ВСЕУКРАЇНСЬКИЙ КОНКУРС СТУДЕНТСЬКИХ НАУКОВИХ РОБІТ З ПРИРОДНИЧИХ, ТЕХНІЧНИХ ТА ГУМАНІТАРНИХ НАУК

СТУДЕНТСЬКА НАУКОВА РОБОТА

УДОСКОНАЛЕННЯ МЕТОДУ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ

Шифр: Роспізнавання

Галузь наук: Інформаційні технології

Харків – 2019

АНОТАЦІЯ

Шифр: "РОЗПІЗНАВАННЯ"

Галузь: Інформаційні технології

Актуальність теми ідентифікації особистості людини обумовлена активною інформатизацією суспільства та збільшенням потоків конфіденційної інформації. Аналіз сучасних методів підвищення інформаційної безпеки свідчить про очевидний рух у бік біометричних методів завдяки їх зручності, надійності та достовірності.

Мета роботи — визначення найбільш ефективного методу підвищення інформаційної безпеки, розробка методу підвищення інформаційної безпеки інформаційно-телекомунікаційної системи.

Завдання наукової роботи полягає в дослідженні методів підвищення інформаційної безпеки.

Використана методика дослідження. В роботі використовувались методи аналізу текстів на основі семантичного диференціала та метод фонетичного аналізу семантичної складової.

Виявлено, що створення системи захисту інформації з використанням біометричних методів ідентифікації користувачів зменшить вплив «людського» фактору що підвищить ефективність процедур ідентифікації й аутентіфікації. Пропонується для збільшення ефективності роботи системи захищати інформацію за допомогою стеганографічного методу.

Загальна характеристика роботи. Робота включає 3 розділи, висновки, літературу. Обсяг роботи 31 сторінок, рисунків - 9, джерел інформації - 9.

Ключові слова: біотехнолгії, ідентифікація, аутентифікація,верифікація, системи доступу, шаблон, зіставлення, сховище даних.

ЗМІСТ

ВСТУП

У сучасному інформаційному суспільстві актуальним для кожної країни є прагнення загальної цифрової ідентифікації громадян. Впровадження для кожної людини обов'язкових атрибутів – ідентифікаційного коду, електронного цифрового підпису, паспортних даних, номеру соціального страхування – потребує надійної ідентифікації, пов'язаної з біологічними особливостями людини (статичними та динамічними), на основі яких можна встановити її особистість у розподілених інформаційних мережах. Біометричні розробки впроваджувались вже не один десяток років, але до цього часу застосовувалися переважно в критичних інформаційних структурах, доступ до яких мала обмежена кількість людей.

Об'єкт дослідження — методи підвищення інформаційної безпеки.

Науково-прикладна задача — підвищення інформаційної безпеки відносно розмежувального доступу до інформаційних ресурсів.

Мета роботи — розробка методу ідентифікації з використанням методів приховування образів.

Методи дослідження — визначення найбільш ефективного методу підвищення інформаційної безпеки.

Основною перевагою біометричних технологій (біометрії або біометрики) є можливість швидкої і простої ідентифікації або верифікації здебільшого без спричинення якихось незручностей індивідуумові. Використання досягнень комп'ютерно-інформаційних і телекомунікаційних технологій дозволяють здійснювати ідентифікацію користувача в режимі реального часу. Біометричні технології засновані на інтеграції досягнень у галузі електроніки, інформатики, математики, медицини й біометрії, а останнім часом і на основі нанотехнологій, що дозволяє істотно зменшити габарити використовуваної апаратури для біометричних систем, що розробляються.

1 АНАЛІЗ ІСНУЮЧИХ ТЕХНОЛОГІЙ АВТОРИЗАЦІЇ ДОСТУПУ

1.1 Аналіз недоліків існуючих технологій авторизації доступу

В наш час захист інформації від несанкціонованого доступу виступає вкрай необхідним заходом для запобігання матеріального та нематеріального збитку її власника. Тому дуже важливо брати у розрахунок ефективність роботи підсистеми управління доступом та захисту даних задля збереження безпеки певної системи інформаційної інфраструктури.

Одним з основних факторів, які визначають стан захищеності тієї чи іншої системи інформаційної інфраструктури, є ефективність роботи системи управління та надання доступу користувачам і захисту інформації, що там зберігається. Головним завданням у проблемі захисту інформації в інформаційних системах від забороненого доступу є завдання розмежування функціональних повноважень. Задача спрямована на запобігання можливості зловмисника зчитувати або модифікувати інформацію, що зберігається.

Дії по захисту інформації від несанкціонованого доступу включають:

– недопущення зловмисника до інформаційної системи (ІС), засноване на засобах розпізнавання користувача;

– створення спеціального забезпечення для захисту інформації;

– використання спеціальних засобів захисту інформації від несанкціонованого доступу.

Одним з напрямків застосування програмно-апаратних засобів є системи контролю та управління доступом. Для успішного функціонування системи контролю та управління доступом до ІС необхідне рішення двох завдань:

1) Зробити неможливим обхід системи управління і розмежування доступу;

2) Гарантувати ідентифікацію користувача, який здійснює вхід до системи.

Сучасні методи ідентифікації користувача розділяють на три основні групи:

1) Парольні – по контрольній парольній фразі або поєднанню букв і символів; засновані на унікальній інформації (пароль, пін-код тощо);

2) Атрибутні – засновані на використанні унікального предмету (ключ, токен тощо);

3) Біометричні – засновані на унікальності біологічних та психологічних даних користувача, за фізіологічними параметрами людського тіла або поведінки людини (відбиток пальця, почерк, голос, сітківка ока тощо).

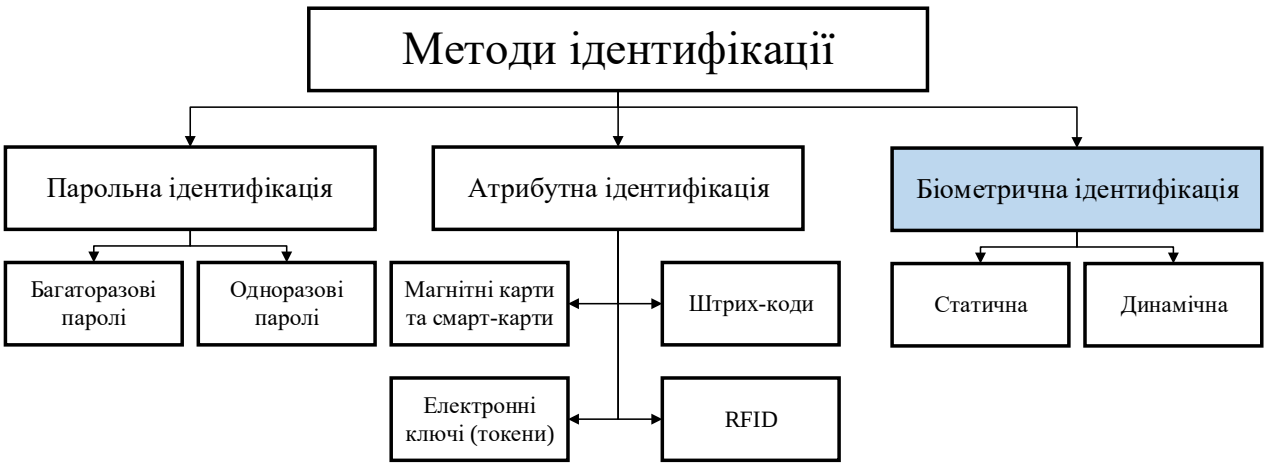

Рисунок 1.1 — Класифікація методів ідентифікації

Проведено аналіз сучасної ситуації в області сучасних систем контролю і управління доступом. За даними компанії IDC системи управління ідентифікацією та доступом складають 59% від загального ринку засобів IT-безпеки. Дослідження проведене CSI/FBI Computer Crime and Security Survey в 2007 році виявило, що 51% компаній для авторизації користувачів застосовують парольні методи, 35% атрибутні методи і тільки 20% біометричні методи. За даними соціологічного дослідження компанії

Unisys 68% клієнтів в світі вважають за краще, щоб ІС різних сфер діяльності для ідентифікації використовували біометрію замість паролів і карт. Компанія AtSecurity на початку 2013 року провела опитування серед європейських IT спеціалістів на предмет використовуваних ними технологій авторизації в різни сферах (рис. 1.2).

