УДК 519.711.3:343

В.Г. Іванов, Н.А. Кошева, Н.І. Мазниченко

Національний університет «Юридична академія України імені Ярослава Мудрого», Харків

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В ЗАДАЧАХ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Розглянуті деякі біометричні характеристики людини, які можуть бути використані для ідентифікації користувачів комп'ютерних систем. Проаналізовані існуючі автоматизовані системи на базі біометричних технологій. Обговорюються деякі пропозиції, метою яких є підвищення надійності існуючих систем ідентифікації користувачів.

Ключові слова: *біометричні технології, інформаційна безпека, ідентифікація користувачів ЕОМ.*

Постановка проблеми

Державна політика інформатизації охоплює всі ділянки життєдіяльності людини, суспільства і держави та визначає основи усіх видів суспільних відносин, що виникають у процесі побудови і розвитку інформаційного суспільства в Україні. Одним з основних видів діяльності держави у сфері інформатизації є охорона і захист інформаційних ресурсів.

З появою і розвитком нових інформаційних технологій стала актуальна проблема інформаційної безпеки, пов'язана із забезпеченням безпечного збереження і конфіденційності інформації, що оброблюється та зберігається в комп'ютерних системах.

Вирішенню цих проблем приділяється все більша увага, удосконалюються існуючі методи захисту інформаційних систем, постійно розробляються нові методи, які дозволяють збільшувати надійність і стійкість систем, призначених для вирішення такого роду задач.

Актуальність задачі інформаційної безпеки набуває ще більшої значущості у зв'язку зі зростанням злочинності в сфері використання комп'ютерної інформації.

Враховуючи різноманіття потенційних загроз інформації, безпечне збереження і конфіденційність інформації може бути досягнута тільки шляхом створення комплексної системи захисту інформації. Одним з основних і невід'ємних елементів комплексної системи безпеки є підсистема управління доступом до інформаційних ресурсів. Доступ користувачів до різних класів інформації повинен визначатися ідентифікацією, тобто процесом розпізнавання параметрів, що однозначно визначають особу користувача. Останнім часом все більше набувають популярності системи на основі біометричних методів розмежування і контролю доступу. Сформувався специфічний ринок біометричних пристроїв і відповідних програмних продуктів. Вже ні у кого не викликає сумнівів той факт що біометричні технології дозволять вирішувати серйозні завдання в області інформаційної безпеки.

Аналіз літератури

У науковій літературі наводяться результати досліджень щодо ідентифікації особи по окремих біометричних характеристиках: за пальцевими відбитками [1, 2], за особливостями голосу та мовлення [3, 4], по розпізнаванню обличчя [5, 6], по рукописному підпису [7, 8], за клавіатурним почерком [9, 10], навіть за навичками роботи з маніпулятором «миша» [11] і т.д. Проте, жоден з перерахованих методів не забезпечує стовідсоткову ідентифікацію об'єкту аналізу.

Розглянувши накопичений досвід наукових досліджень і практичних вживань, можна запропонувати деякі напрямки по вдосконаленню існуючих систем ідентифікації особи користувача комп'ютерних систем з використанням біометричних технологій.

Мета статті

Незважаючи на лавинний і стрімкий попит на біометрію, аналіз існуючих автоматизованих систем ідентифікації особи за біометричними характеристиками показав, що надійність розпізнавання недостатня для потреб сьогоднішнього дня і не відповідає сучасним вимогам інформаційної безпеки. Метою дослідження є огляд та аналіз можливостей використання біометричних характеристик ідентифікації користувача при побудові систем контролю та обмеження доступу до інформаційних комп'ютерних систем, доцільність використання цих технологій та можливі шляхи підвищення точності, надійності та ефективності автоматизованих систем контролю доступу.

Основна частина

У даний час існують три основні підходи до ідентифікації користувачів інформаційних систем [12]:

1) користувачу відоме щось, що він може повідомити системі і що дозволяє однозначно його ідентифікувати (наприклад, пароль, PIN-код, ключ і т.д.);

2) користувач може виконати деяку унікальну процедуру (наприклад, використати всілякі карти, магнітні брелоки і т.д.);

3) вимірювання і використовування унікальних характеристик користувача (біометричних).

Найбільш поширені в даний час методи ідентифікації засновані на використанні паролів. Недоліки цього підходу добре відомі, пароль може бути скомпрометований багатьма способами [12].

