ш

УДК 004.94+519.21

Ш їш \.м>

АЛГОРИТМ РОБОТЩ^^^І' ІМИ АУТІ'НТИФІКАЦІЇ ОСОІНЗА ДИНАМІЧНО ВВЕДЕН®^ ПІДПИСОМ У ІНФОРМАЦІЙНІЙ ^ Щ ж м і

ТернопілйШ ийлержавнийІтехнічний університет

Стаття присвячена р(ЯШшШВшшІ^ шоботи системи аутентификації за динамічно введеним підписом, зок/к иі-Жпщ.і питання розробки математичної моделі динамічно введеного підпису шшнтОн ішгЯобробки, вибору діагностичних ознак особи у інформаційній системі і коитіїїїїьщ 'ш іітз якими проводиться аутентифікація. На основі запропонованих алгоритміШЇЩух'Тоито систему аутентифікації, наведено результати її Щоботи.

Аутентифікація особи у сучасних В Ф^пи5л]Я щЧу-*-1уЗп,і В ||Я їр ‘ серед НИХ 0.60(5.1иве Н ш іс'»цВ |иіО ІЬ]И В е\1 И® 6~1№доі<пЙ-ЧІІїї Ш^^ЯІТіткІп.пі особи. Зокрема, системи, шішВ}> нмвсЯна ііуйім ифікації особи за П!и|Ш ііч11о»нУслСГмітеїЩ іТтш)\ІІ(т-\тмт.\Я і \Ж1к оЖЙЩки, ІІІ ііиЯ Ш ііМ І, Ш^дашіГов'й ІІ,- :і» Я щ івдюіі. ПрВю епня комп'ютерних исД м. Керування якими здійснюється за допомогою пергиртилуса): кишенькових ПК Япланшетних ПК *{ТаЬІеі* РСіда^ЯНгашііїї і т.п., а також графічних планшетів сприяє розширенню потенційних Шоживачів систем аутентифікації за динамічно введеним Підписом.

Розробка систем аутентифікації особи за динамічно введеним підписом є актуальною науково-технічною задачею. Успішна реалізація такої системи можлива за умови чіткого математичного підходу: математична модель—алгоритм—програмне забезпечення. Створення алгоритму роботи системи включає розробку:

- математичної моделі досліджуваного об'єкта - динамічно введеного підпису;
- методів його обробки, в рамках цієї моделі, з метою отримання репрезентативних для особи, що проходить аутентифікацію діагностичних ознак;
- критеріїв прийняття рішень про допуск особи у інформаційну систему на основі отриманих діагностичних ознак.

Рис. 1. Реалізації статичних підписів однієї особи

Під динамічним підписом розуміємо залежність координат x та y положення пера графічного планшету від часу. У результаті відтворення особою свого підпису, в ЕОМ формується два впорядкованих по часовій координаті масиви: /х(Ф =Ї7у ; та *{у{ф =й м щ* що і с дискретним динамічним підписом особи. *Підкреслимо, що з динамічного підпису можна отримати статичний підпис, проте з статичного однозначно отримати динамічний не можливо.* З точки зору користувача динамічний підпис виглядає як звичайний статичний(Рис. 1). На Рис. 2 подано три реалізації динамічного підпису компоненти х(?) та *ш* , які відповідають вищенаведеному статичному підпису (Рис. 1). Одиниці вимірювання часу - мілісекунди *(те),* одиниці вимірю-

вання значень координат x і y – екранні точки (пікселі, *pt*).

