

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ
ІНЖЕНЕРІЇ

КРУТИГОЛОВА ОЛЕГ ІГОРОВИЧ

**ДОСЛІДЖЕННЯ ПІДСИСТЕМ АВТЕНТИФІКАЦІЇ ОСОБИ В
КОМП'ЮТЕРНІЙ СИСТЕМІ З УРАХУВАННЯМ КРИТЕРІЇВ
ЗАХИЩЕНОСТІ ТА ЗРУЧНОСТІ.**

8.05010201 «Комп'ютерні системи та мережі»

Автореферат

дипломної роботи на здобуття освітнього ступеня «магістр»

Тернопіль

2017

Роботу виконано на кафедрі комп'ютерних систем та мереж Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж
Луцків Андрій Мирославович
Тернопільський національний технічний університет імені Івана Пулюя,

Рецензент: кандидат технічних наук, доцент кафедри комп'ютерних наук
Бондарчук Ігор Орестович,
Тернопільський національний технічний університет імені Івана Пулюя

Захист відбудеться 21 лютого 2017 р. о 9⁰⁰ годині на засіданні екзаменаційної комісії №35 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №1, ауд.1-603

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність роботи. Створення зручних та надійних систем аутентифікації зумовлена зростанням кількості електронних систем із якими взаємодіє людина. Такі електронні системи застосовуються практично в усіх сферах життєдіяльності людини: банківському секторі, транспорті (бронювання, замовлення та придбання квитків), освіті (системи дистанційного навчання), медицині (телемедицина), промисловості й виробництві (керування та моніторинг промислових систем), а також у сфері безпеки та оборони країни. У низці випадків питання доступу законного користувача до його даних є доволі критичним, зокрема, це стосується так званих критично важливих систем, у яких аутентифікація й всі наступні дії після авторизації мають відслідковуватись та фіксуватись у електронному журналі. Способи доступу користувачів (операторів) у електронні системи є доволі різноманітними й визначаються середовищем у якому працює користувач: персональний комп'ютер, планшет, смартфон, або спеціалізоване автоматизоване робоче місце. Обладнання, за допомогою якого користувач проходить аутентифікацію також може бути доволі різноманітним й залежати від важливості даних та інших технічних особливостей автоматизованих систем. У більшості випадків, показник захищеності комп'ютеризованих систем є величиною обернено пропорційною до зручності (англ. usability). Водночас поширеність інформаційних комп'ютеризованих систем у нашому повсякденному житті вказує на те, що фактор зручності є доволі важливим. У ході дослідження аналізується питання зручності систем аутентифікації та критерії їх вибору.

Мета і завдання дослідження. Метою роботи є розробка і дослідження ефективних моделей аналізу підсистем автентифікації користувача в комп'ютерній системі з урахуванням критеріїв захищеності та зручності.

Для досягнення поставленої мети в дипломній роботі необхідно вирішити наступні завдання:

- дослідити і класифікувати існуючі засоби і методи аутентифікації людини в комп'ютерній системі;
- дослідити комплексні математичні моделі поведінки та комфорту користувача в комп'ютерній системі;
- дослідити багатокритеріальну модель оцінки біометричних системи аутентифікації особи, відповідно до певних задач (фальсифікація даних, можливість введення допоміжних методів аутентифікації, незмінність біометричних характеристик, чутливість до зовнішніх чинників, швидкість аутентифікації, можливість безконтактної аутентифікації, психологічний комфорт користувача, вартість реалізації біометричних методів, стійкість до

фальсифікації даних та сукупність факторів).

- На основі комплексних математичних моделей поведінки та комфорту користувачів практично реалізувати прототип системи аутентифікації за стуком.

Об'єкт дослідження – засоби аутентифікації людини.

Предмет дослідження – математичні моделі аутентифікації користувачів в комп'ютерних системах.

Методи досліджень. В дипломній роботі використовуються методи системного аналізу складних взаємозв'язаних процесів, багатокритеріальний аналіз, статистичне моделювання, об'єктно-орієнтований підхід до моделювання і розробки складних систем.

