МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

“На правах рукопису”
УДК 57.001

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ Шуклін Г.В.
“____” _____2020 р.

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека

на тему: **СТВОРЕННЯ СИСТЕМИ ДОСТУПУ ДО ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ ЗАСОБІВ ІДЕНТИФІКАЦІЇ**

Студент групи СЗДМ-61 Бондар Олександр Павлович _____
(підпис)

Науковий керівник: к.т.н., доцент Тихонов Юрій Олександрович _____
(підпис)

Нормоконтроль: Пшоннік Володимир Олександрович _____
(підпис)

Київ – 2020

ЗАТВЕРДЖУЮ
Завідувач кафедри СІКЗ
к.т.н. Шуклін Г.В
“__” _____ 2019 р.

З А В Д А Н Н Я

на магістерську кваліфікаційну роботу

студенту Бондару Олександру Павловичу

1. Тема роботи: Створення системи доступу до інформації з використанням біометричних засобів ідентифікації, керівник Тихонов Юрій Олександрович, к.т.н., доцент, затверджені наказом вищого навчального закладу від “14” листопада 2019 року № 518.

2. Термін здачі студентом оформленої роботи “8” січня 2020 р.

3. Предмет дослідження: особливості побудови системи доступу до інформації з використанням біометричних засобів ідентифікації.

4. Об’єкт дослідження: процес створення системи доступу до інформації з використанням біометричних засобів ідентифікації.

5. Мета роботи: підвищення ефективності системи контролю доступу шляхом впровадження біометричних систем ідентифікації.

6. Перелік питань, які мають бути розроблені:

1. Розглянути основні методи розпізнавання особи за допомогою біометричних систем.
2. Розглянути використання та роботу різних біометричних систем ідентифікації. Зробити аналіз їх переваг та недоліків.
3. Створити систему доступу до інформації з використанням біометричних засобів ідентифікації.

7. Перелік публікацій:

Тези доповіді: Бондар О.П., Тихонов Ю.О. Необхідність впровадження систем доступу до інформації з використанням біометричних засобів ідентифікації // Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». – Київ: ДУТ. – 2019.

8. Перелік ілюстративного матеріалу:

1. Презентація виконана на 10 слайдах для подання за допомогою оверхедів (світлопроекторів) та комп’ютерних засобів.

9. Дата видачі завдання “15” вересня 2019 р.

Керівник: Тихонов Юрій Олександрович _____

Завдання прийняв до виконання: Бондар Олександр Павлович _____

КАЛЕНДАРНИЙ ПЛАН

№ З\П	Назва етапів магістерської роботи	Строк виконання етапів	Примітка
1	**2**	**3**	**4**
1	Уточнення постановки завдання	До 20.09.19	Виконано
2	Аналіз літератури	До 15.10.19	Виконано
3	Обгрунтування вибору рішення	До 20.10.19	Виконано
4	Збір даних	До 31.10.19	Виконано
5	Написання першого розділу роботи	До 11.11.19	Виконано
6	Написання другого розділу роботи	До 30.11.19	Виконано
7	Написання третього розділу роботи	До 31.12.19	Виконано
8	Підготовка ілюстративного матеріалу	До 06.01.20	Виконано
9	Отримання рецензій	До 10.01.20	Виконано
10	Захист в ДЕК	16.01.20	Виконано

Студент О.П. Бондар

Науковий керівник Ю.О. Тихонов

АНОТАЦІЯ

В роботі розглянуто основні методи біометричної ідентифікації та їх характеристики, такі як швидкість процесу ідентифікації, зручність даної процедури з точки зору користувача, вірогідність похибок першого та другого роду, коштовність необхідного обладнання та інші; на основі результатів проведеного аналізу обрано тип біометричних технологій для побудови системи контролю доступу до об'єкта.

Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 66 аркушів.

РЕФЕРАТ

У дипломній роботі розглянута розробка проекту по створенню системи доступу до інформації з використанням біометричних засобів ідентифікації. Описано біометричні дані, що використовуються в системах біометричного контролю доступу. Проаналізовано основні методи біометричної ідентифікації, виявлено їх переваги та недоліки. Наведено приклад підвищення ефективності системи контролю доступу до об'єкта шляхом впровадження біометричних технологій. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 66 аркушів.

Об’єктом дослідження в роботі є процес створення системи доступу до інформації з використанням біометричних засобів ідентифікації. **Предмет дослідження** – особливості побудови системи доступу до інформації з використанням біометричних засобів ідентифікації. **Мета роботи** – підвищення ефективності системи контролю доступу до інформації шляхом впровадження біометричних систем ідентифікації.

Як результат у роботі були досліджені існуючі методи захисту обраного об’єкта (приміщень банку), та прийнято рішення щодо удосконалення охоронної системи. До того ж, були надані деякі рекомендації щодо певних адміністративних змін в політиці підприємства при впровадженні біометричної системи доступу.

Галузь застосування: результати досліджень можуть використовуватись в процесі розробки та реалізації сучасної системи контролю доступу до інформації.

Ключові слова: Біометрія, ідентифікація, верифікація, біометричні дані, системи контролю доступу.

ЗМІСТ

ВСТУП

В наш час безперервного розвитку комп'ютерних мереж і розширення сфер автоматизації цінність інформації неухильно зростає. Державні секрети, наукові ноу-хау, комерційні, юридичні і лікарські таємниці все частіше довіряються комп'ютеру, який, як правило, підключений до локальних і корпоративних мереж. Популярність глобальної мережі Інтернет, з одного боку, відкриває величезні можливості для електронної комерції, але, з іншого боку, створює потребу в надійніших засобах безпеки для захисту корпоративних даних від доступу ззовні. Все більше компаній стикаються з необхідністю запобігти несанкціонованому доступу до своїх систем і захистити транзакції в електронному бізнесі.

Практично до кінця 90-х років основним способом персоніфікації користувача була вказівка його мережевого імені і пароля. Справедливості ради потрібно відзначити, що подібного підходу, як і раніше, дотримуються в багатьох установах і організаціях. Небезпеки, зв'язані з використанням пароля, добре відомі: паролі забувають, зберігають в невідповідному місці, нарешті, їх можуть просто вкрасти. Деякі користувачі записують пароль на папері і тримають ці записи поряд зі своїми робочими станціями. Як повідомляють групи в сфері інформаційних технологій багатьох компаній, велика частина дзвінків в службу підтримки пов'язана із забутими або такими, що втратили силу паролями.

Відомо, що систему можна обдурити, представившись іншим іменем. Для цього необхідно лише знати якусь ідентифікуючу інформацію, якій, з погляду системи безпеки, володіє одна-єдина людина. Зловмисник, видавши себе за співробітника компанії, отримує в своє розпорядження всі ресурси, доступні даному користувачеві відповідно до його повноважень і посадових обов'язків. Результатом можуть стати різні протиправні дії, починаючи від крадіжки інформації і закінчуючи виводом з ладу всього інформаційного комплексу.

Розробники традиційних пристроїв ідентифікації вже зіткнулися з тим, що стандартні методи багато в чому застаріли. Для вирішення цієї проблеми потрібні радикально нові методи, засновані на новій ідеології. Проведені дослідження показують, що збиток у випадках несанкціонованого доступу до даних компанії може складати мільйони доларів.

Автоматизованим системам стали довіряти все більш відповідальну роботу, від якості виконання якої залежить життя і добробут окремих людей, організацій, держав і людства в цілому. Автоматизовані системи керують технологічними процесами на підприємствах і атомних електростанціях, рухом літаків і поїздів, різними системами озброєння, виконують фінансові операції, обробляють секретну і конфіденційну інформацію. Швидке зниження вартості коштів обчислювальної техніки привело до різкого розширення сфер її застосування. Без комп'ютерів тепер неможлива будь-яка виробнича і управлінська діяльність, вони широко використовуються в медицині, освіті і багатьох інших сферах людської діяльності.

Широке поширення обчислювальної техніки як засобу обробки інформації привело до інформатизації суспільства і появи принципово нових, так званих, інформаційних технологій.

Поява будь-яких нових технологій, як правило, має як позитивні, так і негативні сторони. Тому безліч прикладів. Атомні і хімічні технологи, вирішуючи проблеми енергетики і виробництва нових матеріалів, породили екологічні проблеми. Інтенсивний розвиток транспорту забезпечив швидке і зручне транспортування людей, сировини, матеріалів і різних товарів в усіх можливих напрямках, але і матеріальний збиток і людські жертви при транспортних катастрофах значно зросли.

Інформаційні технології, також не є виключенням з цього правила, і тому слід заздалегідь подбати про безпеку при розробці та використанні таких технологій.

В цілому, кримінальне використання сучасних інформаційних технологій робить "комп'ютерну злочинність" не тільки вельми прибутковою, але і досить безпечною справою. І не дарма Підкомітет ООН зі злочинності ставить цю проблему в один ряд з тероризмом і наркотичним бізнесом. В одному з банків Великобританії за допомогою комп'ютера в одну мить був викрадений мільярд доларів. Щорічні втрати від "комп'ютерної злочинності" в Європі і Америці становлять кілька десятків мільярдів доларів. При цьому в дев'яноста відсотках випадків не вдається вийти на слід злочинця.

Давно стали звичними і загальновживаними такі категорії, як матеріальні, фінансові, трудові, природні ресурси, які залучаються до господарського обороту, і їх призначення зрозуміло кожному. Але ось з'явилося поняття «інформаційні ресурси», і хоча воно узаконено, але усвідомлено поки ще недостатньо. «Інформаційні ресурси - окремі документи і окремі масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах)». Інформаційні ресурси є власністю, знаходяться у віданні відповідних органів і організацій, підлягають обліку та захисту, так як інформацію можна використовувати не тільки для виробництва товарів і послуг, але і перетворити її в готівку, продавши кому-небудь, або, що ще гірше, знищити. Власна інформація для виробника представляє значну цінність, так як нерідко отримання (створення) такої інформації - досить трудомісткий і коштовний процес. Особливе місце відводиться інформаційним ресурсам в умовах ринкової економіки. Найважливішим фактором ринкової економіки виступає конкуренція. Перемагає той, хто краще, якісніше, дешевше і оперативніше (час - гроші!) виробляє і продає. По суті, це універсальне правило ринку. І в цих умовах головним являється правило: хто володіє інформацією, той володіє світом. У конкурентній боротьбі широко поширені різноманітні дії, спрямовані на отримання (добування, придбання) конфіденційної інформації різними способами, аж до прямого промислового шпигунства з використанням сучасних технічних засобів розвідки. Встановлено, що 47% охоронюваних відомостей видобувається за допомогою

технічних засобів промислового шпигунства. У цих умовах захист інформації від неправомірного оволодіння нею відводиться далеко не останнє місце [3].

Наведемо основні поняття і визначення у сфері інформаційної безпеки.

Інформація - відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх подання.

Документована інформація (документ) - зафіксована на матеріальному носії інформація з реквізитами, що дозволяють її ідентифікувати.

Конфіденційна інформація - документована інформація, доступ до якої обмежується відповідно до законодавства України.

Інформаційні процеси - процеси створення, збору, обробки, накопичення, зберігання, пошуку, розповсюдження та споживання інформації.

Інформаційна сфера (середовище) - сфера діяльності суб'єктів, пов'язана зі створенням, перетворенням і споживанням інформації.

Безпека - стан захищеності життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз.

Життєво важливі інтереси - сукупність потреб, задоволення яких надійно забезпечує існування і можливості прогресивного розвитку особистості, суспільства і держави.

Інформаційна безпека - стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій, держави.

Загроза безпеки - сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави.

Зловмисник - суб'єкт, який впливає на інформаційний процес з метою викликати його відхилення від умов нормального існування.

Інформатизація - процес створення оптимальних умов для задоволення інформаційних потреб і реалізації прав громадян, органів державної влади на основі формування і використання інформаційних ресурсів.

Інформаційна система - організаційно впорядкована сукупність документів (масивів документів) та інформаційних технологій, в тому числі з

використанням засобів обчислювальної техніки і зв'язку, що реалізують інформаційні процеси.

Важливість інформації встановлюється її власником у деякій дискретній шкалі категорій, а саме: Інформація відкритоготого доступу, Конфіденційно (К), Таємно (Т), Цілком таємно (ЦТ), Особливої важливості (ОВ).

Під загрозами інформації, будемо розуміти потенційні чи реально можливі дії по відношенню до інформаційної сфери, що призводять до несанкціонованих змін властивостей інформації (конфіденційність, доступність, достовірність, цілісність). За кінцевим проявом можна виділити наступні загрози інформації: Ознайомлення, Модифікація, Знищення, Блокування.

- *Ознайомлення* з конфіденційною інформацією може проходити різними шляхами і способами, при цьому суттєвим, є відсутність змін самої інформації. Порушення конфіденційності або секретності інформації пов'язано з ознайомленням з нею тих осіб, для яких вона не призначалася.

- *Модифікація* інформації спрямована на зміну таких властивостей як конфіденційність, достовірність, цілісність, при цьому мається на увазі зміна складу і змісту відомостей. Модифікація інформації не має на увазі її повне знищення.

- *Знищення* інформації направлено, як правило, на цілісність інформації та призводить до її повного руйнування. При цьому інформація пропадає безповоротно і не може бути відновлена ніякими засобами. Втрата може статися через руйнування/знищення носія інформації або через його викрадення, в результаті видалення інформації на носіях, через збої в роботі пристроїв, що задіяні в процесах інформаційної діяльності тощо.