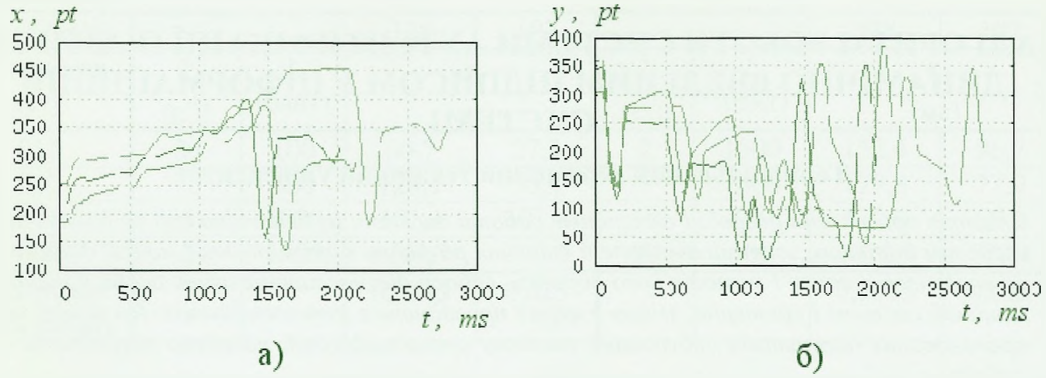

Рис. 2. Графіки трьох реалізацій динамічного підпису за зміною координати x і y у часі

Побудова математичної моделі підпису є первинним і визначальним етапом. Математична модель має адекватно відображати суттєві для задач аутентифікації ознаки динамічно введеного підпису, а також має бути простою та зручною у своєму використанні. Лише на основі математичної моделі динамічного підпису, можна коректно обгрунтувати діагностичні ознаки та розробити методи їх оцінювання, що лежатимуть в основі алгоритмів роботи комп'ютерної системи аутентифікації.

Оскільки, при повторному відтворенні тією ж особою свого підпису його реалізації не будуть співпадати, (хоча будуть подібними), то доцільним є використання стохастичного підходу до побудови його математичної моделі.

Математична модель динамічного підпису особи в рамках стохастичного підходу наведена у роботі [1]. Модель динамічного підпису – вектор двох конструктивно заданих випадкових процесів:

$$\Theta(\omega,t)=\{\xi(\omega,t),\eta(\omega,t)\},\quad \omega\in\Omega,\ t\in[0,\infty), \tag{1}$$

де Ω - множина елементарних подій певного імовірнісного простору. Випадкові процеси $\xi(\omega,t)$ і $\eta(\omega,t)$ відображають часову структуру траєкторії руху пера вздовж осей x та y в часі:

$$\xi(\omega,t)=A_\xi(\omega)\cdot\xi_0(\omega,\alpha_\xi(\omega)\cdot t)+B_\xi(\omega),\quad t\in[0,\infty),\ \omega\in\Omega, \tag{2}$$

$$\eta(\omega,t)=A_\eta(\omega)\cdot\eta_0(\omega,\alpha_\eta(\omega)\cdot t)+B_\eta(\omega),\quad t\in[0,\infty),\ \omega\in\Omega, \tag{3}$$

де $A_\xi(\omega)$ і $A_\eta(\omega)$ – випадкові величини, які враховують варіацію підпису;

$\xi_0(\omega,t)$ і $\eta_0(\omega,t)$ - випадкові процеси, що відповідають компонентам інваріантного підпису;

$\alpha_\xi(\omega)$ і $\alpha_\eta(\omega)$ - випадкові величини, що відображають мінливість тривалості написання динамічного підпису;

$B_\xi(\omega)$ і $B_\eta(\omega)$ – випадкові величини, які враховують тренд динамічного підпису і рівні координатам (x,y) положення пера на площині планшету в початковий момент часу.

В рамках математичної моделі (1)-(3) розроблено методи попередньої і статистичної обробки [1,2]. Методи попередньої обробки зводяться до відшукання компонент конструкції (1)-(3): $A_\xi(\omega)$ і $A_\eta(\omega)$, $B_\xi(\omega)$ і $B_\eta(\omega)$, $\alpha_\xi(\omega)$ і $\alpha_\eta(\omega)$, $\xi_0(\omega,t)$ і $\eta_0(\omega,t)$.