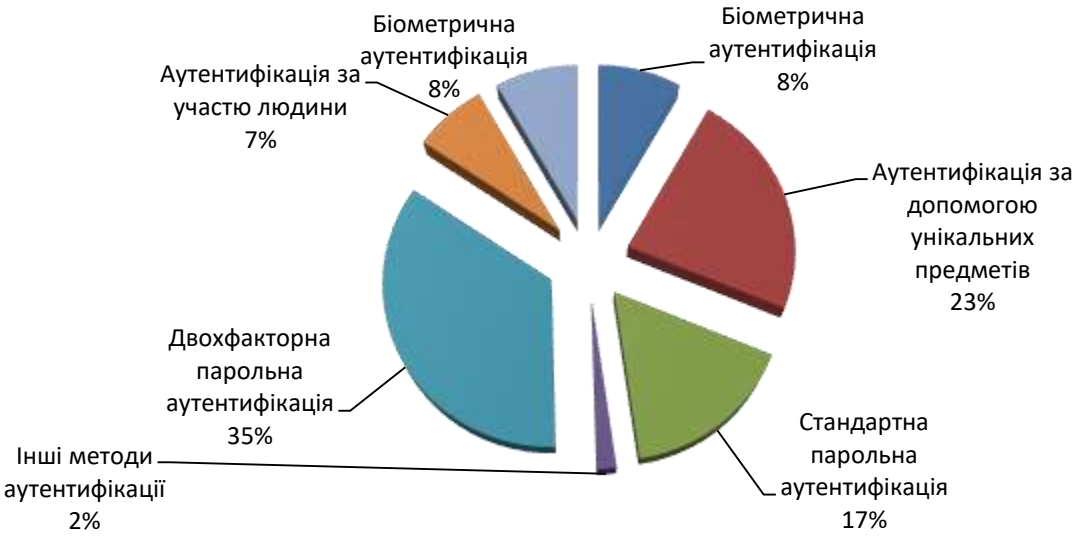

Рисунок 1.2 — Використання в європейських країнах технологій авторизації за даними опитування AtSecuri

Низька популярність біометричних методів пов'язана з високою вартістю і складністю налаштування біометричних систем (БС) захисту інформації. За підсумками аналізу наведених вище фактів, зроблено висновок про те, що найбільш поширеними є парольні та атрибутні системи контролю та управління доступом. Але вони мають ряд суттєвих недоліків.

1.2 Біометрія. Основні методи розпізнавання даних

Біометрі́я — сукупність автоматизованих методів і засобів ідентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці.

Відомі два методи розпізнавання даних: статичні та динамічні методи.

Статичні методи:

– за відбитком пальця;

– за формою долоні;

– за розташуванням вен на тильній стороні долоні;

– за сітківкою ока;

– за райдужною оболонкою ока;

– за формою обличчя;

– за термограмою особи;

– ДНК;

– за допомогою інших методів.

Динамічні методи:

– враховують особливості, характерні для підсвідомих рухів;

– за рукописним почерком;

– за клавіатурним почерком;

– за голосом;

– інші методи [8].

Для оцінки ефективності роботи біометричної ситсеми існують характеристики, за якими легко можна отримати кількісні показники, що визначають надійність створюваних систем.

Ці характеристики супроводжуються наявністю помилок першого і другого роду. Позначається як FRR (False Rejection Rate) – ймовірність помилки першого роду, тобто ймовірність відмови "своєму".

$$FRR = \frac{NFR}{NAA} x100\%, \qquad (1.1)$$

де NFR – номер помилкових відхилень;

NAA – час помилкового відхилення.

Помилка другого роду з'являється при порівняннях "чужий" до "чужому", коли "чужий" визнається "Своїм". Позначається як FAR (False Acceptance

Rate) - ймовірність помилки другого роду, тобто ймовірність пропуску "чужого".

$$FAR = \frac{NFA}{NIA} x100\%, \quad (1.2)$$

де NFA – номер хибного схвалення;

NIA –час помилкового відхилення.

Для визначення ефективності роботи біометричної системи складається графік FAR, FRR.

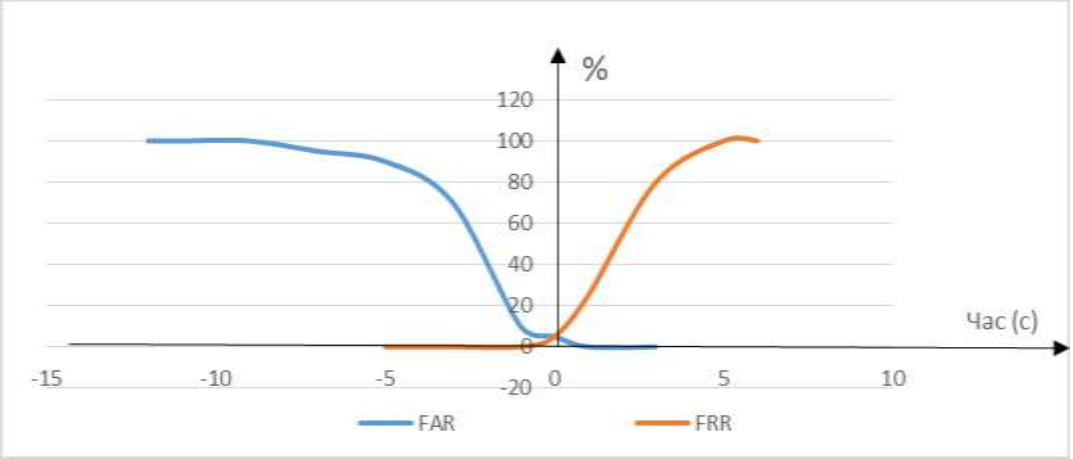

Рисунок 1.3 — Графік FAR, FRR

Наприклад, для отримання статистики помилок першого роду необхідно провести порівняння попарно між шаблонами одного ряду для забезпечення порівнянь типу "свій" до "свого". Якщо перший шаблон у ряду порівнювати з усіма іншими відбитками ряду, то виходить $(m-1)$порівнянь; другий шаблон в ряду порівнювати з усіма шаблонами, що йдуть після нього, оскільки він вже порівнювався з першим шаблоном, то отримуємо $(m-2)$ порівняння і т.д. Передостанній шаблон порівнюється тільки з останнім шаблоном, виходить одне порівняння. Таким чином, число порівнянь в ряду складе:

$$V_i = \frac{m(m-1)}{2}, \quad (1.3)$$

де m – кількість шаблонів в базі даних.

Для отримання статистики помилок другого роду необхідно провести порівняння попарно між шаблонами різних рядів, для забезпечення порівнянь типу "чужий" до "чужому".Перший шаблон першого ряду порівнюється з усіма шаблонами всіх інших рядів, і виходить $(n-1) \times m$ порівнянь; також порівнюється другий шаблон першого ряду, і виходить ще $(n-1) \times m$ порівнянь. Після порівнянь m шаблонів першого ряду з усіма шаблонами інших рядів отримуємо $m^2\ (n-1)$ порівнянь.