- *Блокування* інформації призводить до втрати доступу до неї, тобто до недоступності інформації. Доступність інформації полягає в тому, що суб'єкт, що має право на її використання, повинен мати можливість на своєчасне її отримання в зручному для нього вигляді. При втраті доступу до інформації

вона, як і раніше, існує, але скористатися нею не можна. Тобто суб'єкт не може з нею ознайомитися, скопіювати, передати іншому суб'єкту або представити у вигляді, зручному для використання. Втрата доступу може бути пов'язана з відсутністю або несправністю деякого обладнання автоматизованих систем (АС), непрацездатністю якогось програмного засобу, що задіяний в інформаційній діяльності, та ін. Так як інформацію не втрачено, то доступ до неї може бути отриманий після усунення причин втрати доступу [5].

АКТУАЛЬНІСТЬ. Актуальність біометричних систем доступу, як і самої біометрії, на даний момент є вельми значною. Ми вже спостерігаємо тенденції впровадження новітніх систем, законів та правил в нашій країні та по всьому світі, зокрема перехід до біометричних паспортів як засобів ідентифікації особи. Говорячи про інформаційну безпеку, біометричні системи доступу є більш надійними засобами ніж методи, що ґрунтуються на використанні паролів. Розробники традиційних пристроїв ідентифікації особистості вже зіткнулися з тим, що стандартні засоби багато в чому застаріли. Для вирішення цієї проблеми потрібні радикально нові методи ідентифікації, засновані на новій ідеології. Проведені дослідження показують, що збиток у випадках несанкціонованого доступу до даних компанії може складати мільйони доларів. З цієї точки зору, можна зробити висновок, що тема магістерської роботи, присвячена проблемі створення системи контролю доступу з використанням нових засобів ідентифікації, є актуальною науковою задачею.

МЕТА. Мета дипломної роботи – підвищення ефективності системи контролю доступу до інформації шляхом впровадження біометричних систем ідентифікації.

ЗАДАЧІ. Виходячи з мети, для її досягнення ставляться наступні задачі:

1. Дослідити найпоширеніші методи біометричної ідентифікації, розглянувши основні біологічні дані, що використовуються в біометрії, та особливості роботи з ними

2. Проаналізувати кожен метод, виявити їх переваги та недоліки;

3. Спроектувати систему доступу до об’єкту, що базується на одному з методів біометричної ідентифікації, використання якого, для даного об’єкта (банківський підрозділ обслуговування клієнтів), було б доцільніше.

ОБ’ЄКТОМ роботи є процес створення системи доступу до інформації з використанням біометричних засобів ідентифікації.

ПРЕДМЕТ роботи – особливості побудови системи доступу до інформації з використанням біометричних засобів ідентифікації.

РОЗДІЛ 1. ОСНОВИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Головна ціль впровадження біометричних технологій є організація такої системи реєстрації, що дуже рідко відхиляє доступ повноправним користувачам та одночасно всеціло виключає неправомірний доступ до різних джерел інформації (насамперед комп'ютерних). Така система надає набагато грунтовніший захист відносно застарілих систем з картками та паролями. Біометричне визначення абонента грунтується на порівнянні таких характеристик об'єкта, як його фізіологічні та/або психологічні особливості, з тими параметрами, які зберігаються в базі даних такої системи. Аналогічні процеси всечасно відбуваються в мозку людини, що позволяє, скажемо, впізнавати своїх знайомих та рідних, порівнюючи їх за певними критеріями, що роблять їх унікальними та відрізняє від інших осіб.

Біометричні технології діляться на дві суттєві категорії, що будуть розглянуті далі – фізіологічні і психологічні (поведінкові). Фізіологічні методи дозволяють ідентифікувати користувача за наступними ознаками: риси обличчя, структура ока (сітківки або райдужної оболонки), характеристики пальців (папілярні лінії, рельєф, довжина суглобів і тому подібне), параметри долоні (її топографія або відбиток), форма руки, малюнок вен на зап'ясті або теплова картина. Психологічні методи аналізують такі параметри користувача як голос даної особи, підпис та його особливості, мінливі характеристики письма та специфіка вводу текста з клавіатури [1].

Щоб обрати метод, який найбільш відповідає потребам конкретної ситуації, необхідно враховувати цілий ряд чинників. Описані технології та їх впровадження, звичайно, мають різну ефективність, причому в більшості випадків вартість системи прямо пропорційна рівню захищенності який вона надає.

Фізіологічні атрибути людини, такі як папілярний узор пальця, геометрія долоні або малюнок (модель) райдужної оболонки ока, відносяться до

статичних (постійних) характеристик людини. Як дані фізіологічні параметри, так и результати перевірки особи даним методом практично незмінні. Якщо ж говорти про поведінкові параметри, скажемо, підпис особи, голос почерк, особливості друкування на клавіатурі, то вони зазнають впливу не лише керованих дій, але і менш керованих факторів - різних психологічних чинників. Маючи на увазі те, що поведінкові характеристики досить мінливі та змінюються з часом, внесений до системи біометричний зразок повинен оновлюватися через певний час, в залежності від обраного методу. Враховуючи це, біометричні способи, що грунтуються на поведінкових характеристиках, вимагають набагато менше фінансових ресурсів задля впровадження, проте така система надає менший степінь захисту інформації; в свою чергу, фізіологічні методи ідентифікації особи потребують більших витрат, зате вони точніші та надають більшу безпеку. Так чи інакше, усі перераховані способи ідентифікації набагато надійніші та забезпечують значно вищий рівень захисту, аніж системи з паролями або картками.

Треба сказати, що всі біометричні методи розпізнавання в деякій мірі, так чи інакше, базуються на статистичних особливостях певних якостей особи. Це значить, що результати, отримані під час їх використання, досить мінливі та носять імовірнісний характер. До того ж, усім біометричним методам ідентифікації властиві деякі похибки під час застосування. Розглядають два види помилок при використанні біометричних систем: хибна відмова (коли не розпізнали уповноважену особу) і хибний допуск (дали доступ не уповноваженій особі). Варто відзначити, що ця проблема в теорії вірогідності була розглянута та проаналізована ще в часи становлення радіолокації. Через зіставлення середньої ймовірності відповідно хибної відмови і хибного допуску оцінюється вплив похибок на процедуру розпізнавання. На практиці, дані ймовірності пов’язані зворотною залежністю: іншими словами, якщо намагатися покращити якість конролю доступу, то разом з цим буде підвищуватися ймовірність відмови у доступі уповноваженої особи, і навпаки. Отже, в кожній конкретній ситуації потрібно йти на певний компроміс. Але,

тим не менш, біометричні системи при всіх порівняннях стоять далеко попереду за іншими наявними способами ідентифікації, адже вони набагато надійніші.

Окрім результативності та фінансових затрат, компаніям-користувачам системи також необхідно враховувати реакцію працівників на біометричні процедури розпізнавання. Ознаками бездоганної системи є ненав'язливість, комфортність та простота в використанні, швидкий темп роботи, прийнятність з соціальної точки зору. Але на світі не існує нічого бездоганного, тому будь-яка із вироблених технологій відповідає даному набору вимог тільки в певній мірі. Проте, незважаючи на це, впровадження біометричних технологій приносить власнику безсумнівну вигоду: окрім покращення якості котнролю несанкціонованого доступу до інформації, такий підхід позитивно впливає на імідж компанії, демонструючи пильну увагу до проблеми захищенності даних.

Біометричні гаджети розвиваються у багатьох напрямках, незмінними залишаються їх головні орієнтири - це досконалий на теперішній час рівень захищенності, відсутність усталених вад застарілих систем, що використовують паролі та картки, і першокласна надійність. Проте, нажаль, поширеність біометричних систем пов’язана насаперед з організаціями, де вони вводяться у приказному порядку, для охорони доступу до конфіденційної інформації в зони з підвищенним рівнем контролю, або розпізнавання людей, які розшукуються правоохоронними органами. Власники підприємств ще не достатньо оцінили усі переваги та потенціал біометричних систем. Нерідко менеджери різних організацій не хочуть встановлювати біометрію зважаючи на те, що через можливі похибки у вимірюваннях параметрів користувач не будуть отримувати доступ у ситуаціях, коли вони мають не це право. Тим не менш, сучасні технології досить високими темпами займають позиції на корпоративному ринку. На теперішній час вже існують десятки тисяч комп'ютеризованих місць, сховищ, дослідницьких лабораторій, банків крові, банкоматів, військових споруд, доступ до яких контролюється пристроями, скануючими унікальні фізіологічні або поведінкові характеристики індивідуума [4].

1.1. Методи ідентифікації

Як ми знаємо, ідентифікація заключається у перевірці автентичності суб’єкта, котрим у наш час може виступати не лише певний індивід, але і деякий програмний процес. Розпізнавання особи базується на порівнянні пред'явлених даних з тими, що зберігаються в системі у різних формах. Наприклад:

• пароль, особистий номер, криптографічний ключ, мережева адреса комп'ютера в мережі;

• смарт-карта, електронний ключ;

• зовнішність, голос, рисунок райдужної оболонки очей, відбитки пальців та інші біометричні параметри особи.

Ідентифікація дає змогу раціонально та достовірно надати права доступу до даних, які перебувають у широкому використанні та приймають участь у великій кількості процесів.

Розпізнавання особи по принципу перевірки співпадання характеристик однієї людини в системі зветься верифікацією. Серед переваг такого методу є високий темп обробки та низькі вимоги до обчислювальної потужності комп'ютера. Ідентифікацією називається розпізнавання особи через пошук збігу характеристик серед багатьох людей в системі. Реалізація даного методу являється більш складною за фінансово затратною [2].

Сучасні біометричні системи для верифікації та ідентифікації особи під час своєї роботи застосовують такі персональні параметри людини, як відбитки пальців, риси обличчя, райдужну оболонку і сітківку ока, форму долоні, характерність голосу, мови і підпису. Наразі на етапах тестування та дослідницького використання маються такі біометричні методи, які можуть здійснювати ідентифікацію індивіда по його тепловому полю, малюнку кровоносних судин руки, запаху тіла, температурі шкіри або за специфікою форми вуха.

Усі біометричні технології працюють наступним чином: обробляють один або декілька параметрів особи, за якими буде проводитись розпізнавання, та знаходять їх унікальні особливості, притаманні лише цій конкретній людині. Якщо розглядати абстрактну модель біометричної системи, то її можна поділити на два модулі: модуль реєстрації та модуль ідентифікації. Функція першого – зібрати потрібні для розпізнавання дані. Необхідні параметри особи (фізіологічні або поведінкові) скануються біометричним пристроєм за допомогою спеціальних датчиків та кодуються щоб отримати певну цифрову картину. Далі створена картина проходить обробку, під час якої виділяються специфічні області та генерується шаблон. Прикладом подібних специфічних якостей особи є розмір долоні, тембр голосу, папілярний рисунок відбитку пальця. Кожен унікальний шаблон зберігається в базі даних біометричної системи.

Модуль ідентифікації виконує функцію розпізнавання особи. Біометричні технології сканують параметри індивіда, що проходить ідентифікацію, та трансформують отримані результати у цифрову картину так само, як і шаблон. Отримане закодоване зображення порівнюється зі збереженим в системі шаблоном та на основі цього заключається, чи відповідають зібрані характеристики одній і тій самій людині.

Візьмемо оперативну систему Microsoft Windows: в ній для розпізнавання юзера необхідно вказати такі параметри як ім'я користувача та пароль. Якщо використовувати біометрію для перевірки користувача, зокрема метод аутентифікації за відбитками пальців, то введене ім'я буде використано для пошуку в реєстрі системи відповідних, завчасно збережених, даних, які будуть звірятися з щойно отриманими для підтвердження особистості відбитками, які в даному випадку виконують роль пароля [4]. Отже, під час вибору методу ідентифікації потрібно мати на увазі такі наступні критерії:

- значимість інформації;
- фінансові можливості компанії;
- комфорт працівників та їх ставлення до впровадження біометрії;

Зрозуміло, що чим краще та швидше працює біометрична технологія, тим більше вона коштує, тому при виборі системи захисту необхідно відштовхуватися від значимості інформації та можливих наслідках несанкціонованого доступу до неї. Покращення продуктивності технічних процесів та показників безпеки завжди потребує певних фінансових вкладень, але вони завжди окупаються.

Наразі мається велика кількість способів використання біометричних технологій. Вони діляться на групи, розглянуті далі.

1.1.1. Статичні методи

Статичні методи біометричної ідентифікації базуються на особливостях неповторних фізіологічних параметрів індивіда, притаманних тільки йому.

Існує декілька підвидів даного способу:

• За відбитками пальців. Даний метод грунтується на специфіці розміщення парілярних узорів на поверхні пальців кожної особи. Біометричні технології спочатку сканують відбиток, потім кодують для отримання цифрового зображення, та зіставляють зі завчасно збереженим шаблоном користувача. Цей метод являється найпоширенішим серед усіх біометричних способів ідентифікації;

• За формою долоні. Цей спосіб використовує унікальну геометрію руки людини. Сканування здійснюється дещо складніше: технологія, що має у своєму складі камеру та підсвічуючи діоди, складає тривимірне зображення долоні, яке так само перетворюється за допомогою кодування у шаблон, спираючись на який відбувається розпізнавання особи;

• За розміщенням вен на внутрішній стороні долоні. Інфрачервона камера зчитує зображення вен на внутрішній стороні долоні, отримується певне схематичне зображення, яке кодується та перетворюється в унікальний шаблон;

• По сітківці ока. Якщо точніше, цей метод використовує специфіку розташування кровоносних судин очного дна. Користувач дивиться на світлову крапку, і технологія за допомогою сучасного сканера дуже точно відображає

схему кровоносних судин ока;

• По райдужній оболонці ока. Даний параметр теж є індивідуальним для кожної особи. Сканер, оснащений спеціальним програмним забезпеченням, досліджує картину райдужної оболонки, використовуючи яку біометрична технологія знову таки методом кодування отримує шаблон для розпізнавання індивіда;

• За формою особи. Цей спосіб базується на винятковості образу лиця особи. Сканери отримують схематичне зображення розміщення частин обличчя (наприклад, очей, брів, носа и т.д.), зчитують особливості їх розташування, та виробляють велику кількість цифрових малюнків лиця з різних ракурсів, що зберігаються в одному шаблоні. Детальність даної обробки обличчя та кількість відтворених цифрових зображень залежить від важливості інформації, доступ до якої потрібно контролювати;

• За термограмою особи. Метод також використовує обличчя людини, зокрема таку його характеристику, як специфічність розташування на ньому кровоносних артерій, що виділяють тепло. Біометрична технологія за допомогою інфрачервоного сканера будує термограму користувача, яка зберігається в системі як шаблон;

• За ДНК людини. Звичайно, цей метод вирізняється великою точністю, але процес отримання біометричними технологіями ДНК особи наразі надто довготривалий, тому таким способом користуються тільки у виняткових випадках. Не варто й казати, що такі системи не підходять для корпоративних цілей;

• Інші методи. Вище були перераховані лише найпопулярніші способи розпізнавання особи за допомогою біометричних технологій. На теперішній час мається маса різних методів ідентифікації, наприклад, по піднігтьовому шару шкіри або за формою вух, навіть по запаху тіла і багато інших [1].

