DOI: https://doi.org/10.36910/6775-2524-0560-2025-61-41
УДК:004.056.53
Бутенко Лев Ігорович, аспірант
https://orcid.org/0009-0000-8428-7990
Шарадкін Дмитро Михайлович, к.т.н., доцент
https://orcid.org/0000-0001-6407-8040
Інститут спеціального зв'язку та захисту інформації, м. Київ, Україна

БЕЗПЕРЕРВНА БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ КОРИСТУВАЧІВ НА ОСНОВІ КЛАВІАТУРНОГО ПОЧЕРКУ

Бутенко Л. І., Шарадкін Д. М. Безперервна біометрична автентифікація користувачів на основі клавіатурного почерку. У статті розглянуто сучасні підходи до біометричної автентифікації користувачів, із фокусом на поведінкові методи, зокрема клавіатурний почерк (Keystroke Dynamics, KD). Описано переваги та обмеження фізіологічної та поведінкової біометрії, обґрунтовано доцільність використання клавіатурного почерку як засобу безперервної автентифікації у фоновому режимі. Здійснено аналіз класичних і сучасних досліджень у цій сфері, включно з роботами, що застосовують ансамблеві алгоритми та методи глибокого навчання. Запропоновано модульну архітектуру системи безперервної автентифікації, яка поєднує збір та обробку даних, класифікацію та адаптивне оновлення профілю користувача. Розглянуто ключові метрики оцінки точності (FAR, FRR, EER, TTD) та можливість інтеграції клавіатурного почерку з іншими факторами автентифікації у багатофакторних системах. Аналіз клавіатурного почерку дозволяє підвищити рівень безпеки інформаційних систем без погіршення зручності для користувача, з потенційним застосуванням у військових, фінансових та корпоративних середовищах.
Ключові слова: фізіологічна біометрія, поведінкова біометрія, клавіатурний почерк.

Butenko L., Sharadkin D. Continuous Biometric User Authentication Based on Keystroke Dynamics. The article examines modern approaches to biometric user authentication, focusing on behavioral methods, particularly keystroke dynamics (Keystroke Dynamics, KD). It outlines the advantages and limitations of physiological and behavioral biometrics and substantiates the feasibility of using keystroke dynamics as a means of continuous background authentication. The study includes an analysis of both classical and recent research in this field, including works employing ensemble algorithms and deep learning techniques. A modular architecture of a continuous authentication system is proposed, integrating data collection and processing, classification, and adaptive user profile updating. Key accuracy metrics (FAR, FRR, EER, TTD) are discussed, as well as the potential integration of keystroke dynamics with other authentication factors in multi-factor systems. The analysis of keystroke dynamics enhances the security level of information systems without compromising user convenience and offers potential applications in military, financial, and corporate environments.
Keywords: physiological biometrics, behavioral biometrics, keystroke dynamics.

Постановка проблеми. Сучасні інформаційні системи стикаються з необхідністю забезпечення надійної та зручної автентифікації користувачів у середовищі, де традиційні методи захисту – паролі, PIN-коди, токени – дедалі частіше виявляються недостатньо ефективними. Паролі можуть бути вкрадені, підглянуті або зламані, а фізичні носії – втрачені чи скомпрометовані. У зв'язку з цим усе більшої уваги набувають біометричні технології, здатні ідентифікувати особу за унікальними характеристиками, які складно підробити чи передати третім особам.

Одним із найбільш перспективних напрямів у цій галузі є поведінкова біометрія, зокрема автентифікація на основі клавіатурного почерку. Механізм автентифікації на основі клавіатурного почерку ґрунтується на вивченні темпу та ритму друку, що є унікальними для кожного користувача. На відміну від фізіологічних біометричних систем (наприклад, відбитків пальців чи розпізнавання обличчя), він не потребує спеціального обладнання та може функціонувати у звичайному середовищі введення тексту – під час роботи з клавіатурою, терміналом чи мобільним пристроєм. Завдяки цьому метод є економічно ефективним, ненав'язливим та придатним для широкого впровадження.

Стандартні біометричні процедури автентифікації – як фізіологічні, так і поведінкові – здебільшого виконуються лише на початку сесії, після чого система не має змоги перевіряти, чи користувач залишається тим самим. Це створює критичну вразливість: навіть якщо початковий вхід був здійснений легітимною особою, зловмисник може перехопити активну сесію без необхідності повторної перевірки. Для усунення цього недоліку пропонується підхід безперервної автентифікації, який полягає у постійному

моніторингу поведінкових параметрів користувача протягом усього сеансу роботи. Зокрема, аналіз клавіатурного почерку є оптимальним джерелом таких даних, адже користувач природним чином вводить текст під час взаємодії з системою, що дозволяє системі безперервно підтверджувати його особу у фоновому режимі, без додаткових дій чи переривання робочого процесу.

Проблема полягає у тому, що існуючі системи на основі клавіатурного почерку мають низку обмежень – вони часто не враховують динамічні зміни у поведінці користувача (втома, зміна пристрою, емоційний стан), недостатньо оптимізовані для реального часу та можуть генерувати значну кількість хибних відхилень (False Rejections). Потребує подальшого дослідження питання стійкості алгоритмів до варіативності поведінкових ознак, а також адаптивного оновлення профілю користувача.

Таким чином, актуальність дослідження полягає у необхідності розроблення та вдосконалення методів і архітектур безперервної автентифікації на основі клавіатурного почерку, що поєднують високу точність, адаптивність до змін поведінки користувача та здатність до роботи у реальному часі. Розв'язання цієї проблеми є важливим як для цивільних, так і для спеціалізованих (зокрема, військових) систем, де збереження цілісності доступу має критичне значення.

