МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ

КАФЕДРА КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК 004.031.42(031.43)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Методи біометрії в автоматизованих системах доступу на підприємстві

|  |  |
| --- | --- |
| **Автор:** | Г.А. Савчук |
| **Науковий керівник:** к.т.н., доц. | М.Б. Гумен |
| **Нормоконтролер:** асист. | С.В. Єгоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ Казмірчук С.В.

« » 20 р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта** Савчук Ганна Анатоліївна

1. Тема роботи «Методи біометрії в автоматизованих системах доступу на підприємстві»

затверджена наказом ректора від 02.10.2019 р. № 2265/ст

1. Термін виконання роботи**:** з 14.10.2019 р. по 09.02.2020 р.
2. Вихідні дані роботи: запропоновано покращення технічного завдання системи захисту; реалізовано методи біометрії в АС доступу на підприємстві з використанням спеціалізованого програмного забезпечення.
3. Зміст пояснювальної записки: дослідження існуючих систем контролю доступу на підприємство. Особливості технології сканування відбитків пальців та голосової автентифікації контролю доступу на підприємстві.
4. Перелік обов'язкового ілюстративного матеріалу: рисунки, таблиці.
5. Календарний план-графік

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Завдання | Термін виконання | Примітка |
| 1 | Постановка задачі | 14.10.2019 | Виконано |
| 2 | Аналіз літературних джерел | 15.10.2019 -23.10.2019 | Виконано |
| 3 | Обґрунтування вибору рішення | 23.10.2019 -24.10.2019 | Виконано |
| 4 | Збір інформації | 24.10.2019 -31.10.2019 | Виконано |
| 5 | Визначення існуючих систем доступу на об'єктах | 01.11.2019-15.11.2019 | Виконано |
| 6 | Визначення вимог до пристроїв СКУД | 15.11.2019 -01.12.2019 | Виконано |
| 7 | Аналіз технологій сканування | 02.12.2019 -14.12.2019 | Виконано |
| 8 | Опис об'єкта інформаційної діяльності | 14.12.2019 -24.12.2019 | Виконано |
| 9 | Визначення найкращого методу | 24.12.2020 -16.01.2020 | Виконано |
| 10 | Оформлення та друк пояснювальної записки | 16.01.2020 -17.01.2020 | Виконано |
| 11 | Оформлення презентації | 17.01.2020 -19.01.2020 | Виконано |
| 12 | Перевірка на антиплагіат | 20.01.2020 -09.02.2020 | Виконано |
| 13 | Перевірка на нормоконтроль | 21.01.2020 -28.01.2020 | Виконано |
| 13 | Отримання рецензії від рецензента | 31.01.2020 | Виконано |
| 13 | Підготовка до захисту в ЕК | 01.02.2020 -09.02.2020 | Виконано |

1. Дата видачі завдання: 02 жовтня 2019 р.

Керівник дипломної роботи: Гумен М.Б.

Завдання прийняла до виконання: Савчук Г.А.

**РЕФЕРАТ**

1. Пояснювальна записка до дипломної роботи «Методи біометрії в автоматизованих системах доступу на підприємстві»: 107 с., 45 рис., 4 табл., 46 літературних джерел.

СИСИТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ ДОСТУПОМ, БІОМЕТРІЯ, МЕТОДИ БІОМЕТРІЇ, ВІДБИТОК ПАЛЬЦЯ, ІДЕНТИФІКАЦІЯ, КОНТРОЛЕР, РАЙДУЖНА ОБОЛОНКА, ГОЛОСОВА АУТЕНТИФІКАЦІЯ.

Предмет дослідження: методи біометрії в автоматизованих системах доступу на підприємстві.

Об’єкт дослідження: процедура біометричного контролю доступу на підприємствах.

Мета дипломної роботи: реалізація методів біометрії в АС доступу на підприємстві на базі поєднання декількох підходів щодо автентифікації.

Методи дослідження: базуються на концепціях і принципах системного аналізу, побудові принципових схем та методах їх модернізації, а також на методі дослідження ієрархії.

Значущість виконаної роботи полягає в тому, що було спроектовано технічне завдання системи контролю і управління доступом, вибрано методом аналізу ієрархії оптимізаційний вибір параметрів обладнання СКУД.

Дана система призначена для впровадження на підприємствах, режимних об’єктах та інших організаціях з підвищеними вимогами до безпеки.

*Наукова новизна полягає в тому, що:*

* Було запропоновано підхід щодо покращення використання методів автентифікації в автоматизованих системах, на базі поєднання голосової автентифікації та по відбитку пальця, що дало можливість здійснювати управління та контроль доступу.

Практична значимість: реалізовано методи біометрії в АС доступу на підприємстві з використанням спеціалізованого програмного забезпечення.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 7](#_Toc30864456)

[РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ГАЛУЗІ 12](#_Toc30864457)

[**1.1 Інформаційна безпека підприємств та організацій** 12](#_Toc30864458)

[**1.2 Технології безпечного доступу на об’єкт** 16](#_Toc30864459)

[**1.3 Огляд існуючих систем доступу на підприємство** 17](#_Toc30864460)

[**1.4 Принцип роботи мережевої системи контролю доступу** 21](#_Toc30864461)

[**1.5 Елементи ідентифікації в сучасних системах доступу** 24](#_Toc30864462)

[**1.6 Вимоги до виконавчих пристроїв СКУД** 25](#_Toc30864463)

[**1.7 Постановка задачі дослідження** 29](#_Toc30864464)

[**Висновок до 1 розділу** 33](#_Toc30864465)

[РОЗДІЛ 2. БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ 34](#_Toc30864466)

[**2. Біометричні технології** 34](#_Toc30864467)

[**2.1 Біометричні ідентифікації** 39](#_Toc30864468)

[2.1.1 Дактилоскопія 39](#_Toc30864469)

[2.1.2 Види біометрії відбитка пальця 41](#_Toc30864470)

[2.1.3 Пристрої сканування 41](#_Toc30864471)

[2.1.4 Переваги систем біометрії пальця 42](#_Toc30864472)

[2.2.2 Ідентифікація за райдужною оболонкою і сітківкою ока 42](#_Toc30864473)

[2.2.3 Ідентифікація за геометрією обличчя 45](#_Toc30864474)

[2.2.4 Ідентифікація за геометрією кисті руки 47](#_Toc30864475)

[2.2.5 Ідентифікація за голосом 49](#_Toc30864476)

[2.2.6 Ідентифікація за клавіатурним «почерком» 50](#_Toc30864477)

[**2.3 Нові методи біометричної ідентифікації** 51](#_Toc30864478)

[**Висновки 2 розділу** 54](#_Toc30864479)

[РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ НА ПІДПРИЄМСТВО З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ МЕТОДІВ 55](#_Toc30864480)

[**3.1 Базові параметри біометричного обладнання** 55](#_Toc30864481)

[**3.2 Принцип роботи біометричної СКУД.** 56](#_Toc30864482)

[**3.3 Оптимізаційний вибір параметрів обладнання** 59](#_Toc30864483)

[**3.4 Результат дослідження методом аналізу іієрархії** 72](#_Toc30864484)

[**3.5 Система контролю і управління доступом (СКУД)** 80](#_Toc30864485)

[**3.6 Адміністративні зміни для впровадження біометричної системи доступу** 84](#_Toc30864486)

[**3.7 Голосова аутентифікація** 87](#_Toc30864487)

[**3.7.1** **Види авторизації** 89](#_Toc30864488)

[**3.7.2 Голосова біометрія України** 91](#_Toc30864489)

[**3.8 Система розмежування доступу на основі біометричної мовної верифікації - Voice Key Service** 95](#_Toc30864490)

[**3.9 Порівняльний аналіз** 100](#_Toc30864491)

[**Висновки до 3 розділу** 102](#_Toc30864492)

[ВИСНОВКИ 103](#_Toc30864493)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 105](#_Toc30864494)

# 

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

КД-2- Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину обєктів КС, до яких вона входить.

ЦД-1- Політика довірчої цілісності, що реалізується КЗЗ, повинна визначати множину обєктів КС, до яких вона відноситься.

НР-2- Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються.

НИ-2- Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач,і послуги, для використання яких потрібні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

НК-1- Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації.

НО-1- Політика розподілу обов’язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача.

НЦ-1- Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ.

ПУЕ- Правила улаштування електроустановок.

КД - довірча конфіденційність.

ЦД - довірча цілісність

НР - реєстрація

НИ - ідентифікація і автентифікація

НК - достовірний канал

НО - розподіл обовязків

НЦ - цілісність КЗЗ

**ВСТУП**

Будь-яка організація, що має в своєму розпорядженні конфіденційну чи секретну інформацію, зобов’язана мати систему контролю доступу.

Зарекомендували себе як надійні, гнучкі і функціональні – системи управління доступом. У переліку вироблюваних різними компаніями продуктів для системи контролю управління доступом містяться контролери з централізованою архітектурою, аналогові і цифрові панелі охоронної сигналізації, релейні модулі, зчитувачі і проміжні блоки з власною пам'яттю і вбудованою логікою, здатні працювати автономно, цифрові і аналогові інтерфейси управління кінцевими пристроями і ін. З допомогою контролера система може управляти різними виконавчими пристроями. Звичайно це електромеханічний замок, турнікет, автоматичні ворота та ін.

Системи управління контролю доступом (СКУД) на даний період є невід'ємною частиною багатьох сучасних систем безпеки.

Центром системи контролю доступу є устаткування, що управляє, - контролери. Але системи контролю доступу призначені ще і для відстежування пересувань. Наприклад, можна відстежувати переміщення співробітників усередині будівлі для автоматичного складання табеля обліку робочого часу СКУД. Устаткування систем контролю і управління доступом ділиться на автономні і мережеві системи. Автономні системи контролю доступу мають зчитувачі того або іншого типу, або клавіатуру для набору коду і контролер, що пам'ятає легальні коди та керує замком або іншим виконавчим механізмом.

Мережеві системи контролю доступу включають декілька зчитувачів і один або декілька контролерів. З використанням додаткових інтерфейсних модулів можливе підключення будь-яких зчитувачів.

Сучасні системи контролю доступу мають безліч застосувань, а у кожного замовника - індивідуальні запити. Крім вирішення питань контролю доступу, система здійснює облік робочого часу співробітників, що приводить до підвищення трудової дисципліни і мотивації персоналу. Існують також автономні системи контролю доступу з накопиченням інформації про всі переміщення через точку контролю (двері, шлагбаум, турнікет) - час, дата, ідентифікаційний номер Proximity- або smart- карти або брелка Touch Memory. Вся інформація зберігається в пам'яті контролера. Системи контролю управління доступом дозволяють автоматично контролювати вхід людей в будівлю або приміщення і вихід з нього, а також в'їзд автотранспорту на територію і виїзд. Таким чином, установка скуд просто необхідна тим, хто приділяє належну увагу безпеці. Мережеві системи поєднують в собі функції контролю і управління доступом і охоронної сигналізації, що дозволяє забезпечити комплексний захист об'єкту без використання додаткових засобів.

Недорогі і зручні рішення, коли потрібно управляти доступом в невеликі офіси. Контролери, що застосовуються в монтажі мережевих систем контролю доступу, підключаються до комп'ютера і передають інформацію про проходи через контрольовані двері або турнікет.

СКУД дозволить запобігти доступу небажаних осіб, а співробітникам точно вказати ті приміщення, в які вони мають право доступу. Складніша система дозволить, крім обмеження доступу, призначити кожному співробітникові індивідуальний часовий графік роботи, зберегти і потім проглянути інформацію про події за день. Системи можуть працювати в автономному режимі і під управлінням комп'ютера. СКУД дозволить створити системи контролю доступу будь-якої складності з можливістю контролю і управління проходу співробітників в різні приміщення.

Особливістю можна виділити те, що, ухваливши рішення про придбання, клієнт часто не представляє, скільки можливостей може дати ця система.

У часи стрімкого розвитку інформаційних технологій парольні та атрибутні способи ідентифікації поступово втрачають свою актуальність, а їх мінуси стають все більш вираженими. Центральною проблемою виступає неточність ідентифікації користувача у системі та велика ймовірність щодо порушення її безпеки в результаті крадіжки, імітації певного атрибуту або злому пароля. Також значним мінусом виступає відсутність функціоналу для виявлення підміни авторизованого легітимного користувача. Тобто, злочинець може незаконно потрапити у систему в момент, коли законний користувач залишає її без контролю після етапу проходження авторизації.

Біометричні характеристики користувача, зокрема клавіатурний почерк (КП), як спосіб аутентифікації, можуть гарантувати підвищений рівень безпеки, неможливості відмови від авторства та комфорт для користувачів, враховуючи невід’ємність біометричних даних від певної людини. Неперервний прихований моніторинг дає можливість своєчасно виявити відсутність законного користувача та перекрити доступ до системи для злодія. Тож на сьогоднішній день стає вкрай важливим питання вивчення моделей, способів і алгоритмів визначення клавіатурного почерку користувачів інформаційних систем.

Питання вивчення та залучення клавіатурного почерку до алгоритмів ідентифікації та аутентифікації стало центром досліджень багатьох науковців різних країн світу, таких як Д. Сонг, П. Венабл, А. Перріг, Р. Гайнес, В. Лісовський, С. Пресс, Н. Шапіро, А. Пікок, Дж. Леггет, Д. Умфрес, Дж. Вілліамс, Р. Мініханов тощо. В їх працях було запроваджено традиційну для сьогодення схему аутентифікації користувача. Деякі з дослідників біометрії, зокрема А. Іванов, М.

Десятерик, В. Марченко, визначили головні властивості КП:

* Швидкість вводу – співвідношення кількості введених символів до часу на їх друкування;
* Динаміка вводу – показники інтервалів між натисканням клавіш та тривалості їх натиску;
* Помилки при введенні тексту та частота їх появи;
* Статистика використання певних клавіш;
* Сила, з якою користувач натискає на клавіші.

Науковці А. Лебедєв, В. Дорохов, Т. Щукін та Є. Луценко в своїх працях визначили та дослідили зв’язок між психофізіологічним станом користувача та періодичних відмінностях у його клавіатурному почерку.

Крім того, дослідники В. Волчихін та А. Іванов запропонували застосувати систему штучної нейронної мережі, здатної здійснювати математичну обробку біометричних даних користувачів.

Вищезазначені методи аутентифікації, на жаль, мають значні проблеми та допускають шанс на появу помилок першого та другого роду в разі визначення клавіатурного почерку з використанням лише ключової фрази.

Слід також взяти до уваги, що клавіатурний почерк – це нестатична біометрична риса людини і може змінюватись залежно від психоемоційного та фізичного стану користувача. Тож програмні реалізації спроб визначення клавіатурного почерку мають досить низький рівень точності ідентифікації і аутентифікації, а також великий шанс на утворення похибок першого та другого роду. Це призводить до того, що в результаті вони не придатні для прихованого моніторингу клавіатури та виявлення підміни оператора. Отже, в результаті цього виникає актуальність розробки нової системи визначення КП та її програмного забезпечення, що допомогло б зробити ідентифікацію та аутентифікацію користувача більш якісною і точною.

Тож для математичного дослідження часу утримання клавіш (ЧУК), притаманної для клавіатурного почерку користувача, з’являється необхідність у залученні математичної статистики.

Також в ході досліджень виявлено, що базуючись на методі визначення клавіатурного почерку на основі оцінки тривалості утримання клавіш при залученні системи оцінки КП, за довільним текстом з’являється можливість визначити клавіатурний почерк користувача. Це дає можливість реалізувати процес прихованого моніторингу та виявляти підміну законного користувача.

На основі аналізу введення з клавіатури базується метод визначення КП за довільним текстом, що втілюється за допомогою алгоритму визначення клавіатурного почерку за часом утримання клавіш та часом між натисканням клавіш. Тож для постійного прихованого моніторингу клавіатури в ході роботи було створено програмне забезпечення, інтегроване в інтерфейс інформаційної системи.

# РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ГАЛУЗІ

## **1.1 Інформаційна безпека підприємств та організацій**

Проблемою в інформаційній безпеці підприємств та організацій є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, інформаційних систем і мереж. Це можна пояснити зростаючими можливостями доступу до інформації: технічними та програмними, котрі не завжди є правомірними. Актуальністю проблеми інформаційної безпеки підприємств описується рядом взаємопов’язаних факторів, наслідком є процес інформатизації сучасного суспільства. З однієї сторони, формуються правові засади інформатизації, поширюються інформаційні технології у підприємницькій діяльності, а з іншого боку, висока уразливість інформаційних систем, та стрімкий прогрес розвитку «інформаційної зброї».

У інформаційній сфері історично сформувалися два напрями захисту від несанкціонованого доступу. У системах фізичного захисту вони називаються системами управління доступом (СУД), а в комп'ютерній сфері – системами ідентифікації і аутентифікації.

Особливостями соціально-економічної ситуації, маємо відсутність реальних обмежень щодо доступу до засобів інформаційного нападу, які призводять до численних фактів їх застосування конкурентами, кримінальними елементами, іншими суб’єктами.

Окрім того, за умов жорстокої конкурентної боротьби, суб’єки економічних ринків проводять акт недобросовісної конкуренції, дії котрі пов’язані із промисловим шпигунством, тому виникла потреба в розмежуванні доступу до носіїв інформації безпосередньо та особливо на підприємствах, розділення та визначення порядку отримання та використання інформації обмеженим та/або необмеженим доступом.

Підприємницька діяльність досить насичена не тільки діловими відносинами, їй значною мірою притаманні тісні інформаційні стосунки партнерів та конкурентів. Останні ж регулюються відповідними законодавчими та нормативними актами держави, а також нормативними документами підприємницьких структур.

Згідно зі ст. 60 Закону України «Про банки і банківську діяльність» до банківської таємниці належить інформація про діяльність і фінансовий стан клієнта, що стала відома банку у процесі його обслуговування і взаємовідносин із ним або з третіми особами під час надання послуг банком, розголошення якої може завдати матеріальної чи моральної шкоди.

Тлумачення поняття комерційної таємниці дається у ст. 30 Закону України «Про підприємства в Україні». Зокрема у статті вказується, що під комерційною таємницею підприємства розуміють відомості, пов’язані з виробництвом, технологічною інформацією, управлінням фінансами та іншою діяльністю підприємства, що не є державною таємницею, розголошення (передання, витік) яких може завдати шкоди його інтересам.

Відповідно до ч. 3 ст. 30 Закону України «Про інформацію» власникам конфіденційної інформації надано право самим включати її до категорії конфіденційної, визначати режим доступу до неї та встановлювати систему (способи) її захисту.

Комерційна таємниця підприємства і проблеми її охорони і захисту.

Під комерційною цінністю інформації можна розуміти грошовий еквівалент, який в даному випадку може бути сплачений за право володіння відомостями. Конкуренти і інші суб'єкти, прямо або побічно пов'язані з підприємством, об'єктивно зацікавлені в зборі і отриманні інформації самого різного роду. Потенційна комерційна цінність відомостей має місце у разі, коли при певних обставинах, в певний час і у визначеному місці з'являється або може з'явитися інтерес третіх осіб до придбання інформації про підприємство [3].

Вільний доступ до відомостей означає відсутність заходів, направлених на охорону і захист інформації від спроб ознайомлення з нею третіх осіб. У вільному доступі, як правило, знаходяться загальні довідкові відомості про підприємство - реквізити, історія створення, основні напрями діяльності підприємства в тій частині, в якій вони не захищені положенням про комерційну таємницю. Деякі підприємства, які проводять політику інформаційної відвертості і організаційної прозорості для необмеженого кола осіб, можуть залежно від специфіки своєї діяльності розміщувати інформацію про своїх працівників, ціни на продукцію, що випускається, або послуги, що надаються. У ряді випадків у вільному доступі знаходяться повідомлення прес-служби або іншого підрозділу, адресовані засобам масової інформації, які можуть стосуватися різних питань діяльності підприємства.

Конфіденційність інформації охороняється підприємством, та здійснюється, на підставі виданих локальних нормативних актів, найважливішим з яких є «Положення про комерційну таємницю». Усі заходи безпеки, захисту інформації від несанкціонованого доступу ззовні і усередині підприємства з боку не уповноважених співробітників повинні базуватися саме на положеннях даного документа

Відомості, які доцільно відносити до предмету комерційної таємниці, по сферах і характеру діяльності підприємства можна виділити наступні групи відомостей:

* відомості про фінансову діяльність;
* інформація про ринок;
* відомості про виробництво, виконання робіт і надання послуг;
* відомості про наукові розробки;
* відомості про систему матеріально-технічного забезпечення;
* відомості про персонал підприємства;
* відомості про принципи управління підприємством;
* інші відомості.

Відомості про фінансову діяльність.

Параметри діяльності підприємства, виражені в грошовому еквіваленті, можуть дати обширне і досить вичерпне уявлення про його фінансовий стан, наявність заборгованості, об'єм оборотних коштів, географія вироблюваних платежів і так далі.