Випадкові коефіцієнти $B_\xi(\omega)$ і $B_\eta(\omega)$ відображають зсув усіх реалізацій до спільної початкової точки – початку координат:

$$B_\xi(\omega)=\xi(\omega,0),\ B_\eta(\omega)=\eta(\omega,0). \tag{4}$$

Випадковий масштабуючий коефіцієнт $\alpha(\omega)$ обчислюється за наступним співвідношенням:

$$\alpha(\omega_i)=\frac{1}{t(\omega_i)},\ \omega_i\in\Omega, \qquad (5)$$

де $t(\omega_i)$ - тривалість i-го підпису з усієї множини реалізацій підписів. Даний масштабний коефіцієнт є однаковим як для процесу $\xi(\omega,t)$, так і для процесу $\eta(\omega,t)$ відповідно, оскільки, він визначається тривалістю відтвореного підпису ($\alpha_\xi(\omega)=\alpha_\eta(\omega)=\alpha(\omega)$).

Масштабування за діапазоном варіації (розмахом) дозволяє привести підписи до однакового діапазону їх варіації. Для цього використано масштабні коефіцієнти $A_\xi(\omega)$, $A_\eta(\omega)$, які можна знайти за наступними співвідношеннями:

$$A_\xi(\omega)=\frac{1}{Var\xi(\omega,t)}=\frac{1}{\left|max_{\xi(\omega,t)}-min_{\xi(\omega,t)}\right|}, \qquad (6)$$

$$A_\eta(\omega)=\frac{1}{Var\eta(\omega,t)}=\frac{1}{\left|max_{\eta(\omega,t)}-min_{\eta(\omega,t)}\right|}, \qquad (7)$$

Здійснивши дану операцію над координатами x і y, підпис у цілому буде унормований у вікні $(-1,1)$. А варіація кожного підпису з множини усіх реалізацій буде рівна 1.

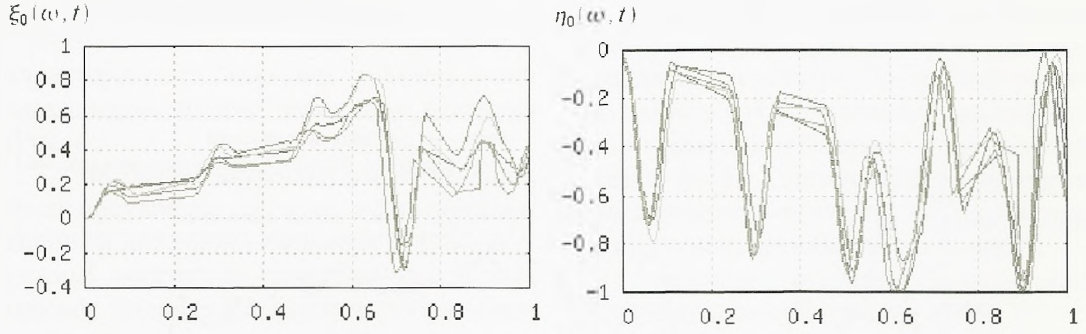

Рис. 3. Реалізації процесів $\xi_0(\omega,t)$ і $\eta_0(\omega,t)$ - компонент інваріантного підпису особи

Врахування вищенаведених коефіцієнтів дозволяє нам ввести деякий ***інваріантний підпис***, який подано у вигляді вектора $\Theta_0(\omega,t)$ двох випадкових процесів $\xi_0(\omega,t)$ і $\eta_0(\omega,t)$ - це деякі випадкові процеси, які характеризують підпис особи незалежно від того в якому місці на планшеті вона почала підписуватися $(B_\xi(\omega)=0, B_\eta(\omega)=0)$, з яким розмахом (амплітудою) написаний підпис $(A_\xi(\omega)=1, A_\eta(\omega)=1)$, протягом якого часу тривав підпис $(\alpha(\omega)=1)$:

$$\xi_0(\omega,t)=\frac{\xi\left(\omega,\frac{1}{\alpha_\xi(\omega)}\cdot t\right)-B_\xi(\omega)}{A_\xi(\omega)}, \qquad (8)$$

$$\eta_0(\omega,t)=\frac{\eta\left(\omega,\frac{1}{\alpha_\eta(\omega)}\cdot t\right)-B_\eta(\omega)}{A_\eta(\omega)}. \qquad (9)$$

На основі запропонованих математичних конструкцій (1) - (9) розроблено алгоритми і програмне забезпечення для попередньої обробки динамічних підписів. Результати обробки показані на Рис. 3.

