Internet in Medicine. – *Taylor & Francis, 2005. – Vol. 2005, Issue 5. 14. Øhrn A. Discernibility and Rough Sets in Medicine: Tools and Applications : PhD thesis, Norwegian University of Science and Technology, Department of Computer and Information Science / A. Øhrn. – 1999. 15. Нікольський Ю.В., Щербина Ю.М. Генетичні алгоритми в екстремальних задачах / Ю.В. Нікольський, Ю.М. Щербина // Вісник Львівського університету, Серія прикладна математика та інформатика. – 2000. – Вип. 2. – С. 191–208.*

УДК 004.93.1

В. М. Заяць[*], М.М. Заяць
[*]Львівський державний інститут новітніх
технологій та управління імені В. Чорновола,
кафедра інформаційно-комп'ютерних технологій та систем;
Національний університет „Львівська політехніка",
кафедра інформаційних систем і мереж

ПІДХОДИ ДО ПОБУДОВИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Розглянуто методи побудови систем захисту інформації від стороннього доступу. Запропоновано підхід до побудови системи захисту комп'ютера на основі використання автоматизованої системи розпізнавання та ідентифікації користувача комп'ютера, що ґрунтується на вимірюванні часових затримок при введенні інформації з клавіатури комп'ютера у дискретні відліки часу. Це дало змогу підвищити ефективність розпізнавання майже в 1,5 раза, автоматизувати процедуру ідентифікації користувачів, забезпечити надійний захист інформації та гарантувати конфіденційний доступ до неї.

In the article the proposed methods to building of the defense system of information from strange access on base of system of computer users recognition with help of model discrete. It is made by measure of time delays at the entered information from a keyboard of computer in the discrete moments of time. It allowed to increase efficiency of recognition almost in 1,5 times and to automate procedure of users authentication and defense of information from strange access created on the basis of discrete models are marked.

Постановка проблеми

При створенні реальних систем захисту інформації від стороннього доступу, дослідженні фізичних явищ чи процесів, побудові систем розпізнавання, ідентифікації та зберігання інформації з бажаними характеристиками доцільно провести їх аналіз та комп'ютерне моделювання шляхом створення математичної моделі системи, що розробляється. Такий підхід вимагає значно менших часових і технічних засобів порівняно з фізичним експериментом, особливо на попередній стадії розробки, коли системи чи пристрою, що розробляється, немає.

Останнім часом в нелінійній динаміці широке застосування знаходять дискретні моделі систем [1–5], для яких дискретність закладена в природі самого об'єкта досліджень, а не є наслідком дискретизації неперервної системи. Доцільність використання дискретних за своєю природою моделей пояснюється такими їх особливостями:

– простотою математичного опису порівняно з неперервними моделями;

– наявністю значно ширшого спектра динамічних режимів порівняно з відомими моделями;

– нескінченною вимірністю, що дає змогу моделювати кожну нову гармоніку шляхом її введення у вектор змінних стану, тоді як для неперервних систем для вирішення цієї задачі необхідно підвищувати розмірність системи;

– відсутністю необхідності визначення параметрів для оптимального проведення комп'ютерного моделювання, вибору оптимального кроку дискретизації змінних стану системи, оцінки локальної і глобальної похибки застосованих числових методів, дослідження областей їх стійкості та синхронізації;

– адаптованістю до постановки комп'ютерного експерименту.

Власне моделі, дискретні за своєю природою, є застосовні як до побудови пристроїв, що мають бажані режими, так і до розпізнавання та ідентифікації таких режимів у системах зі складною динамікою і поведінкою, що дає змогу підвищити ефективність їх роботи та використовувати в інших прикладних задачах, зокрема системах захисту інформації. Водночас різницеві моделі, які є наслідком дискретизації неперервних чи гібридних систем, мають значно вужчу сферу застосувань.

Цілі статті

Метою статті є застосування автоматизованої комп'ютерної системи розпізнавання та достовірної ідентифікації користувача комп'ютера (АКСРІ), що описана та розроблена на основі дискретної моделі, алгоритм побудови якої наведено у статтях [4, 10], з метою підвищення точності розпізнавання та забезпечення автоматизації процесу ідентифікації користувачів. Запропоновано підхід до реалізації процедури санкціонованого доступу до ввімкненого комп'ютера, який не потребує додаткових операцій ні з боку користувача, ні з боку адміністратора. У роботі також визначені перспективні напрямки розвитку систем розпізнавання складних динамічних процесів на основі дискретних моделей та напрямки їх доцільного застосування.

Виклад основного матеріалу

Аналіз основних результатів. При створенні систем захисту інформації від несанкціонованого доступу, встановлені паролів доступу чи консервуванні інформаційних архівів на основі використання систем розпізнавання об'єктів та їх достовірної ідентифікації необхідний системний підхід до розроблення останніх. Суть цього підходу полягає у формуванні первинних інформативних ознак про об'єкт розпізнавання та ідентифікації, встановленні їх пріоритету та вибору або розробленні та реалізації надійних критеріїв розпізнавання та достовірної ідентифікації об'єктів та процесів.