Методи, які відносяться до другого підходу, також досить поширені. Фізичні об'єкти (носії інформації) можуть бути втрачені, вкрадені, передані іншій особі, дубльовані. З цим зв'язані основні недоліки методів даного класу.

Методи, які використовують для ідентифікації унікальні характеристики користувача (біометричні методи), вільні від перерахованих недоліків, тому є найперспективнішими і активно розвиваються останнім часом [13]. Перевага біометричних систем ідентифікації, в порівнянні з традиційними, полягає в тому, що ідентифікується не зовнішній предмет, що належить людині, а власне людина.

Характеристика нерозривно зв'язана з людиною, її неможливо втратити, передати, забути. Та і підробка будь-якої біометричної характеристики достатньо складна і коштовна.

Біометрична ідентифікація - це спосіб ідентифікації особи по окремих специфічних біометричних ознаках (ідентифікаторах), властивих конкретній людині. Сучасний рівень розвитку комп'ютерних технологій дозволяє використовувати подібні ознаки як основу для ідентифікації людини і ухвалення рішення про можливість або неможливість доступу до інформаційних комп'ютерних систем.

Всі біометричні системи працюють практично за однаковою схемою. По-перше, система запам'ятовує зразок біометричної характеристики (це називається процесом запису). Під час запису деякі біометричні системи можуть попросити зробити декілька зразків для того, щоб скласти найточніше зображення біометричної характеристики. Потім одержана інформація обробляється і перетворюється в математичний код. Крім того, система може попросити провести ще деякі дії для того, щоб «приписати» біометричний зразок до певної людини. Наприклад, персональний ідентифікаційний номер (PIN) прикріпляється до певного зразка, або смарт-карта, що містить зразок. В такому разі, знову робиться зразок біометричної характеристики і порівнюється з представленим зразком.

Ідентифікація по будь-якій біометричній системі складається з чотирьох стадій:

1) запис - фізичний або поведінковий зразок запам'ятовується системою;

2) виділення - унікальна інформація витягується із отриманого зразка і складається біометричний зразок;

3) порівняння - збережений зразок порівнюється з представленим;

4) збіг/неспівпадання - система вирішує, чи співпадають біометричні зразки, і виносить ухвалу.

Серед біометричних механізмів ідентифікації можна виділити такі [14]:

1) по статичних ознаках - те, що практично не змінюється з часом, починаючи з народження людини (фізіологічні характеристики);

2) по динамічних ознаках - поведінкові характеристики, тобто ті, які побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Динамічні ознаки можуть змінюватися з часом, але не різко, а поступово.

Серед статичних методів ідентифікації користувача існують наступні:

1. Ідентифікація по відбитку пальця. В основу цього методу покладена унікальність малюнка папілярних узорів на пальцях. Ідентифікація побудована таким чином: за допомогою сканера одержують зображення відбитку, потім це зображення по складному алгоритму перетворюється на спеціальний цифровий код. Далі цей код порівнюється з еталонними кодами, які зберігаються в базі даних.

2. Ідентифікація по розташуванню вен на долоні. Прилад, який прочитує інформацію в цьому випадку, є інфрачервона камера. В результаті на вході програми при формуванні цифрового коду з'являється малюнок вен на руці людини.

3. Ідентифікація по сітківці ока. В даному випадку сканується малюнок кровоносних судин очного дна. Зрозуміло, що цей малюнок спостерігається тільки за певних умов, тому при скануванні людина дивиться на видалене світлове джерело і спеціальна камера сканує його очне дно.

4. Ідентифікація по веселковій оболонці ока. Малюнок веселкової оболонки ока - унікальний для кожної людини. В цьому методі важлива не тільки спеціальна камера, але і надійне програмне забезпечення. Адже саме за допомогою програм-

ного забезпечення із зображення виділяється малюнок потрібної веселкової оболонки.

5. Ідентифікація за формою кисті руки. Цей метод грунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються вимірювання, за допомогою яких формується відповідний цифровий код.

6. Ідентифікація за формою обличчя. Цей метод чимось схожий на метод ідентифікації за формою грона руки. Тут так само будується тривимірний образ обличчя. Спеціальне програмне забезпечення виділяє з цього образу контури очей, губ і інших частин лиця. Далі проводяться точні вимірювання між отриманими контурами. Саме за цими даними будується цифровий код.