1.1.2. Динамічні методи

Динамічні способи біометричної ідентифікації базуються на поведінкових (мінливих) параметрах особи. Вони використовують специфіку певних підсвідомих реакцій людини, які задіяні в процесі відтворення якоїсь дії.

Приклади способів біометричної ідентифікації даного типу:

• За рукописним почерком. Найпоширенішим для цього методу є використання підпису індивіда. Цифровий шаблон для розпізнавання будується за допомогою різних біометричних технологій, найпоширенішим серед яких є графічний планшет. Мається два види ідентифікації за рукописним почерком:

1. За виглядом підпису, при цьому для розпізнавання просто перевіряється введений розпис шляхом звірки із збереженим в системі малюнком-шаблоном.

2. За параметрами написання підпису. В цьому випадку у згенерованому біометричною системою шаблоні будуть міститися такі дані користувача, як манера написання розпису та особливості натиску до поверхні під час нанесення підпису.

• За специфікою введення тексту з клавіатури. Даний спосіб дуже схожий з описаним вище, з тією різницею що замість підпису розпізнавання відбувається на основі якогось певного набору символів, особливості введення яких аналізують спеціальні алгоритми. Для цього методу не обов’язкова наявність сучасної біометричної техніки, достатньо мати звичайну комп’ютерну клавіатуру;

• За голосом. Це дуже перспективний спосіб розпізнавання, який на теперішній час зазнає швидкого прискорення у розвитку. Цифровий шаблон складається із всіляких параметрів голосу, загалом частотних. Очікується масштабне використання даної технології у зв’язку з розповсюдженням смарт-будівель. Досить зручний метод для використання у корпоративних цілях;

• Інші способи. У розділі також були перераховані тільки найпопулярніші способи розпізнавання користувача за поведінковими характеристиками користувача. Серед методів даного виду також наявні варіанти, як

розпізнавання за рухом губ при проголошенні слова-паролю, за особливості рухів при поверненні ключа у замку та інші [1].

Як вже було сказано, основним параметром, що використовується для оцінки надійності різних методів біометричних технологій являються такі статистичні показники, як похибка першого роду (не надати доступ повноправному користувачеві) і похибка другого роду (надати доступ неповноправному користувачеві).

При цьому, неможливо досить точно оцінити різні біометричні системи за статистикою здійснення похибок першого роду, адже на цю статистику значно впливає технічне обладнання, що використовується в процесі роботи технології.

Проте на основі статистики похибок другого роду оцінка різних видів біометричних систем має наступний вигляд (від найзахищеніших до менш надійних):

- За ДНК;
- За райдужною оболонкою ока, сітківкою ока;
- За відбитком пальця, термографією користувача, формою долоні;
- По формі обличчя індивіда, розташуванню вен на гроні руки і долоні;
- На основі розпису;
- За особливостями вводу тексту з клавіатури;
- За специфікою параметрів голосу людини [9].

Можна зробити висновок, що у порівнянні із поведінковими способами розпізнавання користувача, статичні методи значно надійніші, проте слід враховувати, що такі типи біометричних систем потребують більших фінансів для впровадження.

1.2. Параметри продуктивності

Як вже було сказано, в залежності від типу роботи біометричні технології діляться на ідентифікаційні та верифікаційні.

Ідентифікаційна система під час процесу розпізнавання отримує біометричні дані певної особи. Технологія звіряє ці дані із шаблонами, які знаходяться у базі даних збережених біометричних параметрів різних людей. За результатами перевірки технологія або розпізнає індивіда у випадку коли є збіги його характеристик з певним шаблоном, або дає знати що збігів не було знайдено. До біометричних технологій, які працюють таким чином, відносяться, наприклад, системи, які у своїй роботі застосовують правоохоронні органи щоб розпізнати особу за відбитками пальців або знімку. Також такі технології можна задіяти, скажемо, при одержанні певним індивідом соціальної допомоги, щоб запевнитись у його достовірності.

Біометричні технології, що базуються на верифікаційному типі роботи, відрізняються тим, що параметри користувача звіряються не з усіма шаблонами системи, а з конкретною особою, належність до якої вказує користувач. Біометрична система перевіряє запит людини та підтверджує або спростовує його дійсність. Як приклад, такі технології задіяні під час здійснення банківських операцій, коли потрібно упевнитись у автентичності клієнта [4].

Параметри продуктивності біометричних систем, які проводять верифікацію, значно вирізняються від параметрів продуктивності технологій, що проводять ідентифікацію. Ключова характеристика ідентифікаційної системи – вміння цієї системи розпізнати особу за її специфічними параметрами. Оцінка продуктивності залежить від відсотка запитів, при яких була знайдена необхідна особа серед деякої кількості виявлених подібностей.

Як приклад, поліція під час пошуку підозрюваних нерідко застосовують цифровий альбом із фотознімками, які загружаються у комп’ютер. Далі біометрична технологія формує певну кількість знайдених подібностей та список осіб, яких потрібно перевірити. Але в поліції зазвичай звіряють тільки

перші двадцять прізвищ сформованого списку. В даному випадку основна характеристика продуктивності – відсоток випадків, коли підозрювана людина була знайдена серед перших двадцяти прізвищ зі списку з подібностями.

Якщо говорити про біометричні технології, що своєю цілью ставлять саме верифікацію, то продуктивність таких систем залежить від двох характеристик: степеню хибних відмов (система не розпізнає аутентичність правомірного користувача) та степеню хибних підтверджень (система підтверджує достовірність неправомірної особи). Дані характеристики похибок зв’язані один з іншим; певному степеню хибних відмов належить певний степінь хибних підтверджень [7].

Звісно, в ідеалі обидва степені помилок біометричної верифікації мусять рівнятися нулю. Проте, біометричні технології не ідеальні, і доводиться йти на певний компроміс. У випадку, коли для більшої надійності систему налаштують на надзвичайно детальне звіряння параметрів, зменшиться степінь хибних підтверджень, але відповідно збільшиться степінь хибних відмов. З іншого боку, у випадку, коли менеджер для більшого комфорту працівників налаштує систему таким чином, що хибні відмови будуть зведені до нуля, збільшиться степінь хибних підтверджень, таким чином рівень захисту помітно понизиться.

Саме тому зазвичай біометричну систему налаштовують таким чином, щоб досягти певної золотої середини між степенем хибних відмов та хибних підтверджень. У яку сторону будуть схилятися ваги рівноваги залежить від цілей встановлення біометрії для кожного конкретного випадку. Наприклад, якщо впровадити біометричні технології у сучасні банкоматі, то потрібно врахувати крім рівня захисту ще й зручність у використанні та швидкість обробки даних. Тому, для більшої ефективності приладів, степінь хибних помилок логічно зменшити, що трохи збільшить степінь хибних підтверджень.

Висновки до першого розділу

Головна ціль впровадження біометричних технологій є організація такої системи реєстрації, що дуже рідко відхиляє доступ повноправним користувачам та одночасно всеціло виключає неправомірний доступ до різних джерел інформації (насамперед комп'ютерних). Біометричні способи розпізнавання користувача та надання йому доступу до інформації являються набагато безпечнішими та ефективнішими аніж застарілі системи що використовують паролі і картки.

Біометричні методи за параметрами, які вони використовують для ідентифікації особи, діляться на дві групи: фізіологічні та психологічні (поведінкові). До фізіологічної групи відносяться таки методи, як розпізнавання за рисами обличчя, структурою ока (сітківки або райдужної оболонки), характеристиками пальців людини (папілярні лінії, рельєф, довжина суглобів і тому подібне), долоні (її відбиток або топографія), формою руки, схематичним рисунком вен на зап'ясті або тепловим випромінюванням артерій руки. До психологічної групи методів біометрії входять розпізнавання за частотними характеристиками голосу індивіда, специфікою його розпису та почерку, унікальними властивостями введення тексту з клавіатури.

РОЗДІЛ 2. БІОЛОГІЧНІ ДАНІ, ЩО ВИКОРИСТОВУЮТЬСЯ В БІОМЕТРІЇ, ТА ОСОБЛИВОСТІ РОБОТИ З НИМИ

2.1. Відбитки пальців

За останні роки метод біометричного розпізнавання людини за відбитками пальців розпоширився з великою швидкістю та став найбільш перспективним методом серед іншої біометрії. За оцінками дослідників, цей спосіб ідентифікації займає перше місце на корпоративному ринку і в доступному для огляду майбутньому змагатися за лідерство з даною технологією зможе тільки метод розпізнавання за райдужною оболонкою ока.

Урядові і цивільні установи по всій Землі усталено застосовують біометричні системи що грунтуються на порівнянні відбитків пальців як базовим способом перевірки достовірності та розпізнавання людини. І це не дивно, тому що такий параметр особи як його відбитки являється найбільш ефективим параметром, який можна використовувати у комп'ютерних системах для верифікації, через економічність його обробки та значну точність результатів цього процесу. Даною технологією в США користуються, наприклад, відділи транспортних засобів адміністрацій ряду штатів, Mastercard, ФБР, Секретна служба, Агентство національної безпеки, міністерства фінансів і оборони і так далі. Цей метод, впроваджений як система захисту доступу в компанії, значно підвищує ефективність мережевого адміністрування, адже для робітників більше немає необхідності використовувати паролі, тому більше не існує таких проблем як втрата паролю, а, отже, і звернення у службу підтримки [6].

Як правило, біометричні технології визначення особи за відбитками пальців діляться на дві групи: перша використовуються для ідентифікації, друга, відповідно, для верифікації. Перша група в процесі своєї роботи для розпізнавання особи застосовує відбитки всіх десяти пальців. Такі технології

знайшли широкого використання в судових органах. Системи другої групи для верифікації частіше за все використовують дані про відбитки одного пальця, і деколи параметри декількох пальців. Зазвичай, технологія для сканування мається трьох видів: оптичні, ультразвукові та на основі мікрочіпа.

Ключовими характеристиками ідентифікації за відбитками пальців, які зробили цей метод лідером на корпоративному ринку, являються практичність, комфорт у застосування та значний рівень безпеки. Відбитки пальців особи є детальними, майже унікальними, складно підроблюваними та стійкими впродовж життя параметрами людини, що робить їх придатними для ролі довгосторокових маркерів розпізнавання особи. Існує два основних методи перевірки відбитків пальців: по деяким ділянкам (характерним крапкам) та по рельєфу поверхні всього пальця. Перший метод заключається в тому, що спеціальний сканер знімає лише певні деталі, які специфічні для даного відбитку, та обчислює їх розміщення на пальці відносно один одного. Другий метод, відповідно, знімає всю поверхню пальця та аналізую відбиток цілком. На теперішній час біометричні технології нерідко застосовують обидва методи разом, в різній степені. Такий підхід дає змогу позбутися недостатків кожного з алгоритмів та підняти точність процесу розпізнавання.

Зняття відбитку пальця особи за допомогою оптичного сканера не витрачає багато часу. Зображення відбитку отримується використанням маленької CCD-камери, яка може бути як окремим технічним обладнанням, так и просто вбудована у клавіатуру. Тоді, застосовуючи певні алгоритмі, малюнок з відбитком кодується та перетворюється в цифровий образ – схематичне зображення розміщення характерних крапок відбитку, що являють собою унікальні перетини ліній та розриви на відбитку. Це схематичне зображення крапок знову кодується та зберігається в базі даних біометричної системи для розпізнавання осіб. Один такий цифровий образ може містити до сотні мікроточок. Отже, в системі записується не відбиток, а унікальні мікроточки з інформацією про їх розташування, тому користувачам такої технології не варто перейматися щодо конфіденціальності своїх ідентифікаційних параметрів, адже

зображення саме відбитку неможливо відтворити, використовуючи подібні шаблони [10].

Значимий плюс ультразвукового сканування – таким методом можна зняти потрібні параметри без спотворень, що можуть отримуватися через бруд на поверхні пальця. Крім того, отримати характеристику відбитку пальця за допомогою ультразвуку можна навіть через гумові рукавички. Треба сказати, що на теперішній час біометричні технології захищені і від такого способу підроблення відбитку як відрублені пальці, тому що спеціальні чіпи у пристроях можуть аналізувати фізичні характеристики шкіри. На сьогодні, у розробці таких технологій приймає участь більше ніж 50 різних виробників.