Мета статті. Метою даного дослідження є здійснення комплексного аналізу сучасних методів біометричної автентифікації користувачів, зокрема в першу чергу заснованих на клавіатурному почерку, та обґрунтування доцільності застосування даного підходу для реалізації безперервної автентифікації у фоновому режимі. Дослідження спрямоване на узагальнення наявних рішень, виявлення їх переваг і недоліків, а також на розроблення теоретичних передумов впровадження систем безперервної поведінкової ідентифікації користувачів за динамікою натискань клавіш.

Аналіз досліджень і публікацій. Дослідження у сфері ідентифікації користувачів за клавіатурним почерком активно розвиваються з 1980-х років і нині є одним із найперспективніших напрямів поведінкової біометрії.

Однією з перших ґрунтовних робіт у цій галузі стала праця Джойса та Гупти[1], у якій автори запропонували метод аутентифікації користувачів на основі часових затримок між натисканнями клавіш під час введення логіна. Вони дослідили, що кожна людина має унікальний «ритм» набору тексту, який може виступати біометричним ідентифікатором. Методика передбачала фіксацію часу між натисканням і відпусканням клавіш, а також інтервалів між окремими натисканнями. Ці параметри формували індивідуальний профіль користувача. Попри відсутність точних показників достовірності, робота започаткувала новий підхід у поведінковій біометрії, який не потребує спеціального обладнання.

Значного розвитку цей напрям отримав завдяки дослідженням Монроуза та Рубіна[2]. Вони провели масштабний експеримент із 63 користувачами, під час якого фіксували характеристики набору тексту на комп'ютерній клавіатурі – зокрема час натискання, час утримання та паузи між клавішами. Автори порівняли ефективність різних класифікаторів – евклідового, ймовірнісного та байєсівського – і показали, що точність ідентифікації може досягати 92% . Вони також встановили, що використання фіксованого тексту (однакових фраз під час навчання та перевірки) забезпечує вищу точність порівняно зі «вільним текстом», який залежить від емоційного стану й контексту користувача. Дослідження Монроуза та Рубіна стало одним із перших, що продемонструвало практичну придатність клавіатурного почерку для біометричної аутентифікації.

У сучасних дослідженнях спостерігається тенденція до використання методів штучного інтелекту та глибокого навчання для підвищення точності систем автентифікації. Сюань Ван та Дунь Хоу[3] запропонували підхід, заснований на ансамблевому навчанні – методиці, за якої кілька алгоритмів класифікації об'єднуються для прийняття спільного

рішення. В порівнянні з використанням одного класифікуючого методу, ансамбль дозволяє враховувати сильні сторони кожного з алгоритмів та компенсувати їхні недоліки.

У своїй роботі автори використали поєднання трьох моделей:

- Random Forest (випадковий ліс) – алгоритм, що створює велику кількість незалежних «дерев рішень» і визначає підсумковий результат шляхом голосування між ними. Такий підхід зменшує ризик перенавчання та підвищує стійкість до шумових даних.
- Gradient Boosting (градієнтне підсилення) – метод, у якому моделі будуються послідовно, кожна наступна виправляє помилки попередньої, що дозволяє поступово підвищувати точність класифікації.
- XGBoost (екстремальне градієнтне підсилення) – оптимізована версія попереднього методу, яка використовує регуляризацію, паралельні обчислення та ефективне керування пам'яттю для прискорення навчання та зменшення похибок.

Комбінація цих моделей дозволила системі ефективно розрізняти користувачів навіть за умови варіативності їхньої поведінки при наборі тексту. Щоб збалансувати кількість даних між користувачами, дослідники використали метод SMOTE (Synthetic Minority Oversampling Technique) – він штучно створює додаткові приклади для тих груп, які мають менше зразків. Завдяки цьому вибірка стає більш збалансованою, а кількість помилок розпізнавання зменшується.

Дослідники Алі, Рахман, Хасан[4] та їхні колеги зосередили увагу на використанні глибоких нейронних мереж у задачах поведінкової аутентифікації. Вони порівняли ефективність згорткових (CNN), рекурентних (RNN) та гібридних моделей і з'ясували, що глибокі архітектури краще моделюють часові закономірності набору тексту та взаємозв'язки між послідовностями натискань клавіш. Гібридна модель CNN-RNN показала найвищі результати, демонструючи стабільну точність навіть при коротких фрагментах введення текстів. Автори дійшли висновку, що методи глибокого навчання здатні відображати складні патерни поведінки користувачів і забезпечувати підвищену стійкість систем до змін звичок користувача при наборі тексту.

Сучасний підхід запропонував Вицишлік[5], який розробив вдосконалену архітектуру глибокого навчання для біометричної ідентифікації за клавіатурним почерком. Його модель використовує багаторівневу нейронну мережу з оптимізованою функцією втрат, що дозволяє ефективніше розрізняти користувачів із подібними патернами набору. Під час тестування на відкритих наборах даних (зокрема CMU та GREYC) точність ідентифікації перевищила 95 %, що свідчить про потенціал методів deep learning у створенні масштабованих, високоточних систем біометричної автентифікації.

Окремий напрям формують дослідження, засновані на архітектурах TypeNet, які створені спеціально для обробки часових та структурних патернів клавіатурного почерку. У роботі Асьєн та співавторів [6] запропоновано першу версію TypeNet – глибинної нейронної мережі, оптимізованої для моделювання ритмічних характеристик набору тексту. Модель здатна аналізувати як локальні, так і довготривалі залежності між подіями введення, що підвищує точність автентифікації. Подальший розвиток цієї архітектури представлено у дослідженні TypeNet: Scaling Up Keystroke Biometrics [7], де автори адаптували модель для роботи з великими вибірками та підвищеною вимогливістю до обчислювальних ресурсів.

