Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Кучугурної Валерії Андріївни*

академічної групи *125м-19-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Захист біомеричних персональних даних у корпоративних системах відеос-постереження*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.- м.н. Кагадій Т.С.			
розділів:				
спеціальний	ас. Мілінчук Ю.А.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту академічної групи ***Кучугурної В.А.*** ***125м-19-2***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації _____

за освітньо-професійною програмою ***Кібербезпека***

_____

на тему ***Захист біомеричних персональних даних у корпоративних системах відеоспостереження***

_____

Затверджену наказом ректора НТУ «Дніпровська політехніка» від_____№ _____

Розділ	**Зміст**	**Термін виконання**
Розділ 1	Аналіз систем обробки біометричних персональних даних	01.09.20-01.10.20
Розділ 2	Аналіз проблем у системах захисту біометричних персональних даних	02.10.20-31.10.20
Розділ 3	Розробка заходів безпеки	01.11.20-14.11.20
Розділ 4	Економічний розділ	15.11.20-30.11.20
Висновок	Висновок	01.12.20-05.12.20

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: 01.09.20р.

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 101 с., 24 рис., 10 табл., 4 додатки, 25 джерел.

Об'єкт дослідження: Біометричні персональні дані.

Предмет дослідження: методи та засоби захисту біометричних персональних даних

Мета роботи: підвищення рівня захисту біометричних персональних даних у корпоративних системах відеоспостереження.

Методи розробки: спостереження, порівняння, аналіз, опис.

У першому розділі було проаналізовано види систем обробки біометричних персональних даних, основні області застосування біометричних методів ідентифікації та аутентифікації, нормативно-правова база у сфері захисту біометричних даних.

У другому розділі проаналізовано проблеми у системах захисту біометричних персональних даних, проведено аналіз методів та засобів протидії.

У спеціальному розділі проаналізовані можливі атаки на систему відеоспостереження, проаналізовані методи та засоби протиді даним атакам, розроблені рекомендації для безпечної передачі даних у системах захисту біометричних персональних даних.

В економічному розділі були розраховані витрати на реалізацію методик, щодо безпечного зберігання та передачі інформації у системах захисту біометричних персональних даних.

Практичне значення роботи полягає у підвищенні ефективності процесу захисту біометричних персональних даних, за рахунок розробки рекомендацій для безпечного користування системою відеоспостереження.

ІНФОРМАЦІЙНА БЕЗПЕКА, БІОМЕТРИЧНІ ПЕРСОНАЛЬНІ ДАНІ, КІБЕРБЕЗПЕКА, АУТЕНТФІКАЦІЯ

РЕФЕРАТ

Пояснительная записка: 101 с., 24 рис., 10 табл., 4 додатка, 25 источников.

Объект исследования: Биометрические персональные данные.

Предмет исследования: методы и средства защиты биометрических персо-нальных данных

Цель работы: повышение уровня защиты биометрических персональных данных в корпоративных системах видеонаблюдения.

Методы разработки: наблюдение, сравнение, анализ, описание.

В первом разделе были проанализированы виды систем обработки биометрических персональных данных, основные области применения биометрических методов идентификации и аутентификации, нормативно-правовая база в сфере защиты биометрических данных.

Во втором разделе проанализированы проблемы в системах защиты биометрических персональных данных, проведен анализ методов и средств противодействия.

В специальном разделе проанализированы возможные атаки на систему видеонаблюдения, проанализированы методы и средства противодействия данным атакам, разработаны рекомендации для безопасной передачи данных в системах защиты биометрических персональных данных.

В экономическом разделе были рассчитаны затраты на реализацию методики, по безопасному хранению и передаче информации в системах защиты биометрических персональных данных.

Практическое значение работы состоит в повышении эффективности процесса защиты биометрических персональных данных, за счет разработки рекомендаций для безопасного пользования системой видеонаблюдения.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, БИОМЕТРИЧЕСКИЕ ЛИЧНЫЕ ДАННЫЕ, КИБЕРБЕЗОПАСНОСТЬ, АУТЕНТФИКАЦИЯ

ABSTRACT

Explanatory note: 101 p., 24 pic., 10 tab., 4 annexes, 25 sources.

Research object: Biometric personal data.

Subject of research: methods and means of protecting biometric personal data.

Purpose: to increase the level of protection of biometric personal data in corporate video surveillance systems.

Development methods: observation, comparison, analysis, description.

The first section analyzed the types of biometric personal data processing systems, the main areas of application of biometric methods of identification and authentication, the regulatory framework in the field of biometric data protection.

The second section analyzes the problems in the protection systems of biometric personal data, analyzes the methods and means of counteraction.

In a special section, possible attacks on the video surveillance system are analyzed, methods and means of counteracting these attacks are analyzed, and recommendations for secure data transmission in biometric personal data protection systems are developed.

In the economic section, the costs of implementing methods for secure storage and transmission of information in biometric personal data protection systems were calculated.

The practical significance of the work is to increase the efficiency of the process of protection of biometric personal data, by developing recomendations for the safe use of video surveillance.

INFORMATION SECURITY, BIOMETRIC PERSONAL DATA, CYBER SECURITY, AUTHENTICATION

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ПД - персональні дані;

СКУД - система контролю і управління доступом;

FAR – (англ. False Acceptance Rate) коефіцієнт помилкового пропуску;

FRR - (англ. False Rejection Rate) коефіцієнт помилкового відмови.

ISO/IEC – International Organization for Standardization/International Electrotechnical Commission;

НСД – несанкціонований доступ.

ЗМІСТ

ВСТУП

Застосування біометричних технологій досить різноманітне: доступ до робочих місць і мережевих ресурсів, захист інформації, забезпечення контролю доступу на територію об’єктів, встановлення установчих даних особи тощо.

Згідно з прогнозами багатьох експертів у галузі біометричних технологій, біометрія є одним із найдинамічніших сегментів світового ринку інформаційних технологій, що посилено розвиваються. У майбутньому біометричні технології відіграватимуть головну роль у питаннях персональної ідентифікації в багатьох сферах. Використовувані окремо або спільно зі смарт-картками, токенами, різними електронними ключами і підписами, біометрія надалі буде все більше застосовуватися у всіх сферах економіки й особистого життя.

Біометричні персональні дані представляють собою будь-яку інформацію, що відноситься прямо або побічно до певної фізичної особи (суб'єкту персональних даних). До біометричних персональних даних відносяться відомості, які характеризують фізіологічні та біологічні особливості людини, на підставі яких можна встановити його особистість і які використовуються оператором для встановлення особи суб'єкта персональних даних.

Найпоширеніша нині біометрична технологія – ідентифікація за відбитками пальців. Ця технологія продовжує домінувати на ринку, займаючи майже 50% від його обсягу. Вона ввібрала всі сучасні досягнення біометрії і за правом посідає позиції лідера. Другою за ступенем поширеності технологією є ідентифікація за обличчям (15–20% ринку). Вона активно застосовується в «електронних паспортах» та інших документах, які засвідчують особу людини і має тенденцію до невпинного збільшення. Третє місце (майже 7%) оспорюють технології ідентифікації за райдужною оболонкою ока і геометрії та розташування кров’яних судин

руки або пальця, хоча більшість експертів третє місце віддають технології райдужної оболонки ока.

За допомогою сучасних технологій і технологій майбутнього право на приватне життя буде порушено, якщо біометричні дані не будуть захищені.

Прогрес у галузі інформаційних технологій, зокрема у сфері розробки та впровадження програмного забезпечення, активність у формуванні баз персональних даних надзвичайно загострили проблему захисту приватного життя фізичних осіб та захисту інших основних прав і свобод людини.

Об'єкт дослідження: методи та засоби захисту біометричних персональних даних

Мета роботи: підвищення рівня захисту біометричних персона-льних даних у корпоративних системах відеоспостереження.

Предмет дослідження – біометричні персональні дані.

Структура роботи. Магістерська дипломна робота складається зі вступу, чотирьох розділів, висновку, списку використаних джерел.

Практичне значення роботи полягає у підвищенні ефективності процесу захисту біометричних персональних даних, за рахунок розробки рекомендацій для безпечного користування системою відеоспостереження.

РОЗДІЛ 1. АНАЛІЗ СИСТЕМ ОБРОБКИ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ

1.1 Основні області застосування біометричних методів ідентифікації та аутентифікації

Актуальність розвитку біометричних технологій ідентифікації особи обумовлена збільшенням числа об'єктів і потоків інформації, які необхідно захищати від несанкціонованого доступу, а саме: криміналістика; системи контролю доступу; системи ідентифікації особи; системи електронної комерції; інформаційна безпека (доступ в мережу, вхід на ПК); облік робочого часу і реєстрація відвідувачів; системи голосування; проведення електронних платежів; аутентифікація на web-ресурсах; різні соціальні проекти, де потрібна ідентифікація людей; проекти цивільної ідентифікації (пересічення державних кордонів, видача віз на відвідини країни) і т.д. Електронний бізнес і впровадження технології «електронного уряду» можливе тільки після запровадження і виконання певних процедур для ідентифікації особи. Біометричні технології застосовуються в паспортно-візових документах нового покоління, охороні правопорядку, в галузі безпеки банківських транзакцій, інвестування й інших фінансових переміщень, роздрібній торгівлі, питаннях охорони здоров'я, а також у сферах соціальних послуг і особистого життя.

Для технологій біометричної аутентифікації у державному та приватному секторах широко використовують наступні види. Це відбитки пальців, геометрія рук / пальців, розпізнавання обличчя, розпізнавання голосу, сканування райдужної оболонки, сканування сітківки ока, динамічна перевірка підпису і динаміка натискання клавіш.

Для того, щоб розібратися з усіма методами та видами біометричної ідентифікації та аутентифікації, треба розглянути основні терміни:

Біометрія-це будь-яка стійка, відмітна, фізична характеристика або особиста риса людини, яка може використовуватися для ідентифікації або перевірки заявленої особистості цієї людини [3].

Авторизація - керування рівнями та засобами доступу до певного захищеного ресурсу, як у фізичному розумінні (доступ до кімнати готелю за карткою), так і в галузі цифрових технологій (наприклад, автоматизована система контролю доступу) та ресурсів системи залежно від ідентифікатора і пароля користувача або надання певних повноважень (особі, програмі) на виконання деяких дій у системі обробки даних. З позицій інформаційної безпеки авторизація є частиною процедури надання доступу для роботи в інформаційній системі, після ідентифікації і аутентифікації.

Біометрична ідентифікація - здійснення пошуку за принципом "один до багатьох" шляхом розпізнавання і зіставлення одного або двох біометричних даних (параметрів) особи з біометричними даними (параметрами) осіб у відомчих інформаційних системах суб'єктів національної системи.

Аутентифікація - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. З позицій інформаційної безпеки аутентифікація є частиною процедури надання доступу для роботи в інформаційній системі, наступною після ідентифікації і передує авторизації.

Двофакторна аутентифікація-це метод ідентифікації користувача за допомогою запиту аутентифікаційних даних двох різних типів, що забезпечує двошарові, а значить, більш ефективний захист даних від несанкціонованого доступу.

Біометрична аутентифікація, наприклад, за допомогою Face ID, вважається лише одним етапом двофакторної аутентифікації, а в якості другої повинен використовуватися пароль, токен або окремий пристрій на зразок кардрідера.

Біометричні системи включають в себе 3 основних елементи:

1. Реєстрація;
2. Шаблон;
3. Зіставлення.

Реєстрація - це процес збору біометричних зразків у людини і подальшого створення шаблону. Як правило, пристрій приймає три зразки однієї і тієї ж біометрії і потім усереднює їх для створення шаблону реєстрації.

Шаблони - це дані, що представляють біометричні дані людини. Вони створюються біометричним пристроєм, який використовує запатентований алгоритм для вилучення ознак, що підходять для цієї технології.

Зіставлення - це процес порівняння представлених біометричних даних з одним (перевірка) або декількома (ідентифікація) шаблонами в базі даних системи.

Система контролю і управління доступом (скорочено СКУД або СКД) — це комплекс технічних та програмних засобів безпеки, що здійснює регулювання входу / виходу та переміщень людей чи транспортних об'єктів на територіях, які знаходяться під охороною, для адміністративного моніторингу та попереджень несанкціонованого проникнення.

СКУД зручні для користувачів тим, що носії інформації знаходяться завжди при них, не можуть бути загублені або вкрадені. Біометричний контроль доступу вважається більш надійним, тому що ідентифікатори не можуть бути передані третім особам, скопійовані.

Критерії біометричної ідентифікації

Для визначення ефективності СКУД на основі біометричної ідентифікації використовують наступні показники:

FAR - коефіцієнт помилкового пропуску;

FMR - ймовірність, що система невірно порівнює вхідний зразок з невідповідним шаблоном в базі даних;

FRR - коефіцієнт помилкового відмови;

FNMR - ймовірність того, що система помилиться у визначенні збігів між вхідним зразком і відповідним шаблоном з бази даних;

Графік ROC - візуалізація компромісу між характеристиками FAR і FRR;

Коефіцієнт відмови в реєстрації (FTE або FER) - коефіцієнт безуспішних спроб створити шаблон з вхідних даних (при низьку якість останніх);

Коефіцієнт помилкового утримання (FTC) - ймовірність того, що автоматизована система не здатна визначити біометричні вхідні дані, коли вони представлені коректно;

Ємність шаблону - максимальна кількість наборів даних, які можуть зберігатися в системі.

False Reject Rate - FRR (Рівень помилкових відмов) - ймовірність того, що система не ідентифікує зареєстрованого користувача або не підтверджує його справжності.

Як розраховується FRR:

Нехай Nt - кількість еталонів зображень в базі даних. FR - кількість помилкових нерозпізнавань (False Reject - Іванов, що не розпізнано як Іванов).

$$\mathrm{FRR} = \frac{\mathrm{FR}}{N_t} \times 100\ \%; \tag{1.1}$$

False Acceptance Rate - FAR (Рівень помилкових підтверджень) - ймовірність того, що система розпізнавання осіб помилково ідентифікує незареєстрованого користувача або підтверджує його справжність.

Як розраховується FAR:

Нехай Nt - кількість еталонів зображень в базі даних. FA - кількість помилкових распознаваний (False Acceptation - Іванов розпізнано як Петров).

$$\mathrm{FAR} = \frac{\mathrm{FA}}{N_t} \times 100\ \%. \tag{1.2}$$

Перше і найважливіше, що потрібно знати про ці два показники, це те, що вони не абсолютні, а відносні, тобто вони можуть змінюватися в залежності від налаштувань алгоритму розпізнавання осіб.

Друге - це те, що ці показники взаємопов'язані - чим менше FAR тим більше FRR.

Імовірність допуску особи, яка не має права доступу (False Acceptance Rate - FAR), це найбільш небажаний результат, який повинен бути мінімізованим;

Імовірність відмови особі, яка має право доступу (False Rejection Rate - FRR), такий помилковий результат можна виправити.

Ці характеристики взаємопов'язані – чим менше одна, тим більше друга. Точка, у якій ці дві помилки рівні, називається EER (Equal Error Rates). Чим менша величина EER, тим вище безпомилковість системи доступу.

1.2. Нормативно-правова база захисту біометричних даних

Історія формування законодавчої бази захисту біометричних персональних даних бере свій початок з 1948 р., коли в Загальній декларації прав людини було проголошено, що ніхто не може піддаватися свавільному втручанню в особисте та сімейне життя, що кожна людина має право на захист закону від такого втручання. Європейська Конвенція про захист прав і основних свобод людини від 4 листопада 1950 р. конкретизувала це право проголосивши, що кожна людина має право на свободу дотримуватися своєї думки, отримувати й поширювати інформацію та ідеї без втручання з боку державних органів і незалежно від державних кордонів.

Міжнародним пактом про громадянські та політичні права від 16 грудня 1966 р. забороняється не лише свавільне, а й незаконне втручання в особисте та сімейне життя людини Актуальність більш детального регулювання цього права зросла у зв'язку з інтенсивним розвитком комп'ютерних

технологій та обробкою персональної інформації в автоматизованих інформаційних системах. У рамках діяльності міжнародних організацій було прийнято низку міжнародних документів, що регулюють право на захист персональної інформації. У середині 1970-х рр. стало зрозумілим, що національні системи правового захисту даних, з причин наявних особливостей національного менталітету і розходжень законодавчих систем (як за формою, так і за змістом), не можуть забезпечити принцип екстериторіальності персональних даних. Це стримувало вирішення багатьох питань розвитку міжнародного співробітництва. Саме тому потреба в створенні міжнародної системи правового регулювання обробки і передавання даних ставала все більш нагальною.

