ВІСНИК
ОДЕСЬКОГО НАЦІОНАЛЬНОГО
МОРСЬКОГО УНІВЕРСИТЕТУ
№ 1 (79), 2026

HERALD
OF THE ODESA NATIONAL
MARITIME UNIVERSITY
№ 1 (79), 2026

ISSN 2226-1893

УДК 004.32.26:004.056.523
DOI 10.47049/2226-1893-2026-1-214-229

МОДЕЛЮВАННЯ КЛАВІАТУРНОГО ПОЧЕРКУ КОРИСТУВАЧІВ ЗА ДОПОМОГОЮ НЕЙРОННОЇ МЕРЕЖІ

Ю.В. Даус
к.геогр.н., доцент кафедри «Технічна кібернетика
й інформаційні технології ім. проф. Р.В. Меркта»
ORCID: 0000-0001-9737-4663
М.Є. Даус
к.геогр.н., доцент кафедри «Безпека життєдіяльності, екології та хімії»
ORCID: 0000-0001-5298-795X

Одеський національний морський університет, Одеса, Україна

Анотація. *Ідентифікація користувачів в наш час є одною з головних задач сучасної кібербезпеки. Безпечний вхід дозволяє користувачам отримати доступ до чутливих даних: банківських рахунків, податкової служби, соціальних мереж. Втрата паролів або отримання їх зловмисниками можуть завдати непоправної шкоди не тільки окремим громадянам, але й приватним та державним організаціям. В деяких випадках ця шкода може бути непоправною.*

Найбільш популярним методом є ідентифікація по логіну та паролю. Але з розвитком соціальної інженерії, збільшення кількості зломів та витоку паролів, цей метод перестає бути безпечним. Щороку кількість кібератак направлених на викрадення паролів тільки зростає. Тому в останні роки набувають популярності біометричні методи.

Такі методи дозволяють доволі точно ідентифікувати людину по відбитках пальців, біометрії обличчя. Але такі методи вимагають специфічних датчиків. Як правило, частина таких датчиків вже вбудовуються в сучасні мобільні пристрої, але зовсім відсутні в стандартних десктопних комп'ютерах. Доля таких комп'ютерів все ще складає більшу половину всіх пристроїв. Тому доцільно скористатися поведінковою біометрією – клавіатурним почерком, який відображає індивідуальну особливість кожної людини.

Важливо, що для отримання технічних характеристик клавіатурного почерку не потрібно ніяких додаткових сенсорів та приладів.

У статті розглянуті основні характеристики клавіатурного почерку, які дозволять в майбутньому побудувати нейронну мережу з розпізнавання користувачів за клавіатурним почерком.

Отримання декількох технічних характеристик допоможе використати більше параметрів для нейромережі.

Ключові слова: *кібербезпека, вразливості, кіберзлочинці, ідентифікація користувачів, клавіатурний почерк.*

ВІСНИК
ОДЕСЬКОГО НАЦІОНАЛЬНОГО
МОРСЬКОГО УНІВЕРСИТЕТУ
№ 1 (79), 2026

HERALD
OF THE ODESA NATIONAL
MARITIME UNIVERSITY
№ 1 (79), 2026

ISSN 2226-1893

UDC 004.32.26:004.056.523
DOI 10.47049/2226-1893-2026-1-214-229

MODELING USERS KEYBOARD HANDWRITING USING A NEURAL NETWORK

Y.V. Daus
PhD, docent
of the Department «Technical Cybernetics and Information Technologies
named after prof. R.V. Merkt»
ORCID: 0000-0001-9737-4663
M.E. Daus
PhD, docent of the Department «Safety of Life, Ecology and Chemistry»
ORCID: 0000-0001-5298-795X

Odesa National Maritime University, Odesa, Ukraine

Abstract. *User identification is one of the main tasks of modern cybersecurity today. Secure login allows users to access sensitive data: bank accounts, tax authorities, social networks. Losing passwords or obtaining them by attackers can cause irreparable harm not only to individual citizens, but also to private and public organizations. In some cases, this damage can be irreparable.*

The most popular method is identification by login and password. But with the development of social engineering, an increase in the number of hacks and password leaks, this method ceases to be safe. Every year the number of cyberattacks aimed at stealing passwords only grows.

Therefore, biometric methods have become popular in recent years. Such methods allow for fairly accurate identification of a person by fingerprints, facial biometrics. But such methods require specific sensors. As a rule, some of such sensors are already built into modern mobile devices, but are completely absent in standard desktop computers. The share of such computers still makes up more than half of all devices.

Therefore, it is advisable to use behavioral biometrics – keyboard handwriting, which reflects the individual characteristics of each person. It is important that to obtain the technical characteristics of keyboard handwriting, no additional sensors and devices are required.

The article discusses the main characteristics of keyboard handwriting that will allow in the future to build a neural network for recognizing users by keyboard handwriting.

Obtaining several technical characteristics will allow using more parameters for the neural network.

Keywords: *cybersecurity, vulnerabilities, cybercriminals, user identification, keyboard handwriting.*

ISSN 2226-1893

Вступ. У наш час кількість сервісів в яких необхідно автентифікуватися за допомогою паролю постійно зростає. Користувачам стає все складніше запам'ятовувати всі паролі, тому деякі користувачі використовують одні і ті ж паролі для різних сервісів. Такий підхід дуже небезпечний, оскільки витік паролю з одного сервісу ставить під загрозу всі інші сервіси. Доповнення паролей біометричними характеристиками або ж використання біометрії робить значно безпечнішим та надійним банківські сервіси, комунікацію з органами державної влади, покупки в інтернет-магазинах, отримання цільової допомоги, дистанційна робота, отримання документів та багато чого іншого. Тому надійна ідентифікація користувача є найпершою та найвідповідальнішою роботою системних адміністраторів, спеціалістів з кібербезпеки та захисту інформації.