Системи захисту, що ґрунтуються на встановленні паролів доступу до системи [1, 2], не можна вважати надійними, оскільки розгалужена мережа ключів злому паролів дає змогу проникнути практично в найскладнішу систему кодування. Системи захисту інформації на основі нейромережевих технологій є значно надійнішими, але доволі громіздкими і потребують додаткових часових і технічних вират на їх реалізацію. Побудова системи захисту інформації від несанкціонованого доступу шляхом встановлення надійної системи розпізнавання користувача комп'ютера видається доцільною як з погляду надійності її роботи, так і складності реалізації.

Перші дослідження у галузі розпізнавання в нашій країні проводилися А.А. Харкевичем [13] – одним з основоположників та фундаторів теорії інформації та сигналів. Значний внесок у розвиток теорії розпізнавання зробили В.М. Глушков, В.С. Міхалєвич, О.Г. Івахненко, Ю.І. Журавльов, Я.З. Ципкін, В.І. Васильєв. Подальший внесок у розвиток теорії розпізнавання образів зробили У. Гарднер, Р. Дуда, Г. Себастіан, Дж. Ту, К. Фу, П. Харт, С. Ватанабе та інші.

Перші роботи з розпізнавання образів було присвячено теорії і практиці побудови читальних автоматів (під образом розуміли знак, зображення, букву або цифру). Математичним апаратом для розв'язання задач розпізнавання з моменту їх виникнення була теорія статистичних розв'язків [14].

Сьогодні результати теорії статистичних розв'язків стали фундаментальною базою для побудови алгоритмів розпізнавання, що забезпечують віднесення об'єкта до його класу на підставі обробки експериментальних апостеріорних даних – інформаційних ознак, що характеризують об'єкт та апріорних даних (можливо і не повних), що описують класи об'єктів. Надалі математичний апарат теорії розпізнавання та ідентифікації розширився за рахунок використання методів алгебри логіки і деяких розділів прикладної математики, теорії інформації, математичного програмування і системотехніки [8, 14–16].

Незважаючи на те, що методи і алгоритми теорії розпізнавання та ідентифікації все більшою мірою стають невід'ємною складовою таких прикладних галузей природознавства, як медична і технічна діагностика, ідентифікація складних динамічних процесів та інформаційних систем, екологічний моніторинг та соціальна інформатика, метеорологічне прогнозування та геологічна розвідка, локаційні засоби спостереження та системи введення і виведення текстової, графічної та мовної інформації в комп'ютер, інтелектуальні системи прийняття рішень та інформаційні системи керування в літературі – як вітчизняній, так і в іноземній – системний підхід до розв'язання задач розпізнавання, ідентифікації, захисту інформації поки що відсутній.

Сьогодні, як і півстоліття тому, проблема розпізнавання значною мірою ототожнюється з побудовою оптимальних критеріїв розпізнавання та дослідженням умов реалізації певного алгоритму чи моделі. Теоретичні дослідження орієнтовані на розв'язання хоча й актуальних, але часткових задач. До таких задач насамперед треба віднести задачі достовірного розпізнавання, суть яких зводиться до поділу простору ознак, мовою яких описуються об'єкти чи процеси розпізнавання, на області, що відповідають класам цих об'єктів, тобто до вибору найкращих границь (правил) розділення класів. Але розв'язання цих задач можливе тоді, коли апріорі відомі класи об'єктів і ознаки, мовою яких описуються розпізнавані об'єкти та їхні класи. Однак розробник системи розпізнавання, як правило, не володіє цією інформацією. Навіть у найпростіших випадках розпізнавання букв алфавіту, відбитків пальців, слів мови, екстремумів чи особливих точок складних нелінійних функцій (де не виникає питання про класи), їхні інформативні ознаки та апаратура для їх визначення не є відомими – це є предметом нетрадиційних досліджень.

Причиною такого стану речей є те, що задачі класифікації (порівняно з проблемами розпізнавання та прийняття рішення) порівняно легко піддаються формальному і аналітичному розв'язанню, що й визначає їх привабливість для дослідників. Друга причина полягає у тому, що значна частина дослідників обмежує свою діяльність лише теоретичними дослідженнями. Третя проблема в тому, що традиційно вважається, що системи розпізнавання є автономними. Лише в окремих часткових випадках це виправдано, хоча в загальному випадку таке формулювання проблеми не є правомірним. Адже і в системах технічної чи медичної діагностики, в автоматизованих системах управління виробництвом чи розпізнавання дефектів механізмів і машин, визначення діагнозу пацієнта чи розпізнавання складних динамічних режимів, класифікація реальних ситуацій не є самоціллю. Достовірна класифікація та безпомилкове розпізнавання необхідні для отримання вихідної інформації для успішного функціонування управлінської системи з метою прийняття керівних рішень, адекватних результатам розпізнавання невідомих об'єктів, явищ, ситуацій, станів.