Для розв'язання проблеми в 1978 р. в Організації з економічного співробітництва і розвитку була заснована експертна група із завданням розробити комплекс базових принципів захисту приватного життя та індивідуальних свобод у зв'язку з обробкою персональних даних і в зв'язку з транскордонними потоками даних. Ці принципи мали б слугувати підґрунтям для гармонізації відповідних національних законів. Розробка таких принципів і досягнення консенсусу держав – членів ОЕСР виявилося непростим завданням, оскільки досить неоднорідний її склад визначив не менш неоднорідний перелік національних підходів до правового захисту персональних даних. Так, наприклад, деякі національні закони захищали дані стосовно тільки фізичних осіб. Інші країни вважали необхідним захищати як юридичних осіб, так і фізичних. Треті країни дотримувалися захисту персональних даних, які обробляються тільки автоматично, водночас як інші поширювали його також на ручні й друковані дані.

Серед держав – членів ОЕСР були прихильники всіх трьох можливих підходів до побудови системи правового захисту персональних даних: генерального, секторного (галузевого) і змішаного. За підсумками дворічної роботи експертної групи, включаючи процес узгодження принципів із усіма державами-членами, Рада ОЕСР прийняла настанови «Про базові принципи

захисту недоторканності приватного життя і транскордонних потоків персональних даних».

Вони складаються з п'яти частин:

Перша частина містить дефініції і визначає сферу дії базових принципів;

Друга – встановлює вісім базових принципів захисту «прайвеси» у зв'язку з обробкою персональних даних на національному рівні;

Третя – присвячена принципам міжнародного застосування, тобто взаємодії між державами – членами ОЕСР;

Четверта – визначає заходи для здійснення на практиці вищезгаданих принципів і, зокрема, встановлює, що вони мають застосовуватися в «недискримінаційній манері»;

П'ята – присвячена організації співробітництва держав – членів ОЕСР (за допомогою обміну інформації і запобігання несумісним національним процедурам для захисту персональних даних).

Положення базових принципів розроблені з метою:

а) Досягнення державами – членами ОЕСР мінімальних стандартів захисту «прайвеси» у зв'язку з обробкою персональних даних;

б) Зменшення нормативно-правових розходжень між відповідними нормами національного законодавства різних країн;

в) Гарантії того, що в процесі захисту персональних даних на національному рівні будуть братися до уваги інтереси інших країн, зокрема не допускатися неналежне втручання під час передавання персональних даних між країнами;

г) Усунення причин, що могли б спонукати країни обмежити або заборонити транскордонні потоки персональних даних через можливі ризики, асоційовані з такими потоками.

До основних принципів захисту недоторканності приватного життя і міжнародного обміну персональними даними Рада ОЕСР відносить:

1. Обмеження обсягу персональних даних, що збираються;

2. Якість персональних даних;

3. Конкретизацію цілей збору персональних даних;

4. Обмеження на використання персональних даних;

5. Забезпечення безпеки персональних даних;

6. Відкритість політики і практики щодо персональних даних;

7. Індивідуальну участь (права індивідуума на свої персональні дані);

8. Відповідальність (обов'язок розпорядника персональних даних).

9. Дотримання принципів на національному рівні передбачає такі обов'язки для держав – членів ОЕСР, якими передбачено:

10. Прийняти належні національні закони;

11. Заохочувати і підтримувати саморегулювання шляхом прийняття кодексів поведінки/поводження або інших правил;

12. Забезпечити наявність розумних механізмів реалізації індивідуальних прав;

13. Застосувати необхідні санкції та інші засоби захисту персональних даних на випадок невиконання заходів, що передбачені зазначеними принципами;

14. Забезпечити недискримінаційне ставлення до суб'єктів даних.

Комітетом Ради Європи з питань захисту даних були сформульовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення персональних даних. Ці принципи 28 січня 1981 р. отримали закріплення в першій і єдиній на сьогодні міжнародній угоді – Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (відома як Конвенція № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 р. та Додатковий протокол до Конвенції № 108 від 8 листопада 2001 р. згідно з порядком у серії Європейських договорів). З того часу захист персональних даних виокремився в самостійний вид діяльності.

Згідно з Конвенцією № 108 Ради Європи держави, які підписали цей документ, зобов'язуються керуватися її положеннями під час розгляду питань, пов'язаних із захистом персональних даних, що підлягають чи не підлягають автоматизованій обробці, як у суспільному, так і приватному секторах. Держава – член Конвенції № 108 Ради Європи має право визначати види персональних даних, які підлягають захисту (ст. 3 Конвенції).

Кожна держава – член Конвенції № 108 Ради Європи коригує національне законодавство втілення її основних принципів та поставленої мети забезпечення на території держави-члена поваги основних свобод кожної особи незалежно від її громадянства або місця проживання (ст. 4).

До захисту персональних даних висуваються певні вимоги, про що йдеться нижче.

Отримання та обробка персональних даних мають здійснюватися законним шляхом.

Персональні дані мають зберігатися та використовуватися у визначених та законних цілях, бути точними та поновлюваними, допускати ідентифікацію фізичної особи.

Персональні дані, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, не можуть піддаватися автоматизованій обробці, якщо внутрішнє законодавство країни не забезпечує відповідних гарантій. Це правило застосовується також до персональних даних, що стосуються засудження в кримінальному порядку. Засоби та заходи, що застосовують до таких даних, мають передбачати безпеку персональних даних від випадкового та несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження та випадкової втрати (ст. 5–7).

Конвенція № 108 Ради Європи передбачає дуже важливий момент, згідно з яким збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, дані про яку обробляються. Цій особі надано право знати місце роботи та проживання розпорядника

бази персональних даних (відповідального за обробку даних), а також право отримувати відповідні дані без затримки та в зрозумілій формі.

Транскордонні потоки даних мають здійснюватися за умов забезпечення захисту персональних даних.

Допускається обмеження цієї вимоги у разі, коли національне законодавство передбачає особливий порядок упорядкування суспільних інформаційних відносин та визначення окремих видів персональних даних у зв'язку із специфічністю деяких відомостей, крім випадків, коли законодавство іншої держави-члена має аналогічний ступінь захисту (ст. 12).

Щодо забезпечення транскордонних потоків даних Протокол відзначає, що кожна держава-член може дозволити передавання персональних даних:

а) Якщо національне законодавство забезпечує це в зв'язку:

– зі специфічними інтересами суб'єкта даних;

– з необхідністю врахування законних суспільних інтересів;

б) Якщо гарантії, що, зокрема, можуть випливати з договірних зобов'язань, надаються відповідальною за передавання особою і визнаються достатніми компетентним органом нагляду за захистом персональних даних.

27 квітня 2016 р. рішенням Європейського парламенту і Ради був прийнятий новий закон Про захист персональних даних - загальний/Генеральний регламент щодо захисту персональних даних (GDPR-General Data Protection Regulation, далі по тексту-Регламент GDPR). По суті він являє собою два документи: Регламент (EU) 2016/679 Європейського парламенту і Ради «Про захист фізичних осіб щодо обробки персональних даних і про вільне переміщення таких даних і скасування Директиви 95/46 / ЕС (загальні правила захисту даних)» і Директиву (EU) 2016/680 Європейського парламенту і Ради «Про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування кримінальних злочинів, ведення розшукових або судових дій або вико-

нання кримінальних покарань, а також за вільне переміщення таких даних і скасовуючи рамкове рішення Ради 2008/977 / JHA».

Якщо перший документ-регламент, який є документом прямої дії, тобто він стає законом з моменту його прийняття; то другий документ – директива, також. Будучи обов'язковим документом, починає діяти з моменту, коли вона стає частиною національного законодавства. При виникненні конфліктних ситуацій суди в державах-членах ЄС керуються положеннями регламентів, як мають більшу юридичну силу, ніж національні закони (у разі конфлікту регламент скасовує дію національного закону). Директиви за загальним правилом повинні містити вказівки на період часу, протягом якого вони повинні бути затверджені в якості національного законодавства держав-членів.

Регламент GDPR набув чинності 25 травня 2018 р. у всіх державах - членах Європейського Союзу [5].

З прийняттям регламенту GDPR втратила чинність Директива 95/46 / ЄС «Про захист фізичних осіб стосовно обробки персональних даних і вільний рух таких даних» (далі по тексту - Директива 95/46/ЄС)2, однак головний принцип, який був закладений в даному документі, – гарантії прав фізичних осіб при дотриманні публічного інтересу; отримав закріплення і подальший розвиток в новому законі.

Директива 95/46/ЄС, що діяла раніше, була першим документом, в якому декларувалося прагнення до забезпечення вільного переміщення інформації між країнами - членами ЄС, з одного боку, і надання гарантій захисту основних прав громадян, в число яких входить право на недоторканність особистих даних і їх захист від третіх осіб, - з іншого.

Стаття 7 Директиви 95/46 / ЄС зобов'язувала всіх держав-учасниць забезпечити обробку особистих даних виключно у випадках, якщо суб'єкт недвозначно висловив на це свою згоду або така обробка необхідна для укладення/виконання контракту; виконання юридичного зобов'язання, суб'єктом якого є контролер або вона необхідна для захисту життєвих інтересів

суб'єкта даних. Також така обробка вважалася допустимою, якщо вона була необхідна з метою забезпечення законних інтересів контролера або третьої сторони (сторін), яким розкрито дані, крім випадків, коли такі інтереси перекриваються інтересами фундаментальних прав і свобод суб'єкта даних, захист яких вимагається згідно зі ст. 1 директиви, що передбачає, що:

1. Відповідно до цієї Директиви, держави-учасниці захищають фундаментальні права і свободи фізичних осіб, і, зокрема, їх право на недоторканність приватного життя стосовно обробки персональних даних.

2. Держави-учасники не будуть ні обмежувати, ні забороняти вільний потік персональних даних між державами-учасниками з причин, пов'язаних із захистом, що допускається в п.1

Крім цього в директиві 95/46 / ЄС вперше було дано визначення поняття «персональні дані» стосовно обробки персональних даних і їх вільного руху. У пункті а) ст. 2 було закріплено: «персональні дані» означають будь-яку інформацію, пов'язану з ідентифікованою або ідентифікованою фізичною особою («суб'єктом даних»); ідентифікованою особою є особа, яка може бути ідентифікована прямо або побічно, зокрема, за допомогою посилання на ідентифікаційний номер або на один або кілька факторів, специфічних для його фізичної, психологічної, ментальної, або соціальної ідентичності».

З точки зору європейських дослідників, на момент своєї появи і перших років дії директива могла розглядатися як унікальний юридичний інструмент. Ця унікальність полягала в підтримці здійснення права на недоторканність приватного життя і правил захисту персональних даних. Принципи, закладені в директиві, становили золотий стандарт або еталонну модель захисту персональних даних в Європі та за її межами. Однак, відзначаючи гнучкість закладених у Директиві підходів до регулювання процесів збору і використання персональних даних, дослідники акцентували увагу на тому, що з часом ефективність її дії стала підриватися складністю культурних і національних відмінностей, в яких вона повинна була діяти.

Захист біометричних даних в Європі і Великобританії

У травні минулого року в Європі і Великобританії набув чинності законодавчий акт General Data Protection Regulation (GDPR).

Ця постанова забезпечує основу для застосування заходів щодо захисту персональних біометричних даних на практиці: будь-яке вторгнення в приватне життя громадян, наприклад розслідування деталей особистого життя або ділових поїздок, тягне за собою суворі покарання.

Правила GDPR засновані на принципах свободи прав людини про надання будь-яких даних про себе. Наприклад, в акті на законодавчому рівні прописано право «бути забутим» і право на збір персональних даних тільки за згодою користувача

До персональних даних відноситься будь-яка інформація, по якій можна визначити людину прямо або побічно: ім'я, адреса, відомості про стан здоров'я, Логін, Електронна пошта, ip-адреса, релігійна приналежність, фінансовий стан, психічне здоров'я і багато іншого. Навіть підписка на e-mail розсилку підпадає під дію GDPR, оскільки компанія-власник сайту збирає персональні дані користувачів (e-mail адреси) для подальшої розсилки.

GDPR обов'язковий для виконання у всіх 28 країнах Європейського Союзу і компаніях, що займаються збором даних в Європі. Регламент стосується і російських компаній, які взаємодіють з іноземними громадянами і отримують доступ до їх персональних даних.

Захист біометричних даних в Україні

Місце Закону України «Про захист персональних даних» у системі національного законодавства визначається тим, що він є базовим Законом України у сфері захисту персональних даних фізичних осіб в Україні. Інші нормативно-правові акти мають бути приведені у відповідність з його положеннями.

Крім Закону України «Про захист персональних даних», більш ніж два десятки законів України регулюють суспільні відносини, що пов'язані із збиранням, зберіганням, використанням та поширенням інформації про

особу, однак всі вони не мають чіткого та скорельованого з європейським законодавством визначення персональних даних. Вітчизняним законодавством не повністю визначено режим збирання, зберігання, використання та поширення інформації про особу.

Законом України «Про захист персональних даних» установлено детальний порядок реєстрації баз даних..

Чинне законодавство України щодо захисту персональних даних потребує вдосконалення відповідно до положень міжнародних стандартів, за якими персональні дані мають [9]:

1. Бути отримані законним способом;
2. Оброблятися за згодою на це суб'єкта даних і в кількості мінімально необхідної для визначеної діяльності;
3. Бути точними й поновлюватися;
4. Використовуватися тільки в чітко визначених цілях;
5. Бути доступними для суб'єкта даних;
6. Бути захищеними від несанкціонованого доступу.

До базових принципів захисту персональних даних в Україні мають бути віднесені:

- Якість персональних даних, що включає законність їх збирання, обробки і поширення щодо надмірності, вірогідності та анонімності;
- Право суб'єкта персональних даних, що включає право бути повідомленим про місце та мету обробки і вірогідність даних (повідомлення, доступ, виправлення чи знищення), право згоди на обробку даних (право контролю), право судового захисту;
- Безпека, що передбачає вживання заходів захисту за видами персональних даних, адресну відповідальність, контроль доступу до засобів обробки даних, контроль використання носіїв (накопичувачів) даних, контроль вводу, користування і виводу (транспортування) даних, контроль обробки даних й організаційний контроль [9].

Відповідно до Закону України «Про захист персональних даних» завданнями національного законодавства є створення правової бази державного регулювання суспільних відносин людини, суспільства і держави за умов дієвого захисту громадянських прав у сфері персональних даних.

Згідно із законодавством більшості європейських держав персональні дані розділяються за критерієм «чутливості» на дані загального характеру (прізвище, ім'я, по батькові, дата і місце народження, громадянство, місце проживання) і «чутливі» (вразливі) персональні дані (дані про стан здоров'я (історія хвороби, діагнози, етнічна належність, ставлення до релігії, ідентифікаційні коди чи номери, відбитки пальців, записи голосу, фотографії, кредитна історія, дані про судимість тощо). Для чутливих персональних даних передбачений більш високий ступінь захисту. Так, забороняється збирання, зберігання, використання та передавання без згоди суб'єкта даних саме чутливих, а не всіх персональних даних.

У результаті цього розповсюдження всіх без винятку персональних даних, у тому числі навіть прізвища, ім'я, по батькові особи, може здійснюватися тільки за попередньою згодою цієї особи [14].

Отже, будь-яка база клієнтів, список телефонів бізнес-партнерів чи просто купка візиток підпадають під категорію бази персональних даних та потребують реєстрації.

Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особисто.

Також у нормативно-правовій базі України має місце Постанова КМ "Про затвердження Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства". Це положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства. Також воно регулює порядок впровадження та функціонування національної системи біометричної верифікації та ідентифікації громадян України, іно-

земців та осіб без громадянства, а також визначає її структуру та призначення.

1.3 Методи біометричної ідентифікації

При класифікації біометричних технологій виділяють дві групи методів за типом використовуваних біометричних параметрів: статичні біометричні параметри та динамічні параметри.

Статичні методи

Статичні методи біометричної аутентифікації грунтуються на фізіологічній (статичній) характеристиці людини, тобто унікальній характеристиці, даній їй від народження.

Автоматичний face-контроль

Макіяж, вікові зміни, вживання міцних напоїв — всі ці чинники утрудняють ідентифікацію особи по обличчю. Навіть для експерта ідентифікація людини по фотографії десятирічної давності може виявитися дуже складним завданням. Біометричні технології дозволяють проводити face-контроль в автоматичному режимі, вони звіряють параметри обличчя об'єкта, який зафіксований камерою, з даними в базі. І достовірність такого аналізу складає 86–93%. Це значно більше за звичайні людські можливості. Проте проблема полягає в тому, що для здійснення цієї функції необхідне устаткування високої якості. Навіть для проведення візуальної ідентифікації особи відстань між центрами зіниць має бути еквівалентною 200 пікселям. Сюди входять такі методи, як аутентифікація людини за формою обличчя, термограмою обличчя.

