

## АНАЛІЗ МЕТОДІВ ТА ПІДХОДІВ ДО ПОБУДОВИ СИСТЕМ РОЗПІЗНАВАННЯ ТА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРА НА ОСНОВІ ІНФОРМАЦІЙНИХ МОДЕЛЕЙ

© Заяць М.М., Заяць А.В., 2011

Виконано порівняльний аналіз методів та алгоритмів побудови систем розпізнавання користувачів комп'ютера за допомогою інформаційних моделей клавіатурного почерку. Визначено особливості кожного із розглянутих підходів, їх переваги, недоліки та напрями подальшого використання.

**Ключові слова:** дискретна модель, клавіатурний почерк, розпізнавання, ідентифікація, аутентифікація, біометрична система.

In this paper we present the comparative methods and algorithms analysis of computer users recognition systems construction with the help of informative keyboard handwriting models. Such analysis allows defining features of each considered approach its advantages and disadvantages as well as the directions of the expedient use.

**Key words:** discrete model, keyboard handwriting, recognition, identification, authentication, biometric system.

### Вступ. Постановка проблеми

З розвитком новітніх технологій проблема інформаційної безпеки набуває все більшої актуальності. Враховуючи різноманітність потенційних загроз інформації, складність її структури і функцій, а також участь людини в технологічному процесі обробки та збереження інформації, конфіденційності можна досягти тільки створенням комплексного захисту інформації. І одним із основних елементів такої системи захисту є підсистема, що забезпечує ідентифікацію користувача комп'ютера.

Традиційні методи ідентифікації та аутентифікації, основані на використанні карток, електронних ключів чи інших переносних ідентифікаторів, а також паролів і кодів доступу, мають істотні недоліки. Головним недоліком таких методів є неоднозначність ідентифікованої особистості. Річ у тім, що для ідентифікації використовують атрибутивні розпізнавальні характеристики. Цей недолік можна усунути, використовуючи біометричні методи ідентифікації. Біометричні характеристики є невід'ємною частиною людини і тому їх не можна забути, загубити чи передати іншому. Ще одним, не менш важливим недоліком традиційних методів ідентифікації є складність виявлення підміни ідентифікованого користувача.

Використання методів прихованого клавіатурного моніторингу дає змогу реалізувати процедури ідентифікації та аутентифікації. Підміну ідентифікованого користувача можна встановити на основі результатів процедури аутентифікації, що може провадитися безперервно. Крім цього, фактор прихованого спостереження допомагає виявити недозволених користувачів. А вплив психофізичного стану особи на клавіатурний почерк можна використати для визначення незадовільного самопочуття працівника.

### Цілі статті

Метою статті є порівняльний аналіз методів та алгоритмів, що є основою побудови автоматизованих комп'ютерних систем розпізнавання та достовірної ідентифікації користувачів комп'ютера, з метою підвищення точності їх розпізнавання та забезпечення автоматизації процесу ідентифікації користувачів. В роботі також визначено особливості та напрями доцільного використання таких методів.

## **Виклад основного матеріалу**

**Огляд попередніх результатів.** Біометрична система ідентифікації – це сукупність автоматизованих методів і засобів ідентифікації людини на основі дослідження її унікальних фізіологічних та поведінкових характеристик [16].

Різноманітні проблеми створення біометричних систем динамічної ідентифікації розглянуто у роботах В.А. Герасименко, С.Г. Гришина, А.І. Иванова, Н.Н. Куссуля, В.В. Мельникова, А.С. Піскарьова, А.А. Стогнія, В.П. Широчина, Л.Е. Чалої, М.Н. Казаріна, J. Chomicki, D. Denning, M. Gertz, B.G. Lindsay, U.V. Lipeck, F. Monroe, A. Rubin та інших вчених.

Сьогодні виділяють два великі класи біометричних систем ідентифікації користувачів інформаційних систем – статичний та динамічний. Перший клас методів використовується для розробки біометричних систем, що аналізують статичні, незмінні характеристики особи, тобто особливості геометрії обличчя, руки, відбитків пальців. До другого класу належать біометричні методи, що аналізують динамічні, поведінкові характеристики особи. Вони досліджують динаміку відтворення контрольного слова за допомогою рукописного чи клавіатурного почерку чи навіть голосу користувача.