Інформація про використовувані підприємством кредити може бути використана для визначення і з'ясування особливостей нового напряму діяльності (комерційних задумів і проектів) [11].

Інформація про ринок.

Вироблювані підприємством маркетингові дослідження, а також експерименти, пов'язані із залученням потенційних клієнтів до вироблюваної продукції або послуг, що надаються, представляють інтерес як готовий інформаційний продукт, отриманий в ході витратної діяльності. Інформація такого роду повинна охоронятися особливо ретельно, оскільки саме з її допомогою підприємство може добитися істотного збільшення рентабельності своєї діяльності, збільшити свою частку на товарних ринках або ринках послуг.

Відомості про виробництво, виконання робіт і надання послуг.

Об'єм і асортимент продукції, що випускається, або специфіка що надаються є однією з найважливіших економічних характеристик підприємства. Дані характеристики можуть також дати деякі уявлення про використовувані підприємством технології, про наявність або відсутність власного дослідницького підрозділу і тому подібне.

Відомості про наукові розробки.

Це - перспективні високотехнологічні галузі української економіки, такі як розробка програмного забезпечення, телекомунікація, біотехнологія, виробництво устаткування, літакобудування, космонавтика і тому подібне. Наукові розробки можуть бути як на великих, так і на середніх і малих підприємствах, тому особливо важливо не нехтувати заходами безпеки в невеликих колективах - наявність інтересу ззовні залежить не від розміру підприємства, а від наявності перспективних розробок.

Відомості про систему матеріально-технічного забезпечення.

Під системою матеріально-технічного забезпечення зазвичай розуміють зведення про склад клієнтів, представників і посередників, потребу в матеріалах, сировині, аксесуарах і деталях конструкцій і інтер'єрів, джерела задоволення цих потреб, транспортні і енергетичні потреби підприємства.

Відомості про персонал підприємства.

Кількісні і якісні характеристики персоналу дають третім особам можливість за допомогою аналітичних дій робити висновки про деякі інші його параметри - про продуктивність праці і, таким чином, рівень виробництва, про наявність контактів з іноземними постачальниками або клієнтами, що набувають продукції або послугами підприємства, що користуються.

Інші відомості.

Серед інших відомостей, які складають предмет комерційної таємниці підприємства, можна виділити безпосередньо:

* важливі елементи систем безпеки, кодів і процедур доступу до інформаційних мереж і центрів;
* принципи організації охорони і захисту комерційної інформації і комерційної таємниці на підприємстві.

З відомостями такого роду постійно працюють, і часто вони знаходяться не в електронному вигляді, а в твердому (роздруковані). Тому виникає потреба в обмеженні доступу в приміщення, де вони обробляються та зберігаються.

## **1.2 Технології безпечного доступу на об’єкт**

Найбільш часте застосування контроль доступу знаходить в офісних будівлях, готельних комплексах і невеликих готелях, бізнес-центрах, що здають в оренду свої приміщення безлічі компаній, магазинах і, звичайно ж, контрольно-пропускних пунктах (кпп). Службовці часто ходять з одного кабінету в іншій і, природно, можуть забувати закривати двері, коли в приміщенні нікого не залишається. У цьому випадку контроль доступу є невід'ємною частиною загальної системи безпеки будівлі. Крім цього СКУД може застосовуватися на території виробничих або торгових компаній для обмеження доступу персоналу в приміщення з цінними речами. Можливість проходу в них дістають тільки люди, що мають певний рівень довіри і відповідальності. Використання контролю доступу також має місце на стоянках, парковках і в'їздах на територію. Зазвичай проводиться інтеграція засобів СКУД з автоматикою - шлагбаумами і комірами.

Контроль доступу допомагає людині виконувати рутинні завдання і по суті, як і будь-яка інша система безпеки, є інструментом в забезпеченні безпеки, тоді як людина приймає на себе управління в складних ситуаціях, котрі вимагають нестандартних рішень. Контроль переміщення людей або транспорту - це те, що входить в область дії системи, і залежно від наявних засобів і функцій дозволяє протидіяти несанкціонованому проходу, проїзду або проносу на територію, що охороняється, або з неї, вести реєстрацію людей і автомобілів, зберігаючи інформацію про те, коли людина прийшла / пішла, і на підставі цих даних створювати звіти для подальшого аналізу і обробки.

Такого роду автоматизація дозволяє здійснювати рух, реєстрацію людей і транспорту цілодобово, не задіюючи додаткові ресурси. В сукупності з іншими системами безпеки, такими як пожежна або охоронна сигналізація і відео спостереження, контроль доступу здійснює комплексну безпеку з централізованим управлінням.

Контроль доступу може бути автономною або мережевою системою. Мережева скуд на відміну від автономної вимагає додаткового устаткування і програмного забезпечення, за рахунок чого його ціна вища. У випадку з автономним скуд всі дані (код карти, дані про власника, дозволений час проходу і так далі) зберігаються в пам'яті контролера і нікуди не передаються. Такі системи ефективні для невеликих масштабів, коли необхідно ввести контроль доступу на декілька точок доступу, а спектр вирішуваних завдань невеликий. Мережеві системи контролю доступу дозволяють значно розширити можливості по здійсненню безпеки, тому їх частіше застосовують в крупних будівлях з великою кількістю людей, таких як готелі, склади і офісні будівлі [2].

## **1.3 Огляд існуючих систем доступу на підприємство**

Комп'ютери і сервери зі встановленим програмним забезпеченням - верхній рівень класичної мережевої системи контролю управління доступом (СКУД), вони управляють підключеними до них контролерами.

Контрольна панель, або як ще називають контролер, спеціалізований високо надійний комп'ютер. У ньому зберігається інформація про конфігурацію, режими роботи системи, список людей, які мають право входити в приміщення, а також їх права доступу в ці приміщення (коли і куди саме можна ходити).

У великих системах контролерів може бути декілька. У простих випадках мінімальний варіант контролера може бути вбудований в зчитувач.

Зчитувач є другою важливою ланкою в СКУД і підключається до контролера. Зчитувач це пристрій, який дозволяє прочитувати інформацію, записану на ідентифікаторі (картка, брелок). Цю інформацію він передає в панель, яка і ухвалює рішення про допуск людини в приміщення. Можна набудувати панель так, що вона запрошуватиме підтвердження ухваленого рішення у оперативного чергового.

Ідентифікатор (карта, брелок, біометрична ознака) має свій унікальний номер, якому приписаний деякий рівень доступу, відповідно до якого користувач має право проходу через ті або інші двері/турнікети в певні проміжки часу. Якщо ідентифікатор використовується як карта, її одночасно можна використовувати як пропуск з фотографією (нанести фотографію можна за допомогою спеціалізованого принтера карт) [4].

Виконавчі пристрої є “нижніми” елементами СКУД, це може бути електромеханічний або електромагнітний замок, турнікет, шлагбаум, автоматичні ворота і так далі.

Основною функцією такого виконавчого пристрою полягає у виконанні команди контролера на блокування або розблокування проходу (проїзду).

Сучасні СКУД.

Одразу визначемо, що застосування електронних СКУД не виключає участь людини в процесі управління. Найбільш ефективною є система, де функції загального контролю виконує людина, а електроніка, що є всього лише інструментом забезпечення безпеки, бере на себе виконання простих рутинних операцій.

Проте, сучасні СКУД дозволяють ефективно забезпечувати регулювання і контроль процесів доступу, і переміщення людей, машин, будь-яких інших об'єктів в зонах, що охороняються. Залежно від складності, вони дозволяють: попереджати і протидіяти несанкціонованому проникненню осіб в заборонені приміщення, споруди і зони; виявляти факт проносу зброї, заборонених матеріалів і речовин; реєструвати факт проходу кожної людини, з прив'язкою до часу і додатковою службовою інформацією для подальшого аналізу і обробки.

Також в них можуть бути реалізовані можливості дистанційного керування процесом доступу людей і автотранспорту на територію і в кожне приміщення за рахунок застосування спеціалізованих виконавчих пристроїв (турнікети, шлюзи, шлагбауми і інші виконавчі пристрої СКУД). Автоматизація дій і реакцій дозволяє працювати 24 години в добу, не помилявшись при виконанні одноманітних рутинних операцій. Зрештою, підвищується загальна ефективність різних підсистем безпеки за рахунок їх інтеграції в єдиний комплекс з централізованим управлінням: СКУД, системи охоронно-пожежної сигналізації (ОПС), відео-нагляду, управління автоматикою будівель і споруд (інтегровані системи). Найбільш досконалими і ефективними СКУД є системи з комп'ютерним управлінням, в яких широкі можливості електроніки управління доповнюються практично необмеженим потенціалом програмного забезпечення.

Класифікація і функціональні характеристики СКУД.

За способом управління СКУД діляться на: автономні, централізовані (мережеві) і універсальні.

Автономні системи призначені для управління одним або декількома виконавчими пристроями без обміну інформацією з центральним пультом (зазвичай комп'ютером) і без контролю з боку оператора. Їх застосування цілком виправдане, коли потрібно контролювати прохід через одну - дві точки і немає необхідності вести онлайн моніторинг подій доступу. У таких системах часто сам контролер конструктивно об'єднується в одному корпусі зі зчитувачем. Програмуються вказані контролери, як правило, або кнопкових панелей або за допомогою «мастер» - карт, що дозволяють заносити в пам'ять контролера нові карти і видаляти старі.

До переваг автономних систем відносяться невисока вартість, простота програмування системи, оперативність монтажу, зручність використання для невеликих об'єктів, що не мають спеціалізованих охоронних підрозділів.

Небагата функціональність породжує і свої недоліки - це незручність процесу програмування у разі великої кількості дверей і користувачів, відсутність можливості оперативної дії на процес проходу, відсутність можливості обробки протоколу подій і отримання вибіркового звіту по заданих критеріях.

Централізовані (мережеві) системи - це величезний клас СКУД, головна особливість яких в тому, що вони мають можливість конфігурації апаратури і управління процесом доступу з комп'ютерних терміналів. Різні СКУД мають свої індивідуальні особливості і розрізняються по архітектурі, масштабу і можливостям, типу вживаних зчитувачі, ступені стійкості до злому.

Більшість мережевих СКУД зберігають багато переваг автономних систем, основне з яких - робота без використання комп'ютера, що управляє. Це означає, що при виключенні комп'ютера, що управляє, система фактично перетворюється на автономну. Контролери даних систем, так само як і автономні контролери, мають власний буфер пам'яті номерів карт користувачів і подій, що відбуваються в системі. Наявність в системі комп'ютера дозволяє службі безпеці оперативно втручатися в процес доступу і здійснювати управління системою в режимі реального часу.

Найважливішим елементом мережевих СКУД є програмне забезпечення. Воно відрізняється великою різноманітністю - від простих програм (які дозволяють додавати в базу даних нових користувачів і видаляти вибулих) для одного терміналу, що управляє, до складних програм з архітектурою клієнт-сервер.

Перевага мережевих систем полягають в зручності програмування, можливості прямого оперативного управління об'єктами, наочному відображення подій в режимі реального часу, можливості створення систем великого масштабу. Окремо потрібно відзначити широкі можливості інтеграції з іншими системами безпеки [28].

До списоку недоліків входить необхідність навчання персоналу, вища вартість та більші витрати на монтаж.

Універсальні системи є різновидом мережевих СКУД, вони здатні переходити в режим автономної роботи у разі виникнення відмов комп'ютера, мережевого устаткування або обриві зв'язку. Такі системи забезпечують підвищений рівень надійності, проте в деяких системах при переході в автономний режим втрачається ряд важливих функцій, на що потрібно звертати особливу увагу. Це пов'язано з архітектурою систем і ступенем реалізації функцій на апаратному рівні (чим більше реалізовано апаратних функцій, тим вище ступінь автономності і надійності універсальної СКУД) [36].

## **1.4 Принцип роботи мережевої системи контролю доступу**

Співробітники отримують в постійне користування електронний ключ у вигляді картки або брилка із записаним на них унікальним кодом (у випадку з відвідувачами їм видаються гостьові картки). Картки закріплюються за персоналом, а їх дані заносяться в базу даних на робочій станції. На місцях де необхідно організувати точку доступу, встановлюються зчитувачі, що розпізнають код карти і що передають його в контролер. Він порівнює дані з бази з прочитаним кодом, на підставі чого ухвалює рішення - відкривати прохід чи ні. У позитивному випадку подається команда відкриття на виконавчий пристрій, будь-то турнікет, шлагбаум або електромагнітний замок, після чого людина отримує доступ і може пройти. При відмові може бути задіяна охоронно-пожежна сигналізація (опс), блокування дверей або інші дії залежно від функціональності системи контролю доступу. Дані про того, хто і коли пройшов, фіксуються в базі даних. На їх підставі можна формувати звіти, що дозволяють вести облік робочого часу, виявляти порушників трудової дисципліни або простежувати шляхи проходження можливих зловмисників.

Головною перевагою мережевої СКУД є висока масштабованість, тобто здатність системи збільшувати свої можливості шляхом нарощування числа функціональних блоків, що виконують одні і ті ж завдання. Завдяки цьому вона підходить як для приватних будинків і маленьких офісів, так і для крупних готелів, ділових центрів і заводів. Перед системами безпеки і контролю доступу сьогодні стоять непрості завдання: вони повинні надійно захищати від небажаних проникнень на територію, що охороняється, але в той же час безперешкодно пропускати своїх, бути зручними в роботі і доступними за ціною.

Сучасні СКУД - це інтегровані програмно-апаратні системи. Вони дозволяють в режимі реального часу управляти всіма дверима, шлагбаумами і турнікетами за допомогою одного ключового елементу. Це можуть бути електронні ключі з чіпом, радіо пульти, карточки-проксиміті і навіть прилади отримання біометричної інформації (відбитків пальців, долонь, будови сітківки ока і т.д.). Все це - ідентифікатори. Всіма перерахованими процесами управляє спеціалізоване програмне забезпечення. Під час роботи воно проводить швидкий збір, обробку і зберігання даних про перетини охоронних зон, а також надає масу додаткових можливостей: гнучку настройку пропускних режимів, організацію індивідуальних розкладів доступу для кожної особи, збір і аналіз відомостей про тривалість його перебування в тому або іншому приміщенні, реєстрацію спроб несанкціонованого доступу та ін.



Рис. 1.1 Мережева СКУД на одні двері

Система контролю доступу і обліку робочого часу для невеликого офісу з одним входом. Поряд з дверима встановлюються зчитувачі на вхід і на вихід. Прикладаючи картку до зовнішнього зчитувача, співробітник відкриває двері. Час проходу записується в базу даних і служить відміткою про початок робочого дня. При виході в кінці дня прикладена картка відзначає кінець робочого дня. Проходи протягом робочого дня, наприклад, на обід, залежно від настройок програмного забезпечення, можуть відніматися з робочого часу, або не впливати на тривалість робочого дня. Співробітники з різних підрозділів можуть мати різні розклади доступу і робочого часу на день і тиждень. Всього може бути задане до 7 розкладів. Пам'ять контролера зберігає більше 4000 карт доступу і стількох же подій. У разі виключення комп'ютера система працюватиме автономно. Після відновлення зв'язку з комп'ютером всі дані про проходи будуть автоматично записані в базу даних [30].

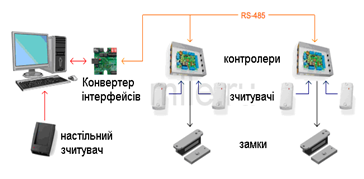


Рис. 1.2 Мережева СКУД на двоє дверей

Мережева система контролю доступу і обліку робочого часу для офісу з двома входами. Для реєстрації карт співробітників використовується настільний зчитувач, що підключається до комп'ютера по USB.

Контролери оснащені вбудованими джерелами безперебійного живлення (Рис.1.3).

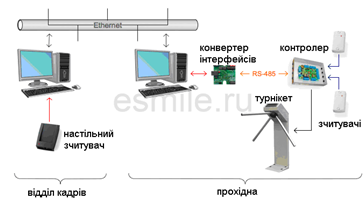


Рис. 1.3 Мережева СКУД на прохідній

Мережева система контролю доступу і обліку робочого часу для устаткування прохідною невеликого підприємства. Комп'ютер, встановлений на прохідній, виконує функції зв'язку з контролером, турнікетом і фотоверифікації. Реєстрація карт співробітників і управління системою контролю доступу здійснюється за допомогою комп'ютера, встановленого у відділі кадрів [32].

## **1.5 Елементи ідентифікації в сучасних системах доступу**

У всіх ключових елементів, використовуваних в системах контролю, одна і та ж мета: передати зчитувальному пристрою «зашитий» в них код доступу. Але роблять вони це по-різному, залежно від пристрою.

Найпростіший спосіб ввести код - просто набрати його вручну з клавіатури. В цьому випадку як зчитуючий елемент може використовуватися цифрова кодова панель з кнопками, і відео-спостереження на "підстраховці". Таке рішення відрізняється дешевизною, але володіє найнижчим ступенем захищеності, комбінацію символів можна підглянути або просто повідомити іншій особі. До того ж кодові панелі не дуже зручні: на набір цифр з клавіатури потрібний час.

Набагато практичніше використовувати пристрої, в яких код доступу вже запрограмований заздалегідь. Це контактний пристрій, і для його використання потрібно всього лише прикласти металеву частину ключа до спеціального гнізда-зчитувача. Код в кожному екземплярі унікальний і не міняється протягом всього терміну експлуатації.

Інший тип контактних ключових елементів - карти з магнітною смугою невеликого формату. Для зчитування необхідно помістити карту потрібною стороною в приймальний пристрій і провести через нього. Така операція вимагає певного часу, до того ж магнітна смуга може забруднитися, не говорячи вже про те, що вона чутлива до дії магнітних полів, здатних вивести її з ладу.

Набагато зручніше безконтактні ключові елементи: карточки-проксиміті, що набули найбільш широкого поширення в СКУД, і ключі з електронним чіпом-транспондером. І в тих і інших чіп починає діяти на відстані 5-15 см від зчитувача, і ідентифікація відбувається практично миттєво. Крім того, часто на лицьову сторону картки поміщають інформацію про власника: прізвище, ім'я і фотографію, що дає можливість використовувати її і як звичайний пропуск [3].

## **1.6 Вимоги до виконавчих пристроїв СКУД**

Вимоги до пристроїв ідентифікації.

Зчитувачі повинні забезпечувати надійне прочитання коду з ідентифікаторів перетворення його в електричний сигнал і передачу на контролер.

Зчитувачі повинні бути захищені від маніпулювання шляхом перебору, підбору коду і радіочастотного сканування.

При введенні невірного коду повинне блокуватися введення на якийсь час, величина якого задається в паспортах на конкретні види зчитувачів. Час блокування повинен бути вибраний так, щоб забезпечити задану пропускну спроможність при обмеженні числа спроб підбору. При трьох спробах введення неправильного коду повинне видаватися тривожне сповіщення. Для систем, що працюють в автономному режимі, тривожне сповіщення передається на звуковий/світловий оповісник, а для систем, що працюють в мережевому режимі, - на центральний пульт з можливістю дублювання звуковим/світовим оповісником. Тривожне сповіщення повинне видаватися також при будь-якому акті вандалізму.

Конструкція, зовнішній вигляд і написи на ідентифікаторі та зчитувачі не повинні приводити до розкриття секретності коду.

Пристрої ідентифікації, аналогічно виконавчим пристроям, повинні бути захищені від впливу шкідливих зовнішніх чинників і вандалізму.

Виробник повинен гарантувати, що даний код ідентифікатора не повториться, або вказати умови повторюваності коду і міри по запобіганню використання ідентифікаторів з однаковими кодами.

Для автономних систем користувач повинен мати можливість змінити або переустановити відкриваючий код в міру необхідності, але не менше 100 разів. Зміна коду повинна бути можлива тільки після введення коду, що діє. При виборі ідентифікаторів слід мати на увазі, що клавіатура забезпечує низький рівень безпеки; магнітні картки - середній; Proximity, Віганд – картки і електронні ключі Touch Memory - високий; біометричні - дуже високий рівень безпеки.

Вимоги до виконавчих пристроїв.

Пристрої повинні забезпечувати відкриття/закриття замкового механізму або пристрою загороди при подачі сигналу, від контролера, а також необхідну пропускну спроможність для даного об'єкту.

Параметри сигналу (напруга, струм і тривалість), що управляє, повинні бути вказані в стандартах і/або ТУ на конкретні види пристроїв загороди.

Величина напруги, що рекомендується, лінія 12 або 24 В. Проте, для деяких видів приводів виконавчих пристроїв (ворота, масивні двері, шлагбауми) допускається використовувати електроживлення від мережі 220/380 В.