Шаблони другого ряду порівнюються з шаблонами всіх $(n-2)$ рядів після нього, оскільки вони вже порівнювалися з відбитками першого ряду, виходить ще $m^2\ (n-1)$ порівнянь. Зазначена процедура здійснюється до передостаннього ряду, який порівнюється вже тільки з єдиним, останнім, поруч, і виходить ще m^2 порівнянь. Це означає, що число можливих порівнянь "чужий" до "чужому" в базі з n зразків по m шаблонів кожного буде:

$$\mathrm{VFAR} = \frac{\mathrm{m^2 n(n-1)}}{2}, \quad (1.4)$$

де n – номер ряду.

Використання такого методу дозволяє отримувати досить велику кількість варіантів порівнянь, необхідних для побудови характеристик при незрівнянно менших кількостях шаблонів в базі даних [7].

Поняття біометричної системи. Методика функціонування.

Слід зазначити, що процес ідентифікації у біометричних системах в цілому поділяється на два види – ідентифікацію та верифікацію.

Визначення цих процесів:

– ідентифікація – це порівняння типу «один до багатьох;

– верифікація – це порівняння типу «один до одного»[4-6].

1.3 Поняття біометричної системи. Методика функціонування

Під біометричною системою розуміється автоматизована система, здатна знімати з сенсорів дані про користувача, обробляти отримані дані, добувати дані ознак з оброблених даних, порівнювати добуті ознаки з даними одного або більше біометричних шаблонів, визначати ступінь їх збігу та відображати успішність верифікації або ідентифікації особистості.

У загальному випадку системи біометричної ідентифікації працюють за наступним принципом. Усі системи спочатку працюють у режимі реєстрації, тобто спочатку система повинна отримати та зберегти певний біометричний ідентифікатор, за допомогою якого надалі буде здійснюватися ідентифікація користувача. Після отримання біометричного ідентифікатора система перетворює його за допомогою відповідних засобів в електронний вигляд — реєстрація. У системі зберігається так званий шаблон ідентифікатора, який являє собою одну або декілька цифрових послідовностей, які були отримані під час оброблення біометричного ідентифікатора. Тобто, біометричний ідентифікатор, який надав користувач через спеціальний пристрій-реєстратор перетворюється в електронний вид, який потім проходить декілька стадій оброблення за різними алгоритмами, внаслідок чого отримується шаблон, за допомогою якого потім здійснюється безпосередньо процедура ідентифікації користувача.

Після того, як процес реєстрації здійснено, система здатна проводити процес ідентифікації, тобто встановлення відповідності особи та визначення її прав на виконання тих чи інших дій.

Концептуальну схему біометричної системи наведено у додатку А [8].

Висновки до розділу 1

За підсумками аналізу зроблено висновок про те, що найбільш поширеними є парольні та атрибутні системи контролю та управління

доступом. Але вони мають ряд суттєвих недоліків та не є ефективними. Аналіз сучасних методів підвищення інформації безпеки свідчить про очевидний рух у бік біометричних методів завдяки їх зручності, надійності та достовірності.

Основною перевагою біометричних технологій (біометрії або біометрики) є можливість швидкої і простої ідентифікації або верифікації здебільшого без спричинення якихось незручностей індивідуумові. Використання досягнень комп'ютерно-інформаційних і телекомунікаційних технологій дозволяють здійснювати ідентифікацію користувача в режимі реального часу. Біометричні технології засновані на інтеграції досягнень у галузі електроніки, інформатики, математики, медицини й біометрії, а останнім часом і на основі нанотехнологій, що дозволяє істотно зменшити габарити використовуваної апаратури для біометричних систем, що розробляються.

2 АНАЛІЗ ПЕРЕВАГ ТА НЕДОЛІКІВ ІСНУЮЧИХ БІОТЕХНОЛОГІЙ

2.1 Переваги існуючих біотехнологій

Головна мета біометричної ідентифікації або аутентифікації полягає у створенні такої системи реєстрації, яка досить рідко відмовляла б у доступі легітимним користувачам і водночас максимально виключала б можливість несанкціонованого входу до комп'ютерних сховищ інформації (баз даних). Порівняно з доступом на основі використання паролів і карток біометричні системи забезпечують набагато надійніший захист: адже складові власного тіла не можна ані забути, ані втратити. Біометричне розпізнавання індивідуума і надання йому права доступу ґрунтується на порівнянні фізіологічних або психологічних особливостей будь-якої особистості з її характеристиками, які були відповідним чином отримані та внесені до бази даних системи.

Ця передова, сучасна міра безпеки має наступні переваги:

– точна ідентифікація. На відміну від більш традиційних форм безпеки, біометрична аутентифікація забезпечує більш високий і більш точний рівень безпеки. За допомогою біометричних зчитувачів, таких як сканери відбитків пальців і діафрагми, надається унікальна форма ідентифікації - функція, яку було б дуже складно дублювати. Це означало б, що ніхто, крім уповноваженої особи, не матиме доступу до всього, що охороняється. Біометричні зчитувачі забезпечують біометричні реєстрації, а потім роблять безпомилковий і чіткий оглядовий слід, за допомогою якого хтось може людина пов'язаний з конкретним випадком або діяльністю. У разі порушення безпеки особа може бути притягнута до відповідальності, оскільки адміністратор системи, а також її замовник безсумнівно буде знати, хто є відповідальною стороною;

– збереження часу. безпека є обов’язковою, але втрата часу для блокування великої кількості різних замків і ланцюгів навколо кожних дверей, щоб забезпечити захист цих виключно цінних ресурсів, може бути монотонною і ризикованою мірою. біометричні системи контролю доступу швидкі, сучасні, надійні і досить просі у використанні;

– підвищена безпека. Це довгострокове рішення забезпечення безпеки сучасно і дає більш прогресивну ступінь захисту в порівнянні зі звичайними методами безпеки. Оскільки біометричний ключ не може бути вкрадений, і зчитувальні пристрої не можуть бути спроектовані або використані будь-ким іншим, крім уповноваженої особи, системи біометричної перевірки особистості забезпечують надійну охорону;

– зручність. Біометрична аутентифікація може бути основним і корисним рішенням потреб для безпеки. Паролі не беруться до уваги, карти та ідентифікаційні засоби стають недоречними - звичайні проблеми з безпекою, які можуть або, можливо, підтримуватися на стратегічній відстані від керівних та підпорядкованих органів. Обмін з біометричними системами передбачає адаптацію до сучасних технологій;

– універсальність. Біометричні ідентифікатори (відбитки пальців, обличчя, райдужна оболонка ока тощо) є у кожної людини, тому ідея застосування біометрії у системах контролю управління доступом виглядає цілком природньо й логічно [6-7].

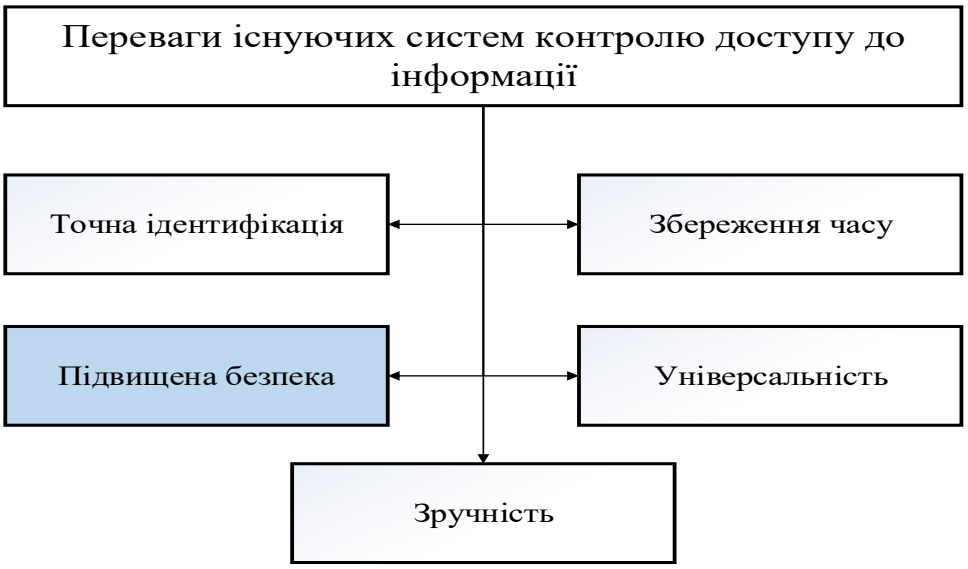

Рисунок 2.1 — Переваги існуючих біометричних систем контролю доступу до інформації

2.2 Недоліки існуючих біотехнологій

Серед усіх типів систем контролю доступу, які використовуються на сьогоднішній день, біометричні системи є найбільш ефективними. Біометрична ідентифікація дозволяє визначати особу користувача на основі його або її біологічних характеристик. Відбиток пальця використовується в якості ідентифікатора людини ще з 1883 року.