Існують два основних способи реалізації розпізнавання осіб в відеоспостереження. При першому способі, процедура розпізнавання осіб може здійснюватися "силами" самої IP-камери і передавати відеопотік, і метадані на сервер (ПК) / відеореєстратор. З позитивних моментів: до сервера (ПК) можливо підключити велику кількість камер, тому що на ресурси продуктивності сервера не надається великого навантаження. Що

стосується недоліків даної системи: в разі розширення необхідно буде завжди використовувати камери одного і того ж виробника, для узгодження бази даних і використовуваних шаблонів розпізнавання осіб.

Другий основний спосіб: здійснювати розпізнавання осіб на стороні сервера за допомогою спеціального ПО, а з камери відеоспостереження передавати тільки відеопотік. Однозначно таку систему зручно використовувати в разі, якщо відеоспостереження вже встановлено на об'єкті, замінити досить старий сервер / відеореєстратор. Чи можна віднести до недоліків дорожнечу встановлюваного сервера, ліцензія якого на канал коштує не мало, через високу продуктивності сервера? Але і самі камери з розпізнаванням осіб на борту коштують не дешево, плюс буде необхідний демонтаж старих камер і установка нових, тому про ціну того чи іншого рішення говорити складно, необхідно розраховувати індивідуально.

За формою обличчя

У даному методі ідентифікації будується тривимірний образ обличчя людини. На обличчі виділяються контури брів, очей, носа, губ і т.д., обчислюється відстань між ними і будується не просто образ, а ще безліч його варіантів на випадки повороту особи, нахилу, зміни виразу. Кількість образів варіюється залежно від мети використання даного способу (для аутентифікації, верифікації, видаленого пошуку на великих територіях і т.д.).

За термограмою обличчя

В основі даного способу аутентифікації лежить унікальність розподілу на обличчі артерій, що забезпечують кров'ю шкіру і виділяють тепло. Для здобуття термограми використовуються спеціальні камери інфрачервоного діапазону. На відміну від попереднього цей метод дозволяє розрізняти близнят.

За відбитком пальця

В основі цього методу лежить унікальність для кожної людини малюнка папілярних узорів на пальцях. Відбиток, отриманий за допомогою спеціального сканера, перетворюється в цифровий код (згортку) і порівню-

ється з раніше введеним еталоном. Дана технологія є найрозповсюдженішою в порівнянні з іншими методами біометричної аутентифікації. Серйозний недолік сканування за відбитками пальців – можливість їх крадіжки і використання не тільки для несанкціонованого доступу, але і для фальсифікації доказів.

За формою долоні

Даний метод побудований на геометрії руки. За допомогою спеціального пристрою, що складається з камери і декількох підсвічуючих діодів (включаючись по черзі, вони дають різні проекції долоні), будується тривимірний образ грона руки, за яким формується згортка і розпізнається людина.

За розташуванням вен на лицьовій стороні долоні

За допомогою інфрачервоної камери прочитується малюнок вен на лицьовій стороні долоні або грона руки. Отримана картинка обробляється, і за схемою розташування вен формується цифрова згортка. Ця технологія досить надійна. Основний її недолік полягає в тому, що якщо за відбитками пальців можна перевірити, чи не знаходиться людина в розшуку, чи має вона судимість, то для таких біометричних параметрів, як венозний малюнок, єдиної бази не існує.

За сітківкою ока

Це спосіб ідентифікації по малюнку кровоносних судин очного дна. Для того, щоб цей малюнок став видний, людині потрібно поглянути на видалену світлову крапку, і очне дно, що таким чином підсвічується, скануєтьс

За радужною оболонкою ока

Малюнок радужної оболонки ока також є унікальною харатеристикою людини. Причому для її сканування досить портативної камери із спеціалізованим програмним забезпеченням, що дозволяє захоплювати зображення частини лиця, з якого виділяється зображення ока, з якого, у свою чергу, виділяється малюнок веселкової оболонки, за яким і будується циф-

ровий код для ідентифікації людини. При використанні цієї технології об'єкта необхідно позиціонувати свою особу для реєстрації якісного зображення веселкової оболонки очей, що, звичайно, не завжди зручно. Наприклад, при face-контролі подібних вимог не існує. Людина йде по коридору, в той момент, коли вона попаде в зону найкращого бачення, камера робить контрольний знімок. При ідентифікації особи за зображенням обличчя і радужної оболонки ока необхідно враховувати також і зовнішні умови. Залежно від фону і рівня освітленості вірогідність розпізнавання міняється. Тому в ідеалі треба помістити людину в стандартизовані умови, наприклад, в ізольовану кабіну.

Основне заперечення проти використання методу розпізнавання за райдужною оболонкою ока пов’язане з можливостями іридодіагностики й отриманням тим самим приватної інформації щодо хвороб людини.

За ДНК

Переваги даного способу очевидні, проте використовувані в даний час методи здобуття і обробки ДНК працюють настільки довго, що такі системи використовуються лише для спеціалізованих експертиз.

Динамічні методи

Динамічні методи біометричної аутентифікації грунтуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії. Розглянемо методи аутентифікації цієї групи.

За почерком

Як правило, для цього виду ідентифікації людини використовується його розпис (інколи написання кодового слова). Цифровий код індентифікації формується залежно від необхідної міри захисту і наявності устаткування (графічний планшет, екран карманного комп'ютера Palm і т.д.) двох типів:

1. За самим розписом, тобто для ідентифікації використовується просто міра збігу двох картинок.

2. За розписом і динамічними характеристиками написання, тобто для ідентифікації будується згортка, в яку входить інформація по безпосередньому підпису, тимчасовим характеристикам нанесення розпису і статистичним характеристикам динаміки натиску на поверхню.

За клавіатурним почерком

Метод у цілому аналогічний описаному, але замість розпису використовується кодове слово (коли для цього використовується особистий пароль користувача, таку аутентифікацію називають двофакторною) і не потрібно жодного спеціального устаткування, окрім стандартної клавіатури. Основною характеристикою, за якою будується згортка для ідентифікації, є динаміка набору кодового слова.

За голосом

Одна із старих технологій, у даний час її розвиток прискорився, оскільки передбачається її широке використання в побудові «інтелектуальних будівель». Існує досить багато способів побудови ідентифікації за голосом, як правило, це різні поєднання частотних і статистичних характеристик голосу. У Росії в МГТУ імені Н.Е. Баумана розроблений програмний продукт, який за 15секундним звучанням фрази дозволяє ідентифікувати людину з досить високою вірогідністю.

Інші методи

Для даної групи методів також описані лише найпоширеніші методи. Існують такі унікальні способи, як ідентифікація за рухом губ при відтворенні кодового слова, за динамікою повороту ключа в дверному замку і т.д. Загальною характеристикою, яку використовують для порівняння різних методів і способів біометричної ідентифікації, є статистичні показники: помилка першого роду (не пустити в систему «свого») і помилка другого роду (пустити в систему чужого). Сортувати і порівнювати описані вище біометричні методи за свідченнями помилок першого роду дуже складно, оскільки вони є різними для одних і тих же методів у зв'язку з залежністю від устаткування, на якому вони реалізовані. За показниками помилок дру-

гого роду загальне сортування методів біометричної аутентифікації виглядає приблизно так (від кращих до гірших):

- ДНК.
- Радужна оболонка ока, сітківка ока.
- Відбиток пальця, термограма обличчя, форма долоні.
- Форма обличчя, розміщення вен на долоні та кисті руки.
- Розпис.
- Клавіатурний почерк.
- Голос.

1.4 Технічні операційні стандарти

Існує безліч міжнародних, регіональних і національних стандартів, що охоплюють важливі елементи і периферійні функції. Власники, користувачі і споживачі біометричних систем орієнтуються на ці стандарти, щоб забезпечити гарантовано ефективну роботу їх додатків протягом усього експлуатаційного циклу відповідно до функціональних характеристиками, закладеними виробником. Вони також використовують дані стандарти для забезпечення надійності таких процесів, як і технічне обслуговування і ремонт біометричної системи, особливо якщо вона являє собою частину великої національної або міжнародної мережі, що здійснює обмін даними.

Оцінка відповідності дає потенційному покупцеві, який можливо не до кінця розбирається в тонкощах системи або продукту, гарантію того, що даний продукт відповідає технічним стандартам і стандартам безпеки або іншим зазначеним критеріям. Існують три види ОВ. Постачальник проводить оцінку відповідності першої стороною, користувач - оцінку відповідності другою стороною, але найбільш надійною є оцінка відповідності третьою стороною, що проводиться незалежними органами.

Цей процес носить назву сертифікації, оскільки, як правило, після успішного проведення оцінки продукту або послуги видається сертифікат, який служить підтвердженням того, що продукт або послуга відповідає пе-

вній специфікації або стандарту ISO / IEC. Регіональні органи також можуть розробляти стандарти з метою уніфікації систем і методів роботи в групі країн.

Наприклад, Європейський комітет з стандартизації (ЄКР) об'єднує національні органи по стандартизації з 34 європейських країн.

В рамках Комітету діє спеціальна Робоча група за біометричними даними (РГ-18), яка призводить розроблені міжнародними або національними організаціями стандарти у відповідність з європейськими вимогами в таких областях, як недоторканність приватного життя і законодавство про захист даних.

Деякі стандарти розробляються на національному рівні відповід-ними організаціями для своїх країн: наприклад, в США діють такі організації, як Американський національний інститут стандартів (АНІС) і Національний інститут стандартів і технологій (НІСТ), які розробляють стандарти, що застосовуються в криміналістиці і в пов'язаних з нею біометричних додатках.

Багато країн широко застосовують стандарти НІСТ в таких важливих областях, як електронна передача відбитків пальців по мережах. НІСТ також проводить порівняльні випробування і становить рейтинги наявних на ринку алгоритмів пошуку і зіставлення біометричних даних для застосування до інших біометричних модальностей, таких як особа і райдужна оболонка ока. Завдяки цьому потенційні покупці систем зіставлення біометричних даних можуть отримати об'єктивні відомості про відносну ефективності алгоритмів, що використовуються конкуруючими виробниками на міжнародному ринку.

Біометричні системи, що використовуються, повинні відповідати стандартам, які пред’являють до біометричної ідентифікації провідні міжнародні, галузеві й регіональні організації, міждержавні та урядові структури. Деякі з них наведені нижче:

BioAPI є стандартом BioAPI Consortium розроблений спеціально для уніфікації програмних інтерфейсів програмного забезпечення розробників біометричних пристроїв.

XML Common Biometric Format - стандарт, розроблений технічним комітетом OASIS. XCBF, визначає набір криптографічних повідомлень, представлених у вигляді XML-тегів, які можуть бути використані для безпечного збирання, обробки та зберігання біометричної інформації. Сумісний зі специфікаціями BioAPI, і стандартами X9.84 і CBEFF.

AAMVA Fingerprint Minutiae Format / National Standard for the Driver License / Identification Card DL / ID-2000 - американський стандарт на формат подання, зберігання і передачі відбитків пальців для водійських прав. Сумісний зі специфікаціями BioAPI і стандартом CBEFF.

CBEFF (Common Biometric Exchange File Format) - єдиний формат уявлення біометричних даних, який був запропонований NIST в 2001 році для заміни біометричних форматів, використовуваних виробниками різних сегментів біометричного ринку в своєму обладнанні і програмному забезпеченні. При створенні CBEFF були враховані всі можливі аспекти його застосування, в тому числі криптографія, багатофакторна біометрична ідентифікація і інтеграція з картковими системами ідентифікації.

ANSI / NIST-ITL 1-2000 Fingerprint Standard Revision - американський стандарт, який визначає загальний формат уявлення і передачі даних з використанням відбитка пальця, особі, натільною шрамів і татуювань для використання в правоохоронних органах США.

CDSA / HRS (Human Recognition Services) являє собою біометричний модуль в архітектурі Common Data Security Architecture, розробленої Intel Architecture Labs і схваленого консорціумом Open Group. CDSA - визначає набір API, що представляє собою логічно пов'язані безліч функцій, що охоплюють такі компоненти захисту, як шифрування, цифрові сертифікати, різні способи аутентифікації користувачів, в список яких за допомогою HRS

додана і біометрія. CDSA / HRS сумісний зі специфікаціями BioAPI і стандартом CBEFF.

Міжнародна організація зі стандартизації (ISO) виклала розроблені нею стандарти в документі «Юридичні та соціологічні міркування щодо застосування. Частина 1. Загальне керівництво »(ISO / IEC TR 24714: 2008) та в Керівних вказівках 71 : 2014, де мова йде про етичні аспекти, а також в Керівних вказівках 71 про стандарти забезпечення доступності для осіб похилого віку та інвалідів.

Міжнародна організація по стандартізації (ISO) розробляє і публікує стандарти з широкого кола галузей, включаючи біометрію і криміналістику. ISO - це всесвітнє об'єднання національних органів по стандартизації з 162 країн, які вносять вклад в розробку стандартів за допомогою участі в роботі різних профільних комітетів. Інші країни можуть приєднатися до ISO в якості асоційованих членів або членів-передплатників для отримання інформації про стандарти.

Крім того, існують два спільних комітету ISO та Міжнародної електротехнічної комісії (МЕК), які розробляють стандарти і проводять оцінки відповідності (ОВ) для всієї електричної, електронної та пов'язаної з цим продукції.

Методи та класифікатори автоматизованої класифікації відбитків пальців

Процес класифікації полягає у наступному – спочатку відбиток на основі відповідних ознак відноситься до одного з класів, а потім за локальними ознаками здійснюється порівняння відбитка з відбитками, які є у базі даних, поки не буде знайдено відповідність. Зараз існує декілька підходів до автоматичної класифікації, усі ці підходи поділено на п’ять категорій:

1. На основі моделі – цей підхід заснований на використанні моделі розташування особливих точок (ядер та розбіжностей). Цей підхід використовує знання людини-експерта, він застосовує правила для

класифікації відбитків на базі створеної вручну моделі, тому потребує вивчення.

2. На основі структури – цей підхід використовує оцінку орієнтаційного поля на відбитку, для того щоб віднести його до відповідного класу, безпосередня класифікація відбувається на основі нейронної мережі.

3. На основі частоти – даний підхід використовує спектр частот відбитків пальців та ряди Фур'є для проведення класифікації.

4. Синтаксичний підхід – використовує формальну граматику для подання та класифікації відбитків пальців.

5. Гібридні підходи – використовують комбінацію двох або більше підходів для проведення класифікації відбитків пальців.

Найбільш перспективний серед цих підходів багатоканальний підхід. Кожен із цих підходів здійснює класифікацію відбитків спираючись на спеціальну методологію, яка називається класифікатор. Класифікатор визначає яким чином буде встановлюватися приналежність відбитка до того чи іншого класу. Існує декілька видів класифікаторів:

- Класифікатор "К-найближчий" ;
- Класифікатор нейронна мережа;
- Двоетапний класифікатор;
- Класифікатор на основі прихованої моделі Маркова;
- Класифікатор на основі «дерева рішень»;
- Гібридні класифікатори

Методи розпізнавання на основі райдужної оболонки ока

Існує кілька методів ідентифікації на основі райдужної оболонки ока. Проте у загальному випадку всі вони діють за однією і тією ж самою схемою. Схема наведена на рис. 1.1.

Рисунок 1.1 – Спрощена схема процеса ідентифікації на основі райдужної оболонки ока

Дана схема складається з кількох етапів:

- Отримання зображення ока;
- Аналіз якості зображення РОО;
- Виділення райдужної оболонки на зображенні;
- Нормування розмірів зображення райдужної оболонки;
- Обчислення ознак і формування з них набору роговиці;
- Порівняння отриманого набору з еталонним.

Методи та механізми голосової ідентифікації

Задача біометричної ідентифікації за голосом може бути поділена на два типи – задача розпізнавання окремих слів та задача розпізнавання зв'язної мови. Для розв'язання цих задач використовують фізіологічні та артикуляційні ознаки голосу. Сьогодні існує два головних методи створення систем голосової ідентифікації:

1. Еталонний метод.
2. Фонемно-орієнтований метод.

Еталонний метод засновано на порівнянні деяких ознак голосу (це можуть бути як фізіологічні, так і артикуляційні ознаки) з деяким еталоном. Як еталон використовують деяку групу окремих слів.

Фонемно-орієнтований метод засновано на виділенні з потоку мови окремих фонем. Не можна сказати, що якийсь з цих методів має перевагу, бо кожний з них доцільно використовувати у певних ситуаціях. Проте кожний з цих двох методів може бути застосовано для створення систем голосової ідентифікації, які можна поділити на наступні класи:

- Текстозалежні;
- Текстонезалежні;
- Дикторозалежні;
- Дикторонезалежні

Дикторозалежні системи – це системи, які орієнтовані на ознаки мови певної людини або групи осіб, тому вони можуть використовуватися для ідентифікації тільки цієї особи (групи осіб). При зміні диктора (особи, яка ідентифікується системою) необхідно настроювати систему знову з використанням голосових ознак нового диктора.