Застосування відбитків пальця для розпізнавання людини - найкомфортніший серед всіх біометричних способів. Можливість похибки при перевірці достовірності особи значно менша, аніж у інших способів біометричної верифікації. Проте, точність отриманого зображення відбитку та правильність його аналізу системою зазнає впливу від стану поверхні пальця, а також розміщення пальця відносно знімаючого пристрою. Вплив таких характеристик зняття відбитку на кінцевий результат коливається в залежності від вартості самої системи та від обраного типу перевірки відбитку. Скажемо, ідентифікація за окремими мікроточками стає складнішим якщо на поверхні пальця є бруд. Тип перевірки відбитку шляхом сканування цілої поверхні пальця не зазнає такого сильного впливу бруду, проте, в свою чергу, цей метод потребує достатньо точного розташування пальця на скануючому пристрої. Технічні засоби розпізнавання людини за відбитком пальця не займають багато місця, їх можливо вмонтувати у звичайну комп’ютерну мишу або клавіатуру [1].

2.1.1. Методи зняття відбитків пальців

На теперішній момент розвивається велика кількість пристроїв та способів електронного знімання відбитків пальців. Найпоширеніші серед них оптичний, ємнісний, радіо, нажимний, мікроелектромеханічний та температурний методи.

2.1.1.1. Оптичний метод

При застосуванні даного методу для зняття відбитку можна використати технологію, яка працює аналогічно цифровій камері. Поверхня пальця кладеться на скляну поверхню, висвітлену спеціальним образом. Потрібен лише специфічний об'єктив, що має змогу функціонувати при такому близькому розміщенню суб'єкту знімального процесу. Необхінда картинка отримується завдяки наявності в пристрої сучасної матриці та інших спеціальних технологій. Потім отримані дані перетворюються у чорнобілий малюнок з відтінками сірих кольорів (зазвичай, від 2 до 16 віддтінків є задовільною кількістю). Одним з мінусів такого методу являється те, то сліди відбитку, непримітні для ока, можуть лишитись на скляній пластині де прикладався палець, і зловмисник може застосувати це для отримання несанкціонованого доступу. Ще одним недоліком є те, що даним способом складно розпізнати справжній палець від детально заготовленої підробки [3].
Існує декілька видів оптичного зняття відбитку пальців, описані нижче.

Оптичний метод на відображення використовує такий фізичний ефект як порушення повного внутрішнього відбиття. Сутність ефекту заключається в тому, що при падінні світла на границю розділу двох середовищ світлова енергія ділиться на дві частини - одна відбивається від границі, інша проникає через границю в інше середовище. Частка відображеної енергії залежить від кута падіння світлового потоку. Починаючи з деякої величини даного кута, вся світлова енергія відбивається від границі розділу. Це явище називається повним

внутрішнім відбиттям. Цей метод використовують оптичні FTIR сканери (рис. 2.1).

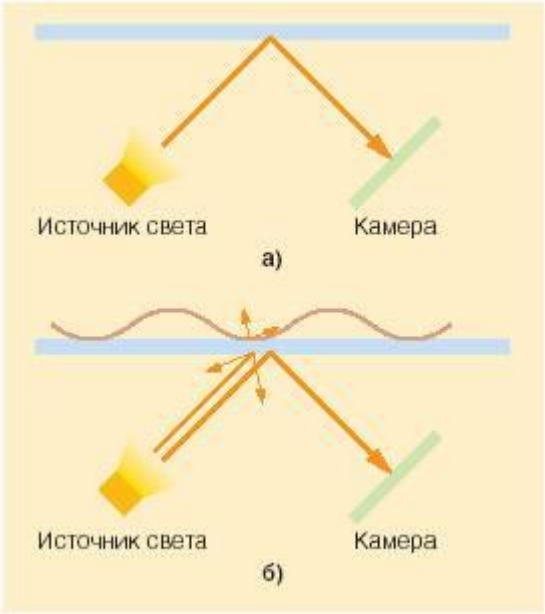

Рис. 2.1 Принцип роботи FTIR сканерів

У разі контакту більш щільного оптичного середовища (поверхні пальця) з менш щільним в точці повного внутрішнього відображення пучок світла проходить через цю межу. Таким чином, від границі відбиваються лише пучки світла, що потрапили в певні точки повного внутрішнього відображення, до яких не було прикладено папілярний узор пальця. Для захоплення отриманої світлової картинки поверхні пальця застосовується датчик зображення особливого призначення.

Недоліки методу:

• Можливість хибного підтвердження при засосуванні підробки;

• Чутливість до забруднень.

Сканери, що застосовуються в технологіях **оптичного методу на просвіт**, представляють собою оптоволоконну матрицю, в якій всі хвилеводи на виході з'єднані з фотодатчиками (рис. 2.2).

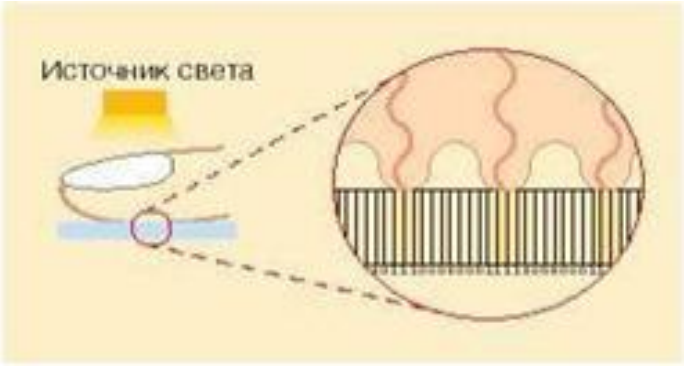

Рис. 2.2 Принцип функціонування оптоволоконних сканерів

Чутливість кожного датчика дозволяє фіксувати залишкове світло, що проходить через палець, в точці дотику пальця з поверхнею матриці. Зображення всього відбитка формується за даними, що зчитуються з кожного фотодатчика.

У даного методу набагато більше плюсів:

• Висока надійність зчитування;

• Стійкість до обману.

Однак у даного методу є також істотний недолік - складність його реалізації.

При **оптичному безконтактному методі** застосовуються оптичні безконтактні сканери (touchless scanners), які не вимагають повного прикладання пальця до поверхні знімаючого пристрою. Палець прижимється до спеціального отвору, кілька світлових діодів освітлюють його поверхню з різних ракурсів, а в центрі пристрою розміщується лінза, яка збирає дані та передає на спеціальну камеру, яка вже конвертує зібрану інформацію в цифровий малюнок відбитка пальця (рис. 2.3) [8].

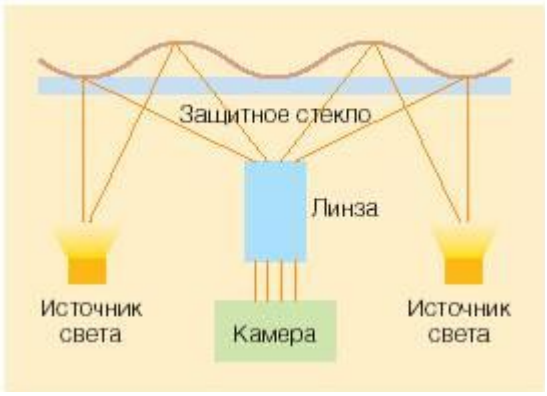

Рис. 2.3 Загальна схема роботи безконтактного сканера

2.1.1.2. Ємнісний метод

Метод грунтується на наступному принципі: поверхня пальця кладеться на спеціалізований прилад, який у своєму складі має матрицю елементів, які сприйнятливі до електричного заряду. Через те, що електропровідність виступів та западин поверхні пальця різна (виступи на шкірі у своєму складі мають воду, а западини включають лише повітря), то ємність елементів матриці змінюється. Таке явище дає змогу установити розміщення виступів та западин і сформувати цифровий малюнок відбитку. Цей спосіб являється одним з найпоширенішим, хоча така технологія зняття інформації відбитку пальця має певні недоліки, такі як чутливість пристрою до електростатичних розрядів та різним паразитним електричним полям.

2.1.1.3. Радіо метод

У випадку, коли через поверхню пальця проводяться радіохвилі малої щільності, можна з’ясувати відносне розміщення виступів та западин шкіри, використовуючи пристрій з матрицею антенних елементів, налаштованих належним чином. Для цього необхідно, щоб поверхня пальця прикладалася до спеціального датчика, частина якого випромінює радіохвилі. Даний спосіб базується знову таки на фізіологічних характеристиках шкіри, а тому отримати несанкціонований доступ шляхом використання підробки пальця майже неможливо. Недоліком цією технології є вимога прискіпливого процесу

піднесення пальцю до пристрою, випромінююча частина якого має властивість нагріватись, що позначається на зручності використання.

2.1.1.4. Нажимний метод

Щоб отримати характеристики відбитку пальця можна використовувати пристрої, матриця п'єзоелектричних елементів яких сприйнятлива до натиску. Дані технології мають достатньо слабких місць, таких низька чутливість елементів, неспроможність розрізняти палець користувача від підробки, можливість нанесення пошкоджень через надмірні зусилля і так далі. Проте існують виробники біометричних пристроїв, які все ще розробляють прилади, що базуються на даній технології.

2.1.1.5. Мікроелектромеханічний метод

Дані технології ще тільки розвиваються, проходячи стадію розробки та досліджень, проте поступово інтегруються задля аналізу їх ефективності. Цей метод також знімає дані про розміщення виступів та западин на поверхні пальця, використовуючи розроблену матрицю мікроелектромеханічних датчиків. Поки що важко робити висновки про стійкість елементів задіяного пристрою та точність інформації, що можна отримати даним способом, проте до списку недоліків уже можна внести неспроможність виявити підробку пальця.

2.1.1.6. Температурний метод

Спосіб базується на здатності піроелектричних елементів за зміною температури виробляти деяку напругу. Саме це явище застосовується в процесі роботи інфрачервоних сканерів. Спеціальний датчик працюючого по даній методиці приладу, при контакті з поверхнею пальця, дозволяє отримати значення температур у місцях стику елементів пристрою з виступами та западинами на шкірі.

Така технологія налічує велику кількість переваг, серед яких можна виділити відсутність впливу на процес роботи пристрою електростатичного розряду та високу зручність при використанні, так як палець не зазнає ніякого випромінювання. До того ж, пристрої що грунтуються на цьому методі дозволяють отримати точну інформацію про поверхню пальця за будь-якої температури довкілля та виявити підробку пальця, с чим не справляється достатня кількість методів.

Єдиним недоліком цього методу є те, що отримуване цифрове зображення пальця користувача досить нестабільне і його потрібно швидко фіксувати. Це відбувається через те, що в момент прикладення поверхні пальця до приладу різниця їх температур створює певний степінь напруги, але вона на протязі дуже малого часу (менше десятої секунди) поступово згасає, адже температура пальця та сканеру приходить до рівноваги [1].

2.1.2. Інформаційні ознаки відбитків пальців

По кожному відбитку пальця виділяють дві групи ознак - глобальні і локальні.

Глобальні ознаки – такі, що являються видимими без використання спеціальних засобів:

• Папілярний узор.

• Область образу – велика частина відбитку, у якій зібрані усі інформативні фрагменти.

• Ядро – точка, що знаходиться посередині відбитку або певного фрагменту.

• Пункт «дельта» – початкова точка. Може бути як місцем поділу або злиття борозенок папілярних ліній, так і досить малою за розміром однією борозенкою.

• Тип лінії – визначається двома найбільшими лініями, що спочатку паралельні, але далі розминаються та проходять по периферії усієї області образу.

• Лічильник ліній – визначається кількістю ліній на всій області образу або між ядром і пунктом «дельта».

Рис. 2.4 Типи папілярних рисунків

1 – 4 – рисунок виду «петля» (ліва, права, центральна, подвійна), 5 і 6 – рисунок виду «дельта» або «дуга» (проста і гостра), 7 і 8 – рисунки виду «спіраль» (центральна і змішана).

Друга група ознак – ***локальні***. Вони мають назву мінуції – неповторні параметри відбитку, які характеризують точки, в яких форма папілярних ліній змінюється (наприклад, утворюються закінчення, роздвоєння, розриви та тому подібне), а також вміщують розміщення цих ліній та описаних віще точок. Будь-який відбиток складається з приблизно сімдесяти мінуцій [11].

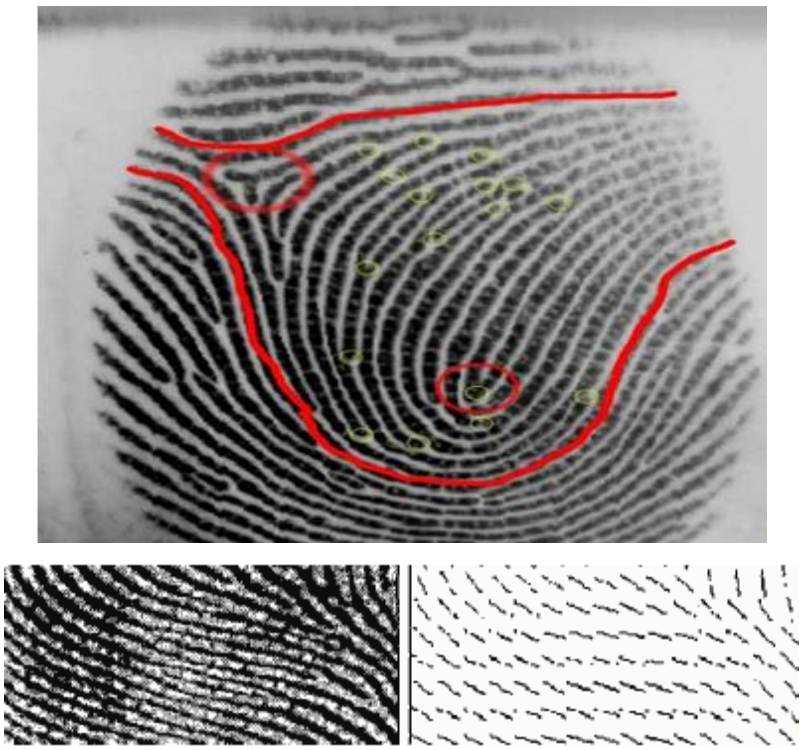

Рис. 2.5 Установлення поля орієнтації папілярних ліній

При аналізі показаного відбитку можна помітити такі параметри:

- дві лінії – «тип лінії»; Областю образу може бути все, що знаходиться поміж цих ліній, проте у багатьох випадках аналізується вся площа відбитку;

- червоне коло зліва – пункт «дельта»; червоне коло нижче – ядро;

- жовтими кругами відмічені мінуції.