Ідентифікація користувачів з використанням сучасних мобільних пристроїв дозволяє широко використовувати біометричну ідентифікацію по відбитку пальців, сканеру сітківки ока або по ідентифікатору обличчя (Face ID). Це дозволяє переконатися в тому, що це пристрій використовує саме та людина, яка запросила доступ до даного сервісу.

Однак, наразі використовується ще дуже багато пристроїв, що не мають відповідних датчиків та не можуть сканувати біометричні характеристики. Тому постає актуальна задача з додаткової ідентифікації користувача. В наш час широко використовується двофакторна ідентифікація: коли доступ потрібно підтвердити на іншому пристрої. Але, якщо цей пристрій попаде до рук зловмисника, то він з легкістю введе потрібну інформацію та отримає доступ до сервісів користувача.

У даному випадку, як додатковий шар захисту, можна використовувати поведінкову біометрію. До поведінкової біометрії можна віднести особливості рухів людини при ходьбі, бігу, роботи пальців, рух м'язів. Одним із видів поведінкової біометрії є клавіатурний почерк – це та особливість кожної людини, з якою він працює на клавіатурі та набирає текст. Аналіз клавіатурного почерку не потребує додаткових датчиків та сенсорів, можна обійтися спеціальним програмним забезпеченням, що дозволить нам отримати технічні характеристики клавіатурного почерку, зробити аналіз цих характеристик та застосувати в самих різноманітних моделях ідентифікації користувача по клавіатурному почерку.

Класифікація характеристик клавіатурного почерку. Напевно, початком класифікації за клавіатурним почерком можна вважати кінець 19 століття, коли почали запроваджувати телеграф. І вже тоді телеграфісти доволі легко впізнавали один одного за манерою роботи з телеграфним ключем, динамікою набирання символів та об'ємом «буферної пам'яті» оператора, швидкістю та ритмом передачі. Все це в купі давало можливість однозначно ідентифікувати людину, що передавала телеграфне сповіщення. Пізніше таке розпізнавання поширилось і на радіопередачі під час Другої світової війни, що дозволяло підтвердити факт передачі сповіщення авторизованим радистом, а не підмінною людиною [1].

Особливості клавіатурного почерку можна фіксувати за допомогою спеціальних датчиків, які можуть фіксувати різноманітні характеристики: силу натискань, час утримання клавіші, інтервальну рівномірність тощо. Але в такому випадку клавіатура стає дуже дорогою і економічний ефект від впровадження такої

ISSN 2226-1893

технології зникає. Тоді вже є сенс використовувати датчики, які дозволяють одразу перевіряти відбитки пальців або індивідуальні особливості обличчя. Для економічної доцільності варто використовувати саму звичайну клавіатуру та спеціальне програмне забезпечення.

Потрібно визначити, які саме технічні характеристики ми можемо збирати написавши спеціальну програму, що буде відстежувати роботу клавіатури під час введення паролю. Виходячи з цієї задачі ми можемо розділити ці характеристики на дві великі групи: інтегральні характеристики та вимірювальні (таблиця 1).

Таблиця 1

Технічні характеристики клавіатурного почерку

Вимірювальні	Інтегральні
Час утримання	Дираф
Міжклавішний інтервал	Триграф
Час перекриття	Загальний час введення паролю

До інтегральних характеристик ми можемо віднести загальний час введення паролю, диграфи та триграфи. Диграфи – це загальний час введення двох символів, а триграфи – це загальний час введення трьох символів. Іншими словами загальний час введення характеризує наскільки швидко користувач вводить цей пароль і наскільки довго ним користується, адже під час тривалого введення одного і того самого паролю виробляється автоматизм і людина не замислюється про сам процес набирання паролю. Диграфи та триграфи більше характеризують ступінь володіння користувача клавіатурою, скільки пальців задіяно при набиранні паролю, пароль вводиться з листочка чи з пам'яті.

Вимірювальні характеристики оцінюють наступне:

- утримання клавіші DT (Dwell Time) – час від натиснення клавіші та її відпускання;
- міжклавішний інтервал FT (Flight Time) – час між відпущенням поточної клавіші та натисненням наступної клавіші;
- час перекриття OT (Overlap Time) – це час коли одночасно натиснено дві клавіші: ще не відпущена попередня клавіша, але вже натиснута наступна клавіша;
- час натискання двох клавіш DG (диграф);
- час натискання трьох клавіш TG (триграф)

Унікальність цих показників пояснюється індивідуальними особливостями моторики людини, об'ємом буферної пам'яті, сформованими звичками та навіть психологічними факторами та навколишнім оточенням. Тому кожен користувач має власний «клавіатурний підпис», який може бути використаний для ідентифікації людини.

Вибір моделі. Необхідно вибрати такий математичний інструмент, що дозволить однозначно ідентифікувати людину за клавіатурним почерком. Існує дуже багато підходів різних авторів в цьому питані. Можна виділити основні:

ISSN 2226-1893

- на основі диграфів та триграфів була розроблена модель [2] з використанням квадратичного індексу нечіткості;

- застосування розпізнавання методом описання даних опорними векторами (SVDD) і однокласове навчальне векторне квантування (LVQ) [3];

- побудова нейронної мережі для розпізнавання клавіатурного почерку вчених Махершаві та Вікрама Пуді [4].

Найбільш прогресивним та перспективним є побудова нейронної мережі. Це дозволить використовувати як вимірювальні так і інтегральні характеристики клавіатурного почерку. Які саме із отриманих характеристик будуть найбільш підходити для побудови нейронної мережі ми зможемо виявити в результаті проведення експерименту з навчання нейронної мережі на різних даних.

Отримання експериментальних даних. Для отримання даних по клавіатурному почерку введення паролю користувача нами була розроблена програма KeyPress5 на мові програмування Java для фіксування технічних характеристик клавіатурного почерку. Програма розрахована на безліч користувачів та довжину паролю не більше 18 символів. Програма вбудовувалась в автозавантажувач, що давало можливість автоматично викликати програму під час завантаження комп'ютера. Для зручності перехід на наступне поле відбувається при натисненні клавіші ENTER, яка не враховується як символ в полі паролю.