Умисне пошкодження зовнішніх електричних сполучних ланцюгів не повинне приводити до відкриття пристрою загороди.

У разі зникнення електроживлення в пристроях, повинна передбачатися можливість живлення від резервного джерела струму, а також аварійне механічне відкриття пристроїв загороди.

Аварійна система відкриття повинна бути захищена від можливості використання її для несанкціонованого проникнення.

Пристрої повинні бути захищені від впливу шкідливих зовнішніх чинників (електромагнітних полів, статичної електрики, нестабільної напруги живлення, пилу, вологості, температури і тому подібне) і вандалізму.

Вимоги до пристроїв контролю і управління доступом.

Контролери, що працюють в автономному режимі, повинні забезпечувати прийом інформації від зчитувачів, обробку інформації і вироблення сигналів управління для виконавчих пристроїв.

Контролери, що працюють в мережевому режимі, повинні забезпечувати:

* обмін інформацією по лінії зв'язку між контролерами і керівним комп'ютером або провідним контролером;
* збереження пам'яті, установок, кодів ідентифікаторів при обриві зв'язку з комп'ютером (провідним контролером), що управляє, відключенні живлення і при переході на резервне живлення;
* контроль ліній зв'язку між окремими контролерами і між контролерами і комп'ютером, що управляє.

Для гарантованої роботи СКУД відстань між окремими компонентами не повинна перевищувати величин, вказаних в паспортах (якщо не використовуються модеми).

Протоколи обміну інформацією і інтерфейси повинні бути стандартних типів. Види і параметри інтерфейсів повинні бути встановлені в паспортах і/або інших нормативних документах на конкретні засоби з урахуванням загальних вимог ГОСТ 26139.

Типи інтерфейсів, що рекомендуються:

- між контролерами RS 485;

- між контролерами і комп'ютером, що управляє, -RS 485.

Вигляд і ступінь захисту повинні бути встановлені в паспортах на конкретні види засобів або систем. Відомості, приведені в технічній документації, не повинні розкривати секретність захисту.Програмне забезпечення при необхідності належного бути захищено від несанкціонованого копіювання.

Програмне забезпечення повинне бути захищене від несанкціонованого доступу за допомогою паролів.

Кількість рівнів доступу по паролях повинна бути не менше 2.

Рівні доступу за типом користувачів, що рекомендуються:

* + перший ("адміністрація") - доступ до всіх функцій контролю і доступу;
  + другий ("оператор") - доступ тільки до функцій поточного контролю;
  + третій ("системщик") - доступ до функцій конфігурації програмного забезпечення, без доступу до функцій, що забезпечують управління пристроїв.

При введенні пароля на екрані дисплея не повинні відображатися знаки, що вводяться. Число символів пароля повинне бути не менше 5.

Вимоги до електроживлення.

Електропостачання засобів СКУД повинне здійснюватися від вільної групи щита чергового освітлення або від спеціально встановленого для цих цілей електрощита. Щит електроживлення, що встановлюється поза приміщенням, що охороняється, повинен розміщуватися в металевій шафі і повинен бути заблокований на відкриття.

Основне електроживлення СКУД повинне здійснюватися від мережі змінного струму частотою 50 Гц з номінальною напругою 220 В. СКУД повинні зберігати працездатність при відхиленнях напруги від -15 до +10 % і частоти до ±1 Гц від номінального значення.

Електроживлення окремих СКУД допускається здійснювати від інших джерел з іншими параметрами вихідної напруги, вимоги до яких встановлюються в нормативних документах на конкретні типи систем.

Засоби СКУД повинні в обов'язковому порядку мати резервне електроживлення при пропажі основного джерела електроживлення.

Перехід на резервне живлення і назад повинен відбуватися автоматично без порушення встановлених режимів роботи і функціонального стану СКУД. Номінальна напруга резервного джерела живлення повинна бути 12 або 24 В.

При використанні, як резервне джерело, живлення акумуляторної батареї, повинна забезпечуватися робота засобів СКУД не менше 8 годин.

При використанні, як джерело живлення акумулятора або сухих батарей, повинна бути передбачена індикація розряду акумулятора або батареї нижче за допустиму межу.

## **1.7 Постановка задачі дослідження**

При дослідженні я керувалася такими нормативними документами:

1.НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”

2.НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”

3.ДСТУ 4163-2003 Вимоги до оформлювання документів

4.Закон України „Про інформацію”

5.Закон України „Про науково-технічну інформацію”

6.ДСТУ 3008 – 95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення

7.ГОСТ 34.602-89 вимоги до технічного завдання на проектування автоматизованих систем

Згідно з ГОСТ 34.602- 89 технічне завдання має вигляд:

1. Загальні відомості:

- повне найменування системи і її умовне позначення – «Методи біометрії в АС доступу на підприємстві »;

- Найменування розробника/замовника системи – ФККПІ, БІКС, БІ-241М, Савчук Г.А./ФККПІ БІКС

2. Причини і мета створення (розвитку) системи.

Метою створення системи є: з використанням біометричних методів спроектувати систему контролю доступу на підприємстві.

3. Вимоги до системи:

- вимоги до структури і функціонування системи, перелік підсистем;

– до складу системи входять наступні підсистеми: система управління виконуючими пристроями (замки, турнікети); система порівняння даних отриманих з біометричних датчиків.

Вимоги до структури.

Згідно з НД ТЗІ 2.5-005-99 дана система відповідає стандартному функціональному профілю захищеності в КС, що входять до складу АС класу 2, з підвищеними вимогами до забезпечення конфіденційності і цілісності оброблювальної інформації.

2КЦ.1={КД-2,ЦД-1,НР-2,НИ-2,НК-1,НО-1,НЦ-1}

**Система контролю управління доступом (СКУД)** дозволяє візуально контролювати вхід/вихід, і навіть спробу входу в недозволене доступом приміщення співробітника або відвідувача об'єкта, що охороняється.

СКУД дозволяє призначити кожному співробітнику індивідуальний часовий графік роботи, зберегти та потім переглянути інформацію про події за день. Системи можуть працювати в автономному режимі та під управлінням комп'ютера. Залежно від розмірів об'єкта, кількості приміщень і чисельності персоналу може вибиратися той чи інший вид устаткування та програмного забезпечення.

**Система контролю доступу в якості компонента загальної системи безпеки дозволяє:**

* Виключити потрапляння на територію підприємства сторонніх осіб. Система виводить на монітор охорони фотографію людини, проходить через прохідну, здійснює пропуск співробітників строго відповідно до графіка роботи даної категорії персоналу, а також виконує облік робочого часу.
* Здійснити автоматичний доступ в різні приміщення тільки тих співробітників підприємства, які внесені в список допущених для проходу в кожне з контрольованих приміщень.
* Формувати протокол подій.

**Система контролю управління доступом складається з:**

* Основних елементів (комп'ютер, контролери, програматор, зчитувачі).
* Виконавчі елементи (електромеханічні замки, електрозащіпки, електро-магнітні замки, турнікети).
* Якщо підбір основного обладнання залежить від складності об'єкта, що захищається, та кількості користувачів в системі, то виконавчі елементи залежать від матеріалу (поверхні), на яку вони будуть змонтовані, при цьому необхідно враховувати також естетичні нюанси.

Сучасні **СКУД** легко інтегруються з 1С-бухгалтерією (для формування табеля робочого часу) та іншими системами безпеки. СКУД також використовуються в сфері розважального бізнесу - це забезпечення платного проходу та оплата послуг на об'єктах де є зацікавленість використання єдиної системи оплати (єдина карта з якимось грошовим еквівалентом) - це катки, гірськолижні курорти та ін.

При виборі систем безпеки необхідно враховувати, що з часом системи безпеки мають властивість морально застарівати та стають більш уразливими для зловмисників. З кожним роком з'являються нові й більш доступні засоби та методи, за допомогою яких можна обдурити систему безпеки та завдати шкоди у вигляді викрадення матеріальних цінностей або інформації. В середньому розрахований термін служби системи безпеки - 5-10 років, по закінченню цього терміну систему доводиться модернізувати або міняти повністю (в залежності від того, яке обладнання було встановлено спочатку).

Ефективність **системи контролю доступу** помітно зростає при інтеграції з системами відеоспостереження та сигналізації.

**Для обслуговування великого об'єкта бажано встановлювати комплекс автоматизованої системи безпеки, який складається з:**

* Системи пожежної сигналізації.
* Системи оповіщення про пожежу.
* Системи охоронної сигналізації.
* Системи охоронного відеоспостереження.
* Системи контролю управління доступом.

Для інтеграції всіх складових комплексу автоматизованої системи безпеки передбачений **програмний комплекс BIS (Building Integration System)**.  
  
Даний комплекс є інтегральною платформою для об'єднання всіх систем безпеки, а також інших систем, наприклад: інженерного обладнання, яке необхідно для нормального функціонування чергових та диспетчерських служб.

Автоматизованим методом ідентифікації за відбитком пальців дуже поширений у багатьох країнах світу. Технологія використовується в офісах, на підприємствах, в організаціях, де необхідно забезпечити надійну перевірку осіб, допущених до їх відвідування. Контролювати доступ зручніше за відбитком пальця.

## **Висновок до 1 розділу**

При проведенні аналізу розглянутих вище систем контролю доступу, основаних на класичних методах, було виявлено ряд недоліків:

1. Проблеми виникають із забороною подвійного проходу, функція якого є в більшості СКУД, контролюючих не тільки вхід, але і вихід. Ця функція призначена для того, щоб утруднити можливість передачі ключа-ідентифікатора іншій особі: якщо даним ключем вже скористалися при вході, ідентифікатор буде блокований до тих пір, поки контролер не зафіксує вихід його власника з об'єкту. Проте в житті виникає безліч ситуацій, при яких чоловік, скориставшись ключем, не входить в приміщення або зволікає з входом. Ось в цьому випадку при повторному використанні ідентифікатора система відмовляє співробітникові у вході, оскільки по її відомостях він вже увійшов і знаходиться на об'єкті.

2. Певні проблеми можуть виникнути, якщо співробітник втратив, забув або десь залишив свій ідентифікатор. Якщо подібна ситуація відбулася поза об'єктом, що охоронявся, то питання входу можна без особливих проблем вирішити з охоронцем або оператором СКУД. Але якщо ключ загубився на роботі, а людина не може вийти з приміщення, що охороняється, і пропускає час, після якого виходи блокуються автоматично, то проблема може бути набагато складнішою.

3. Ідентифікатор може бути викрадений або дубльований, тоді безпека підприємства під загрозою. Тим більше, що дані системи не можуть забезпечувати захист об’єктів з підвищеними вимогами безпеки.

Виходом з даної ситуації може бути використання засобів біометричної ідентифікації. Оскільки в них ідентифікується не предмет, (брелок, магнітна карта та ін.), а сама особа - носій біометричної інформації.

# РОЗДІЛ 2. БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ

## **2. Біометричні технології**

Біометрична ідентифікація – це спосіб ідентифікації особистості за окремими специфічними біометричними ознаками (ідентифікаторами), які властиві конкретній людині. Біометричні технології базуються на біометрії, вимірюванні унікальних характеристик окремо взятої людини. До них належать унікальні ознаки, отримані нею з народження (ДНК, відбитки пальців, райдужна оболонка ока) або характеристики, придбані згодом або ж здатні змінюватися з віком або в результаті зовнішнього впливу (почерк, голос або хода) [1].

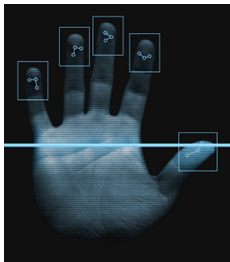


Рис. 2 Знак біометрії

Біометрія - унікальна, вимірна характеристика людини для автоматичної ідентифікації або верифікації. Термін «автоматично» означає, що біометричні технології повинні розпізнавати або верифікувати людину швидко і автоматично, в режимі реального часу. Ідентифікація за допомогою біометричних технологій припускає порівняння раніше внесеного біометричного зразка з біометричними даними, що знову надаються.

Біометричні технології застосовуються в багатьох областях, пов’язаних із забезпеченням безпеки доступу до інформації й матеріальних об’єктів, а також у завданнях унікальної ідентифікації особистості.

Біометричний захист ефективніший порівняно з такими методами, як використання смарт-карт, паролів, PIN-кодів і тому подібне, оскільки біометрія дозволяє ідентифікувати людину, а не пристрій. Традиційні методи захисту не виключають можливості втрати або крадіжки інформації, унаслідок чого вона стає доступною незаконним користувачам. Відбиток же пальця або малюнок радужної оболонки унікальні, їх майже неможливо відняти і не можна забути.

Застосування біометричних технологій різноманітні: доступ до робочих місць і мережних ресурсів, захист інформації, забезпечення доступу до певних ресурсів і безпека. Ведення електронного бізнесу й електронних урядових справ можливе тільки після дотримання певних процедур з ідентифікації особистості. Біометричні технології використовуються в області безпеки банківських обігів, інвестування тощо, а також роздрібній торгівлі, охороні правопорядку, питаннях охорони здоров’я, а також у сфері соціальних послуг.

За останні два десятиліття біометричні технології зробили великий крок уперед. Багато в чому цьому сприяло поширення мікропроцесорних технологій. Використання в системах контролю й управління доступом (СКУД) біометричних сканерів практично не ускладнює систему безпеки, і їх вартість для деяких біометричних методів дуже низька. Навіть більше, близько третини ноутбуків та смартфонів випускаються зараз із вбудованою системою зчитування відбитка пальців, а за наявності в ноутбуці відеокамери на ньому можна встановити систему розпізнавання людини за геометрією обличчя.

**Сучасний стан.** Інформація, яка міститься в кількох біометричних параметрах, може бути інтегрована за допомогою різних методів на різних рівнях і в різному контексті. Прийнято поєднувати в один клас мультимодальні та багатофакторні рішення.

У мультимодальних системах ідентифікатори одного типу (наприклад, відбитки пальців) обробляються за допомогою різноманітних алгоритмів з метою підвищення надійності ідентифікації.

У багатофакторних системах разом з біометричними використовуються також і інші ідентифікатори (Pin-код, пароль, смарт-карта тощо).

Основною метою багатофакторних систем є прискорення процесу ідентифікації та/або надання можливості розпізнавання без звертання до централізованої бази даних ідентифікаторів.

Першими роботами з мультибіометричної ідентифікації вважають експерименти 1976–1978 рр. із застосування логічних класифікаторів для іденти- фікації за кількома біометричними характеристиками [21].

Існує безліч різних джерел інформації, які можуть бути використані для розширення можливостей біометричної системи.

Сьогодні виділяють такі методи інтеграції: – різні біометричні характеристики (зображення обличчя і відбиток пальця); – множинні біометричні характеристики (відбитки різних пальців, райдужна оболонка лівого і правого ока); – різні способи отримання біометричних зразків (зображення обличчя у видимому та інфрачервоному діапазоні); – різні сканери (дві фотокамери); – кілька зразків однієї біометричної характеристики; – кілька алгоритмів порівняння біометричних зразків [22].

Незалежно від методу має місце сильна або слабка двостороння інтеграція інформації з різних джерел.

У першому випадку вихідні сигнали від різних біометричних сенсорів можуть бути використані для створення сукупності більш точних та інформативних вхідних сигналів.

У другому – зв’язок між вхідними сигналами (наприклад, обличчя і відбитку пальця) буде досить слабким або взагалі відсутнім. У цьому випадку інтеграція відбувається на рівні автономних сенсорів, і кожен пристрій незалежно від інших оцінює біометричний зразок. Властивості і шаблони, які виділені однією біометричною системою, неприйнятні для іншої, тоді як значення персональних біометричних параметрів піддаються інтеграції.

У системах ідентифікації особистості інтеграція кількох біометричних характеристик відбувається або на рівні ухвалення рішення або на рівні обчислень [21]. Кількість помилок у системах біометричної ідентифікації визначається точністю, з якою внутрішній біометричний пристрій зіставлення зможе визначити, яка з гіпотез є дійсною. Вводячи біометричні зразки, можна будувати дві гіпотези: нульову та альтернативну.

Завдання визначення оптимального методу подібності можна звести до завдання оцінювання щільностей біометричних порівнянь. Але на етапі навчання мультибіометричної системи (визначення розподілів біометричних порівнянь) доступна лише досить обмежена інформація, яка використовується для оцінювання статистичних властивостей біометричних систем.

Це призводить до того, що по-перше, при використанні емпіричних частот як оцінок дійсних функцій розподілу спостерігають сильну залежність від навчальної вибірки й значну дисперсію результатів навчання.

По-друге, навіть при прийнятті певних припущень про динаміку помилок розпізнавання дисперсія прогнозу зі зменшенням рівня Коефіцієнту Невірного Допуску (КНД) росте неприйнятними темпами, що пояснюється нездатністю емпіричних щільностей до узагальнення на генеральну сукупність.

По-третє, слід враховувати, що інтеграцію технології застосовують для побудови систем ідентифікації з дуже низьким КНД, тому проблемою є верифікація результатів [22]. Для статистично залежних біометричних характеристик можна використовувати методи оцінювання щільностей розподілів, які оперують із багатомірним простором результатів порівнянь та залежно від рівня інтеграції біометричних технологій. Найпоширенішим випадком інтеграції залежних технологій є використання кількох алгоритмів порівнянь із метою поліпшення якості розпізнавання й підвищення надійності системи ідентифікації. Отриманий комбінований алгоритм можна розглядати як нову одномодальну біометричну технологію, що усуває проблеми з верифікацією результатів завдяки тому, що навчання і випробування можна провести на доступних масивах за окремими біометричним характеристикам [11; 21]. Постановка проблеми. Недостатній рівень достовірності результатів ідентифікації зумовлений неадекватним вибором методу або комбінації методів, помилками під час формування апаратних засобів і низькою інформативністю обраних критеріїв і характеристик.

**За принципом дії біометричні методи** **ідентифікації** поділяються на статичні (за ознаками, даними людині з народження), динамічні (за ознаками, що набуті в процесі існування) та комбіновані (поєднання двох перших) [6]. Фізіологічні (статичні) методи біометричної ідентифікації: – сканування райдужної оболонки ока; – сканування сітківки ока; – сканування рисунку вен долоні; – геометрія кисті руки (відбитки пальців – дактилоскопія, розмір, довжина і ширина долонь); – розпізнавання рис обличчя (контур, форма; розташування очей і носа); – структура ДНК-сигнатури.

Поведінкові (динамічні) методи;

– аналіз підпису (форма букв, манера письма, натиск);

– аналіз тембру голосу;

– аналіз клавіатурного почерку тощо [4; 7].

**За технологією реалізації**, методи ідентифікації особистості бувають: оптоелектронні, напівпровідникові, ультразвукові, піроелектричні, електрооптичні, комбіновані, телевізійні та тепловізійні. Найпоширенішими методами біометричної ідентифікації особистості є сканування райдужної оболонки і відбитків пальців, які разом становлять 2/3 від усього обсягу систем ідентифікації.

Більшість людей вважають, що в пам’яті комп’ютера зберігається зразок відбитка пальця, голосу людини або картинка райдужної оболонки його ока. Але в реальності це не так.

У спеціальній базі даних зберігається цифровий код довжиною до 1 000 біт, який асоціюється з конкретною людиною, що має право доступу. Сканер або будь-який інший пристрій, який використовується в системі, зчитує певний біологічний параметр людини, потім обробляє отримане зображення або звук, перетворюючи їх на цифровий код. Саме цей ключ і порівнюється із вмістом спеціальної бази даних для ідентифікації особистості [5].

## **2.1 Біометричні ідентифікації**

### 2.1.1 Дактилоскопія

Дактилоскопія – найбільш розроблений на цей час біометричний метод ідентифікації особистості. Швидкому розвитку методу слугувало його широке використання в криміналістиці ХХ століття. Розпізнавання відбитка пальця базується на аналізі розподілу особливих точок (кінцевих точок і точок розгалуження папілярних ліній), розташування яких задається в декартовій системі координат.



Рис.2.2.1 Вібиток вальця

Кожна людина має візерунок відбитків пальців, що є унікальний, завдяки цьому й здійснюється ідентифікація. Алгоритм ідентифікації використовує характерні точки на відбитках пальців, тобто закінчення лінії візерунка, розгалуження лінії, поодинокі точки. Також використовується інформація про морфологічну структуру відбитка пальця, його відносне положення замкнених ліній папілярного візерунка, аркових і спіральних ліній. Завдяки таким особливостям візерунка, отримана інформація перетворюються на унікальний код, що зберігає інформативність зображення відбитка в базі даних.

Основними алгоритмами порівняння, отриманого коду з шаблоном із бази даних є два: за характерними точками і за рельєфом усієї поверхні пальця.

Першим випадком виявляють характерні ділянки і запам’ятовується їхнє взаємне розташування. А другим – запам’ятовується вся «картина» в цілому.

