МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ВИСОЦЬКА Олена Олександрівна

УДК 004.056.523:57.087.1(043.3)

МЕТОДИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ЗА ЇХ КЛАВІАТУРНИМ ТА РУКОПИСНИМ ПОЧЕРКОМ

05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2019

Дисертацією є рукопис.
Робота виконана в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.

Науковий керівник: кандидат технічних наук, старший науковий співробітник
Давиденко Анатолій Миколайович,
Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України,
провідний науковий співробітник.

Офіційні опоненти: доктор технічних наук, професор
Терейковський Ігор Анатолійович,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри системного програмування і спеціалізованих комп'ютерних систем;

кандидат технічних наук
Фесенко Андрій Олексійович,
Київський національний університет імені Тараса Шевченка, асистент кафедри кібербезпеки та захисту інформації.

Захист відбудеться « 08 » листопада 2019 р. о 16^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, Київ, пр. Космонавта Комарова, 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий « 08 » жовтня 2019 р.

Учений секретар
спеціалізованої вченої ради
д.т.н., доцент С. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Постійне зростання частоти використань на підприємствах майже всіх сфер діяльності, інформаційних систем (ІС), які реалізують різноманітні інформаційні технології та, насамперед, обробляють і зберігають конфіденційну інформацію, привело до загострення необхідності створення ефективних систем розмежування доступу до ІС. Одним з основних способів реалізації подібних систем є автентифікація користувачів ІС, які необхідно захищати. Існує декілька способів розв'язання задачі антентифікації, але у кожного з них є свої недоліки (неприпустимо велика імовірність неправильного розпізнавання користувача, необхідність носити з собою картки доступу або пам'ятати пароль, висока вартість та інші). Наявність вказаних недоліків робить актуальним пошук нових способів розв'язання задачі автентифікації користувачів (АК).

Завдяки використанню, для автентифікації, біометричних характеристик людини, відпадає велика кількість вказаних проблем існуючих методів розпізнавання користувачів. Останнім часом часто використовують статичні біометричні методи автентифікації, тобто ті, що використовують для розпізнавання притаманні людині фізичні параметри (відбиток пальця, параметри ока, форма обличчя та інші). Але ті з статичних методів, що забезпечують високу достовірність розпізнавання, є занадто дорогими. Цього недоліку позбавлені динамічні біометричні методи автентифікації, тобто ті, що використовують для розпізнавання поведінкові характеристики людини (голос, клавіатурний почерк, рукописний почерк та інші). Підпис людини вже дуже давно використовується для розпізнавання людини. Одним з дослідників в напрямку розпізнавання за рукописним почерком (РП) був Ланцман Р.М., а за клавіатурним почерком (КП) – Леггетт Дж. Але розвиток сучасних інформаційних технологій зробив можливим використовувати не тільки статичний підпис, а й динаміку його відтворення, що значно підвищує достовірність автентифікації. На сьогоднішній день найбільш відомі дослідницькі праці з напрямку динамічних біометричних методів автентифікації за КП та РП наступних науковців: Іванова О.І., Чалої Л.Е., Расторгуєва С.П., Брюхомицького Ю.А., Леггетт Дж., Вільямс Г., Колтел О., Кітлер Й., Амфрес Д., Блеха С.А., Бергадано Ф., Натан К.С., Грейвс А., Фіцджеральд Дж., Вонг М.Х., Генуе Р., Кечаді Т. та інш.

Розвиток методів біометричної автентифікації є актуальним не тільки для захисту ІС, а й для контролю та обліку доступу на різноманітні об'єкти, наприклад, заводи, банки, поліцейські відділи та інші об'єкти з обмеженим доступом.

Крім того, методи розпізнавання за допомогою динамічних біометричних параметрів можна використовувати не тільки для АК ІС з метою захисту від порушників, а й для виявлення факту аномального стану у людини (стресу, хвороби, тощо) та під час прийому на роботу, для аналізу таких характеристик людини, як уважність, вміння сконцентруватися, акуратність. Розв'язання останніх двох задач корисне на підприємствах для працівників найбільш критичних професій, наприклад для диспетчерів в аеропортах та для банківських працівників. Цей факт ще раз аргументує актуальність дослідження та розвитку динамічних біометричним методів розпізнавання об'єктів.

Існує декілька механізмів вирішення задачі біометричної автентифікації, одним з котрих є нейронні мережі. Враховуючи той факт, що автентифікація по суті представляє собою більш поширену задачу – задачу класифікації об'єктів, то можна сказати що найбільш придатним для вирішення цієї задачі є такий різновид нейронних мереж, як імовірнісні нейронні мережі (ІНМ). Але цей механізм вирішення даної задачі є ще не досить розвинутим, тому дослідження ефективності використання нейронних мереж та насамперед ІНМ для АК та створення систем на базі цього методу є актуальним питанням роз-

витку сучасних методів захисту інформації.

Таким чином, можна сказати, що створення біометричних методів АК ІС за їх КП та РП, використовуючи для розпізнавання ІНМ, є актуальною задачею розвитку сучасних систем захисту інформації, що зберігається, обробляється і передається в ІС.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження, що проводились, при виконанні дисертаційної роботи виконувались у відповідності з планом науково-дослідних робіт Інституту проблем моделювання в енергетиці (ІПМЕ) ім. Г.Є. Пухова НАН України в рамках наступних науково-дослідних тем: НДР «Кріт» «Розробка методів побудови та формального опису критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» №0101U006700 (2001р.–2004р.). НДР «МодА» «Дослідження і розробка методів розпізнавання, які базуються на використанні спектральних перетворень, для інформаційного забезпечення безпеки енергетичних об'єктів» №0105U001296 (2005р.–2008р.). НДР «МодБ» «Дослідження та розробка методів підвищення безпеки та ефективності розподілених високопродуктивних інформаційних технологій при вирішенні задач енергетики» №0108U010588 (2009р.–2013р.). НДР «МОД-Д» «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» №0114U002361 (2014р.–2018р.). Також частка досліджень виконувалась в рамках: Науково-технічної програми «Розвиток системи технічного захисту інформації в Україні», Постанова Кабінету Міністрів України від 21.06.2000р. №681-009 та програми робіт з організації, стандартизації та сертифікації в галузі ТЗІ це роботи, які проводились ІПМЕ ім. Г.Є. Пухова НАН України разом з КПІ в інтересах Державної служби спеціального зв'язку та захисту інформації України НДР «РизикМ» договір №239-01 від 15.09.2001р. (2001р.–2007р.). Результати дисертаційної роботи також застосовувалися при проведенні практичних робіт з експертизи технічних систем захисту. Прикладом такої роботи є експертиза «Створення та проведення первинної державної експертизи комплексної системи захисту інформації на об'єкті, що належить Департаменту військово-технічної політики, розвитку озброєння, та військової техніки Міністерства оборони України», яка виконувалась ІПМЕ ім. Г.Є. Пухова НАН України (27.06.2018р.–31.12.2018р.), відповідно до договору №149 від 27.06.2018р. Одержані результати дисертаційної роботи також застосовувались при виконанні НДР №116/09.01.09, Національного авіаційного університету «Криптографічні методи захисту в сучасних інформаційно-комунікаційних системах та мережах» (01.09.2018р.–30.06.2019р.).

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення імовірності правильного розпізнавання користувачів інформаційних систем за рахунок розробки нових методів автентифікації користувачів, які використовують для розпізнавання біометричні характеристики користувача, застосовуючи нейронні мережі для ідентифікації його біометричного образу.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

1. Проаналізувати існуючи біометричні методи розпізнавання та програмні і апаратні засоби на їх основі, з метою здійснення вибору методів автентифікації користувачів інформаційних систем, застосування яких забезпечить задану імовірність правильного розпізнавання користувачів та не потребуватиме суттєвих витрат на впровадження.

2. Розробити методи первинної обробки навчальних даних, використання яких дозволить збільшити імовірність правильного розпізнавання користувачів інформаційних систем та зменшить затрачувані ресурси.

3. Розробити методи автентифікації користувачів інформаційних систем, які базують-

ся на обраних біометричних методах розпізнавання і використовують для цього обраний різновид нейронної мережі.

4. Створити програмне забезпечення, яке на основі розроблених методів розпізнавання користувачів, виконуватиме автентифікацію користувачів інформаційних систем за обраними біометричними характеристиками, та по-перше, оцінюватиме імовірність їх правильного розпізнавання, по-друге, на основі аналізу накопичених даних даватиме змогу здійснити вибір конфігураційних параметрів систем розпізнавання.

Об'єкт дослідження: процеси біометричної автентифікації користувачів інформаційних систем на основі їх клавіатурного та рукописного почерку.

Предмет дослідження: методи автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком.

Методи дослідження: комп'ютерне моделювання (для дослідження імовірнісної нейронної мережі), статистичний аналіз (для визначення імовірності правильного розпізнавання, яку забезпечують методи автентифікації), теорія імовірності (для кількісного аналізу параметрів систем захисту), лінійна алгебра (для визначення вагових коефіцієнтів, в методах навчання імовірнісної нейронної мережі), методи емпіричних та теоретичних досліджень (для побудови методів автентфікації), комбінаторний аналіз (для визначення кількісних параметрів надійності розпізнавання), об'єктно-орієнтовані інформаційні технології (для програмної реалізації запропонованих методів), математичний апарат нейронних мереж (для автентифікації користувачів).

Наукова новизна одержаних результатів полягає в наступному:

1. Вдосконалено класифікацію біометричних систем розпізнавання, що дало змогу здійснити вибір біометричних методів автентифікації користувачів інформаційних систем, застосування яких забезпечує задану імовірність правильного розпізнавання користувачів та не потребує суттєвих витрат на впровадження.