В нашому експерименті приймало участь три користувача. Назвемо їх користувач A, B та C. Кожен з них повинен був ввести свій пароль не менше 100 разів. Окремі вимоги були до самих паролів користувачів: не менше 6 символів, обов'язково повинен містити велику літеру, число та спеціальний символ. Потім кожен користувач отримував паролі двох інших користувачів і набирав ці паролі як «зловмисник», що намагається увійти в систему під чужим паролем та логіном. В подальшому дані що набирає сам користувач ми будемо називати оригінальними, а ті дані що набирає «зловмисник» − підробленими. Також візуалізуємо сам пароль по наступній методиці, щоб не говорити про справжні паролі:

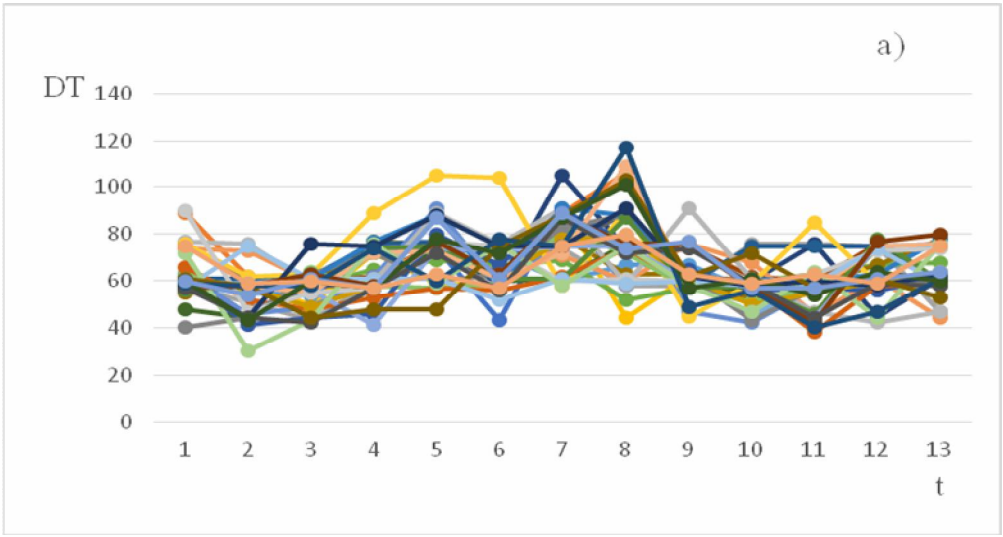
- велика літера це символ A;
- маленька літера це символ a;
- число – символ n;
- спеціальний символ - @.

Використовуючи таке кодування, ми можемо вказати що користувач A мав пароль Aaaaaaaaa@nnn, користувач B – Aaaaannnn@ і користувач C – Aaaa@nnnn. Як бачимо паролі доволі різні як по довжині, так і по розміщенню спеціального символу та розміщення чисел.

Отримані експериментальні дані ми візуалізували для виявлення можливих закономірностей. Для прикладу на рис. 1 наведено графік утримання клавіші DT для оригінального введення та введенням «зловмисника».

Як видно з графіків, помітна різниця між оригінальним введенням та введенням «зловмисника». Екстремуми знаходяться в різних символах паролю. Ще більш очевидною стає ця різниця коли ми побачимо графік технічної характеристики FT – міжклавішного інтервалу який представлений на рис 2. Очевидно, що кількість сигналів буде на 1 менше ніж довжина паролю.

ISSN 2226-1893



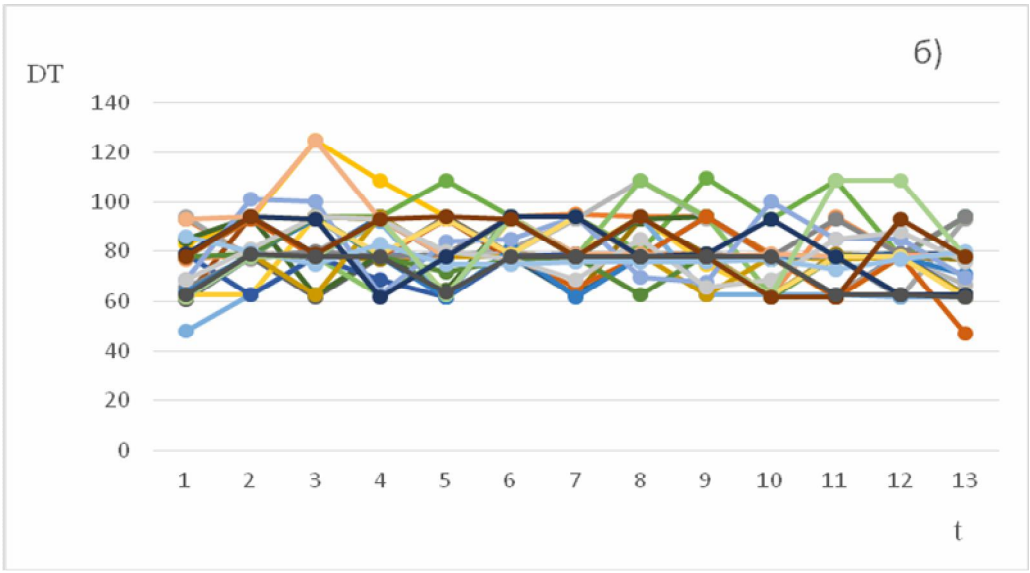


Рис. 1. Час утримання клавіші в мілісекундах користувача А:
а) оригінальне введення; б) введення «зловмисником»

