Тернопільський національний технічний університет
імені Івана Пулюя

Макаров Ігор Євгенович

УДК 519.711.3:343.98

ЗАСОБИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ОСОБИ У СИСТЕМАХ МОНІТОРИНГУ СТАНУ ЗДОРОВ'Я

163 – Біомедична інженерія

Автореферат дипломної роботи магістра

Тернопіль – 2018

Роботу виконано на кафедрі біотехнічних систем Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: кандидат технічних наук, доцент,
завідувач кафедри біотехнічних систем
Ткачук Роман Андрійович,
Тернопільський національний технічний університет
імені Івана Пулюя,

Захист відбудеться 26 грудня 2018 р. о $10^{.00}$ годині на засіданні екзаменаційної комісії №22 у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Текстильна, 28, навчальний корпус №9, ауд. 9-507.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Впровадження біометричних систем в життя суспільства є незаперечним фактом. Світові аналітики прогнозують підвищення попиту на біометрії в усіх галузях і розширення сфери її застосування.

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об’єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; інформаційна безпека; облік робочого часу та реєстрація відвідувачів; системи голосування, проведення електронних платежів; автентифікація на Web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (перетин державних кордонів, видача віз на відвідування країни).

Ідентифікація на основі біометричні данні - це засіб автоматичного розпізнавання особистості на базі унікальних фізичних або поведінкових параметрів. Ідентифікація виконується за допомогою порівняння отриманих біометричних характеристик і шаблонів, що зберігаються у базі даних.

Для користувачів, які застосовують системи біометричної ідентифікації і автентифікації, дуже важливим є зручність застосування цих засобів (це не тільки швидкість і простота проведення процедури, але і можливість використання звичного обладнання). На сьогодні оптимальним співвідношенням між надійністю автентифікації, ціною і зручністю використання має визначення особистості по обличчю, чим і пояснюється високий темп розвитку і поширення таких технологій.

Невпинне розширення сфери застосування засобів комп'ютерної обробки інформації і комп'ютерних засобів телекомунікації залучають до сфери інформаційних технологій все більше коло людей, що підвищує ризики виникнення інформаційних загроз та їх реалізації. Не зважаючи на широкі технологічні можливості забезпечення захисту, на сьогоднішній день, кількість злочинів та шахрайства зростає з кожною хвилиною.

Однією з найпоширеніших технологій захисту є біометричні системи захисту. Вони є найзручнішими, оскільки не потребують зберігання у пам’яті складних паролів чи носіння з собою спеціальних ідентифікаторів (ключів, карток, і т. ін..), а достатньо буде тільки сказати кодове слово, прикласти палець чи кисть руки, або підставити лице для сканування, щоб отримати доступ.

Одна з головних переваг біометричних технологій – відсутність необхідності в паролі. При використанні біометричної автентифікації користувачам не потрібно пам'ятати складні паролі, а співробітникам служб технічної підтримки - вирішувати пов'язані з цим проблеми. Біометричні пристрої відрізняються величезною різноманітністю і використовують для автентифікації людини різні біологічні параметри.

Необхідно відзначити, що останні розробки біометричних систем захисту інформації прекрасно взаємодіють з новими інформаційними технологіями, зокрема, з мережевими технологіями зв'язку, такими як Інтернет і стільникові системи зв'язку. Аналіз показує, що сучасні можливості біометричних технологій вже сьогодні забезпечують необхідні вимоги по надійності автентифікації, простоті

використання і низької вартості засобів автентифікації користувача та є дуже перспективними на найближчі десятиліття.

Актуальність біометричного захисту є беззаперечною оскільки такий захист є значно ефективніший порівняно з такими методами, як використання смарт-карт, паролів, PIN-кодів і тому подібне, оскільки біометрія дозволяє ідентифікувати людину, а не пристрій. Традиційні методи захисту не виключають можливості втрати або крадіжки інформації, унаслідок чого вона стає доступною незаконним користувачам.

Вирішення задачі захисту з використанням біометричних характеристик є актуальною задачею, що стає популярнішою щодня, це є цілком виправдано враховуючи преваги які надають дані методи захисту.

Мета і задачі дослідження. *Метою дослідження* є розробка засобів біометричної ідентифікації особи у системах моніторингу стану здоров'я за допомогою клавіатурного почерку на основі нейромережевої моделі.

Досягнення цієї мети вимагає розв'язання таких задач:

1. Проаналізувати основні існуючі методи біометричного захисту та їх основні складові.
2. Дослідити основні можливі механізми реалізації відомих методів біометричної ідентифікації та визначити найбільш оптимальний метод.
3. Розробити засіб біометричної ідентифікації особи у системах моніторингу стану здоров'я за допомогою клавіатурного почерку на основі нейромережевої моделі.