Можна стверджувати, що достовірне розпізнавання ситуацій не є достатньою умовою потенціально можливої ефективності системи управління. Але це є необхідна умова. Важко уявити, щоб лікар, який поставив неправильний діагноз, знайшов правильний метод лікування. Невиявлення нестійких коливних режимів також не забезпечить надійної роботи технічного пристрою при виборі параметрів, що відповідають режиму нестійкості.

Для розроблення будь-яких систем розпізнавання необхідний системний підхід, суть якого полягає в тому, щоб в умовах неминучих фінансових і технічних обмежень система розпізнавання забезпечила системі управління реалізацію потенціально можливої ефективності. Вибору чи створенню критеріїв розпізнавання повинна передувати процедура вимірювання первинних ознак про

процес розпізнавання, встановлення пріоритету цих ознак та їх впливу на інтегральні характеристики досліджуваного процесу чи об'єкта. З математичного погляду опис такої системи має забезпечувати мінімальну похибку розпізнавання та достовірну ідентифікацію об'єкта розпізнавання за певними ознаками та критеріями прийняття рішення.

Лише за умови надійної безпомилкової роботи АКСРІ можна побудувати систему захисту інформації, що зберігається на комп'ютері від стороннього вторгнення.

Метод ідентифікації користувача шляхом виділення дискретних інформативних ознак. Суть побудови методу полягає у тому, щоб забезпечити процедуру розпізнавання конкретного користувача при його роботі за клавіатурою комп'ютера. Деякі загальні міркування щодо створення такої системи подані в роботі [15].

Очевидно, для організації процесу розпізнавання у пам'ять комп'ютера необхідно ввести "почерк" (набраний текстовий файл з клавіатури комп'ютера) кожного із легальних користувачів комп'ютера. За відсутності зразка об'єкт не розпізнається або пропонується створити новий клас об'єктів шляхом завдання зразку почерку (це, власне кажучи, і пропонується використати для забезпечення санкціонованого доступу до ресурсів комп'ютера). Паралельно при створенні зразка за рукомоторними ознаками об'єкта формується інформаційна модель об'єкта шляхом визначення функцій розподілу часових затримок при введенні інформації в комп'ютер. Як первинні інформаційні ознаки про об'єкт о використано різні часові затримки при роботі об'єкта за клавіатурою комп'ютера. При ідентифікації об'єкта знову реалізуємо процедуру вибору або розроблення критеріїв прийняття рішення і на основі цих критеріїв [15–17] і приймаємо рішення про віднесення об'єкта до певного класу. У випадку неоднозначного рішення можна застосувати функції відстані (детермінований підхід) і однозначно обрати клас (з найменшим середньоквадратичним відхиленням ознак).

Зазначимо, що різні інформаційні ознаки можуть мати різний пріоритет, який також необхідно встановити аналітично або шляхом комп'ютерного моделювання. Для реалізації цієї мети запропоновано скористатися методом послідовних наближень, який описано в роботі [16]. Встановити пріоритет кожної із первинних ознак можна експериментально. Суть цього підходу полягає у моделюванні процесу розпізнавання при задання однієї ознаки з послідовною заміною її на інші і видаленням попередньої. Порівнюючи результати розпізнавання, можна чітко встановити пріоритет кожної із ознак та їх комбінацій по дві, три доти, поки не буде досягнута мінімальна похибка розпізнавання. З метою підвищення ефективності системи доцільно відсікати непрогнозовані хаотичні рухи руки особи шляхом попередньої фільтрації інформації, що вводиться користувачем в режимі реального часу, створюючи тим самим неперервні послідовності (набори) символів, що вводяться користувачем комп'ютера.

У роботі [10–13] сформульовано і проаналізовано велику кількість характеристик. Наведемо лише найбільш інформативні та доступні для швидкого формування. Отже, для побудови системи розпізнавання особи за її рукомоторними реакціями було обрано такі характеристики з врахуванням їх інформаційного пріоритету:

1) відносна девіація паузи перед клавішем – розподіл відносних відхилень паузи перед певним клавішем до середнього значення паузи перед всіма клавішами у певній неперервній послідовності набору

$$DevB = \frac{t_i - t_{cp}}{t_{cp}} \cdot 100\%., \qquad (1)$$

де t_i – тривалість паузи перед i–м клавішем, t_{cp} – середня тривалість паузи перед клавішами в послідовності набраного тексту;

2) відносна девіація утримання клавіша – розподіл відносних відхилень тривалості утримання натиснутим даного клавіша до середньої тривалості утримання клавіша у даній неперервній послідовності

$$DevP = \frac{t_i - t_{cp}}{t_{cp}} \cdot 100\% \cdot \quad (2)$$

Приклад такого розподілу зображено на рис. 1. На осі абсцис відкладено відносні відхилення у відсотках, а на осі ординат – відносну частоту потраплянь у відповідний інтервал відхилень.

