

АНОТАЦІЯ

Дослідження систем прийняття рішень в біометричних системах аутентифікації людини // Дипломна робота // Комарніцький Максим Костянтинович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних систем та мереж, група СІм-61 // Тернопіль, 2014 // с. – 123, рис. – 14, табл. – 11, кресл. – 7, додат. - 2, бібліогр. – 31.

Робота присвячена дослідженню систем прийняття рішення в біометричних системах аутентифікації людини. Проаналізувавши існуючі методи аутентифікації, для дослідження системи було обрано біометричні дані отримані внаслідок динамічного введення підпису. Динамічний підпис має стохастичний нестационарний характер і він піддається дії випадкових факторів під час введення: початкова точка вводу, розмах стилуса та тривалість відтворення. Для розв'язку задачі аутентифікації людини за динамічним підписом використано методи його обробки і застосовано нормований підпис, у вигляді вектора двох гаусових випадкових процесів. Використано такі класи аутентифікаційних ознак як математичне сподівання та дисперсія нормованого підпису для визначення величини «коридору» допуску особи в систему. Враховуючи, що кожного разу при аутентифікації отримуються різні біометричні дані, розроблено алгоритм допуску в систему та зберігання даних. Запропонована схема нечіткого екстрактора, що складається з безпечного скетчу та екстрактора. Робота нечіткого екстрактора базуються на використанні помилко-коректуючих кодів Ріда-Соломона та хеш-функції SHA-256. Розроблені методи обробки біометричних даних дозволяють сформулювати криптографічний ключ використовуючи нечіткий екстрактор. Розроблено програмне забезпечення для отримання, обробки, імітаційного моделювання та аутентифікації за динамічним підписом.

Ключові слова: безпечний скетч, біометрична аутентифікації людини, динамічно введений підпис, імітаційне моделювання, коди Ріда-Соломона, математична модель, нечіткий екстрактор, статистичні методи обробки, SHA-256.