До динамічних методів біометричної ідентифікації особи в першу чергу належать методи ідентифікації за голосом, рукописним чи клавіатурним почерком. Порівняно низька вартість систем динамічної біометрії зумовлена тим, що вони використовують стандартні комп'ютерні засоби мультимедіа (наприклад, стандартний графічний планшет чи стандартну звукову карту). Статичний образ особи (відбитки пальців) неможливо зберегти в секреті чи змінити. Образи динамічної біометрії, навпаки, легко змінити і зберегти в таємниці. Остання властивість особливо важлива для ідентифікації особистості у відкритому інформаційному просторі. Недоліком цього класу біометричних методів є вплив психофізичного стану особи та зовнішніх факторів на роботу. Незважаючи на це, системи динамічної біометрії дуже ефективні, оскільки поведінкові навички людини (вроджені чи пов'язані з професійною діяльністю) залишаються стабільними протягом декількох десятиліть.

У класі динамічних систем особливе місце займають системи на основі клавіатурних методів ідентифікації. Ще в 80-х роках минулого століття велись дослідження особливостей динаміки клавіатурного набору з метою ідентифікації. Вперше в своїй роботі Гейнс [19] використовував час натискання клавіш для процедури ідентифікації. Хоч в експерименті брало участь лише сім секретарів, Гейнс отримав практичне підтвердження того, що у людини, яка довгий час працює за клавіатурою, виробляється так званий клавіатурний почерк. Подібний експеримент здійснив Леггет [8], але уже з групою програмістів, отримавши аналогічний результат. Тобто експериментально доведено існування особливостей динаміки роботи на клавіатурі у користувачів, що працюють за комп'ютером довгий час.

Популярність динамічних систем ідентифікації за допомогою клавіатурного почерку пояснюється тим, що вони мають низьку вартість – лише витрати на додаткове програмне забезпечення. Крім того, сьогодні ця технологія може однаково успішно використовуватись в таких напрямках:

- для ідентифікації користувача, що претендує на доступ до комп'ютерної системи;
- для аутентифікації користувача комп'ютерної системи;
- для прихованого клавіатурного моніторингу користувача комп'ютерної системи.

### **Математичні методи розпізнавання клавіатурного почерку**

Клавіатурним почерком користувача називатимемо сукупність індивідуальних характеристик, що визначають особливості його роботи в режимі введення тексту з клавіатури (наприклад, час утримання клавіші, час між натисканнями клавіш, частота використання функціональних клавіш тощо) [11].

Зрозуміло, що високої швидкості введення інформації з клавіатури можна досягти, використовуючи усі пальці обох рук. У кожної людини з'являється свій унікальний клавіатурний почерк. Традиційно доступ до інформації обмежують за допомогою введення паролльної фрази. При вводі

парольної фрази з клавіатури відбуваються події натискання і відпускання клавіш, котрі дають змогу зафіксувати час утримання кожної клавіші натиснутою і інтервал часу між натисканням клавіш [16].

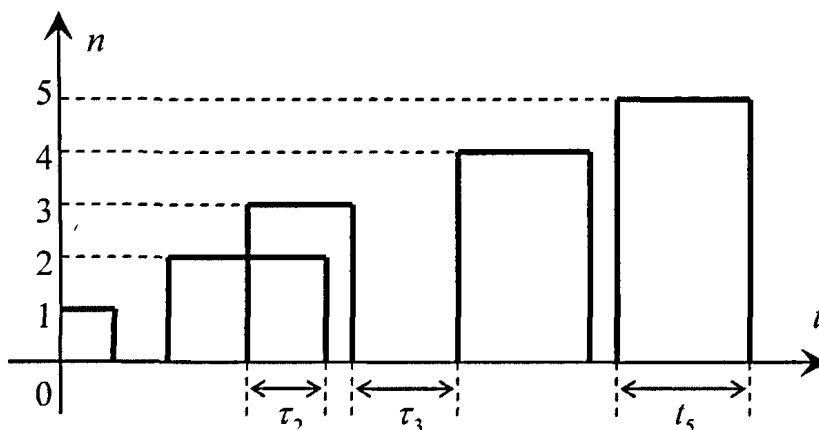


Рис. 1. Часова діаграма вхідних даних

На рис. 1 схематично зображено часову діаграму вхідних даних, де:  $t_i > 0$  – час утримання  $i$ -ї клавіші натиснутою,  $\tau_j > 0$  – час паузи між натиснутими сусідніми клавішами,  $\tau_j < 0$  – час перекриття.