3) відносна девіація паузи після клавіша – аналогічна попередній характеристиці:

$$DevA = \frac{t_i - t_{cp}}{t_{cp}} \cdot 100\%; \quad (3)$$

4) відношення величини паузи перед клавішем до тривалості утримання клавіша;

5) відношення величини паузи перед клавішем до величини паузи після клавіша;

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

7) розподіл частот використання клавіш зміни регістру.

Разом в роботі [11] розглянуто 18 характеристик, але найбільш інформативними є вищенаведені. Зазначимо, що дослідження похибки розпізнавання (шляхом комп'ютерного моделювання проводилося і для абсолютних значень відзначених часових характеристик та відношень їх абсолютних величин при введенні символів в реальному режимі часу. Розглядалися варіанти випадкових комбінацій пар клавіш та їх час утримання та відповідні паузи. У всіх розглянутих випадках похибка розпізнавання порівняно з використанням характеристик 1–6 зростає від 10% до 35%.

Характеристики 1–6 формувалися для кожного клавіша, що був задіяний у наборі. Щоби спростити процедуру встановлення пріоритету характеристик, при побудові системи прийнято рішення об'єднати перші шість характеристик у групи, оскільки це значно зменшує їх кількість (а в межах групи можна розгадати їх як еквівалентні). На спосіб групування характеристик безпосередньо впливає обраний метод їх зіставлення.

За першим варіантом побудови системи розпізнавання для реалізації процедури ідентифікації було використано функції відстані. Оскільки вага характеристик кожної групи могла бути різною, то відстані обчислювались окремо за кожною групою характеристик. Відстань між класами Ω і Z в межах кожної групи характеристик обчислюється за формулою середнього квадратичного відхилення:

$$Dist(l) = \sqrt{\frac{1}{n} \cdot \sum_{i=1}^{n} \left(m_i^{\Omega} - m_i^{Z} \right)^2}, \quad (4)$$

де m_i – середнє значення вибірки і-ї характеристики певної групи класу Ω, $Dist(l)$ – відстань між класами за групою характеристик λ.

Відстані вимірюються між середніми значеннями, оскільки середнє можна оцінити вже після відносно невеликої кількості дослідів (10–20), що є важливим для зменшення обсягу тексту, що набирається об'єктами розпізнавання.

Групи характеристик 1–6 не еквівалентні за якістю рішень, що приймаються на їх основі. Перед об'єднанням результатів для прийняття рішення з розпізнавання необхідно збалансувати ваги груп між собою. Баланс характеристик обернено пропорційний ймовірностям припустити помилку другого роду (коли два об'єкти різних класів розпізнаються як такі, що належать до одного класу) за кожною з груп характеристик, зокрема: $1/p_1$: $1/p_2$: $1/p_3$: $1/p_4$: $1/p_5$: $1/p_6$: $1/p_7$. Експериментально було отримано відношення ваг груп 1–7 як 4:12:8:6:5:2:6 відповідно. Недоліком системи на основі функцій відстані є те, що вона принципово не може визначити ймовірність правильності або неправильності рішення щодо розпізнавання. Кожний сторонній користувач буде схожий на того чи іншого зареєстрованого користувача системи.

Розроблений другий варіант побудови системи розпізнавання ґрунтується на використанні методу довірчих інтервалів. Для перевірки гіпотези про приналежність пари об'єктів одному класу перевіряються гіпотези про рівність середніх значень розподілів [17] всіх характеристик кожної групи. Для цього обчислюються значення середнього a та вибіркового стандарту s за формулами:

$$a = \frac{1}{n} \cdot \sum_{i=1}^{n} x_i \quad ; \tag{5}$$

$$s = \sqrt{\frac{1}{n-1} \cdot \sum_{i=1}^{n} (x_i - a)^2} \quad . \tag{6}$$

Для розрахунку довірчих інтервалів враховується закон розподілу середнього значення:

$$f\left(x_{\text{ср}}\right) = \frac{\sqrt{n}}{s \cdot \sqrt{2p}} \cdot e^{-\frac{n}{2 \cdot s^2} \cdot \left(x_{\text{ср}} - x_0\right)} \quad . \tag{7}$$

Для вибірок малого обсягу оцінка середнього значення уточнюється за допомогою розподілу Стьюдента [17], за яким розподілена величина $u = \frac{a-m}{s_{\text{ср}}}$. Його густина розподілу задається формулою:

$$S(u,n) = \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right) \cdot \sqrt{p \cdot n}} \cdot \left(1 + \frac{u^2}{n}\right)^{-\frac{n+1}{2}} \quad . \tag{8}$$

Нехай при порівнянні пари відповідних розподілів ми допускаємо помилку першого роду P_a, а всього порівнюємо N таких пар. Отже, логічно припустити, що інтегральна характеристика групи класу і об'єкта збігається з ймовірністю $\geq 1 - P_a$, якщо кількість непідтверджених гіпотез N_a не перевищує числа $P_a \cdot N$. В іншому випадку вважаємо, що об'єкт не належить класу. Такого типу (так/ні) результат ми отримаємо для кожної з шести груп характеристик. Як і у випадку системи на основі функції відстані, ці групи не еквівалентні за якістю рішень, що приймаються на їх основі. Кожна з них має свою ймовірність помилки другого роду.