Об'єкт дослідження: процес біометричної ідентифікації особи

Предмет дослідження: метод автентифікації за клавіатурним почерком.

Методи дослідження на базі теорії обчислювальних процесів для обґрунтування створення програмного забезпечення інформаційно-аналітичної системи модульного типу. Для програмної реалізації алгоритмів опрацювання використано об'єктно-орієнтовану мову програмування Java.

Наукова новизна отриманих результатів. Удосконалено метод автентифікації за клавіатурним почерком з послідовним використання мережі Кохонена та ймовірнісної нейромережі; вперше використано метод автентифікації за клавіатурним почерком на основі нейромережевого підходу за рахунок двоблокової нейромережевої моделі; удосконалено підхід до автентифікації за клавіатурним почерком за рахунок надання додаткової інформації стосовно фізично стану.

Апробація результатів дослідження. Викладені в дипломній роботі результати доповідалися і обговорювалися на X Всеукраїнській студентській науково-технічній конференції „Природничі та гуманітарні науки. Актуальні питання" (м. Тернопіль, 2017 р.).

Структура та обсяг. Дипломна робота складається із вступу, семи розділів, висновку, викладених на 94 сторінках, списку використаних джерел на 5 сторінках, додатків на 9 сторінках. Загальний обсяг роботи становить 108 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі шляхом аналізу та порівняння методів і засобів оцінювання варіабельності рівня глюкози в крові для пацієнтів з діабетом обґрунтовано актуальність теми роботи, сформульовано мету і задачі дослідження, визначено об’єкт, предмет і методи дослідження, показано наукову новизну та практичне значення отриманих результатів, розкрито питання апробації результатів роботи на конференціях і семінарах.

У першому розділі «Стан і тенденції розвитку систем біометричної ідентифікації» представлено загальний опис внутрішніх особливостей, що набули найбільшого поширення у біометричних технологіях.

Аналіз показав, що підвищення захисту інформації в інтелектуальних системах моніторингу стану здоров’я досягається за рахунок сертифікації, ліцензування та впровадженням необхідних засобів технічного й програмного захисту; створення спеціалізованих організаційних структур, які забезпечують постійне функціонування захисту та засобів генерації ключів і паролів.

Підвищення ефективності захисту інформації в системах моніторингу стану здоров’я досягається сумісним використанням декількох методів захисту інформації. Використання спеціальних цифрових носіїв підвищує захист інформації в системах моніторингу стану здоров’я.

У другому розділі «Механізми реалізації відомих методів біометричної ідентифікації» на основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів систем моніторингу стану здоров’я, можна впевнено сказати, що парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використовування інших механізмів захисту парольний захист, сам по собі, не є надійним, оскільки не може забезпечити потрібного захисту. Досить розповсюдженими в якості ідентифікаторів є також різноманітні електронні ключі (токени, карти і т.п.). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до систем моніторингу стану здоров’я. Таким чином, розглянувши технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем комплексної (або багатофакторної) ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до парольної аутентифікації. Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об’єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/аутентифікації, яке обираєте (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого»

потрібно захищати). Але безперечною порадою є обов'язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів систем моніторингу стану здоров'я**.**

У третьому розділі «Прототип мобільного додатку**»** встановлено, що сучасні методи ідентифікації особи не спроможні забезпечити необхідний рівень надійності. Одним із можливих рішень цієї проблеми є застосування біометричних технологій для ідентифікації особи. Біометричні технології, на відміну від парольної ідентифікації, є більш надійними та дозволяють значно підвищити певність процесу ідентифікації особи, для них вже створена розвинена база технічних рішень. Звідси можна зробити висновок, що в інфокомунікаційних мережах процес ідентифікації особи буде реалізовуватися саме на базі біометричних технологій.

У четвертому розділі «Спеціальна частина» описано методика ідентифікації за біометричними параметрами.

У п'ятому розділі «Обґрунтування економічної ефективності» на підставі виконаних розрахунків та нормативних даних встановлено, що планова калькуляція вартості проведення досліджень по темі становить 72421,87 грн., а кількісна оцінка науково-технічна ефективність науково-дослідної роботи, яка здійснюються експертним шляхом за десятибальною шкалою і визначається як середньоарифметичне, що складає 0,685 від максимального числа 1, а рекомендації за результатами виконання НДР можуть бути сформульовані після ретельного аналізу отриманих результатів

У шостому розділі «Охорона праці та безпека в надзвичайних ситуаціях**»** висвітлено результати проведеного аналізу шкідливих факторів та чинників, що впливають, або можуть вплинути, на коректну роботу персоналу установи, де використовується представлений метод дослідження пацієнта з використанням спеціального обладнання. Був встановлений чіткий порядок розробки і впровадження технологій та вимог, щодо запобігання шкідливим факторам та чинникам.