Підхід до комбінування рекурентних нейронних мереж з ансамблевими методами розглянуто у дослідженні Кіяні та співавторів [8]. У роботі запропоновано рекурентну модель із механізмом довіри, яка оцінює послідовності натискань у реальному часі, що дозволяє точніше враховувати часовий контекст під час безперервної автентифікації у вільному тексті.

Методи на основі згорткових нейронних мереж для безперервної автентифікації детально розкрито у роботі Сяофена Лу та співавторів [9]. У дослідженні показано, що

згорткові нейронні мережі здатні ефективно виділяти характерні патерни друку завдяки своїй здатності автоматично знаходити локальні закономірності у часових послідовностях. Згорткові нейронні мережі виконують послідовну обробку даних через згорткові фільтри, що дозволяє моделі виявляти стійкі поведінкові ознаки, які повторюються у процесі введення тексту. Автор наголошує, що згорткові архітектури успішно працюють навіть без попередньої сегментації введення на окремі слова чи фрази, що робить їх придатними для аналізу повністю вільного тексту.

Систематичний огляд викликів безперервної автентифікації подано в статті Байга та Ескеланда (Sensors, 2021) [10], де розглядаються ключові проблеми точності, приватності та зручності використання поведінкових біометричних систем. Автори підкреслюють, що безперервна автентифікація потребує балансу між надійністю та непомітністю роботи, а також захисту конфіденційних даних, які збираються у режимі реального часу.

У більш загальному контексті історію та розвиток клавіатурної біометрії узагальнено в огляді Пін Шен Теха, Ендрю Бен Джин Тео та Шиган Юе [11], який залишається одним із ключових фундаментальних матеріалів у галузі. У цьому огляді систематизовано основні підходи до моделювання динаміки натискань, наведено класифікацію методів за типами ознак, описано еволюцію від ранніх статистичних моделей до сучасних нейромережевих архітектур. Робота містить ґрунтовний аналіз переваг та недоліків різних технік, що робить її важливою теоретичною базою для подальших досліджень і практичних розробок у сфері поведінкової автентифікації.

На важливість мовних факторів у процесі автентифікації звертає увагу дослідження Алтвайджрі [12], у якому показано, що стиль набору помітно змінюється залежно від мови введення. У роботі зазначено, що перехід між мовами впливає на тривалість інтервалів між натисканнями, частоту використання службових клавіш та загальну ритміку друку. Тому моделі, навчені на одному мовному контексті, можуть втрачати точність у багатомовних системах, що вимагає адаптивних або мультимовних підходів.

Можливості прихованого моніторингу поведінки користувача детально розглянуто в дослідженні Кочегурова та Затеєва (2022) [13]. У роботі доведено, що клавіатурний почерк може використовуватися не лише для ідентифікації, а й для непомітного відстеження зміни користувача у фоновому режимі. Це дозволяє системі фіксувати потенційно небезпечні відхилення без повторного запиту автентифікації, що є важливим у середовищах, де необхідна постійна контрольована робота.

Огляд сучасних прикладних рішень подано у дослідженні Садікан, Рамлі та Фудзі [14], де узагальнено основні підходи до використання клавіатурної біометрії у практичних системах. У роботі зазначено, що автентифікація може здійснюватися як у режимі фіксованого тексту, так і у вільному введенні, що розширює можливості її застосування. Також проаналізовано переваги статистичних моделей і глибинних мереж, звернено увагу на важливість вибору інформативних ознак та здатність алгоритмів працювати у реальному часі. У роботі запропоновано класифікацію наявних методів та окреслено фактори, що впливають на їх точність і стабільність, що робить це дослідження корисною теоретичною основою для побудови сучасних систем автентифікації.

Класичні моделі автентифікації через динаміку набору тексту описано в матеріалі Монроуза та співавторів [15], де розглядаються базові характеристики, такі як час утримання клавіш та інтервали між натисканнями. Ця робота стала однією з фундаментальних у галузі й визначила основні підходи до побудови перших систем на основі клавіатурного почерку.

Розширені можливості сімейства TypeNet подано у статті Баха та Алуфі [16]. У ній автори вдосконалили архітектуру оригінальної моделі, підвищивши її здатність виділяти інформативні ознаки у довгих послідовностях та забезпечивши стабільніші результати на

великих масивах даних. Таке вдосконалення робить TypeNet одним із найбільш перспективних рішень для масштабованих систем безперервної автентифікації.

Перспективним напрямом розвитку є поєднання клавіатурної біометрії з додатковими сенсорними сигналами. У роботі Сенератха та співавторів [17] продемонстровано, що використання даних інерційних сенсорів смартфона – зокрема акселерометра та гіроскопа, які фіксують мікрорухи та положення пристрою у просторі – дозволяє точніше аналізувати поведінкові особливості користувача під час введення тексту. Такий підхід значно підвищує стійкість системи до змін стилю друку та формує новий клас багатомодальних моделей, здатних працювати у складних і мінливих сценаріях.

Виклад основного матеріалу.

Фізіологічні та поведінкові підходи у біометричній автентифікації.