2. Вперше запропоновано метод первинної обробки зразків клавіатурного почерку, який за рахунок аналізу спектральних характеристик почерку користувача, дозволяє виключити хибні зразки почерку, які є нехарактерними і викликані випадковими помилками користувача при наборі тексту, що забезпечує більш високу і рівномірну якість характеристик почерку і, завдяки цьому, збільшується імовірність правильного розпізнавання користувачів.

3. Вдосконалено метод автентифікації користувачів інформаційних систем за їх клавіатурним почерком, який за рахунок використання для розпізнавання імовірнісної нейронної мережі та виконання первинної обробки зразків клавіатурного почерку, збільшує імовірність правильного розпізнавання користувачів інформаційних систем.

4. Вперше запропоновано метод первинної обробки зразків рукописного почерку, в якому за рахунок автоматизації процесу відбору контрольних точок в зразках рукописного почерку, чиї характеристики аналізуються, видаленню помилкових точок п'яти типів та проведенню корекції даних трьох типів, досягається збільшення імовірності правильного розпізнавання користувачів інформаційних систем та, завдяки зменшенню кількості ознак в зразках, що аналізуються, зменшення затрачуваних ресурсів.

5. Вдосконалено метод автентифікації користувачів інформаційних систем за їх рукописним почерком, який за рахунок використання для розпізнавання імовірнісної нейронної мережі та виконання первинної обробки зразків рукописного почерку, збільшує імовірність правильного розпізнавання користувачів інформаційних систем.

Практичне значення одержаних результатів. Створене в роботі програмне забезпечення, на основі розроблених методів розпізнавання людей за клавіатурним та рукопис-

ним почерком, на базі імовірнісної нейронної мережі, може використовуватися для автентифікації користувачів в інформаційних систем; для розпізнавання працівників в системах контролю доступу та обліку користувачів; для визначення аномального стану працівника на підприємствах, на яких для їх нормального функціонування критична наявність у працівників уважності під час роботи.

Практична цінність роботи полягає в наступному:

– на основі запропонованого методу розпізнавання користувачів за їх клавіатурним почерком, з використанням методу обробки навчальних даних, створено програмне забезпечення для реалізації біометричної автентифікації користувачів інформаційних систем за їх клавіатурним почерком, яке дозволяє збільшити ступінь багатофакторності автентифікації інформаційних систем, не вимагаючи для цього додаткового обладнання.

– на основі запропонованого методу розпізнавання користувачів за їх рукописним почерком, з використанням методу обробки навчальних даних, створено програмне забезпечення для реалізації біометричної автентифікації користувачів інформаційних систем за їх рукописним почерком, що дозволяє збільшити ступінь багатофакторності автентифікації інформаційних систем, при наявності стандартних сенсорних засобів вводу графічної інформації.

– на основі результатів проведених експериментів, за допомогою розробленого програмного забезпечення, здійснено вибір конфігураційних параметрів, налаштування яких є найбільш критичним для збільшення імовірності правильного розпізнавання користувачів інформаційних систем та отримана оцінка імовірності правильного розпізнавання користувачів інформаційних систем за обраними біометричними характеристиками, яку забезпечує використання імовірнісної нейронної мережі.

– результати дисертаційних досліджень впроваджені в наступних організаціях: в Управлінні верифікації Генерального штабу Збройних сил України (акт від 25.03.2010р.), в управлінні Пенсійного фонду України у Києво-Святошинському районі (акт від 27.05.2010р.), в підприємстві «Інтегратор» (акт від 24.12.2013р.), в ТОВ «НВЦ «ІНФОЗАХИСТ» (акт від 12.12.2018р.), в ІПМЕ ім. Г.Є. Пухова НАН України (акт від 11.01.2019р.), а також використовуються у навчальному процесі кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету (акт від 29.05.2019р.).

Особистий внесок здобувача. Всі результати, які становлять основний зміст дисертації, автор отримав особисто. У роботах написаних у співавторстві, автору дисертації належить: [1] – розробка методу розпізнавання користувачів інформаційних систем за клавіатурним почерком та дослідження ефективності використання його при багатофакторній автентифікації; [2,3,25] – розробка методу автентифікації користувачів інформаційних систем за рукописним почерком; [4,6,19] – збір інформації, програмна реалізація системи біометричної автентифікації, проведення експериментів та дослідження, на основі аналізу їх результатів, процесу використання імовірнісної нейронної мережі для біометричної автентифікації з метою визначення критичних параметрів систем автентифікації; [7,8] – класифікація біометричних систем автентифікації; [15] – розробка технології попередньої обробки даних при автентифікації за клавіатурним та рукописним почерком та оцінка ефективності її застосування; [21] – дослідження особливостей використання біометричних методів в системах контролю доступу, побудова алгоритму роботи системи біометричного контролю доступу; [26] – розробка та програмна реалізація методу автентифікації користувачів за рукописним почерком для розмежування доступу до інформаційних систем; [27,28] – дослідження особливостей використання клавіатурного почерку людини для реалізації функції моніторингу.

Апробація результатів дисертації. Результати дисертації доповідались та обговорювались на конференціях та на науково-методичному семінарі, серед яких: XXIII та XXIV ЩНТК «Моделювання» (Київ, 2004р., 2005р.), V МНПК «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2002р.), пятая МНТК «Проблемы информатики и моделирования» (Харьков, 2005р.), VII ВНПК рятувальників «Пожежна безпека та аварійно-рятувальна справа: стан, проблеми і перспективи» (Київ, 2005р.), НТК молодих вчених і спеціалістів «Моделювання» (Київ, 2006р., 2010р.), НМС «Декларування безпеки об'єктів підвищеної небезпеки як засіб регулювання безпеки регіону (держави)» у рамках IV МВФ «Технології захисту – 2007» (Київ, 2007р.), 18-а НПК «Проблеми створення, розвитку та застосування інформаційних систем спеціального призначення» (Житомир, 2011р.), XX ВНПК «Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення» (Житомир, 2014р.), The Second International Conference on Computer Science, Engineering and Education Applications (ICCSEEA2019) (Kiev, 2019у.), Conférence scientifique et pratique internationale «La science et la technologie à l'ère de la société de l'information» (Bordeaux, France, 2019а.), IX МНТК «ITSec: Безпека інформаційних технологій» (Київ, 2019р.), XII МНПК «Комп'ютерні системи та мережні технології» (CSNT-2019) (Київ, 2019р.), X ВНПК «Актуальні проблеми управління інформаційною безпекою держави» (Київ, 2019), VII МНТК «Захист інформації і безпека інформаційних систем». (Львів, 2019р.).

Публікації. Матеріали дисертації опубліковано в 28 наукових працях, в тому числі в 1 науковій статі у міжнародному рецензованому виданні, що входить до бази даних Scopus [1], в 1 науковій статі у закордонному фаховому науковому журналі [2], в 1 науковій статі у міжнародному рецензованому виданні, що входить до бази даних Index Copernicus [3], в 14 статтях у наукових фахових журналах та збірниках (зокрема в 9 – без співавторів [5,9–14,16–17]) [4–17], а також в 11 тезах доповідей конференцій, в матеріалах конференцій, в тезах доповідей науково-методичного семінару (зокрема в 5 – без співавторів [18,20, 22–24]) [18–29].

Структура та обсяг дисертації. Дисертація складається з анотації, переліку умовних скорочень, вступу, чотирьох розділів, висновків, списку використаних джерел та трьох додатків. Робота містить 35 рисунків, 5 таблиць. Список використаних джерел складається з 200 найменувань і займає 20 сторінок. Додатки розміщені на 97 сторінках. Загальний обсяг дисертації складає 272 сторінок, основний текст роботи викладено на 140 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність і доцільність обраної теми дисертаційної роботи; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мета і завдання дослідження; визначено об'єкт, предмет і методи дослідження; окреслені наукова новизна та практичне значення одержаних результатів; зазначений особистий внесок здобувача; вказані апробація результатів дисертації та кількість і характер публікацій.

У першому розділі проаналізовані існуючи типи АК ІС; вдосконалено класифікацію існуючих біометричних систем розпізнавання; обрані біометричні характеристики, оптимальні для автентифікації, за їх допомогою, користувачів ІС, а саме КП та РП; виконано порівняльний аналіз найбільш поширених методів розпізнавання користувачів (з відкритих джерел) за обраними біометричними характеристиками (табл.1); проаналізовані існуючи види нейронних мереж та обраний найбільш придатний їх різновид для вирішення задачі АК, а саме ІНМ.

Вдосконалена класифікація виконується за наступними параметрами: методом біометричної автентифікації, що використовується; імовірністю правильного розпізнавання (ІПР); відкритістю характеристик, що аналізуються; методом реалізації; кількістю механізмів захисту в одній системі захисту; функціональністю; призначенням; автономністю; способом надання доступу; типом управління; багаторазовостю виконання розпізнавання; швидкістю автентифікації; роздільною здатністю; максимально можливим об'ємом інформації, що зберігається; частотою використання.