Від’ємне значення паузи  $\tau_j < 0$  відповідає часу перекриття, яке виникає у разі одночасного натискання двох клавіш. З рис. 1 видно, що час утримання клавіш  $t_1, t_2, \dots, t_N$  та інтервал часу між натисканнями  $\tau_1, \tau_2, \dots, \tau_{N-1}$  можуть бути різними і, відповідно, значення цих параметрів можуть використовуватися для виявлення характерних особливостей індивідуального клавіатурного почерку. Ці параметри дуже суттєво залежать від того, скільки пальців використовує користувач у наборі, від характерних для користувача співвідношень руху різних пальців руки і від характерних рухів при наборі. В процесі переходу до сліпого набору тексту всіма пальцями обох рук дуже істотно проявляється індивідуальність клавіатурного почерку користувача.

Задачу ідентифікації можна розділити на декілька етапів, основними з яких є навчання системи і розпізнавання. Очевидно, для організації процесу розпізнавання система визначає та запам’ятовує у базі даних значення часових характеристик зареєстрованих користувачів. На основі значень цих параметрів створюються зразки (шаблони) почерку користувачів комп’ютера [5]. Для ідентифікації об’єкта система порівнює зразок почерку на основі введених даних з шаблоном, збереженим в базі даних.

Отже, в процесі біометричної ідентифікації можна виділити такі етапи:

- введення тексту з клавіатури об’єктом розпізнавання;
- визначення біометричних характеристик користувача;
- створення біометричного зразка почерку;
- порівняння отриманого зразка почерку зі збереженими в базі даних.

Огляд методів ідентифікації користувача комп’ютера дає змогу виділити чотири основні математичні підходи до розв’язання задачі розпізнавання клавіатурного почерку:

- статистичний;
- ймовірно-статистичний;
- на базі теорії розпізнавання образів та нечіткої логіки;
- на основі нейронних мереж.

Суть першого методу полягає в тому, що під час реєстрації користувачів в системі відбувається збір статистики у вигляді обчислених параметрів особливостей динаміки роботи на комп’ютері. Після цього знаходять середнє значення статистичних даних, які і вважаються

біометричним еталоном користувача. В режимі ідентифікації користувача знову вводиться ключова фраза, котра порівнюється з отриманим біометричним еталоном. Порівняння відбувається за допомогою знаходження коефіцієнта близькості одним із відомих методів. Зазвичай такий підхід використовують для ідентифікації за допомогою паролльної фрази.

Другий підхід спирається на теорію ймовірності та математичну статистику. Відмінністю цього методу від попереднього є те, що час натискання і відпускання клавіш під час набору тексту на клавіатурі розглядають як ймовірнісні події. Вважається, що значення часу натискання і пауз між натиснутими клавішами розподілені за нормальним законом.

Наступним поширеним математичним підходом до розв'язання задачі розпізнавання клавіатурного почерку є використання різних алгоритмів теорії розпізнавання образів і нечіткої логіки. Більшість цих алгоритмів спирається на правило Байєса та його модифікації.

Використання нейронних мереж також є перспективним підходом у системах розпізнавання клавіатурного почерку. Проте для навчання нейронних мереж потрібні значні обчислювальні ресурси. Ще один недолік їх використання пов'язаний з процесом реєстрації нового користувача в системі. В цьому випадку потрібне повторне навчання мережі.

Одним з простих і поширених способів представлення біометричних характеристик є метод матриць середніх значень [18]. Цей метод відображення біометричних характеристик базується на припущенні, що значення часових характеристик натискання клавіші підпорядковується нормальному закону. Отже, нехай значення часу утримання клавіші з кодом  $C_k$  утворює скінченну множину значень  $T_k = \{t_1^k, t_2^k, \dots, t_l^k\}$ , де,  $l > 0$ ,  $k \in [1, M]$ . Значення пауз між натиснутими сусідніми клавішами з кодом  $C_k$  і  $C_i$ ,  $k, i \in [1, M]$  утворюють множину  $\Theta_{ki} = \{\tau_1^{ki}, \tau_2^{ki}, \dots, \tau_m^{ki}\}$ ,  $m > 0$ ,  $i \in [1, M]$ , тоді множина  $\Theta_k = \{\Theta_{k1}, \Theta_{k2}, \dots, \Theta_{kM}\}$  містить всі значення пауз між натиснутою клавішею  $C_k$  та іншими клавішами. Отже, вхідну часову послідовність можна розглядати як множину  $\Omega = \{\Psi_1, \Psi_2, \dots, \Psi_M\}$ , де  $\Psi_k = \{T_k, \Theta_k\}$  – множина значень часу утримання клавіші з кодом  $C_k$  та пауз між цією і всіма іншими натиснутими клавішами.