Біометрична автентифікація розглядається як перспективна альтернатива традиційним методам захисту, таким як паролі та токени, оскільки вона ґрунтується на унікальних фізіологічних або поведінкових характеристиках людини (відбитки пальців, геометрія обличчя, райдужка ока, голос тощо), що забезпечує високий рівень достовірності ідентифікації. Основними перевагами біометричних систем є підвищена безпека, зручність для користувача та відсутність потреби у зберіганні зовнішніх ключів. Одночасно їх застосування супроводжується значними обмеженнями, зокрема високими вимогами до апаратного забезпечення, потенційними ризиками витоку біометричних даних та нормативно-правовими обмеженнями щодо їх обробки та зберігання.

Біометричні методи поділяються на фізіологічні та поведінкові. Фізіологічні методи (відбитки пальців, райдужка та сітківка ока, геометрія долоні тощо) базуються на відносно стабільних анатомічних ознаках, що забезпечує високу точність ідентифікації, проте їх застосування часто потребує спеціалізованого обладнання та є чутливим до умов зчитування. Поведінкові методи (клавіатурний почерк, рукопис, траєкторії руху миші, жести на сенсорних пристроях) оцінюють унікальні патерни поведінки користувача. Існує припущення, що такі методи можуть бути застосовані для безперервного моніторингу під час сеансу, однак їх ефективність у цьому контексті потребує подальших досліджень.

Кожна категорія методів має специфічні переваги та обмеження: фізіологічні методи забезпечують високу точність, але можуть бути вразливими до неякісних зчитувань або підробок, тоді як поведінкові методи менш інвазивні і потенційно придатні для фонового моніторингу, проте їхня надійність залежить від варіативності поведінкових патернів користувача [18]. Для підвищення стійкості систем часто застосовують комбіновані підходи, які поєднують біометричні ознаки з традиційними методами автентифікації.

Клавіатурний почерк як поведінкова біометрична ознака. Клавіатурний почерк відображає унікальні поведінкові патерни користувача під час набору тексту. До основних характеристик належать час утримання клавіш (dwell time), інтервали між натисканнями (flight time) та характерні послідовності натискань (які можуть включати як окремі натискання клавіш, так і комбінації з двох або трьох клавіш, натиснутих одночасно), які разом формують унікальний профіль користувача [19]. На відміну від фізіологічних методів, клавіатурний почерк не потребує спеціального обладнання і може застосовуватися для непомітної, фонової автентифікації під час роботи користувача. Ця особливість робить метод перспективним для захисту систем, де одноразової перевірки (логін і пароль) недостатньо.

Окрім основних часових характеристик, у процесі аналізу враховуються додаткові поведінкові ознаки, такі як варіативність ритму набору, стабільність швидкості друку чи характерні послідовності натискань. Дослідження Зеленського [25] також демонструє, що включення таких параметрів, як сила натиску на клавіші, може суттєво підвищувати точність ідентифікації користувача. Ці показники відображають не лише технічні навички користувача, а й можуть свідчити про його фізичний або емоційний стан [20]. Залучення

такого спектра параметрів підвищує точність і надійність системи, забезпечуючи її стійкість до змін у поведінці користувача.

Важливою перевагою клавіатурного почерку є ненав'язливість. Автентифікація відбувається у природний спосіб – під час звичайного введення тексту – без потреби у додаткових діях з боку користувача. Такий підхід робить метод придатним для фонової перевірки особи під час роботи з комп'ютером або іншим пристроєм. Саме тому клавіатурна динаміка активно застосовується для контролю доступу до критично важливих систем, а також для моніторингу стану оператора у сферах, де потрібна висока концентрація уваги.

Модульна архітектура системи безперервної автентифікації. Система безперервної автентифікації на основі клавіатурного почерку складається з кількох взаємопов'язаних модулів. Першим етапом є збір даних, де фіксуються натискання та відпускання клавіш, часові інтервали між ними, а також додаткові параметри – наприклад, частота помилок, використання клавіш Backspace чи Shift. Ці дані накопичуються у вигляді потоків подій.

Далі відбувається попередня обробка та нормалізація. Система усуває шумові сигнали (наприклад, випадкові затримки через відволікання користувача) та масштабує часові параметри для подальшої класифікації на основі отриманих даних [22]. Використовуються статистичні методи та фільтрація короткострокових відхилень. Зокрема, у роботі Маслія [23] показано ефективність застосування статистичних підходів, зокрема критерію Манна–Вітні, для підвищення точності розмежування користувачів.

На наступному етапі формується ковзне вікно аналізу: система не чекає завершення великого текстового фрагмента, а оцінює останні N натискань. Це дозволяє виявляти зміну користувача протягом кількох секунд після початку сесії.

Модуль класифікації порівнює поточні характеристики з моделлю користувача. Для цього застосовуються алгоритми машинного навчання:

- k-NN (k-Nearest Neighbors) – відносить новий зразок до класу на основі найближчих сусідів у просторі ознак, забезпечуючи просту й швидку класифікацію;
- Random Forest – ансамбль дерев рішень, що підвищує стійкість до шуму та варіативності поведінки;
- SVM (Support Vector Machine) – будує гіперплощину для відокремлення профілю користувача від потенційних зловмисників;
- рекурентні нейронні мережі (RNN, LSTM, GRU) – враховують часові залежності та послідовності натискань;

Ансамбль слабких класифікаторів дає рішення краще за кожен з цих класифікаторів окремо [21];

Якщо відхилення перевищує допустимий рівень, система може:

- запустити додаткову перевірку (наприклад, запитати повторне введення пароля чи одноразового коду),
- тимчасово обмежити доступ до критичних функцій,
- повністю завершити сесію у випадку високої ймовірності компрометації [24].

Важливим компонентом є можливість адаптивного оновлення профілю. Поведінка користувача змінюється з часом (втома, нова клавіатура, інший стиль набору), тому система поступово коригує модель, використовуючи методи інкрементального навчання. Це дозволяє зберігати баланс між точністю та гнучкістю.