Глобальні ознаки деяких осіб можуть бути невідрізними, тому ідентифікувати користувачів лише за цими параметрами не є ефективним. Проте мінуції різних людей завжди індивідуальні, тому зазвичай глобальні ознаки застосовують для розподілення бази даних на певні степені та на перших рівнях ідентифікації. На останніх рівнях розпізнавання застосовують мікроточки [3].

2.1.3. Стандарти на відбитки пальців

Наразі як правило застосовуються стандарти ANSI (Американський інститут національних стандартів) та ФБР США. За ними образ відбитку має відповідати наступним параметрам:

• будь-який образ подається у вигляді нестиглого зображення формату TIF;

• образ має обладати роздільною здатністю не нижче 500 точок на дюйм;

• образ має мати 256 степеней яскравості;

• Відбиток має відхилятися по вертикалі не більш ніж на 15 градусів;

• Базовим видом мінуцій для розпізнавання виступають закінчення і роздвоєння.

Прийнято зберігати у сховищі шаблонів одразу декілька образів одного і того ж образу, задля покращення ефективності ідентифікації. Допускаються відмінності між шаблонами за невеликими поворотами та зсувами. При цьому масштабування образів залишається сталим, адже відбитки знімаються з одного й того ж приладу [1].

2.1.4. Принципи порівняння відбитків за локальними ознаками

Зіставлення відбитків ділиться на наступні етапи:

• Етап 1. Покращення властивостей відсканованого малюнку. Покращується чіткість межі розподілу ліній відбитку.

• Етап 2. Розрахунок розміщення папілярних ліній. Малюнок ділиться на певні блоки квадратної форми, сторона яких не менше 4 пікселів, та розраховується кут розміщення ліній для кожного витягу відбитку.

• Етап 3. Опрацювання малюнку до півтонового виду. За допомогою спеціальних алгоритмів малюнок стає чорно-білим.

• Етап 4. Утоншення ліній отриманого малюнку відбитку. Витончення

застосовується до того моменту, поки розмір товщини ліній не стане 1 піксель (рис. 2.6).

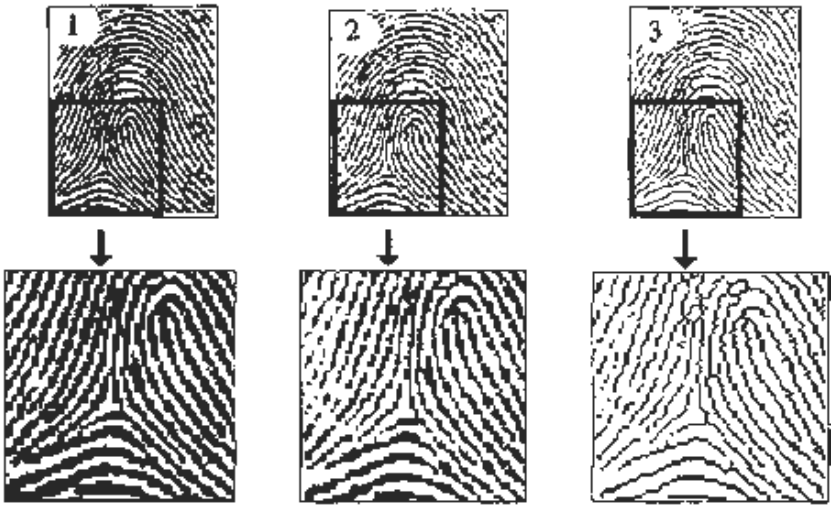

Рис. 2.6 Етап 4. Витончення ліній відбитку

• Етап 5. Акцентування мінуцій. Спочатку малюнок ділиться на квадратні блоки зі стороною 9 пікселів. Потім за допомогою алгоритмічного опрацювання технологія знаходить кількість чорних пікселів, які розміщуються в центральній зоні. Такий піксель називається мінуцією, у випадку коли він сам чорний та поряд з ним знаходяться один (тип «кінцівка») або два (тип «подвоєння») чорних пікселі (рис. 2.7).

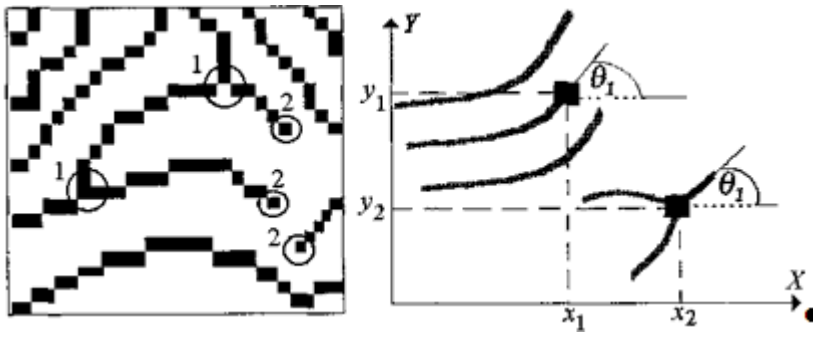

Рис. 2.7 Етап 5. Акцентування мінуцій

Координати знайдених мікроточок, їх кути положення та загальна кількість обчислюються за певною векторною формулою, і саме вона буде зберігатися у системі як шаблон з даними конкретного користувача. В процесі ідентифікації формула буде встановлювати достовірність відбитку [12].

• Етап 6. Порівняння мікроточок

Пара відбитків двох користувачів можуть мати різні зрушення один відносно одного, не кажучі про поверхню контакту пальця з приладом дивлячись на те, як особа прижимає його до пластини. Саме через це верифікація відбитків індивіда методом звичайного зіставлення неможлива. Тому робота пристрою по порівнянню параметрів відбитку повинна проходити по кожній мікроточці шаблона та отриманого знімку. Даний етап проходить за наступним алгоритмом:

• Реєстрація параметрів.

• Пошук пар відповідних мінуцій.

• Визначення ідентичності відбитків.

В момент реєстрації знаходять характеристики розміщення (кут повороту, масштаб та зсуви), враховуючи які певна мікроточка з одного вектора співвідноситься певній мінуції з іншого.

В процесі цього для будь-якої мікроточки необхідно врахувати до тридцяти випадків кутового повороту (від -15 градусів до +15), 500 величин зсуву (від -250 пікселів до +250 пікселів – проте деколи границі обираються в дещо менших розмірах) та 10 величин масштабу (від 0,5 до 1,5 з кроком 0,1). Усього існує до 150 000 таких врахувань, які можна застосувати до всякої із 70 вірогідних мікроточок. Але в технології опрацювання відбитків усі врахування параметрів не використовуються, адже після врахування можливих специфік розміщення якоїсь однієї мікроточки вже можна починати застосовувати отримані обчислення для інших з даного відбитку. В іншому випадку шляхом багатьох обчислень можна співвіднести майже всі відбитку один до одного.

Визначення ідентичності відбитків здійснюється за формулою:

$$K = \frac{D*D*100\%}{p*q},$$

де D - число мікроточок, що виявились тотожними, p - число мікроточок шаблону, q - число мікроточок відбитку, який звіряється [13]. В разі, коли збіг

по кількості мінуцій являється більшим за 65%, система підтверджує достовірність відбитку. (процент збігу для підтвердження можна змінювати в залежності з достатнім для клієнта рівнем захищеності) Система, працююча в цілях верифікації, після отриманого результату припиняє роботу. Якщо необхідна саме ідентифікація, то потрібно таке порівняння провести по усім відбиткам, збереженим в системі. Після цього знаходиться шаблон, степінь збігу з яким найбільший серед інших. Степінь тотожності в цьому випадку має бути більшим ніж 65% [1].

2.1.4.1. Інакші методи зіставлення відбитків.

Описана технологія являється дуже точною та ефективною, проте біометричні системи активно розвиваються і тому досліджуються нові способи зіставлення параметрів відбитків, які згодом можуть виявитись більш результативними. Так, наприклад, при використання **методу, що грунтується на глобальних ознаках**, спочатку визначаються глобальні ознаки відбитку (наприклад, ядро, дельта та інші). Потім за числом цих параметрів та їх відносному розміщенню визначається тип узору. Верифікація та ідентифікація проходить, використовуючи вже локальні ознаки. Кількість обчислень, які необхідно здійснити системі для зіставлення відбитків таким способом менша, а отже працюють вони швидше.

Метод, що використовує графи, працює на основі алгоритму, що відображений на рис. 2.8. Отриманий малюнок відбитку (1) перетворюється в схематичне відображення розташування папілярних ліній (2). Далі знаходять фрагменти з аналогічним розміщенням ліній та границі між такими фрагментами (3). Після цього установлюються центри фрагментів та таким чином отримують граф (4). На етапі, що помічений стрілкою "d", відбувається збереження отриманої інформації відбитку особи у систему. Зіставлення відбитків та оцінка їх тотожності відбувається у квадраті (5). Далі технологія працює таким самим чином, як і за попереднім способом – ідентифікація за мікроточками.

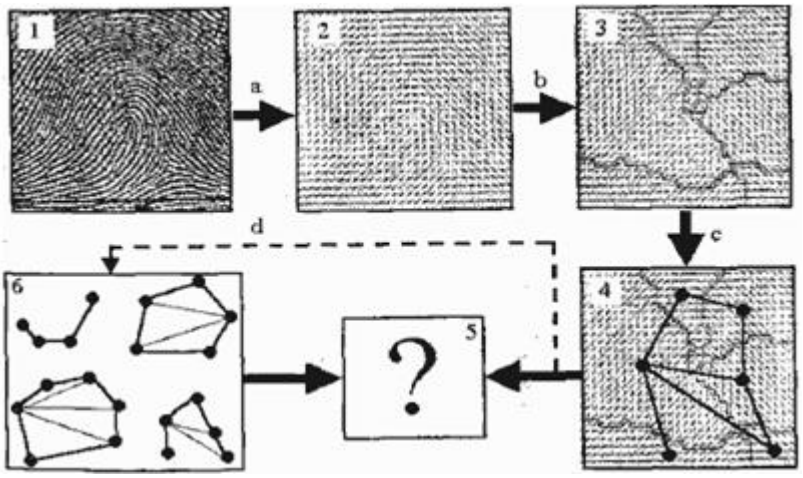

Рис. 2.8 Метод з використанням графів

2.1.5. Методи обходження такої системи доступу

1. Конденсація. У деяких випадках якщо подихати на контактуючу поверхню можна побачити сліди відбутку особи, яка користувалася пристроем до цього. Спосіб може спрацювати тільки для пристрою з оптичним сканером. Для напівпровідникових така махінація неможлива.

2. Можна підробити відбиток іншої особи за допомогою скотча, проте, як і до цього – спосіб можливий тільки при використанні оптичних сканерів.

3. Можна скористатися жуйкою для вироблення підробки, проте даний спосіб не спрацює через те, що відбиток отримається у вигляді дзеркального відображення. Але, мабуть, підготовлені спеціалісти зможуть підробити відбиток з подібного матеріалу.

4. Використання відрізаного пальця не дасть результату, адже мертві тканини моментально починають втрачати попередній вигляд. До того ж, деякі системи застосовують технологію, яка виявляє такі параметри як температура, пульс и так далі, проте вони і коштують значно більше. Можна підвищити надійність системи доступу шляхом впровадження додаткової технології, наприклад, розпізнавання за райдужною оболонкою ока..

5. Підробка з використанням желатину. Досить ефективний спосіб, що був продемонстрований на конференції з безпеки Міжнародного Союзу

телекомунікацій в Сеулі. Аспірант університету Йокогами Цутому Мацумото (Tsutomu Matsumoto), застосовуючи клей, желатин та предмет з відбитками іншої особи, зумів обійти системи розпізнавання, що функціонують за допомогою різних типів скануючих пристроїв. Коштовність складових підробки знаходиться у межах 10 доларів, а виробити муляж можливо навіть в домашніх умовах. Статистика хибного підтвердження була від 70 до 95% [2].

2.1.6. Оцінка біометричної системи ідентифікації за відбитками пальців

Переваги:

1. Відсутність необхідності користування логіном та паролем, отже можна не перейматися через можливість їх втрати.

2. Дуже складно виробити муляж (відношення ціни та надійності дуже високе).

3. Невеликі габарити скануючих пристроїв дає змогу впроваджувати їх навіть на мобільні прилади. Подібні технології будуть дуже ефективними у наш час, коли переважна більшість осіб має мобільні телефони та USB-пристрої для зберігання інформації. У випадку викрадення приладів з вмонтованою біометричною системою можна не перейматися за те, що особисті дані стануть доступні посторонній людині.

Недоліки:

1. Вважається, що дані, зібрані з відбитків пальців користувачів деяких систем, стануть застосовуватись правоохоронними органами без відома осіб, яким вони належать.

2. Розпізнавання характеристик відбитку неможливе у випадку пошкодження шкіри пальця.

3. Достовірність верифікації також ускладнюється наявністю бруду на поверхні пальця.