Серед динамічних методів можна назвати наступні:

1. Ідентифікація по голосу. В даний час існує безліч програм по розпізнаванню голосу. В методі ідентифікації по голосу важливі частотні характеристики голосу людини. Саме по частотних характеристиках і будується цифрова модель.

2. Ідентифікація по почерку. При ідентифікації цим методом звичайно досліджується підпис людини. Перевіряються такі динамічні характеристики, як: графічні параметри, сила натиску на поверхню, швидкість нанесення підпису. По цих характеристиках і будується цифровий код.

3. Ідентифікація по клавіатурному почерку. Даний метод аналогічний ідентифікації по почерку, але замість того, щоб ставити автограф, людині необхідно надрукувати кодове слово. Цифровий код будується по динаміці набору певного слова.

При всьому теоретичному різноманітті можливих біометричних методів тих, що застосовуються на практиці для ідентифікації користувачів комп'ютерних систем серед них небагато. Основних методів три - розпізнавання по відбитку пальця, по зображенню особи (двомірному або тривимірному) і по веселковій оболонці ока.

Існує два статистичні показники, що визначають якість, точність біометричних технологій: FAR (False Acceptance Rate) - вірогідність помилкового розпізнавання, тобто вірогідність того, що система визнає "чужого" за "свого"; FRR (False Rejection Rate) - вірогідність помилкового нерозпізнавання, тобто того, що система не розпізнає знайомого їй суб'єкта. Будь-яку біометричну систему можна налаштувати на різний ступінь "пильності", тобто на різне значення вірогідності помилкового розпізнавання FAR. При цьому, чим нижчий FAR, тобто чим пильніше система, тим вище вірогідність помилкового нерозпізнавання FRR (система менш чутлива). Ідеальні характеристики системи - це такі показники помилки і відмови ідентифікації, коли одночасно при великій надійності ідентифікації (помилка 0,0001%) досягається відмова ідентифікації всього долі відсотка.

В загальному випадку для кожної технології ці показники різняться, але для кожного конкретного виробника і його обладнання ці дані вказуються точно. Тому при виборі необхідно звертати увагу на ці показники. Залежно від конкретної задачі система настроюється на певний компроміс між допустимими значеннями FAR і FRR. На сьогоднішній день всі біометричні технології є імовірнісними, жодна з них не здатна гарантувати повну відсутність помилок FAR/FRR, і нерідко дана обставина служить основою критики біометрії.

Висновки

Розглянуті під час дослідження комплекси рішень щодо доступу користувачів інформаційних комп'ютерних систем до інформації обмеженого використання зручні в застосуванні для сучасних інформаційних технологій і дозволяють використовувати біометричні технології в сучасних системах контролю доступу до інформаційних ресурсів. Біометричні технології надійніші і зручніші за класичні засоби захисту, які широко застосовувалися до недавнього часу.

Незважаючи на активну діяльність протягом останніх років у напрямку розробки та вдосконалення методів ідентифікації користувачів з метою управління доступом до ресурсів інформаційних систем, надійність та стійкість існуючих систем недостатня для потреб сьогоднішнього дня. Тому актуальною бачиться проблема розробки і дослідження комплексних систем, що використовують для прийняття рішення доступу до інформаційних систем декілька біометричних характеристик користувача (наприклад, використовувати разом особливості клавіатурного почерку, голосу, динаміки роботи користувача з маніпулятором «миша» або використання відбитків декількох пальців і т.д.)

Деякі виробники вже розпочали інтеграцію двох методів розпізнавання облич, включаючи дво- і тривимірні зображення.

Досягти підвищення надійності та точності автоматизованих систем контролю та управлінням доступом до комп'ютерної інформації можна за рахунок об'єднання використання біометричних характеристик разом з класичними способами ідентифікації користувачів (наприклад, парольний захист, PIN-код, використання різноманітних карт і т.д.). Проте абсолютно захищеної системи, як і раніше, не існує.

Список літератури

1. Гирман М.Г. Использование автоматизированных дактилоскопических идентификационных систем в раскрытии и расследовании преступлений [Текст] // Матеріалы III звітної науково-практичної конференції професорсько-викладацького та курсантського складу Кримського факультету Національного університету внутрішніх справ, 2001. – Ч.2. – С. 59-64.