На основі практичних експериментів з розпізнавання з кожною групою характеристик досліджувалися помилки другого роду. Окремі гіпотези система перевіряла з рівнем значущості $a = 0.05$. Так були отримані ймовірності помилок другого роду 35%, 13%, 20%, 27%, 32%, 78%. Отримані ймовірності помилок були отримані для порівняно невеликої кількості експериментів з ідентифікації (105 експериментів). Для великої групи людей ймовірності помилок можуть дещо відрізнятися від наведених.

При тестуванні розробленої системи на досліджуваних об'єктах було допущено лише одну помилку на 22 проведені розпізнавання (запропоновано два схожі на об'єкт класи, один серед яких був правильний).

Комп'ютерна система розпізнавання користувача за його рукомоторними реакціями. У розробленій комп'ютерній системі передбачено роботу у режимі користувача та адміністратора. Робота з системою починається із входження в головне меню. У ньому можна вибрати режим адміністратора, користувача або завершити роботу.

У режимі користувача відкривається нове діалогове вікно. Користувачу пропонується виконати набір декількох речень завдання. Якщо користувач зареєстрований у системі, то після набору 5–8 речень завдання система розпізнає його і виведе на екран відповідне повідомлення з прізвищем та ім'ям користувача. Інакше йому доведеться набрати 15–20 речень, після чого система (без повідомлень) автоматично зареєструє користувача як стороннього і повідомить його, що він не має права входити до системи і має звернутися до адміністратора для реєстрації. Для зручності

система дає змогу за бажанням користувача вводити довільний текст. Користувач також може увімкнути режим прихованого тексту для захисту вхідної інформації від стороннього спостерігача. Адміністратор входить у систему за допомогою звичайного паролю. Цей режим передбачає контроль за роботою користувачів.

Система веде журнал із записами дати і часу запуску системи, входу і виходу користувачів, також протоколює важливі дії адміністратора (вхід, реєстрація, редагування, видалення користувачів). За бажанням адміністратор може очистити журнал.

На сторінці «Список користувачів» адміністратор може реєструвати/ редагувати (виправляти, змінювати, видаляти, додавати) користувачів. Сторінка "Перегляд характеристик" створена для першого знайомства, візуального контролю й аналізу та вивчення рукомоторних характеристик.

На ній можемо вибрати користувача, тип характеристики, клавіш і подивитись одну з гістограм. На сторінці «Додаткові параметри» можна отримати числові значення математичного сподівання, дисперсії, середнього квадратичного та моди для кожної неперервної послідовності літер, що вводяться у комп'ютер у реальному режимі часу.

Наближена оцінка помилки прийняти об'єкт одного класу за об'єкт іншого не перевищує 35% за наявності 200 зареєстрованих у системі класів.

Система розпізнає зареєстрованого користувача після набору ним 5–8 речень по 60 знаків кожне, тобто після введення 300–500 знаків. За достатньої кваліфікації користувача (швидкість набору тексту 200 знаків за хвилину) система розпізнає користувача, який набирає замість завдання довільний текст. У деяких випадках зареєстровано розпізнавання особи при наборі тексту англійською мовою. Це характерно для висококваліфікованого користувача (швидкість набору тексту понад 300 символів за хвилину), коли ймовірність хаотичних рухів руки від усталеного часового режиму є малоймовірною.

Підхід до опису системи розпізнавання користувача комп'ютера на основі дискретної моделі. Запропонований підхід для побудови дискретних моделей коливних процесів зі складною структурою, запропонований в роботах [5–9], можна застосувати до опису динамічної системи будь-якої природи за умови, що її стани характеризуються дискретними ознаками. Для довільної кількості ознак N маємо N – вимірний вектор змінних стану, а матрицю переходу станів **A** будуємо так, щоб її визначник дорівнював одиниці. Найпростіше це можна зробити, якщо $N - 2$ рядки матриці мають одиниці на головній діагоналі, а позадіагональні елементи дорівнюють нулю. При цьому останні два рядки цієї матриці є комбінацією гармонічних функцій початкової фази φ

$$\mathbf{A}(j) = \begin{pmatrix} 1 & 0 & 0 & \mathbf{K} & 0 & 0 & 0 \\ 0 & 1 & 0 & \mathbf{K} & 0 & 0 & 0 \\ 0 & 0 & 1 & \mathbf{K} & 0 & 0 & 0 \\ \mathbf{M} & \mathbf{M} & \mathbf{M} & \mathbf{K} & \mathbf{M} & \mathbf{M} & \mathbf{M} \\ 0 & 0 & 0 & \mathbf{K} & 1 & 0 & 0 \\ 0 & 0 & 0 & \mathbf{K} & 0 & \cos j & \sin j \\ 0 & 0 & 0 & \mathbf{K} & 0 & -\sin j & \cos j \end{pmatrix}. \quad (9)$$