У сучасних системах використовується також комбінація обох алгоритмів, що підвищує рівень надійності системи.

Під час оцінки, надійності процедури ідентифікації за відбитками пальців виникає питання чи існує можливість їхнього копіювання й використання іншими особами для отримання несанкціонованого доступу. Одним із варіантів введення в оману терміналу фахівці називають виготовлення штучної кисті з нанесеними на неї відбитками пальців.

Адекватним способом боротьби з такою фальсифікацією є використання інфрачервоного детектора, який дозволяє фіксувати теплове випромінювання від руки або пальця. Іншим способом підроблення є безпосереднє нанесення папілярного візерунка пальців законного користувача на руки зловмисника за допомогою спеціальних плівок. Однак у цьому випадку необхідно отримати якісні відбитки пальців законного користувача, причому саме тих пальців, які були зареєстровані системою.

Переваги методу:

1) висока достовірність (статистичні показники методу вищі за показники способів ідентифікації за обличчям, голосом, підписом);

2) низька вартість пристроїв, які сканують зображення відбитка пальця;

3) доволі проста процедура сканування відбитка.

Недоліки методу:

1) папілярний візерунок відбитка пальця дуже легко пошкоджується дрібними подряпинами, порізами;

2) недостатня захищеність від підроблення зображення відбитка.

### 2.1.2 Види біометрії відбитка пальця

За використання електронної дактилоскопії по алгоритмам виконання процедури, системи контролю, що діляться на такі типи:

* ідентифікація по характерних точках;
* розпізнання рельєфу всього відбитка пальця;
* комбіновані.
  + 1. Ідентифікація по характерних точках, технологія, що виконує аналіз тільки унікальних ділянок пальця, та здійснює обчислення їх взаємного розташування.
    2. У другому варіанті, використовується весь рельєф досліджуваного об'єкта.
    3. Комбінований алгоритм поєдніє в собі два перщі методи. Цей спосіб найкраще підвищує достовірність ідентифікації.

### 2.1.3 Пристрої сканування

З біометричних систем обладнання по скануванню відбитків пальця найпоширеніше. Пристрої використовуються в комерційних, державних структурах в понад, ніж 50-ти країнах світу. Компактні прилади ідентифікують відбитки випускаються виробниками з використанням однієї з наступних технологій:

* ультразвукова;
* оптична;
* напівпровідникова.

За ціною і якістю практичними системами вважаються пристрої, що використовують оптичну технологію сканування.

### 2.1.4 Переваги систем біометрії пальця

У порівнянні зі звичайними системами контролю, що використовують спеціально виготовлений ідентифікатор, біометричні пристрої дактилоскопії мають наступні переваги:

* високий ступінь захисту, що виключає підробку;
* відсутня ймовірність несанкціонованого доступу за допомогою ключів;
* немає необхідності в носінні карт, ключів;
* відсутня можливість втрати, передачі третім особам;
* виключаються витрати на відновлення, заміну ключів.

Сучасні системи ідентифікації по біометрії пальця найзручніші. Вони дають змогу чітко та якісно знімати відбитки пальців. Володіють високою пропускною здатністю. Термін сканування в більшості пристроїв не перевищує 1с. У системах також передбачено захист від муляжів. На даний період життя вони є одним з найнадійніших пристроїв по забезпеченню контролю доступу.

### 2.2.2 Ідентифікація за райдужною оболонкою і сітківкою ока

Біометрична ідентифікація за райдужною оболонкою і сітківкою ока.

У 1994 р. Дж. Даугман у США запатентував метод розпізнавання особи за райдужною оболонкою ока, який використовується й дотепер.

Райдужна оболонка ока є унікальною характеристикою людини. Малюнок райдужки формується на восьмому місяці внутрішньоутробного розвитку, остаточно стабілізується у віці близько двох років і практично не змінюється протягом життя, окрім як в результаті сильних травм або складних патологій. Метод є одним з найточніших серед біометричних технологій. Система ідентифікації особистості за райдужною оболонкою логічно ділиться на дві частини: пристрій захоплення зображення, його первинного оброблення й передачі на обчислювач; обчислювач, який здійснює порівняння зображення із зображеннями в базі даних і передає команду про допуск виконавчому пристрою. Розрізняють активні й пасивні системи розпізнавання. У системах першого типу користувач повинен сам налаштувати камеру, пересуваючи її для більш точного наведення. Пасивні системи є простішими у використанні, оскільки камера в них настроюється автоматично.

Зазначемо, що райдужки правого і лівого ока за малюнком суттєво відрізняються.

Переваги методу:

1) статистична надійність;

2) захоплення зображення райдужної оболонки може здійснюватись на відстані від кількох сантиметрів до кількох метрів, при цьому фізичний контакт людини з пристроями не відбувається;

3) райдужна оболонка захищена від пошкоджень рогівкою;

4) стійка протидія підробкам.

Недоліки методу: вартість системи для захоплення райдужної оболонки вища за вартість сканера відбитків пальця і камери для захоплення 2D зображення обличчя.

Напрям біометричної ідентифікації за сітківкою ока розвивається з 1976 р., коли у США була утворена компанія Eyedentify, яка досі зберігає монополію на виробництво комерційних систем ідентифікації за ретиною.

До останнього часу вважалося, що найнадійніший метод біометричної ідентифікації – це метод, що базується на скануванні сітківки ока. Він поєднує в собі кращі риси ідентифікації за райдужною оболонкою і за рисунком вен руки.

Сканер зчитує малюнок капілярів на поверхні сітківки ока. Сітківка має нерухому структуру, що незмінна в часі, окрім як у результаті очної хвороби, наприклад катаракти. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, спрямованого через зіницю до кровоносних судин на задній стінці ока. Сканери сітківки ока отримали широке поширення в системах контролю доступу на особливо секретні об’єкти, тому що в них один з найнижчих відсотків відмови в доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу.

На жаль, низка труднощів виникає під час використання цього методу біометрії. Під час ідентифікації за сітківкою ока вимірюється кутовий розподіл кровоносних судин на поверхні сітківки щодо сліпої плями ока та інші ознаки.

Капілярний малюнок сітківки очей відрізняється навіть у близнюків і може бути з великим успіхом використаний для ідентифікації особистості. Усього нараховують близько 250 ознак. Подібні біометричні термінали забезпечують високу вірогідність ідентифікації на рівні з дактилоскопією, але вимагають від особи, що перевіряється, значний час не рухатися і фіксувати погляд на об’єктиві сканера.

Переваги методу:

1) високий рівень статистичної надійності;

2) завдяки невеликому поширенню систем імовірність розроблення засобів їх «обману» досить низька;

3) безконтактний метод реєстрації даних.

Недоліки методу:

1) складна у користуванні система і досить довгий час оброблення;

2) висока вартість системи;

3) відсутність широкого ринку пропозиції і, як наслідок, недостатня інтенсивність розвитку методу.

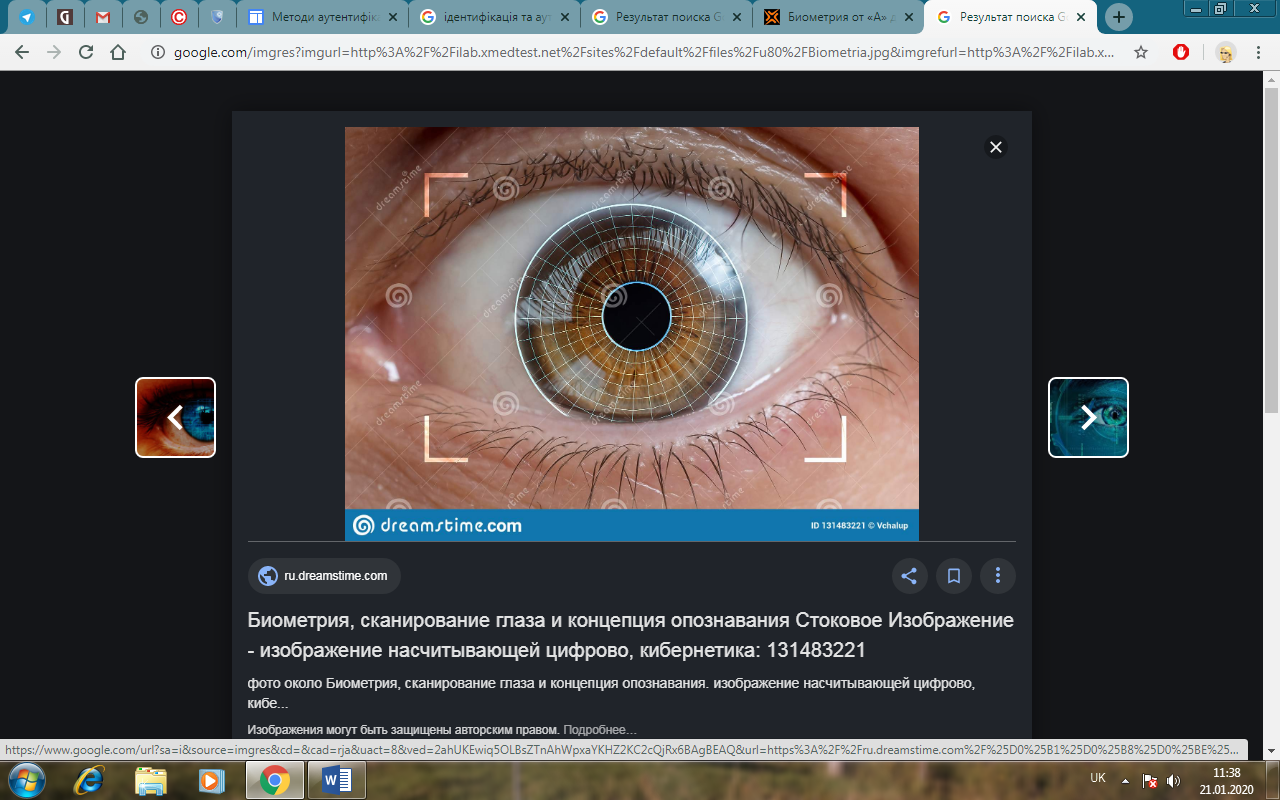


Рис. 2.2.2 Сканування ока

### 2.2.3 Ідентифікація за геометрією обличчя

Біометрична ідентифікація за геометрією обличчя, кисті руки та венозним рисунком долоні. Існує безліч методів розпізнавання за геометрією обличчя. Всі вони базуються на тому, що риси обличчя і форма черепа кожної людини індивідуальні. Технічна реалізація методу – більш складна (з математичної точки зору), ніж розпізнавання відбитків пальців, що вимагає дорогої апаратури (необхідна цифрова відео- або фотокамера і плата захоплення відео-зображення). Але метод має один істотний плюс: для зберігання даних одного зразку ідентифікаційного шаблону потрібно небагато пам’яті, оскільки людське обличчя можна «розкласти» на відносно невелику кількість ділянок, незмінних у всіх людей.

Наприклад, для обчислення унікального шаблону, відповідного конкретній людині, необхідно всього 12…36 характерних ділянок. Розпізнавання людини за зображенням обличчя відрізняється від інших біометричних систем тим, що, по-перше, не вимагає спец-устаткування, по-друге, відсутній фізичний контакт людини із пристроями. Не треба очікувати дотику або зупинки для спрацьовування системи.

У наш час існують чотири основних методи розпізнавання обличчя, які відрізняються складністю реалізації і метою застосування:

1) “Eigenface” або «власне обличчя»;

2) аналіз «відмітних рис»;

3) «нейронна мережа»;

4) автоматичне оброблення зображення обличчя.

Технологія Eigenface використовує двовимірні зображення в градаціях сірого, які представляють характеристики зображення особи, відмінні від інших.

Метод Eigenface є основою для інших методів розпізнавання обличчя. Комбінуючи характеристики 100–120 Eigenface, можна відновити велику кількість облич. В момент реєстрації Eigenface кожної конкретної людини представляється у вигляді ряду коефіцієнтів.

Для режиму встановлення особистості, у якому зображення використовується для перевірки ідентичності, «живий» шаблон порівнюється із вже зареєстрованим з метою визначення коефіцієнта відмінності.

Ступінь відмінності між шаблонами визначає факт ідентифікації. Технологія Eigenface оптимальна при використанні в освітлених приміщеннях, коли є можливість сканування особи. Аналіз рис, відмінних від інших, – ще одна із широко використовуваних технологій ідентифікації, яка подібна до технології Eigenface, але в більшому ступені адаптована до зміни зовнішності або міміки людини (усміхнене або насуплене обличчя).

У зазначеній технології використовуються десятки характерних рис різних областей обличчя, причому враховується їхнє відносне місце розташування. Індивідуальна комбінація цих параметрів визначає особливості кожного конкретного обличчя людини, яке є унікальним і досить динамічним.

**Метод автоматичного оброблення зображення особи** – найпростіша технологія, що використовує відстані та їх відношення між точками обличчя, такими як очі, кінець носа, куточки рота. Хоча даний метод і не настільки потужний, як Eigenface або «нейронна мережа», але він досить ефективний в умовах слабкого освітлення.

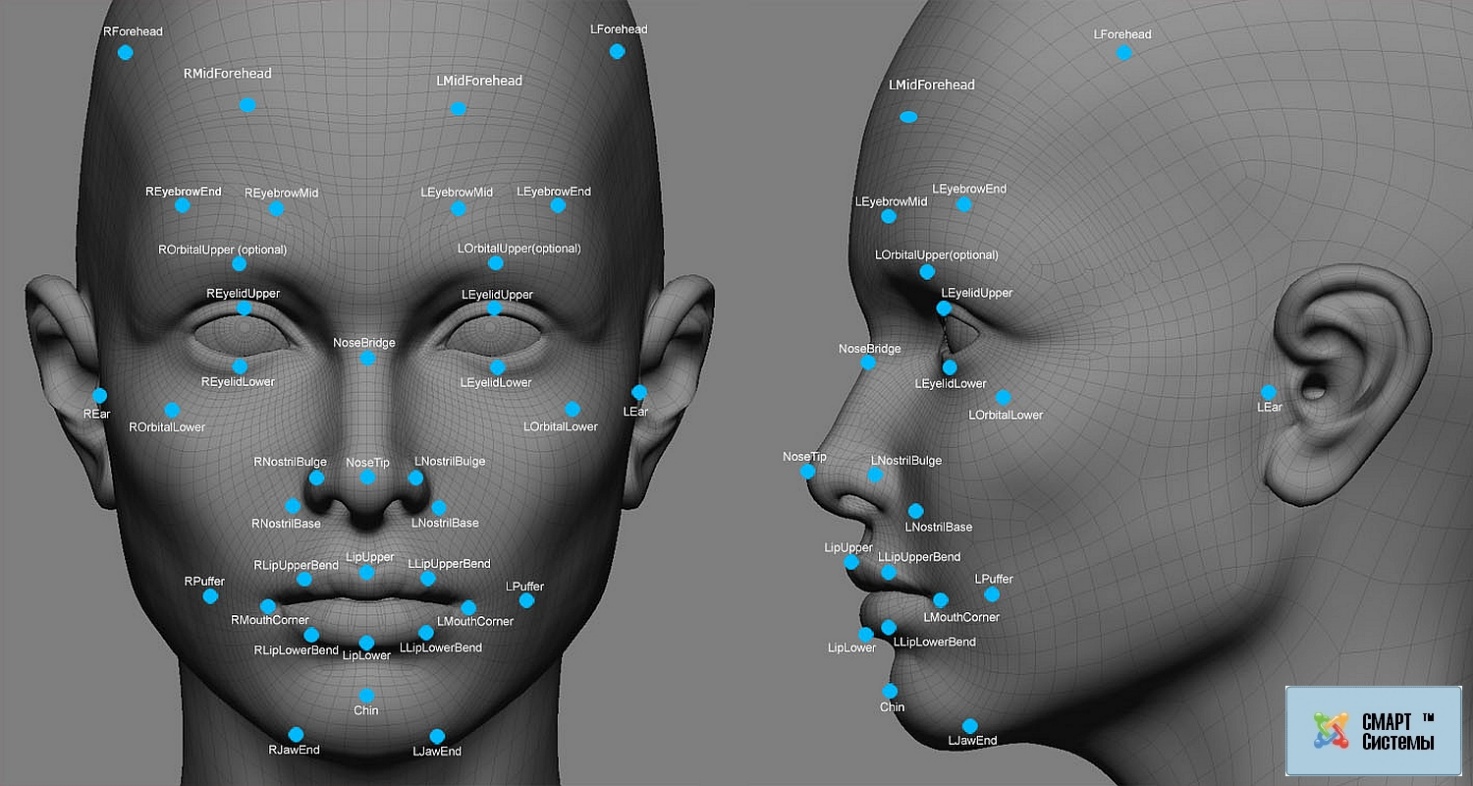


Рис. Геометрія обличчя по точкам

### 2.2.4 Ідентифікація за геометрією кисті руки

**Біометрична ідентифікація за геометрією кисті руки** за своєю технологічною структурою і рівнем надійності повністю аналогічна методу ідентифікації особистості за відбитком пальця. Статистична ймовірність існування двох кистей рук з однаковою геометрією надзвичайно мала. Математична модель ідентифікації за даним параметром вимагає небагато інформації – усього 9 байт, що дозволяє зберігати великий обсяг записів і швидко здійснювати пошук. Пристрої ідентифікації особистості за геометрією руки знаходять широке застосування.

На даний момент, у США пристрої для зчитування відбитків долонь встановлено приблизно більше ніж на 14 000 об’єктах. Пристрій Handkey сканує як внутрішню, так і бічну сторону долоні, використовуючи для цього вбудовану відеокамеру та алгоритми стиску [7]. Ідентифікація користувачів за геометрією руки використовується в законодавчих органах, міжнародних аеропортах, лікарнях, імміграційних службах тощо. Переваги ідентифікації за геометрією долоні адекватні перевагам ідентифікації за відбитком пальця з погляду надійності, хоча пристрій для зчитування відбитків долонь займає більше місця. Біометрична ідентифікація за малюнком вен руки – нова технологія у сфері біометрії, яка базується на інфрачервоному скануванні вен із подальшим цифровим обробленням. Дана технологія була розроблена для використання в системі охорони здоров’я, щоб допомогти лікарям знайти у пацієнтів вени для ін’єкцій. Але враховуючи те, що, обчислювальна техніка та автоматизація тура вен у кожної людини індивідуальна, ця технологія викликала інтерес фахівців з ідентифікації, як більш надійна відносно технології ідентифікації за відбитком пальця, оскільки відтворити модель кровоносної системи неможливо. Малюнок вен зчитується із зовнішнього боку долоні або кисті руки за допомогою інфрачервоної камери і дозволяє отримати достатньо чітке зображення кровоносних судин, таке, що навіть відносно невеликі порізи чи бруд на поверхні шкіри не перешкоджають успішній реєстрації особи. Поглинаючи випромінювання, відновлений гемоглобін переносить кисень по венах і скорочує ступінь відбиття та відображення малюнка вени у вигляді чорного унікального візерунка.

Далі отримане зображення обробляється, і залежно від розташування вен на руці формується цифрова згортка.

Переваги методу:

1) висока достовірність отриманих результатів;

2) відсутність необхідності прямого контакту з пристроєм, що здійснює сканування;

3) висока ступінь захищеності – рисунок неможливо отримати від людини «на вулиці», а у випадку використання муляжу кисті малюнок вен не буде зчитаний інфрачервоною камерою;

Недоліки методу:

1) недопустиме засвічення сканера сонячними променями і променями галогенних ламп;

2) вплив деяких захворювань, наприклад артриту, на прийняття рішення.