Наукова новизна одержаних результатів. У роботі досліджена комплексна математична модель поведінки та комфорту користувача в комп'ютерних системах, що базується на часових і просторових моделях, з використанням функції щільності ймовірності, й враховує динаміку поведінки користувачів, статистичні властивості поведінки користувачів. Статистичні параметри аутентифікованої особи призначені для виявлення можливих змін в поведінці користувачів й використовуються як засіб ідентифікації користувача в системі.

Практичне значення отриманих результатів. На основі комплексних математичних моделей поведінки та комфорту користувачів практично реалізований прототип системи аутентифікації за стуком, що дозволяє ідентифікувати користувача досить точно і навіть може бути підлаштована під ритм індивідуально для кожної окремої людини за звичним для людини стуком по поверхні (стукіт у двері).

Апробація результатів роботи. Основні положення дипломної роботи проводився на міжнародній науково-технічній конференції молодих учених та студентів. Актуальні задачі сучасних технологій – Тернопіль 17-18 листопада 2016.

Публікації. Основний зміст роботи викладений у тезах доповідей наукової конференції.

Структура та об'єм роботи. Дипломна робота складається з вступу, 6 розділів, висновків, списку використаних джерел та 2 додатків на 12 сторінках. Загальний обсяг дисертації – 113 сторінки, основний текст дисертації містить 17 таблиці та 14 рисунків.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовані доцільність та актуальність проблеми, мета роботи,

її значимість для науки і техніки, викладена суть виконаних досліджень.

У першому розділі роботи розглянуто поширеності типів комп'ютерних систем, здійснено загальний аналіз методів аутентифікації: парольна аутентифікація, біометричні методи і статичні методи, визначені їх переваги і недоліки. Аналіз показує, що дані технологія аутентифікації із застосуванням біометричних методів має достатньо суттєві переваги ґрунтовані на характеристиці людини, тобто унікальній властивості, даній їй від народження і невід'ємній від нього.

У даному розділі здійснений аналіз рольових моделей роботи користувача, які показують, що більшість сучасних методів розпізнавання не пропонують можливості описувати користувача з різних точок зору, розглядати окремі сторони його взаємодії з комп'ютером спільно, що допускає збільшення надійності аутентифікації. Також в даному розділі розглянуто характеристики для визначення надійності та зручності систем аутентифікації, де зручність характеризують: швидкість, ефективність, простота навчання і доступність запам'ятовування. За надійність у свою чергу відповідають помилки: FAR, FFR і EER. Аналіз існуючих характеристик показав, що саме дані характеристики можуть виступати основою для проведення дослідження згідно теми дипломної роботи.

У другому розділі досліджено метод який базується на функції щільності ймовірності даних, які отримані з сенсора. Сенсор отримує часове і просторове розміщення особи, яка проходить аутентифікацію. Тут розглядаються математичні моделі користувача, модель забезпечення комфорту і проаналізовані методи розрахунку параметрів FAR і FRR. Процес навчання системи аутентифікації і визначення відповідного порогу розпізнавання на основі даних моделей дає змогу максимально автоматизувати процес аутентифікації й зробити його максимально прозорим для людини, що проходить аутентифікацію. Також тут наведено розрахунки характеристик FAR і FRR, які дають змогу налаштувати будь-яку біометричну систему на різний ступінь «щільності», тобто на різне значення FAR. Як вже зазначалося, це означає, що система буде налаштована таким чином, що ймовірність помилки визначення зловмисника за клієнта буде мінімальною. Але зменшення FAR завжди приводить до зменшення чутливості методу або, що еквівалентно до збільшення FRR, тобто ймовірності того, що система не розпізнає зареєстрованого в ній об'єкта. Т.ч., чим більш строго налаштована система на блокування зловмисника, тим вона менш чутлива, а це значить, що вона гірше пропускає зареєстрованого користувача. Також в даному розділі розглянуті критерії вибору техніки аутентифікації на основі багатокритеріальної моделі оцінки біометричних системи аутентифікації особи. Також в даному розділі описані тенденції застосування методів

мобільної біометрії. Яка базуються на рольових моделях користувачів, що робить їх невід'ємною складовою зручної організації захисту даних. У даному розділі здійснений багатокритеріальний аналіз, що базується на алгоритмах обчислення біометричної інформації і також згідно нього здійснено порівняльний аналіз методів біометричної інформації на основі методу відносної ентропії.