Автомати позбавлені впливу «людського фактору». Вони здійснюють ідентифікацію об’єктивно, на основі жорстко детермінованих і заданих наперед ознак. Для підвищення якості ідентифікації в деяких системах використовують додатково верифікацію, а іноді – аутентифікацію. Незважаючи на величезні переваги біометрії, існують і певні недоліки:

– захист та дискримінація. Не виключено, що дані, отримані під час біометричного зарахування, можуть бути використані таким чином, яким

заявник не погодився. Наприклад, більшість біометричних ознак можуть розкривати фізіологічні та / або патологічні захворювання (наприклад, деякі зразки відбитків пальців пов'язані з хромосомними захворюваннями, візерунки раковини можуть виявити генетичний секс, моделі ручної вени можуть виявити судинні захворювання, більшість поведінкових біометричних засобів можуть виявити неврологічні захворювання, тощо);

– підроблення біометричних даних. Немає 100% гарантії, що зразок біометричних даних не буде сфальсифікованим. Зловмисники мають змогу вигадати досить велику кількість способів аби зламати систему;

– вартість. Чим надійніша біометрична система контролю доступу до інформації (БСКДІ), тим вищу вартість вона має. Так, наприклад, вартість системи для захоплення райдужної оболонки вища за вартість сканера відбитків пальця і камери для захоплення 2D зображення обличчя і так далі;

– крадіжка особистості. Побоювання щодо крадіжки особистих даних через використання біометрики ще не вирішені. Якщо номер кредитної картки людини вкрадено, наприклад, це може спричинити певні труднощі. Якщо ж зразки сканування райдужної оболонки ока були вкрадені, що дозволяє зловмиснику доступ до особистої, фінансової чи секретної облікової інформації, збиток може бути незворотнім, тому що на відміну від використання ключів або ключових фраз, біометричні дані людини не можуть бути змінені. Як тільки вони будуть викрадені, їх не можна використовувати надалі;

– вплив захворювань. Деякі види захворювань можуть впливати на прийняття рішення системою. Наприклад, через артрит не може бути вірно ідентифікована інформація за малюнком вен на руці людини. У разі звичайної простуди змінюється голос людини, тому ідентифікація особистості за ним також стає неможливою. Є велика кількість захворювань, пов’язаних із зоровим апаратом людини, розпізнавання особи за очним яблуком, сітківкою ока і тому подібне, також стає неможливим.

Рисунок 2.2 — Недоліки існуючих біометричних систем контролю доступу до інформації

Не зважаючи на кількість недоліків, які наведені на рисунку 2.2, з кожним вдосконаленням БСКДІ їх кількість та значимість мінімізується. Натомість перелік технологій, які можуть бути використані в системах безпеки, постійно розширюється, і більшість з них вважаються досить перспективними [7-8].

Висновки до розділу 2

Проведений аналіз літературного контенту, присвяченого методам біометричної ідентифікації та технологіям їх реалізації, підтвердив актуальність існуючої проблеми ідентифікації і аутентифікації особистості і визначив її як одну з пріоритетних, вирішення якої сприяє якісному збереженню персональних даних, забезпечує надійний доступ до об’єктів таємної інформації, наукових розробок тощо.

З інформаційного погляду саме системи біометричної ідентифікації особи найбільше відповідають вимогам часу, здійснюючи ідентифікацію особистості автоматично і використовуючи при цьому нестійкі величини. На даний час біометрія, як наука ідентифікаційного дослідження особи, має декілька

практично незалежних наукових напрямів, у кожного з яких є свої технічні доробки. Уже сформувався специфічний ринок біометричних апаратних пристроїв і програмного забезпечення до них, а також послуг з підтримки, тестування та адаптації біометричних систем при практичному їх використанні.

3 РОЗРОБКА МЕТОДУ ІДЕНТИФІКАЦІЇ З ВИКОРИСТАННЯМ СТЕГАНОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

3.1 Проблеми ідентифікації на основі райдужної оболонки ока

Ідентифікація особистості на основі райдужної оболонки має дуже великий ступінь надійності й точності, проте існує й низка проблем. У першу чергу, це те, що для успішної ідентифікаці необхідно щоб око потрапило у поле зору об'єктива камери під певним діапазоном кутів. Решта проблем пов'язані з особливостями структури ока людини і показані на рис. 3.1.

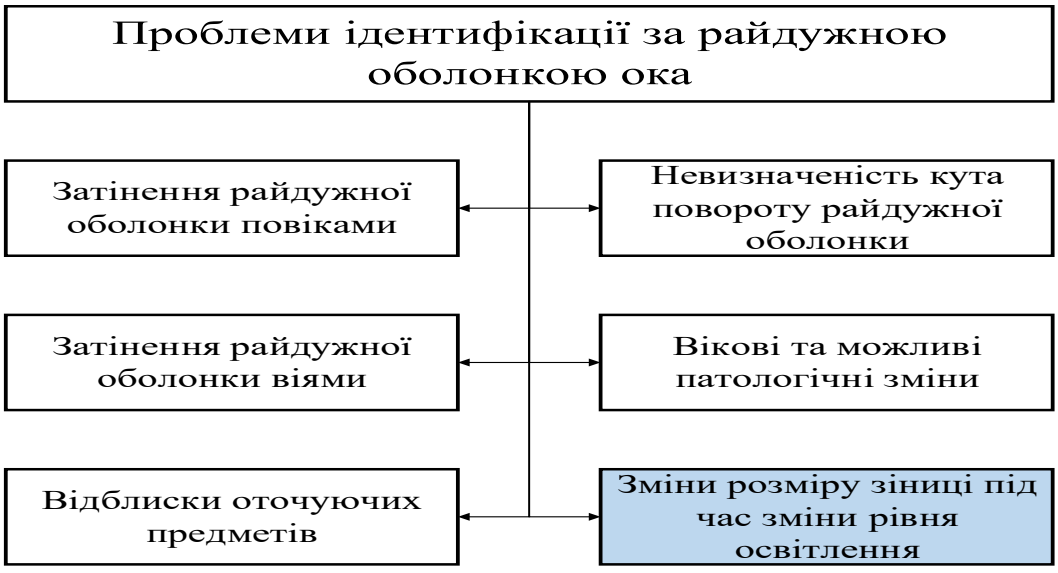

Рисунок 3.1 – Проблеми ідентифікації на основі райдужної оболонки

– 1 затінювання роговиці повіками. Ця проблема може вирішуватися спеціальним алгоритмом пошуку повік або відбраковуванням частин зображення при порівнянні послідовних кадрів;

– затінювання роговиці віями, що стирчать донизу. Алгоритм пошуку повік на подібних знімках відпрацьовує успішно і з великою впевненістю, про те виділена ним область, не підходить для розпізнавання. Проблема може вирішуватися алгоритмом відбраковування за послідовністю зображень. Роговиця і повіки з віями рухаються відносно одна одної, тому ті частини зображення, де вії і повіки нависають над рогівкою, постійно змінюються (вії поперемінно закривають різні частини роговиці). Навпаки, відкриті ділянки роговиці на нормованому зображенні відносно стабільні;