Для оцінки ефективності застосовуються стандартні метрик якості біометричних систем: FAR (False Acceptance Rate) – частка випадків, коли зловмисник помилково прийнятий за легітимного користувача; FRR (False Rejection Rate) – частка випадків, коли легітимного користувача помилково відхилено; EER (Equal Error Rate) – точка, де FAR = FRR. Додатково враховується TTD (Time-to-Detect) – час, необхідний для виявлення

аномалії. У сучасних дослідженнях також використовуються метрики ANIA (Average Number of Impostor Actions) – середня кількість дій, які може виконати зловмисник до виявлення, та ANGA (Average Number of Genuine Actions) – середня кількість дій, необхідних для підтвердження легітимного користувача.

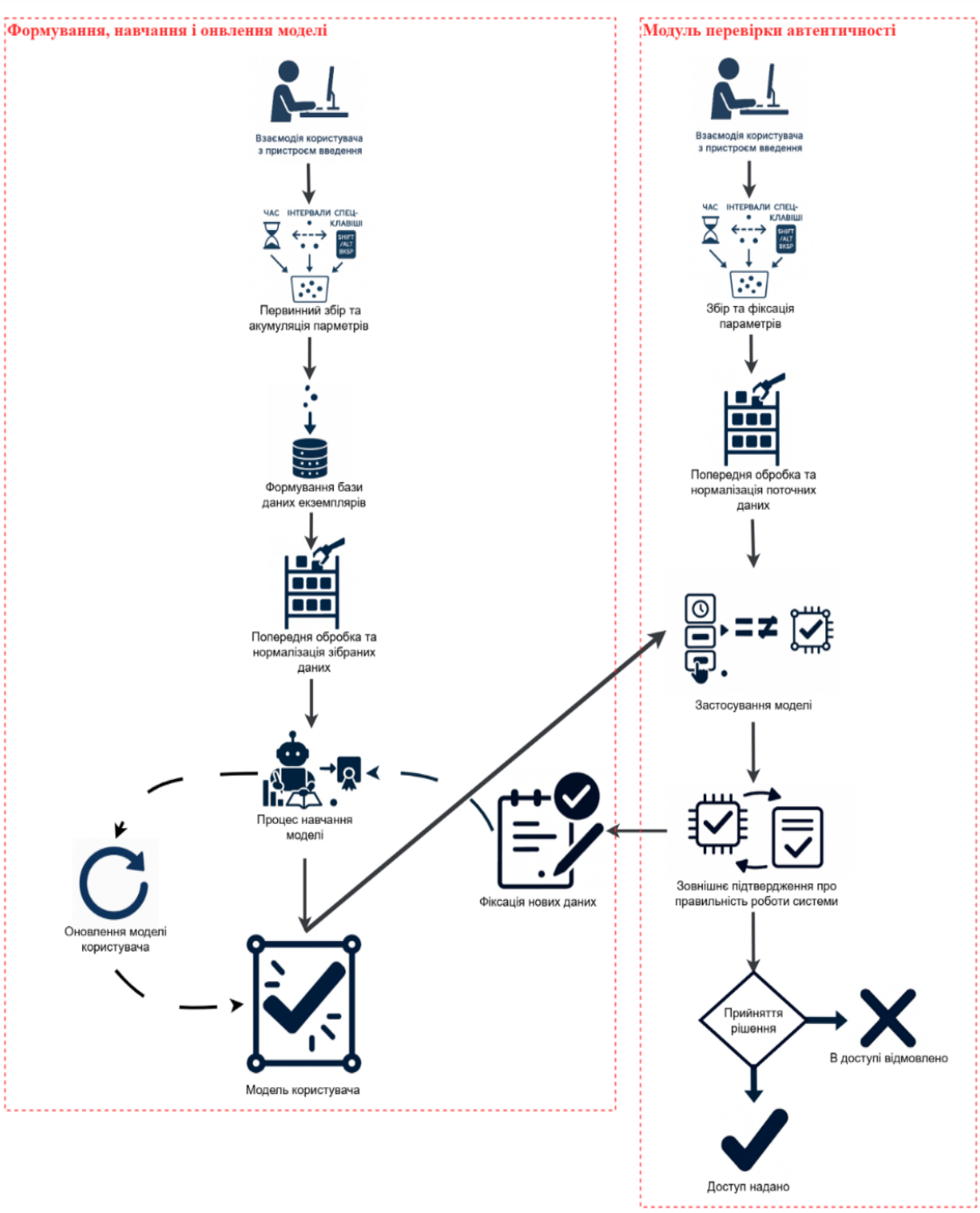

Рис.1. Модульна архітектура системи безперервної біометричної автентифікації користувачів на основі клавіатурного почерку

Ефективність подібних систем визначається якістю збору та обробки часових характеристик, вибором алгоритмів класифікації, здатністю моделі адаптуватися до змін поведінки користувача, а також вибором адекватної метрики для оцінки якості розпізнавання. Використання сучасних методів машинного та глибокого навчання, ансамблевих алгоритмів і інкрементального оновлення профілю забезпечує підвищену

точність та стійкість до варіативності введення. Додаткове застосування ковзних вікон аналізу і динамічного порогового контролю скорочує час виявлення несанкціонованої активності (Time-to-Detect) і знижує показники помилкових спрацювань (FAR, FRR).

Застосування сучасних методів машинного та глибокого навчання, а також ансамблевих алгоритмів і алгоритмів донавчання дозволяє досягти високої точності та стабільної роботи системи навіть при зміні стилю введення тексту. Додаткове використання ковзного аналізу та динамічного регулювання порогових значень допомагає швидше виявляти підозрілу активність (Time-to-Detect) і зменшує кількість помилкових спрацювань (FAR, FRR).