Дикторонезалежні системи – це системи, які не прив'язані до голосових ознак певної особи, та можуть використовуватися для ідентифікації будь-якої особи. Такі системи самі виділяють необхідні ознаки голосу та порівнюють їх з еталоном з бази.

Текстозалежні системи – це системи голосової ідентифікації, які здійснюють ідентифікацію особи за допомогою певного ключового слова або ключової фрази, яку повинна вимовити особа, яка проходить ідентифікацію.

Тестонезалежні системи – це системи, які здійснюють ідентифікацію особи за допомогою голосу без прив'язки до будь-яких ключових слів. У даному випадку важливе значення мають артикуляційні ознаки голосу людини, саме вони використовуються як головні ознаки, а фізіологічні ознаки виступають як вторинні. Схема класифікації наведена на рисунку 1.2.

Рисунок 1.2 – Класифікація методів голосової ідентифікації

Методи ідентифікації за рукописним підписом

Підписи можна отримати за допомогою електронних пристроїв як прості бітові карти для того, щоб зменшити кількість паперу, необхідного для їх зберігання і транспортування. Крім того, обсяг транзакцій, авторизованих за допомогою підписів, сьогодні величезний, що робить автоматизацію процесу зчитування підпису дуже важливою.

Нещодавно були розроблені методи підрахунків положення і напрямів ручки з використанням видимого світла. Ці методи, ймовірно, дозволять знизити вартість зчитування і навіть можуть призвести до створення тривимірних підписів.

Існує два незалежних способи ідентифікації за підписом:

– Ідентифікація за малюнком підпису на документі;

– Ідентифікація за динамікою підпису, що вводиться в комп'ютер

У першому способі потрібно порівняти два зображення. З цим краще впорається людина.

У другому способі є дані про коливання пера при відтворенні підпису у тривимірному просторі (X, Y – координати і Z – тиск на планшет). З цим може впоратися тільки комп'ютер. Схема зображена на рисунку 1.3.

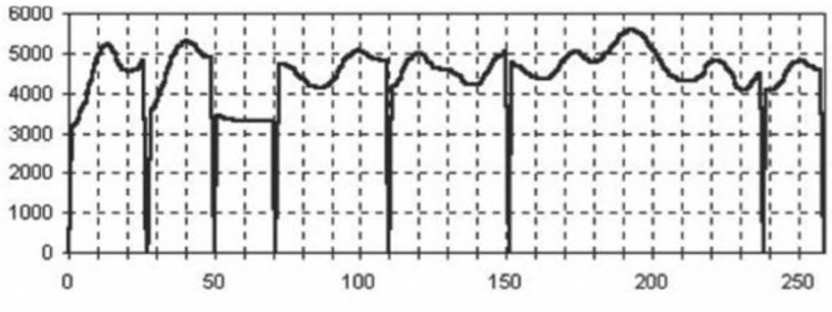

Рисунок 1.3 – Коливання пера по вертикалі (нульові значення функції відповіда-ють моментам відриву пера від планшета)

Методи розпізнавання за геометрією кисті руки

У біометриці виділяються два основних методи розпізнавання за геометрією кисті руки:

– Перший метод – заснований виключно на геометричних характеристиках кисті руки. У найпростішому варіанті зберігається тільки інформація про довжину та ширину пальців, більш складні системи вимірюють профіль руки, який включає обсяг кисті, пальців, нерівності долоні, розташування складок шкіри на вигинах;

– Другий (більш сучасний) заснований на змішаних характеристиках геометричних й образних. До останніх відносяться образи на вигинах між фалангами пальців, візерунки (розташування) підшкірних кровоносних судин. З руки знімаються чотири характеристики, з яких три є скалярами і відносяться до розмірів пальців. Сутність першого методу можна побачити на рисунку 1.4.

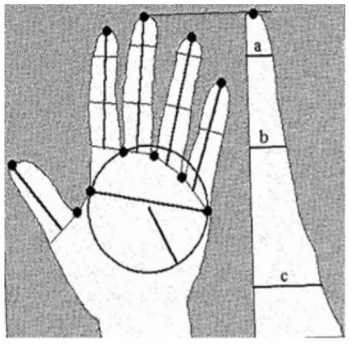

Рисунок 1.4 – Аналіз геометрических характеристик руки

На рисунку показано 3D-геометрію руки. У розглянутому підході вся інформація, яка цікавить нас, зібрана у горизонтальному і вертикальному силуеті кисті руки. На даному рисунку показані контрольні (характеристичні) точки силуету руки і 17 вихідних геометричних ознак руки, у даному випадку відмічені відрізками прямих ліній, які не входять до силуету кисті. Як бачимо, вихідними біометричними ознаками руки є ширина долоні, радіус вписаного в долоню кола, довжини пальців (визначені як відстані від виділених верхніх контрольних точок до середини ліній, що з'єднують нижні контрольні точки), ширина пальців і висота кисті руки у трьох пунктах, зазначених лініями a, b і c.

Сутність іншого методу – «зняття» з долоні чотирьох характеристик, з яких три є скалярами і відносяться до розмірів пальців, а четверта – являє собою напівтонове зображення складок шкіри на вигині між фалангами. Три перші характеристики – це ширина вказівного пальця 1, висота вказівного пальця 2 і довжина середнього пальця 3, оцінювана так, як показано на рис. Характеристика 4 в розглянутому випадку являє собою зображення складок шкіри на вигині між середньою і нижньою фалангами вказівного пальця. Вся інформація про долоню у розглянутому класі систем може бути записана не більше ніж 9 байтами. Спосіб отримання всіх чотирьох характеристик показаний на рисунку 1.5.

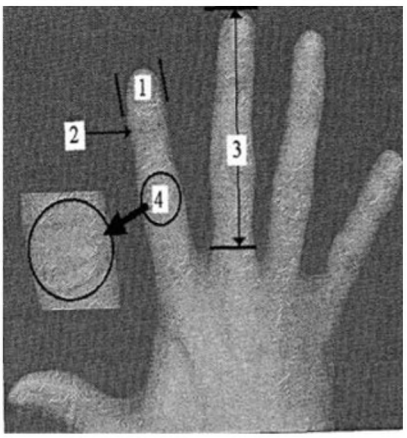

Рисунок 1.5 – Отримання змішаних характеристик долоні

Методи ДНК-ідентифікації

Сьогодні процес ДНК-ідентифікації успішно розвивається, збільшилася швидкість проведення ідентифікації, зменшилася складність самого процесу ідентифікації.

Для проведення ДНК-ідентифікації використовується низка методів, а саме:

1. Метод ПДРФ (поліморфізм довжин рестрикційних фрагментів (Restriction fragment length polymorphism, RFLP) – цей метод ідентифікації заснований на дослідженні ДНК шляхом її розрізання за допомогою ендонуклеаз рестрикції і подальшого аналізу розмірів отриманих фрагментів (рестриктів) шляхом ДНК електрофорезу. За допомогою ПДРФ можна ідентифікувати відмінності у послідовності нуклеотидів ДНК. ПДРФ був розроблений як перший і дешевий метод для масового застосування.

2. Метод ПЛР (полімеразної ланцюгової реакції) – цей метод ДНКідентифікації більш досконалий, ніж ПДРФ-метод. Він дозволяє домогтися значного збільшення малих концентрацій певних фрагментів нуклеїнової кислоти (ДНК) у біологічному матеріалі (пробі). Даний метод сьогодні найбільш популярний, його сутність полягає у наступному: вихідний зразок ДНК (складається з комплементарних ланцюжків, що містять повторювані послідовності, які й використовуються для ідентифікації) нагрівають до температури 94°С, додають праймер (короткий фрагмент нуклеїнової кислоти – олігонуклеотид), що призводить до поділу ланцюжків ДНК на окремі фрагменти ДНК. Після цього відбувається охолодження і праймери прикріплюються до фрагментів ДНК, потім додається ДНК полімереза, яка запускає процес ампліфікації (розмноження, копіювання) фрагментів ДНК.

За допомогою ДНК-електрофорезу ампліфіковані фрагменти поділяються за довжиною і порівнюються з контрольним зразком ДНК на результат відповідності. Метод ПЛР ДНК-ідентифікації є найпоширенішим, сьогодні існує кілька різновидів цього методу: – вкладе-

на ПЛР; – інвертована ПЛР; – ПЛР зі зворотною транскрипцією; – асиметрична ПЛР; – кількісна ПЛР; – ступінчаста ПЛР; – метод молекулярних колоній; – ПЛР довгих фрагментів; – груп-специфічна ПЛР; – ПЛР з використанням гарячого старту; – віртуальна ПЛР або електронна ПЛР (е-ПЛР).

Всі ці методи відрізняються алгоритмом проведення аналізу, але всі вони використовують механізм полімеразної ланцюгової реакції.

Методи, засновані на геометричних характеристиках обличчя

Один із найперших методів – це аналіз геометричних характеристик особи. Сутність його полягає у виділенні набору ключових точок (або областей) особи і наступному виділенні набору ознак. Кожна ознака є або відстанню між ключовими точками, або відношенням таких відстаней. На відміну від методу порівняння еластичних графів, тут відстані обираються не як дуги графів. Набори найбільш інформативних ознак виділяються експериментально. Ключовими точками можуть бути куточки очей, губ, кінчик носа, центр ока тощо. Як ключові області можуть бути прямокутні області, що включають у себе: очі, ніс, рот. У процесі розпізнавання порівнюються ознаки невідомої особи з ознаками, що зберігаються у базі. Задача знаходження ключових точок наближається за трудомісткістю безпосередньо до розпізнавання, і правильне знаходження ключових точок на зображенні багато в чому визначає успіх розпізнавання.

Схема зображена на рисунку 1.6.

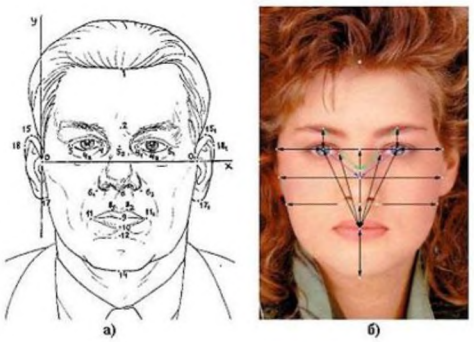

Рисунок 1.6 - Ідентифікаційні точки на відстані: а) використовувані при криміналістичній експертизі; б) найбільш часто використовувані при побудові автоматизованих систем ідентифікації.

Тому зображення обличчя людини має бути без завад, що заважають процесу пошуку ключових точок. До таких завад відносять окуляри, бороди, прикраси, елементи зачіски й макіяжу. Освітлення бажано рівномірне й однакове для всіх зображень. Крім того, зображення обличчя повинно мати фронтальний ракурс, можливо з невеликими відхиленнями. Вираз обличчя має бути нейтральним. Це пов'язано з тим, що у більшості методів немає моделі врахування таких змін. Таким чином, даний метод висуває суворі вимоги до умов зйомки, потребує надійного механізму знаходження ключових точок для загального випадку. Крім того, потрібне застосування більш досконалих методів класифікації або побудови моделі змін. У загальному випадку цей метод не найоптимальніший, проте для деяких специфічних завдань перспективний. До таких завдань можна віднести документний контроль, коли потрібно порівняти зображення обличчя, отримане у поточний момент з фотографією у документі. При цьому інших зображень цієї людини немає, і отже механізми класифікації, засновані на аналізі тренувального набору, недоступні.

Порівняння еталонів

Порівняння еталонів (Template Matching) полягає у виділенні областей особи на зображенні, й у наступному порівнянні цих областей для двох різних зображень. Кожна область, що збігається, збільшує міру подібності зображень. Це також один із історично перших методів розпізнавання людини за зображенням особи. Для порівняння областей використовуються найпростіші алгоритми як попіксельне порівняння. Недолік цього методу полягає у тому, що він вимагає багато ресурсів як для зберігання ділянок, так і для їх порівняння. З причини того, що використовується найпростіший алгоритм порівняння, зображення повинні бути зняті у суворо встановлених умовах: не допускається помітних змін ракурсу, освітлення, емоційного вираження та ін. Приклад зображений на рисунку 1.7.

Рисунок 1.7 - Порівнювальні області – еталони обличчя

Гнучкі контурні моделі особи

У даних методах розпізнавання проводиться на основі порівняння контурів особи. Контури звичайно беруться для ліній голови, вух, губ, носа, брів та очей. Контури представлені ключовими позиціями, між якими положення точок, що належать контуру, обчислюються інтерполяцією. Для локалізації контурів у різних методах використовується як апріорна інформація, так й інформація, отримана в результаті аналізу тренувального набору. Спочатку ключові точки розміщувалися вручну на наборі тренувальних зображень. Потім вилучалася інформація про інтенсивність пікселів, що лежать на лінії, перпендикулярній контуру для кожної точки контуру. При пошуку контурів нового обличчя використовувався метод симуляції з цільовою функцією з двох складових. Перша з них максимізувалася при відповідності інтенсивностей пікселів, вилучених на перпендикулярній контуру лінії аналогічним пікселям з тренувальної вибірки. Друга – при збігу контуру з формою контурів тренувальних прикладів. Таким чином, вилучався не просто контур, а контур рис обличчя. Як має виглядати типовий контур рис обличчя, процедура пошуку знала з тренувальних прикладів. Для порівняння зображень використовувалися значення головних компонент, обчислених на наборі векторів, що являють собою координати ключових точок. У даній роботі контурна модель використовувалася разом з напівтоновою моделлю, спільне їх використання підвищувало точність розпізнавання. Головним завданням при

розпізнаванні за контурами є правильне виділення цих контурів. У загальному вигляді ця задача за складністю порівняна безпосередньо з розпізнаванням зображень. Крім того, використання цього методу самого по собі для задачі розпізнавання недостатнє.

Лінійний дискримінантний аналіз

Метод власних облич вимагає для свого застосування ідеалізованих умов, таких як єдині параметри освітленості, нейтральний вираз обличчя, відсутність завад на зразок окуляр та борід. Цих умов у загальному випадку не можна досягти шляхом попереднього оброблення. При недотриманні цих умов головні компоненти не будуть відображати міжкласові варіації, і класи перестають являти собою кластери у власному просторі.

Наприклад, за різних умов освітлення, метод власних облич практично непридатний, оскільки перші головні компоненти переважно відображають зміни освітлення, і порівняння видає зображення, що мають схожий рівень освітленості. Лінійний дискримінантний аналіз (лінійний дискриминант Фішера – Linear Discriminant Analysis, LDA) обирає проекцію простору зображень на простір ознак таким чином, щоб мінімізувати внутрішньокласову й максимізувати міжкласову відстань у просторі ознак.

У цих методах передбачається, що класи лінійно розділені. Як бачимо у цьому випадку проектування на власний простір змішує класи, що робить розпізнавання неможливим, а лінійний дискримінант обирає проекцію на простір ознак таким чином, щоб розділити різні класи. Матриця W для проектування простору зображення на простір ознак обирається з наступної умови:

$$W_{opt} = \arg\max_{W} \left| \frac{W^T S_B W}{W^T S_W W} \right|, \tag{1.3}$$

де SB – матриця міжкласової дисперсії; SW – матриця внутрішньокласової дисперсії. Може існувати до c–1 векторів складових базис просто-

ру ознак, де с – загальне число класів. За допомогою цих векторів простір зображень переводиться у простір ознак. Оскільки робота безпосередньо з матрицею складна через її розмірність, використане попереднє зменшення розмірності за допомогою методу головних компонент, і потім обчислення проводяться у просторі меншої розмірності:

$$W_{fld}=\arg\max_{W}\left|\frac{W^{T}W_{pca}^{T}S_{B}W_{pca}W}{W^{T}W_{pca}^{T}S_{W}W_{pca}^{T}W}\right| \qquad (1.4)$$

де Wpca – матриця для проектування у простір меншої розмірності (простір голавних компонент). У зазначеній роботі такий метод був названий обличчями Фішера (Fisherfaces). Так само як і власні вектори, зображення базисних дискримінантних векторів мають обличчяподібну форму.

Порівняння еластичних графів

У цьому методі (Elastic Bunch Graph Matching) особа представляється у вигляді графа, вершини якого розташовані на ключових точках особи, таких як контури голови, губ, носа та їх крайніх точках. Кожна грань позначена відстанями між її вершинами. У кожній такій точці обчислюються коефіцієнти габорових функцій для п'яти різних частот і восьми орієнтацій. Набір таких {Jj} коефіцієнтів називається джетом (jet).

Джети характеризують локальні області зображень і служать для двох цілей. По-перше, для знаходження точок відповідності у заданій області на двох різних зображеннях. По-друге, – для порівняння двох відповідних областей різних зображень.