У третьому розділі розглянуті питання, пов'язані з апаратною і програмною реалізацією власного прототипу системи аутентифікації на основі досліджених математичних моделей. Проаналізована система забезпечує аутентифікацію особи за секретним стуком по поверхні. Для реалізації системи було використано апаратно-програмну платформу Arduino і п'єзо датчик. Це дало можливість використовувати запропоновану систему в звичному для людини середовищі, а також забезпечити необхідну надійність і адаптивність під індивідуальні вимоги безпеки. Проведено обчислювальний експеримент та розраховано параметри FARi FRR.

В частині «Обґрунтування економічної ефективності» розглянуто питання організації виробництва і проведено розрахунки техніко-економічної ефективності проектних рішень.

В частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто питання планування робіт по охороні праці в приміщенні, де проектується система, правові основи забезпечення безпеки в надзвичайних ситуаціях, а також проаналізовано заходи щодо усунення виникнення надлишкової напруги на корпусах обладнання чи при випадковому дотиканні до струмопровідних частин.

В частині «Екологія» проаналізовано сучасний екологічний стан України, розглянуто питання забруднення довкілля, що виникає внаслідок розробки і використання системи аутентифікації, а також запропоновано заходи щодо їх усунення.

ВИСНОВКИ

1. Здійснено аналіз існуючих засобів і методів аутентифікації людини в комп'ютерній системі, зокрема: парольна аутентифікація та біометричні методи (статичні і динамічні). Також проаналізована багатофакторна аутентифікація. Проведено аналіз рольових моделей роботи користувача в системі аутентифікації. Показано, що більшість сучасних методів розпізнавання, на основі відповідних математичних моделей, не дають змоги комплексно описувати користувача, зокрема розглядати окремі аспекти його взаємодії з комп'ютером. Сформульовано вимоги до математичних моделей як враховують ці недоліки.

2. Проведено багатокритеріальний аналіз параметрів біометричних системи аутентифікації особи, відповідно до наступних критеріїв зокрема: фальсифікація даних, можливість введення допоміжних методів аутентифікації, незмінність біометричних характеристик, чутливість до зовнішніх чинників, швидкість аутентифікації, можливість безконтактної аутентифікації, психологічний комфорт користувача, вартість реалізації біометричних методів, стійкість до фальсифікації даних та сукупність факторів. А також здійснено розрахунок характеристик FAR і FRR, які дають змогу налаштувати будь-яку біометричну систему на різний ступінь «пильності», тобто на різне значення FAR. Це означає, що система буде налаштована таким чином, що імовірність помилки визначення зловмисника за клієнта буде мінімальною. Але зменшення FAR завжди приводить до зменшення чутливості методу або, що еквівалентно до збільшення FRR, тобто ймовірності того, що система не розпізнає зареєстрованого їй об'єкта. Т.ч., чим більш строго налаштована система на блокування зловмисника, тим вона менш чутлива, а це значить, що вона гірше пропускає зареєстрованого користувача.
3. На відміну від існуючих підходів, запропонована модель дозволяє забезпечити комплексний підхід до методу аутентифікації користувачів за біометричною ознакою фізичної ритмічної вібрації (зокрема стуку по поверхні з певним ритмом). Здійснено комплексний аналіз математичних моделей поведінки користувачів та обґрунтовано їх використання. Математичні моделі будуються поведінкових характеристиках і унікальних особливостях аутентифікованої особи.
4. На основі комплексних математичних моделей поведінки та комфорту користувачів практично реалізований прототип системи аутентифікації за стуком, що дозволяє ідентифікувати користувача досить точно і навіть може бути підлаштований під ритм індивідуально для кожної окремої людини за звичним для людини стуком по поверхні (стукіт у двері). Для реалізації даного прототипу було використано: апаратно-обчислювальну платформу Arduino Leonardo, п'єзоперетворювач (сенсор розпізнавання звукових коливань та вібрації) і відповідне програмне рішення. З їх допомогою показано альтернативний спосіб біометричної аутентифікації, який володіє високою надійністю, є доступний за ціною і простий в застосуванні. Очевидним є те що можна, розробити й інші способи біометричної аутентифікації людини, більш широко використовуючи досліджувані моделі користувача.