2. R. Adhami, P. Meenen. Fingerprinting for security // IEEE Potentials, vol. 20, no. 3, pp. 33-38, Aug.-Sept. 2001.

3. Костюченко Е.Ю. Выбор обучающего набора ключевых параметров речового сигнала / Е.Ю. Костюченко // Научная сессия ТУСУР – 2008: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых. Тематический выпуск «Системная интеграция и безопасность». Томск, 4-8 мая 2008 г.: В п'яти частях. Ч.3 Томск: «В-Спектр», 2008. – 248с. С. 152-155.

4. Иванов А.И. Идентификация человека по особенностям его голоса [Текст] // Современные технологии безопасности. 2003. №3. С. 25-28.

5. Белоцерковский О.М. Компьютерное распознавание человеческих лиц [Текст] / О.М. Белоцерковский, А.С. Глазунов, В.В. Щанников // Зарубежная радиоэлектроника. Успехи современной радиоэлектроники. 1997. № 8. С. 3-14.

6. P.J. Phillips, H. Moon, S.A. Rizvi, P.J. Rauss. The FERET evaluation methodology for face recognition algorithms // IEEE Trans. PatternAnalysis and Machine Intelligence, vol.22, no 10, pp. 1090-1104, Oct. 2000.

7. Брюхомицкий Ю.А. Система аутентификации личности по почерку [Текст] / А.Ю. Брюхомицкий, М.Н. Казарин // Сборник трудов научно-практической конференции «Информационная безопасность». Таганрог, 2002. С. 22-29.

8. Иванов А.И. Масштабирование сигналов в системах биометрической аутентификации по динамике подписи [Текст] / А.И. Иванов, В.А. Кологоров, И.А. Сорокин. // Новые промышленные технологии. Вып. 6. 1998. С. 37-41.

9. Шарипов Р.Р. Идентификация и аутентификация пользователей по клавиатурному почерку [Текст] // Электронное приборостроение. Научно-практический сборник. – Казань:ЗАО «Новое знание», 2005. – вып.3 (44). С. 50-54.

10. Костюченко Е.Ю. Определение пользователя по клавиатурному почерку на основе нейросети [Текст] / Е.Ю. Костюченко, Р.В. Мещеряков // Интеллектуальные системы в управлении, конструировании и образовании. Выпуск 3 / Под ред. А.А. Шелупанова. – Томск: STT, 2004. – С. 153-158.

11. Диденко С.М. Исследование динамики работы пользователя с манипулятором мышь [Текст] / С.М. Диденко, В.А. Шапцев // Математическое и информационное моделирование. Тюмень: Изд-во Тюм. ун-та, 2004. С. 295-304.

12 Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Текст]. Под ред. В.Ф. Шаньгина. 2-е изд. – М.: Радио и связь, 2001. – 376 с.

13. Голубев Г.А., Габриелян Б.А., Современное состояние и перспективы развития биометрических технологий // Нейрокомпьютеры: разработка, применение. 2004, № 10. с. 39-46.

14. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека [Текст] / Г.А. Кухарев. – СПб.: Политехника, 2001. – 240 с.

Надійшла до редколегії 27.03.2012

Рецензент: д-р ф.-м. наук, проф. М.Г. Любарський, Національний університет «Юридична академія України імені Ярослава Мудрого», Харків.

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ В ЗАДАЧАХ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ИНФОРМАЦИОННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

В.Г. Иванов, Н.А. Кошевая, Н.И. Мазниченко

Рассмотрены некоторые биометрические характеристики человека, которые могут быть использованы для идентификации пользователей компьютерных систем. Проанализированы существующие автоматизированные системы на базе биометрических технологий. Обсуждаются некоторые предложения, целью которых является повышение надежности существующих систем идентификации пользователей.

Ключевые слова: *биометрические технологии, информационная безопасность, идентификация пользователей ЭВМ.*

BIOMETRICS TECHNOLOGIES ARE IN THE TASKS OF AUTHENTICATION OF USERS OF THE INFORMATIVE COMPUTER SYSTEMS

V.G. Ivanov, N.A. Koshevaya, N.I. Maznichenko

Some biometric descriptions of man, which can be used for authentication of users of the computer systems, are considered. The existent automated biometric systems are analyses. Some suggestions the purpose of which there is the increase of reliability of the existent systems of authentication of users comes into question.

Keywords: *biometrics technologies, information security, identification of users of COMPUTER.*