2.2. Геометрія особи

Сучасний метод розпізнавання людини, який зазнав значного розвитку в останній час – визначення особи за її зовнішнім виглядом. Забезпечити ефективність такої системи не проста задача. У процесі розробки такої технології багато часу витратили на те, щоб навчитися одержувати необхідні дані, застосовуючи фото або відеокамери. Уряд США та Німеччини навіть виділив фінансову допомогу для великої кількості організацій, що займалися розробкою таких систем. Відповідно, на початку розвитку такі технології планували впроваджувати для збільшення ефективності правоохоронних органів, проте згодом подібні системи почали використовувати і в інших сферах.

Прилади, що працюють за цим принципом, дозволяють проводити сканування індивідів будь-де та в будь-який час. Спеціальні камери, підключені до відповідних комп’ютерів, знімають фото людини и технологія підтверджує або спростовує відповідність особи з тією, характеристики якої зберігаються в системі. Методика процесу ідентифікації по зовнішності базується на новітніх способах перетворення зображень у цифрові дані, які у своєму складі мають такі характеристики обличчя як взаємне розташування, форма та розміри очей, носа, губ і таке інше. Такі оцифровані дані виконують роль мінуцій при ідентифікації за відбитками пальців, тобто являють собою унікальні мікрокрапки, які є неповторними для кожного користувача. Зазвичай для надійного розпізнавання достатньо визначити близько 40 таких точок обличчя, в той час як технологія знаходить близько 2 тисяч таких характеристик. Система може знайти так багато оригінальних параметрів особи за допомогою аналізу її обличчя, що точність та достовірність отриманої інформації не залежить від повороту голови, використання косметики чи окулярів.

Біометричні технології ідентифікації особи за зовнішністю діляться на два види. Системи першого виду грунтуються на статистичному методі: знімається зображення людини, за допомогою певних алгоритмів отримується

оцифрований шаблон який представлений набором чисел, які визначають конкретного індивіда. Така технологія дуже популярна, проте результати розпізнавання виходять не достатньо точні.

Системи другого виду здатні підлаштовуватися до факторів мінливості зовнішності людини. Вони враховують наявність бороди на обличчі, окулярів та навіть вік. Це означає що такі технології дозволять для розпізнавання застосовувати і застарілі фото особи. Деякі системи здатні обчислювати необхідні дані навіть за рентгенівськими знімками. Ефективність даного способу обумовлена тим, що він користується принципом, аналогічним до того, як сама людина аналізує іншу з метою розпізнати її. Встановлення достовірності людини за її зображенням на паспорті, як і за унікальним підписом, являється одним з найзручніших та ефективних способів.

Такі методи доцільно застосовувати і в цілях контролю доступу до інформації, тому що вони не займають багато часу та розпізнавання відбувається за відсутності безпосереднього контакту користувача з біометричним приладом, що, знову ж таки, досить зручно.

Технології ідентифікації/верифікації особи за її зовнішністю можливо застосовувати в різних сферах: від пошуку певної особи, порівнюючи його зображення, відзняте з камер спостереження, з шаблоном, збереженим в системі, до звичайного контролю доступу. Такі методи встановлення достовірності користувача втрачають ефективність тільки в тому випадку, коли відбулись великі зміни в зовнішності (як приклад, через певний нещасний випадок), що приводить до неможливості розпізнати людину навіть іншим особам.

Як ми вже знаємо, усі біометричні технології в залежності від параметрів які вони застосовують мають як свої переваги, так і недоліки. Тому немає сенсу гадати, що певна технологія досягне більш високої ефективності для будь-якої ситуації. Проте серед біометричних систем існують найбільш універсальні технології, такі як встановлення особи за відбитками пальців, райдужній

оболонці ока або зовнішності, і людина повинна сама, враховуючи конкретну ситуацію, обрати придатну для неї систему.

Технологія встановлення персони індивіда за його зовнішністю у своїх перевагах має той факт, що людині не потрібно тісно взаємодіяти з біометричним пристроєм та виконувати певні дії.

Варто наголосити, що ідентифікація людини за неповторними рисами обличчя – один з небагатьох біометричних методів встановлення персони, в процесі використання якого немає необхідності у специфічних приладах. Метод використовує близький до людського підхід, адже ми впізнаємо знайомих нам людей завдяки рисам зовнішності, а не займаємося зіставленням відбитків пальців та звірянням райдужної оболонки ока. Цей спосіб відомий вже досить давно, за часів, коли застосування фото для встановлення персони було одним з єдиних на той час методів біометричної ідентифікації. Саме тому впроваджувати цей метод у сучасні технології досить просто, адже представлення про нього вже давно закоренилося у свідомості людей.

Технологія ідентифікації людини за зовнішнім виглядом також є найкращим біометричним методом встановлення достовірності індивіда з точки зору багатоцільового використання. Якщо розпізнавання особи іншими способами застосовується в основному для надання доступу або зіставлення даних зі збереженими в системи, то спосіб розпізнавання за зовнішністю дає змогу як одразу використовувати характеристику особи, знятої на відеокамеру, так і проігнорувати отримане зображення, якщо це не потрібно. Якщо казати про спроби обійти таку систему, то через вмонтований інфрачервоний випромінювач технологія здатна відрізнити маску від справжнього обличчя людини. Біометрична система визначає людську шкіру та міміку обличчя, і при підозрі муляжу одразу сповіщує про це активацією спеціального сигналу. Процес зйому зображення зовнішності проходить непомітно, на певній відстані від об’єкта, часто без його відома. Звичайно, для роботи правоохоронних органів це є значимим параметром. Але правозахисники виражають незадовільність даними методами, спираючись на порушення права людини на

анонімність. Проте розробники біометричних пристроїв потурбувалися про подібні скарги. Права людини не порушуються, адже у випадку, коли технологія не підтверджує достовірність особи з тою, яку потрібно визначити, то вона автоматично стирає всі отримані дані відзнятої людини, яка потрапила до зони зйому відеокамери [3].

До того ж розробники запевняють, що в технологіях розпізнавання використовуються звичайні камери відеоспостереження, особливості роботи яких давно установлюються чинним законодавством. Наприклад, на теперішній час існує правило, згідно якого в місцях с відеоспостереженням оголошується відповідне попередження.

Такими технологіями розпізнавання особи користуються служби безпеки переважної більшості різних організацій, не кажучи про урядові установи.

Практика використання розпізнавання особи по обличчю

Спосіб встановлення особи за зовнішнім виглядом безсумнівно закріпив за собою звання однієї з найефективніших технологій. Цей метод застосовується такими установами, як Банк Німеччини, Європейський центр ядерних досліджень, корпорації Microsoft, Siemens та багато інших. Атомні електростанції та більшість надтаємних контрольованих зон також користуються даними біометричними системами. Завдяки впровадженню компанією ZN Vision Technologies першої цифрової бази даних фотографій з технологіями встановлення персони, велика кількість охоронних служб в різних країнах досягли величезного покращення ефективності процесу пошуку зловмисників.

2.3. Геометрія руки

Біометричні технології даного типу працюють за принципом використання обладнання, що встановлює особу за допомогою порівняння унікальних характеристик долоні. В процесі розпізнавання системою розглядається більше

90 параметрів, таких як розміри долоні, показники довжини та ширини пальців, особливості суглобів і так далі. На практиці застосування цього способу розпізнавання особи зустрічається в законодавчих органах, міжнародних аеропортах, лікарнях, імміграційних службах та багатьох інших. Серед позитивних моментів використання таких технологій можна назвати такий самий степінь точності та швидкості обробки даних як в системах що користуються відбитками пальців, а недоліком являється те, що пристрої для зчитування інформації за формою руки не такий компактний як того вимагають деякі випадки [1].

2.4. Геометрична карта судин долоні

Науково-технічний журнал IEEE Spectrum присвятив статтю використанню систем біометричної ідентифікації за геометричною картою судин долоні при проведенні платежів в Японії. З 2005 року банки країни впровадили "біометрії" в 80 тис. Банкоматів, а також в торгові термінали та інші пристрої. Технологія настільки добре себе зарекомендувала, що новою технологією зацікавилися банки не тільки Японії, але також Бразилії, Польщі та Туреччини.

Системи, запропоновані незалежно один від одного компаніями Hitachi і Fujitsu, засновані на скануванні малюнка кровоносних судин руки. У кожної людини суто індивідуальний малюнок вен, артерій і капілярів, він ідентифікує людину краще, ніж відбитки пальців.

На відміну від сканерів райдужної оболонки ока, сканер судин працює швидко і просто, а сам пристрій набагато дешевше.

Hitachi і Fujitsu вже кілька років працюють над комерційним впровадженням подібних систем - у кожної з них своя реалізація, різні методи просвічування руки, проте сканери Hitachi сканують тільки пальці, а не долоню цілком.

Поки що сканер капілярів всього лише доповнює (або навіть замінює) PIN-код карти, але в майбутньому можлива заміна всієї карти цілком, тобто оплачувати товар можна буде, пред'явивши машині руку. Це буде повноцінна біометрична платіжна система: новий рівень абстракції в нашому розумінні грошей.

Така система набагато складніше, ніж нинішня реалізація, адже замість простої верифікації особистості потрібно буде здійснити повноцінне розпізнавання особистості. Компанія Fujitsu недавно поділилася результатами експерименту, в якому брало участь 5 млн користувачів: система коректно розпізнає людину в середньому за 1,34 секунди.

Першим європейським банком, що почав використовувати банкомати, що дозволяють знімати клієнтам гроші з рахунків на основі біометричних даних, став польський банк BPS SA, котрий використовував технологію Finger Vein, розроблену компанією Hitachi. Усередині кожного біометричного банкомату знаходиться сканер, який отримує дані про унікальну для кожної людини систему кровоносних судин в пальці.

У вересні 2012 року японський банк Ogaki Kyoritsu Bank першим в світі запустив нову біометричну платіжну систему: для зняття грошей в банкоматі не потрібна пластикова картка, досить просто піднести руку до сканера, ввести PIN-код і дату народження.

Прискорити роботи щодо практичного впровадження нової технології японський банк змусили тодішні природні катастрофи, що залишили десятки тисяч людей без документів і банківських карт.

Сканери можуть використовуватися і в торгових автоматах. Наприклад, якщо ви хочете купити пляшку мінералки в торговому автоматі, потрібно всього лише доторкнутися рукою до сканера - і ви отримаєте свій товар.

2.5. Термограма особи

Метод встановлення людини за термограмою заснований на дослідженнях, які показали, що термограма особи є унікальним параметром кожного індивіда.

Термограму отримують за допомогою камер інфрачервоного діапазону. Метод має перевагу відносно систем розпізнавання за зовнішністю, оскільки він може розрізняти близнюків. Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, температура тіла, охолодження шкіри обличчя в морозну погоду не впливають на точність термограми. Через невисоку якість ідентифікації, метод на даний момент не має широкого поширення [1].

2.6. Райдужна оболонка ока

Даний тип систем також є одним з найефективніших. Це пов’язано з тим фактом, що райдужка оболонка ока є неповторним персональним параметром кожної окремої людини, що є різним навіть у близнюків. Розпочалося дослідження райдужної оболонки ока з суто медичними цілями - вивчення симптомів певних недугів. Серед усього іншого вчені прийшли до висновків, що деякі захворювання викликають появу на райдужній оболонці різних пігментів. Враховуючи цей фактор, біометричні технології що базуються на даному методі, застосовують чорно-білі малюнки.

Біометрична технологія у методиці своєї роботи використовує як основний визначаючий параметр для створення шаблону особливу тканину, що розвивається у плоду до восьмого місяця вагітності і завдяки якій можна побачити розподіл райдужної оболонки на радіальні сектори. Решта параметрів має у своєму складі такі особливості як унікальні кільця, борозни, веснянки та область корони. За допомогою райдужної оболонки 11-міліметрового розміру біометричні системи можуть знайти приблизно 3-4 біт цифрових даних на 1 мм2 площі. Райдужна оболонка містить до 266 специфічних мікроточок що використовуються для розпізнавання, на відміну від більшості біометричних технологій, що працюють з мікрокрапками у кількості від 10 до 60 штук.

Саме тому переконливо займають лідируючі позиції на ринку біометрії такі системи, що використовують даний метод, адже можна переконливо заявити що ефективність таких технологій є однією з найкращих.

Розглянемо, яким чином проходить процес розпізнавання особи за райдужною оболонкою в біометричній системі. Сканування ока та отримання його зображення виконується спеціальним пристроєм, при чому відбувається це на дистанції до одного метра. Наступні процеси дослідження та обчислення параметрів ока можна поділити на такі етапи: процес захвату райдужної оболонки, процес виділення зіниці, процес аналізу та обчислення характеристик райдужної оболонки та процес установлення результатів перевірки. Перший та другий процес в методиці свого функціонування оперує наступними факторами: круглою формою райдужної оболонки та зіниці та високим степенем контрасту на фоні білої частини ока. На теперішній момент мається багато методів оперативного визначення кругів на малюнку, проте одним з найпопулярніших являється спосіб, що грунтується на перетворенні Хафа. В процесі отримання результату розпізнавання особи, технологія застосовує збережені в базі даних шаблони зареєстрованих користувачів, на фоні яких проходить перевірка параметрів особи, у якій потрібно удостовіритись. Кількість ознак, за якими буде проходити розпізнавання, залежить від цілі такої перевірки, тобто яке саме розпізнавання відбувається – верифікація або ж ідентифікація.

Отже, як вже було сказано раніше, біометричні системи, працюючі на принципі унікальності параметрів райдужної оболонки ока, відрізняються високим рівнем захисту. Наведемо певні статистичні дані, які демонструють надійність таких технологій найкращим образом. Степінь показнику похибки другого роду, коли особа, не маючи достатніх прав, проходить перевірку та отримує несанкціонований доступ, для технології даного типу виражається у вірогідності 1 до 1,2 мільйонів випадків ідентифікації.