Тоді амплітуді коливань відповідатиме середньоквадратичне значення N –вимірного вектора змінних стану, яке може бути обчислене із завданням конкретного набору функцій f. Ефективність такого підходу до опису наведено у попередньому розділі комп'ютерної системи розпізнавання користувача комп'ютера за його рукомоторними реакціями, які визначаються різними часовими інтервалами (час утримання клавіші, тривалість паузи перед натисканням клавіші, тривалість паузи після натисканням клавіші) як абсолютних, так і віднесених до їх середнього значення, або одного часового інтервалу до іншого підтверджена результатами комп'ютерного моделювання.

На основі запропонованого підходу реалізована в середовищі DELPHI комп'ютерна система розпізнавання користувача комп'ютера за його рукомоторними діями. У реальному режимі часу в

процесі набору користувачем заданого тексту формуються функції розподілу різних часових затримок, які апроксимуються нормальним законом розподілу. На основі зіставлення поточних значень математичних сподівань і дисперсій для кожного із сформованих розподілів з апріорі заданими зразками ідентифікується той чи інший користувач. Ефективність такої системи не перевищує 65 % при реєстрації всіх часових ознак.

Для підвищення ефективності розробленої системи запропоновано описувати її у вигляді системи дискретних рівнянь шостого порядку відповідно до сформованих значень дискретних ознак (часових затримок). Вибір базових функцій для опису такої системи розпізнавання є проблематичним, оскільки це мають бути імовірнісні функції розподілу, які відповідно до рукомоторних дій користувача мають передбачати появу тієї чи іншої літери на клавіатурі комп'ютера і прогнозувати величину часової затримки при її натисканні чи величину паузи до і після натискання. Але незалежно від вигляду цих базових функцій у випадку опису процесу у вигляді дискретної моделі, якщо за ознаки вибрати відношення девіацій часу утримання до паузи перед клавішею та відношення девіацій паузи до часу утримання клавіша, максимальна інформативність яких підтверджена результатами комп'ютерного моделювання, оцінити період повторення натискання літер на клавіатурі можна за формулою [5]:

$$T = \frac{2 \cdot p}{j}. \qquad (10)$$

Якщо виходити з реального середнього часу утримання клавіші 0,3 с, то з урахуванням пауз до і після утримання клавіша період набору літер не перевищуватиме 1 с, що відповідає початковій фазі коливань 2π. Отже, при введенні в алгоритм розпізнавання блоку формування неперервної послідовності літер, коли в реальному режимі часу відсікаються будь-які хаотичні рухи (випадкова неуважність, механічна затримка, натискання кількох клавіш, вимушена пауза тощо), ефективність такої системи ідентифікації користувача значно зростає. Як показали результати статистичних випробувань, за наявності 200 користувачів в базі даних похибка розпізнавання не перевищувала 5%.

Суть підходу до побудови системи захисту інформації, що працює в реальному режимі часу. Наявність надійних засобів для розпізнавання та ідентифікації користувача комп'ютера, що працює за клавіатурою комп'ютера, дає змогу сформулювати алгоритм побудови системи захисту інформації, що зберігається в комп'ютері, не втручаючися в його роботу.

Традиційні системи захисту комп'ютера від доступу сторонніх осіб ґрунтуються на встановленні пароля на рівні плати BIOS або на рівні операційної системи. Такі системи мають право на існування, але їх надійність вельми незначна з урахуванням розвиненої мережі ключів для злому комп'ютерних систем. У зв'язку з цим розроблення нових підходів до побудови надійних автоматизованих засобів захисту комп'ютерних систем від стороннього доступу є актуальним завданням.

Запропоновано підхід до побудови системи захисту комп'ютера від стороннього доступу шляхом використання системи розпізнавання та ідентифікації особи, що працює за клавіатурою комп'ютера в реальному режимі часу. Пропонується на системному рівні, якщо впродовж визначеного проміжку часу (3–5 хвилин) клавіш клавіатури комп'ютера не натискали, автоматично під'єднується автоматизована комп'ютерна система розпізнавання й ідентифікації користувача (АКСРІ) за його рукомоторними реакціями [10]. У разі неуспішного розпізнавання комп'ютер автоматично вимикається. З урахуванням того, що похибка, описана в роботах [4, 11, 12] АКСРІ не перевищує 5%, надійність захисту комп'ютера від стороннього проникнення гарантована. Треба зазначити, що використання вказаної АСРІ не впливає на роботу зареєстрованих користувачів, оскільки не вимагає ніяких інших дій від нього, окрім натискання клавіш клавіатури комп'ютера.