ISSN 2226-1893

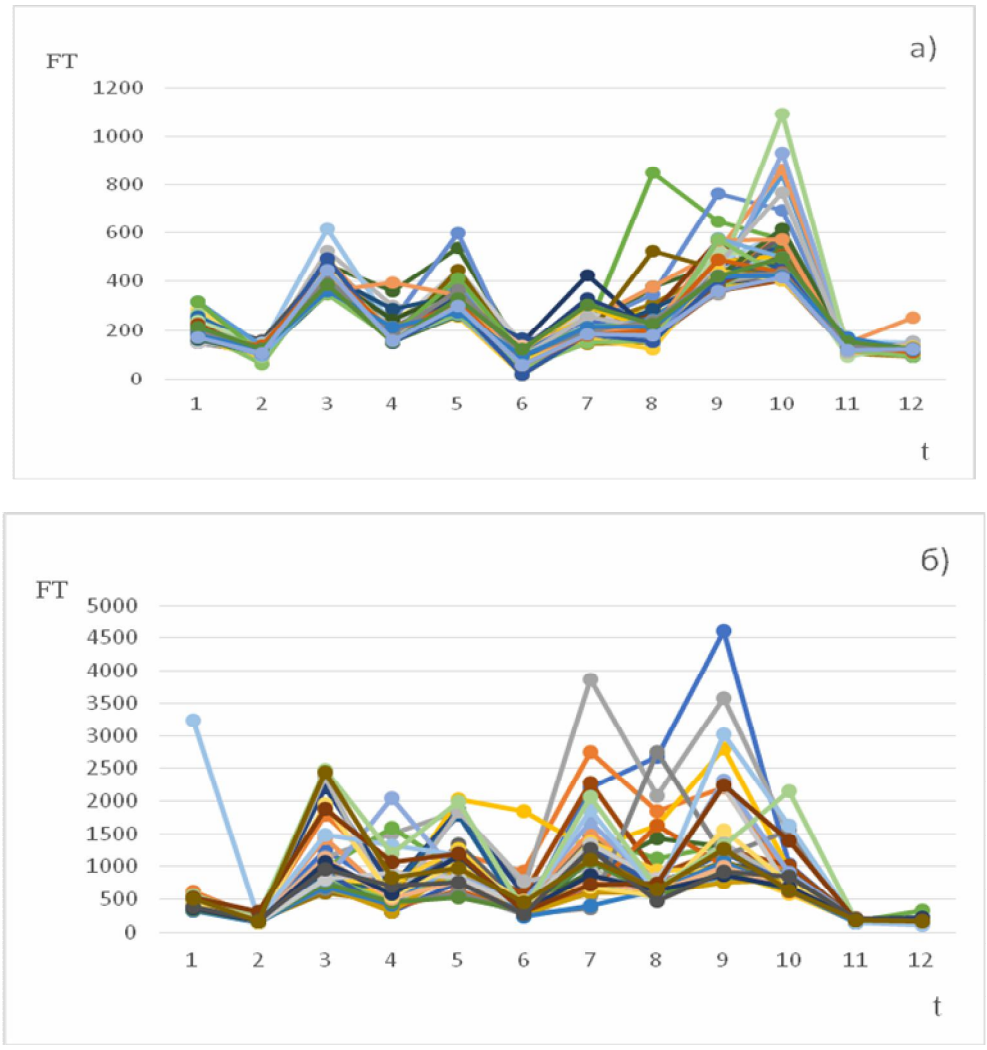


Рис. 2. Міжклавішний інтервал в мілісекундах користувача А:
а) оригінальне введення; б) введення «зловмисником»

Звертає увагу, що максимальні значення у зловмисника значно вищі ніж у оригіналу. Крім того, в оригіналу видна чітка структура набору паролю, практично відсутні коливання. Деякі дані виходять за межі, але людина не робот і не автомат, може відчувати втому та мати погане самопочуття і це може впливати на технічні характеристики клавіатурного почерку.

Ще одна інтегральна характеристика це диграфи та триграфи. Практично графіки мало чим відрізняються один від одного, але відрізняється оригінальне введення та введення «зловмисника». На рис. 3 представлений типовий графік інтегральної характеристики – диграфа.