Проаналізовані наступні методи розпізнавання, які засновані на: АФЩРІВЗ – аналізі функції щільності розподілу імовірностей випадкових змінних; ВКВБ – використанні класифікатора з векторним базисом; ВШНМ – використанні штучних нейронних мереж; АСХ – аналізі статистичних характеристик; АСХФПФ – аналізі статистичних характеристик для фіксованої парольної фрази; АМОД – аналізі математичного очікування та дисперсії; АМОДДЗ – аналізі математичного очікування та дисперсії, з виконанням додаткового зважування; ВРКС – використанні рангової кореляції Спірмена; ВКР – використанні корекції рангів; АРКНПРЗК – аналізі ритму клавіатурного набору з пороговим завданням класів; АРКНПЗК – аналізі ритму клавіатурного набору з пропорційним завданням класів; ВКНС – використанні К-найближчих сусідів; ВБП – використанні багатошарового персептрона; ТААУ – технології аналізу Амфреса Д. і Вільямса Г.; ТАІ – технології аналізу Іванова; ВПММ – використанні прихованих Марковських моделей; ВБРНМ – використанні багатовимірних рекурентних нейронних мереж; FSRP – метод синтаксичного аналізу; ТАГК – технології аналізу Генуе Р. і Кечаді Т.; ВПНК – використанні параметричного навчання класифікатора. Данні методи проаналізовані за наступними характеристиками: Т – біометрична характеристика, яка використовується для автентифікації; О – імовірність помилкової відмови доступу легальному користувачеві; Н – імовірність помилкового надання доступу порушникові; Д – необхідна довжина зразка почерку; Ф – використання для аналізу функціонального стану користувача; Х – використання для аналізу характеристик, необхідних працівникам критичних професій (уважності, сконцентрованості, акуратності); Б – використання в якості етапу багатофакторної автентифікації; А – необхідність додаткового апаратного забезпечення; Л – невід'ємність; П – не-

Таблиця 1

Порівняння найбільш поширених методів розпізнавання користувачів

Характеристика / Метод	Т	О	Н	Д	Ф	Х	Б	А	Л	П	У	К
АФЩРІВЗ	КП	М	М	В	-	-	-	-	В	С	С	С
ВКВБ	КП	В	М	В	-	-	-	-	В	С	С	С
ВШНМ	КП	В	М	С	-	-	-	-	В	С	С	С
АСХ	КП	С	С	В	-	-	-	-	В	С	С	С
АСХФПФ	КП	С	В	С	-	-	-	-	В	С	С	С
АМОД	КП	М	М	В	-	-	-	-	В	С	С	С
АМОДДЗ	КП	М	М	В	-	-	-	-	В	С	С	С
ВРКС	КП	М	М	В	-	-	-	-	В	С	С	С
ВКР	КП	М	М	В	-	-	-	-	В	С	С	С
АРКНПРЗК	КП	М	М	В	-	-	-	-	В	С	С	С
АРКНПЗК	КП	М	М	В	-	-	-	-	В	С	С	С
ВКНС	КП	В	М	С	-	-	-	-	В	С	С	С
ВБП	КП	М	В	С	-	-	-	-	В	С	С	С
ТААВ	КП	В	С	В	-	-	-	-	В	С	С	С
ТАІ	КП	С	С	М	+	-	+	-	В	С	С	С
ВПММ	РП	В	В	В	-	-	-	+	В	С	С	С
ВБРНМ	РП	С	С	М	-	-	-	+	В	С	С	С
FSRP	РП	С	С	С	-	-	-	+	В	С	С	С
ТАГК	РП	М	М	С	-	-	-	+	В	С	С	С
ВПНК	РП	М	М	С	-	-	-	+	В	С	С	С

підробленість; У – унікальність; К – Стабільність. Деякі позначення значень характеристик: В – велика; С – середня; М – маленька.

Другий розділ присвячено розробці методу АК ІС за їх КП (АККП) та методу первинної обробки ЗР КП користувачів ІС (ПОЗКП), необхідного для виконання АК ІС за їх КП. В якості механізму розпізнавання використана ІНМ. Для передачі зразка КП користувача в комп'ютер, використовувалася клавіатура комп'ютера. Тобто в даному розділі будується функція *R_K* – функція розпізнавання людей за динамікою вводу пароля, який вводиться за допомогою клавіатури комп'ютера.

Для розробки методів АККП та ПОЗКП використовується наступна модель даних:

$\boldsymbol{US\_K}=\{\bigcup_{p=1}^{m} US\_K_p\}$; $p=\overline{1,m}$; m – кількість членів множини $\boldsymbol{US\_K}$; $\boldsymbol{US\_K}$ – множина користувачів, які можуть спробувати отримати доступ до системи, що захищається; $\boldsymbol{USL\_K}=\{\bigcup_{t=1}^{l} USL\_K_t\}=\{USL\_K_1, USL\_K_2,\ldots, USL\_K_t,\ldots, USL\_K_d,\ldots, USL\_K_l\}$; $t=\overline{1,l}$; l – кількість легальних користувачів; $\boldsymbol{USL\_K}$ – множина легальних користувачів даної системи; здійснюється умова, що $\boldsymbol{USL\_K}\subset\boldsymbol{US\_K}$; US_K_X – користувач ІС, який проходить автентифікацію; здійснюється умова, що $US\_K_x\in\boldsymbol{US\_K}$; USL_K_d – легальний користувач, за якого видає себе авторизована сторона, що автентифікується; здійснюється умова, що $((USL\_K_d\in\boldsymbol{US\_K})\wedge(USL\_K_d\in\boldsymbol{USL\_K}))$; $\boldsymbol{USB\_K}=\{\bigcup_{tb=1}^{lb} USB\_K_{tb}\}$; $tb=\overline{1,lb}$; lb – кількість порушників даної системи; $\boldsymbol{USB\_K}$ – множина порушників даної системи, тобто користувачів, які в ній не зареєстровані, але намагаються отримати до неї доступ; здійснюється умова, що $((\boldsymbol{USB\_K}\subset\boldsymbol{US\_K})\wedge(\boldsymbol{USB\_K}\not\subset\boldsymbol{USL\_K}))$; $\boldsymbol{AT\_K}=\{\bigcup_{if=1}^{ks\_kf+1} AT\_K_{if}\}$; $if=\overline{1,ks\_kf}$; ks_kf – кількість символів в ключовій фразі (КФ); $\boldsymbol{AT\_K}$ – множина ознак КП користувача; елементи множини $\boldsymbol{AT\_K}$: TM_K_{if} – часовий інтервал між вводом (if-1)-ого та if-ого символів КФ; $\boldsymbol{NSL}=\{\bigcup_{in=1}^{kns} NSL_{in}\}$; $\boldsymbol{NSL}_{in}=\{\bigcup_{ns=1}^{ksn} SL_{in,ns}\}$; відповідно множина $\boldsymbol{NSL}$ приймає вид: $\boldsymbol{NSL}=\{\bigcup_{in=1}^{kns}\bigcup_{ns=1}^{ksn} SL_{in,ns}\}$; $in=\overline{1,kns}$; kns – кількість наборів слів; $\boldsymbol{NSL}$– множина наборів слів, навчальні зразки (НЗ) динаміки вводу яких є в БДНЗ; $ns=\overline{1,ksn}$; ksn – кількість слів в in-ому наборі; $\boldsymbol{NSL}_{in}$ – множина слів в in-ому наборі; $\boldsymbol{NSL}_{mao}$ – набір слів, для якого амплітуда відсотка помилок у користувачів мінімальна; $\boldsymbol{O\_K}=\{\bigcup_{t=1}^{l}\bigcup_{nz=1}^{knz_t} \boldsymbol{O\_K}_{t,nz}\}$; $\boldsymbol{O\_K}_{t,nz}=\{\bigcup_{i=1}^{ks\_k} TM\_K_{t,nz,i}\}$; відповідно множина $\boldsymbol{O\_K}$ приймає наступний вид: $\boldsymbol{O\_K}=\{\bigcup_{t=1}^{l}\bigcup_{nz=1}^{knz_t}\bigcup_{i=1}^{ks\_k} TM\_K_{t,nz,i}\}$; $nz=\overline{1,knz_t}$; knz_t – кількість НЗ КП t-ого користувача в БДНЗ, які використовуються в даному сеансі розпізнавання; $\boldsymbol{O\_K}$ – множина НЗ КП з БДНЗ, які використовуються в даному сеансі розпізнавання; ks_k – кількість символів в КФ, динаміка вводу яких використовується при АК; $\boldsymbol{O\_K}_{t,nz}$ – nz-ий НЗ КП t-ого користувача, який є множиною ознак КП користувача; здійснюється умова, що $\boldsymbol{O\_K}\subset\boldsymbol{At}$; $\boldsymbol{ON\_K}=$

$= \{\bigcup_{i=1}^{ks\_k} TM\_K_i\}$; ***ON_K*** – зразок КП, якій подається на ІНМ для розпізнавання; здійснюється умова, що $\boldsymbol{ON\_K} \subset \boldsymbol{At}$.

Відповідно до розробленої моделі даних, функція *R_K* має вигляд:

$$R\_K = \begin{cases} 1, \text{ при } (US\_K_{\ X} \in \boldsymbol{USL\_K}) \wedge (US\_K_{\ X} = USL\_K_{\ d}); \\ 0, \text{ при } ((US\_K_{\ X} \in \boldsymbol{USL\_K}) \wedge (US\_K_{\ X} \neq USL\_K_{\ d})) \vee (US\_K_{\ X} \in \boldsymbol{USB\_K}). \end{cases}$$

В розробленому методі ПОЗКП виконується первинна обробка зразків КП користувачів, що накопичуються в БДНЗ. **Цей метод складається з двох етапів.**

Етап 1. Вибір ключової фрази та характеристик, що будуть аналізуватися під час АК ІС: виконується аналіз зразків з пробної БДНЗ для вибору набору КФ та символів КФ, динаміка вводу яких буде аналізуватися під час АК ІС. КФ, в даній роботі, – це слово або фраза, динаміка вводу символів з якої, буде аналізуватися під час АК ІС. Даний етап складається з двох кроків. На першому кроці, за критеріями мінімуму амплітуди ($A\_OCH\_K_{in}$) розподіл відсотка помилок ($OCH\_K_{t,in}$) у користувачів, під час вводу КФ, обирається робочий набір КФ (***NSL***$_{mao}$), тобто набір КФ, динаміка вводу яких буде аналізуватися під час АК в даній ІС. На другому кроці за допомогою пошуку мінімуму значення функції (H_i) від математичного очікування $M_{t,i}$ та дисперсії $S_{t,i}$, для значень $TM\_K_{t,nz,i}$ для кожного символу КФ, в КФ робочого набору обираються символи, динаміка вводу яких є характерною для групи користувачів. Для визначення значення функції H_i використовуються наступні формули:

$$H_i = \frac{\sum_{r=1}^{l-1} \sum_{c=r+1}^{l} \frac{(S_{r,i} + S_{c,i})}{|M_{r,i} - M_{c,i}|}}{komb}; \quad komb = \frac{l!}{2!*(l-2)!} = \frac{l!}{2*(l-2)!},$$

де *komb* - кількість можливих комбінацій з *l* по дві (кількість можливих пар для порівняння). Головною вимогою для характеристик, що аналізуються, є: H_i<1, але чим H_i менше, тим краще буде розпізнавання за цією ознакою.