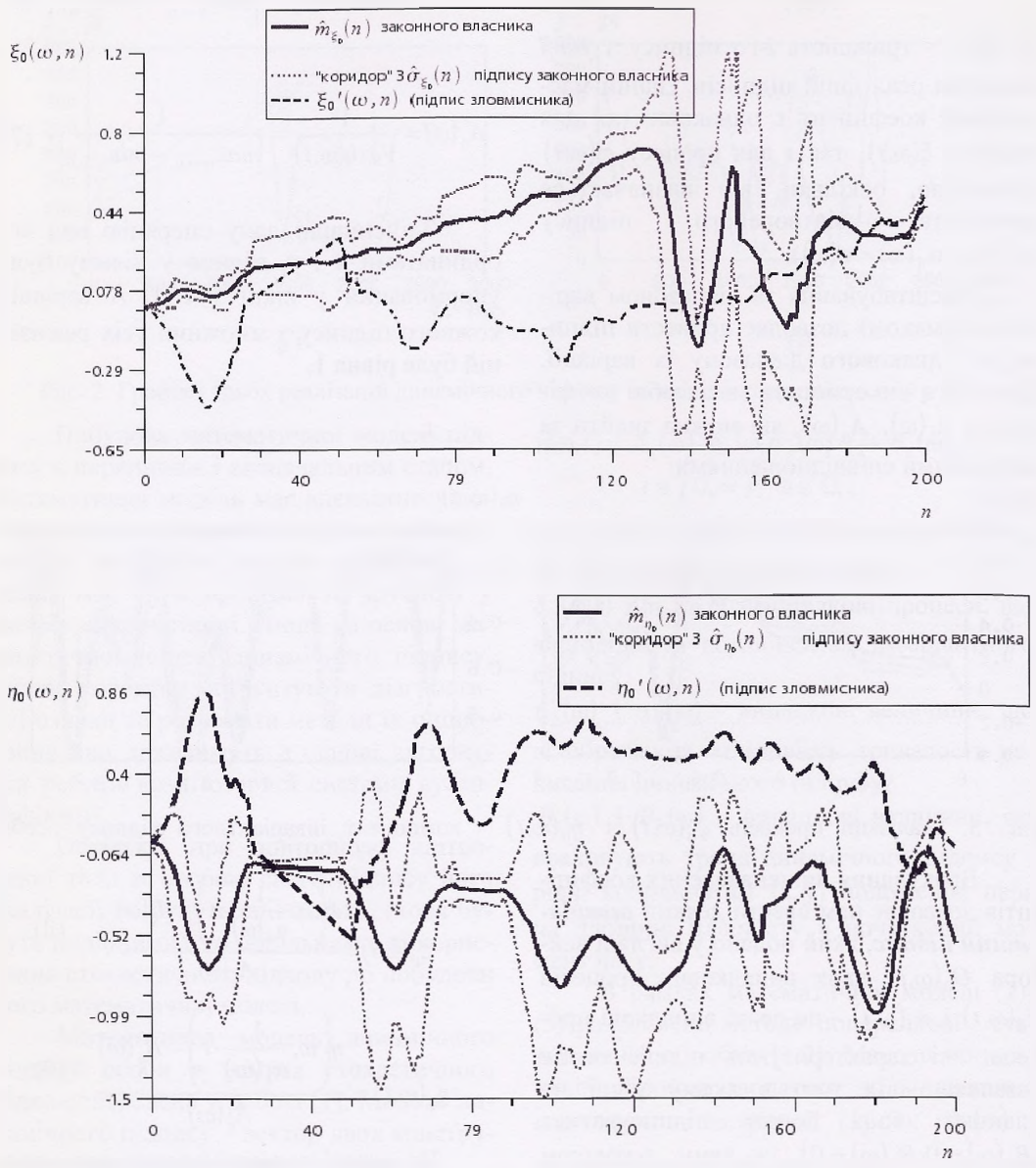

Рис. 4. Інваріантний підпис у "коридорі" $m \pm 3\sigma$ і підпис зловмисника (процеси $\xi_0(\omega,n)$ і $\eta_0(\omega,t)$)