Сучасні пристрої мають змогу розпізнавати особу навіть у випадку затінення (або ушкодження) райдужої оболонки, коли величина таких змін

складає 2/3 від площі оболонки та менше. При таких умовах показник похибки розпізнавання особи складає вірогідність 1 до 100 тисяч процесів ідентифікації.

Якщо казати про спроможність даних систем протистояти різним методам обману, то біометрія заснована на зніманні характеристик райдужної оболонки ока володіє багатьма рівнями захисту, наприклад: розпізнавання муляжу зіниці; зчитування даних, знайдених на рогівці; визначення наявності контактних лінз, застосування інфрачервоного світла з метою перевірки стану тканин ока. Саме тому дуже важко знайти опис ситуацій, в яких зловмисникам вдалося обійти цю біометричну систему.

Недоліком даних технологій є висока вартість пристроїв, проте вона відповідає їх параметрам якості та ефективності [1].

2.7. Сітківка ока

Рівень захисту, який предоставляється біометричними системами даного типу, можна порівняти з методом встановлення особи за райдужною оболонкою ока. Принцип знімання параметрів сітківки ока достатньо непростий (потрібно мати специфічний прилад, який за допомогою інфрачервоного світла робить видимим шукані характеристики), проте даний спосіб розпізнавання людини відомий досить давно. Дослідники Саймон та Голдштайн ще у 1935 році відкрили специфічність узору кровоносних судин очного дна будь-якої людини. Згодом стало відомо, що даний параметр являється персональним та неповторним в тому числі і для близнюків.

Якщо не враховувати певні види захворювань ока та випадки пошкоджень голови, зображення узору кровоносних судин залишається досить усталеним на протязі всього життєвого циклу особи.

Широке розповсюдження даного способу розпізнавання призупиняється тим, що воно достатньо складне та процес взаємодії пристрою та користувача не такий комфортній, як при використанні інших систем. За статистикою, тільки 85% від усієї кількості людей зазвичай проходять процес зняття

параметрів сітківки з першої спроби. При цьому особі треба приблизити око до спеціального скануючого приладу, необхідна дистанція між оком та скануючою поверхнею становить 1-1,5 сантиметри максимум. В момент знімання зображення людина фокусує погляд на маленькому зеленому світлодіоду, що повертається навколо своєї осі. На відміну від, скажімо, методу перевірки індивіда за допомогою відбитків пальців, де застосовується приблизно 30-40 мікроточок, прилад що працює по принципу специфіки сітківки зчитує з її зображення більше 400 унікальних мікроточок, обчислює їх та формує образ, який зберігається в базі даних системи та використовується надалі для розпізнавання особи. Саме тому цьому виду біометричних систем властива надійність, що перевершує більшість різних способів розпізнавання людини.

Якщо казати про статистичні показники похибок при застосуванні даних систем, то для похибки другого типу (надати доступ неуповноваженій особі) величина вірогідності становить 0,0001%, що вказує на великий степень захищеності яку пропонує дана технологія. Проте показник похибки першого типу (не надати доступ уповноваженій особі) набагато більший – аж 0,1%. Такі цифри пов’язані з тим, що на початку формування методу подібні технології вироблялися для використання у військових організаціях, а тому основною задачею створеної системи було ліквідувати можливість несанкціонованого доступу до об’єкта, а комфортабельність застосування такого способу відводилася на другий план. Планувалося, що через досить високу для системи доступу вірогідність хибної відмови особа матиме можливість пройти процес перевірки на достовірність в декілька спроб. Враховуючи описані фактори, така технологія на теперішній момент не зазнала великого поширення серед цивільних замовників систем контролю доступу.

Серед недоліків методу можна назвати також певну незручність, з якою проходить процес знімання даних з сітківки ока, і, як в випадку методу ідентифікації за райдужною оболонкою ока, велику вартість приладів – середня ціна становить близько 4000 доларів.

Цікаво, що у сучасному світі комп’ютерні технології розвинулися до такого степеню, що можуть не просто побачити особу та відрізнити її на фоні довкілля, проте ще й розпізнати персону людини та виконувати функції контролю доступу [1].

2.8. Голос та мова

Велика кількість компаній займаються розробкою біометричних систем, які мають змогу розпізнавати особу за особливостями її голосу. Грунтується метод на таких характеристиках як частотні особливості, інтонація, висота тону і таке інше. Серед переваг таких систем можна назвати відсутність застосування пристроїв дорогої вартості, можна здійснити ідентифікацію використовуючи тільки звукову плату та мікрофон.

Проте дана технологія, не зважаючи на зручність використання, не настільки точна на фоні інших типів систем. Особа, яка захворіла і голос якої в результаті цього змінився, може не отримати підтвердження при проходженні верифікації. Взагалі голос людини зазнає впливу багатьох фізіологічних та психологічних факторів, через це основним недоліком систем даного типу є невисока надійність оцінки розпізнавання. Але це не заважає таким біометричним технологіям впроваджуватись до систем контролю доступу до об’єктів невисокого рівня секретності [1].

2.9. Підпис

Підпис особи – персональний неповторний параметр, хоча і не являється невід’ємною фізіологічною частиною. Це більш звичний спосіб розпізнавання індивіда, адже його використання не викликає у свідомості асоціації з кримінальною сферою, як це трапляється у випадку знімання відбитків пальців. Такий метод є досить ефективним, принцип ідентифікації базується на специфіці параметрів руху особою руки в момент письма. Методи

розпізнавання людини за параметрами письма можна поділити на два типи: звичайне звіряння отриманого підпису з шаблоном та більш складну динамічну верифікацію. Методика першого типу не відрізняється точністю результатів перевірки, тому що просте звіряння з шаблоном, збереженим в системі, не зовсім ефективний спосіб. Особа може вводити один і той же підпис по різному, тому подібна перевірка матиме досить високу вірогідність похибки. Системи другого типу розпізнавання особи за підписом використовують значно більших факторів та у своїй методиці використовують такі характеристики введення підпису як особливості руху руки особи в певних моментах написання, сила тиску та довготривалість виведення кожного фрагменту підпису. Саме тому обхитрити таку систему буде не в змозі навіть спеціаліст, що займається імітацією підписів, адже в точності та деталях повторити підсвідомі рухи руки будь-якої особи надзвичайно складно.

Особа, застосовуючи звичайний дигітайзер та ручку, спокійно вводить свій персональний підпис, а технологія в цей час фіксує характеристики написання та перевіряє з шаблоном, збереженим в системі. Якщо характеристики тотожні до тих, що зберігаються в базі даних, технологія додає до документа, що підписується, дані, які складаються з ім'я користувача, його електронної пошти, посади, поточного часу та дати, характеристики введення підпису, великої кількості особливостей руху написання (швидкість, прискорення, напрям, тиск), та інше. Отримана інформація зашифровується, за спеціальною формулою розраховується контрольна сума, і таким чином формується біометрична мітка. В цілях налаштування системи особі необхідно декілька разів (від 5 до 10) повторно здійснити введення підпису, таким чином утворюється більш досконалий шаблон.

Застосування біометричних систем розпізнавання, що працюють на основі перевірки підпису, не має сенсу, якщо цілью впровадження являється охорона доступу до певного приміщення чи комп’ютерної системи. Але в організаціях, в процесі функціонування яких завжди проходить документообіг з великою кількістю конфіденційної інформації (скажемо, банківська сфера), подібна

методика перевірки достовірності людини може бути відмінним вибором через зручність використання та відносну простоту впровадження [1].

Висновки до другого розділу

На даний час є безліч систем біометричної ідентифікації людини, які працюють по-різному і мають різний ціновий діапазон і ефективність (стійкість до взлому). Це все залежить від типу використання біометричних даних. Біометричні системи доступу можуть використовувати біометричні дані таких типів: відбитки пальців, зовнішність людини, геометрія руки, геометрична карта судин долоні, термограма особи, райдужна оболонка ока, сітківка ока, голос та мова, підпис. Кожна біометрична система може використовувати як один певний тип, так і декілька типів біометричних даних.

Особливу увагу було виділено біометричному методу ідентифікації на основі відбитків пальців, так як даний метод являється домінуючим на корпоративному ринку.

РОЗДІЛ 3. СТВОРЕННЯ СИСТЕМИ ДОСТУПУ НА ОБ'ЄКТ (БАНКІВСЬКИЙ ПІДРОЗДІЛ ОБСЛУГОВУВАННЯ КЛІЄНТІВ) З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ ЗАСОБІВ ІДЕНТИФІКАЦІЇ

3.1. Технічне завдання

Відповідно до ГОСТ 34.602- 89 технічне завдання на автомитазовані системи (АС) виглядає наступним чином:

1. Загальні відомості

- повне найменування системи та її умовне позначення – «Біометрична система контролю доступу до об'єкту» / БСКД;

- найменування розробника/замовника системи – Банківський підрозділ обслуговування VIP клієнтів;

2. Причини і мета створення (розвитку) системи

- перелік об'єктів, на яких передбачається використовування системи –, кабінет директора, кабінет зам. директора, зал засідань, кабінет адміністратора, приміщення камер схову, вхід до касових кабінок;

Метою створення системи є: посилення захищенності системи контролю доступу, покращення швидкості процесу надання доступу, відмова у доступі до контрольованої зони неуповноваженим індивідам.

3. Вимоги до системи

- перелік підсистем – Система має мати у своєму складі наступні підсистеми: система управління автоматизованих приладів (замки, турнікети), система обробки характеристик, знятих за допомогою біометричних датчиків;

- вимоги до структури – забезпечення рівня захищеності згідно з НД ТЗІ 2.5-005 -99, що відповідає класу 1;

- вимоги до персоналу: чисельність – 14 чоловік;

- режим роботи: початок – 08:00 год/ кінець – 20:00 год;

Що стосується стандартних функціональних профілів захищеності то згідно з НД ТЗІ 2.5-005 -99 система відноситься до п.7.1.7 (Стандартні

функціональні профілі захищеності в комп'ютерних системах (КС), що входять до складу АС класу 1, з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблюваної інформації), а саме має відповідати пункту 1-КЦ. 1 = { НР-1, НИ-1, НК-1, НО-1,НУ-1, НТ-1 }, де:

НР-1 реєстрація;

НИ-1 ідентифікація і автентифікація;

НК-1 достовірний канал;

НЦ-1 цілісність;

НТ-1 самотестування.

3.2. Вибір технічної реалізації системи

Проаналізувавши найефективніші технології контролю доступу до об'єкта та спираючись на специфіку контрольованої зони та поставлених цілей, було вирішено застосовувати наступний тип системи:

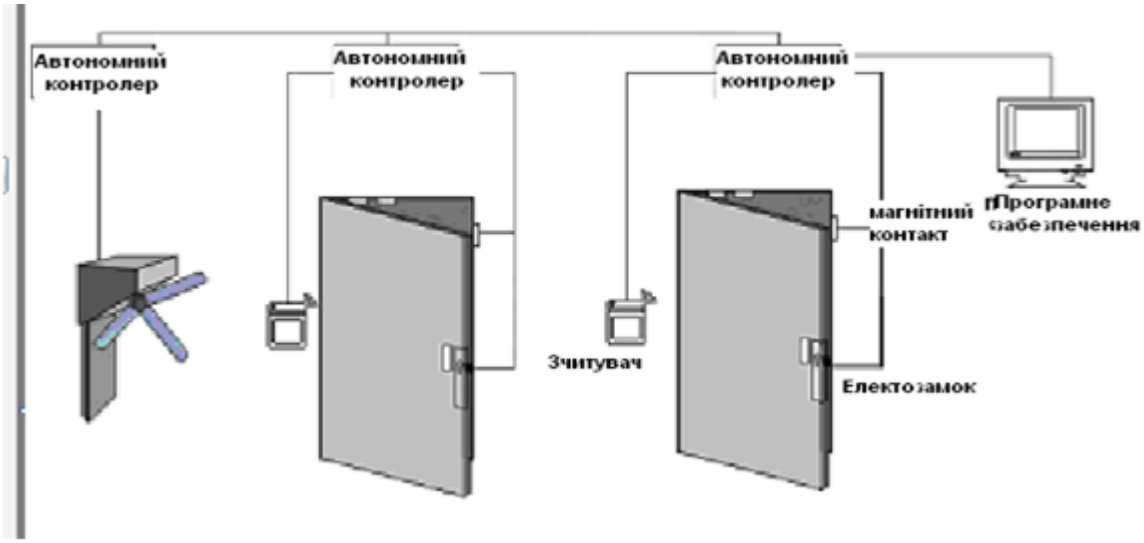

Рис. 3.1 Схема обраної реалізації системи

Введені прилади біометричного захисту:

Сканер, вбудований в клавіатуру.

Сканер відбитків пальців, вбудований у стандартну клавіатуру, усуває потребу працівника запам’ятовувати складні паролі та надає більш ефективний та зручний метод верифікації. Завдяки впровадження такого приладу особа має можливість комфортно увійти в систему за допомогою будь-якого комп’ютера не витрачаючи зайвий час.

Сканер в замку.

На відміну від стандартних ключів та не зовсім зручних для працівників кодових замків використовується сканер відбитків. Застосування таких пристроїв являється більш надійним способом контролю доступу до приміщень; до того ж процес надання доступу займає значно менше часу.

Турнікет.

Турнікети з біометричним сканером набагато ефективніші ніж інші типи, що функціонують на основі смарт-карток.