– відблиски від навколишніх предметів на роговиці. Роговиця працює як сферичне дзеркало, відбиваючи навколишній світ. Ці відбиття (особливо відображення джерел світла, плям сонячного світла і ділянок денного неба) можуть бути в кілька разів яскравішими деталей роговиці і повністю пригнічувати їх. Для вирішення цієї проблеми застосовують високоінтенсивне у вузькій області спектра освітлення (що значно перевершує сонячне за освітленістю, найчастіше використовують інфрачервоне випромінювання) і реєстрацію зображення у цій самій області спектра;

– різний розмір зіниці при змінних умовах зйомки. Як уже зазначалось, афінне перетворення зображення роговиці до стандартного розміру вирішує цю проблему лише у першому наближенні, тому що розтягування роговиці підпорядковується нелінійному, надто складному закону. Для вирішення цієї проблеми пропонується, наприклад, запам'ятовувати розмір зіниць людини при реєстрації у системі, а при розпізнаванні домагатися акомодації (розширення чи звуження) зіниць до цього розміру, маніпулюючи яскравістю спеціального джерела видимого світла;

– патологічні й вікові зміни. На роговиці дуже чітко відбивається стан організму, у тому числі різного роду патології (хвороби, травми, отруєння). У зв'язку з цим виникає питання про стійкість (за часом) розпізнавання об'єкта, підданого цим змінам. Проте, на роговиці існує значна кількість вроджених ознак і ознак, які не змінюються протягом усього життя. Вроджені та набуті ознаки розділити практично неможливо, проте людину можна розпізнавати на

підставі збігу навіть незначної кількості ознак. Необхідний мінімум – це 30% і навіть у цьому випадку ймовірність помилкового допуску не перевищує 10–64;

– невизначеність кута повороту роговиці. У системі з реєстрацією двох роговиць або у системі, що комбінує роговицю й обличчя, цієї проблеми не існує. Для так званої «одноокої» системи можна визначати кут за конфігурацією повік, децентрацією зіниці або за якоюсь важливою характерною ознакою на роговиці. Всі ці ознаки можуть змінюватися з часом. У такому випадку залишається перебирати кути повороту (істотно збільшується час роботи системи) або вираховувати ознаки, інваріантні до повороту (таких ознак в десятки разів менше, отже, сильно знижується надійність системи). Крім усього вищеперерахованого системи біометричної ідентифікації повинні бути стійкими до використання підробок. Для систем ідентифікації на основі райдужної оболонки в якості підробки можуть застосовувати або об'ємну фотографію роговиці або макет ока, так само можуть застосовувати відчуження біометричних ознак (у даному випадку «вирване» око);

Існує два способи вирішення цієї проблеми:

1. За спектром відбиття роговиці. Роговиця «живого» ока постійно зволожується, «мертве» око швидко пересихає. Спектри відбиття вологої і сухої роговиць відрізняються.

2. За реакцією ока на освітлення. Зіниця певним чином і з певним запізненням реагує на зовнішні подразники (спалах світла, гучний звук і т.д.), причому ця реакція керується головним мозком.

Сканування райдужної оболонки ока, електронні відбитки пальців і розпізнавання підпису, безумовно, краще, ніж написаний на приліпленому до монітора папірці пароль. Проте, за словами дослідників, біометричну інформацію легко вкрасти або скопіювати. «У зв'язку з цим бажано розробити такий пристрій ідентифікації, при роботі з яким не потрібно було б робити секрету з біометричних даних», — говорять вони.

У своїй статті для журналу International Journal of Biometrics, учені під керівництвом Масакутсу Нішигаки і Дайсуки Араї з Університета Шизуоки пишуть, що їм вдалося розробити альтернативний метод аутентифікації, заснований на унікальній рефлекторній реакції очного яблука людини. Нішигаки і Араї використовують як біометричний ідентифікатор ненавмисну реакцію очного яблука на зовнішню дію, вимірювану укупі з обчисленням його мертвих зон, які також називають сліпими зонами.

Сліпа пляма - зорова проекція диска зорового нерва. Ця ділянка ока округлої форми розмірами близько 1.9 мм, не може формувати зорове зображення. Людські очі мають область сліпої плями, однак, завдяки бінокулярності зору, сліпа пляма залишається непомітною, оскільки дані галузі накладаються при зіставленні зображень правого і лівого ока. Навіть якщо закрити одне око, побачити сліпу пляму непросто. Мозок компенсує недоотриману зорову інформацію, і сліпа пляма залишається непоміченою. Збільшення розмірів сліпої плями може говорити про ряд очних захворювань і є диагностическім критерієм в офтальмології.

У кожного хребетного в оці є мертва зона, де зоровий нерв віддаляється від сітківки. Цей візуальний розрив візуально не сприймається, оскільки поле зору іншого ока перекриває цю мертву зону. Учені використовують цю мертву зону, щоб засікти рух ока. Людині демонструють візуальний образ, що знаходиться як в її межах, так і за межами, і вимірюють час реакції ока до моменту почала рухи очного яблука. Пропонуються і інші варіанти використання цього методу, такі як положення мертвих звін і час звуження зіниці.

Нішигаки особливо звертає увагу на той факт, що використовувати одне тільки положення мертвих зон як ідентифікатор нітрохи не безпечніше, ніж користуватися скануванням райдужної оболонки, оскільки для обходу системи в цьому випадку можна скористатися контактними лінзами або навіть хірургічним втручанням.

3.2 Розробка методу ідентифікації

Метод розпізнавання особи за райдужною оболонкою та реакцією очного яблука людини на подразники складається з наступних етапів:

1. Запит на процес ідентифікації, тобто встановлення відповідності особи та визначення її прав на виконання тих чи інших дій. Особа, яка хоче отримати доступ до даних повинна наблизити обличчя до сканера, зафіксувати його положення і направити погляд на спеціальну мітку на дисплеї сканера. Далі камера робить знімки з швидкістю десятки кадрів у секунду, і отримані зображення обробляються спеціальною програмою. Промінь, падаючий на викривлену поверхню, згинається - чим більше кривизна поверхні, тим сильніше вигин променя. Спочатку при цьому застосовувався джерело видимого світла. Потім видиме світло буде замінене на інфрачервоне.

2. Введення людиною ключа (паролю). Ключ — це правило для стеганографічного перетворення зробленого системою знімку. Ключ — певна послідовність літер/цифр, відомих системі, особі, яка подає запит на ідентифікацію та адміністратору системи. За допомогою нього система розміщує дані по контейнеру, таким чином зловмисник не знатиме в які блоки контейнера занесено стеганографічно зміни. Користувач повинен ввести 2 ключі:

– Перший для закриття інформації;

– Другий для стеганографічного розміщення в контейнері.

Таким чином підвищується складність доступу в систему неавторизованих користувачів.

3. Формування шаблону на основі зробленого знімку. На першому етапі обробки видаляються зображення, на якому обличчя не видно взагалі або присутні сторонні предмети, що заважають ідентифікації. За отриманими знімками відновлюється 3-D модель особи, на якій виділяються і віддаляються непотрібні перешкоди (зачіска, борода, вуса й окуляри). Потім проводиться аналіз моделі - виділяються антропометричні особливості.

Проходить виділення «кола» зіниці із загального зображення очного яблука та виділення сліпих зон. Вимірюється час реакції очного яблука людини на подразники.