Для отриманої вибірки знаходимо математичне сподівання, дисперсію та середньоквадратичне відхилення значень часу утримання для кожної клавіші  $C_k$ .

$$M(T_k) = \frac{1}{l} \sum_{i=1}^l t_i^k, \quad (1)$$

$$D(T_k) = \frac{1}{l-1} \sum_{i=1}^l (t_i^k - M(T_k))^2, \quad (2)$$

$$\sigma_k^T = \sqrt{D(T_k)}. \quad (3)$$

Аналогічно за допомогою формул (4–6) знаходимо математичне сподівання, дисперсію та середньоквадратичне відхилення значень пауз між двома утриманими клавішами  $C_k$  та  $C_i$ .

$$M(\Theta_{ki}) = \frac{1}{m} \sum_{j=1}^m \tau_j^{ki}, \quad (4)$$

$$D(\Theta_{ki}) = \frac{1}{m-1} \sum_{j=1}^m (\tau_j^{ki} - M(\Theta_{ki}))^2, \quad (5)$$

$$\sigma_{ki}^O = \sqrt{D(\Theta_{ki})}. \quad (6)$$

Отримані значення в формулах (1) – (6) утворюють дві матриці середніх значень  $F$  і  $R$ . Перша матриця  $F$  розміром  $M \times M$  – діагональна, на головній діагоналі розміщені оцінки математичного сподівання та середньоквадратичне відхилення часу утримання кожної клавіші.

$$F = \begin{bmatrix} M(T_1), \sigma_1^T & 0 & \dots & 0 \\ 0 & M(T_2), \sigma_2^T & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & M(T_M), \sigma_M^T \end{bmatrix}$$

Друга матриця  $R$  розміром  $M \times M$  містить оцінки математичного сподівання та середньоквадратичне відхилення пауз між утриманням кожної клавіші з іншою.

$$R = \begin{bmatrix} M(\Theta_{11}), \sigma_{11}^T & M(\Theta_{12}), \sigma_{12}^T & \dots & M(\Theta_{1M}), \sigma_{1M}^T \\ M(\Theta_{21}), \sigma_{21}^T & M(\Theta_{22}), \sigma_{22}^T & \dots & M(\Theta_{2M}), \sigma_{2M}^T \\ \dots & \dots & \dots & \dots \\ M(\Theta_{M1}), \sigma_{M1}^T & M(\Theta_{M2}), \sigma_{M2}^T & \dots & M(\Theta_{MM}), \sigma_{MM}^T \end{bmatrix}$$

Використання описаного методу представлення біометричних характеристик дає високі показники в системах аутентифікації за допомогою паролльної фрази [18].