Логічна схема приладів контролю доступу, які будуть застосовуватися в системі:

Рис. 3.2 Логічна схема обраних приладів контролю доступу

3.3. Опис наявної системи захисту

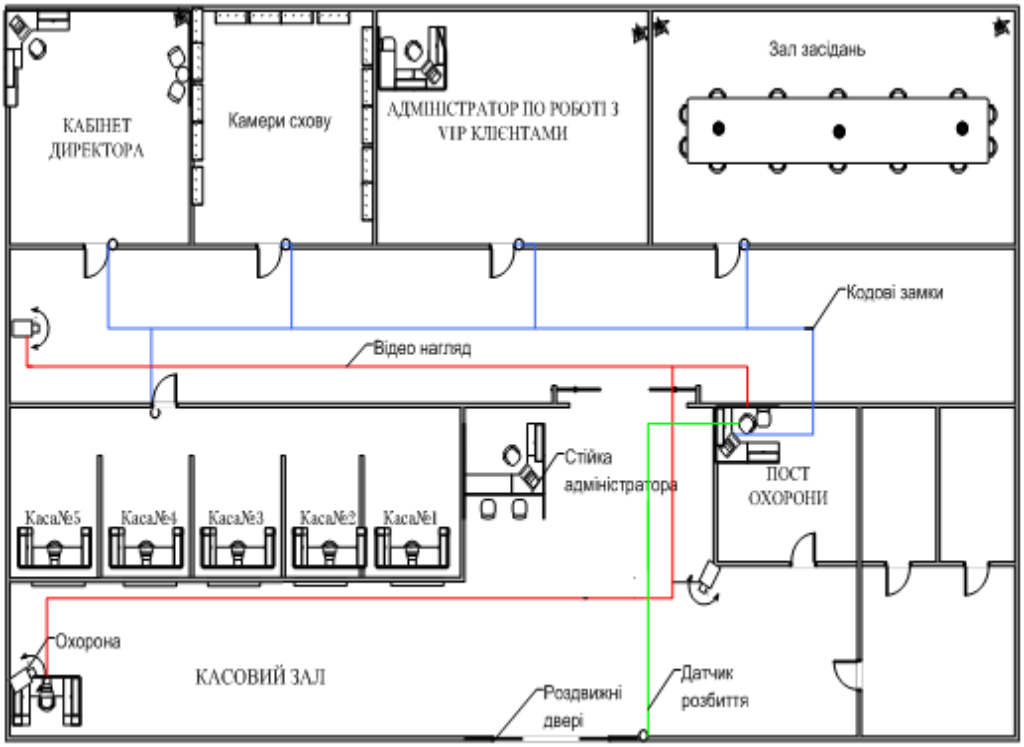

Рис. 3.3 Наявна схема захисту

Об’єкт являє собою банківську філію для роботи з VIP та звичайними клієнтами, тому застосування специфічних засобів контролю доступу до касового залу не є необхідним. Достатньо забезпечити дану зону камерами відеоспостереження та охоронцями. Друга частина будівлі теж обмежується відеокамерами, а вхід до кабінетів - кодовими замками. Для надання доступу охорона проводить перевірку документів, після чого особа отримує картку доступу, що діє протягом якогось часу. Такий метод не є ефективним через зайвий час, що витрачається на ідентифікацію людини та на відкриття кодових замків. До того ж, система з карткою доступу не цілком безпечна через можливість викрадення картки для отримання несанкціонованого доступу. Також потрібно регулярно змінювати коди доступу. Сучасні засоби контролю доступу надають набагато більше можливостей та підвищують надійність системи в декілька раз. Отже, задача підвищити надійність системи без великих змін в політиці компанії.

3.4. Проект системи контролю доступу на об’єкт з використанням методів біометричної ідентифікації

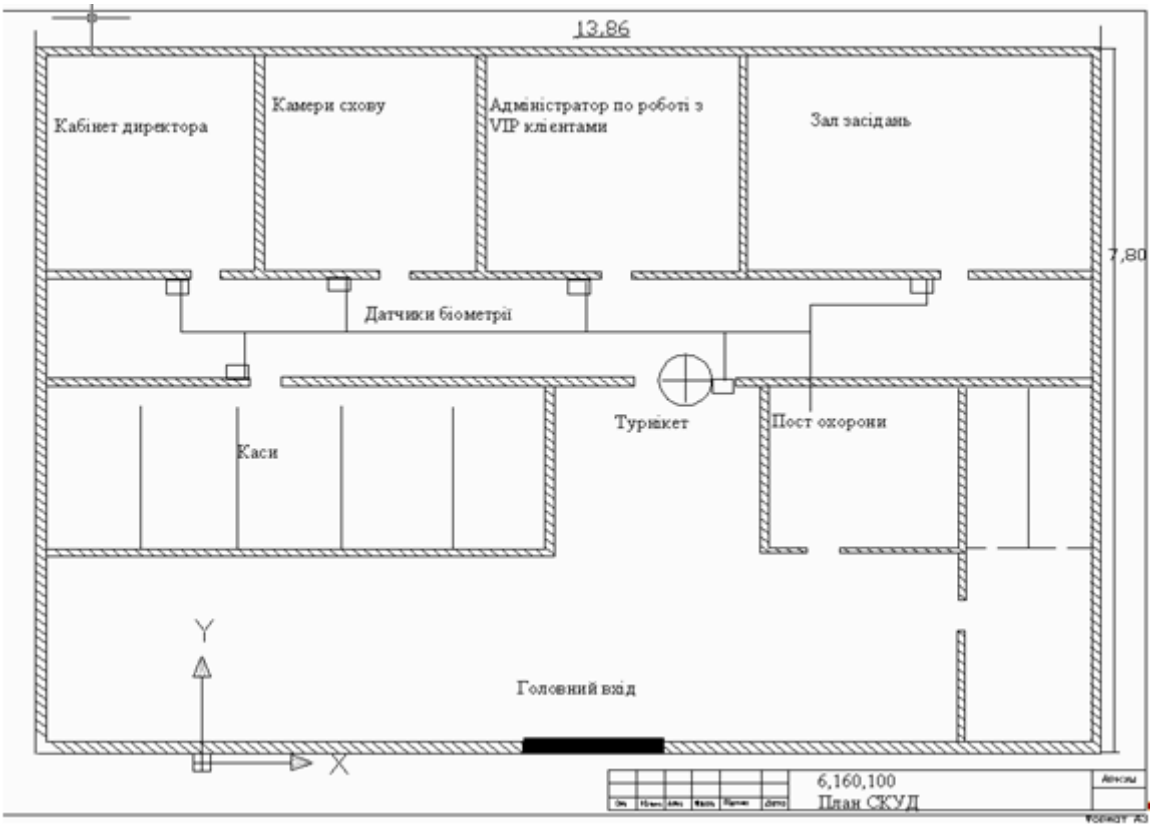

Рис. 3.4 Пропонована схема доступу на об’єкт

Як бачимо з малюнку, принципово система не відрізняється, ми тільки заміняємо її складові. Тепер щоб потрапити до другої частини приміщення клієнт повинен пройти біометричну ідентифікацію.

Після заміни системи клієнти повинні один раз при першому відвідуванні зареєструватися в системі. Для цього на посту охорони є спеціальний зчитувач відбитків, через який дані клієнта вносяться до системи. Далі все просто: клієнт підходить до турнікету, притуляє палець і через 1,5 секунди (якщо в нього є права доступу) він може проходити далі.

3.5. Необхідні адміністративні зміни при впровадженні біометричної системи доступу

Впровадження системи доступу потребує внесення змін в існуючий режим роботи. Можливо, необхідно внести зміни в штатний розклад: ввести нові посадові одиниці або скоротити деякі посади, змінити обов'язки робітників.

Перераховані нижче рекомендації дозволять значно спростити рішення адміністративних питань, пов'язаних з підготовкою до впровадження системи контролю та управління доступом (СКУД).

- Заключення нового договору зі службою охорони:

Потрібно узгодити з охороною питання підключення нової системи до вже існуючої або її повна заміна.

- Зміни штатного розкладу:

При впровадженні системи контролю доступу зміни штатного розкладу непотрібні, так як в штатному розкладі передбачена посада адміністратора офісу компанії, відповідального за порядок в залі кас та відкриття/закриття приміщення. Так як режим роботи підприємства 6 днів на тиждень по 10 годин, то режим роботи адміністратора перевищує 8 годин на добу. Тому передбачається, що дві людини будуть виконувати обов'язки адміністратора позмінною

В зв'язку з впровадженням системи необхідно додати ряд нових обов'язків в посадову інструкцію адміністратора офісу та зняти з нього обов'язки, які він неповинен буде виконувати.

- Зміна посадових обов'язків.

Обов'язки що необхідно додати в посадову інструкцію адміністратора офісу:

- Ведення електронної бази даних системи контролю доступу, введення даних про прийнятих та звільнених співробітниках;
- Надання та обмеження прав доступу в різні приміщення;
- Перевірка стану датчиків зняття відбитків пальців;

- Фіксація всіх подій в спеціальному журналі або комп’ютері;
- Передача/зняття приміщення з охорони;
- Повідомлення про правила доступу працівників та клієнтів.

Обов’язки що повинні бути зняті з адміністратора:

- Ведення картотеки співробітників на спеціальних бланках;
- Щоденна видача ключів;
- Обхід всіх приміщень компанії;
- Організація заміни замка при втраті ключа.

Висновки до третього розділу

Розглянувши використання та методи різних біометричних систем ідентифікації та зробивши аналіз їх переваг та недоліків, а також дослідивши існуючі на підприємстві методи захисту доступу об’єкта, були прийняті рішення щодо удосконалення охоронної системи банку. Було використано біометричну систему доступу до об’єкту, що використовує метод ідентифікації за відбитками пальців, що надає на порядок вищий ступінь захисту на відміну від вже застосованого. Також біометрична система ідентифікації за відбитками пальців є більш дешевою на фоні різних проаналізованих біометричних системам ідентифікації.

ВИСНОВКИ

Основною цілью впровадження біометричних технологій у системи контролю доступу є покращення ефективності розпізнавання особи шляхом автоматизації процесу верифікації/ідентифікації. Базові вимоги що висуваються до таких систем – відсутність можливості надання несанкціонованого доступу неуповноваженій особі та мінімальна вірогідність похибок перевірки користувачів, за яких відбувається помилкова відмова у доступі уповноваженим особам. Відносно застарілих систем надання доступу, методи яких оперують паролями та картками, біометричні технології пропонують значно більший степінь захисту.

У дипломній роботі були розглянуті та вирішені такі задачі:

1) Розглянуто основні типи біометричних систем.

Біометричні системи за базовими параметрами, які застосовуються в процесі розпізнавання особи, діляться на дві групи - фізіологічні та психологічні (поведінкові). Перша група досліджує наступні унікальні характеристики людини: риси обличчя, структура ока, особливості відбитків пальців і т.п. Параметри, які аналізує друга група біометричних технологій - голос людини, специфіка підпису, особливості введення тексту з клавіатури та інші.

2) Розглянуто використання та роботу біометричних систем ідентифікації. Виконано аналіз їх переваг та недоліків.

На даний час є безліч біометричних систем, які працюють по-різному і мають різну стійкість до взлому. Біометричні системи доступу можуть використовувати біометричні дані таких типів: відбитки пальців, геометрія особи, геометрія руки, геометрична карта судин долоні, термограма особи, райдужна оболонка ока, сітківка ока, голос і мова, підпис. Біометричні системи можуть використовувати як один певний тип біометричних даних, так і складатися із декількох типів біометричних даних. Кожна біометрична система в залежності від методу, на якому базується її функціонування, має як свої

переваги, так і недоліки. Ознайомившись із основними методами біометричної ідентифікації та їх характеристиками, такими як швидкість процесу ідентифікації, зручність даної процедури з точки зору користувача, вірогідність помилок першого та другого роду, коштовність необхідного обладнання, було проведено аналіз кожної з біометричних систем, внаслідок чого виконана робота, описана в наступному пункті.

3) Обрано одну з біометричних систем для побудови системи контролю доступу до об'єкта.

Дослідивши існуючі методи захисту обраного об’єкта (приміщень банку), було прийнято рішення щодо удосконалення охоронної системи. Для цього було вирішено замінити дійсні засоби контролю доступу на біометричну систему ідентифікації за відбитками пальців, що надає на порядок вищий ступінь захисту на відміну від вже застосованого. Біометрична система ідентифікації за відбитками пальців є більш дешевою в порівнянні з іншими біометричними системами ідентифікації, а також більш зручною в користуванні. До того ж, були описані деякі адміністративні зміни в політиці підприємства при впровадженні біометричної системи доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Книги

1. Синіцин І. М., Ушмаєв О. С. Метрологічні і біометричні технології та системи, 2008.

2. Ушмаєв О.С., Босов А.В. Реалізація концепції багатофакторної ідентифікації в інтегрованих аналітичних системах, 2007.

3. Ушмаєв О.С. Реалізація біометричної системи в правоохоронних системах, 2007.

4. Домарев В.В. Захист інформації та безпека комп'ютерних систем. 2007.

5. Б. Н. Локотош, А. В. Колесников. Теорія інформації , 2002.

6. Біячуєв Т. А. Безпека корпоративних мереж, 2004.

7. Алексеєнко В. Н. Система захисту комерційних об'єктів / В. Н. Алексеєнко, Б. В. Сокольський., 1992.

Електронні ресурси

8. Задорожній В. В. Ідентифікація за відбитками пальців. Частина 1 [Електронний ресурс] / В. В. Задорожній – Режим доступу до ресурсу: http://www.bre.ru/security;

9. International biometrics and idenity association [Електронний ресурс] – Режим доступу до ресурсу: www.ibia.org.;

10. Biolink біометричні системи [Електронний ресурс] – Режим доступу до ресурсу: www.biolink.ru.;

11. Biometric terminals add security to a variety of processes [Електронний ресурс] – Режим доступу до ресурсу: www.bioscrypt.com;.

12. From identity and secure access to biometric identity [Електронний ресурс] – Режим доступу до ресурсу: www.crossmatch.com;

13. Everywhere Identity Matters [Електронний ресурс] – Режим доступу до ресурсу: www.identix.com;