ОСНОВНИЙ ЗМІСТ РОБОТИ ВИКЛАДЕНО У ТАКИХ ПУБЛІКАЦІЯХ:

Луцків А.М. Критерії вибору систем біометричної аутентифікації / А.М. Луцків, О.І. Крутигорова // Актуальні задачі сучасних технологій : зб. тез доповідей міжнар. наук.-техн. Конф. Молодих учених та студентів, (Тернопіль, 17–18 листоп. 2016.) / М-во освіти і науки України, Терн. націон. техн. ун-т ім. І. Пулюя [та ін]. – Тернопіль : ТНТУ, 2016. – 71-73С.

АНОТАЦІЯ

Крутигорова О.І. Дослідження підсистем автентифікації особи в комп'ютерній системі з урахуванням критеріїв захищеності та зручності.

Дипломна робота магістра. 8.05010201 - Комп'ютерні системи та мережі. Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль 2017.

Дипломна робота присвячена дослідженню комплексної математичної моделі поведінки та комфорту користувача в комп'ютерних системах, що базується на часових і просторових моделях, з використанням функції щільності ймовірності, що враховує динаміку поведінки користувачів, сеансову (статистичну) складову, а саме: статистичні властивості поведінки користувача, необхідні для виявлення можливих змін в його поведінці, як засіб ідентифікації користувача в системі. Також досліджено, багатокритеріальну модель оцінки біометричних системи аутентифікації особи, відповідно до наступних критеріїв зокрема: фальсифікація даних, можливість введення допоміжних методів аутентифікації, незмінність біометричних характеристик, чутливість до зовнішніх чинників, швидкість аутентифікації, можливість безконтактної аутентифікації, психологічний комфорт користувача, вартість реалізації біометричних методів, стійкість до фальсифікації даних та сукупність факторів.

На основі комплексних математичних моделей поведінки та комфорту користувачів практично реалізований прототип системи аутентифікації за стуком, що дозволяє ідентифікувати користувача досить точно і навіть може бути підлаштований під ритм індивідуально для кожної окремої людини за звичним для людини стуком по поверхні (стукіт у двері).

Ключові слова: біометрична аутентифікація, рольові моделі користувачів, надійність системи, критерії оцінки, сеансова модель, алгоритм, порівняльний аналіз.

ANOTATION

Krutyholova O.I. Investigation of human authentication subsystems in a computer system based on safety and convenience criteria.

The diploma paper for Master's Computer systems and network – Ternopil Ivan Puluj National Technical University, Ternopil 2017.

The diploma paper is dedicated to the research of complex mathematical model of behavior and user comfort in the computer systems that are based on time and spatial samplers, using the function of compactness probability, namely: statistical characteristics of the user behavior, necessary for defining the possible changes in his behavior, as means of identification the user in the system.

We have also examined the multicriteria model of biometric system evaluation of person authentication according to the following criteria: the falsification of data, the possibility of introduction the subsidiary methods of authentication, the invariability of biometric characteristics, the sensibility to external factors, the speed of authentication, the possibility of noncontact authentication, the psychological comfort of the user, the cost of realization of biometric methods, the stability to data falsification and the combination of factors.

On the basis of complex mathematical models of the behavior and user comfort the prototype of system authentication according to knock is almost realized. It allows identifying the user quite precisely and even can be adapted to the individual rhythm for each person according to knocking on the surface (knocking at door).

Key words: biometric authentication, user role models, reliability of system, the criteria of evaluation, session model, algorithm, comparative analysis.