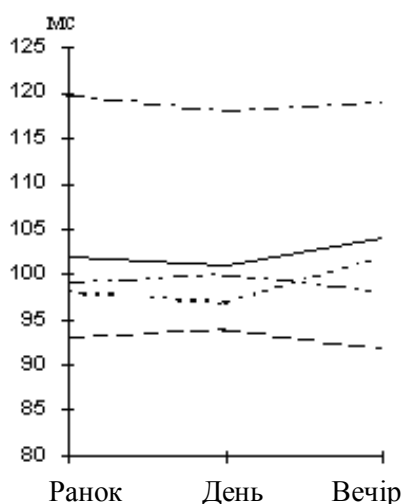


Рис. 2. Динаміка зміни часу утримання клавіш користувачами 1-5 в різний час

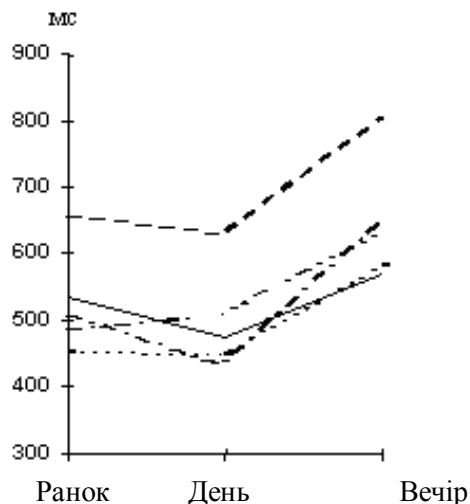


Рис. 3. Динаміка зміни пауз між натисканнями клавіш користувачами 1-5 в різний час

Класичний статистичний підхід розпізнавання за клавіатурним почерком під час набору ключових слів виявив цікаві особливості: суттєва залежність почерку від послідовності букв у слові; існування зв'язку при наборі окремих символів; наявність “затримок” під час введення певних символів. Крім того, виявляється, найактивніше певний користувач працює в середині робочого дня (символічна назва “День”), трошки повільніше – зранку і набагато повільніше – ввечері [17]. Динаміку зміни середнього часу утримання клавіш п'ятьма користувачами в різний період доби подано на рис. 2, а динаміку зміни середніх інтервалів часу між натисканнями клавіш користувачами 1-5 в різний період доби – на рис. 3. В процесі дослідження клавіатурного почерку розглянуто дві моделі біометричної аутентифікації користувачів: з мультиплікативним та з адитивним способом порівняння біометричних характеристик.

Побудова першої моделі біометричної аутентифікації полягає в аналізі відношень нових біометричних характеристик до відповідних еталонних значень, тобто відношення часу утримання клавіш до еталонних зразків, і час пауз між натисканнями клавіш до відповідних еталонних значень. Всі відношення, що лежать у межах допустимих значень, обнуляють, а ті, що залишилися за межею допустимих значень, – залишаються незмінними і є так звані вершинами мультиплікативної характеристики. Така процедура обробки даних називається мультиплікативним фільтром.

$$m_{\min}^i \leq m^i \leq m_{\max}^i, \quad (7)$$

де  $m^i = \frac{t_{ym}^i}{T_{ym}^i}$ ,  $m_{\min}^i$ ,  $m_{\max}^i$  – нижня та верхня межі мультиплікативного фільтра.

Після цього загальну кількість утримань  $i$ -ї клавіші, порівняльні характеристики якої стали піковими, тобто не ввійшли в межі нерівності (10), підсумовують і перевіряють згідно з таким правилом:

$$M_{\min}^i \leq \frac{K_{ym}^i}{N_{ym}^i} \cdot 100 \leq M_{\max}^i \quad (8)$$

де  $K_{ym}^i$  – кількість утримань  $i$ -ї клавіші, порівняльні характеристики якої не ввійшли в межі нерівності (7);  $N_{ym}^i$  – загальна кількість утримань  $i$ -ї клавіші в процесі створення порівняльних характеристик;  $M_{\min}^i, M_{\max}^i$  – мінімальне та максимальне допустимі значення вершин для  $i$ -клавіші в процентах.

Аналогічно для дослідження часових інтервалів між натиснутими клавішами використовуються такі математичні вирази:

$$m_{\min}^n \leq \frac{t_{in}^n}{T_{in}^n} \leq m_{\max}^n, \quad (9)$$

$$M_{\min}^n \leq \frac{K_{in}^n}{N_{in}^n} \cdot 100 \leq M_{\max}^n. \quad (10)$$

Експериментальні дослідження мультиплікативного фільтра показали, що дисперсія відхилення часу утримання клавіш є малою щодо дисперсії відхилень міжсимвольних інтервалів.

Недоліком мультиплікативного підходу є те, що результати розпізнавання користувача є найдостовірнішими в період ранок-день, чого не можна сказати про ранок-вечір.