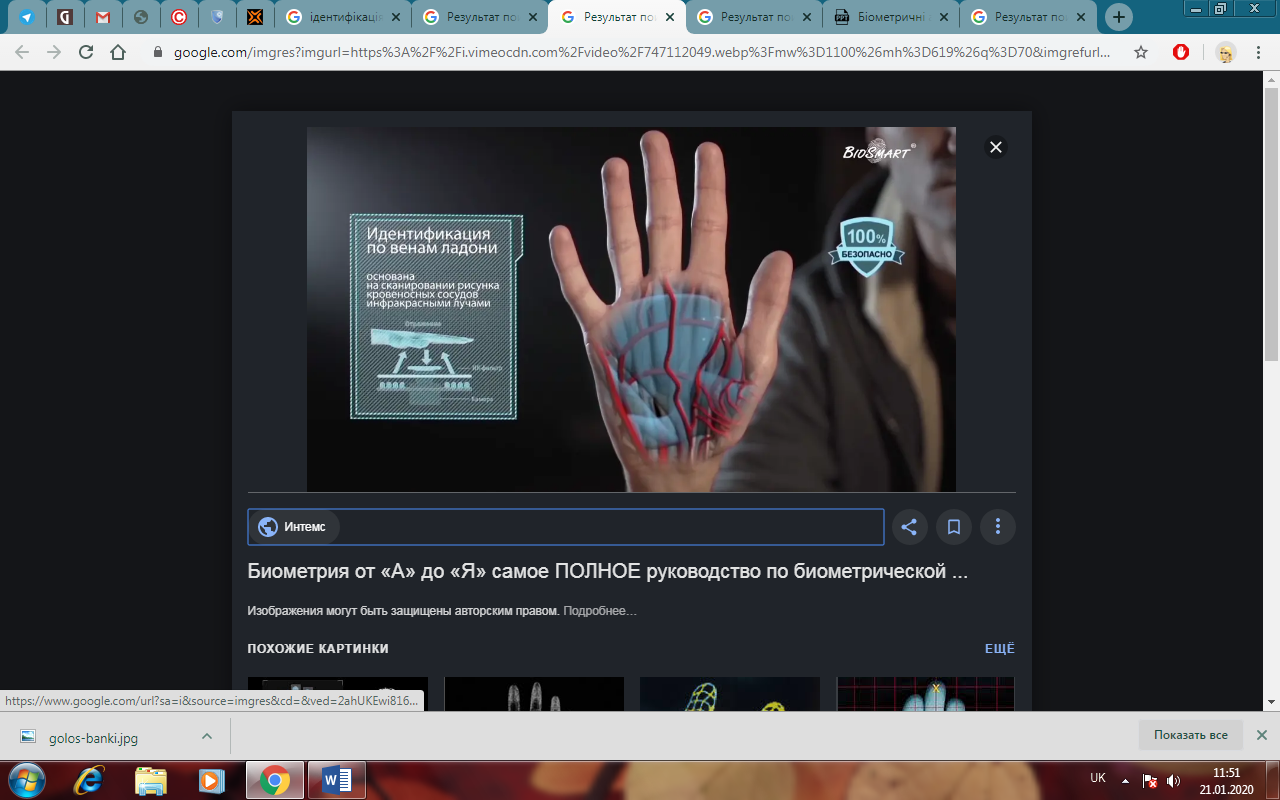


Рис.2.2.4 Ідентифікація по венам долоні

### 2.2.5 Ідентифікація за голосом

Біометрична ідентифікація **за голосом** досить зручна та інформативна, але за умови, що вона здійснюється не людиною, а технічними засобами, до яких належать програмні комплекси, автоматизовані системи, комп’ютеризовані пристрої тощо. Автомати позбавлені впливу «людського фактору». Вони розрізняють голос і здійснюють ідентифікацію об’єктивно, на основі жорстко детермінованих і заданих наперед ознак. Для підвищення якості ідентифікації за голосом в деяких системах використовують додатково верифікацію голосу, а іноді – аутентифікацію. Технологія біометричної ідентифікації добре зарекомендувала себе в системах верифікації особистості за голосом в окремих каналах зв’язку, підтвердила більш високу надійність порівняно із частотним набором особистого номера.



Рис.2.2.5

### 2.2.6 Ідентифікація за клавіатурним «почерком»

В останні роки набуває все більшого розповсюдження **біометрична ідентифікація за клавіатурним «почерком»** користувача як таким, що за наявності високої стабільності дозволяє ідентифікувати з високим рівнем достовірності особу користувача.

При цьому застосовуються статистичні методи обробки вихідних даних і формування вихідного вектора, що є ідентифікатором даного користувача. Як вихідні дані використовують часові інтервали між натисканням клавіш на клавіатурі і часом їх утримання. При цьому інтервали між натисканням клавіш характеризують темп роботи, а час утримання клавіш характеризує стиль роботи із клавіатурою – різкий удар або плавне натискання [7].

Принципова відмінність цих двох способів полягає в тому, що у першому випадку використовується ключова фраза, яка задається користувачем у момент реєстрації його в системі (пароль), а в другому – використовуються ключові фрази, які генеруються системою щоразу в момент ідентифікації користувача. Застосування способу ідентифікації за клавіатурним почерком доцільне тільки стосовно користувачів з досить тривалим досвідом роботи з комп’ютером і почерком роботи на клавіатурі, що сформувався, тобто до програмістів, секретарів тощо.

Еталонні характеристики користувача, отримані на етапі навчання системи, дозволяють зробити висновки про ступінь стабільності клавіатурного почерку користувача і визначити довірчий інтервал розкиду параметрів для наступної ідентифікації користувача.

## **2.3 Нові методи біометричної ідентифікації**

Перелік технологій, які можуть бути використані в системах безпеки, постійно розширюється, і більшість з них вважаються досить перспективними:

1) аналіз термограми обличчя в інфрачервоному діапазоні випромінювання;

2) оцінювання характеристики ДНК;

3) аналіз структури шкіри та епітелію на пальцях з використанням цифрової ультразвукової спектроскопії шкіри;

4) аналіз форми вушної раковини;

5) аналіз характеристик ходи людини;

6) аналіз індивідуальних антропометричних особливостей людини;

7) розпізнавання за рівнем солоності шкіри.

**Технологія побудови та аналізу термограм** з використанням інфрачервоних камер є одним з останніх досягнень в області біометрії, оскільки дає унікальну картину об’єктів, що знаходяться під шкірою людини. Термограма особи є суворо індивідуальною, завдяки чому можна впевнено розрізняти навіть близнюків. З інших властивостей цього підходу можна відмітити його інваріантність стосовно будь-яких косметичних змін та прихованість процедури реєстрації.

Технологія, що побудована **на аналізі характеристик ДНК** (метод геномної ідентифікації), є хоча і найбільш тривалою, але й найбільш перспективною із відомих систем ідентифікації. Метод базується на тому, що в ДНК людини є поліморфні локуси (локус – положення хромосоми в гені або аллелі), які часто мають 8–10 аллелей. Визначення набору цих аллелей для декількох поліморфних локусів в конкретного індивіда дозволяє отримати геномну карту, характерну тільки для цієї людини. Точність даного методу визначається характером і кількістю проаналізованих поліморфних локусів сьогодні дозволяє досягти рівня 1 помилки на 1 млн осіб.

**Технологія аналізу відбитків долонь** стала розвиватися порівняно недавно, але вже має певні досягнення. Ряд компаній-розробників (наприклад у Великобританії) зосередилися на технології, що аналізує не малюнок ліній на шкірі, а обрис долоні, який також має індивідуальний характер. Аналогічна система, що працює з відбитками пальців, успішно використовується британськими поліцейськими вже 5 років. Але одних лише відбитків пальців, як стверджують криміналісти, часто виявляється недостатньо. До 20% слідів, що залишаються на місці злочину, – це відбитки долонь. Комп’ютеризація цього процесу дозволить використовувати відбитки долонь більш широко й приведе до істотного збільшення розкривання злочинів. Слід відмітити, що пристрої сканування долоні зазвичай мають високу вартість, тому оснастити ними велику кількість робочих місць не так уже й просто [7, с. 20]. Технологія аналізу форми вушної раковини є однією з найбільш останніх розробок у біометричній ідентифікації людини. За допомогою недорогої Web-камери можна отримувати досить надійні зразки для порівняння й ідентифікації. Цей спосіб поки що недостатньо вивчений, тому у науковотехнічній літературі достовірна інформація про поточний стан практично відсутня. До перспективних слід віднести системи «електронний ніс», що реалізують процес розпізнавання за запахом. Наявність генетичного впливу на запах тіла дозволяє вважати цю характеристику можливого для використання з метою біометричної ідентифікації особистості. Цій технології, як і технології аналізу форми вушної раковини, ще треба буде пройти довгий шлях розвитку, перш ніж вона стане задовольняти біометричним вимогам.

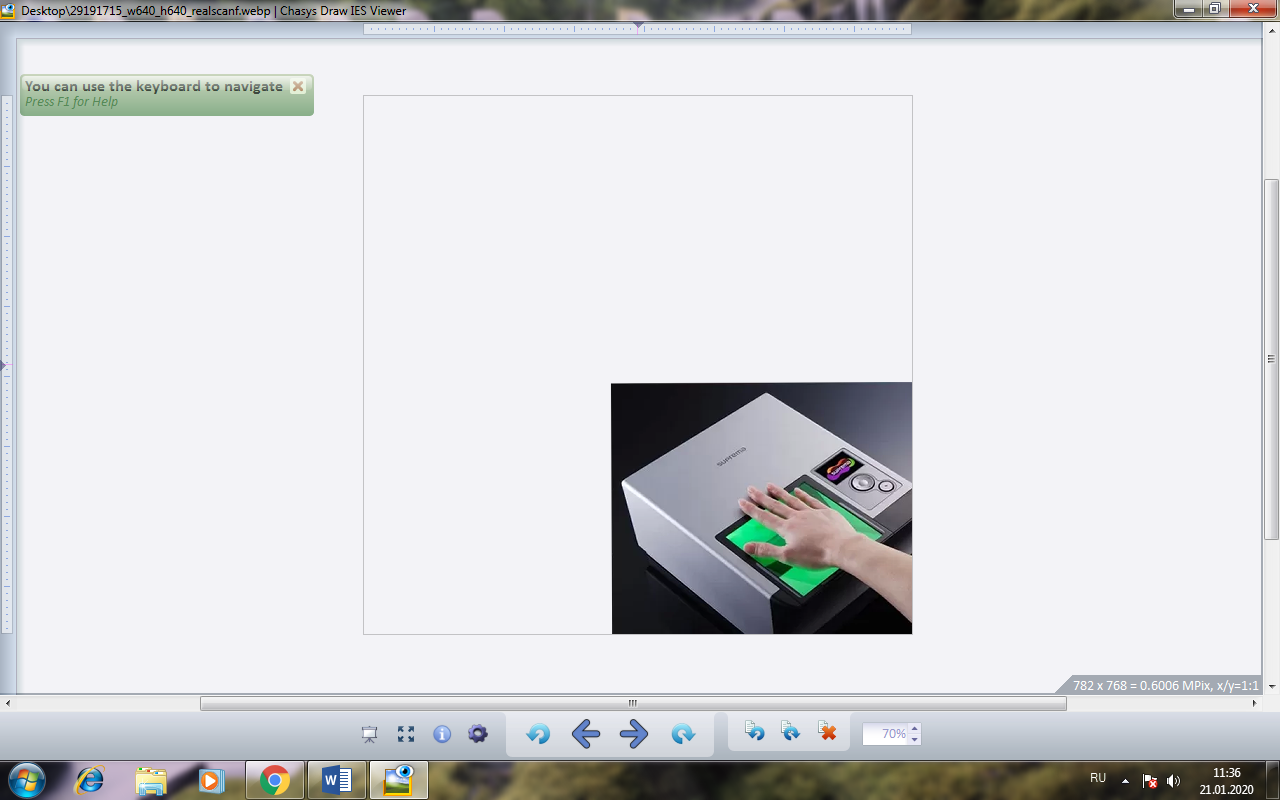


Рис.2.3 Ідентифікація по відбитку долоні

## **Висновки 2 розділу**

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. Показано, що поєднання паролів із біометричними характеристиками людини підвищує надійність системи доступу в сотні і тисячі разів. Наведені переваги, недоліки та основні характеристики біометричних ідентифікаційних технологій методів біометричної ідентифікації дозволили класифікувати їх на статичні (за відбитками пальців, за райдужною оболонкою ока, за геометрією обличчя або кисті руки, за венозним малюнком руки, за сітківкою ока) та динамічні (ідентифікація за голосом, за набором на клавіатурі, за підписом).

Серед нових методів біометричної ідентифікації варто зазначити про такі: за термограмою обличчя, за характеристиками ДНК, за спектроскопією шкіри, за формою вушної раковини, за ходою людини; за індивідуальними антропометричними особливостями людини, за рівнем солоності шкіри. Критичний аналіз цих методів підтвердив їхню життєздатність і перспективи розвитку.

# РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ НА ПІДПРИЄМСТВО З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ МЕТОДІВ

## **3.1 Базові параметри біометричного обладнання**

Принцип роботи біометричної СКУД ґрунтується на технології ідентифікації людини шляхом сканування відбитків пальців. Використання останніх технічних розробок в області біометрії забезпечують високу надійність системи при достатній простоті і зручності її експлуатації.

Основні функції:

Контроль і управління доступом:

* ідентифікація людини шляхом сканування відбитку пальця;
* доступ тільки зареєстрованих співробітників і відвідувачів;
* управління виконавчими пристроями (дверима, турнікетами, шлагбаумами);
* формування сигналу тривоги при спробі несанкціонованого доступу;
* ведення журналу подій;
* розмежування доступу по часових зонах

Облік робочого часу співробітників:

* автоматизований облік часу приходу і відходу співробітників;
* ведення табеля робочого часу;
* створення звітів про наявність або відсутність співробітника на робочому місці, про запізнення і ранні відходи;
* створення і ведення бази даних співробітників (електронна картотека);
* імпорт даних в програму Microsoft Excel і ін.

Забезпечення безпеки приміщень:

інтеграція з будь-якими існуючими системами контролю доступу і охоронної сигналізації;

Переваги.

Завдяки використанню методу дактилоскопічної ідентифікації людини у біометричних СКУД є ряд переваг перед традиційними системами контролю доступу, що використовують магнітні карти і електронні ключі:

* виключається можливість несанкціонованого використання ключів;
* забезпечується високий ступінь захисту від імітації;
* відпадає необхідність обов’язкового носіння ключів;
* виключається вплив людського чинника (втрата або псування ключа, забудькуватість, передача ключів третім особам і тому подібне);
* відсутні витрати на виготовлення нових ключів, заміну або відновлення тих, що існують.

СКУД є мережевою, розподіленою системою, з розмежуванням прав доступу користувачів, при необхідності нарощуваної, відкритої для інтеграції з пристроями інших виробників. Організація мережі будується з використанням інтерфейсу Rs485, виділених ліній зв’язку Ethernet, що вже існують на підприємстві або стільникових мереж формату GSM. Контролери об’єднуються в магістраль Rs485 (до 255 шт.). Для підключення до ПК застосовуються перетворювачі інтерфейсів Usbrs485, Lanrs485, Gprsrs485. [12,126-145]

## **3.2 Принцип роботи біометричної СКУД.**

Реєстрація користувачів проводиться з допомогою ПО і контрольного зчитувача, що підключається через Usb порт персонального комп'ютера. На кожного користувача можна зареєструвати до 10 відбитків пальців, при цьому в базу даних записуються математичні шаблони відбитків, що робить неможливим зворотне відтворення їх графічного зображення. Далі користувачеві привласнюються права доступу на конкретні точки проходу, при цьому шаблони відбитків в кодованому вигляді передаються по лінії зв'язку в контролер і надалі зберігаються в нім незалежно від комп'ютера.

Коли користувач прикладає палець до сканера контролера, відбувається пошук в базі даних контролера зареєстрованих шаблонів. При успішній ідентифікації контролер видає сигнал на блок управління реле по захищеному цифровому каналу, який у свою чергу включає виконавчі пристрої (електромагнітні замки, турнікети і ін.). Тим самим виключається можливість несанкціонованого доступу в приміщення шляхом замкнення проводів або імітації сигналу управління. При успішній ідентифікації в журнал подій записується відповідна інформація. У разі ідентифікації неуспіху або заборони проходу для користувача події також фіксуються.

Контролер може працювати із зовнішніми датчиками, для цього на блоці управління реле передбачено два дискретні входи. Перший дискретний вхід застосовується для підключення виносної кнопки виходу з приміщення. Другий дискретний вхід може застосовуватися для підключення датчика відкриття дверей, датчика турнікета, пожежної сигналізації. Всі події по зовнішніх датчиках також фіксуються в журналі.

Основні компоненти біометричної СКУД.



Рис. 3.1 Контролер біометричний

Призначення.

Контролер біометричний - електронний модуль призначений для ідентифікації відбитків пальців. Контролер має незалежну пам'ять на 9000 відбитків пальців, 12800 подій, 64 тимчасових групи, 5 інтервалів на кожен день, 32 свята. Всі події в контролері записуються в хронологічному порядку з вказівкою точного часу. Контролер оснащений світловим індикатором і звуковим зумером для інформування користувача про результати ідентифікації.

Основні технічні характеристики:

* максимальна кількість відбитків 9000;
* максимальна кількість подій 12800;
* часові зони 64 тимчасових групи, 5 інтервалів на кожен день, 32 свята;
* сканер відбитків пальців;
* вірогідність помилкового надання доступу FAR не більше 0.0001%;
* вірогідність помилкової відмови в доступі FAR не більше 0.001%;
* час ідентифікації 1:1000 не більше 1 сік;
* розмір даних відбитку 256 ~ 384 байти;
* інтерфейс зв'язку Rs485, 115200 б/сек;
* незалежна пам'ять для журналу подій;
* ключ шифрування даних 256 бітний AES;
* живлення, максимальне споживання 12 В пост. струму;
* габаритні розміри (L x W x H) 175х75х54;
* температурний діапазон від -40 до +50 °С;
* датчик відкриття корпусу є.



Рис. 3.2 Сканер відбитків пальців для ПК Fs-80

Призначення

Сканером Fs80 є модуль для захоплення і передачі на ПК образу відбитку пальця. Унікальна технологія, що використовує прецизійну матрицю CMOS, дозволяє отримувати зображення відбитку пальця з високою якістю. Сканер Fs80 може застосовуватися в будь-яких застосуваннях, де потрібна ефективна і достовірна ідентифікація людини. У сканер Fs80 вбудована спеціальна електронна схема - Lfd\*, що дозволяє відрізнити живий палець від муляжу.

Основні технічні характеристики

* інтерфейс USB 1.1;
* дозвіл робочій поверхні 508 dpi;
* розміри робочої поверхні сканування 16x24 мм;
* розмір відсканованого зображення 480х320 мм;
* температурний діапазон від 0 до +55 °С;
* напруга живлення через USB порт;
* вага 80 г;
* швидкість передачі даних 6 Мбіт/сек.

## **3.3 Оптимізаційний вибір параметрів обладнання**

У цьому розділі за допомогою методу аналізу ієрархій реалізованому в безкоштовній програмі MPRIORITY 1.0 ми обираємо найбільш оптимальні варіанти обладнання що буде використано в проектованій системі. На рисунку 3.1 зображено найбільш поширені на ринку датчики біометричної ідентифікації.

    
(а) Touch SAFE Personal (S400) (б) Sagem 100MA

    
 (в) Software SR100 (г) U.are.U Digital Persona

Рис. 3.1 (а,б,в,г) Датчики біометричної ідентифікації.

У таблиці 3.1 наведено найважливіші технічні характеристики біометричних датчиків.

Таблиця 3.1

Основні технічні характеристики

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Характеристики/фірми | Touch SAFE Personal (S400) | Sagem (100MA) | Software (SR100) | U.areU.(Digital Persona) |
| Помилка першого роду % (False Reject Rate,FRR) | 2 | 1 | 2 | 3 |
| Помилка другого роду % (False Accept Rate,FAR) | 0,001 | 0,001 | 0,01 | 0,1 |
| Час регістрації,с | 20 | 15 | 22 | 20 |
| Час ідентифікації,с | 1 | 0.3 | 2 | 1 |
| Джерело живлення | Зовнішнє 12V | Зовнішнє 12V | Зовнішнє 12V | Зовнішнє  12V |
| Підключення (інтерфейс) | RS-485 | RS-485 | RS-232 | USB |
| Ціна | 3200 | 4000 | 2900 | 3000 |

У таблиці 3.2 приводяться критичні характеристики, що при виборі датчиків повинні бути враховані в першу чергу.

Саме ці характеристики використовувались в методі аналізу ієрархій.

Таблиця 3.2

Характеристики що використовувались для порівняння

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Характеристики/фірми | Touch SAFE Personal (S400) | Sagem (100MA) | Software (SR100) | U.areU.(Digital Persona) |
| Помилка першого роду % (False Reject Rate,FRR) | 2 | 1 | 2 | 3 |
| Помилка другого роду % (False Accept Rate,FAR) | 0,001 | 0,001 | 0,01 | 0,1 |
| Час регістрації,с | 20 | 15 | 22 | 20 |
| Час ідентифікації,с | 1 | 0.3 | 2 | 1 |
| Ціна | 3200 | 4000 | 2900 | 3000 |

Далі на рисунках наведено результати дослідження датчиків біометрії по методу аналізу ієрархій. Порівняння здійснювалось з допомогою програми MPRIORITY 1.0 [40].

Результати аналізу ієрархії.



Рис. 3.2 Побудова ієрархії

З допомогою якісної шкали зображеної на рисунку 3.3 ми проводимо визначення приоритетного параметру.