Оскільки, динамічний підпис має яскраво виражений нестаціонарний характер, то в результаті попередньої обробки, яка по суті є нормуванням за тривалістю і масштабом та синхронізацією усіх реалізацій динамічного підпису, можна досліджувати динамічний підпис як випадковий процес за ансамблем засинхронізованих та узгоджених реалізацій.

Було проведено статистичний [2] експеримент в ході якого отримано експериментальні дані, здійснено статистичне оцінювання експериментальних даних, згідно методів викладених у [2]: оцінено

математичне сподівання, дисперсію, кореляційну функцію інваріантного підпису і випадкових масштабуючих коефіцієнтів. Оцінено функцію розподілу інваріантного підпису – це нормальний закон розподілу. Нормальність (гаусовість) вказує на те, що випадковий процес характеризується математичним сподіванням і дисперсією, а також вказує на те, що випадкові величини розсіяні згідно з правилом "трьох сігм" відносно математичного сподівання. А це дозволяє розробити критерії прийняття рішень про належність чи неналежність підпису особі. Зокрема, еталоном підпису законного власника є оцінки математичних сподівань процесів $\hat{m}_{\xi_0}(\omega,t)$ і $\hat{m}_{\eta_0}(\omega,t)$, а дисперсії $\hat{d}_{\xi_0}(\omega,t)$ і $\hat{d}_{\eta_0}(\omega,t)$ характеризують "коридор" у якому може знаходитись підпис законного власника (Рис. 4).

На основі запропонованих підходів було побудовано систему аутентифікації особи за динамічно введеним підписом, у режимі реєстрації користувачів система працює згідно з алгоритмом зображеним на Рис. 5.

Користувач проходячи реєстрацію у системі вводить своє реєстраційне ім'я і декілька динамічних підписів. Після цього введені динамічні підписи обробляються згідно співвідношень (4)-(9), результати попередньої обробки підлягають статистичному аналізу: проводиться оцінювання математичного сподівання і дисперсії інваріантного підпису. Згідно до оцінок експертів-графологів[3], є приблизно 5% людей, які мають нестабільний почерк, а значить їх підпис не може бути об'єктом за яким здійснюється аутентифікація. Тому, на етапі реєстрації особи у інформаційній системі необхідно передбачити перевірку тестових підписів на можливість їх використання у якості об'єкта аутентифікації. Для визначення людей з нестабільним почерком можна використати наступні підходи:

1) емпірично визначити максимальний рівень дисперсії підписів, які особа вводить при реєстрації і при перевищенні цього рівня відмовляти у реєстрації;
2) проводити серію психологічних тестів особи з метою виявлення певних захворювань і розладів, які, як правило, є причиною нестабільності почерку;
3) висновки експертів за результатами медичного обстеження особи.

Можна припустити, що 2-й і 3-й способи можуть бути замінені першим.