ISSN 2226-1893

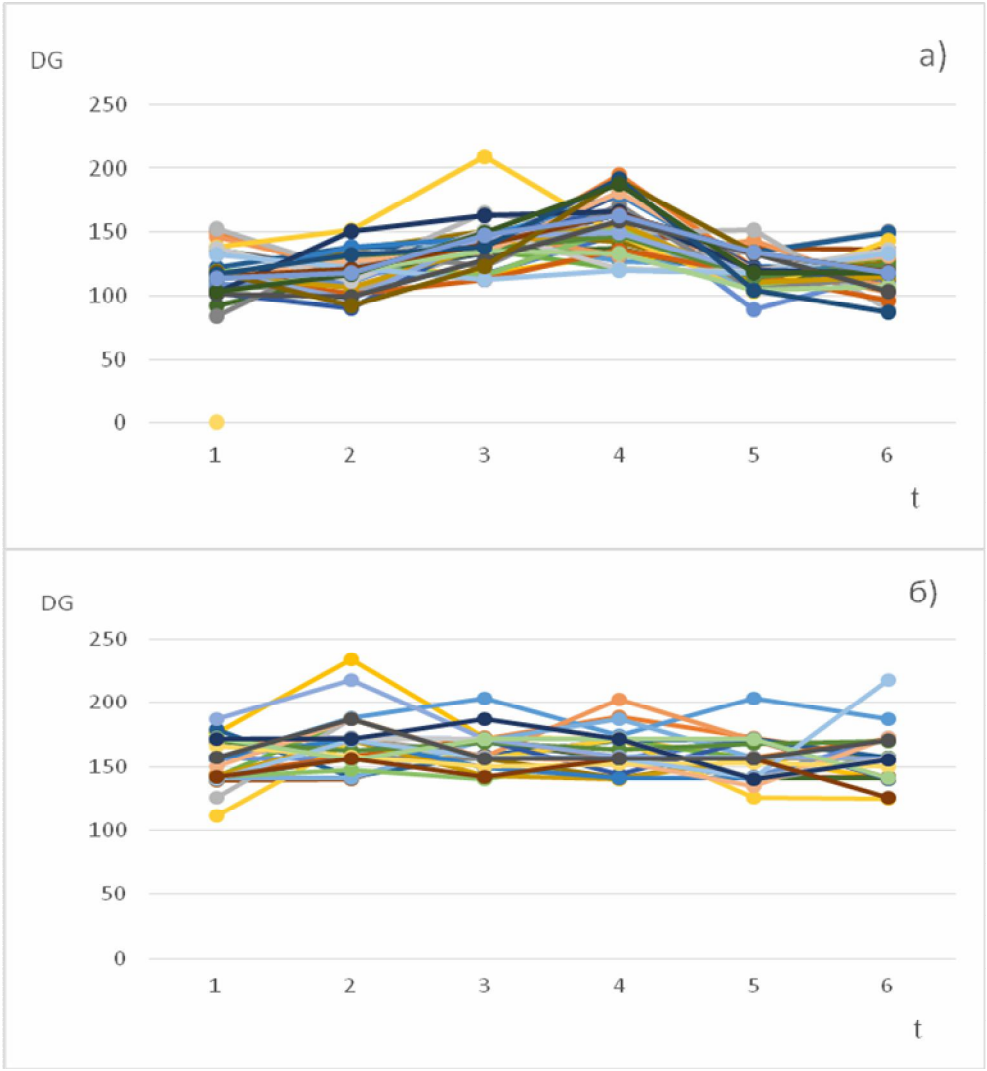


Рис. 3. Інтегральний показник дограф в мілісекундах користувача А:
а) оригінальне введення; б) введення зловмисником

Тут також помітна відмінність між оригінальним введенням та введенням «зловмисника». В оригінальному введенні ми бачимо скупчення піків на 4 позиції, а в «зловмисника» на другій позиції.

Ще однією з характеристик є час перекриття або overlap time (OT) – це різниця між утриманням попереднього символу та поточного. Графік цієї характеристики представлений на рис. 4. Він характеризує динаміку введення тексту.

ISSN 2226-1893

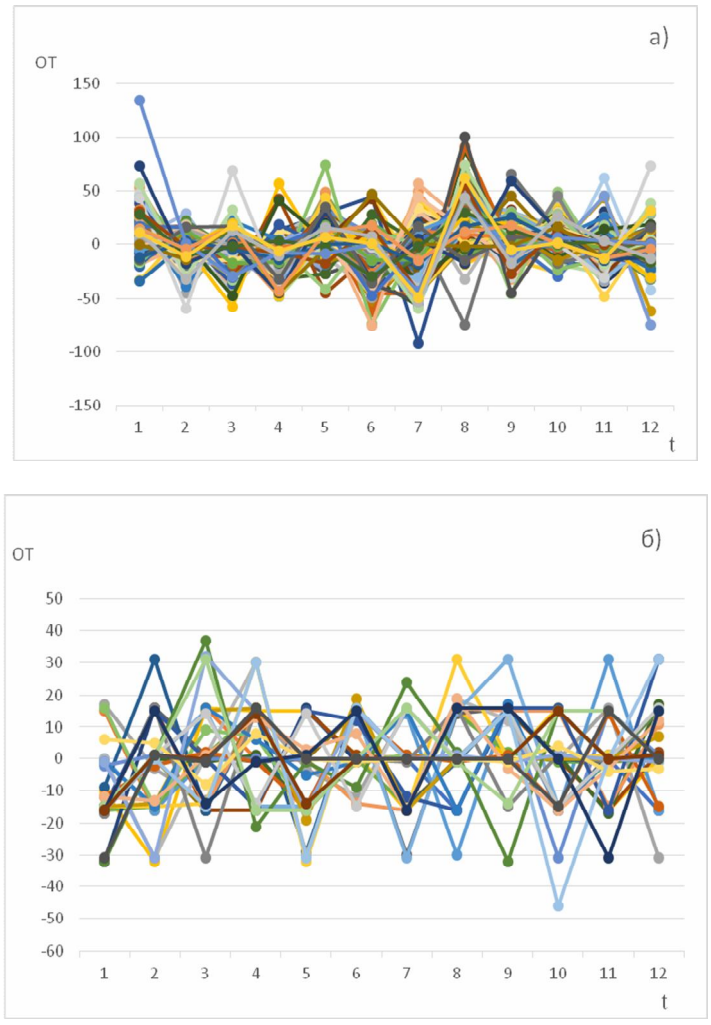


Рис. 4. Динаміка введення паролю користувачем А:
а) оригінальне введення; б) введення зловмисником

З графіка видно доволі суттєві відмінності в динаміці набору паролю. Але можна помітити дуже значну варіативність цього ряду. Наскільки ця характеристика буде впливати на навчання нейронної мережі ми побачимо в ході проведення експерименту.

Таким чином, у нас достатньо експериментальних даних для побудови та навчання нейронної мережі. І нашою головною задачею буде знаходження характеристики або комплексу характеристик, що дозволить побудувати нейронну мережу, яка зможе з вірогідністю більше ніж 95 % встановити автора набору паролю. Це надасть нам можливість застосовувати клавіатурний почерк як один з методів поведінкової біометрії.

ISSN 2226-1893

Вибір нейронної мережі. Спираючись на роботи Махершаві та Вікрама Пуді [4], Даус Ю.В. [5] доцільно вибрати повнозв'язану нейронну мережу прямого поширення. Це найбільш поширена схема в нашому випадку. Зробимо деяку модифікацію навчання нейронної мережі. В роботі [5] розглядався метод зворотного розповсюдження помилки. Ми додаємо сюди ще метод градієнтного спуску для вагових коефіцієнтів. Таким чином ми можемо змінювати крок зміни цих коефіцієнтів прискорюючи вихід на плато помилки.