Сутність роботи ACPI ґрунтується на вимірюванні часових затримок (пауз до і після натиснення клавіша, часу його утримання, частоти зміни регістрів, віднесених до середніх значень вказаних параметрів) при введенні символів з клавіатури комп'ютера. Для кожного з символів формується неперервна послідовність часових затримок, яка апроксимується нормальним законом розподілу імовірності. Після визначення усереднених значень математичного очікування і дисперсії за всіма затримками відбувається зіставлення з відповідними зразками "почерку", зареєстрованими в комп'ютері. Якщо відносна величина відхилення зазначених характеристик за всіма користувачами перевищує 10%, то комп'ютер автоматично вимикається. Інакше відбувається ідентифікація користувача і автоматичне оновлення еталона його почерку, якщо відхилення отриманих характеристик від зареєстрованих не перевищує 1%.

За таким підходом, окрім захисту комп'ютера від несанкціонованого доступу до нього, реалізується також механізм адаптації ACPI до змін почерку користувача комп'ютера.

Експериментальну версію системи захисту комп'ютера написано мовою програмування Delphi 7.0. Схему роботи системи захисту комп'ютера від несанкціонованого доступу наведено на рисунку.

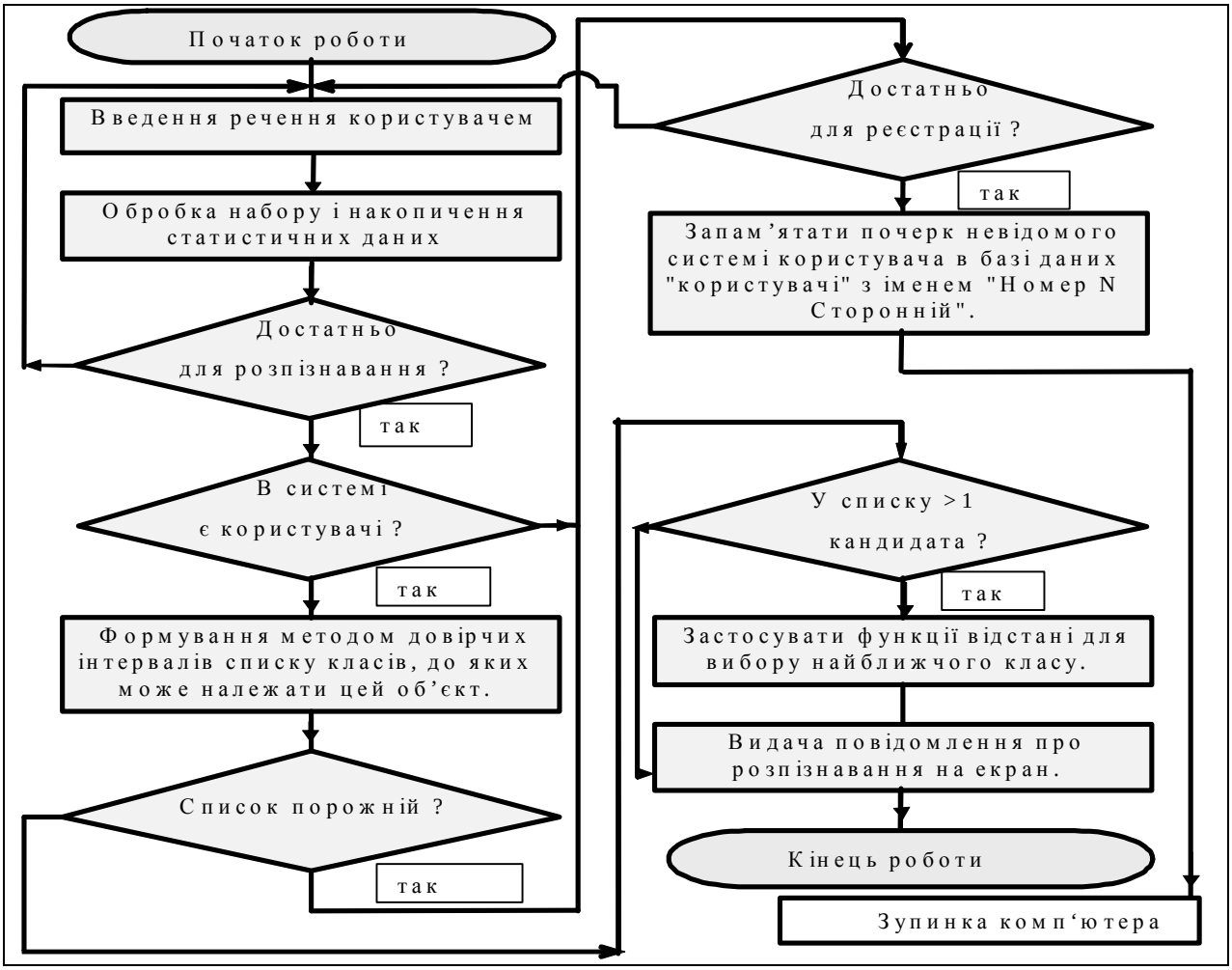

Схема роботи автоматизованої системи захисту комп'ютера від несанкціонованого доступу