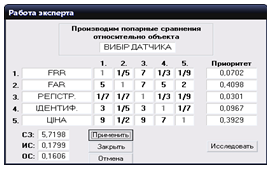


Рис. 3.3 Визначення приоритетного параметра

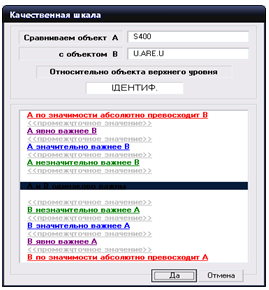


Рис. 3.4 Якісна шкала

Після попарного порівняння всіх критеріїв виводиться діаграма з приоритетним критерієм.

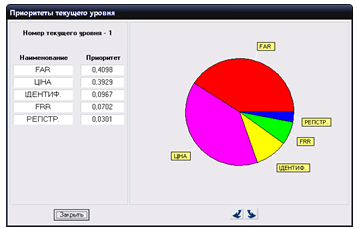
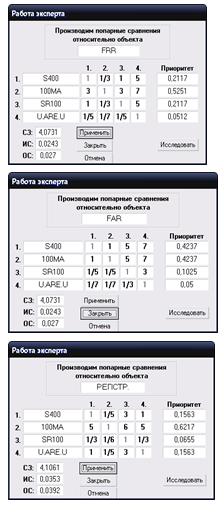
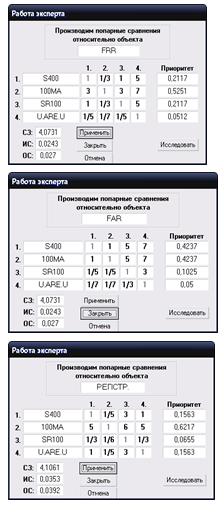
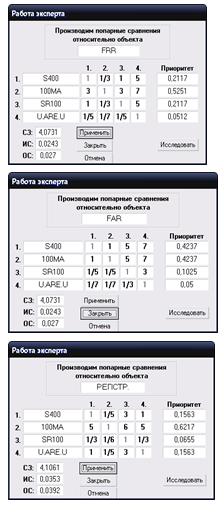


Рис. 3.5 Пріоритет поточного рівня

Після визначення головного критерію проводиться попарне порівняння датчиків по кожному з критеріїв.оль біометриний об’єкт.



(а) (б)

(в) (г)  


(д)

Рис. 3.6 (а,б,в,г,д) Попарне порівняння всіх критеріїв

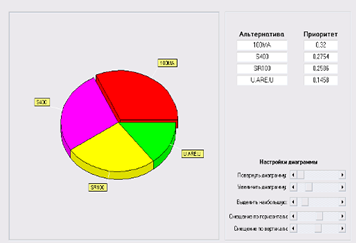


Рис. 3.7 Кінцевий результат

Після проведеного дослідження виводиться кінцевий результат, діаграма з якої, що найкращим варіантом є датчик фірми Segam 100MA.

Таким же чином проводиться вибір інших компонентів системи.



Рис. 3.8 Контролер КОДОС Elsys-MB-Light-2A-00-TП

Технічні характеристики:

* напруга живлення (мережа змінного струму) – 220 В;
* споживана потужність - не більше 40 Вт;
* час роботи від акумуляторної батареї - не більше 12 год ;
* температура навколишнього середовища - -10°С . +55°С;
* відносна вологість - не більше 80%;
* габаритні розміри - 300 х350х165 мм;
* маса - не більше 6 кг;
* протокол зв'язку з пристроєм, що управляє (інтерфейс) RS 485;
* довжина сполучного кабелю - не більше 1000 м;
* максимальне число користувачів 65 000;
* максимальне число подій 100 000;
* кількість контролерів доступу, що підключаються, - не більше 6 шт.;
* тип лінії зв'язку з контролерами доступу - чотирох жильний;
* протокол зв'язку з комп'ютером - Rs-458;
* ціна 6450грн. [27].

Типи виконавчих пристроїв, що підключаються - турнікети, електромагнітні замки і так далі)



Рис. 3.9 Контролер TSS-201-2W/p

Технічні характеристики

* напруга живлення (мережа змінного струму) – 220 В;
* споживана потужність - не більше 40 Вт;
* час роботи від акумуляторної батареї - не більше 9 год;
* температура навколишнього середовища - 0°С . +60°С;
* відносна вологість - не більше 80%;
* габаритні розміри - 400 х450х155 мм;
* протокол зв'язку з пристроєм, що управляє (інтерфейс) RS 485;
* довжина сполучного кабелю - не більше 1000 м;
* максимальне число ідентифікаторів 3000;
* максимальне число подій 10 000;
* кількість зчитувачів, що підключаються, - 2 шт.;
* тип лінії зв'язку з контролерами доступу - чотирох жильний;
* протокол зв'язку з комп'ютером - Rs-458;
* ціна 8200грн.

Типи виконавчих пристроїв, що підключаються - турнікети, електромагнітні замки і так далі).



Рис. 3.10 Контролер LNL-2220

Технічні характеристики

* напруга живлення (мережа змінного струму) – 220 В;
* споживана потужність - не більше 40 Вт;
* час роботи від акумуляторної батареї - не має акумулятора;
* температура навколишнього середовища - +5°С . +36°С;
* відносна вологість - не більше 75%;
* маса - не більше 2,5 кг;
* протокол зв'язку з пристроєм, що управляє (інтерфейс) RS 485;
* довжина сполучного кабелю - не більше 1000 м;
* максимальне число ідентифікаторів 4000;
* максимальне число подій 6000;
* кількість зчитувачів, що підключаються, - 2 шт.;
* тип лінії зв'язку з контролерами доступу - чотирох жильний;
* протокол зв'язку з комп'ютером - Rs-458;
* ціна 3600грн. [27].

Типи виконавчих пристроїв, що підключаються - турнікети, електромагнітні замки і так далі.

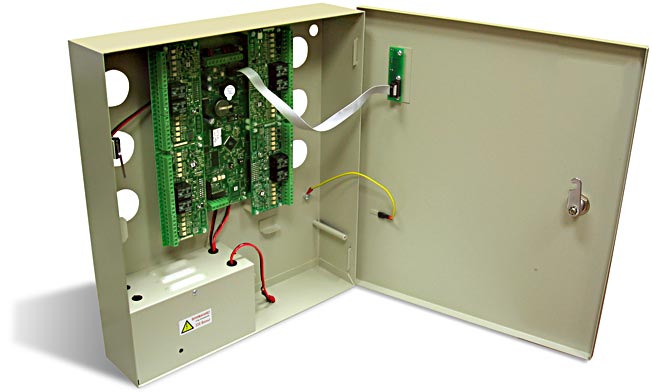


Рис. 3.11 Контролер Tss-207-4w

Технічні характеристики:

* напруга живлення (мережа змінного струму) – 220 В
* споживана потужність - не більше 40 Вт;
* час роботи від акумуляторної батареї - не більше 10 год
* температура навколишнього середовища - +5°С . +55°С;
* відносна вологість - не більше 80%;
* габаритні розміри - 360 х 310 х 90 мм
* маса - не більше 5,7 кг;
* Протокол зв'язку з пристроєм, що управляє (інтерфейс) RS 485
* довжина сполучного кабелю - не більше 1000 м;
* максимальне число ідентифікаторів 5000
* максимальне число подій 8 000
* кількість зчитувачів, що підключаються, - 4 шт.;
* тип лінії зв'язку з контролерами доступу - чотирох жильний;
* протокол зв'язку з комп'ютером - Rs-458;
* ціна 12000грн. [27].

Типи виконавчих пристроїв, що підключаються - турнікети, електромагнітні замки і так далі).

Таблиця 3.3

Характеристики що використовувались для порівняння

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Характеристики, контролери | Контролер КОДОС Elsys-MB-Light-2A-00-TП | Контролер TSS-201-2W/p | Контролер LNL-2220 | Контролер Tss-207-4w |
| Кількість ідентифікаторів | 5000 | 3000 | 4000 | 5000 |
| Число подій що зберігаються в пам’яті | 10000 | 10000 | 6000 | 8000 |
| Час роботи від акумулятора | 12 | 9 | - | 10 |
| Кількість зчитувачів, що підключаються | 6 | 2 | 2 | 4 |
| ціна | 6450 | 8200 | 3600 | 12000 |

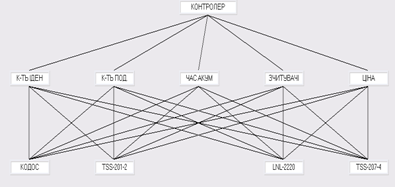


Рис. 3.12 Побудова ієрархії

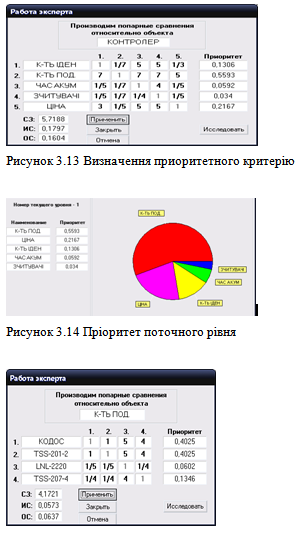


Рис. 3.13 Визначення пріоритетного критерію

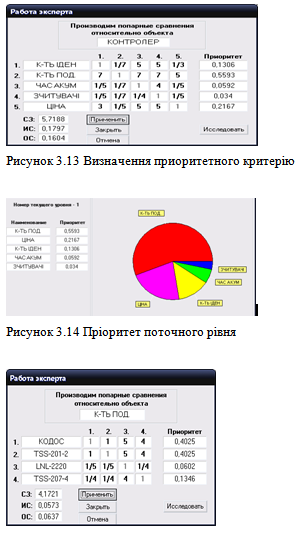
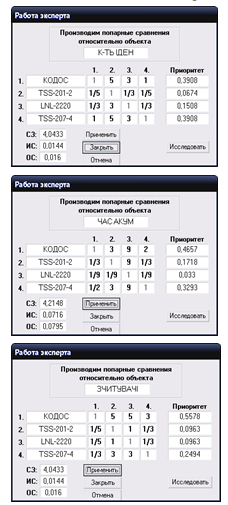
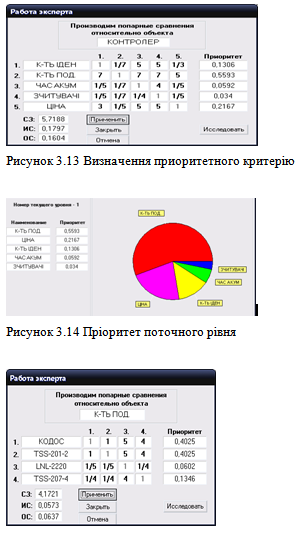
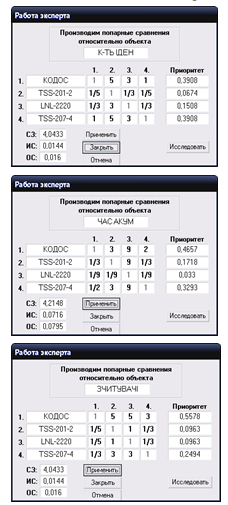


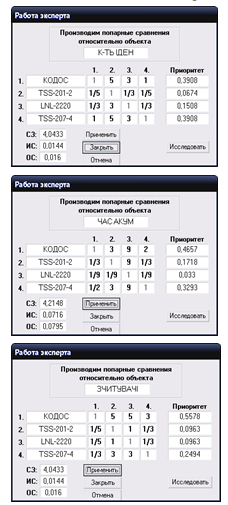
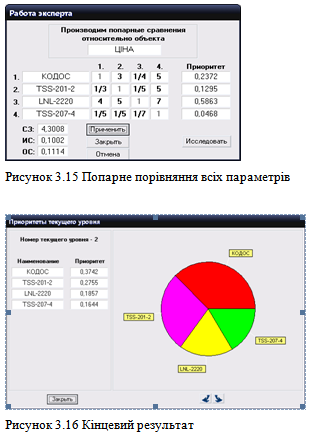
Рис.3.14 Пріоритет критичного рівня



(а) (б)



(в)

(г) (д)

Рис.3.15(а,б,в,г,д) Попарне порівняння

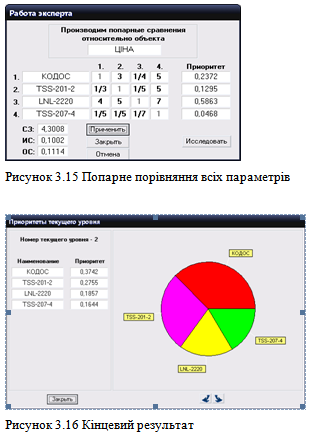


Рис.3.16 Кінцевий результат

За результатами дослідження оптимальним варіантом є контролер КОДОС.

## **3.4 Результат дослідження методом аналізу іієрархії**

Результатом дослідження методом аналізу ієрархії в системі будуть використані:



Рис. 3.17 Контролер КОДОС Elsys-MB-Light-2A-00-TП

Технічні характеристики:

* напруга живлення (мережа змінного струму) – 220 В
* споживана потужність - не більше 40 Вт;
* час роботи від акумуляторної батареї - не більше 12 год
* температура навколишнього середовища - -10°С . +55°С;
* відносна вологість - не більше 80%;
* габаритні розміри - 300 х350х165 мм;
* маса - не більше 6 кг;
* Протокол зв'язку з пристроєм, що управляє (інтерфейс) RS 485
* довжина сполучного кабелю - не більше 1000 м;
* максимальне число користувачів 5000;
* максимальне число подій 10000;
* кількість контролерів доступу, що підключаються, - не більше 6 шт.;
* тип лінії зв'язку з контролерами доступу - чотирох жильний;
* протокол зв'язку з комп'ютером - Rs-458;
* ціна 6450грн.

Типи виконавчих пристроїв, що підключаються - турнікети, електромагнітні замки і так далі)



Рис. 3.18 MA 100

Технічні характеристики зчитувача MA 100 (базова модель)

* Сканер відбитків пальців: 14х20 мм (500 крапок на дюйм)
* Час верифікації: <1с
* Час ідентифікації: <1,5с
* Інтерфейси: Rs-485 або Ethernet 10/100baset
* Живлення: 12 В пост. Струму
* Робочі умови: -10°.+45°С, 0-90% без конденсату
* Габарити: 142х84х46 мм
* Вага зчитувача: 675 г [32].

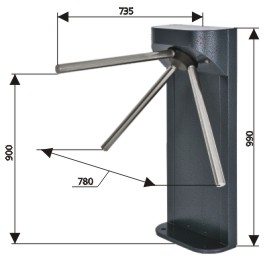


Рис. 3.19 Турнікет модель Т83M

Технічні характеристики:

* Пропускна спроможність 30 чоловік в хвилину.
* Вид стопора Електромагнітний замок, розташований в корпусі турнікета фіксує механізм в закритому положенні.
* Світлова індикація Зелений колір світлових індикаторів - прохід дозволений, червоний колір світлових індикаторів - прохід заборонений.
* Напрацювання на відмову 2 000 000 проходів.
* Напруга живлення -12V
* Споживаний струм 1,5 А
* Умови експлуатації Від 0с до +50С використання в приміщенні.
* Види покриття Фарбування корпусу порошковою фарбою.
* Комплект постачання Корпус турнікета, пульт управління турнікетом.
* Термін гарантії 1 рік
* Термін експлуатації 8 років [32].

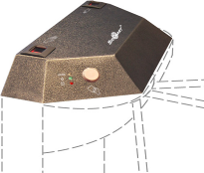


Рис. 3.20 біометричний термінал Biosmart Т- 83м.

Основні технічні характеристики:

* Максимальна кількість відбитків в локальному режимі 4500
* Максимальна кількість відбитків в серверному режимі 30000
* Максимальна кількість подій 12800
* 5 інтервалів на кожен день
* 32 свята
* Сканер відбитків пальців оптичний
* Вірогідність помилкового надання доступу FAR не більше 0.0001%
* Вірогідність помилкової відмови в доступі FRR не більше 0.001%
* Час ідентифікації 1:1000 шаблонів в локальному режимі не більше 1 сек
* Час ідентифікації 1:1000 шаблонів в серверному режимі не більше 0,1 сек
* Розмір даних відбитку 256 ~ 384 байти
* Інтерфейс зв'язку Rs485, Ethernet
* Wiegand-26 інтерфейс 1 вхід, 1 вихід
* Незалежна пам'ять для журналу подій
* Ключ шифрування даних 256 битий AES
* Живлення, максимальне споживання 12 В пост. струму, 1,5 А
* Температурний діапазон від -20 до +50 °С
* Габаритні розміри (L x W x H) 410х190х50 мм
* Виконання металевий антивандальний корпус



Рис. 3.21Електромагнітний замок Al-400

Призначений для установки на легкі міжкімнатні пластикові або дерев'яні двері. Тягове зусилля - до 400 кг Робоча температура - від -100С до +400°С [30].



Рис. 3.22 Кнопка виходу

Металева, накладна.

Вбудована світло-діодна індикація.



Рис. 3.23 Доводчик Dorma Ts-73

Призначений для установки на всі стандартні типи дверей масою до 110 кг, як усередині приміщення, так і на вулиці. Робоча температура - від -200С до +400°С. Кольори: сріблястий, темно-коричневий, білий.



Рис. 3.24 Датчик положення дверей ZN002

Частота: 2.4ghz

Температура діяльності: -20 до 80°С

Чутливість: - 97db



Рис. 3.25 Настільний сканер

Сканером є модуль для захоплення і передачі на ПК образу відбитку пальця. Унікальна технологія, що використовує прецизійну матрицю CMOS, дозволяє отримувати зображення відбитку пальця з високою якістю. Сканер може застосовуватися в будь-яких застосуваннях, де потрібна ефективна і достовірна ідентифікація людини. У сканер вбудована спеціальна електронна схема - LFD, що дозволяє відрізнити живий палець від муляжу.

Основні технічні характеристики:

Інтерфейс USB 1.1.

Дозвіл робочій поверхні - 508 dpi .

Розміри робочої поверхні сканування 16x24 мм .

Розмір відсканованого зображення 480х320 мм.

Температурний діапазон від 0°с до +55 °С.

Напруга живлення через USB порт.

Маса 80 г .

Швидкість передачі даних 6 Мбіт/сек.

Габаритні розміри 60 x 45 x 25 мм.



Рис. 3.26 Перетворювач інтерфейсу

Призначений для перетворення інтерфейсу Rs485 в USB і забезпечує обмін даними між комп'ютером, що управляє, і контролерами

Інтерфейс Rs485.

Швидкість обміну 38400, 57600 115200 біт/сек.

Живлення від USB порту.

Індикація режиму прийом/передача - є.

Шина даних USB 1.1 або 2.0.

## **3.5 Система контролю і управління доступом (СКУД)**

Біометрична СКУД складається з наступних елементів:

А) Станційне устаткування, до складу якого входять: сервер СКУД та сервер системи відео нагляду.

Б) Лінійне устаткування, що включає контролери СКУД .

Контролери сполучені між собою двопровідною лінією зв'язку з

інтерфейсом Rs-485 по схемі загальної шини. Як середовище передачі даних

інтерфейсу Rs-485 використовуються мідні виті пари. Ці групи

контролерів підключені до сервера, з якого здійснюється управління і

програмування кожного контролера.

В) Абонентські пристрої: електромагнітні замки, датчики положення дверей, зчитувачі відбитків пальців.

Точки контролю доступу СКУД

До складу СКУД входять точки контролю доступу (ТКД) двох типів:

* Двері з одностороннім контролем - в приміщенні будівлі;
* Турнікети: прохідна будівлі;

Точка контролю доступу функціонально складається з контролера доступу виконавчого механізму (турнікет, електричний замок ), зчитувачів, датчиків положення пристрою, що перегороджує, пультів (кнопок) управління виконавчим механізмом. До складу ТКД входить джерело резервованого живлення для підтримки працездатності пристроїв при тимчасовій пропажі

напруги живлячої мережі. Прохід через точки з контролем доступу здійснюється при спів паданні шаблону з запропонованим відбитком. У разі успішної виконавчий пристрій розблоковується дозволяючи прохід.

Робоче місце адміністратора

Управління системою і моніторинг за її роботою здійснюється з сервера системи, контроль здійснює адміністратор. Він з допомогою настільного сканера заносить відбитки співробітника чи відвідувача в базу системи доступу та назначає для кожного права доступу. Дані з шаблонами відбитків та правами назначеними для їх власників передаються в пам’ять контролера. Контролери доступу підключаються до сервера за допомогою перетворювача інтерфейсів USB <> Rs-485. Всі дані фіксуються в протоколі подій, який надалі дозволяє відновити картину що відбулася. Окрім подій системи на сервері розташовується база даних персоналу і конфігурації системи.

Сервер працює під управлінням операційної системи WINDOWS-XP Professional.

Входи в приміщення будівлі.

Із зовнішнього боку дверей, обладнаних одностороннім доступом встановлюється зчитувач відбитків пальців, а з внутрішньої сторони - кнопка виходу (рисунок 3.27).