Розроблення ефективної архітектури безперервної автентифікації на основі клавіатурного почерку вимагає вирішення низки технічних завдань: оптимізації алгоритмів для роботи в реальному часі, мінімізації затримок. У цьому контексті перспективними є підходи, що ґрунтуються на машинному навчанні, які дозволяють підвищити рівень точності розпізнавання.

На рисунку нижче запропоновано модульну архітектуру системи безперервної автентифікації користувачів на основі клавіатурного почерку**,** яка передбачає наявність двох взаємопов'язаних модулів: модуля навчання, що включає процеси формування й оновлення моделі, та модулю застосування навеної моделі, в якій і відбувається процес перевірки автентичності користувача. Передбачається, що взаємодія цих модулів може покращити адаптивність системи та сприяти більш ефективному виявленню змін у поведінці користувача.

Завдяки своїй архітектурі безперервна автентифікація на основі клавіатурного почерку може розглядатися як потенційний невидимий захисний шар у сучасних інформаційних системах. Імовірно, у корпоративному середовищі така система здатна реагувати на невідповідність поведінкових параметрів, що теоретично може призводити до автоматичного обмеження доступу.

Інтеграція клавіатурного почерку з додатковими факторами для підвищення рівня захисту. Одним із ключових напрямів удосконалення є використання гібридних моделей, що поєднують статистичні методи та алгоритми глибинного навчання. Статистичні підходи забезпечують швидку обробку та базову стійкість до шумів, тоді як глибинні нейронні мережі здатні виявляти складні нелінійні залежності у поведінкових даних. Поєднання цих підходів може підвищити точність класифікації та зменшити кількість хибних відхилень.

Біометрична автентифікація на основі клавіатурного почерку може ефективно поєднуватися з різними методами автентифікації, утворюючи багатофакторний підхід, що значно підвищує рівень захисту інформаційних систем. Найбільш природним є поєднання з паролем: під час введення система перевіряє не лише правильність символів, а й ритм їх набору. Це створює подвійний бар'єр – знання секретної комбінації та унікальний стиль друку, який складно відтворити зловмиснику навіть за наявності викраденого пароля.

Поширеним варіантом і перспективним для подальшого дослідження є інтеграція з одноразовими паролями (OTP) або SMS-кодами, що належать до фактора володіння. У такій комбінації користувач підтверджує свою особу за допомогою мобільного пристрою, а клавіатурний почерк виступає додатковим поведінковим рівнем перевірки. Аналогічно працює поєднання з апаратними токенами чи смарт-картами: навіть якщо фізичний носій буде викрадено, система зможе додатково перевірити користувача за його стилем набору.

Важливим напрямом є поєднання клавіатурного почерку з фізіологічною біометрією, такою як відбитки пальців, розпізнавання обличчя чи райдужної оболонки ока. У цьому випадку створюється багаторівнева біометрична система: фізіологічний фактор підтверджує особу на вході, а поведінковий забезпечує безперервний контроль протягом усього сеансу.

Додатково клавіатурний почерк може інтегруватися з push-сповіщеннями у мобільних додатках. Користувач підтверджує вхід на пристрої, а система паралельно аналізує його поведінкові характеристики. Це дозволяє знизити ризик компрометації навіть у випадку викрадення мобільного пристрою.

Висновки. У ході аналізу встановлено, що автентифікація на основі клавіатурного почерку є одним із найбільш перспективних напрямів поведінкової біометрії, який поєднує високу інформативність ознак із практичною зручністю впровадження. На відміну від фізіологічних методів, цей підхід не потребує спеціального обладнання, а отже, може бути реалізований у будь-якій інформаційній системі, де присутня клавіатура або аналогічний пристрій введення.

Метод безперервної автентифікації, може забезпечити постійний моніторинг користувача протягом усього сеансу роботи. Такий підхід потенційно дозволяє усунути ключовий недолік традиційних систем – відсутність контролю після початкового входу в систему. Безперервна перевірка, що базується на динаміці натискань клавіш, дає змогу своєчасно виявляти підміну користувача, реагувати на аномальні дії й забезпечувати додатковий рівень захисту без необхідності ручного втручання.

Безперервна біометрична автентифікація на основі клавіатурного почерку може розглядатися як важливий етап еволюції систем інформаційної безпеки. Її подальший розвиток пов'язаний із удосконаленням алгоритмів адаптивного навчання, зменшенням похибок класифікації, підвищенням швидкодії та інтеграцією з багатофакторними механізмами ідентифікації. Реалізація таких систем у практичних умовах здатна забезпечити баланс між надійністю, зручністю та непомітністю захисту, що є ключовим критерієм для сучасних і майбутніх кіберзахисних технологій.

Перспективним є застосування цієї технології у сферах, де необхідно гарантувати високий рівень безпеки та оперативне виявлення відхилень у поведінці користувача. Зокрема, у фінансових і державних системах вона може сприяти зниженню ризику шахрайства та несанкціонованого доступу, а в освітніх і корпоративних платформах – забезпечувати додаткову перевірку автентичності під час онлайн-взаємодії. Крім того, у військових та медичних інформаційних середовищах подібні підходи можуть допомагати виявляти потенційні загрози, відстежувати зміни у стані операторів або контролювати доступ до критично важливих систем. У хмарних платформах і сервісах віддаленого адміністрування така автентифікація може використовуватися для моніторингу активності користувачів і вчасного виявлення ознак компрометації облікових записів. Також технологія може бути впроваджена в інформаційних системах державного управління, судових і банківських реєстрах, де потрібен постійний контроль за достовірністю дій користувача, а в кіберзахисних комплексах і системах моніторингу інцидентів – для автоматичного визначення поведінкових аномалій, що свідчать про внутрішні загрози або атаки.