Механізм адитивного порівняння характеристик полягає в тому, що від інтервалів між натисканнями клавіш однієї матриці віднімають відповідні еталонні значення другої матриці. Якщо результат менший від нуля, то порівнюваний час менший від еталонного, а якщо результат більший від нуля – то більший. Відхилення від еталонного значення виражатиметься у відсотках, причому відхилення є позитивним, якщо відношення більше від нуля, і від’ємним в протилежному випадку. Після отримання результатів адитивної характеристики всі відхилення, що лежать в межах допустимих значень відхилень, обнуляють, а ті відхилення, що залишилися за межами допустимих значень, – залишаються незмінними і є так звані вершинами адитивної характеристики. Ця процедура називається адитивним фільтром.

Порівняння часових характеристик утримання  $i$ -ї клавіші і відповідного їй еталонного значення виконують за допомогою адитивного фільтра (11):

$$a_{\min}^i \leq a^i \leq a_{\max}^i. \quad (11)$$

Після цього загальна кількість утримань  $i$ -ї клавіші, порівняльні характеристики якої не ввійшли в межі нерівності (11), підсумовують і перевіряють згідно з таким правилом:

$$A_{\min}^i \leq \frac{K_{ym}^i}{N_{ym}^i} \cdot 100 \leq A_{\max}^i. \quad (12)$$

Для дослідження часових інтервалів між натиснутими клавішами математичні вирази будуть аналогічними:

$$a_{\min}^n \leq a^n \leq a_{\max}^n, \quad (13)$$

$$A_{\min}^n \leq \frac{K_{in}^n}{N_{in}^n} \cdot 100 \leq A_{\max}^n. \quad (14)$$

Як для співвідношень часу утримання клавіш, так і для співвідношень інтервалів між натисканнями клавіш прослідковується тенденція достовірнішого розпізнавання користувача. Недоліком адитивної фільтрації є те, що якість розпізнавання користувача є вищою лише в період ранок-вечір.

Ідея об'єднання мультиплікативного та адитивного підходів привела до створення мультиплікативно-адитивного механізму порівняння біометричних характеристик користувачів.

У роботах [1, 2, 5] для побудови системи розпізнавання особи за її рукомоторними реакціями сформульовано і проаналізовано значну кількість характеристик, які містять первинну інформацію про користувача комп'ютера і вибрано такі найінформативніші характеристики:

1) відносна девіація паузи перед клавішею – розподіл відносних відхилень паузи перед цією клавішею до середнього значення паузи перед всіма клавішами у заданій неперервній послідовності набору

$$DevB = \frac{t_i - t_{cp}}{t_{cp}} \cdot 100\%, \quad (15)$$

де  $t_i$  – тривалість паузи перед  $i$ -ю клавішею;  $t_{cp}$  – середня тривалість паузи перед клавішами в послідовності набраного тексту;

2) відносна девіація утримання клавіші – розподіл відносних відхилень тривалості утримання натиснутою клавіші до середньої тривалості утримання клавіші у заданій неперервній послідовності

$$DevP = \frac{t_i - t_{cp}}{t_{cp}} \cdot 100\%; \quad (16)$$

3) відносна девіація паузи після клавіші – аналогічна до попередньої характеристики:

$$DevA = \frac{t_i - t_{cp}}{t_{cp}} \cdot 100\%; \quad (17)$$

4) відношення величини паузи перед клавішею до тривалості утримання клавіші;

5) відношення величини паузи перед клавішею до величини паузи після клавіші;

6) відношення величини паузи після клавіші до тривалості утримання клавіші;

7) розподіл частот використання клавіш зміни регістра.

Загалом у роботі [2] розглянуто 18 характеристик, але найінформативнішими є вищенаведені.

На основі практичних експериментів з розпізнавання з першою групою характеристик, в яку об'єднано перші шість, досліджувалися помилки другого роду. Окремі гіпотези система перевіряла з рівнем значущості  $\alpha = 0.05$ . Так отримано ймовірності помилок другого роду 35 %, 13 %, 20 %, 27 %, 32 %, 78 %. Ці ймовірності помилок визначено для порівняно невеликої кількості експериментів з ідентифікації (105 експериментів). Для великої групи людей ймовірності помилок можуть дещо відрізнятись від наведених.

Під час тестування розробленої системи на досліджуваних об'єктах допущено лише чотири помилки на 108 розпізнавань (запропоновано два схожих на об'єкт класи, один серед яких був правильним).