Етап 2. Попередній відбір НЗ, які будуть використовуватись для розпізнавання: виконується видалення з БДНЗ, зразків з грубими помилками (ГПМ) за допомогою порівняння ознаки $TM\_K_{t,nz,i}$ з її середньоарифметичним значенням $Sr_{t,i}$ для *t*-ого користувача.

Метод АККП. У розробленому методі для АК ІС аналізується множина ознак його КП ***AT_K***, яка описана в моделі даних. Ця множина складається зі значень часових інтервалів між натисканням двох сусідніх символів КФ (TM_K_i). При цьому задачу АК можна звести до задачі класифікації або розпізнавання образів. При розробці методу АККП за основу були взяті технології розпізнавання за КП двох видів: за динамікою набору одного випадково обраного слова з заздалегідь підібраного набору слів, при цьому можуть аналізуватися всі отримані характеристики, але часові інтервали між натисканням двох сусідніх символів порівнюються з відповідними характеристиками тільки такого ж слова; за динамікою набору одного випадково обраного слова зі заздалегідь підібраного набору слів, але у всіх цих словах повинен бути однаковий фрагмент і аналізуються часові інтервали між натисканням сусідніх символів саме з цього фрагмента, хоча порівнюватися вони можуть з відповідними ознаками цього фрагмента з будь-якого слова даного набору.

Розроблений метод АККП складається з наступних дев'ятьох етапів: попереднє формування множини ознак КП користувача ІС (***AT_K***$= \{\bigcup_{i=1}^{ks\_k+1} AT\_K_i\}$); налаштування

параметрів, які є найбільш критичними при АК ІС за їх КП; накопичення пробної БДНЗ (для вибору оптимальної КФ, в роботі була накопичена пробна БДНЗ по динаміці вводу *kns* наборів з *ksn* слів, з яких кожен раз, під час АК, випадковим чином буде обиратися одне слово для вводу; при цьому, в кожному слові є послідовність символів, яка повторюється у всіх словах відповідного набору); вибір КФ на основі аналізу накопичених зразків КП з пробної бази даних (виконується Крок 1, Етапу 1, методу ПОЗКП); накопичення БДНЗ (накопичуються НЗ $\boldsymbol{O\_K}_{nz}$ з множини ознак $\boldsymbol{AT\_K}=\{\bigcup_{i=1}^{ks\_k+1} AT\_K_i\}$); вибір характеристик, що будуть аналізуватися при АК ІС (виконується Крок 2, Етапу 1, методу ПОЗКП); попередній відбір НЗ, які будуть використовуватись для розпізнавання (виконується Етап 2, методу ПОЗКП); виконання, за необхідністю, відбору за словами НЗ з БДНЗ; виконання АК ІС за їх КП.

В якості механізму автентифікації була обрана ІНМ. Для розпізнавання на ІНМ подається зразок ***ON_K***. Обрана мережа складається з чотирьох шарів. Кількісно архітектуру мережі, виходячи з даної задачі, визначається наступним чином:

1. Число вхідних елементів дорівнює числу ознак – *n*.
2. Число елементів шару зразків дорівнює числу НЗ – $\sum_{t=1}^{l} knz_t$.
3. Число елементів шару додавання дорівнює числу класів – *l*.
4. Вихідний шар має один елемент. Він визначає клас (користувач), до якого з найбільшою імовірністю належить невідомий зразок.

Активність елементу шару зразків обраховується за наступною формулою:

$$AK\_K_{nz} = \exp\left(\frac{\sum_{i=1}^{ks\_k} ON\_K_i \cdot O\_K_{i,nz} - 1}{\sigma^2}\right),$$

де σ – ширина функції активності. Для використання цієї формули, вектор вхідних даних повинен бути нормалізовано, тобто всі ознаки з множин ***ON_K*** та ***O_K*** необхідно нормалізувати. Вихідний елемент являє собою дискримінатор граничної величини, який вказує елемент шару додавання з максимальним значенням, тим самим вказує до якого класу належить невідомий екземпляр, тобто визначає ім'я користувача, який намагається отримати доступ до ІС. Якщо це ім'я дорівнює імені, що пред'явлено під час АК, тоді система дозволяє доступ до ІС.

Метод АККП має сенс використовувати не тільки, як самостійний метод автентифікації, а й як один з етапів багатофакторної автентифікації. Крім того, розроблений метод АККП можна використовувати не тільки для АК ІС, а й для моніторингу функціонального стану працівників критичних професій та під час прийому на роботу, для аналізу поточного стану таких характеристик людини, як уважність, сконцентрованість, акуратність.

Третій розділ присвячено розробці методу АК ІС за їх РП (АКРП) та методу первинної обробки зразків РП користувачів ІС (ПОЗРП), необхідного для виконання АК ІС за їх РП. В якості механізму розпізнавання використовується ІНМ. Для передачі зразка РП користувача в комп'ютер, використовувався графічний планшет (ГП), як один з варіантів пристрою з сенсорним екраном, який застосовується для динамічного передавання характеристик РП користувача. Тобто в даному розділі будується функція *R* – функція розпізнавання людей за паролем, який вводиться за допомогою ГП.

Для розробки методів АКРП та ПОЗРП використовується наступна модель даних:

$\boldsymbol{US\_R}=\{\bigcup_{p=1}^{m} US\_R_p\}$; $p=\overline{1,m}$; m – кількість членів множини ***US_R***; ***US_R*** – множина користувачів, які можуть спробувати отримати доступ до системи, що захищається; $\boldsymbol{USL\_R}=\{\bigcup_{t=1}^{l} USL\_R_t\}$; $t=\overline{1,l}$; l – кількість легальних користувачів; ***USL_R*** – множина легальних користувачів даної системи; здійснюється умова, що $\boldsymbol{USL\_R} \subset \boldsymbol{US\_R}$; US_R_X – користувач ІС, який проходить автентифікацію; здійснюється умова, що $US\_R_X \in \boldsymbol{US\_R}$; USL_R_d – легальний користувач, за якого видає себе авторизована сторона, що автентифікується; здійснюється умова, що $((USL\_R_d \in \boldsymbol{US\_R}) \wedge (USL\_R_d \in \in \boldsymbol{USL\_R}))$; $\boldsymbol{USB\_R}=\{\bigcup_{tb=1}^{lb} USB\_R_{tb}\}$; $tb=\overline{1,lb}$; lb – кількість можливих порушників даної системи; ***USB_R*** – множина порушників даної системи, тобто користувачів, які в ній не зареєстровані, але намагаються отримати до неї доступ; здійснюється умова, що $((\boldsymbol{USB\_R} \subset \boldsymbol{US\_R}) \wedge (\boldsymbol{USB\_R} \not\subset \boldsymbol{USL\_R}))$; $\boldsymbol{T}=\{\bigcup_{az=1}^{v} T_{az}\}$; $az=\overline{1,v}$; v – кількість точок в зображенні ключової фрази (КФ); $\boldsymbol{T}$ – множина всіх точок зображення; $\boldsymbol{TS}=\{\bigcup_{c=1}^{ks} \boldsymbol{TS}_c\}$; $\boldsymbol{TS}_c=$ $=\{\bigcup_{a=1}^{vc} TS_{c,a}\}$; відповідно множина ***TS*** приймає вигляд: $\boldsymbol{TS}=\left\{\bigcup_{c=1}^{ks}\bigcup_{a=1}^{vc} TS_{c,a}\right\}$; $c=\overline{1,ks}$; ks – кількість символів в КФ; ***TS*** – множина точок зображень символів КФ; $a=\overline{1,vc}$; vc – кількість точок в c-ому символі; $\boldsymbol{TS_c}$ – множина точок c-го символу; здійснюється умова, що $\boldsymbol{TS} \subset \boldsymbol{T}$; $\boldsymbol{KTS}_c=\{\bigcup_{g=1}^{w} KTS_{c,g}\}$; $g=\overline{1,w}$; w – кількість контрольних точок (КТ) в c-ому символі; $\boldsymbol{KTS}_c$ – множина КТ; $\boldsymbol{AT\_R}=\{\bigcup_{i=1}^{n} AT\_R_i\}$; $i=\overline{1,n}$; n – кількість ознак РП користувача; ***AT_R*** – множина ознак РП користувача; $\boldsymbol{AT1\_R}=\{\bigcup_{c=1}^{ks}\bigcup_{a1=1}^{3\cdot vc} ATX1\_R_{c,a1}\}=\{XT_{1,1}, YT_{1,1}, TPT_{1,1}, XT_{c,1}, YT_{c,1}, TPT_{c,1}, \ldots, XT_{c,a}, YT_{c,a}, TPT_{c,a}, \ldots, XT_{ks,vc}, YT_{ks,vc}, TPT_{ks,vc}\}$; ***AT1_R*** – множина ознак РП, які використовуються в першому раунді АК; елементи множини ***AT1_R***: ***XT***, ***YT***, ***TPT*** – вектори значень координат X і Y та типу точок зображення, відповідно; $\boldsymbol{XT} \subset \boldsymbol{AT1\_R}$; $\boldsymbol{YT} \subset \boldsymbol{AT1\_R}$; $\boldsymbol{TPT} \subset \boldsymbol{AT1\_R}$; $\boldsymbol{AT2\_R}=\{\bigcup_{c=1}^{ks}\bigcup_{a2=1}^{5\cdot vc+5} ATX2\_R_{c,a2}\}=\{TPT_{1,1}, PT_{1,1}, UT_{1,1}, TMT_{1,1}, VT_{1,1}, TPT_{c,1}, PT_{c,1}, UT_{c,1}, TMT_{c,1}, VT_{c,1}, \ldots, TPT_{c,a}, PT_{c,a}, UT_{c,a}, TMT_{c,a}, VT_{c,a}, \ldots, TPT_{ks,vc}, PT_{ks,vc}, UT_{ks,vc}, TMT_{ks,vc}, VT_{ks,vc}, PL_c, KT_c, KU_c, CH_c, KP_c\}$; ***AT2*** – множина ознак РП, які використовуються в другому раунді АК; елементи множини ***AT2_R***: ***PT***– вектор значень тиску, з яким користувач натискає ручкою (чи іншим подібним пристроєм) на сенсорний екран під час створення точок; ***UT***– вектор значень кута зміни напрямку написання при створенні точок; ***TMT*** – вектор значень часу, який пройшов від початку написання символу до створення конкретної точки; ***VT*** – вектор значень швидкості переміщення ручки від попередньої точки в дану точку; ***PL*** – вектор значень площ зображень символів; ***KT*** – вектор значень кількостей точок символів, що аналізуються під час розпізнавання; ***KU*** – вектор значень кутів нахилу символів; ***CH*** – вектор значень частот точок символів, що зафіксовано системою; ***KP*** – вектор значень кількостей повторів точок в зображені