Список використаних джерел

1. Joyce R., Gupta G. Identity authorization based on keystroke latencies. *Communications of the ACM.* 1990. Vol. 33, No. 2. P. 168–176. Available https://dl.acm.org/doi/10.1145/75577.75582.
2. Monrose F., Rubin A. D. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems.* 2000. Vol. 16, No. 4. P. 351–359. Available: https://doi.org/10.1016/S0167-739X(99)00059-X.
3. Wang X., Hou D. Enhancing Keystroke Dynamics Authentication with Ensemble Learning and Data Resampling Techniques. *Electronics.* 2024. Vol. 13, No. 22, 4559. Available: https://doi.org/10.3390/electronics13224559.
4. Arsh A. et al. Multiple Approaches Towards Authentication Using Deep Learning. *Procedia Computer Science.* 2024. Vol. 230. P. 234–241. Available: https://www.sciencedirect.com/science/article/pii/S1877050924009220.
5. Wyciślik Ł. The Improved Biometric Identification of Keystroke Dynamics Using Deep Learning. *Sensors.* 2024. Vol. 24, No. 12, 3763. Available: https://www.mdpi.com/1424-8220/24/12/3763.

6. A. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, J. Fierrez, *TypeNet: Deep Learning Keystroke Biometrics*, arXiv Preprint, Jan. 2021. [Online]. Available: https://arxiv.org/abs/2101.05570.
7. A. Acien, J. V. Monaco, A. Morales, R. Vera-Rodriguez, J. Fierrez, *TypeNet: Scaling up Keystroke Biometrics*, arXiv Preprint, Apr. 2020. [Online]. Available: https://arxiv.org/abs/2004.03627.
8. K. Tanveer Kiyani, A. Lasebae, K. Ali, M. Ur Rehman, B. Haq, *Continuous User Authentication Featuring Keystroke Dynamics Based on Robust Recurrent Confidence Model and Ensemble Learning Approach*, IEEE Access, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3019467.
9. "Continuous authentication by free-text keystroke based on CNN and …", ScienceDirect, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820301334.
10. "Security, Privacy, and Usability in Continuous Authentication: A Survey", MDPI Sensors, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/17/5967.
11. of Keystroke Dynamics Biometrics", PMC article, 2013. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3835878.
12. "Authentication by Keystroke Dynamics: The Influence of Typing Language", MDPI Applied Sciences, (2023). [Online]. Available: https://www.mdpi.com/2076-3417/13/20/11478.
13. "Hidden Monitoring Based on Keystroke Dynamics in Online ...", PMC, 2022. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9707207. Accessed on: Oct. 2025.
14. "A survey paper on keystroke dynamics authentication for current applications", ResearchGate / AIP, 2019. [Online]. Available: https://www.researchgate.net/publication/337190342_A_survey_paper_on_keystroke_dynamics_authentication_for_current_applications.
15. "Authentication via keystroke dynamics", ACM Digital Library. [Online]. Available: https://dl.acm.org/doi/10.1145/266420.266434.
16. "Enhanced-TypeNet for Biometric Keystroke Authentication", ETASR Journal, 2025. [Online]. Available: https://etasr.com/index.php/ETASR/article/view/11468.
17. "BehaveFormer: A Framework with Spatio-Temporal Dual Attention Transformers for IMU enhanced Keystroke Dynamics", arXiv, 2023. [Online]. Available: https://arxiv.org/abs/2307.11000.
18. Заяць, М. М., Заяць, А. В. *Аналіз методів та підходів до побудови систем розпізнавання та ідентифікації користувачів комп'ютера на основі інформаційних моделей клавіатурного почерку*. – Львівський політехнічний університет. 2011. [Online]. Available: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3374/1195.pdf.
19. Єнгаличев, С. О., Семенов, С. Г. *Біометрична автентифікація на основі аналізу клавіатурного почерку*. – Національний університет «Київський політехнічний інститут». 2012. [Online]. Available: http://openarchive.nure.ua/handle/document/145.
20. Липовий, Т. В. *Біометрична аутентифікація за клавіатурним почерком*. – 2015. [Online]. Available: https://core.ac.uk/download/pdf/60823423.pdf.
21. Кондратенко, Н. Р., Мельник, Л. С. *Автентифікація за клавіатурним почерком на основі нейромережевого підходу*. – Вінницький національний технічний університет. [Online]. Available: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14564/zbirnyk-2015-Kondr2.pdf.
22. Касянчук, Н. В. *Автентифікація користувачів на основі клавіатурного почерку*. – Вінницький національний технічний університет. 2020. [Online]. Available: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/45225/8332.pdf.
23. Маслій, Д. В. *Динамічна аутентифікація за клавіатурним почерком з використанням критерію Манна-Вітні*. – Харківський національний університет радіоелектроніки. [Online]. Available: https://openarchive.nure.ua/server/api/core/bitstreams/2a1a7177-a5d4-406b-8c00-f570fbe985c4/content.
24. Башков, Є. О., Алтухова, Т. В., Єжова, Є. О. *Розробка методу аутентифікації користувача на основі клавіатурного почерку*. – ДонНТУ. 2023. [Online]. Available: https://iktv.donntu.edu.ua/wp-content/uploads/2023/03/09_bashkov.pdf.
25. Зеленський, І. Б. *Дослідження ефективності ідентифікації особи за клавіатурним почерком з урахуванням сили тиску на клавіші*. – Харківський національний університет радіоелектроніки. 2024. [Online]. Available: https://openarchive.nure.ua/entities/publication/0d7bb389-b7ec-4a13-9404-901f06e42c23.