### **Напрями модифікації та застосування дискретних моделей коливних систем до аналізу динаміки складних об'єктів**

Результати порівняльного аналізу методів та підходів до побудови комп'ютерних систем ідентифікації та розпізнавання користувачів комп'ютера підтверджують доцільність використання дискретних моделей для розв'язання широкого класу прикладних проблем, пов'язаних з розпізнаванням складних динамічних режимів, у системах розпізнавання об'єктів.

Розроблено метод формування первинних ознак у безрозмірній приведеній формі при побудові комп'ютерної системи розпізнавання користувачів комп'ютера та запропоновано алгоритми реалізації такої системи на основі використання дискретних моделей, що зв'язують тривалості пауз до і після натискання клавіш комп'ютера з часом утримання клавіші під час введення інформації з клавіатури комп'ютера. Їх з успіхом можна використовувати для процедури розпізнавання користувача, визначення психофізичного стану персоналу за клавіатурним почерком, а також для захисту комп'ютера від несанкціонованого доступу.

Цей метод також застосовують і для підвищення надійності роботи системи захисту інформації за рахунок достовірного розпізнавання (похибка не перевищує 5 %) та ідентифікації користувача комп'ютерної техніки [12, 13]. У цій системі захисту інформації передбачено механізм її адаптації до змін почерку зареєстрованих користувачів системи за допомогою систематичного оновлення зразків їх почерку за умови зменшення часових витрат на створення зразка. Запропонована система захисту інформації від несанкціонованого доступу має ще ту перевагу, що не створює додаткових незручностей під час роботи за комп'ютером, оскільки не потребує додаткових часових витрат на ідентифікацію.

Цю систему, з несуттєвою модифікацією, можна ефективно застосувати і для розв'язання задач медичної діагностики та створення біометричних вимірювальних систем [14]. Адже очевидно, що рукомоторні реакції людини, а значить, і клавіатурний почерк змінюються при зміні психофізіологічного стану. Цей стан визначається особливостями підсвідомих рухів людини незалежно від форми її діяльності. Порівняно з методами визначення стану працівника, які використовують у промисловості, методи клавіатурного почерку мають такі переваги:

- введення інформації з клавіатури комп'ютера є найприроднішим способом роботи оператора автоматизованого робочого місця (АРМ);
- для отримання інформації про зміни у клавіатурному почерку оператора АРМ протягом зміни потрібен лише лічильник часу і контролер обробки сигналу від пристрою введення інформації.

Отже, істотні зміни клавіатурного почерку протягом робочої зміни є підтвердженням змін у психофізіологічному стані працівника.

Використання методів прихованого клавіатурного моніторингу дасть змогу:

- вирішувати проблему виявлення підміни користувача автоматизованих інформаційно-управлінських систем;
- виявляти користувачів, що пошкоджують автоматизовані системи;
- виявляти часткові психофізичні відхилення користувача від його нормальної поведінки, що виникають в результаті стресів, хворобливого стану, поганого самопочуття;
- провадити професійний відбір користувачів.

Також доцільно застосовувати описаний метод для побудови системи розпізнавання рукописних літер, алгоритм та архітектуру якої описано в роботах [20 – 21], на основі структурного підходу. Очевидно, тут варто відштовхуватися не від структури написання літери, а будувати систему розпізнавання за напрямком руху руки (рух зверху вниз і в зворотному напрямку, рух зліва направо і в зворотному напрямку) та з часу написання літери. Оцінивши математичне сподівання часу написання кожної літери, характерне для кожного користувача, можна реалізувати процедуру розпізнавання. З математичного погляду, з урахуванням напрямку руху руки, це буде дискретна система 12-го порядку.

Цей інтервально-часовий підхід до формування первинних інформативних ознак про об'єкти чи процес дослідження, орієнтований на використання дискретних моделей, з успіхом можна застосувати для побудови систем захисту інформації, медичної діагностики, біометричних систем, розв'язання транспортних задач, опрацювання потоків даних та створення інтелектуальних баз знань.

### Висновки

У роботі виконано порівняльний аналіз методів формування первинних ознак при побудові комп'ютерних систем ідентифікації та розпізнавання користувачів комп'ютера. Відзначено особливості їх застосування, способи модифікації, з метою підвищення точності ідентифікації та забезпечення достовірності розпізнавання користувачів на основі використання дискретних моделей, що зв'язують тривалості пауз з часом утримання клавіш при введенні інформації з клавіатури.