символів (точок, які йдуть підряд, з однаковими обома координатами); ***TPT*** $\subset$ ***AT2_R***; ***PT*** $\subset$ ***AT2_R***; ***UT*** $\subset$ ***AT2_R***; ***TMT*** $\subset$ ***AT2_R***; ***VT*** $\subset$ ***AT2_R***; ***PL*** $\subset$ ***AT2_R***; ***KT*** $\subset$ $\subset$ ***AT2_R***; ***KU*** $\subset$ ***AT2_R***; ***CH*** $\subset$ ***AT2_R***; ***KP*** $\subset$ ***AT2_R***; ***O1_R***$_c$ = $\{\bigcup_{s1=1}^{3\cdot w} OX1\_R_{s1}\}$; ***O1_R***$_c$ – множина НЗ написання *c*-го символу, з БДНЗ, що подаються на ІНМ в першому раунді АК; ***O1_R***$_c$ $\subset$ ***AT1_R***; ***O2_R***$_c$ = $\{\bigcup_{s2=1}^{5\cdot w+5} OX2\_R_{s2}\}$; ***O2_R***$_c$ – множина НЗ стилю написання *c*-го символу, з БДНЗ, що подаються на ІНМ в другому раунді АК; ***O2_R***$_c$ $\subset$ ***At2_R***; ***ON1_R*** = $\{\bigcup_{s1=1}^{3\cdot w} ONX1\_R_{s1}\}$; ***ON1_R*** – зразок РП, який подається на ІНМ для розпізнавання в першому раунді АК; ***ON1_R*** $\subset$ ***At1_R***; ***ON2_R*** = = $\{\bigcup_{s2=1}^{5\cdot w+5} ONX2\_R_{s2}\}$; ***ON2_R*** – зразок РП, який подається на ІНМ для розпізнавання в другому раунді АК; ***ON2_R*** $\subset$ ***At2_R***.

В дисертаційній роботі, для підвищення якості розпізнавання користувачів, запропоновано розділити процес АК на наступні два раунди: розпізнавання КФ, що написана; розпізнавання стилю написання КФ.

Відповідно функція *R_R* має вигляд:

$$R\_R = \begin{cases} 1, \text{ при } (US\_R_{\ X} \in \textbf{\textit{USL\_R}}) \wedge (US\_R_{\ X} = USL\_R_{\ d}); \\ 0, \text{ при } ((US\_R_{\ X} \in \textbf{\textit{USL\_R}}) \wedge (US\_R_{\ X} \neq USL\_R_{\ d})) \vee (US\_R_{\ X} \in \textbf{\textit{USB\_R}}). \end{cases}$$

В даній роботі розроблено метод ПОЗРП, необхідний для виконання АК ІС за їх РП.

Розроблений метод ПОЗРП полягає у видаленні або виправленні помилок в зразках РП користувачів ІС. Необхідність цієї обробки викликана специфікою використання ГП для АК за РП.

Метод ПОЗРП складається з двох етапів, виконання яких необхідно на різних стадіях роботи методу АКРП.

Етап 1. Попередній відбір даних, які будуть використовуватись для розпізнавання: полягає у видаленні помилок перших п'яти типів (послідовність точок з нульовим тиском, крім першої подібної точки з кожної послідовності; випадкові точки, невеликої кількості; повтори, тобто послідовність точок, що йдуть підряд, у яких значення координат по обом осям не змінилися, крім випадку, коли в одній з точок нульовий тиск; випадкові невеликі загини, зазвичай, з гострим кутом, на початку ліній; неякісний зразок, який відкидається через неможливість розбивки зображення КФ на задану кількість зображень символів) і складається з п'яти кроків, на кожному з яких видаляється помилка відповідного типу. Наприклад, умовою визнання (az +1)-ої точки помилкою 3-го типу і, відповідно її видалення, є умова: $(XT_{az} = XT_{az+1}) \wedge (YT_{az} = YT_{az+1}) \wedge (PT_{az} \neq 0) \wedge (PT_{az+1} \neq 0)$.

Етап 2. Корекція даних, які будуть використовуватись для розпізнавання зразків РП користувачів ІС: полягає у виправленні помилок 6-8 типів, які викликані неправильним розміщенням написаної КФ на робочій області ГП. Для виправлення цих помилок виконувались відповідні три типи корекції даних (посимвольний поворот, посимвольний зсув та посимвольне пропорційне масштабування зображень кожного символу на всю робочу область обраного розміру), під час яких вектори ***XT***, ***YT*** перетворюються в вектори ***XTP***, ***YTP***. Перетворення відбувається на трьох кроках. Наприклад, для виконання корекції 1-го типу використовувались наступні формули:

$$UG = arctg(\frac{MAXYT_{ks} - MAXYT_1}{MAXXT_{ks} - MAXXT_1}).$$

Поворот виконується за наступними формулами:

$$SX = \frac{MAXXT_c - MINXT_c}{2};\quad SY = \frac{MAXYT_c - MINYT_c}{2};$$

$$XTP_{c,a} = round((XT_{c,a} - SX + MINXT_c)\cdot\cos(UG) + (YT_{c,a} - SY + MINYT_c)\cdot\sin(UG)) + round(SX + MINXT_c);$$

$$YTP_{c,a} = round((YT_{c,a} - SY + MINYT_c)\cdot\cos(UG) - (XT_{c,a} - SX + MINXT_c)\cdot\sin(UG)) + round(SY + MINYT_c).$$

Розроблений метод АКРП складається з наступних десяти етапів: попереднє формування множини ознак РП користувача ІС ($AT\_R = \{\bigcup_{i=1}^{n} At\_R_i\}$); налаштування параметрів, які є найбільш критичними при АК ІС за їх РП; формування БДНЗ користувачів ІС; видалення помилок 2,3,4 типів (виконуються Крок 2–Крок4, Етапу 1, методу ПОЗРП); умовне розділення зображення КФ на зображення окремих символів (з множини ***T*** формується множина ***TS***, можлива необхідність виконання Кроку 5, Етапу 1, методу ПОЗРП); корекція даних, які будуть використовуватись для розпізнавання зразків РП користувачів ІС (виконується Етап 2, методу ПОЗРП); формування множини контрольних точок; виконання першого раунду АК ІС за їх РП (розпізнавання КФ, що написана); первинна обробка зразків РП користувачів ІС, яка необхідна для виконання другого раунду АК ІС за їх РП; виконання другого раунду АК ІС за їх РП (розпізнавання стилю написання КФ).

