Повідайко П. М., к.т.н., доц.
Іванюк В.А., магістрант, факультет ІКТ, гр.СІ-66м
Житомирський державний технологічний університет

БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ В СИСТЕМАХ КОНТРОЛЮ ДОСТУПУ НА ОБ'ЄКТ

Засоби ідентифікації біометричних даних є важливими компонентами сучасних інтелектуальних інформаційних систем. Вони забезпечують перевірку справжності суб'єкта відповідно до заявленого ним ідентифікатора і дозволяють впевнитись у тому, що суб'єкт є дійсно тим, за кого він себе видає. При виборі методу ідентифікації слід передбачити надійний захист від зловмисних дій. Поряд з такими характеристиками системи ідентифікації, як швидкодія й об'єм пам'яті, ступінь захищеності та стійкості від загроз є дуже важливим параметром.

Для порівняння ефективності та надійності методів біометричної ідентифікації розглянуто найбільш розвинені на даний момент біометричні технології розпізнавання за статичними характеристиками: за відбитком пальця, формою долоні, райдужною оболонкою ока та голосом.

Серед біометричних методів ідентифікації суб'єкта найбільш практичними вважаються ті, що використовують ознаки: відбитки пальців, райдужну оболонку ока, риси обличчя. Їх і взято за основу дослідження. Для оцінки надійності та ефективності взято розрахунки коефіцієнта помилкової відмови в доступі та коефіцієнта помилкового допуску особи на об'єкт, а також усереднену вартість встановлення таких систем.

Виходячи з цього, для вирішення задач інформаційної безпеки найбільш оптимальним є використання систем, побудованих на скануванні і розпізнаванні відбитка пальця. Даний метод має коефіцієнт помилкової відмови в доступі всього лише 5%, коефіцієнт помилкового допуску особи на об'єкт - 10^{-9}. Усереднена вартість таких систем становить близько 200$, що на порядок нижче, наприклад, ніж у системах розпізнавання райдужної оболонки ока чи термограми обличчя.

У порівнянні з технологіями розпізнання за сітківкою і райдужною оболонкою ока сканування відбитка пальця є дешевшим і зручнішим, сканери відбитків пальців на порядок менш громіздкі і процес безпосереднього зчитування ідентифікуючих ознак проходить швидко і не викликає дискомфорту. Також, у технології ідентифікації за відбитком пальця на кілька порядків кращі статистичні показники помилок першого і другого роду. Це ж відноситься і до систем розпізнання за голосом.

Візерунки відбитка пальців мають такі властивості: індивідуальність, неповторність, стійкість, відновлюваність. Ці властивості дають можливість абсолютно надійно ідентифікувати особу. Значною популярністю користуються автоматичні системи розпізнавання відбитків пальців – AFIS (Automated fingerprint identification systems).

Дослідивши на прикладі роботу однієї з таких систем, було з'ясовано, що система дає можливість за 0,1 с зчитати відбиток пальця, а за 0,2 с – розпізнати його і дозволити доступ до інформації. На відміну, наприклад, від систем сканування сітківки ока, AFIS не створює дискомфорт користувачам. Відбиток пальців індивідуальний і не змінюється з часом. Системи розпізнавання за відбитками пальців демонструють високі показники точності: ймовірність того, що доступ до секретних даних одержить неавторизований користувач, практично дорівнює нулю. В даний час активно розробляються алгоритми, стійкі до шуму в зображеннях – образах відбитку пальця, що дозволяє досягти збільшення точності й швидкості розпізнавання в реальному часі.

Завдяки ергономічності та малим розмірам сканувальні пристрої можуть бути інтегровані в складові елементи комп'ютерних систем ідентифікації. Серед біометричних систем автентифікації сканери відбитків пальців найбільш економічно вигідні і користуються попитом на ринку, а тому часто можуть потрапляти під вплив хакерів. Для зменшення випадків зламу такої системи проводиться постійне вдосконалення існуючого обладнання і програмного забезпечення. Зараз розробляється велика кількість алгоритмів для захисту як самого процесу розпізнавання ідентифікатора, так і процесу зчитування.

З усього сказаного можна зробити висновок: системи на базі розпізнавання відбитків пальця стали ефективним засобом убезпечення всіх видів власності, захисту від шахрайства, фальсифікації та криміналу. Їх подальше впровадження в різні галузі є актуальним завданням, адже забезпечить створення зручних і надійних інструментів як для державного сектора, індустріальних і комерційних структур, так і для окремих громадян.