Найбільш складним завданням є вибір функції активації. Одними з популярних функцій є Rectified Linear Unit (ReLU) та сигмовидна функція. Функція ReLU [6], набула широкої популярності в останні роки завдяки своїй обчислювальній ефективності та здатності уникати проблеми зникання градієнту. Функція ReLU (1) є кусково-лінійною функцією, яка виводить нуль для від'ємних входів і саме вхідне значення для додатних входів, таким чином вносячи нелінійність у модель, зберігаючи при цьому обчислювальну простоту

$$f(x) = max(0, x) = \frac{x + |x|}{2} = \begin{cases} x, & x > 0, \\ 0, & x \leq 0 \end{cases} \quad (1)$$

Переваги її в простоті, швидкості навчання і зменшенні проблем із зникання градієнту. З недоліків це «відмирання» деяких нейронів при негативних значення вхідного сигналу.

Іншою відомою функцією активації є сигмовидна функція (2), класичним прикладом якої є логістичне рівняння, яке приводить вхідні дані до значення між 0 і 1, тим самим дозволяючи моделі вивчати вірогіднісні зв'язки між вхідними і вихідними даними [7]

$$\sigma(x) = \frac{1}{1 + e^{-x}} = \frac{e^x}{1 + e^x} = 1 - \sigma(-x) \quad (2)$$

Переваги цієї фукнції в безперевності диференціювання, гладкості, що сприяє стабільності градієнтного спуску при навчані. З недоліків – це дуже маленькі значення при наближенні до нуля і вони можуть спричиняти зникнення градієнта вагових коефіцієнтів. Тому, в останій час цю функцію використовують частіше в останньому шарі при переході на вихідний нейрон. Це дуже зручно, адже значення цієї функції можна прирівняти до вірогідності в долях одиниці.

Ще дуже часто використовують гіперболічний тангенс та модифікацію ReLU – Leaky ReLU, в якій вирішується проблема «смерті нейронів» шляхом додавання невеликого (деякого) нахилу при від'ємних значеннях.

Для навчання нашої нейронної мережі ми розробили програмний комплекс NeuroNet на мові програмування Java. В якості набору даних завантажується файл в форматі CSV (coma separated value), що означає «дані розділені комою». Передбачається, що дані розділені комою, а десяткові знаки відокремлені крапкою. На жаль, таке можливо тільки при певній локалізації програмного забезпечення – американській. Ще більше це не спрацьовує коли в комірці знаходиться текст з

ISSN 2226-1893

комами. Тоді система вважає що тут кілька полів. Ми застосували свій знак закінчення значення зміної та початку нової – це крапка з комою «;». Оскільки такий знак доволі рідко зустрічається в наборах даних, то використання його виправдано. Крім того, ми будемо використовувати кому як роздільник десяткових знаків, що явно стосується такого регіону як Україна.

Всі інші підготовки даних ми будемо проводити безпосереньо в нашому програмному комплексі. Одною з таких підготовок є номалізація даних. Якщо ми подивимося на наші дані, то ми побачимо їх дуже велику варіабельність від 30 до 4500 мілісекунд. При навчані нейронної мережі ми можемо стикнутися з такою ситуацією, що максималльні значення будуть максимально впливати через вагові коефіцієнти. Це буде сприяти «виродженню» деяких нейронів та виключенню їх з процесу навчання. Щоб уникнути такої ситуації необхідно проводити так звану нормалізацію даних – це процес перетворення всіх значень в діапазон від 0 до 1. Для цього використовуються максимальні та мінімальні значення ряду. Виникає питання: чи це дійсно всі максимальні та мінімальні можливі значення ряду. Це значення тільки поточного експерименту. При розширенні ряду максимальні та мінімальні значення зміняться. Ми не можемо передбачити ці значення. Але якщо ми будемо брати поточні максимальні та мінімальні значення у нас точно буде одне значення дорівнювати 0 а інше 1. Нульове значення зовсім не підходить для навчання, тому що помножене на ваговий коефіцієнт воно дасть 0, що приведе до виключення цього нейрону з навчання. Найкращою практикою буде зменшити та збільшити ці значення приблизно на 10 %. Таким чином, ми уникнемо нульових значень при мінімумі. Тоді в подальшому, для прогнозу та ідентифікації користувача ми можемо брати поточні дані і, можливо, вони увійдуть в цей діапазон.

Дуже часто дані «склеюються» з двох частин – авторські введення паролю, та введення паролю «зловмисником». Останні значення дописуються в кінець і тому дані не є однорідними. Відмінністю в даних буде також значення нашої цілі або мішені – це авторське або не авторське введення паролю. При авторському введені паролю ціллю буде 1 та при не авторському це буде 0. Також приймаємо гіпотезу, що при отриманні значення від 1 до 0,51 будемо вважати це авторським введенням, при значення < 0,5 – будемо вважати, що введення паролю було зроблено «зловмисником». Щоб уникнути такого розшарування даних ми проводимо перемішування даних випадковим способом не менше ніж 1000 раз. Після цього, ми відокремлюємо 20 % даних для тестування на незалежному матеріалі. А 80 % використовуємо для навчання нашої моделі. Таке розділення дозволить нам досить об’єктивно оцінити наскільки правильно наша модель може визначити авторське та не авторське введення паролю.

Навчання нейронної мережі. Після підготовки даних ми можемо провести навчання нашої нейронної мережі на різноманітних сетах даних для трьох учасників експерименту. Ми будемо навчати окремо на тих технічних характеристиках що ми визначили в таблиці 1, а також їх комбінаціями.

Для створення рівних умов всі обчислення по експериментальним даним ми будемо проводити, виходячи з наступних правил:

ISSN 2226-1893

- за функцію активації приймаємо ReLU;
- кількість епох навчання – 15 000;
- оптимізатор – Adam;
- кількість прихованих шарів – 3;
- кількість нейронів в прихованих шарах – 50, 100, 50;
- цільова функція оптимізації – середньоквадратичне відхилення δ.