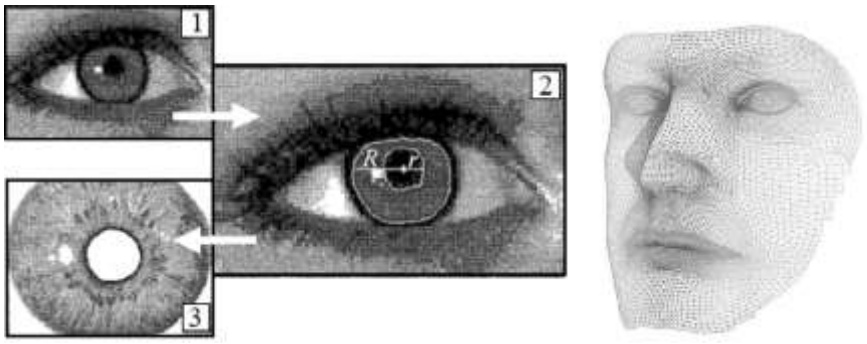

Рисунок 3.2 — Формування 3-D шаблону для розпізнавання особи та отримання «кола» зіниці

4. Формування контуру зображення. Для цифрових зображень найбільш корисною семантичним навантаженням мають контури об'єктів. Контури являють собою лінії, які проходять на межах однорідних областей. Елементи $z_{i,j}$ просторово-часового подання зображення, значення яких не перевищують певного порогу, формують однорідні області. Це задається наступною умовою:

$$\left| z_{\max} - z_{\min} \right| \le 1, \tag{3.1}$$

де z_{max} — елемент області зображення, який володіє найбільшим значенням, визначається на основі наступного виразу:

$$z_{\max} = \max_{1 \le i \le x} \{ z_{i,j} \} \quad j = \overline{1, y}, \tag{3.2}$$

де z_{min} — елемент області зображення, який володіє найменшим значенням, визначається на основі формули:

$$z_{\min} = \min_{1 \le i \le x} \{ z_{i,j} \} \quad j = \overline{1, y}, \tag{3.3}$$

де 1— поріг виявлення однорідних областей.

Найбільш поширені і застосовуються на практиці підходи для виявлення контурів є градієнтні методи. Найбільш поширеним способом пошуку контурів є обробка зображення ковзною маскою. Маска являє собою квадратну матрицю з коефіцієнтами. Процес обробки зображення на основі матриці називається фільтрацією або маскуванням і задається наступним функціоналом *f(Z , K)*(рисунок 3.1):

$$M = f(Z, K), \tag{3.4}$$

де М — зображення, отримане в результаті обробки зображення Z на основі маски К.

Процес фільтрації заснований на поступовому просторовому переміщенні маски фільтра від елемента до елемента зображення. З аналізу рисунку 3.1 видно, що значення елемента $m_{i,j}$ (відгуку фільтрації) обчислюється з використанням значень попередніх і наступних елементів у двомірній площині.

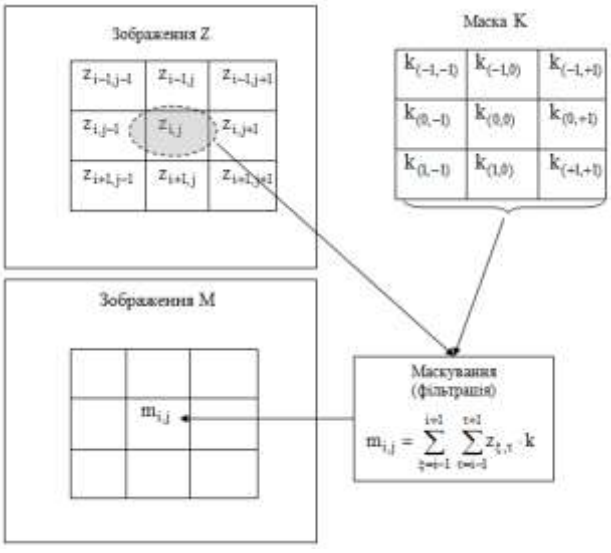

Рисунок 3.3 — Схема маскування зображення на основі змінної маски

5. Вбудовування даних в найменш значимі біти (НЗБ) просторового представлення зображення. НЗБ обираються за допомогою введеного другого ключа користувачем на етапі №2. Вбудовування повідомлення відбувається в молодший біт зображення, який несе в собі найменше інформації. Процес вбудовування показано на рисунку 3.2:

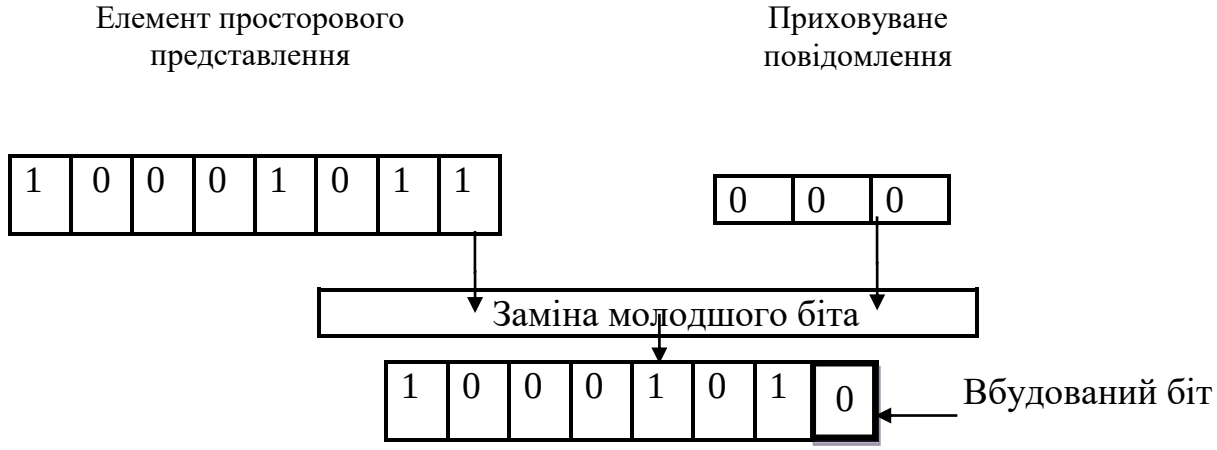

Рисунок 3.4 — Стеганографічне вбудовування в НЗБ

Фактично, НЗБ – це шум, тому його можна використовувати для вбудовування секретного повідомлення. В просторово-часовому представлені зображення вбудовування даних відбувається на основі використання властивостей 24-бітного представлення зображення.

24-бітний колір в комп'ютерній графіці – метод представлення і збереження зображення, що дозволяє відобразити велику кількість кольорів, півтонів і відтінків. Колір представляється з використанням 256 рівнів для кожної з трьох компонент моделі RGB: червоного (R), зеленого (G) і синього (B), що в результаті дає 16 777 216 (224) різних кольорів.

Зазвичай при кодуванні пікселя на кожен з каналів (червоний, зелений, синій канали) відводиться по одному байту; четвертий байт (якщо використовується) зазвичай відводиться або для зберігання даних альфа-каналу, або просто ігнорується.

Розмір вбудованого повідомлення може складати 1/8 загального обсягу контейнера. Наприклад, в зображення розміром 512x512 можна вбудувати 32 кБайт інформації. Якщо модифікувати два найменших біта, то пропускну спроможність можна збільшити вдвічі.

Метод вбудовування даних в спектральну область є дещо складнішим, в порівнянні з вбудовою повідомлення в просторово-часову область зображення. Вбудовування інформації відбувається після дискретно-косинусного перетворення (ДКП) зображення.