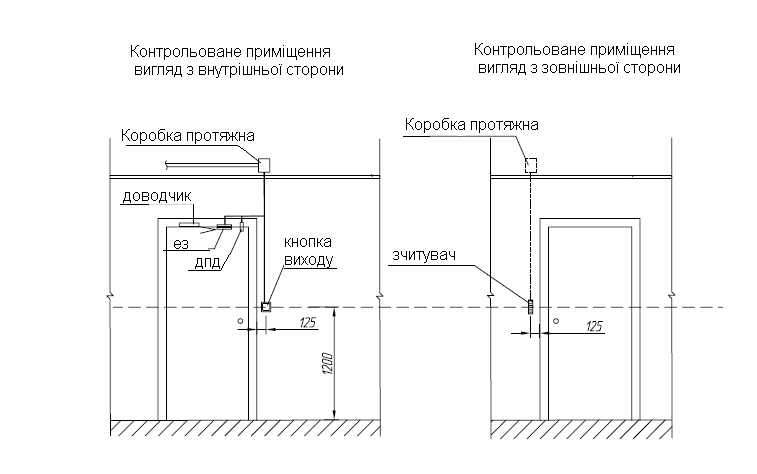


Рис. 3.27 Розміщення елементів СКУД

Блокування дверей здійснюється електромеханічним замком, що встановлюється в косяк. Закривання дверей забезпечує гідравлічний доводчик. Контролер управління дверима встановлюється в безпосередній близькості від точки доступу. Розміщення устаткування контролю доступу дверей вказано на рисунку №3.28 «Схема установки устаткування дверей з одностороннім доступом - ТКД1».

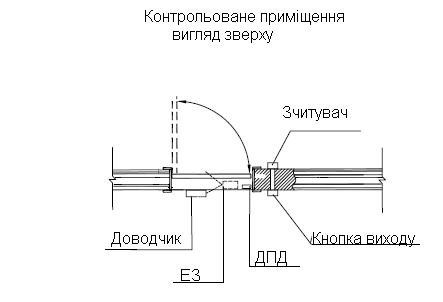


Рис. 3.28 Схема установки устаткування дверей з одностороннім доступом.

Прохід через точку доступу здійснюється таким чином:

• Співробітник або відвідувач, прикладає палець до зчитувача, встановленому поряд з контрольованими дверима. При успішній ідентифікації (наявності прав доступу у відповідну зону контролю) двері розблоковується, дозволяючи здійснити одноразовий вхід.

• Для виходу з контрольованої зони співробітник або відвідувач повинні натиснути кнопку виходу, при цьому двері розблоковуються, дозволяючи здійснити одноразовий вихід.

Електропостачання.

Живлення СКУД здійснюється від мережі змінної напруги 220в, 50гц. Захист кабелю здійснюється автоматичними вимикачами. Розрахунок струмів споживання системи контролю і управління доступом. При відключенні централізованого електропостачання вбудовані в контролери джерела безперебійного живлення забезпечують нормальну роботу системи.

Вимоги до монтажу устаткування і прокладки кабельних трас

а. Контролери СКУД встановлюються в безпосередній близькості від точок проходу в недоступному для сторонніх осіб місці, згідно схема розташування устаткування. Кріплення проводиться саморізами і пластиковими дюбелями.

б. Турнікети встановлюються згідно до «схеми установки турнікета» та інструкції по експлуатації. Установлюється на бетонну поверхню. За відсутності сформуваної раніше бетонної підстави згідно інструкції.

в. Дроти до турнікетів підводяться в гофрованих трубах під

поверхнею підлоги згідно інструкції з експлуатації.

г. Зчитувач встановити на привід турнікета відповідно до

технічних умов.

д. Зчитувачі, контролюючі прохід через двері встановити на рівні

1,2м від рівня підлоги, згідно схем установки устаткування дверей

і інструкції з експлуатації.

е. Електромагнітні замки, доводчики встановити згідно інструкції по

експлуатації і кресленням виробника.

є. Підведення мережевого живлення до автоматів живлення СКУД здійснюється в відповідності з ПУЕ.

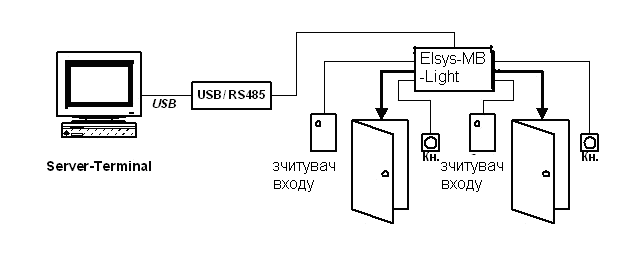


Рис. 3.29 Принципова схема мережі

## **3.6 Адміністративні зміни для впровадження біометричної системи доступу**

Для покращення системи безпеки, вносяться зміни до сталого режиму роботи підприємства. Можливо, потрібно буде внести зміни до штатного розкладу: ввести нові посадові одиниці або скоротити деякі посади, змінити посадові обов'язки працівників.

Необхідно виконати наступні заходи:

* Укладення договору обслуговування комерційним охоронним підприємством, якщо раніше такого договору не було. За наявності такого договору знадобиться погоджувати з охронним підприємством питання підключення нових охоронних приладів
* Зміна штатного розкладу.

При впровадженні системи безпеки в даній компанії зміна штатного розкладу не потрібна, оскільки в штатному розкладі передбачена посада адміністратора офісу Компанії. З урахуванням режиму роботи підприємства (5 днів по 10 годин) режим роботи адміністратора в дні чергування перевищує 8 годин тому передбачається, що дві люди позмінно виконують функції адміністратора.

У зв'язку з впровадженням системи слід додати ряд нових обов'язків в інструкцію адміністратора.

Зміна посадових обов'язків.

Обов'язки, що підлягають додаванню в посадову інструкцію адміністратора офісу:

• Ведення електронної бази даних біометричної системи безпеки, введення даних про прийнятих і звільнених співробітниках за допомогою програмного забезпечення.

• Надання та обмеження відповідних прав доступу в приміщення за допомогою програмного забезпечення.

• Перевірка стану приміщень Компанії перед закриттям офісу та здачею його на охорону допомогою програмного забезпечення або візуального огляду.

• Передача, або зняття приміщення з охорони.

• Фіксування запізнень співробітників на роботу; надання звітів про трудову дисципліну керівникові Компанії.

• Інформування відвідувачів про правила користування системою. Розмістити інформаційний плакат про роботу системи поряд з стійкою адміністратора.

Обов'язки, що підлягають видаленню з посадової інструкції адміністратора офісу:

• Ведення картотеки співробітників на спеціальних бланках кадрового обліку, в журналі.

• Щоденна видача ключів від приміщень компанії.

Обов'язки, що підлягають видаленню з посадової інструкції керівника Компанії:

• Контроль над дотриманням співробітниками посадових обов'язків, що вимагає особистої присутності.

Обов'язки, що підлягають додаванню в посадові інструкції співробітників Компанії:

• Використання власних відбитків для входу у відповідні приміщення компанії.

Обов'язки, що підлягають видаленню з посадових інструкцій співробітників Компанії:

• Щоденне отримання ключів від приміщень на початку робочого дня.

• Щоденна здача ключів від приміщень після закінчення робочого дня.

• Закриття приміщення на ключ у всіх випадках, коли в приміщенні не залишається жодного співробітника (перерва на обід і тому подібне).

Необхідні нормативні документи вимагають створення або доопрацювання у зв'язку з впровадженням біометричної системи доступу:

• Положення про внутрішньо-об'єктовий режим - документ призначений для викладу співробітникам компанії графіка роботи офісу, порядку доступу співробітників і відвідувачів, порядку здачі офісу під охорону і зняття з охорони. Документ включає розділ по забезпеченню пожежної безпеки, регламентує або забороняє куріння в офісі.

• Плакат про відео-спостереження, що ведеться, - для інформування відвідувачів і співробітників.

Посадова інструкція адміністратора офісу Компанії

Загальні положення

Адміністратор офісу Компанії співробітник відноситься до категорії технічних виконавців.

На посаду адміністратора офісу Компанії призначається особа, що має вищу професіональну освіту, без пред'явлення вимог до стажу роботи, або середню (повну) і спеціальну підготовку за встановленою програмою, без пред'явлення вимог до стажу роботи.

Призначення на посаду і звільнення від неї проводиться наказом керівника Компанії.

Адміністратор офісу Компанії повинен знати:

* структуру підприємства і режим роботи його підрозділів;
* нормативні правові акти, положення, інструкції, інші керівні матеріали і документи, що регламентують пропускний режим на підприємстві;
* правила і порядок надання доступу;
* основи організації праці;
* основи трудового законодавства;
* правила внутрішнього трудового розпорядку;

Адміністратор офісу Компанії підкоряється безпосередньо керівникові компанії.

На час відсутності адміністратора офісу Компанії (відпустка, хвороба, інше) наказом керівника підприємства призначається тимчасова особа.

Посадові обов'язки Адміністратор офісу Компанії:

* оформляє і надає права доступу для співробітників та відвідувачів.
* знімає приміщення з охорони перед початком робочого дня.
* здає приміщення на охорону після закінчення робочого дня.
* стежить за дотриманням порядку в приміщенні.
* стежить за працездатністю системи охоронної і пожежної сигналізації і при виникненні несправностей повідомляє про це керівництво компанії. При виникненні тривожної ситуації діє відповідно до інструкції про пожежну безпеку.

Адміністратор офісу Компанії має право:

* Ознайомитися з проектами, що стосуються його діяльності.
* Вимагати від керівництва підприємства сприяння у виконанні своїх посадових обов’язків.

Адміністратор офісу Компанії несе відповідальність.

## **3.7 Голосова аутентифікація**

Голос кожної людини, як і відбитки пальців є унікальним. На відміну від аутентифікації на основі аналізу сітківки ока або відбитків пальців, ідентифікація по голосу (voice biometrics) не вимагає великої кількості дорогих сканерів, аналіз відбувається на основі телефонного дзвінка, де голос людини звіряється з еталоном на центральному сервері. Сама технологія не нова і раніше були спроби використання так званої активної голосової біометрії - коли людині на початку діалогу пропонується назвати свою кодову фразу, яка буде звірятися з еталонною. Даний підхід мав ряд недоліків - користувачі в більшості випадків відмовлялися використовувати такий тип аутентифікації через психологічні причини і використання такого сервісу становила трохи більше 30% від усіх, хто телефонує. На зміну їй прийшла технологія пасивної голосової біометрії - коли людина спілкується з роботом (NLU) або з оператором і система в фоновому режимі порівнює його голос з еталонним зліпком.

Технологія Пасивної Голосовий біометрії має ряд переваг в порівнянні з активною голосової біометрією:

* Активна голосова біометрія не отримала популярності через додаткового навантаження на клієнта
* Вимагає явного дії клієнта для реєстрації та верифікації
* Відсутність підтримки з боку клієнтів
* Пасивна Голосова Біометрія активно використовується, завдяки прихованій роботі
* Відсутня перебивання клієнта і спрямоване дію
* Прозоро працює не впливаючи на дзвінок
* Потай реєструє і верифікує
* Оперує з високою точністю системами підприємства замовника.

Середній час необхідне для проведення голосової верифікації становить 15 секунд, достовірність верифікації становить понад 96%, зазвичай порівняння проводиться один до одного - тобто голос людини порівнюється з єдиним зліпком, але в деяких випадках може застосовуватися і метод «один до багатьох», коли зліпок порівнюється з невеликою групою зліпків (до 50) - що дозволяє ефективно шукати шахраїв, чий голос вже записаний і ефективно боротися зі фродом по телефону .

Використання голосу як пароля підвищує безпеку проведення активних операцій і може використовуватися як додатковий спосіб верифікації користувачів, також економить час операторів на проведення ручної аутентифікації.

Перспективи використання мови для авторизації користувачів в системах розмежування доступу

Перед будь-яким підприємством у сучасному світі гостро стоїть проблема захисту від несанкціонованого доступу до своїх матеріальних (приміщення, будівлі) і віртуальним (файли, бази даних) ресурсів. Для її вирішення застосовуються різні системи розмежування доступу. Важливим елементом такої системи розмежування доступу є спосіб авторизації (підтвердження автентичності особистості) користувача. Найпростішим в реалізації способом підтвердження прав доступу до матеріального ресурсу або об'єкта є використання механічного замку з ключем, а до віртуального - пароля доступу. Проте існують і інші, більш сучасні і надійні, методи підтвердження прав доступу.

**3.7.1** **Види авторизації**

1.**Однофакторна авторизація**

При однофакторній авторизації для отримання прав доступу до будь-якого ресурсу достатньо надати системі одне (будь-яке затверджене) підтвердження своїх прав. Всі використовувані в цьому випадку методи авторизації можна розділити на три види:

1). Знання людини. Доступ до ресурсу надається на підставі інформації, відомої людини. Наприклад, для доступу до комп'ютерної системи може використовуватися ім'я користувача (login) і парольна фраза. Варіантом цього методу служить система з однократними паролями (one time passwords), коли людина знає не сам пароль, а алгоритм його отримання за даними, наданими системою.

2). Об'єкти володіння. У користувача, що бажає отримати доступ до системи, є якийсь матеріальний об'єкт: брелок з записаним у нього електронним ключем, паперовий пропуск із штрих-кодом, ключ для механічного замку і т.п.

3). Невід'ємні властивості особистості. Антропометричні характеристики людини, які використовуються для його ідентифікації. Найбільш відомі приклади: відбитки пальців, відбиток долоні, малюнок на сітківці ока, мовні ознаки, елементи особи.

2. **Багатофакторна авторизація**

Основним недоліком всіх видів однофакторної авторизації, за винятком біометричної, є те, що елемент, на підставі якого надається доступ, може бути добровільно або насильно передано іншій особі. Пароль можна випадково («записав на папірці і втратив») або спеціально передати зловмисникові, електронний або паперовий пропуск можна «позичити» іншій людині, або його можуть забрати. Більш того, не всі біометричні ознаки дійсно є «невід'ємною частиною людини». Якщо важливість ресурсу, до якого необхідний несанкціонований доступ, дуже велика, зловмисники можуть отримати.   
Отже, для підвищення надійності обмеження доступу рекомендується використовувати багатоступінчасту систему авторизації, побудовану на комбінації двох або більше способів. Це може бути комбінація: пароль і відбиток пальця, або пароль і карту доступу.

Голосову біометрію, що включає в себе технології ідентифікації та верифікації особистості, не слід плутати з технологіями розпізнавання мови. Застосовуючи технології розпізнавання мови можна розпізнати, що людина говорить, але не ким він є. Отже, використання технологій розпізнавання мовлення обмежені в сфері забезпечення безпеки. Навпаки, технології ідентифікації та верифікації особистості по голосу знаходять своє застосування тоді, коли необхідно підтвердити, чи є людина тим, ким він є.

Результат біометричного вимірювання голосу повністю залежить від:

* вхідних даних;
* математичних алгоритмів;
* обчислювальної потужності.

Під вхідними даними мається на увазі біометричний зразок, або голосовий відбиток, що зберігається в базі даних. Якість біометричного зразка багато в чому залежить від типу пристрою введення (наприклад, професійний мікрофон або мобільний телефон) і навколишнього середовища (гучна вулиця або тихе приміщення). Існують технології, які автоматично визначають якість голосового відбитка, потім очищають його від шуму, щоб отримати більш якісний зразок.

Алгоритми в біометричних системах використовуються для того, щоб порівняти отриманий голосовий відбиток зі зразком в базі даних. Чим досконаліша алгоритм, тим точніше результат порівняння.

Під обчислювальною потужністю розуміють швидкість і якість обробки біометричних ознак користувача.

## **3.7.2 Голосова біометрія України**

Незважаючи на наявний покладиний досвід впровадження і використання голосових біометрій в сфері безпеки, Україну не можна вважати лідером в цій області. Традиційно тон на ринку нових технологій задають США, а також компанії з  Західної Європи та Ізраїлю.

На території колишнього СРСР найбільш активну позицію по масштабному впроваджені технології голосової біометрії сьогодні займає МВС Республіки Білорусь.Розпочалася реалізація програми зі створення фонообліку в Республіці Казахстан.

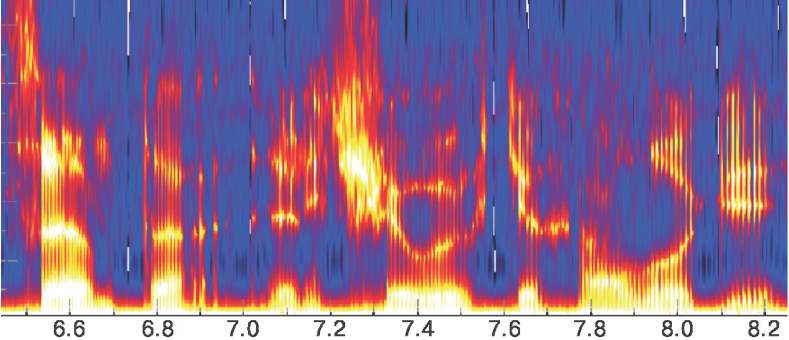


Рис. 3.7.1. Формантноє уявлення фрази "Центр мовних технологій"

Незважаючи на відставання, в України є реальний шанс надолужити згаяне і стати одним з світових лідерів в області біометрії. Створено і все активніше працює Українське біометричне суспільство, розробка біометричних стандартів, все більше державних замовлень на виконання ДКР, пов`язаних з розробкою систем голосової біометрії, розміщені у наукових інститутах та комерційних компаніях.

Приклад автоматично виділеного основного тону при проголошенні фраз"Центр мовних технологій" наводиться на рис. 3.7.

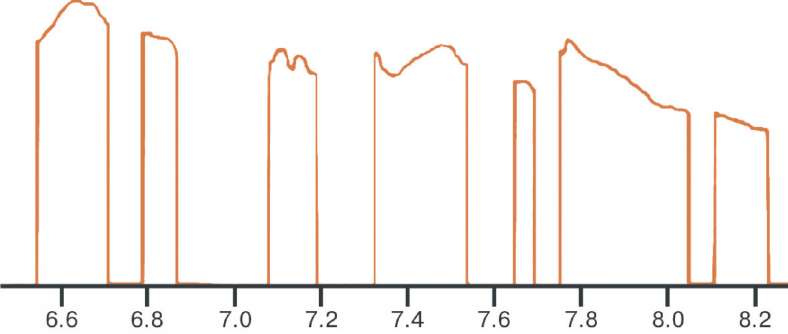


Рис.3.7.2. Крива основного тону при проголошенні фрази "Центр мовних технологій"

Практика застосування різних технологій верифікації-ідентифікації в реальних умовах показала залежність надійності роботи систем голосової біометрії від якості сигналу: рівня широкосмугових завад і спотворень, що вносяться до сигнал при передачі по каналах зв'язку. У зв'язку з цим фахівцям ЦРТ довелося вирішувати завдання щодо зниження рівня широкосмугових шумів, видаленню тривалих немовних фрагментів сигналу (у тому числі технічних сигналів), "нор-малізаціі на канал" (компенсація канальних спотворень АЧХ).

У 2006-2007 роках у ЦРТ був реалізований метод верифікації на основі СГР (суміші гауссових розподілень). Використання даного методу дозволяє істотно підвищити надійність верифікації на коротких фрагментах мови. Але на практиці цей метод демонструють високу ефективність тільки щодо мовних сигналів високої якості при відношенні сигнал / шум вище 20 дБ.

У цьому році ЦРТ завершує розроботку нової модифікації системи "Трал" для використання в оперативних підрозділах правоохоронних органів, продовжує удосконалювати методи і середовища криміналістичної ідентифікації осіб по мові, не залежною від мови проголошення, проводить адаптацію технологій верифікації для роботи в різних каналах зв'язку.

Перспективи використання мови для авторизації користувачів в системах розмежування доступу.

Перед будь-яким підприємством у сучасному світі гостро стоїть проблема захисту від несанкціонованого доступу до своїх матеріальних (приміщення, будівлі) і віртуальним (файли, бази даних) ресурсів. Для її вирішення застосовуються різні системи розмежування доступу. Важливим елементом такої системи розмежування доступу є спосіб авторизації (підтвердження автентичності особистості) користувача. Найпростішим в реалізації способом підтвердження прав доступу до матеріального ресурсу або об'єкта є використання механічного замку з ключем, а до віртуального - пароля доступу. Проте існують і інші, більш сучасні і надійні, методи підтвердження прав доступу.

Особливості використання мови для авторизації доступу.