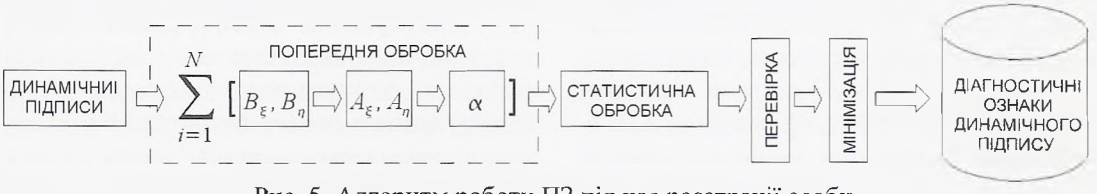

Рис. 5. Алгоритм роботи ПЗ під час реєстрації особи

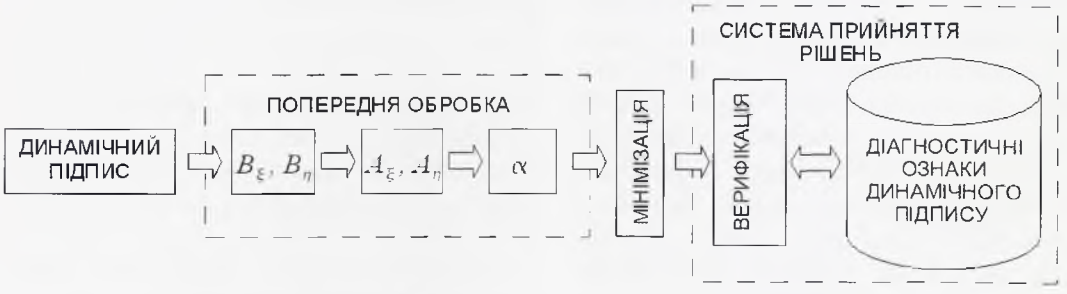

Рис. 6. Алгоритм роботи ПЗ під час аутентифікації особи

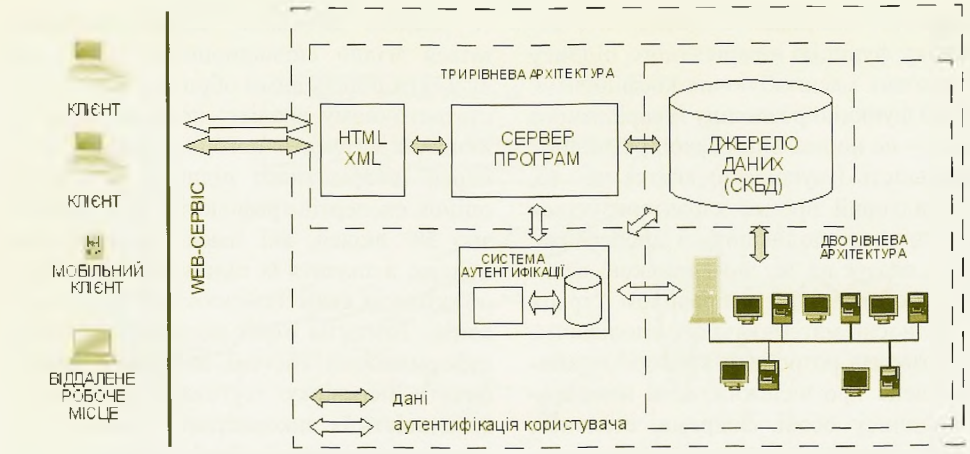

Рис. 7. Структура корпоративної мережі з аутентифікацією осіб за динамічно введеним підписом

За умови можливості використання динамічного підпису система перейде до наступного етапу, у іншому випадку в реєстрації буде відмовлено. Етап мінімізації діагностичних ознак полягає у розкладі оцінок математичного сподівання і дисперсії у ряд за ортогональним базисом, наприклад, поліномами Чебишева. Отримані коефіцієнти зберігаються у базі даних системи аутентифікації.

Таким чином у системі зберігається реєстраційне ім'я користувача і «пароль» у вигляді оцінок математичного сподівання і дисперсії інваріантного підпису.

Алгоритм роботи системи у режимі аутентифікації особи зображено на Рис. 6. Робота системи зводиться до наступного: користувач вводить своє реєстраційне ім'я після чого засвідчує себе за допомогою динамічного підпису. Після вводу динамічного підпису здійснюється його попередня обробка і мінімізація діагностичних ознак, аналогічна до описаної вище. На основі мінімізованих діагностичних ознак щойно отриманого підпису і збереженого у базі даних відбувається їх порівняння. Якщо отримані коефіцієнти належать «коридору» законного власника, то аутентифікація проходить успішно і користувач авторизується системою, у іншому випадку система розглядає введений користувачем підпис, як підпис зловмисника.

У результаті тестування системи оцінено ймовірності помилок І-го роду - 0,088 і ІІ-го роду - 0,012, що вказує на високу точність запропонованих методів обробки і роботи системи загалом.