Застосування ReLU в якості функції активації була вибрана з урахуванням її простоти та можливості практичного застосування результатів навчання нейронної мережі. Також постає задача зворотної нормалізації. Оскільки навчання проводять на нормалізованих даних, то для практичного застосування в моделі потрібно мати всі екстремальні значення. Спеціально для цього зберігаємо ці значення в моделі для використання та нормалізації прогностичних даних в майбутньому.

Отримані результати будемо порівнювати по двом значенням середньоквадратичного відхилення: значення δ для навчання (80% даних) і значення δ для незалежного тестування (20 % даних від загальної вибірки, які не беруть участі в навчанні). Таким чином, нам треба визначити ті технічні характеристики клавіатурного почерку, або їх комбінації, що дозволять нам отримати надійну нейронну мережу не для одного користувача, а для декількох.

Окремо потрібно зупинитися на значенні кількості нейронів в прихованих шарах. Тут думки вчених розділилися. В роботі Махершаві та Вікрама Пуді [4] використовують також 3 прихованих шари з кількістю нейронів 100, 400, 100. Це значно більше, ніж пропонуємо ми. В попередніх роботах [5] ми знайшли ті мінімальні значення, при яких нейромережа достатньо вдало працює, але з розширенням кількості учасників та значної варіабельності даних, пропонуємо все таки збільшити кількість нейронів в прихованих шарах, щоб була можливість оптимально описати складну ієрархію взаємозв'язків у різних користувачів.

Ми провели серію навчань нашої нейронної мережі та тестування на незалежному матеріалі, результати яких представлені в таблиці 2.

Як видно з таблиці 2 найкращою одинарною характеристикою, що досить точно описує наша нейронна мережа, є параметр FT – це інтервал між відпущенням поточної клавіші та натисканням наступної клавіші. Можемо звернути увагу, що не у всіх користувачів одна і та ж характристика не є визначальною. В деяких дуже мала похибка в навчанні, але вона іноді різко зростає при перевірці на незалежному матеріалі. Тому для вибору технічних характристик нам необхідно вибрати такий парметр, що давав би мінімальні значення як в ході навчання, так ів ході перевірки.

Середньоквадратичні помилки δ навчання нейронної мережі та перевірки на незалежному тесті в залежності від технічних характеристик клавіатурного почерку.

Давайте розглянемо приклад з найбільшим значенням похибки – це характеристика триграф (TG) у користувача C. На рис. 5 представлено графік актуальних значень (Actual) та вирахованих по нашій нейронній мережі (Predicted).

ISSN 2226-1893

Таблиця 2

Технічна характе-ристика почерку	Користувач А		Користувач В		Користувач С	
	δ навчання	δ перевірки	δ навчання	δ перевірки	δ навчання	δ перевірки
DT	0,00001370	0,00139200	0,00000028	0,00000590	0,00000080	0,00417800
FT	0,00001010	0,00061000	0,00000072	0,00000825	0,00000027	0,00000046
DG	0,00000533	0,05759456	0,00000011	0,00634364	0,00000117	0,06280557
TG	0,00000462	0,04276893	0,00000001	0,00015623	0,00000009	0,10465119
OT	0,00006087	0.13358385	0.00005641	0.11875949	0,00008977	0.13483899
FT+DT	0,00000262	0,00000002	0,00000038	0,00000019	0,00000006	0,05878089
FT+DG	0,00000007	0,00001523	0,00000027	0,00000137	0,00000013	0,00557712
FT+DG+TG	0,00000087	0,00000934	0,00000014	0,00000135	0,00000034	0,05577482

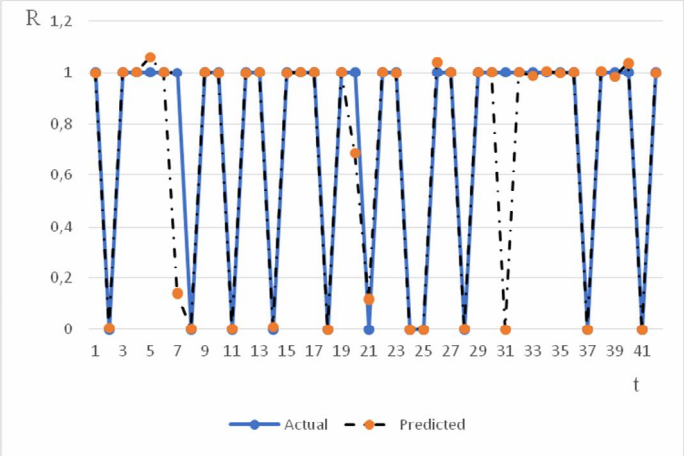


Рис. 5. Актуальні значення авторського введення паролю (Actual) та не авторське введення (Predicted) користувача С

Не співпало тільки одне значення під номером 31. Всі інші значення вписуються в нашу гіпотезу: що значення R від 0,5 до 1 – це авторське введення, а значення R менше 0,5 – не авторське введення паролю, або іншими словами введення паролю зловмисником. Практично, це графік з самою великою помилкою при перевірці на незалежному матеріалі, але вона прийнятна в нашому випадку.

Найкращий результат з урахуванням як помилки при навчанні так і помилки перевірки на незаледному матеріалі є комбінація харатеристики FT з характеристикою DT.

Використання такого поєднання дозволяє нам на наявному матеріалі говорити про доволі точний опис та розпізнавання нашої нейронної мережі. Ми не показували тут метрику точності прогнозу (accuracy), але навіть в самому поганому випадку, який ми описали вище, вона дорівнює 94.4 % що говорить про достатньо велику точність прогнозу. В інших випадках значення точності прогнозу ще вище.