Головною перевагою мови в системах біометричної верифікації є те, що, на відміну від постійних ознак людини, які він не може довільно змінювати, він може на свій розсуд керувати тим, що він говорить. Тобто, рішення про допуск може прийматися не тільки на основі унікальних для кожної людини ознак голоси, але і на підставі аналізу виголошеній парольного фразі, інтонації мови. Наприклад, можлива така, досить проста, схема: для кожного дня тижня записується свій мовний пароль. При цьому: 1) ідентифікація користувача по голосу є текстозалежною (навіть без перекладу мови в текст); 2) забезпечується відразу два види авторизації: людина знає необхідне слово і несе в собі необхідні для авторизації характеристики. Іншим незаперечним достоїнством використання мови як біометричного ознаки є можливість верифікації особи за ознакою її емоційного стану. Припустимо, якщо людину примушують вимовити парольний фразу «під дулом пістолета», його голос, поза волею (або свідомо) змінюється. Цей факт можна використати як підставу для відмови в доступі на охоронюваний об'єкт, так і для визначення того, що парольна фраза говориться під примусом. Можна заперечити, що ця перевага буде одночасно і недоліком системи біометричної верифікації на основі мови, оскільки потенційно призводить до відносно високому відсотку «відмови своєму». За інформацією його величина зазвичай складає 1-5%, у деяких системах може досягати 40%. Однак, цей недолік досить легко долається за допомогою самотренування людини, та використання адаптивних алгоритмів верифікації, які відстежують невеликі зміни в характеристиках голосу.

У розряд достоїнств голосової біометричної верифікації можна сміливо віднести мінімальні витрати на її експлуатацію. Системи з її використанням не вимагають установки складного дорогого устаткування, такого як зчитувачі відбитків пальців або райдужної оболонки.

Ще одним недоліком верифікації за допомогою мови багато хто вважає можливість використання аудіозаписів для отримання несанкціонованого доступу. Проте не потрібно забувати, що біометричні ознаки, використовувані для верифікації, значною мірою залежать від особливостей мовного апарату конкретної людини і спотворюються при використанні технічних засобів, як на етапі запису, так і на етапі відтворення. Використання запису також не принесе «позитивного» результату, у разі правильного підбору залежності парольних фраз від зовнішніх умов.

Наприклад, можна побудувати систему авторизації таким чином, щоб користувач вимовляв назву дня тижня і кольору, зображеного на екрані. Колір відображається генератором випадкових чисел з трьох можливих, що дає 21 парольну фразу. У такій ситуації зловмисник повинен не тільки записати звук потрібного обличчя, але й знати алгоритм його використання. Такий підхід дозволяє створити нескінченну безліч подібних легко запам`ятованих схем верифікації.

Також в числі недоліків системи управління доступом, що використовує авторизацію по голосу, вказується відносне незручність її використання при організації доступу великої кількості користувачів протягом короткого часового періоду. У ситуації, коли 200 чоловік повинні пройти через двері, оснащених «мовним замком», буде потрібно близько 20 хвилин тільки на обговорювання парольного фрази (при її тривалості 5-7 секунд). Проте, відзначимо, що подібні недоліки є і в інших схемах авторизації, як за біометричними ознаками, так і при використанні ключа або коду. У порівнянні з іншими, системи верифікації по голосу більш «доброзичливі» до користувачів: багато людей відчувають дискомфорт при використанні сканера райдужної оболонки або сканера відбитків пальців. Запам'ятати ж парольний фразу, або спосіб її утворення і впевнено її вимовити, здатна практично будь-яка людина.

На жаль, верифікація по голосу не може бути застосована у випадку, якщо людина володіє обмеженими можливостями мови (страждає сильним заїканням, не здатний говорити). Але такі «недоліки», як неправильне вимовляння окремих звуків, не є перешкодою до використання верифікації по голосу. В якості додаткової міри для підвищення надійності верифікації по голосу можна використовувати технологію пошуку ключових слів або розпізнавання мови.

## **3.8 Система розмежування доступу на основі біометричної мовної верифікації - Voice Key Service**

Система Voice Key Service розроблена компанією ТОВ «Центр Мовних Технологи» призначена для організації регламентованого доступу користувачів до корпоративних інформаційних ресурсів за заданою парольною фразою. VoiceKey-Service є ефективним рішенням, яке дозволяє доповнити систему інформаційної безпеки підприємства, побудовану на основі групових політик, засобами біометричної верифікації.

Основні характеристики:

* + Клієнт-серверна архітектура.
  + Web-інтерфейс для проходження верифікації.
  + Час підходу - не більше 5 сек.
  + Тривалість парольної фрази - достатньо 3 сек.
  + Вимоги до парольної фрази - достатньо 5-6 різних голосних звуків російської мови в ударній позиції.
  + Механізм контролю якості та актуалізації еталонних карток.
  + Засоби адміністрування користувачів та аудиту верифікації.
  + Клієнтські ПК повинні бути оснащені звичайними мікрофонами, підключені до стандартних мультимедійних звуковим картам.

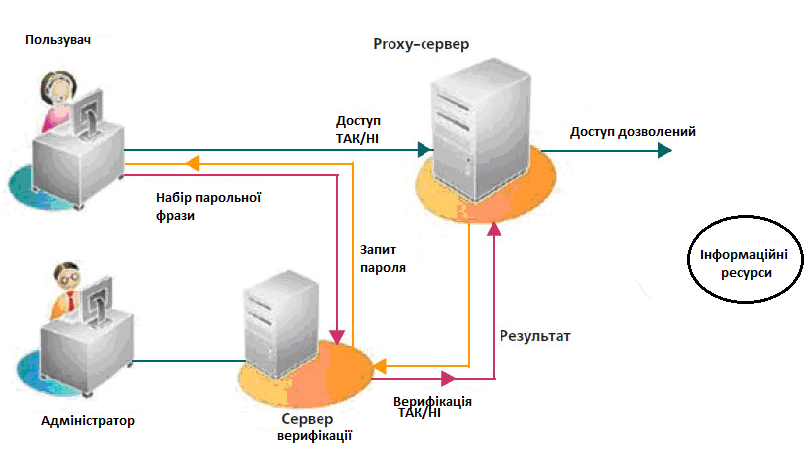


Рисунок 3.7.3. Архітектура сервісу

Архітектура сервісу і опис його роботи

При доступі користувачів до інформаційного ресурсу їх запит переадресовується на сервер верифікації. Сервер верифікації завантажує на робоче місце співробітника web-сторінку з пропозицією вимовити в мікрофон, підключений до його комп'ютера, задану парольну фразу. Користувач вимовляє пароль, звукові дані надходять на сервер верифікації, де проводиться їх порівняння з еталоном. У разі успішного проходження верифікації користувачеві надається доступ до інформації.

Відмінні риси:

• унікальні алгоритми аутентифікації;

• не вимагається установки програмного забезпечення на клієнтських робочих місцях;

• мінімальна кількість часу і дій при процедурі верифікації;

• коштів аудиту, що підтверджують необхідний рівень надійності верифікації;

• біометричний мовної ключ неможливо втратити, вкрасти або скопіювати як електронний ключ, smart-карту або пароль, що вводиться з клавіатури;

• низька вартість впровадження і швидке повернення інвестицій.

Приклади впровадження систем авторизації на основі мовної біометрії  
VoiceKey Service Центр Мовних Технологій - голосова авторизація використовується для розмежування доступу до різних Internet і Intranet ресурсів. Система розгорталася для створення універсального способу авторизації по голосу з використанням Web-браузера.

VoicePay - система електронних платежів, повністю керована голосом.  Перша в світі платіжна система, всі операції в якій виробляються за допомогою голосу. Користувачеві не потрібно запам'ятовувати паролі, система не зберігає особистих даних і, відповідно до твердження власників, повністю безпечна.

Банківська група ABN AMRO - біометрична голосова система використовується для ідентифікації користувачів банківських послуг по телефону. Запущено біометричну аутентифікацію по голосу для клієнтів, які запитують різну інформацію про свій рахунок, таку як баланс, інформацію про переведення грошей і т.п.

Australian social security agency Centrelink - біометрична голосова система використовується для авторизації запитів по телефону. Також використовується для виявлення спроб шахрайства, наприклад виявлення факту доступу до декількох рахунках одного диктора. Крім того, різні види голосової біометрії були поза дрени для контролю доступу в багатьох інших організаціях, таких як US Department of Agriculture , Volkswagen Financial Services, уряд Австралії, Bell Canada, Aeroplan

У засобах масової інформації все частіше з'являється інформація про впровадження нових технологій верифікації в сервіси, доступні широкому колу користувачів, що підкреслює високий рівень їх надійності та безпеки. Але, з міркувань безпеки, компанії не прагнуть до розголошення інформацій впровадженні на підприємстві систем розмежування доступу та механізми їх реалізації, хоча попит на подібні рішення зростає рік від року.

Існує ряд факторів, які можуть сприяти виникненню помилок верифікації та ідентифікації, наприклад:

* неправильне проголошення або прочитання парольного слова або фрази;
* емоційний стан диктора (стрес, проголошення парольної фрази під примусом та ін.);
* складна акустична обстановка (шум, перешкоди, радіохвилі тощо.);
* різні канали зв'язку (використання різних мікрофонів під час реєстрації диктора і верифікації);
* простудні захворювання;
* природні зміни голосу.

Деякі з них можуть бути усунені, наприклад, шляхом використання більш якісних мікрофонів.

Процес верифікації особистості по голосу складається з 5 етапів: прийом мовного сигналу, параметризація, або виділення характерних ознак голосу, порівняння отриманого зразка голосу з раніше встановленим еталоном, прийняття рішення «допуск / відмова», навчання, або оновлення еталонної моделі. Схема верифікації представлена ​​на малюнку 4.

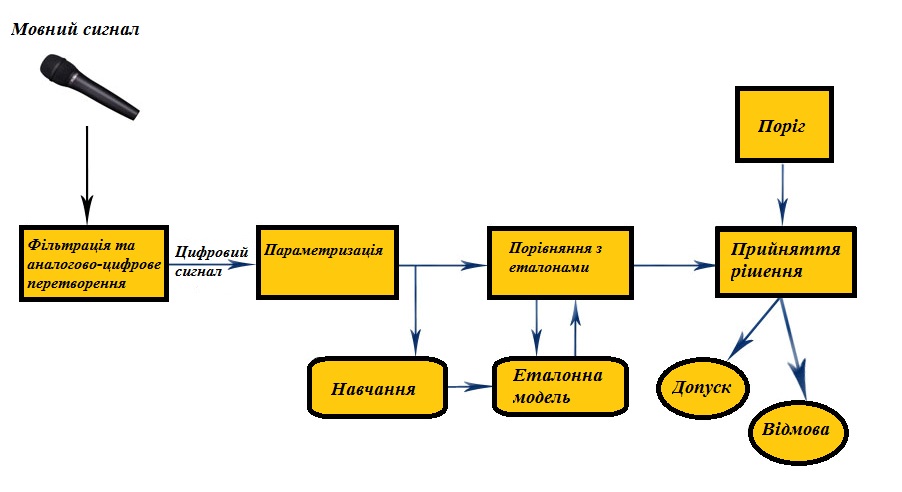


Рис.3.7.4. Схема верифікації.

Під час реєстрації новий користувач вводить свій ідентифікатор, а потім вимовляє кілька разів ключове слово або фразу, таким чином створюються еталони. Число повторів ключової фрази може варіюватися для кожного користувача, а може бути постійним для всіх.

Для того щоб комп'ютер міг обробити мовний сигнал, звукова хвиля перетворюється в аналоговий, а потім в цифровий сигнал.

На етапі виділення ознак голосу мовний сигнал розбивається на окремі звукові кадри, які згодом перетворюються в цифрову модель. Ці моделі називають «голосовими відбитками». Знову отриманий «голосовий відбиток» порівнюється з раніше встановленим еталоном. Для розпізнавання особистості говорить найважливішими є найбільш яскраві відмінні ознаки голосу, які дозволили б системі з високою точністю розпізнавати голос кожного конкретного користувача.

Нарешті, система приймає рішення допустити або відмовити користувачеві у допуску в залежності від збігу або розбіжності його голосу з встановленим еталоном. Якщо система невірно зіставили пред'явлений їй голос з еталоном, то виникає помилка «помилковий допуск» (FA). Якщо ж система не впізнала біометричний ознака, який відповідає наявному в ній ідеалу, то говорять про помилку «помилковий відмова» (FR). Помилка помилкового допуску створює пролом в системі безпеки, а помилка помилкового відмови призводить до зменшення зручності користування системою, яка іноді не розпізнає людини з першого разу. Спроба знизити ймовірність виникнення однієї помилки призводить до більш частого виникнення іншої, тому в залежності від вимог до системи вибирається певний компроміс, тобто встановлюється поріг прийняття рішення.

## **3.9 Порівняльний аналіз**

Кожен з біометричних методів, розглянутих вище, має свої переваги і недоліки. Приведено порівняння методів за сімома вимогами, що пред'являються до біометричних ознак.

Таблиця 4

На додаток існує декілька приватних вимог до розробки біометричних методів :

|  |  |  |  |
| --- | --- | --- | --- |
| Біометрични метод  Характеристика | По відбитку пальця | По голосу | По голосу + відбиток пальця |
| Придатність для багато кратної ідентифікації | Висока | Середня | Висока |
| Захищеність | Висока | Середня | Висока |
| Експлуатація | Середня/Висока | Низька | Середня |
| Зручність використання | Висока | Висока | Висока |
| Універсальність | Середня | Середня | Середня |
| Унікальність | Висока | Середня | Висока |
| Ефективність | Середня | Середня | Висока |
| Доступність | Висока | Висока | Висока |

Н- низька, С- середня, В- висока

## **Висновки до 3 розділу**

За неналежного виконання або невиконання своїх посадових обов'язків, передбачених цією посадовою інструкцією, в межах, визначених трудовим законодавством України.

За правопорушення, здійснені в процесі здійснення своєї діяльності, в межах визначених адміністративним, кримінальним і цивільним законодавством України.

За спричинення матеріального збитку в межах, визначених трудовим і цивільним законодавством України.

Спроектована система відзначається високою надійністю, автономністю, енерго – незалежністю, може легко розширюватися та інтегруватися зі вже існуючими.

Дана система призначена для впровадження на режимних об’єктах та інших організаціях з підвищеними вимогами до безпеки.

З доступних сьогодні видів біометричних технологій голосова біометрія є найбільш вигідною і зручною для користувача, тому незабаром рішення з використанням голосової біометрії стануть застосовуватися повсюдно. PIN-коди можуть бути забуті, магнітні картки - загублені або вкрадені, а спеціальні скануючі пристрої вимагають вкладення чималих грошей. Навпаки, голосова біометрія робить ідентифікацію можливої ​​в будь-якому місці в будь-який час. Все що Вам потрібно - це скористатися мобільним або стаціонарним телефоном, або мікрофоном.

# ВИСНОВКИ

При виконанні дипломної роботи було виконано ряд завдань, які є необхідними при проектуванні системи, а саме:

1. Проведено аналіз сучасного ринку контролю доступу.
2. Визначено критерії захищеності системи.
3. Досліджено технології створення біометричних систем контролю доступу.
4. Досліджено ефективність впровадження системи
5. Досліджено біометричні методи.

Виходом з даної ситуації може бути використання засобів біометричної ідентифікації. Оскільки в них ідентифікується не предмет, а сама особа - носій біометричної інформації.

У дипломній роботі було використано методи, які базуються на концепціях і принципах системного аналізу, побудові принципових схем та методах їх модернізації, а також на методі дослідження ієрархії.

Спроектована система відзначається високою надійністю, автономністю, енерго – незалежністю, може легко розширюватися та інтегруватися зі вже існуючими.

Дана система призначена для впровадження на режимних об’єктах та інших організаціях з підвищеними вимогами до безпеки.

У зв’язку зі світовою тенденцією поширення використання біометричних систем дана розробка являється дуже актуальною та включає в себе передові технології захисту інформації.

З доступних сьогодні видів біометричних технологій голосова біометрія є найбільш вигідною і зручною для користувача, тому незабаром рішення з використанням голосової біометрії стануть застосовуватися повсюдно. PIN-коди можуть бути забуті, магнітні картки - загублені або вкрадені, а спеціальні скануючі пристрої вимагають вкладення чималих грошей. Навпаки, голосова біометрія робить ідентифікацію можливої ​​в будь-якому місці в будь-який час. Все що Вам потрібно - це скористатися мобільним або стаціонарним телефоном, або мікрофоном.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анін Б. Захист комп’ютерної інформації. СПб.: БХВ - Петербург, 2000. – 384 с.
2. Безконтактна інтегральна схема: Рішення про видачу патенту на винахід по заявці МA 2003121045/28(022822) від 11.07.2003 / Конявский В.А., Лівшиц В.И. - ФІПС, № 2003121045/28(022822) від 27.06.2004.
3. Герасименко В.А., Малюк А.А. Основи захисту інформації. — М.: МГИФІ, 1997.
4. ГОСТ 28147-89. Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення.
5. ДНАОП 0.00-1.31-99. Правила охорони праці під час експлуатацiї електронно-обчислювальних машин. - Київ: Наказ Комітету по нагляду за охороною праці України Міністерства праці та соціальної політики України від 10 лютого 1999 року № 21, 1999.
6. ДСанПіН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин. - Київ: Головне санітарно-епідеміологічне управління Міністерства охорони здоров’я України, 1998.
7. ДСТУ 3008 – 95. Документація. Звіти у сфері науки і техніки. Структура і правила оформлення.
8. Зима В.М.. Молдовян А.А., Молдовян Н.А. Комп’ютерні мережі і захист інформації, що. — СПб.: СПбГУ, 1998.
9. Ігнатов В.В. Захист інформації в корпоративних TCP/IP мережах. //Конфідент. Захист інформації. 1998, №3. — с. 44.
10. Конявский В.А., Гадасін В.А. Основи розуміння феномена електронного обміну інформацією. Мн.: Белліт фонд. – 2004, 453с.
11. Леонов А. П., Леонов К. П., Фролов Г. В. Безпека автоматизованих банківських і офісних технологій. — Мінськ : Нац. кн. палата Білорусі, 1996.
12. Мельников В.В.Захист інформації в комп’ютерних системах. — М.: Фінанси і статистика, 1997.
13. Оліфер В.Г., Оліфер Н.А. «Комп’ютерні мережі. Принципи, технології, протоколи» - СПб.: Петербург, 2001 - 672 с.
14. Оцінки і прогнози. //Конфідент. Захист інформації. 1998, №4.— с.7.
15. Петренко C.А. Симонов С.В. Економічно виправдана безпека. Управління інформаційними ризиками. - М.: ДМК, 2003.
16. Програмно – апаратний комплекс засобів захисту інформації від НСД для ЭВМ(PC)“Акорд–АМДЗ” (версії 2.0, 3.0, 4.0) Опис використання. – 234с.
17. Програмно – апаратні засоби забезпечення інформаційної безпеки. Захист програм і даних/ П. Ю. Бєлкін, О. О. Михальський, А. С. Першаков и др. – М.: Радіо і зв’язок. – 2000, 345с.
18. Романец Ю.В.. Тимофєєв П.А., Шаньгін В.Ф. Захист інформації в комп’ютерних системах і мережах. — М.: Радіо і зв’язок, 1999.
19. Сініцин І.Н., Губін А.В., Ушмаїв О.С. Метрологічні і біометричні технології та системи. - 2008. №7. С.41 – 44.
20. Теоретичні основи комп’ютерної безпеки /П. Н. Дев’янін, О. О. Михальський, Д. И. Правиков та ін. – М.: Радіо і зв’язок, 2000. – 192 с.
21. Тимофєєв П.А. Принципи захисту інформації в комп’ютерних системах. //Конфідент. Захист інформації. 1998, № 3. — с. 72.
22. Ушмаїв О.С. Використання біометрії в аеропортах Biometrics TTS 2007.
23. Ушмаїв О.С. Реалізація біометричної системи в правоохоронних системах. – 2007, 254с.
24. Ушмаїв О.С., Босов А.В. Реалізація концепції багатофакторної ідентифікації в інтегрованих аналітичних системах 2007. Т.3. № 4. С.13-2

ЕЛЕКТРОННІ РЕСУРСИ

1. http://www.nist.gov
2. http://www.fbi.gov/hq/cjisd/iafis
3. http://www.smartcardalliance.org/
4. http://www.biometrics.org
5. http://www.ibia.org
6. http://www.bioapi.org
7. http://www.bioscrypt.com
8. http://www.digitalpersona.com
9. http://www.ethentica.com
10. http://www.identix.com
11. http://www.precisebiometrics.com
12. http://www.saflink.com
13. http://www.accord.ru
14. http://csrc.nist.gov/encryption/aes/round1/docs.html
15. http://www.citforum.ru
16. www.biolinkusa.com

41.НД ТЗІ 2.5-005-99 “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”.

42.НД ТЗІ 2.5-004-99 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”.

43.ДСТУ 4163-2003 Вимоги до оформлювання документів.

44.Закон України „Про інформацію”.

45.Закон України „Про науково-технічну інформацію”.

46.ГОСТ 34.602-89 вимоги до технічного завдання на проектування автоматизованих систем.