Кожен коефіцієнт для точок з однієї області різних зображень, характеризується амплітудою aj, яка повільно змінюється зі зміною положення точки і фазою, яка обертається зі швидкістю, пропорційною частоті хвильового вектора базисного вейвлета.

Тому у найпростішому випадку для пошуку на новому зображенні точки з аналогічними характеристиками у функції подібності фазу не враховують:

$$S_a(j,J') = \frac{\sum_j a_j a'_j}{\sqrt{\sum_j a_j^2 \sum_j a'^2_j}} \qquad (1.5)$$

Функція подібності з одним джетом у фіксованій позиції та іншим зі змінною позицією є досить гладенькою, для того щоб отримати швидку і надійну збіжність при пошуку із застосуванням найпростіших методів, таких як дифузія або градієнтний спуск. Більш досконалі функції подібності залучають інформацію про фаз. Приклад зображений на рисунку 1.8.

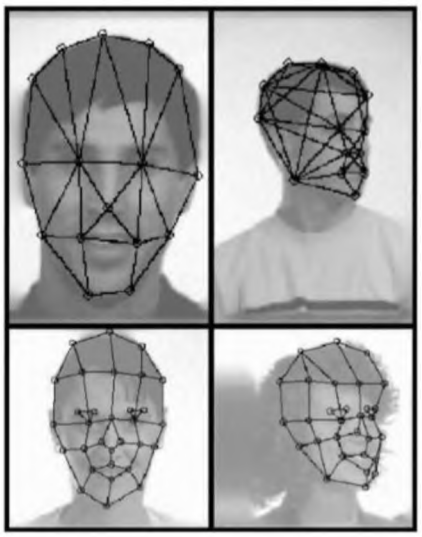

Рисунок 1.8 - Еластичний граф, який покриває зображення обличчя

Для різних ракурсів відповідні ключові точки відзначені вручну на тренувальному наборі. Крім того, щоб для однієї і тієї самої особи надати різні варіації її зображення в одному й тому самому графі, для кожної точки використовуються кілька джетів, кожен з яких може відповідати різним ло-

кальним характеристикам даної точки, наприклад, відкритого і закритого ока.

Процес розпізнавання невідомої особи складається з порівняння графа зображення обличчя G1 з усіма іншими графами з набору B за допомогою функції подібності:

$$S_B(G^I, B) = \frac{1}{N}\sum_n \max_m \left(S_\phi(J_n^I J_n^{Bm}) \right) - \frac{\lambda}{E}\sum_l \frac{(\Delta\vec{x}_l^I - \Delta\vec{x}_l^B)^2}{(\Delta\vec{x}_l^B)^2}. \qquad (1.6)$$

Ліва сума характеризує подобу джетів, обчислену із застосуванням фазочутливої функції; права – топографічну відповідність, яка пропорційна квадрату різниці відстаней між відповідними вершинами порівнюваних зображень; N – кількість вершин; E – кількість граней. У наданому вище вигляді метод здатний досить надійно розпізнавати при змінах ракурсу до 22°; при великих кутах точність розпізнавання різко зменшується, функція подібності виявляється більш чутливою до ракурсу, ніж до міжкласових відмінностей. Зміни умов освітленості у роботі не проводилися.

Метод Віллі-Джонса

Метод був розроблений і представлений у 2001 р. Полом Віолою та Майклом Джонсом. Він досі є ефективним методом для пошуку об'єктів на зображеннях і відеопослідовностей у режимі реального часу. Слід зазначити, що цей детектор має вкрай низьку ймовірність помилкового виявлення особи. Метод добре працює і виявляє риси обличчя навіть при спостереженні об'єкта під невеликим кутом, приблизно до 30°. При куті нахилу понад 30° ймовірність виявлення обличчя різко падає. Зазначена особливість методу не дозволяє у стандартній реалізації детектувати обличчя людини, повернене під довільним кутом, що значною мірою ускладнює або унеможливлює використання алгоритму в сучасних виробничих системах з урахуванням їх зростаючих потреб. Для того, щоб розрахувати яскравість прямокутної ділянки зображення, використовують

інтегральне подання. Таке уявлення використовується часто і в інших методах, наприклад, у вейвлет-перетвореннях, Speeded up robust feature (SURF), фільтрах Хаара і багатьох розроблених алгоритмах. Інтегральне подання дозволяє швидко розраховувати сумарну яскравість довільного прямокутника на даному зображенні, причому час розрахунку не залежить від площі прямокутника. Інтегральне подання зображення являє собою матрицю, що збігається за розмірами з вихідним зображенням. У кожному її елементі зберігається сума інтенсивностей всіх пікселів, що знаходяться лівіше і вище даного елемента. Елементи матриці розраховуються за такою формулою:

$$L(x, y) = \sum_{i=0, j=0}^{i \le x, j \le y} I(i, j), \tag{1.7}$$

де I(x, y) – значення точки (x, y) інтегрального зображення; i(x, y) – значення інтенсивності вихідного зображення. На основі застосування інтегрального подання зображення обчислення ознак однакового виду, але з різними геометричними параметрами, відбувається за однаковий час.

Кожен елемент матриці I(x, y) являє собою суму пікселів у прямокутнику від i(0,0) до i(x, y), тобто значення кожного елемента I(x, y) дорівнює сумі значень усіх пікселів лівіше і вище даного пікселя i(x, y). Розрахунок матриці займає лінійний час, пропорційний числу пікселів у зображенні і його можна здійснювати за такою формулою:

$$I(x, y) = i(x, y) - I(x-1, y-1) + I(x, y-1) + I(x-1, y). \tag{1.8}$$

Інтегральне подання має цікаву особливість. За інтегральною матрицею можна дуже швидко вирахувати суму пікселів довільного прямокутника.

Метод головних компонент

Метод головних компонент (Principal Component Analysis, PCA) застосовується для стиснення інформації без суттєвих втрат інформативності. Він полягає у лінійному ортогональному перетворенні вхідного вектора X розмірності N у вихідний вектор Y розмірності M, N < M. При цьому компоненти вектора Y є некорельованими і загальна дисперсія після перетворення залишається незмінною. Матриця X складається з усіх прикладів зображень навчального набору.

Застосування для задачі розпізнавання людини за зображенням обличчя має наступний вигляд. Вхідні вектори являють собою відцентровані й приведені до єдиного масштабу зображення облич. Власні вектори, обчислені для всього набору зображень облич, називаються власними обличчями (eigenfaces).

Метод головних компонент у застосуванні до зображень облич так само називають методом власних облич. Власні обличчя мають корисну властивість, яка полягає у тому, що зображення, яке відповідає кожному такому вектору має обличчяподібну форму. За допомогою обчислених раніше матриць вхідне зображення розкладається на набір лінійних коефіцієнтів, називаних головними компонентами. Сума головних компонент, помножених на відповідні власні вектори, є реконструкцією зображення. Приклади зображені на рисунку 1.9 та 1.10 відповідно.

Рисунок 1.9 – Приклад зображень власних векторів (власні обличчя)

Рисунок 1.10 – Приклад зображень обличчя: а) вирівняне зображення; б) реконструкція за 85-ма головними компонентами; в) JPEG-реконструкція (530 байт)

Для кожного зображення обличчя обчислюються його головні компоненти. Звичайно береться від 5 до 200 головних компонент. Інші компоненти кодують дрібні відмінності між обличчями та шум. Процес розпізнавання полягає у порівнянні головних компонент невідомого зображення з компонентами всіх інших зображень. Для цього застосовують будь-яку метрику (найпростіший випадок – евклідова відстань).

При цьому передбачається, що зображення облич, що відповідають одній людині, згруповані в кластери у власному просторі. З бази даних (або тренувального набору) вибираються зображення-кандидати, які мають найменшу відстань від вхідного (невідомого) зображення.

Подальше удосконалення полягало у використанні метрики Махаланобіса і гауссівського розподілу для оцінки близькості зображень. Для врахування різних ракурсів у цій самій роботі використовувався многомодальний розподіл зображень у власному просторі. Додаткове підвищення надійності досягалося за рахунок додаткового застосування аналізу головних компонент до окремих ділянок обличчя, таких як очі, ніс, рот.

Розпізнавання осіб в системах відеоспостереження, технологія, яка

з'явилася в даній сфері відносно недавно і дуже впевнено захопила частку на ринку. Технологія розпізнавання осіб на основі біометрії особи є «вершиною» відеоаналітики: вона ставить найбільш складні завдання і задіє широкий спектр математичних інструментів.

З одного боку, біометрична система реалізує функцію розпізнавання, встановлюючи вірогідну зв'язок зображення з ідентифікаторами людей, зареєстрованих в базі даних. З іншого боку, біометрична система вимагає бездоганної роботи функцій виявлення і стеження.

Завданням подальшої роботи є:

1.Розглянути поняття та основні області застосування біометрії;

2.Проаналізувати нормативно-правову базу захисту біометричних даних;

3. Зробити дослідження особливостей захисту біометричних персональних даних у корпоративних системах відеоспостереження;

4. Проаналізувати можливі атаки на систему, розроблені методики захисту від даних атак, створені методики безпечної передачі даних у системах захисту біометричних персональних даних;

5. Розрахувати витрати на реалізацію методик, щодо безпечного зберігання та передачі інформації у системах захисту біометричних персональних даних.

ВИСНОВОК

У розділі було розглянуто основні області застосування біометричних методів ідентифікації та аутенифікації, нормативно-правова база у сфері захисту біометричних даних, класифікація систем обробки біометричних персональних даних та методи біометричної ідентифікації.

Двовимірна фотографія обличчя індивідуума є найбільш прийнятною для суспільства, оскільки є безконтактним і найтрадиційнішим способом ідентифікації особи. Тривимірна цифрова фотографія у цьому сенсі нічим не відрізняється від звичайної, але набагато підвищує точність автоматичної ідентифікації. Зовнішність людини, на відміну від інших характеристик, – її найбільш природний ідентифікатор, який може використовуватися оператором-людиною для перевірки рішення, ухваленого комп'ютером.

Оскільки серед методів біометричної ідентифікації одним з найбіш ефективних методів був метод ідентифікації за формою обличчя, у наступних розділах буде більш детально досліджено цей метод, в тому числі аналіз архітектури на базі типового підприємства, яке використовує цей метод.

РОЗДІЛ 2.АНАЛІЗ ПРОБЛЕМ У СИСТЕМАХ ЗАХИСТУ БІОМЕТРИЧНИХ ПЕРСОНАЛЬНИХ ДАНИХ

2.1 Види атак на системи біометричних персональних даних

Спільні етапи у різних системах біометрії зображені на рисунку 2.1

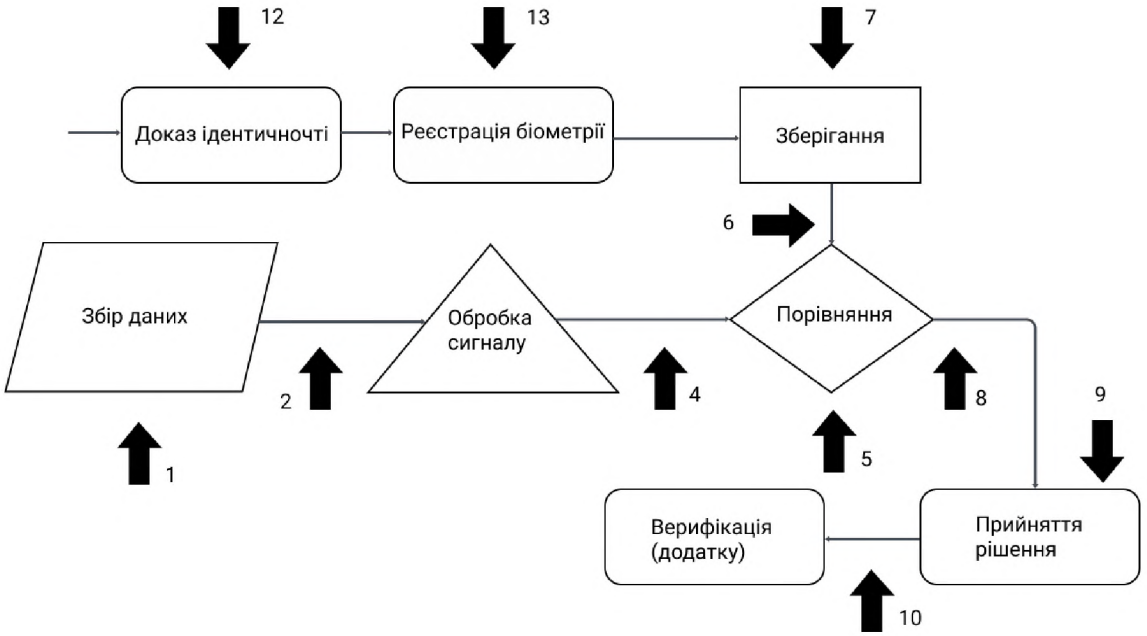

Рисунок 2.1 – Схема спільних етапів у системах біометрії

У розділі буде розглянуті можливі атаки на кожен з етапів у системах біометрії.

1. Збір даних

Можливі загрози:

1. Підміна
2. Використання недовірених пристроїв (підміна пристроїв)
3. Перевантаження пристроїв (виведення з ладу)

Підміна об’єкта (spoofing). Спуфінг або спуфінг-атака — це випадок, коли особа або програма маскується під іншу за допомогою фальсифікації даних, і тим самим отримує незаконну перевагу. Типові приклади: несправжній DNS-сервер, підміна IP-адреси джерела (IPspoofing), несправжній ARP-запит (ARPspoofing).

Перевантаження пристроїв. Блокування зловмисником доступу до інформаційних об'єктів чи сервісів шляхом перевантаження системи управління доступом запитами з використанням атак типу «спрямований шторм» (Syn Flood), анонімної електронної пошти (spam), чи вірусних атак спеціального типу.

SYN Flood - одна з різновидів мережевих атак типу відмова від обслуговування, яка полягає у відправці великої кількості SYN-запитів (запитів на підключення по протоколу TCP) в досить короткий термін (RFC 4987).

2. Обробка сигналу

Загроза:

1. Внесення даних порушника
2. Заміна компонентів

Внесення даних порушника - підміна (імітація) довіреного об'єкта або суб'єкта із підробкою мережних адрес тих об'єктів, що атакують.

Заміна компонентів - зміна параметрів маршрутизації й змісту інформації, що передається, внаслідок відсутності контролю за маршрутом повідомлень чи відсутності фільтрації пакетів із невірною адресою

3. Порівняння

Загроза

1. Внесення даних порушника
2. Заміна компонентів
3. Вгадування/ перебір (FAR атака)
4. Маніпуляція результатами (рейтингом) порівняння
5. Hill-climbing

FAR атака - атака методом перебору (підбору значень). Атака методом перебору базується на однойменному математичному методі, в якому правильне рішення (кінцеве число, або символьна комбінація) знаходиться за допомогою перебору різних варіантів. Фактично кожне значення з зада-

ної множини потенційних відповідей (рішень) перевіряється на правильність.

Атаки методом перебору - тип атаки на пристрій, при якому атакуючий перебором значень (облікових записів, паролів, сесійних даних) намагається отримати доступ до пристрою, або даних.

Hill-climbing - відправка згенерованих шаблонів і, на основі отриманого вердикту від модуля порівняння, генерація модифікованих шаблонів для проходження успішної перевірки)

4. Прийняття рішення

Загроза:

1. Hill-climbing
2. Маніпуляція налаштуваннями порогових значень
3. Маніпуляція прийняттям рішення
4. Заміна компонентів

5. Додаток (верифікація)

Загроза:

1. Шкідливий код

Шкідливий код - модифікація чи підміна програмних кодів, чи їхніх частин шляхом впровадження руйнуючих програмних засобів чи зміни логіки роботи програмного файлу із використанням спеціальних типів вірусних атак, спроможних здійснити те чи інше порушення цілісності.

6. Зберігання

Загроза:

1. Компрометація бази даних (читання біометричного шаблону, заміна шаблону, зміна зв'язки)

Компрометація бази даних - подолання криптографічної захищеності інформаційних об’єктів робочих станцій. Несанкціонований доступ до інформаційних об’єктів із використанням недоліків систем ідентифікації та автентифікації, заснованих на атрибутах користувача (ідентифікатори, паролі, біометричні дані та т.ін.) із розкриттям ключових наборів.

7. Передача “сирих” даних, передача оброблених даних

Загроза:

1. Перехват
2. Повтор
3. “Людина посередині”
4. Підбір / перебір (FAR атака)

Перехват - розвідка, аналіз трафіка. Перехоплення інформації, що пересилається, у незашифрованому вигляді в широкомовному середовищі передачі даних, відсутність виділеного каналу зв’язку між об’єктами.

Атака “Людина посередині” - селекція потоку інформації та збереження її шляхом впровадження в розподілену обчислювальну систему хибних об’єктів. Використання недоліків алгоритмів віддаленого пошуку.