Коефіцієнти ДКП (транформанти) упорядковуються відповідно до їх важливості, наприклад відповідно до внеском в інформаційний зміст, так що трансформанти з невеликим інформаційним змістом можна опустити (відкинути). Решта трансформанти квантуються, кодуються і передаються або запам'ятовуються. Важливість коефіцієнтів можна зіставляти, наприклад, візуально (суб'єктивно), відповідно до їхнього внеску в картину яскравості відновлюваного зображення на дисплеї; тим самим можна обійти питання кореляції елементів зображення і оцінити результат стиснення. Відмінною вважається архівація, при якій неможливо на око розрізнити початкове і розпакувати (відновлене) зображення, хорошою – коли відмінність видно лише для поруч знаходяться зазначених зображень. При подальшому збільшенні ступеня стиснення, як правило, стають помітні побічні ефекти, характерні для застосовуваного алгоритму стиснення.

Вбудовування здійснюється побітно: один біт інформації в одне значення низькочастотного коефіцієнта ДКП. Для цього інформаційні біти перетворюються в полярний вид.

6. Надсилання стеганографічно перетвореного зображення в «хмарне» середовище. Кожна біометрична система має підсистему зберігання даних — реєстраційну базу, яка служить для зберігання шаблонів. Пропонується зберігати, стеганографічно перетворювати шаблони та порівнювати їх в захищеному хмарному середовищі.

Хмарні технології – це технології обробки даних, в яких комп’ютерні ресурси надаються Інтернет користувачеві як онлайн сервіс, одна велика концепція, що включає в себе багато різних понять, що надають послуги.

Можна виокремити наступні загальні характерні властивості хмарної моделі використання сервісів:

– масовість (великі масштаби) застосування;

– гомогенність (однорідність) інфраструктури;

– віртуалізація додатків; стійкість (надійність) виконання обчислень;

– дешеве програмне забезпечення;

– географічна необмеженість використання;

– сервісна орієнтованість;

– передові технології безпеки.

Можливості хмарних обчислень:

– доступ до особистої інформації з будь-якого комп'ютера, що підключений до Інтернету;

– можливість працювати з інформацією з різних пристроїв (персональні комп’ютери , планшети, телефони і т.п.);

– незалежність від операційної системи комп’ютера користувача - веб-сервіси працюють в браузері будь-яких операційних систем;

– одну інформацію можна переглядати і редагувати одночасно з різних пристроїв;

– багато платних програм є безкоштовними (або дешевшими) веб-додатками;

– запобігання втрати інформації, вона зберігається в хмарних сховищах;

– завжди актуальна і оновлена інформація;

– використання останніх версій програм і оновлень;

– можливість об’єднання інформації з іншими користувачами;

– легко ділитися інформацією з людьми в будь-якій точці земної кулі.

Класифікувати хмарні обчислення можна таким чином: загальна «хмара», публічна «хмара» (public cloud), приватна «хмара» (private cloud) і гібридна «хмара». Оптимальним рішенням для більшості організацій служать гібридні системи. Їх застосування зводить до мінімуму можливі ризики, оскільки найбільш важливі застосування залишаються під контролем власника, а менш важливі програми з нерівномірним коефіцієнтом використання зберігаються на серверних фермах.

7. Порівняння шаблону з інформацією в реєстраційній базі даних. Отриманий шаблон для проведення верифікації порівнюється з тим, що зберігається, для того, щоб визначити, чи збігаються ці шаблони. Ця технологія використовує установчі дані (ключі, введені користувачем) користувача як покажчика для отримання облікового запису абонента системи, який зберігається, та перевірки відповідності «один до одного» (аутентифікація або верифікація) між шаблоном, отриманого під час верифікації параметрів біометричного показника, і вже наявним для цього імені користувача шаблоном. У іншому випадку (процедура ідентифікації) шаблон параметра біометричного показника, що пред’являється, зіставляється з усім набором шаблонів, що зберігаються.

8. Прийняття рішення системою («свій» / «чужий») [1,9].

Принцип роботи системи наведений у додатку Б.

Висновки до розділу 3

Запропоновано схему роботи ідентифікаційної системи розпізнавання за райдужною оболонкою та реакцією очного яблука людини на подразники з використанням стеганографічного перетворення. У даному розділі було обґрунтовано актуальність застосування даної системи та доведено, що метод розпізнавання саме за наведеними ознаками є новітнім та ефективним. Розвиток систем, що використовують зображення та відео для передачі даних, змушує впроваджувати методи цифрової стеганографії для захисту даних.

ВИСНОВОК

У даній роботі ми проаналізували методи підвищення інформаційної безпеки інформаційно-телекомунікаційної системи, проаналізували основні переваги та недоліки даних методів, обрали найбільш ефективний та провели наліз перспектив розвитку обраного методу – біометричної ідентифікації.

Згідно з моїми розрахунками щодо аналізу ситуації в області сучасних систем контролю і управління доступом було виявлено, що для авторизації користувачів 51% компаній різних сфер використання застосовують парольні методи, 35% – атрибутні методи, 20% – біометричні методи. Тобто, найбільш поширеними є парольні та атрибутні системи контролю та управління доступом, але вони мають ряд суттєвих недоліків, та не є ефективними.

Згідно з прогнозами багатьох експертів у галузі біометричних технологій, біометрія є одним із найдинамічніших сегментів світового ринку інформаційних технологій, що посилено розвиваються.

Було запропоновано створити біометричну розпізнавання за райдужною оболонкою та реакцією очного яблука людини на подразники з використанням стеганографічного перетворення (використання 2 ключів вводу користувачем для закриття та стеганографічного розміщення інформації). Збереження даних буде відбуватись в хмарнму середовищі.

Таким чином, аналіз досягнень у сфері розробки і використання біометричних систем показав, що це один з перспективних напрямів наукового дослідження, результати якого можуть ефективно використовуватися не тільки в охоронних системах або системах стеження, але і в експертних системах, що є нагальною потребою сьогодення.

ЛІТЕРАТУРА

1 Пєвцов Г. В. Інформаційна безпека у воєнній сфері: проблеми, методологія, система забезпечення. Монографія / Г. В. Пєвцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський — Х: Цифрова друкарня № 1, 2013. – 272 с.

2 Сидченко С. А., Сапрыкина Т.В., Школяренко В.А. Метод составления текста с заданной суггестивной направленностью контекста / С. А. Сидченко, Т. В. Саприкина, В. А. Школяренко – Х.: ХУПС. – 2014. – Вип. 4 (70). – в печати (6 с.).

3 Гнідець Т.Я. Біометрія: сильна та слабкі сторони. Монографія / Т.Я. Гнідець, Н.Л. Гула. — Л.: Львівський державний університет внутрішніх справ, 2014. — 326 с.

4 Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. Монографія / А.О. Мороз, К.Д. Чернов. — К: Пітер, 2016 — 184 с.

5 Різник О.О. Система біометричної ідентифікації користувача комп’ютерної мережі / О.О. Різник, Д.В. Дзюба, С.О. Чернодуб. — К.: Акта, 2015 — 202 с.

6 Лакін Г.Ф., Біометрія / Г.Ф. Лакін, О.О. Олеченко. — М.: Вища школа, 2014 — 352 с.

7 Козирев С.П. Аналіз біометричних засобів захисту інформації / С.П. Козирев, А.О. Корченко, О.М. Мацьків, А.К. Гречишкіна. — К.: Пітер, 2015. — 180 с.

8 Захаров В.П Біометричні технології в XXI столітті та їх використання органами. Посібник / В.П. Захаров, В.І. Рудешко. — Л.: ЛьвДУВС, 2015 — 492 с. — ISBN 978-617-511-169-7

9 Кметюк Я.І. Метод підвищення ефективності розмежування доступу до автоматизованих систем управління спеціального призначення / Я.І. Кметюк, М.В. Пархоменко, В.В. Димчук, Д.Б. Жуйков // Радиоэлектроника и информатика. – 2019. - № 4(87). Х.: ХНУРЕ, 2019.