Наприклад, **Етап 7. Формування множини контрольних точок** полягає в наступному. В даній роботі аналізуються характеристики не всіх точок, а тільки найбільш значимих для кожного символу – контрольних точок (КТ). При цьому для кожного символу, з множини $\boldsymbol{TS}_c$ виділяється множина $\boldsymbol{KTS}_c$, яка і буде використовуватися для розпізнавання. Відповідно ***XTP→XKT,YTP→YKT,TPT→TPKT, PT→PKT,UT→UKT,TMT→TMKT,VT→VKT***. Від правильності розстановки КТ значно залежить ІІР об'єктів. В даній роботі виділяються 3 типи КТ: початкові та кінцеві точки кожної лінії (на рис.1 це позначені квадратами точки 1 та 15); кутові точки ліній (на рис.1 це позначені колами точки 2,3,4, 5,6,7,9,10,11,12,13); точки перетинання ліній (на рис.1 це позначені трикутниками точки 8 та 14). Наприклад, умовою того, що a-я точка є кутовою КТ, є: $((a \neq 1) \wedge (a \neq vc) \wedge (PT_{c,a} \neq 0) \wedge (PT_{c,a-1} \neq 0) \wedge (PT_{c,a+1} \neq 0) \wedge (c_a = c_{a-1} = c_{a+1}) \wedge ((\mathrm{sgn}(XT_{c,a} - XT_{c,a-1}) \neq \mathrm{sgn}(XT_{c,a+1} - XT_{c,a}))$. Для визначення хибних кутових КТ використовується умова: $\sum_{cd=cdn}^{cdk} \sqrt{(XTP_{c,cd} - XTP_{c,cd+1})^2 + (YTP_{c,cd} - YTP_{c,cd+1})^2} < D$, (де *cdn* і *cdk* – номера, під якими зберігаються в множині $\boldsymbol{TS}_c$, відповідно дві точки, які згодом визначились як сусідні кутові КТ; *D* – довжина відрізка лінії, на якій треба залишити тільки одну, найбільш значущу кутову КТ). Якщо ця умова виконується, тоді в множині КТ треба залишити тільки ту точку, в якій кут вигину лінії менший, але не дорівнює нулю.

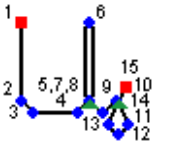

Рис. 1. Приклад розстановки КТ

На Етапі 8 та 10 для виконання першого та другого раунду АК ІС за їх РП відповідно, в якості механізму АК ІС за їх РП була обрана ІНМ. Для розпізнавання на ІНМ подаються зразки ***ON1_R*** та ***ON2_R*** відповідно, які складаються з множин ознак ***AT1_R*** та ***AT2_R*** відповідно. Кількісно архітектура мережі в 1-му та 2-му раундах АК, виходячи з даних задач, визначається наступним чином:

1. Число вхідних елементів дорівнює числу ознак – $3 \cdot w$ та $5 \cdot w+5$ відповідно.

2. Число елементів шару зразків дорівнює числу НЗ – $\sum_{cu=1}^{ks} kol\_u_{cu}$ (*kol_u* – масив, елементи якого дорівнюють кількостям НЗ для кожного з *ks* символів) та $\sum_{t=1}^{l} kol\_us_t$ (*kol_us* – масив, елементи якого дорівнюють кількостям НЗ стилю написання КФ для *l* користувачів ІС) відповідно.

3. Число елементів шару підсумовування дорівнює числу класів – *ks* та *l* відповідно.

4. Вихідний шар складається з одного елементу. Він визначає клас (відповідно символ та користувач), до якого з найбільшою імовірністю належить невідомий зразок.

Активність елементу шару зразків обраховується відповідно за формулами:

$$AK1\_R_{nz} = \exp\left(\frac{\sum_{s1=1}^{3\cdot w} ONX1\_R_{s1}\cdot OX1\_R_{s1,nz} - 1}{\sigma^2}\right),\ AK2\_R_{nz} = \exp\left(\frac{\sum_{s1=1}^{5\cdot w+5} ONX2\_R_{s1}\cdot OX2\_R_{s1,nz} - 1}{\sigma^2}\right),$$

де σ – ширина функції активності. Для використання цих формулі, вектор вхідних даних повинен бути нормалізовано. Якщо в першому раунді всі написані символи розпізнані правильно, тобто дорівнюють відповідним символам КФ, тоді приймається рішення, що КФ написана правильна. В даній роботі при цьому приймається рішення, що користувач US_R_X пройшов АК ІС успішно.

Метод АКРП має сенс використовувати не тільки, як самостійний метод автентифікації, а й як один з етапів багатофакторної автентифікації. Так як і метод АККП, метод АКРП можна використовувати не тільки для АК ІС, а й для аналізу поточного стану таких характеристик людини, як уважність, сконцентрованість, акуратність, під час прийому на роботу.

Четвертий розділ присвячено тестуванню розроблених в роботі методів АК ІС за їх КП (АККП) і за їх РП (АКРП), з використанням розроблених методів первинної обробки ПОЗКП і ПОЗРП, відповідно. В якості механізму розпізнавання використовувалась ІНМ. Для розроблених методів оцінювалась ІПР користувачів ІС при різних значеннях критичних конфігураційних параметрів системи розпізнавання. ІПР можна виразити через імовірності, що визначаються відсутністю помилок першого роду (не пропустити в систему «свого») і другого роду (пустити в систему «чужого»). Ця імовірність обчислюється за формулою: $P = P_1 \cdot P_2 = (1 - P_{o1}) \cdot (1 - P_{o2}) = 1 - P_{o1} - P_{o2} + P_{o1} \cdot P_{o2}$, де P – ІПР, P_1 – імовірність відсутності помилки 1-го роду, P_2 – імовірність відсутності помилки 2-го роду, P_{o1} – імовірність помилки 1-го роду, P_{o2} – імовірність помилки 2-го роду.

Для виконання поставлених задач, відносно АК за їх КП та РП, спочатку, на основі розроблених методів, були створені автоматизовані системи. Ці системи написані мовою C++ Builder (для АККП) та Delphi (для АКРП). Для обробки та зберігання даних використовувалася програма для роботи з базами даних Database Desktop та SQL-запити. Потім, за допомогою створеного програмного забезпечення, було накопичено пробні БДНЗ КП та РП користувачів, після чого, на основі цих даних було проведено ряд експериментів. Основні результати експериментів показані в таблиці 2 та на рис. 2-3 (для АККП) і в таблиці 3 та на рис.4-5 (для АКРП). Результати експериментальних досліджень підтверджують коректність розроблених в дисертаційній роботі методів. Більш детальний опис проведених експериментів, їх результати та зроблені висновки наведені в дисертаційній роботі.

Таблиця 2

Залежність ІПР АК ІС за їх КП, від різних значеннях критичних конфігураційних параметрів системи розпізнавання

Параметр, що змінюється	Залежність
$l = \overline{2,8}$ з кроком 1	$\Delta P<0 \because \Delta l>0$
$knz_t = \overline{100,1500}$ з кроком 100	$\Delta P>0 \because \Delta knz_t>0$
n={3,6,11}	$\Delta P>0 \because \Delta n>0$; $\Delta P_{(n(3\to6))} >> \Delta P_{n(6\to11)}$ (рис. 2)
$\sigma = \overline{0.01,1}$ з кроком 0.01	$\Delta \sigma$ слабо впливає на ΔP
$OCH\_K_{t,in} = \{\overline{1\%,6\%}, \overline{7.5\%,9.6\%,10\%,16.4\%}\}$	$\Delta P>0 \because \Delta OCH\_K_{t,in}<0$
A_OCH_K	$\Delta P>0 \because \Delta A\_OCH\_K<0$
Наявність усереднення навчальних даних (usr={true, false})	$\Delta P>0 \because usr$=false
Наявність відбору за словами (ots={true,false})	$\Delta P>0 \because ots$ =false
Наявність виключення НЗ з ГПМ ($vykl$={true,false}). Виключення за яким методом виконується (ПОЗКП, або еталонним) (a_vykl ={1,2})	$\Delta P>0 \because vykl$=true; $\Delta H<0 \because vykl$=true; ($\Delta P_{(vykl=true)} > \Delta P_{(vykl=false)}$) $\because$ чим більше l; залежність P від knz_t значно зменшується $\because vykl$=true; $H_{(a\_vykl=1)}<H_{(a\_vykl=2)}$ (рис. 3); $S_{t,i(a\_vykl=1)}< S_{t,i(a\_vykl=2)}$; $P_{(a\_vykl=1)}> P_{(a\_vykl=2)}$; чим більше значення l, тим більший ΔP у випадку $\Delta knz_t>0$.
k в $\lvert TM\_K_{t,nz,i} - Sr_{t,i}\rvert \le k * Sr_{t,i}$	$\Delta P > 0 \because \Delta k < 0$; чим менше k, тим менша залежність P від l

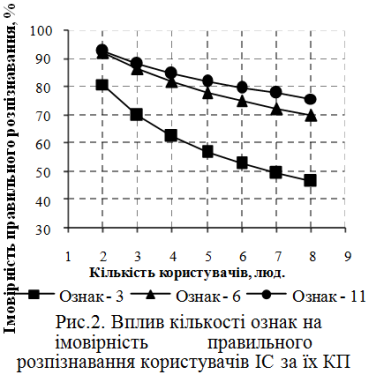

Рис.2. Вплив кількості ознак на імовірність правильного розпізнавання користувачів ІС за їх КП

Рис. 3. Вплив виключення грубих помилок на якість останніх 6 ознак в слові «телефонізація»

Таблиця 3

Залежність ІПР АК ІС за їх РП та часу розпізнавання (TR), від різних значеннях критичних конфігураційних параметрів системи розпізнавання

Параметр, що змінюється	Залежність
Використання множини КТ $\boldsymbol{KTS}_c$ кожного з 3-х типів (mkt={true,false})	$\Delta P > 0 \because mkt$ = true; $\Delta TR < 0 \because mkt$ = true (рис. 4)
Відбір найбільш значимих кутових КТ (vkt= ={true,false})	$\Delta P>0 \because mkt= vkt$; $\Delta TR<0 \because mkt= =vkt$
Видалення помилок 2-4 типів ($p24$={true,false})	$\Delta TR < 0 \because mkt$ = true; $\Delta P > 0 \because mkt$ = true
Виконання корекції 1-3 типів ($kor13$={true,false})	$\Delta P>0 \because kor13$=true (рис. 5)
D	$\Delta P > 0 \because \Delta D < 0; \Delta TR > 0 \because \Delta D < 0$
Виконання згладжування даних (sgl={true,false})	$\Delta P<0 \because \Delta sgl$= true

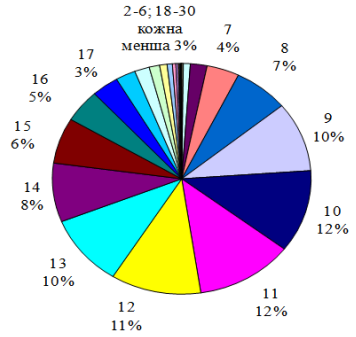

Рис. 4. Розподіл значень кількості КТ в одному символі

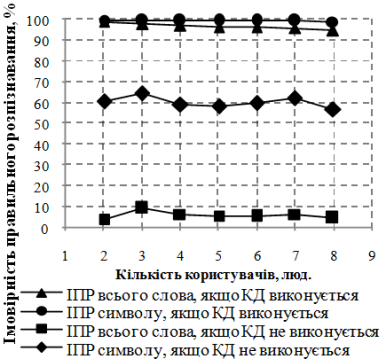

Рис. 5. Імовірність правильного розпізнавання користувачів ІС за їх РП

У додатках містяться акти впровадження результатів дисертаційної роботи, опис структури розробленого програмного забезпечення для АК ІС за їх КП і РП та лістинг основних його функцій.