Оскільки, як випливає з поставлених комп'ютерних експериментів (на прикладі двохсот користувачів), при середній швидкості введення тексту (150 – 200 символів на хвилину) час на

розпізнавання і ідентифікацію не перевищує 1,5 – 3 хвилини, то за наявності такої системи захисту комп'ютера зайвих незручностей його користувачів не виникає.

Висновки

Описано підхід до побудови системи захисту інформації працюючого комп'ютера від несанкціонованого доступу на основі використання автоматизованої системи розпізнавання та ідентифікації користувача комп'ютера. При цьому розроблено метод формування первинних ознак при побудові комп'ютерної системи розпізнавання користувачів комп'ютера, запропоновано алгоритм та наведено схему реалізації такої системи, зазначено особливості її функціонування та запропоновано шляхи підвищення достовірності розпізнавання та ідентифікації користувачів на основі використання дискретних моделей, що зв'язують тривалості пауз до і після натискання клавіш комп'ютера з часом утримання клавіша при введені інформації з клавіатури комп'ютера.

Порівняно з існуючими системами захисту інформації [1, 2, 18] підвищенj надійність її роботи за рахунок проведення достовірного розпізнавання (похибка не перевищує 5%) та ідентифікації користувача комп'ютерної техніки.

У wsq системі захисту інформації передбачено механізм її адаптації до змін почерку зареєстрованих користувачів системи шляхом систематичного оновлення зразків їх почерку за умови зменшення часових затрат 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 проведення ідентифікації.

1. Вовк О.Б. Проблеми захисту шрифтів як специфічних об'єктів авторського права // Вісник Нац. ун-ту „Львівська політехніка". – 2008.– № 610. – С. 85–83. 2. 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, Євпаторія, 2008, Т. 1, – С. 39–43. 3. Динамика одномерных отображений / А.Н. Шарковский, С.Ф. Коляда, А.Г. Сивак, В.В. Федоренко.– К.: Наук. думка, 1989. – 216 с. 4. Заяць В.М. Перспективні напрямки розвитку та застосування систем розпізнавання та ідентифікації об'єктів і процесів на основі дискретних моделей коливних систем / В.М Заяць, М.М. Заяць // Вісник Нац. ун-ту „Львівська політехніка". – 2008. – № 610. – С.137–147. 5. Заяць В.М. Построение и анализ модели дискретной колебательной системы // Кибернетика и системный анализ. – 2000. – С. 161–165. 6. Заяць В.М. Моделі дискретних коливних систем // Комп'ютерні технології друкарства. – 1998. – С.37–38. 7. Заяць В.М. Аналіз динаміки та умов стійкості дискретних моделей коливних систем // Вісник Нац. ун-ту „Львівська політехніка". – 2004. – № 519. – С.132–142. 8. Шустер Г. Детерминированный хаос: Введение. Пер. с англ. – М.: Мир, 1988. – 240 с. 9. Zayats V. Chaos searching algorithm for second order oscillatory system / V. Zayats// Proc. International Conf. "TCSET – 2002".– Lviv-Slavsk.– 2002.– P. 97–98. 10. Заяць В.М. Алгоритмічне та програмне забезпечення системи розпізнавання людини за її рукомоторними реакціями // Вісник Держ. ун-ту „Львівська політехніка". – 2000. – № 392. – С.73–76. 11. Заяць В.М Підхід до опису системи розпізнавання користувача комп'ютера // Комп'ютерні технології друкарства. – 2006.– С. 46–53. 12. Заяць В.М. Математичний опис системи розпізнавання користувача комп'ютера // Зб. "Фізико-математичне моделювання та інформаційні технології". – Львів. – 2005. – Вип. 1.– С. 146–152. 13. Харкевич А.А. Опознание образов // Радиотехника. – 1959. – Том 14. – С. 15–19. 14. Фукунага К. Введение в статистическую теорию распознавания. – М.: Наука, 1979. – 512 с. 15. Горелик А.Л. Методы распознавания – М.: Высшая школа, 1989. – 232 с. 16. Дуда Р. Распознавание образов и анализ сцен. – М.: Мир, 1976. – 512 с. 17. Березин И.С. Методы вычислений. – М.: Физматиздат, 1962. – 639 с. 18. Томашевський О.М. Методи та алгоритми системи захисту інформації на основі нейромережевих технологій: Автореф. дис. … канд. техн. наук: спец. 05.13.23. – Львів, 2002.– 20 с.