References

1. Joyce R., Gupta G. Identity authorization based on keystroke latencies. *Communications of the ACM.* 1990. Vol. 33, No. 2. P. 168–176. Available: https://dl.acm.org/doi/10.1145/75577.75582.
2. Monrose F., Rubin A. D. Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems.* 2000. Vol. 16, No. 4. P. 351–359. Available: https://doi.org/10.1016/S0167-739X(99)00059-X.
3. Wang X., Hou D. Enhancing Keystroke Dynamics Authentication with Ensemble Learning and Data Resampling Techniques. *Electronics.* 2024. Vol. 13, No. 22, 4559. Available: https://doi.org/10.3390/electronics13224559.
4. Arsh A. et al. Multiple Approaches Towards Authentication Using Deep Learning. *Procedia Computer Science.* 2024. Vol. 230. P. 234–241. Available: https://www.sciencedirect.com/science/article/pii/S1877050924009220.
5. Wyciślik Ł. The Improved Biometric Identification of Keystroke Dynamics Using Deep Learning. *Sensors.* 2024. Vol. 24, No. 12, 3763. Available: https://www.mdpi.com/1424-8220/24/12/3763.

6. A. Acien, A. Morales, J. V. Monaco, R. Vera-Rodriguez, J. Fierrez, *TypeNet: Deep Learning Keystroke Biometrics*, arXiv Preprint, Jan. 2021. [Online]. Available: https://arxiv.org/abs/2101.05570.
7. A. Acien, J. V. Monaco, A. Morales, R. Vera-Rodriguez, J. Fierrez, *TypeNet: Scaling up Keystroke Biometrics*, arXiv Preprint, Apr. 2020. [Online]. Available: https://arxiv.org/abs/2004.03627.
8. K. Tanveer Kiyani, A. Lasebae, K. Ali, M. Ur Rehman, B. Haq, *Continuous User Authentication Featuring Keystroke Dynamics Based on Robust Recurrent Confidence Model and Ensemble Learning Approach*, IEEE Access, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3019467.
9. "Continuous authentication by free-text keystroke based on CNN and …", ScienceDirect, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820301334.
10. "Security, Privacy, and Usability in Continuous Authentication: A Survey", MDPI Sensors, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/17/5967.
11. "A Survey of Keystroke Dynamics Biometrics", PMC article, 2013. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3835878. Accessed on: Oct. 2025.
12. "Authentication by Keystroke Dynamics: The Influence of Typing Language", MDPI Applied Sciences, (2023). [Online]. Available: https://www.mdpi.com/2076-3417/13/20/11478.
13. "Hidden Monitoring Based on Keystroke Dynamics in Online ...", PMC, 2022. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9707207. Accessed on: Oct. 2025.
14. "A survey paper on keystroke dynamics authentication for current applications", ResearchGate / AIP, 2019. [Online]. Available: https://www.researchgate. net/publication/3371 90342_A_s urvey_paper_on_keystroke_dynamics_authentication_for_current_applications.
15. "Authentication via keystroke dynamics", ACM Digital Library. [Online]. Available: https://dl.acm.org/doi/10.1145/266420.266434.
16. "Enhanced-TypeNet for Biometric Keystroke Authentication", ETASR Journal, 2025. [Online]. Available: https://etasr.com/index.php/ETASR/article/view/11468.
17. "BehaveFormer: A Framework with Spatio-Temporal Dual Attention Transformers for IMU enhanced Keystroke Dynamics", arXiv, 2023. [Online]. Available: https://arxiv.org/abs/2307.11000.
18. Zaiats M. M., Zaiats A. V. *Analysis of methods and approaches to building user recognition and identification systems based on keystroke dynamics information models*. – Lviv Polytechnic National University, 2011. Available: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3374/1195.pdf.
19. Yenhalychev S. O., Semenov S. H. *Biometric authentication based on keystroke analysis*. Kyiv Polytechnic Institute, 2012. Available: http://openarchive.nure.ua/handle/document/145.
20. Lypovyi T. V. *Biometric authentication based on keystroke dynamics*. – 2015. Available: https://core.ac.uk/download/pdf/60823423.pdf.
21. Kondratenko N. R., Melnyk L. S. *Keystroke dynamics authentication based on neural network approach*. – Vinnytsia National Technical University. Available: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/14564/zbirnyk-2015-Kondr2.pdf.
22. Kasianchuk N. V. *Keystroke-based user authentication*. – Vinnytsia National Technical University, 2020. Available: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/45225/8332.pdf.
23. Maslii D. V. *Dynamic authentication using keystroke dynamics with Mann–Whitney criterion.* – Kharkiv National University of Radioelectronics. Available: https://openarchive.nure.ua/server/api/core/bitstreams/2a1a7177-a5d4-406b-8c00-f570fbe985c4/content.
24. Bashkov Ye. O., Altukhova T. V., Yezhova Ye. O. *Development of an authentication method based on keystroke dynamics*. – DonNTU, 2023. Available: https://iktv.donntu.edu.ua/wp-content/uploads/2023/03/09_bashkov.pdf.
25. Zelenskyi I. B. *Study of identification efficiency using keystroke dynamics with pressure-force analysis*. – Kharkiv National University of Radioelectronics, 2024. Available: https://openarchive.nure.ua/entities/publication/0d7bb389-b7ec-4a13-9404-901f06e42c23.