods and their integration with mobile device sensors. The purpose of the work is to analyze aspects of building and applying keystroke dynamics analysis systems for user authentication using artificial intelligence methods and to study the prospects for their development for creating multimodal biometric systems. The article solves the following tasks: forming a model of the architecture of multilevel keystroke dynamics systems; systematizing artificial intelligence methods for analyzing temporal patterns of text typing; analyzing approaches to integrating gyroscopes and accelerometers of mobile devices to create multimodal biometric systems; studying methods for interpreting the results of deep learning models in the context of biometric authentication. The following methods are used: mathematical processing of temporal sequences of keyboard input; deep learning with LSTM, CNN, and Transformer architectures; statistical analysis of behavioral patterns; machine learning with supervised and unsupervised algorithms; ensemble approaches to improve classification accuracy. The following results were obtained: the principles of building a multi-level architecture of keystroke dynamics systems were formulated; artificial intelligence methods for analyzing biometric characteristics of typing were systematized; modern commercial implementations with EER indicators of 0.10-0.20% for leading systems were analyzed; the prospects for integrating mobile device sensors to achieve EER up to 6.4% in multimodal systems were investigated. Conclusions: the use of the method of combining keystroke dynamics with gyroscope and accelerometer data allows creating high-precision continuous authentication systems with increased resistance to imitation attacks and the ability to adapt to the evolution of user behavioral patterns.

Keywords: keystroke dynamics; biometric authentication; artificial intelligence; deep learning; multimodal systems.