Розроблене програмне забезпечення може бути використано у якості заміни звичайної парольної аутентифікації або як доповнення до неї у інфраструктурі комп'ютерної мережі (Рис.7).

Застосування аутентифікації особи за динамічним підписом можливе також у системах електронного документообігу. Інтегрування динамічних підписів у електронні документи, дозволяє замість електронних (криптографічних) ключів використовувати динамічно введені підписи. Такі програмні засоби пропонуються рядом фірм (*SOFTPRO* (*http://www.signplus.com*), *Cybersign Inc.* (*http://www.cybersign.com*), *Communication Intelligence Computer Corporation, Ltd.* та інші) для інтегрування у документи формату *PDF* (*Portable Document Format*) і документів офісного пакету *MS Office*, проте за останні кілька років великої популярності набув відкритий пакет офісних програм OpenOffice.org [4] з форматом зберігання документів – *ODF* (*Open*

Document Format). На жаль, аналогічні комерційним, засоби захисту *ODF*-документів відсутні на ринку, оскільки, формат є новим і відкритим, що передбачає відкритість використовуваних технологій захисту, а ліцензійні і патентні обмеження зазначених програмних продуктів цього не передбачають. Зазначимо, що *ODF* з 3 травня 2006 року прийнятий як міжнародний стандарт *ISO/IEC* 26300 і у країнах Євросоюзу, США, Австралії та інших планується його використання, як державного стандарту документообігу.

Офісний пакет OpenOffice.org має зручні засоби розробки: на мовах *C++*, *OpenOffice.org Basic* і *JAVA*, що дозволяє відносно просто інтегрувати розроблене у даній роботі ПЗ з *OpenOffice.org*.

Розроблене програмне забезпечення використовується у вигляді системи комп'ютерних програм для аутентифікації особи у системі обліку робочого часу співробітників [5,6].

Висновки

Побудовано математичну модель динамічно введеного підпису, в рамках якої запропоновано методи обробки і діагностичні ознаки, які можуть репрезентувати особу у інформаційній системі. У свою чергу методи обробки дозволили розробити алгоритми, які послужили основою для створення системи програм, які дозволяють отримувати сигнал, здійснювати попередню і статистичну обробку, імітаційне моделювання і досліджувати динамічно введений підпис.

Результати тестування системи вказують на високу точність роботи системи і можливість її використання для розв'язку поставленої задачі. Наведено приклади можливого застосування системи.

Список літератури

1. *Бойко І., Лупенко С., Луцків А.* Математичне моделювання та статистичні методи обробки динамічного підпису для задач аутентифікації особи в інформаційних системах // Електроніка та системи управління. - 2006. - №2(8). - С.27-37.

2. *Бойко І., Лупенко С., Луцків А.* Оцінювання ймовірнісних характеристик динамічно введеного підпису для задач аутентифікації особи в інформаційних системах //Електроніка та системи управління. – 2006. - №4(10). - С.15-27.

3. *Наджимов О.К.*, Как узнать характер человека по его подписи или практическая графология http://www.lib.ru/URIKOVA/GRAFOLOG/aybek/aybek.txt, 1998

4. *Бойко І.Ф., Лупенко С.А., Луцків А.М.* Розробка і проектування систем біометричної аутентифікації на основі динамічного підпису// Матеріали II Міжнародної науково-практичної конференції "Дні науки-2006". Т. 30. - Сучасні інформаційні технології. - Дніпропетровськ: Наука і освіта, 2006. - С. 47-49С.

5. *Lutskiv A.* Biometry authentication system based on on-line signature verification. //Proceedings of the international conference on computer science and information technologies. Lviv, 2006. – P.43-48.

6. *Бойко І., Лупенко С., Луцків А.* Відкрите програмне забезпечення для розробки інформаційних систем: порівняльний аналіз і перспективи розвитку в Україні // Міжнародний науково-технічний журнал "Комп'ютинг". -Тернопіль: "Економічна думка", 2005.- №1, Т.4.-С.99-104.