У восьмому розділі «Екологія» проаналізовано питання екології.

У **додатках** наведено тексти програм, розроблені для ПК (ОС Windows XP).

ВИСНОВКИ

У дипломній роботі магістра розв'язано актуальну наукову задачу розробка засобів біометричної ідентифікації особи у системах моніторингу стану здоров'я за допомогою клавіатурного почерку на основі нейромережевої моделі.

При цьому отримано такі результати:

Загальний опис внутрішніх особливостей, що набули найбільшого поширення у біометричних технологіях та їх аналіз показав, що підвищення захисту інформації в інтелектуальних системах моніторингу стану здоров'я досягається за рахунок сертифікації, ліцензування та впровадженням необхідних засобів технічного й програмного захисту; створення спеціалізованих організаційних структур, які забезпечують постійне функціонування захисту та засобів генерації ключів і паролів.

Підвищення ефективності захисту інформації в системах моніторингу стану здоров’я досягається сумісним використанням декількох методів захисту інформації. Використання спеціальних цифрових носіїв підвищує захист інформації в системах моніторингу стану здоров’я.

На основі аналізу загроз інформаційній безпеці та існуючих засобів ідентифікації та аутентифікації користувачів систем моніторингу стану здоров’я, можна впевнено сказати, що парольний захист на сьогодні є одним з найпоширеніших способів захисту інформації від несанкціонованого доступу як в окремих комп'ютерах і системах, так і в мережах світового масштабу. Проте без використовування інших механізмів захисту парольний захист, сам по собі, не є надійним, оскільки не може забезпечити потрібного захисту. Досить розповсюдженими в якості ідентифікаторів є також різноманітні електронні ключі (токени, карти і т.п.). Але слід зауважити, що останнім часом все більшого поширення набувають системи ідентифікації, які використовують біометричні характеристики людини при вирішенні задачі доступу до систем моніторингу стану здоров’я.

На основі аналізу технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем комплексної (або багатофакторної) ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до парольної аутентифікації. Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об’єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації/аутентифікації, яке обираєте (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого» потрібно захищати). Але безперечною порадою є обов’язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів систем моніторингу стану здоров’я.

АНОТАЦІЯ

Макаров Ігор Євгенович. Метод оцінювання варіабельності рівня глюкози у крові для глюкометричних систем. – Рукопис.

Дипломна робота магістра за спеціальністю 163 – біомедична інженерія, Тернопільський національний технічний університет імені Івана Пулюя, Тернопіль, 2018.

Дипломну роботу магістра присвячено розробленню засобів біометричної ідентифікації особи у системах моніторингу стану здоров’я за допомогою клавіатурного почерку на основі нейромережевої модел

В роботі встановлено, що підвищення захисту інформації в інтелектуальних системах моніторингу стану здоров’я досягається за рахунок сертифікації, ліцензування та впровадженням необхідних засобів технічного й програмного захисту; створення спеціалізованих організаційних структур, які забезпечують постійне функціонування захисту та засобів генерації ключів і паролів.

На основі аналізу технології апаратної (або електронної), парольної, біометричної ідентифікації та аутентифікації можна зробити висновок, що надалі у міру зростання обчислювальних потужностей все більш запитаним буде саме вживання систем комплексної (або багатофакторної) ідентифікації та аутентифікації, що дозволить уникнути людських помилок, зв'язаних із застосуванням слабких паролів і посилити вимоги до парольної аутентифікації.

Ключові слова: біометрія, ідентифікація, система контролю

SUMMARY

Makarov I. The means of a person biometric identification in the health monitoring systems. – Manuscript.

Master's thesis work on specialty 163 – biomedical engineering, Ternopil National Technical University named after Ivan Pul'uj, Тернопіль, 2018.

The thesis of the master's degree is devoted to the development of means of biometric identification of a person in health monitoring systems with the help of keyboard handwriting based on a neural network model

The work determined that the increase of information security in intelligent health monitoring systems is achieved through certification, licensing and implementation of the necessary means of technical and software protection; Creation of specialized organizational structures that ensure the continuous functioning of protection and means of generating keys and passwords.

Based on the analysis of the hardware (or electronic), passive, biometric identification and authentication technology, it can be concluded that in the future as the computing power grows, the use of complex (or multi-factor) identification and

authentication systems will be increasingly demanded, thus avoiding human errors, ie using weak passwords and enforcing password authentication requirements.

Keywords: biometrics, identification, control system/