ISSN 2226-1893

Висновки. В наш час нейронні мережі все частіше застосовуються в самих різноманітних областях. Тут можуть бути як побутові асистенти людини, так і навігація автомобілів чи багаторівневий кіберзахист складних інформаційних об'єктів. Використання клавіатурного почерку може забезпечити додатковий ступіть захисту наших інформаційних систем використовуючи поведінкову біометрію. Використання клавіатурного почерку не потребує додаткового обладнання, а тільки програмне забезпечення, що робить введення такої ідентифікації доволі простим.

Аналізуючи технічні характеристики клавіатурного почерку, можемо сказати, що на перше місце за інформативністю та впливом на розпізнавання клавіатурного почерку ми можемо поставити інтервал між відпущенням поточної клавіші та натисненням наступної FT (Flight Time). Ця технічна характеристика клавіатурного почерку якнайкраще характеризує поведінкову біометрію оскільки тут відслідковуються дуже багато параметрів, які вносять свій неповторний вплив в кінцевий результат:

- кількість пальців задіяних в наборі;
- швидкість набору;
- буферна пам'ять набирача паролю;
- особливості володіння правою чи лівою рукою.

Наступною за значенням технічною характеристикою, яка впливає на навчання нейронної мережі та ідентифікацію по клавіатурному почерку є час утримання клавіші (DT) – це час від натиснення клавіші та її відпущення. Ця характеристика є гарним доповненням до FT але може виступати окремою та самодостатньою характеристикою при навчанні нейронної мережі без залучення інших характеристик. Помилка при навчанні не набагато нижча ніж в FT і при обмеженому обчислювальному ресурсі може застосовуватися одноосібно.

Інтегральні характеристики диграфи та триграфи також вносять своє покращення в навчання нейронної мережі у складі інших характеристик. Недоліком цих характеристик є не велика кількість даних: при довжині паролю 6 символів диграфів буде тільки 3 значення, а триграфів взагалі тільки 2 значення. Така не значна кількість даних відчутно впливає на точність навчання нашої нейронної мережі, але може їх значно доповнювати в поєднанні з іншими технічними характеристиками.

Зовсім низькі результати показала така технічна характеристика як час перекриття OT (Overlap Time). Помилка навчання тут варіювала від 0,00005641 до 0,00008977. Це говорить про те що ця характеристика не відтворює в достатній мірі особливості клавіатурного почерку та складність міжнейронних зв'язків.

Побудована нами нейронна мережа може бути застосована в комплексних системах захисту інформаційно-телекомунікаційних систем, інтелектуальних агентів раннього сповіщення про кіберзагрози та спільного використання з firewall останнього покоління з штучним інтелектом.

Застосування ідентифікації по клавіатурному почерку може значно знизити загрозу несанкціонованої автентифікації та зменшити площину кіберзагроз.

ISSN 2226-1893

СПИСОК ЛІТЕРАТУРИ

1. Bryan, W. L., & Harter, N. (1897). Studies in the physiology and psychology of the telegraphic language. Psychological Review, 4(1), P. 27-53. – https://doi.org/10.1037/h0073806.
2. Чалая Л.Є. Модель ідентифікації користувачів по клавіатурному почерку. «Штучний інтелект», №4. 2004р., С. 811-817.
3. Shaffer L.H. Reading and Typing – https://www.researchgate.net/publication/233266615_Reading_and_Typing.
4. Saket Maheshwary, Soumyajit Ganguly, Vikram Pudi. Deep Secure: A Fast and Simple Neural Network based approach for User Authentication and Identification via Keystroke Dynamics. https://www.researchgate.net/ publication/322952671_Deep_Secure_A_Fast_and_Simple_Neural_Network_based_approach_for_User_Authentication_and_Identification_via_Keystroke_ Dynamics.
5. Даус, Ю., Самойлов, С., Даус, М., & Ларін, Д. (2025). Ідентифікація користувачів за клавіатурним почерком з використанням нейронних мереж. Вісник Одеського національного морського університету, (75), P. 212-227. https://doi.org/10.47049/2226-1893-2025-1-212-227.
6. Bishop C. M., Pattern Recognition and Machine Learning. – Springer New York, 2016 – 778 p.
7. The influence of the sigmoid function parameters on the speed of back-propagation learning / Han J., Moraga C. // Springer Berlin Heidelberg: materials Conference Computational Models of Neurons and Neural Nets. – Berlin, 1995. – P. 195-201.

REFERENCES

1. Goroshko, M.P., Myklush, S.I., Khomyuk, P.G. Biometrics – Lviv: Publishing house «Kamula», 2004. – 236 p.
2. Shaffer L.H. Reading and Typing – https://www.researchgate.net/publication/233266615_Reading_and_Typing.
3. Chalaya L.E. User identification model based on keyboard handwriting. «Artificial Intelligence», No. 4. 2004, P. 811-817.
4. Saket Maheshwary, Soumyajit Ganguly, Vikram Pudi. Deep Secure: A Fast and Simple Neural Network based approach for User Authentication and Identification via Keystroke Dynamics. https://www.researchgate.net/ publication/322952671_Deep_Secure_A_Fast_and_Simple_Neural_Network_based_approach_for_User_Authentication_and_Identification_via_Keystroke_Dynamics.
5. Daus, Y., Samoilov, S., Daus, M., & Larin, D. (2025). User identification by keyboard handwriting using neural networks. Bulletin of the Odessa National Maritime University, (75), P. 212-227. https://doi.org/10.47049/2226-1893-2025-1-212-227.

ISSN 2226-1893

6. Bishop C.M., Pattern Recognition and Machine Learning. – Springer New York, 2016 – 778 p.
7. The influence of the sigmoid function parameters on the speed of back-propagation learning / Han J., Moraga C. // Springer Berlin Heidelberg: materials Conference Computational Models of Neurons and Neural Nets. – Berlin, 1995. – P. 195-201.

Дата надходження статті: 09.02.2026
Дата прийняття статті: 06.03.2026
Дата публікації статті: 02.04.2026