ДОДАТКИ

ДОДАТОК А

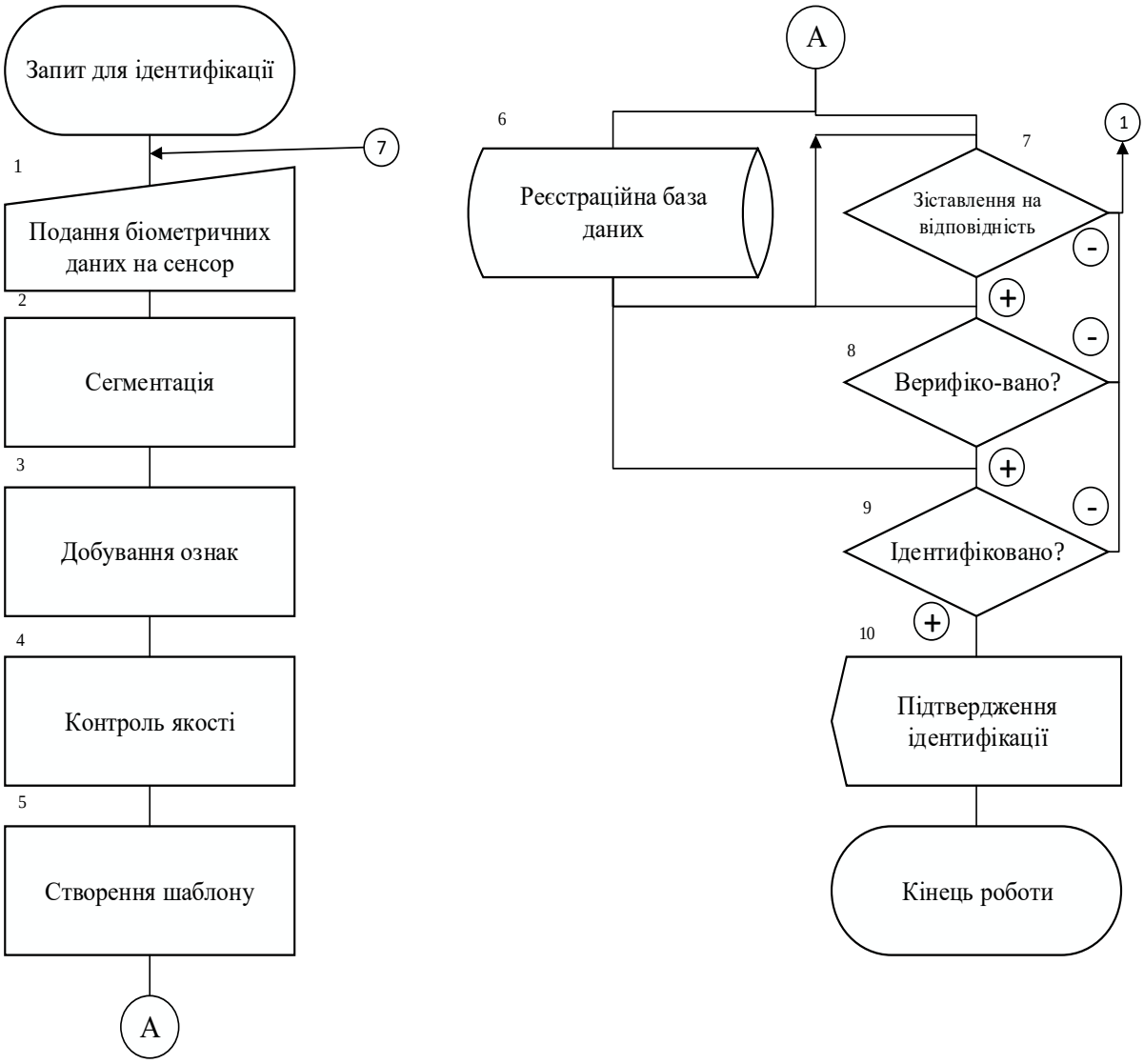

Рисунок А – Концептуальна схема узагальненої біометричної системи

ДОДАТОК Б

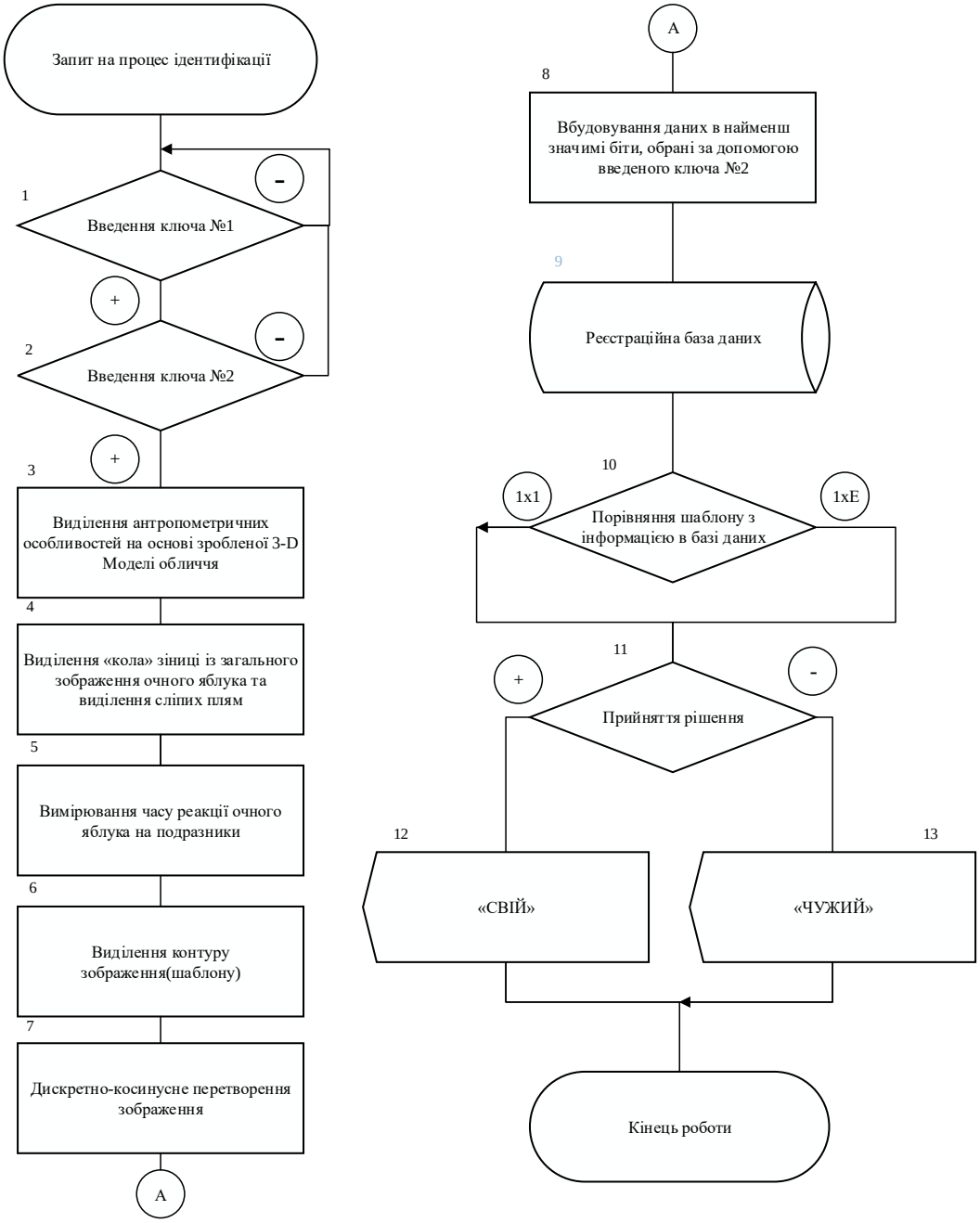

Рисунок Б — Принцип роботи ідентифікаційної системи розпізнавання за райдужною оболонкою та реакцією очного яблука людини на подразники з використанням стеганографічного перетворення