1. Заяць В.М. Построение и анализ модели дискретной колебательной системы / В.М. Заяць // Кибернетика и системный анализ. – 2000. – С. 161–165. 2. Заяць В.М. Математичний опис системи розпізнавання користувача комп'ютера / В.М. Заяць, М.М.Заяць // Зб. "Фізико-математичне

модельовання та інформаційні технології". – Львів. – 2005. – Вип. 1.– С. 146–152. 3. Фукунага К. Введение в статистическую теорию распознавания / К. Фукунага.– М.: Наука, 1979. – 512 С. 4 Горелик А.Л. Методы распознавания / А.Л. Горелик, В.А. Скрипник. – М.: Высшая школа, 1989. – С.232. 5. Заяць В.М. Визначення пріоритету детермінованих ознак при побудові системи розпізнавання об'єктів / В.М.Заяць, О.Шокира // Зб. праць науково-практичної конф. ЛДІНТУ імені В. Чорновола "Математичне моделювання складних систем". – 2007. – С.135–137. 6. Заяць В.М. Архітектура подіє-орієнтованих систем на прикладі системи розпізнавання рукописного тексту / В.М.Заяць, Д.О. Іванов // Вісник НУ „Львівська політехніка” „Комп'ютерна інженерія та інформаційні технології”. – Львів. – 2004. – № 530. – С. 78–83. 7. Томашевський О.М. Методи та алгоритми системи захисту інформації на основі нейромережових технологій. Автореф. дис... к-та техн. наук: 05.13.23. / О.М.Томашевський – Львів, 2002. – С.20. 8.Leggett J. Verifying identity via keystroke characteristics / J. Legget, G. Willams // International journal of Man-Machine Studies.– 1988 – V. 28, n.1.– P. 67-76. 9. Cohell O. Biometric Identification System Based in Keyboard Filtering / O. Cohel., J.Badia,G. Torres // Proc. Of XXXIII Annual IEEE International Carnahan Conference of Security Technology/– 1999.– P. 203-209. 10. Kittler J. On Combining Classifiers / J. Kittler M., Hatef R. Duin, J. Matas // IEEE Trans. Pattern Anal. Mach. Intell., IEEE Computer Society. – 1998. – Vol. 20. – P. 226–239. 11. Чалая Л.Є. Сравнительный анализ методов аутентификации пользователей компьютерных систем по клавиатурному почерку / Л.Э. Чалая // Системи обробки інформації.– Вип. 1 (68).– С. 108-116. 12. Вовк О.Б. Проблеми захисту шрифтів як специфічних об'єктів авторського права / О.Б. Вовк // Вісник НУ „Львівська політехніка” "Інформаційні системи та мережі". – 2008. – № 610. – С.85–83. 13. Платонов А.В. Використання експертних ситуативних моделей у сфері державної безпеки / А.В. Платонов, І.В. Баклан, К.В. Крамер // Зб. праць міжнар. наукової конф. ISDMCI' 2008.-Том 1, Євпаторія. – 2008. – С. 39–43. 14. Суздальцев А.И. Определение психофизического состояния оперативного персонала по клавиатурному почерку на нефтеперерабатывающих мини-заводах / А.И. Суздальцев, В.А. Лобанова, В.Г. Абашин // Нефтегазовое дело.– 2006.– С. 1-6. 15. Zayats V. Structural method of hand-written text recognition / V.Zayats, D.Ivanov // Pros. International Conf. "The experience of designing and application of CAD systems in microelectronics". – Lviv–Polyana. – 2005. – P. 493–494. 16. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений. – Пенза: ПТУ, 2000. – 188 с. 17. Широкин В.П. Динамическая аутентификация на основе анализа клавиатурного почерка / В.П.Широкин, А.В. Кулик, В.В. Марченко // Вісник НТУ України «Київський політехнічний інститут» – «Інформатика, управління та обчислювальна техніка». – 1999. – № 32. 18 . Брюхомицький Ю.А. Метод биометрической идентификации по клавиатурному почерку на основе разложения Хаара и меры близости Хемминга./ Ю.А. Брюхомицький , М.Н. Казарин // 19. Gaine R. Autentication by keystroke timing: some preliminary results / Gaine. R., Lisovski W., Press S. // Rand Rep. R-2560-NSF, Rand Corporation, 1980.