ВИСНОВКИ

У дисертаційній роботі, на основі проведених теоретичних та експериментальних досліджень, розроблені методи АК ІС, які використовують для розпізнавання біометричні характеристики користувача, застосовуючи для ідентифікації біометричного образу користувача нейронні мережі, а також здійснено пошук способів підвищення ІПР користувачів ІС та зниження об'єму затрачуваних ресурсів. У результаті виконання дисертаційної роботи отримані наступні результати:

1. На основі удосконаленої класифікації існуючих біометричних систем розпізнавання та їх порівняльного аналізу, здійснено вибір біометричних методів АК ІС, застосування яких забезпечує задану ІПР користувачів та не потребує суттєвих витрат на впровадження.

2. Вперше запропоновано метод первинної обробки зразків КП, який за рахунок аналізу спектральних характеристик почерку користувача, дозволяє виключити хибні зразки почерку, які є нехарактерними і викликані випадковими помилками користувача при наборі тексту і відрізняється від еталонного методу (метод Расторгуєва С.П.) тим, що забезпечує більш високу (в 2-3 рази) та рівномірну якість характеристик почерку та, завдяки цьому, збільшується ІПР користувачів на 10-20%.

3. Вдосконалено метод АК ІС за їх КП, який за рахунок використання для розпізнавання ІНМ та виконання первинної обробки зразків КП, збільшує ІПР користувачів ІС, в порівнянні з еталонним методом (метод ВШНМ), на 4-8%.

4. Вперше запропоновано метод первинної обробки зразків РП, в якому за рахунок автоматизації процесу відбору КТ в зразках РП, чиї характеристики аналізуються, видаленню помилкових точок п'яти типів та проведенню корекції даних трьох типів, досягається збільшення ІПР користувачів ІС на 35-40% та, завдяки зменшенню кількості ознак в зразках, що аналізуються, зменшення затрачуваних ресурсів.

5. Вдосконалено метод АК ІС за їх РП, який за рахунок використання для розпізнавання ІНМ та виконання первинної обробки зразків РП, збільшує ІПР користувачів ІС, в

порівнянні з еталонним методом (метод ВБРНМ), на 7-8%.

6. На основі запропонованих методу та алгоритму розпізнавання користувачів за їх КП, з використанням методу обробки навчальних даних, створене програмне забезпечення для реалізації біометричної АК ІС за їх КП, яке дозволяє збільшити ступень багатофакторності автентифікації ІС не вимагаючи для цього додаткового обладнання.

7. На основі запропонованих методу та алгоритму розпізнавання користувачів за їх РП, з використанням методу обробки навчальних даних, створене програмне забезпечення для реалізації біометричної АК ІС за їх РП, що дозволяє збільшити ступень багатофакторності автентифікації ІС при наявності стандартних сенсорних засобів вводу графічної інформації.

8. На основі результатів проведених експериментів, за допомогою розробленого програмного забезпечення, здійснено вибір конфігураційних параметрів, налаштування яких є найбільш критичними для збільшення ІПР користувачів ІС та отримана оцінка ІПР користувачів ІС за обраними біометричними характеристиками, яку забезпечує використання ІНМ.

9. Результати дисертаційних досліджень впроваджені в наступних організаціях: в Управлінні верифікації Генерального штабу Збройних сил України (акт від 25.03.2010р.), в управлінні Пенсійного фонду України у Києво-Святошинському районі (акт від 27.05.2010р.), в підприємстві «Інтегратор» (акт від 24.12.2013р.), в ТОВ «НВЦ «ІНФОЗАХИСТ» (акт від 12.12.2018р.), в ІПМЕ ім. Г.Є. Пухова НАН України (акт від 11.01.2019р.), а також використовуються у навчальному процесі кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету (акт від 29.05.2019р.).

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1.O.Vysotska, A.Davydenko, «Keystroke Pattern Authentication of Computer Systems Users as One of the Steps of Multifactor Authentication», *Advances in Computer Science for Engineering and Education II. Advances in Intelligent Systems and Computing*, vol. 938, pp. 356-368, 2019.

2.O.Vysotska, A.Davydenko, «Authentication of information systems users, based on the analysis of their handwriting», *Scientific and Practical Cyber Security Journal (SPCSJ)*, vol.2, no.4, pp. 51-63, 2018.

3.О.Корченко, А.Давиденко, О.Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», *Захист інформації*, Том 21, №1, С. 40-51, 2019.

4.Е.А.Высоцкая, А.Н.Давиденко, «Количественный и качественный анализ учебных данных с целью повышения эффективности аутентификации пользователей комп'ютерной системы при помощи нейронных сетей», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 24, С. 110-116, 2003.

5.Е.А.Высоцкая, «Компьютерное моделирование задач аутентификации пользователя компьютерных систем с помощью вероятностных нейронных сетей», *Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова*, Вип. 24, С. 3-9, 2004.

6.Е.Высоцкая, А.Давиденко, «Исследование эффективности применения вероятностных нейронных сетей для решения задачи аутентификации пользователя компьютерных систем», *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Наук.-техн. зб.*, Вип. 9, С. 103-110, 2004.

7.Е.А.Высоцкая, А.Н.Давиденко, «Классификация биометрических систем антентификации», *Збірник наукових праць Інституту проблем моделювання в енергетиці ім. Г. Є. Пухова*, Вип. 27, С. 108-114, 2004.

8.Е.А.Высоцкая, А.Н.Давиденко, «Определение критичных параметров при выборе биометрической системы аутентификации», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 27, С. 80-86, 2004.

9.Е.А.Высоцкая, «Оценка качества методов биометрической аутентификации и способы его повышения», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 28, С. 94-102, 2004.

10.Е.А.Высоцкая, «Исключение учебных данных с грубыми ошибками, как один из способов повышения эффективности применения вероятностных нейронных сетей для аутентификации пользователей компьютерных систем по клавиатурному почерку», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 29, С. 52-59, 2005.

11.Е.А.Высоцкая, «Выбор анализируемых параметров при аутентификации пользователей компьютерных систем по клавиатурному почерку при помощи вероятностной нейронной сети», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип.30, С. 45-52, 2005.

12.Е.А.Высоцкая, «Влияние исключения учебных данных с грубыми ошибками на зависимость эффективности применения вероятностных нейронных сетей для антентификации пользователей компьютерных систем по клавиатурному почерку от различных параметров», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 28, С. 3-10, 2005.

13.Е.А.Высоцкая, «Влияние параметров учебных данных на качество аутентификации при помощи вероятностной нейронной сети», *Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України*, Вип. 32, С. 10-17, 2006.

14. Е.А.Высоцкая, «Задача распознавания написанного ключевого слова, как одна из задач, решаемых при выполнении аутентификации пользователей компьютерных систем по рукописному почерку», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип.36, С.67-76, 2006.

15.Е.А.Высоцкая, А.Н.Давиденко, «Анализ технологии предварительной обработки данных при аутентификации пользователей компьютерных систем по клавиатурному и рукописному почеркам», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 55, С. 34-41, 2010.

16.Е.А.Высоцкая, «Выбор анализируемых характеристик при аутентификации пользователей компьютерных систем по рукописному почерку на разных этапах развития вычислительной техники», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип.56, С.31-39, 2010.

17.О.О.Висоцька, «Моніторинг роботи користувачів комп'ютерних систем за допомогою технологій розпізнавання за клавіатурним почерком», *Моделювання та інформаційні технології. Зб. наук. праць*, Вип. 84, С. 119-125, 2018.

18.Е.А.Высоцкая, «Влияние параметров учебных данных на качество аутентификации пользователей компьютерных систем», *Моделювання: XXIV Науково-технічна конференція*, Київ, 2005, С. 3.

19.А.М.Давиденко, С.Я.Гільгурт, О.О.Висоцька, А.А.Кочурков, Ю.О.Чернова, «Експериментальне дослідження програми для автентифікації користувачів комп'ютерної системи за клавіатурним почерком за допомогою імовірнісної нейронної мереж»,*Проблемы информатики и моделирования: пятая междунар. научно-технич. конф.*, Харьков, 2005, С.24,66-69.

20.Е.А.Высоцкая, «Метод проведения аутентификации пользователей компьютерных систем по рукописному почерку», *Моделювання: науково-технічна конф. молодих вчених і спеціалістів*, Київ, 2006, С. 9-10.