8. Пошук біометричного шаблону

Загроза:

1. Перехват
2. Повтор
3. “Людина посередині”

9. Передача результату порівняння

Загроза:

1. Hill-climbing
2. Маніпуляція результатами (рейтингом) порівняння
3. Заміна компонентів

10. Взаємодія з додатком (верифікатором)

Загроза:

1. Перехват
2. Маніпуляція з прийнятим рішенням по порівнянню

2.2 Аналіз методів та засобів протидії загрозам на системи біометричних персональних даних

Проаналізувавши види атак та загрози, були розроблені міри нейтралізації цих загроз на кожному з етапів.

Під «жвавістю» розуміється:

1) Рандомізація

Випадкові фрази, випадкові комбінації жестів, випадкові комбінації пальців

2) Комбінація біометричних методів

3) Аналіз динаміки

Взаємна аутентифікація (англ. mutual authentication) - варіант аутентифікації сторін, при якому кожна зі сторін перевіряє, що взаємодіє з нею сторона - саме та, за яку себе видає. Взаємна аутентифікація реалізується таким протоколом ідентифікації, в якому кожен з учасників є одночасно і тим, що доводить свою справжність, і перевіряючим. Це дозволяє за один сеанс виконання протоколу кожним з учасників довести іншому учаснику свою ідентичність.

Таблиця 2.1 – Загрози та методи протидії етапу збору даних

Елемент системи	Загроза	Міра нейтралізації
Збір даних	Підміна	Виявлення “жвавості” Запит / Відповідь
	Використання недовірених пристроїв (під-міна пристроїв)	Взаємна аутентифікація
	Перевантаження пристроїв (ви-ведення з ладу)	Пристрої в захищеному виконанні

Таблиця 2.2 – Загрози та методи протидії етапу обробки сигналу

Елемент системи	Загроза	Міра нейтралізації
Обробка сигналу	Внесення даних порушника	Перевірені алгоритми
	Заміна компонентів	“Підписані” компоненти

Таблиця 2.3 – Загрози та методи протидії етапу порівняння

Елемент системи	Загроза	Міра нейтралізації
Порівняння	Внесення даних порушника	Перевірені алгоритми
	Заміна компонентів	“Підписані” компоненти
	Вгадування/ перебір (FAR атака)	Перевірені алгоритми комбінація біометричних методів
	Маніпуляція результатами (рейтингом) порівняння	Захист від отладки
	Hill-climbing (відправка згенерованих шаблонів і, на основі отриманого вердикту від модуля порівняння, генерація модифікованих шаблонів для проходження успішної перевірки)	Захищений канал Довіренний сенсор (взаємна аутентифікація)

Таблиця 2.4 – Загрози, методи протидії етапу прийняття рішення

Елемент системи	Загроза	Міра нейтралізації
Прийняття рішення	Hill-climbing	Захищений канал Довіренний сенсор (взаємна аутентифікація)
	Маніпуляція налаштуваннями порогових значень	Контроль доступу Захист даних
	Маніпуляція прийняттям рішення	Захист від отладки
	Заміна компонентів	“Підписані” компоненти

Таблиця 2.5 – Загрози, методи протидії етапу верифікації

Елемент системи	Загроза	Міра нейтралізації
Додаток (верифікація)	Шкідливий код	Відповідність стандартам (BioAPI, CBEFF) Підписання коду)

BioAPI - стандарт BioAPI Consortium. Розроблений спеціально для уніфікації програмних інтерфейсів програмного забезпечення розробників біометричних пристроїв.

CBEFF (англ. Common Biometric Exchange File Format) - єдиний формат уявлення біометричних даних, який був запропонований NIST в 2001 році для заміни біометричних форматів, використовуваних виробниками різних сегментів біометричного ринку в своєму обладнанні і програмному забезпеченні. При створенні CBEFF були враховані всі можливі аспекти його застосування, в тому числі криптографія, багатофакторна біометрична ідентифікація і інтеграція з картковими системами ідентифікації.

Таблиця 2.6 – Загрози, методи протидії етапу зберігання

Елемент системи	Загроза	Міра нейтралізації
Зберігання	Компрометація бази даних (читання біометричного шаблону, заміна шаблону, зміна зв'язки)	Захист серверів Контроль доступу до баз даних Шифрування та елекроний підпис біометричного шаблону Зберігання шаблонів на смарт-картах або інших пристроях

Таблиця 2.7 – Загрози, методи протидії етапу передачі оброблених даних

Елемент системи	Загроза	Міра нейтралізації
Передача “сирих” даних, передача оброблених даних	Перехват	Захищений канал передачі
	Повтор	Взаємна аутентифікація Підписні дані Використання тимчасових міток / Time-to-live
	“Людина посередині”	Захищений канал Прив’язка біометрії до сертифікату відкритого ключа
	Підбір / перебір	Таймаути / Блокування

Таблиця 2.8 – Загрози, методи протидії етапу пошуку біометричного шаблону

Елемент системи	Загроза	Міра нейтралізації
Пошук біометричного шаблону	Перехват	Захищений канал передачі
	Повтор	Взаємна аутентифікація Підписні дані Використання тимчасо-вих міток / Time-to-live
	“Людина посередині”	Захищений канал Прив’язка біометрії до сертифікату відкритого ключа

Таблиця 2.9 – Загрози, методи протидії етапу передачі результату порівняння

Елемент системи	Загроза	Міра нейтралізації
Передача результату порівняння	Hill-climbing	Захищений канал Довіренний сенсор (вза-ємна аутентифікація)
	Маніпуляція результатами (рейтингом) порівняння	Захищений канал Взаємна аутентифікація
	Заміна компонентів	Заміна компонентів

Таблиця 2.10 – Загрози, методи протидії етапу взаємодія з додатком (верифікатором)

Елемент системи	Загроза	Міра нейтралізації
Взаємодія з додатком (верифікатором)	Перехват	Захищений канал
	Маніпуляція з прийнятим рішенням по порівнянню	Захищений канал

ВИСНОВОК

У розділі було розглянуто види атак на системи біометричних персональних даних та аналіз методів та засобів протидії. Було знайдено спільні етапи у різних системах біометрії, та проаналізувавши види атак та загрози, були розроблені міри нейтралізації цих загроз на кожному з етапів:

1. Загрози та методи протидії етапу обробки сигналу
2. Загрози та методи протидії етапу обробки сигналу
3. Загрози та методи протидії етапу порівняння
4. Загрози, методи протидії етапу прийняття рішення
5. Загрози, методи протидії етапу верифікації
6. Загрози, методи протидії етапу зберігання
7. Загрози, методи протидії етапу передачі оброблених даних
8. Загрози, методи протидії етапу пошуку біометричного шаблону
9. Загрози, методи протидії етапу передачі результату порівняння
10. Загрози, методи протидії етапу взаємодія з додатком (верифікатором)

Біометричні системи розпізнавання представляють зручний інструмент ідентифікації людини. Однак гостро постає питання довіри до них; невідомо, наскільки добре вони захищені.

РОЗДІЛ 3.РОЗРОБКА ЗАХОДІВ БЕЗПЕКИ

3.1 Аналіз архітектури системи відеоспостереження типового підприємства

В цьому розділі буде розглядатися архітектура та захист біометричних персональних даних у корпоративній системі відеоспостереження на прикладі підприємства ТОВ “FITHAUS”.

Це підприємство використовує для захисту біометричних персональних даних систему управління відеоспостереження HikCentral.

HikCentral - система управління відеоспостереженням, контролем доступу, охоронної сигналізації, обліком робочого часу, порівнянням осіб та іншими функціями. ПО володіє широкими можливостями інтеграції зі сторонніми рішеннями забезпечення безпеки для різних вертикальних сценаріїв застосування.

Архітектура системи зображена на рисунку 3.1

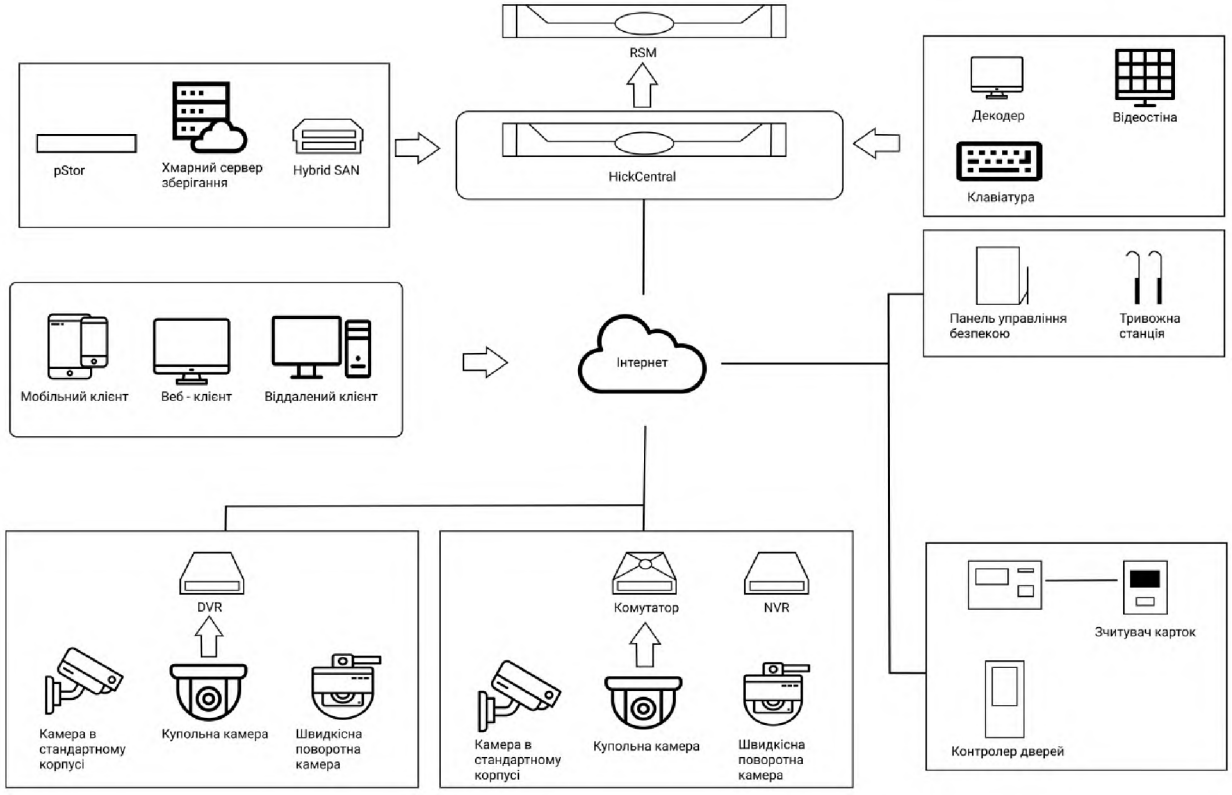

Рисунок 3.1 – Архітектура системи

Архітектура складається з декількох рівнів:

- Рівень сервера
- VSM сервер
- Потоковий сервер

Призначений для користувача рівень:

- Веб-клієнт
- Клієнт управління
- Мобільний / планшетний клієнт

Рівень пристрою:

- Підтримка камер, NVR / DVR
- Забезпечення централізованого зберігання з pStor / гібридних СГД / хмарність сервером зберігання
- Підтримка управління декодерами / відео стіни / клавіатурами
- Підтримка контролерів дверей і керування дверима / терміналів розпізнавання осіб / турнікетів Hikvision
- Підтримка панелей охоронної сигналізації і колон екстреного виклику

Структура “ТОВ FITHAUS”складається з декількох підрозділів:

- FitPRO
- Система безпеки
- Система відеоспостереження
- Система охоронної сигналізації
- Система контролю доступу
- Відділ продаж порівняння / розпізнавання осіб

Система безпеки вкючає в себе:

- Система відеоспостереження в усіх клубах
- Систему контолю доступу
- Система безпеки з підключенням на пульт охоронного агенства

Безпека: всі камери в усіх клубах підключені до відеорегістраторів.

З відеорегістраторів (по факту звернення пристроїв) через інтернет передається інформація на певні пристрої, а саме:

Система відеоспостереження може бути проглянута різними програмами від HickVision (IVMS 4200, IVMS 4500). Вони мають певні обмеження по кількості камер, та підключень. Враховуючи закладену ємність клубу, цього не достаньо.

Саме тому підприємство використовує систему HickCentral, яка в змозі зберігати більше, ніж 10000 клієнтів. Доступ до відеосистеми отримують ті, кому надається доступ через мобільний додаток. Служба безпеки має змогу спостерігати через відеостіну. У служби охорони окрім відеостіни є тривожна станція. В залежності від ситуації спрацьовує система та викликається потрібна служба.

Відділ продаж має доступ до:

- Системи порівняння/розпізнавання облич
- Системи зчитування карток
- Контролеру дверей (турнікетів)

Адже саме вони при реєстрації нового клієнта додають його до системи Face Id, При реєстрації клієнта у Face id він має змогу безперешкодно мати доступ до входу у приміщення через турнікет системи розпізнавання облич.

Система розпізнавання облич

Термінал розпізнавання осіб серії є варіантом пристрою контролю доступу для розпізнавання осіб.

Особливості продукту (Термінал розпізнавання облич)

- 7-дюймовий сенсорний РК-екран із співвідношенням сторін 16: 9 і роздільною здатністю 1024 × 600 пікселів для відображення інтерфейсу, виявлення осіб в режимі реального часу, перегляду відео в режимі реального часу і т. Д.
- Ширококутний об'єктив з дозволом 2 000 000 пікселів
- Ручне або автоматичне регулювання яскравості підсвічування

- Аутентифікація по QR-коду
- Відстань розпізнавання осіб: 0,3 ... 1 м
- Передбачувана висота розпізнавання осіб: 1,4 ... 1,9 м
- Виявлення живих осіб: Виявлення та розпізнавання відбувається тільки для живих осіб
- Алгоритм глибинного навчання
- Зберігання не більше 10 000 зображень осіб
- Тривалість розпізнавання осіб становить ≤0,5 с / користувач; точність розпізнавання осіб - ≥99%
- Управління параметрами пристрою, пошук і налаштування
- Імпортує призначені для користувача дані і дані карти на пристрій через протокол TCP / IP або USB-накопичувач
- Автономна робота
- Передача даних (результатів перевірки автентичності і захоплених зображень) в клієнтське програмне забезпечення через TCP / IP і збереження даних в клієнтському програмному забезпеченні
- Прив'язка і збереження захоплених зображень
- Імпорт даних (зображень облич і шаблонів осіб) на пристрій за допомогою USB накопичувача або з клієнтського програмного забезпечення
- Експорт даних (зображень облич, подій і знімків) з пристрою за допомогою USB накопичувача
- Управління, пошук і установка даних пристрою після реєстрації на сервері системи • Підключення до одного зовнішнього пристрою для зчитування карт або контролера доступу по протоколу RS-485
- Підключення до контролера зовнішнього доступу або інтерфейсу Wiegand через протокол Wiegand
- Підключення до блоку управління дверима по протоколу RS-485, щоб уникнути відкриття дверей в разі знищення терміналу

Зовнішній вигляд терміналу розпізнавання облич зображений на рисунку 3.2

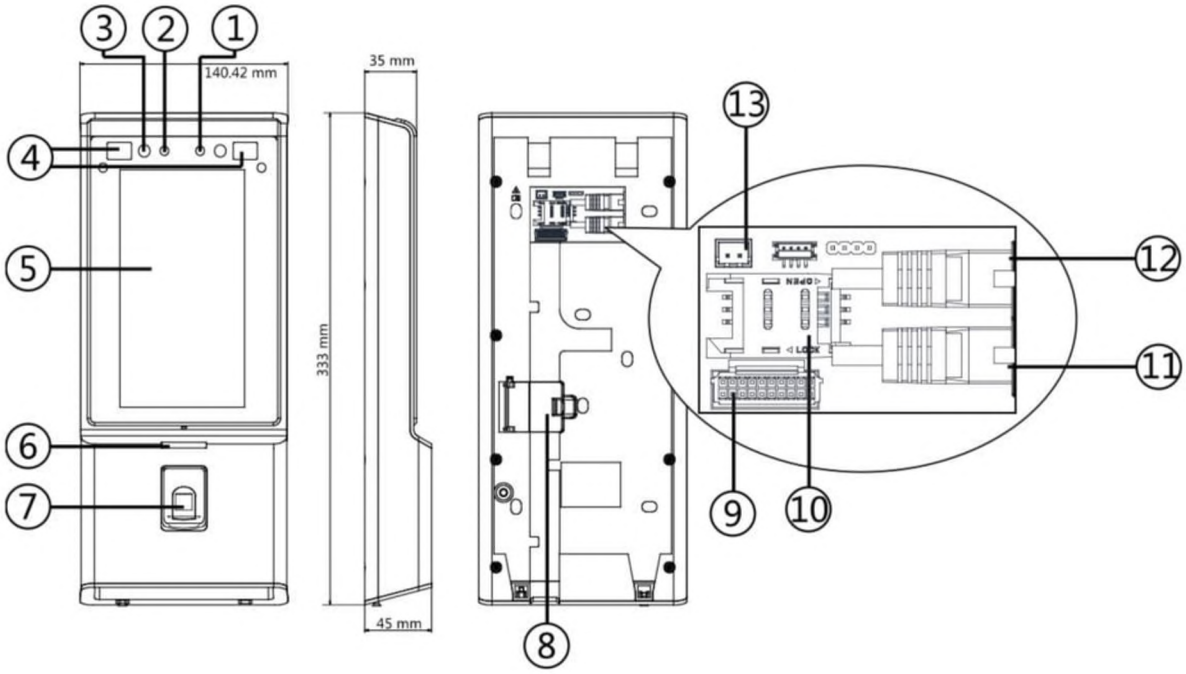

Рисунок 3.2 - Зовнішній вигляд терміналу розпізнавання облич

Таблиця 2.8 – Опис системи терміналу розпізнавання облич

Назва	Опис системи терміналу розпізнавання облич
Камера (Біле світло)	Камера білого світла для запису або зйомки відео або зображень при білому світі.
Камера (ІК – світло)	Камера ІК-світла для запису або зйомки відео або зображень в ІК-світлі
Додаткова підсвітка (Біле світло)	Додаткове підсвічування для камер білого світла
Екран	7-дюймовий сенсорний РК-екран з роздільною здатністю 1024 × 600.

Назва	Опис системи терміналу розпізнавання облич
Індикатор	Безперервне свічення червоним кольором: Режим очікування. Миготіння червоним кольором: Помилка при аутентифікації. Безперервне свічення зеленим кольором: Аутентифікація пройдена успішно. Блимання зеленим кольором: Аутентифікація (комбінована).
Роз'єм для PSAM-карти	Вставка PSAM-карти. PSAM-карта являє собою карту з модулем безпечного доступу, який підтримує кілька методів безпечного надання доступу і дозволів. Вона також забезпечує встановлення безпечного зв'язку.
Клеми	Підключення до інших зовнішніх пристроїв, включаючи зчитувач карт RS-485, зчитувач карт Wiegand, дверний замок, вхід / вихід сигналу тривоги і т.д.
Слот для Micro SIM-карти	Забезпечує можливість використання SIM карт.
Мережевий інтерфейс	Підключення до мережі Ethernet.
Інтерфейс подачі живлення	Підключення до джерела живлення.

Спільно з інтелектуальними пристроями Hikvision, HikCentral надає потужні функції:

- Захоплення і порівняння осіб;
- Відображення захопленого зображення особи в реальному часі (включаючи камери, які не що знаходяться в режимі реального часу);

- Пошук тільки по співпалим зображенням по групі порівняння осіб;
- Відправка повідомлення про тривогу, викликану збігом або розбіжністю зображень осіб;
- Відображення збігшихся осіб з кожної групою порівняння в режимі реального
- часу;
- Пошук по всім захопленим зображенням і виконання вторинного пошуку (включаючи камери віддалених об'єктів);
- Пошук тільки по співпалим зображенням по групі порівняння осіб;
- Відправка повідомлення про тривогу, викликану збігом або розбіжністю зображень осіб;

Обладнання, яке використовується на підприємстві:

Рис 3.3 - 4 Мп IP видеокамера Hikvision DS-2CD2443G0-IW (2.8 MM)

Рис 3.4 - DS-2CD2543G0-IS (2.8 MM) 4МП міні IP відеокамера Hikvision з ІК підсвічуванням

Рис 3.5 - DS-2CD2T43G0-I8 (4 MM) 4 Мп IK відеокамера Hikvision

Рис 3.6- DS-2CD2143G0-IS (2.8 MM) 4 Мп IK купольна відеокамера Hikvision

Рис 3.7 - DS-2CD2643G0-IZS (2.8-12 MM) 4 Мп IK мережева відеокамера з моторизованим об'єктивом

Рис 3.8 - DS-2CD2T45FWD-I8 (4 MM) 4 Мп IP видеокамера Hikvision с WDR

Рис 3.9 - Мережевий реєстратор HikVision DS-7632NI-K2

Рис. 3.10 - Комплект для розпізнавання осіб DS-K5603-Z

Рис 3.11 - Термінал розпізнавання обличчя DS-K1T500S

Рис 3.12 - Тумбовий распашний турнікет DS-K3M200-601

Рис. 3.13 - Викликаюча панель Hikvision DS-K1T500S

3.2 Модель порушника функціонування системи

Порушник – фізична особа (у загальному випадку не обов'язково користувач системи), яка здійснює порушення політики безпеки системи.

Нормативними документами України («Типове положення про службу захисту інформації в автоматизованій системі») рекомендовано таку структуру опису загрози:

На порушення яких властивостей інформації або АС спрямована загроза:

Порушення конфіденційності;

- Порушення цілісності;
- Порушення доступності інформації;
- Порушення спостереженості та керованості АС.

Джерела виникнення загрози:

Суб'єкти АС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу

Можливі способи здійснення загрози:

- Технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;
- Каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;
- Несанкціонованим доступом шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп'ютерних вірусів.

Перші два способи за принципом відносяться до фізичного доступу, останній – до логічного доступу.

Модель порушника– це всебічна структурована характеристика порушника, яка використовується сумісно з моделлю загроз для розробки політики безпеки інформації. В Україні прийнята така структура моделі порушника:

Категорія осіб, до якої може належати порушник:

- Внутрішні порушники;
- Користувачі,
- Інженерний склад,
- Співробітники відділів, що супроводжують ПЗ,
- Співробітники служби безпеки,
- Керівники;
- Зовнішні порушники.

Мета порушника:

- Отримання необхідної інформації;
- Отримання можливості вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

- Нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Повноваження порушника в АС:

- Запуск фіксованого набору задач (програм);
- Створення і запуск власних програмних засобів;
- Керування функціонуванням і внесення змін у конфігурацію системи;
- Підключення чи зміна конфігурації апаратних засобів.

Технічна оснащеність порушника:

- Апаратні засоби;
- Програмні засоби;
- Спеціальні засоби.

Модель порушника:

1) Можливий порушник – Співробітник

Можливий мотив:

- Безвідповідальність
- Самозатвердження
- Корисливий мотив

Обізнаність, які (не) має порушник:

- Знає функціональні особливості системи
- Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
- Знає структуру, функції й механізми дії засобів захисту, їх недоліки.
- Знає недоліки та “вади” механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості.
- Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.

2) Можливий порушник – Найманий хакер

Можливий мотив:

- Корисливий мотив

Обізнаність, які (не) має порушник:

- Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
- Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації систем відео нагляду.
- Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування

3) Можливий порушник – Хакер

Можливий мотив:

- Самозатвердження
- Корисливий мотив

Обізнаність, які (не) має порушник:

- Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
- Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
- Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації систем відео нагляду.

3.3 Розробка контрзаходів

В ході роботи були представлені різні атаки на біометричні персональні дані у корпоративних системах відеоспостережння. У більшості випадків пов'язаних з атаками на системи не вдається виявити шахраїв так як вони використовують шифрування даних.

Досить часто при підключенні систем та при під’єднанні хмарного носія співробітники нехтують таким важливим фактором як шифрування бездротового з’єднання.

Таким чином на даний час одним з ключових факторів боротьби з атаками на системи відеоспостереження в першу чергу є комплексна система захисту інформації.

Система комплексного захисту забезпечує виконання таких функцій:

1. Захист від незахищених каналів передачі інформації
2. Розробка і відладження порядку обробки інформації
3. Захист від несанкціонованого доступу до хмарного сховища
4. Своєчасна передача інформації для збереження
5. Постійні заходи з проведення навчання обслуговуючого персоналу
6. Своєчасне оновлення програмного забезпечення системи
7. Постійні оновлення кодів доступу до систем.

3.4 Розробка методики протидії типовим атакам

Протидія атакам спуфінгу

Потенційну загрозу представляють атаки спуфінгу (spoofing).

Спуфінг - це обман біометричних систем шляхом надання біометричного сенсора копій, муляжів, фотографій, відрізаних пальців, заздалегідь записаних звуків і т. п. Мета атаки спуфингу аутентифікації - уявлення незаконного користувача в системі як законного, а при ідентифікації – домогтися невиявлення індивідуума, що міститься в базі даних (БД).

Заходи антиспуфінгу в біометричних системах включають такі методи:

1) Рандомізація даних верифікації

Система може рандомізувати відбитки пальців або вирази облич, запитуваних для верифікації. Це зменшує ймовірність надання фальшивих біометричних зразків для верифікації.

2) Використання декількох біометричних зразків

У процесі реєстрації в системі на кожного користувача реєструється, наприклад, кілька відбитків пальців (в ідеалі всі 10). Після цього в процесі

аутентифікації у користувача запитуються для перевірки кілька пальців в до-вільній послідовності, що значно ускладнює вхід в систему за фальшивими пальцях.

3) Мулипімодальна біометрія.

Для виявлення живучості можна використовувати кілька біометричних характеристик одночасно, наприклад відбиток пальця і форма особи або райдужна оболонка ока і т. д. Це створює для зловмисника труднощі сфальсифікувати кілька біометричних характеристик одночасно, ніж чим одну характеристику.

4) Мультифакторна аутентифікація.

Мультифакторна аутентифікація, яка використовує поряд з біометрією смарт-карти, токени або паролі, може зменшити ймовірність обману біометричних систем. В цьому випадку для обману останньої зловмисникові разом з фальшивими біометричними даними потрібні додаткові ідентифікатори. але мультифакторна аутентифікація також зменшує основна перевага біометричних систем – зручність використання.

5) Контроль над процесом аутентифікації (ідентіфікації).

Контроль над операціями біометричних систем може підвищити рівень безпеки системи. Зрозуміло, що зробити атаку спуфингу проти контрольованої біометричної системи в цьому випадку важче.

6) Запит - відповідь.

У методі запит - відповідь користувача просять подивитися на щось, прослухати або відчути щось, а потім у відповідь зробити щось. Запит, що вимагає один відповідь з декількох можливих, може ускладнити просте відтворення сигналів, заздалегідь записаних зловмисником. Як приклад можна привести зміну виразу обличчя (посміхнутися або хмуритися)

7) Виявлення живучості.

Мета виявлення живучості в біометричних системах полягає в тому, щоб переконатися, що для реєстрації, та ідентифікації використовуються тільки "справжні" біометричні дані. У методах виявлення живучості в якос-

ті ознак життя використовується фізіологічна або поведінкова інформація або інформація, що міститься в біометричний зразку. В системах розпізнавання відбитків пальців для виявлення живучості використовуються вимір температури, пульсу, діелектричного опору, виявлення підшкірних ознак, порівняння послідовно прийнятих біометричних зразків і т. д.

Для інших біометричних характеристик методи виявлення живучості, як правило, ґрунтуються на аналізі довільного і мимовільного поведінки. Системи розпізнавання обличчя можуть вимагати від користувача руху голови, губ, очей або зміни виразу обличчя.

Протидія атакам SYN-Flood

Як вже було зазначено вище атака SYN-Flood є однією з типових атак при використанні систем обробки біометричних персональних даних.

SYN-флуд - одна з різновидів мережевих атак типу відмова від обслуговування, яка полягає у відправці великої кількості SYN-запитів (запитів на підключення по протоколу TCP) в досить короткий термін.

Згідно процесу «триразового рукостискання» TCP, клієнт посилає пакет зі встановленим прапором SYN (synchronize). У відповідь на нього сервер повинен відповісти комбінацією прапорів SYN + ACK (acknowledges). Після цього клієнт повинен відповісти пакетом з прапором ACK, після чого з'єднання вважається встановленим.

Атака ґрунтується на вразливості обмеження ресурсів операційної системи для напіввідкритих з'єднань, описаної в 1996 році групою CERT, згідно з якою чергу для таких підключень була дуже короткою (наприклад, в Solaris допускалося не більше восьми підключень), а тайм-аут підключень - досить тривалим (по RFC один тисяча сто двадцять дві - 3 хвилини).

Запропонованим рішенням було використання SYN cookie, або обмеження запитів на нові підключення від конкретного джерела за певний проміжок часу. Мережевий протокол транспортного рівня SCTP, який є більш сучасним порівняно з TCP, використовує SYN cookie і не схильний до SYN-флуд-атакам.

SYN cookie - техніка протидії SYN-флуд-атаці. Винахідник техніки Daniel J. Bernstein. Визначив SYN cookie як «Особливий вибір початкової TCP-послідовності з боку сервера».. Використання SYN cookie дозволяє серверу уникати скидання нових з'єднань, коли черга TCP-з'єднань переповнена. Сервер відправляє назад клієнту правильну послідовність SYN + ACK, але не зберігає нове з'єднання в черзі. Якщо сервер потім отримає ACK відповідь від клієнта, то він зможе відновити своє значення SYN послідовності за прийнятим від клієнта значенням.

Прості міжмережеві екрани, які дозволяють будь-який вихідний трафік і дозволяють вхідний трафік тільки до певних портів, блокуватимуть SYN-запити тільки до закритих портів. Якщо SYN cookie включені, то необхідно звернути увагу, що зловмисник не може обійти такі міжмережеві екрани відправкою ACK-пакетів з довільним номером послідовності поки не підбере правильний. SYN cookies потрібно включати тільки для публічно доступних портів.

3.5 Рекомендації щодо безпечного користування системами обробки біометричних персональних даних

Рекомендації щодо безпечного користування системами обробки біометричних персональних даних:

1. Використовувати засоби захисту інформації сучасних класів та сертифіковані;
2. Виключити зберігання біометричних даних на автоматизованому робочому місці, призначеному для збору і обробки біометрії, після завершення реєстрації даних;
3. Забезпечити реєстрацію доступу уповноважених співробітників до об'єктів системи збору біометрії , реєстрацію передачі електронних повідомлень з біометричними даними між структурними підрозділами підприємства та інше.

ВИСНОВОК

У розділі було розглянуто аналіз архітектури системи відеоспостереження типового підприємства, модель порушника функціонування системи, розробка контрзаходів, розробка методики протидії типовим атакам, рекомендації щодо безпечного користування системами обробки біометричних персональних даних. Будь-які персональні дані, в тому числі і біометричні, не можуть бути повністю захищені від розкрадання. Максимум, що можна зробити - це проектувати системи, які знецінюють вкрадені дані.

Ряд біометричних характеристик є публічними. Наприклад, наше обличчя можна сфотографувати, а голос - записати на диктофон.

Для забезпечення довіри користувачів до біометричної ідентифікації необхідно забезпечити надійність і безпеку використовуваних систем.

РОЗДІЛ 4. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою розділу є обґрунтування економічної доцільності створення методик протидії типовим атакам на системи обробки біометричних персональних даних. Щоб визначити ефектвність необхідно розрахувати:

- Капітальні витрати на розробку, впровадження та підтримку методик;
- Трудомісткість витрати на розробку,впровадження та підтримку методик, а також трудомісткість на підтримку захисту біометричеих персональних даних;
- Річні експлуатаційні витрати на впровадження та підтримку захисту біометричних персонаьних даних;
- Показники економічної ефективності.

4.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції:

1. Вартість розробки проекту інформаційної безпеки (розробка схем пристроїв, політики функціонування системи тощо);
2. Вартість створення основного й додаткового програмного забезпечення (ПЗ);
3. Витрати на первісні закупівлі апаратного забезпечення;
4. Витрати на навчання технічних фахівців і обслуговуючого персоналу.

Спершу розрахуємо час, який буде витрачено на створення ПЗ:

$$t = tmз + tв + tа + tпр + tопр + tд, \text{ годин,} \qquad (3.1)$$

де $tmз$ – тривалість складання технічного завдання на розробку ПЗ;

$tв$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$tа$ – тривалість розробки блок-схеми алгоритму;

$tпр$ – тривалість програмування за готовою блок-схемою;

$tonp$ – тривалість опрацювання програми на ПК;

$tд$ – тривалість підготовки технічної документації на ПЗ.