21.А.Н.Давиденко, Е.А.Высоцкая, «Использование биометрических систем защиты для уменьшения риска возникновения чрезвычайных ситуаций», *Декларування безпеки об'єктів підвищеної небезпеки як засіб регулювання безпеки регіону (держави): науково-*

методич. семінар у рамках IV Міжнародного виставкового форуму «Технології захисту – 2007», Київ, 2007, С.123-126.

22.Е.А.Высоцкая, «Аутентификация пользователей компьютерных систем по клавиатурному почерку при помощи вероятностной нейронной сети», *Моделювання: XXIX Науково-технічна конф.*, Київ, 2010, С. 10.

23.О.О.Висоцька, «Використання біометричних технологій розпізнавання в системах моніторингу роботи користувачів комп'ютерних систем», *Проблеми створення, розвитку та застосування інформаційних систем спеціального призначення: 18-а науково-практична конф.*, Житомир, 2011, С.219-220.

24.О.О.Висоцька, «Підвищення рівня безпеки комп'ютерних систем за допомогою біометричної автентифікації», *Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення: XX Всеукраїнська науково-практична конференція*, Житомир, 2014, С. 190-191.

25.O.Vysotska, A.Davydenko, «The usage of handwriting recognition systems of information systems users for their authentication», *La science et la technologie à l'ère de la société de l'information: conférence scientifique et pratique internationale*, Bordeaux, France, 2019, vol.9, pp.48-51.

26.О.Висоцька, А.Давиденко, В.Щербина, «Формалізація процедури аналізу рукописного почерку людини для організації розмежування доступу до інформаційних систем», *ITSec: Безпека інформаційних технологій: IX Міжнародна науково-технічна конф.*, Київ, 2019, С.22-23.

27.А.М.Давиденко, О.О.Висоцька, «Визначення функції моніторингу стану санкціонованих користувачів комп'ютерних систем за допомогою аналізу їх клавіатурного почерку», *Комп'ютерні системи та мережні технології (CSNT-2019): XII Міжнародна науково-практична конф.*, Київ, 2019, С.41-42.

28.А.М.Давиденко, О.О.Висоцька, «Моніторинг функціонального стану представників критичних професій, за допомогою аналізу їх клавіатурного почерку», *Актуальні проблеми управління інформаційною безпекою держави: X Всеукраїнська науково-практична конф.*, Київ, 2019, С.201-203.

АНОТАЦІЯ

Висоцька О.О. Методи біометричної автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет. Київ, 2019.

Дисертація присвячена вирішенню задачі автентифікації користувачів (АК) інформаційних систем (ІС) за їх біометричними характеристиками. В роботі спочатку проаналізовані існуючі типи АК ІС; вдосконалено класифікацію біометричних систем розпізнавання; обрані біометричні характеристики, оптимальні для автентифікації, за їх допомогою, користувачів ІС, а саме клавіатурний почерк (КП) та рукописний почерк (РП); виконано порівняльний аналіз найбільш поширених методів розпізнавання за обраними біометричними характеристиками. Проаналізовані існуючі види нейронних мереж та обраний найбільш придатний їх різновид для вирішення задачі АК, а саме імовірнісна нейронна мережа (ІНМ). Запропоновані та програмно реалізовані методи АК ІС за їх КП та РП за допомогою ІНМ. Важливою складовою вдосконалених методів є розроблені методи первинної обробки зразків почерку, використання яких збільшує імовірність правильного розпізнавання (ІПР) користувачів ІС. На основі результатів проведених експериментів, за до-

помогою розробленого програмного забезпечення, здійснено вибір конфігураційних параметрів, налаштування яких є найбільш критичним для збільшення ІПР користувачів ІС при їх автентифікації за КП і РП та отримана оцінка ІПР користувачів ІС за обраними біометричними характеристиками, яку забезпечує використання ІНМ.

Ключові слова: автентифікація, біометрія, клавіатурний почерк, рукописний почерк, імовірнісні нейронні мережі, розпізнавання, інформаційні системи.

АННОТАЦИЯ

Высоцкая Е.А. Методы биометрической аутентификации пользователей информационных систем по их клавиатурному и рукописному почерку. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет. Киев, 2019.

Диссертация посвящена решению задачи аутентификации пользователей (АП) информационных систем (ИС) по их биометрическим характеристикам (БХ), применяя в качестве механизма распознавания нейронные сети. Также осуществляется поиск способов уменьшения затрачиваемых ресурсов и увеличения вероятности правильного распознавания пользователей (ВПР).

В ходе работы проанализированы существующие типы АП ИС, усовершенствована классификация существующих биометрических систем распознавания, выбраны БХ, оптимальные для аутентификации, с их помощью, пользователей ИС. На основе полученных результатов, для дальнейшего использования выбраны методы распознавания по клавиатурному почерку (КП) и рукописному почерку (РП). Их применение обеспечивает достаточно хорошую ВПР и не требует существенных затрат на внедрение. Затем выполнен сравнительный анализ наиболее распространенных методов распознавания по выбранным БХ. Также проанализированы существующие виды нейронных сетей и выбрана наиболее пригодная их разновидность, а именно вероятностная нейронная сеть (ВНС).

Предложены и программно реализованы два метода АП ИС – по КП и по РП. Учитывая тот факт, что динамическим БХ человека свойственна некоторая нестабильность, в качестве механизма распознавания использовалась ВНС, которая позволяет отслеживать изменения БХ пользователей ИС, тем самым, уменьшая вероятность их ошибочного распознавания. При распознавании по КП анализируются временные интервалы между нажатием аутентифицируемым пользователем на клавиатуре компьютера двух соседних символов пароля. При распознавании по РП анализируются характеристики написания аутентифицируемым пользователем пароля, на каком-либо устройстве с сенсорным экраном (например, на графическом планшете (ГП)), основные из которых, это – координаты X и Y создаваемой точки изображения пароля; ее тип; давление, с которым пользователь давит ручкой на ГП при создании точки.

Проанализировав спектральные характеристики КП и РП пользователей, для увеличения вероятности их правильного распознавания, предложены и реализованы алгоритмы первичной обработки анализируемых данных. В случае распознавания по КП, первичная обработка заключается в исключении из процесса распознавания, образцов почерка, которые содержат хотя бы один признак, чье значение отличается от средне арифметического значения этого же параметра всех хранимых учебных образцов, на значение, больше максимально допустимого (настраиваемое значение). Такие отклонения являются нехарактерными и вызваны случайными ошибками пользователя при наборе текста. Если при наборе пароля сделана ошибка (нажата ошибочная клавиша) или временной интервал перед вводом символа слишком большой (настраиваемое значение), тогда этот образец также считается ошибочным, но факт совершения ошибки сохраняется для последу-

ющего использования, как индивидуальный показатель внимательности пользователя. В случае распознавания по РП, первичная обработка также включает в себя процедуру удаления из анализируемых данных ошибочной информации, появление которой вызвано случайными ошибками пользователей и спецификой использования ГП. В работе выделяются пять типов ошибок, которые необходимо удалять и выполняется три типа коррекции данных, необходимость которой вызвана случайным характером размещения анализируемого рукописного текста на рабочей области ГП.С целью уменьшения затрачиваемых ресурсов при распознавании по РП, за счет автоматизации процесса отбора наиболее значимых точек в образцах РП, достигается уменьшение количества признаков в анализируемых образцах РП, не снижая, при этом, ВПР.

В работе создано программное обеспечение для АП ИС на базе ВНС: на языке Builder C++ для аутентификации по КП и на языке Delphi для аутентификации по РП. Для обработки и хранения информации использовалась программа для работы с базами данных Database Desktop 7.0 и SQL-запросы. С помощью созданного программного обеспечения накоплены пробные базы данных учебных образцов почерков пользователей, после чего, на основе этих данных проведено ряд экспериментов. В этих экспериментах исследовалась эффективность использования ВНС в качестве механизма распознавания пользователей по КП и РП. Также в ходе экспериментов определены конфигурационные параметры систем аутентификации, которые, при их настройке, являются наиболее критичными для снижения объема затрачиваемых ресурсов и повышения ВПР пользователей ИС.

Ключевые слова: аутентификация, биометрия, клавиатурный почерк, рукописный почерк, вероятностная нейронная сеть, распознавание, информационные системы.

ABSTRACT

Vysotska O. Methods of biometric authentication of information systems users by their keystroke pattern and handwriting. – Manuscript.

Thesis for a Candidate of Technical Science degree in specialty 05.13.21 – «Information security systems». – National Aviation University. Kyiv, 2019.

Thesis is devoted to solving the problem of authentication of information systems users (AISU) by their biometric characteristics. The work first analyzes the existing types AISU; the classification of biometric recognition systems has been improved; selected biometric characteristics, optimal for authentication, with their help, users of information systems, namely keystroke pattern and handwriting; a comparative analysis of the most common recognition methods by selected biometric characteristics was performed. Existing types of neural networks were analyzed and their most suitable variant was chosen for solving the AISU problem, namely probabilistic neural network (PNN). The methods AISU by their keystroke pattern and handwriting by means of PNN are offered and programmatically implemented. An important component of advanced methods is developed methods of primary processing of samples of keystroke pattern and handwriting, the using these methods increases the probability of correct recognition of information systems users. The choice of configuration parameters was carried out on the basis of the results of the experiments and using the developed software. Adjusting these configuration parameters is the most critical to increasing the probability of correct recognition of the information systems users when they are authenticated by keystroke pattern and handwriting. The estimation of probability of correct recognition of information systems users by the selected biometric characteristics, which is provided by the use of PNN, was obtained.

Keywords: authentication, biometrics, keystroke pattern, handwriting, probabilistic neural network, recognition, information systems.