Умовна кількість оперантів у програмі:

$$Q = q \cdot c\,(1 + p), \quad \text{штук}, \tag{3.2}$$

де q – очікувана кількість операторів - 4; c – коефіцієнт складності програми - 2;

p – коефіцієнт корекції програми в процесі її опрацювання - 0.05.

$$Q = 4 \cdot 2(1 + 0.05) = 8{,}4, \text{ штук}.$$

Оцінка тривалості складання технічного завдання на розробку ПЗ ttз– 3 год. Тривалість вивчення технічного завдання:

$$t_B = \frac{Q*b}{(75...85)*k} = \frac{8.4*1.2}{75*0.8} = 0.168, \text{годин} \tag{3.3}$$

де B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, B = 1,2...1,5; k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом: до 2 років – 1,0;

Тривалість розробки блок-схеми алгоритму:

$$t_a = \frac{Q}{(20...25)*k} = \frac{8{,}4}{20*0.8} = 0.525, \text{годин} \tag{3.4}$$

Тривалість складання програми за готовою блок-схемою:

$$tпр = \frac{Q}{(20...25)\cdot k} = \frac{8{,}4}{20\cdot 0.8} = 0.525, \text{ годин}. \tag{3.5}$$

Тривалість опрацювання програми на ПК:

$$tonp = \frac{2Q}{(4...5)\cdot k} = \frac{2 \cdot 8.4}{4\cdot 0.8} = 5.25, \text{ годин}. \tag{3.6}$$

Тривалість підготовки технічної документації на ПЗ:

$$t_д = \frac{Q}{(15...20)} + \frac{Q}{15...20} \cdot 0,75 = \frac{8.4}{} + \frac{8.4}{} \cdot 0.75 = 0.945, \text{ годин.} \quad (3.7)$$

t = 4 + 0.189 + 0.591 + 0.591 + 4.43 + 1.261=11.413 годин.

Розрахунок витрат на створення програмного продукту

$$К_{пз} = З_{зп} + З_{мч}. \text{ грн} \quad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 11.413 \cdot 22.024 = 251.359, \text{ грн,} \quad (3.9)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр– средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_м}{168} = \frac{3700}{168} = 22.024, \text{ грн/годину.} \quad (3.10)$$

де $З_м$ – середня заробітна плата на місяць – 3700грн.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_д = 1.466 \cdot 5.25 + 0.945 = 8.6415, \text{грн.} \quad (3.11)$$

$$З_{мч} = (t_{опр} \times С_{мч} + t_д),$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_{Д}$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t_{нал} \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p}$$

$$C_{мч} = 0.5 \cdot 2.1 + \frac{4000 \cdot 0.1}{1920} + \frac{800 \cdot 0.5}{1920} = 1.466, \text{ грн/год.} \quad (3.12)$$

де Р – встановлена потужність ПК, 0.5 кВт;

C_e – тариф на електричну енергію, 2.1грн/кВт·година; $Ф_{зал}$ – залишкова вартість ПК на поточний рік, 4000 грн.; H_a – річна норма амортизації на ПК, 0.1 частки одиниці;

$H_{апз}$–річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

F_p– річний фонд робочого часу (за 40-годинного робочого тижня F_p= 1920 год).

$$K_{пз} = 251.359 + 8.6415 = 224 \text{ грн.} \quad (3.8)$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$K = K_{пз} + K_{навч} + K_{н}, \text{ тис. грн.} \quad (3.13)$$

де $K_{пз}$ – вартість створення програмного продукту, тис. грн;

$K_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$K_{н}$ – витрати на встановлення обладнання та налагодження системи

інформаційної безпеки, тис. грн.

Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень, що складають 3 тис. грн;

$К_{навч} = 3$ тис. грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають, 0.8 тис. грн.

$К_н = 0.8$ тис. грн.

$$К = 0.2 + 3 + 0.8 = 4 \text{ тис. грн.} \quad (3.13)$$

4.2 Експлуатаційні витрати:

$$С_к = С_н + С_а + С_з + С_{єв} + С_е + С_{ел} + С_{тос} \quad (3.14)$$

де витрати на навчання персоналу й кінцевих користувачів ($С_н$). визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації – 1тис. грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) – 20% або1317 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} = 3723 \cdot 12 + 3723 \cdot 0.22 \cdot 12 = 54\,504{,}72 \text{ грн.} \quad (3.15)$$

де $З_{осн}$, $З_{дод}$– основна мінімальна заробітна плата на рік 01.01.2019, грн на Єдиний соціальний внесок – 0.22, частки одиниці;

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0.5 \cdot 365 \cdot 24 \cdot 2.1 = 9\,198 \text{грн,} \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення вторгнень визначаються у відсотках від вартості капітальних витрат 20%. А саме:

$$С_{тос} = К \cdot 0.2 = 0.8 \text{ грн}$$

$$Ск = 1 + 1.317 + 54.504 + 9.198 + 0.8 = 66{,}819 \text{ , тис. грн.} \quad (3.14)$$

4.3 Оцінка можливого збитку від атаки (злому) на вузол корпоративної мережі

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

1. порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);
2. порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);
3. порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);
4. порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Вихідні дані:

$t_п$ =72 годин – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$=12годин – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$=6 годин – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі,

годин;

$З_о$=3723грн – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$=4300 грн – місячна заробітна плата співробітника атакованого вузла корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$=2 – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$=3 – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О = 30 000 грн – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$П_{зч}$ = 4000 грн – вартість заміни встаткування або запасних частин, грн;

I=1 – число атакованих вузлів або сегментів корпоративної мережі; N = 40 – середнє число можливих атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_{П} + П_{В} + V, \text{ грн.} \quad (3.15)$$

де $П_{П}$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_{В}$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за 60 годин простою внаслідок атаки:

$$Пп = \frac{\sum Зс \cdot Чс}{F} \cdot t_{П}, \quad (3.16)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

$$П_{п} = \frac{\sum 4300 \cdot 3}{160} \cdot 48 = 3870, \text{грн.}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_{В} = П_{ВИ} + П_{ПВ} + П_{ЗЧ}, \text{ грн.} \quad (3.17)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$– витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати 4300 грн 3 співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$=6:

$$П_{ви} = \frac{\sum 4300}{160} \cdot 6 = 161.25, \text{грн.} \quad (3.18)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ = 12 і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum 3723}{160} \cdot 12 = 279.225, \text{грн.} \quad (3.19)$$

$$П_в = 161.25 + 279.225 + 4000 = 4440.51 \text{ грн.} \quad (3.17)$$

Втрати від зниження очікуваного обсягу продаж в 200 000 грн за 90 годин простою атакованого вузла або сегмента корпоративної мережі виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви}) = \frac{30000}{9340} \cdot (72 + 12 + 6) = 289.08, \text{ грн} \quad (3.20)$$

де $F_г$ – річний фонд часу роботи організації становить близько 9340 ч.

$$U = П_п + П_в + V = 3870 + 4440.51 + 289.08 = 8599.59 \text{ грн.} \quad (3.15)$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum_i \sum_n U = 8599.59 \cdot 35 \cdot 1 = 300985.65 \text{ грн.} \quad (3.21)$$

4.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C = 300985.65 \cdot 0.6 - 66.819 = 180524.57 \text{ грн,} \quad (3.22)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузолабо сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

4.5 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{E}{K} = \frac{180.524}{4} = 45.131, \text{частки одиниці,} \quad (3.23)$$

Де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Термін окупності: To=K/E=1/ROSI=0.022роки

4.5 Висновок

В економічному розділі у результаті розрахованих витрат потрібних на

реалізацію створення основного й додаткового програмного забезпечення, розробки проекту інформаційної безпеки, була доведена економічна ефективність і період окупності витрат.

Розрахунок (фіксованих) капітальних витрат:

1) Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 4 тис.грн

2) Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень складають 3 тис. грн;

3) Вартість машинного часу для налагодження програми на ПК складає 8.6415,грн.

Експлуатаційні витрати:

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення вторгнень становлять 66,819 , тис. грн.

Оцінка можливого збитку від атаки (злому) на вузол корпоративної мережі

Загальний збиток від атаки на вузол, або сегмент корпоративної мережі становить 300985.65 грн.

Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить 180524.57 грн,

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Термін окупності: 80 днів

Проект економічно доцільний та його можно використовувати на підприємстві.

ВИСНОВОК КВАЛІФІКАЦІЙНОЇ РОБОТИ

Проблема захисту біометричних персональних даних на даний момент є однією з ключових проблем.

Як звичайні користувачі не хочуть втратити свої біометричні персональні дані і не стати жертвою шахрайства, так і підприємства бажають зберегти свою репутацію.

З кожним днем з'являються все нові, більш вдосконалені атаки на системи обробки біометричних персональних, в основному вони базуються на вже існуючих видах атак.

Існують різні причини, за якими збір і зберігання певних біометричних характеристик може стати неприйнятним для суспільства.

Наприклад, зняття відбитків пальців на паперовий носій традиційно асоціюються з розслідуванням злочинів.

Для багатьох істотним є і те, що розпізнавання за папілярними узорами пальців (контактний спосіб) вимагає дотику до контактого місця сканера, якого перед тим торкалися інші особи.

Суттєвий аспект – наскільки проста («комфортна») кожна технологія. Процес повинен бути швидким і простим, наприклад, встати перед відеокамерою, сказати декілька слів у мікрофон або доторкнутися до відведеного місця у сканері відбитків пальців.

Головною вимогою до біометричних технологій, яка і є їхньою суттєвою перевагою, є швидка і проста ідентифікація без спричинення яких-небудь незручностей людині.

Відеоаналітіка в системах відеоспостереження не стоїть на місці, таким функціоналом, як вихід з периметра, пропажа предмета з області, детекция пішоходів та інше, вже нікого не здивувати.

На зміну приходять все більш інтелектуальні сценарії і функції.

Для забезпечення довіри користувачів до біометричної ідентифікації необхідно забезпечити надійність і безпеку використовуваних систем.

Щоб ставлення користувачів до систем біометричної ідентифікації стало довірливішим, краще пропонувати рішення, в яких для підтвердження особи треба, наприклад, подивитися безпосередньо в об'єктив камери або на певну мітку. Це усуне побоювання на рахунок прихованого стеження і несанкціонованого контролю.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бурячок, В. Алгоритм оцінювання ступеня захищеності спеціальних інформаційно – телекомунікаційних систем [Текст] / В. Л. Бурячок // Захист інформації. НАУ. - К. – 2011. - №3. – С. 1-9.

2. Болл, Р. Руководство по биометрии [Текст] / Болл Р.М., Коннел Дж.Х., Панканти Ш., Ратха Н.К., Сеньор Э.У. – М. : Техносфера, 2007. - 368 с. - ISBN 978-5- 94836-109-3, 0-387-40089-3.

3. Гарасим, Ю. Дослідження та аналіз перспективних технологій ідентифікації особи в захищених корпоративних мережах зв'язку [Текст] / Ю. Р. Герасим, Т. Б. Крет. // Системи обробки інформації. / Харківський університет Повітряних Сил. – 2010, вип. 3(84). – С. 7-10. – ISSN 1681-7710

4. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листоп. 2001 р Міжнародний пакт про громадянські і політичні права [Електронний ресурс] : Міжнародний пакт від 16 груд. 1966 р.

5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи № 108 від 28 січ. 1981 р.

6. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. [Текст] // Математичні машини і системи / Інститут проблем математичних машин і систем НАН України. – 2011. - №1. – С. 39- 45. – ISSN 1028-9763.

7. Лисенко А.М., Мельник О.С. Застосування біометричних систем для ідентифікації особи [Текст] // Вісник Київського національного університету ім. Т. Шевченка, серія «Юридичні науки». – 2004. - №60- 62. – С. 87 – 91.

8. Обуховська Т. І. Персональні дані: теорія та реальність / Т. І. Обуховська, В. П. Шуляк // Електронне урядування. – 2011. – № 2. – С. 76–88.

9. Обуховська Т. І. Нормативно-правове забезпечення обробки та циркуляції персональних даних / Т. І. Обуховська // Вісн. НАДУ. – 2011. – № 4. – С. 119–126.

10. Права человека и защита персональных данных / [А.А. Баранов, В.М. Брыжко, К. Базанов]. – Харьков: ХПГ-Фолио, 2000. – 280 с. – (Издана при содействии Харьковской правозащитной группы и Национального фонда поддержки демократии США).

11. Про захист осіб у зв'язку з обробкою персональних даних та вільним обігом цих даних [Електронний ресурс] : Директива 95/46/ЄС Європейського парламенту та Ради від 24 жовт. 1995 р.

12. Про обробку персональних даних і захист прав осіб у телекомунікаційному секторі [Електронний ресурс] : Директива 97/66/ЄС Європейського парламенту та Ради від 15 груд. 1997 р.

13. Проценко В.А. Особливості механізмів захисту персональних даних в законодавстві ЄС // Правова інформатика. – № 2(34)/2012. – С. 45

14. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування суспільних інформаційних відносин у зв'язку з автоматизованою обробкою даних у правоохоронній діяльності : посібник. – Кн. 2 / [В. Брижко, М. Швець та ін.] ; за ред. д.е.н., професора М. Швеця. – К. : ТОВ "Пан Тот", 2006 р. – 509 с.

15. Теремецький В.І., Цвірюк Д.В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні / Часопис Академії адвокатури України. – Т. 7. – № 2(23)2014.

16. Чернобай А.М. Правові засоби захисту персональних даних працівника : дис. На здобуття наук. ступеня канд. юрид. наук : спец. 12.00.05 / Антонина Миколаївна Чернобай. – Одеса : Нац. юридична академія, 2006. – 203 с.

17. Павленко Д. Як захистити персональні дані [Електронний ресурс] / Д. Павленко. – Режим доступу : http://www.epravda.com.ua/columns/2011/09/30/300156/

18. Про захист персональних даних [Електронний ресурс] : Закон України № 2297-VI від 1 черв. 2010 р. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/ main.cgi?nreg=2297-17

19. Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення [Електронний ресурс] : Постанова Кабінету Міністрів України від 25 трав. 2011 р. №616. – Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/ main.cgi?nreg=616-2011-%EF

20. Про захист прав людини і основоположних свобод [Електронний ресурс] : Конвенція від 4 листоп. 1950 р. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_004

21. Schuckers S. A. C. Spoofing and Anti-Spoofing Measures//Information Security Technical Report, Elsevier. 2002. V. 7. No 4. P. 56-62.

22. Antonelli A., Cappelli R., Maio D., Maltoni D. Fake finger detection by skin distortion analysis//IEEE Transactions on Information Forcnsics and Security. V. 1. Issue 3. 2006.

23. Deng G., Coo B., Miao J., Gao W., Zhao D. A Liveness Check Algorithm Based on Eye Movement Model Using SVM// The Chinese Journal of Computer aided design and computer graphics (in Chinese language). 2003. V. 15. No. 7. P. 853-857.

24. Baldissera D., Franco A., Maio D., Maltoni D. Fake Fingerprint Detection by Odor Analysis//Proceedings of International Conference on Biometric Authentication 2006 — ICBA06, Lecture Notes in Computer Science, 2006. V. 3832. P. 265-272

25. Nixon K. A., Rowe R. K., Allen J., Corcoran S. et al. Novel spectroscopy-based technology for biometric and liveness verification//Proc. SPIE. Biometric Technology for Human Identification, 2004. V. 5404. P. 287-295.

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Зміст	2	
3	А4	Вступ	2	
4	А4	1 Розділ	42	
5	А4	2 Розділ	11	
6	А4	3 Розділ	17	
7	А4	Економічний розділ	10	
8	А4	Висновки	2	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік файлів на електронному носії

1. Пояснювальна Записка.docx
2. Презентація_Диплом.ptt

ДОДАТОК В. Відгук керівника економічного розділу

Керівник: _____ к.е.н, доц. Пілова Д. П.
(підпис)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студентки групи 125м-19-2
Кучугурної Валерії Андріївни
на тему: «Захист біометричних персональних даних
у корпоративних системах
відеопостереження»

Пояснювальна записка складається зі вступу, чотирьох розділів і висновків, викладених на 108 сторінках.

Метою кваліфікаційної роботи є удосконалення захисту інформації у системах захисту біометричних персональних даних.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення поставленої мети в кваліфікаційній роботі вирішуються наступні задачі: аналіз нормативно-правової бази у сфері забезпечення кібербезпеки, аналіз методів біометричної ідентифікації, визначення основних загроз та атак на системи біометричної ідентифікації та розроблені методики протидії типовим атакам на них.

Практичне значення результатів кваліфікаційної роботи полягає у підвищенні ефективності процесу захисту біометричних персональних даних, за рахунок розроблених рекомендацій.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з незначними відхиленнями від стандартів.

Недоліком роботи відсутність достатньо аргументованих висновків в підрозділах та розділах роботи.

В цілому за час дипломування Кучугурна В.А. проявила себе фахівцем, здатним вирішувати поставлені задачі та заслуговує присвоєння кваліфікації магістр за спеціальністю 125 Кібербезпека, освітньо-професійної програми «Кібербезпека».

Рівень запозичень у кваліфікаційній роботі не перевищує вимог "Положення про систему виявлення та запобігання плагіату".

Кваліфікаційна робота заслуговує оцінки «задовільно»/70б.

Керівник кваліфікаційної роботи Т.С. Кагадій

Керівник спец. Розділу Ю. А. Мілінчук