Лекція 4

Методи та засоби захисту інформації від несанкціонованого доступу

План лекції

2.1. *Способи та методи несанкціонованого доступу в сучасних інформаційно-комунікаційних системах.*
2.2. Основні принципи захисту інформації від НСД.
2.3. Класичні моделі розмежування доступу.
2.4. Ідентифікація і аутентифікація користувачів

Історичний ракурс

Історія

Указ Імператриці Єлизавети Петрівни
(С. Петербургские ведомости, 1750 г., №46)

«Мы с крайним неудовольствием уведомились, что многие как из наших подданных, так и живущих здесь в нашей службе и в нашей протекции иностранцев, разглашая многие лживые ведомости о нынешних статских, политических и воинских делах, присовокупляя к тому развратные толкования и совсем нескладные рассуждения, с столь большею продерзостью, сколь меньшее об оных имеют они сведение и понятие; и для того запотребно рассудили мы чрез сие для известия каждого объявить: что ежели кто отныне, разглашая какие-либо известия или еще и вымышляя оные, о не принадлежащих до него особливо политических и воинских делах превратные толкования и рассуждения делать станет, а нам о том донесется, такой неминуемо всю тягость нашего гнева почувствует»

2.1. Способи та методи несанкціонованого доступу в сучасних інформаційно-комунікаційних системах

Способи та методи несанкціонованого доступу в сучасних ІКСМ

За принципом

- фізичний НСД;
- логічний НСД

По положенню джерела

- джерело розташовано у локальній мережі;
- джерело розташовано поза локальною мережею.

По режиму виконання

- виконуються при постійній участі людини;
- виконуються спеціально розробленими програмами

За типом використаних вразливих місць

- недоліки політики безпеки,
- помилки адміністративного управління;
- недоліки алгоритмів захисту,
- помилки реалізації проекту системи захисту.

По шляху

- використання прямого стандартного шляху доступу до комп'ютерних ресурсів;
- використання схованого нестандартного шляху доступу до комп'ютерних ресурсів.

По місцю розташуванню об'єкта атаки

- зовнішні запам'ятовуючі пристрої;
- інформація, яка передається в лініях зв'язку;
- інформація, яка обробляється в основній пам'яті комп'ютера.

По безпосередньому об 'єкту атаки

- на політику безпеки і процес адміністративного управління,
- на постійні компоненти системи захисту,
- на змінні елементи системи безпеки;
- на протоколи взаємодії;
- на функціональні елементи комп'ютерної системи.

Алгоритм підготовки і реалізації несанкціонованого доступу в сучасних ІКС

Висновок з питання 1

Таким чином, на основі проведеного аналізу актуальних методів та способів несанкціонованого доступу в сучасних інформаційних системах та мережах проведено їх класифікацію за базовими критеріями.

На основі проведених досліджень виділено основні недоліки при проектуванні системи захисту інформації, а саме від несанкціонованих дій користувачів і програм; втрати інформації і порушення працездатності комп'ютерної системи та адміністративного управління мережею.

2.2. Основні принципи захисту інформації від НСД

Основні принципи захисту інформації від НСД

1 ***Принцип обґрунтованості доступу***

✓ **Користувач повинен мати достатню «форму допуску» для отримання доступу до інформації даного рівня конфіденційності;**

✓**Користувачу необхідний доступ до даної інформації для виконання його виробничих функцій**

Основні принципи захисту інформації від НСД

2 *Принцип достатньої глибини контролю доступу*

Відомості про засоби захисту інформації повинні включати механізми контролю доступу до всіх видів інформації та програмного забезпечення ресурсів, які відповідно до принципу розумності повинні розділені між користувачами

Основні принципи захисту інформації від НСД

3 ***Принцип розмежування потоків інформації***

Потоки інформації повинні розмежовуватися в залежності від рівня її конфіденційності

(для реалізації принципу всі ресурси, які містять конфіденційну інформацію, повинні мати відповідні мітки, що відображають рівень конфіденційності)

Основні принципи захисту інформації від НСД

4 ***Принцип чистоти ресурсів, що повторно використовуються***

Повинна бути передбачено очищення ресурсів, що містять конфіденційну інформацію, до перерозподілу даних ресурсів іншим користувачам

Основні принципи захисту інформації від НСД

5 *Принцип персональної відповідальності*

✓ Індивідуальна ідентифікація користувачів та процесів, що ними ініціюються

(ідентифікатори повинні містити відомості про форму допуска користувача та його прикладної області)

✓ Перевірка справжності користувачів та їх процесів по пред'явленому ідентифікатору (аутентифікації)

✓ Реєстрація (протоколювання) роботи механізмів контролю доступу до ресурсів систем з вказанням дати, часу, ідентифікаторів особи, що запитує ресурс, включаючи невдалі спроби доступу

Основні принципи захисту інформації від НСД

6 *Принцип цілісності засобів захисту*

Система захисту інформації повинна точно виконувати свої функції у відповідності з основними принципами і бути ізольованою від користувачів

(побудова засобів захисту проводиться в рамках окремого монітору звернень , який контролює будь-які запити до даних або програм з боку користувачів)

Монітор звернень

Вимоги:

Механізми контроля →
- **Захищені від стороннього втручання в їх роботу**
- **Завжди працюючий в належному стані**
- **Достатньо малі за розміром**

Висновок з питання 2

1. Наведено та проаналізовано основні принципи захисту інформації від НСД в сучасних ІКС. До них відносять принципи: обґрунтованості доступу, достатньої глибини контролю доступу, розмежування потоків інформації, чистоти повторного використання ресурсів, персональної відповідальності, цілісності засобів захисту .
2. Визначено, що реалізація перерахованих принципів здійснюється за допомогою «монітора звернень», який контролює будь-які запити до даних або програм з боку користувачів.

2.3. Класичні моделі розмежування доступу

Класичні моделі розмежування доступу

1 Вербальний опис правил розмежування доступу

Модель розмежування доступу до захищеної ОС ADEPT-50 (розроблена на замовлення МО США)

1. **Користувачу дозволено доступ в систему, якщо він входить в множину відомих системі користувачів**
2. **Користувачу дозволено доступ до терміналу, якщо він входить у підмножину користувачів, що закріплені за даним терміналом.**
3. **Користувачу дозволений доступ до файлу, якщо:**

   а) рівень конфіденційності користувача не нижче рівня конфіденційності файлу;

   б) прикладна область файлу включає прикладну область завдання користувача;

   в) режим доступу до споруд користувача включає режим доступу;

   г) користувач входить в підмножину допущених к файлу користувачів.

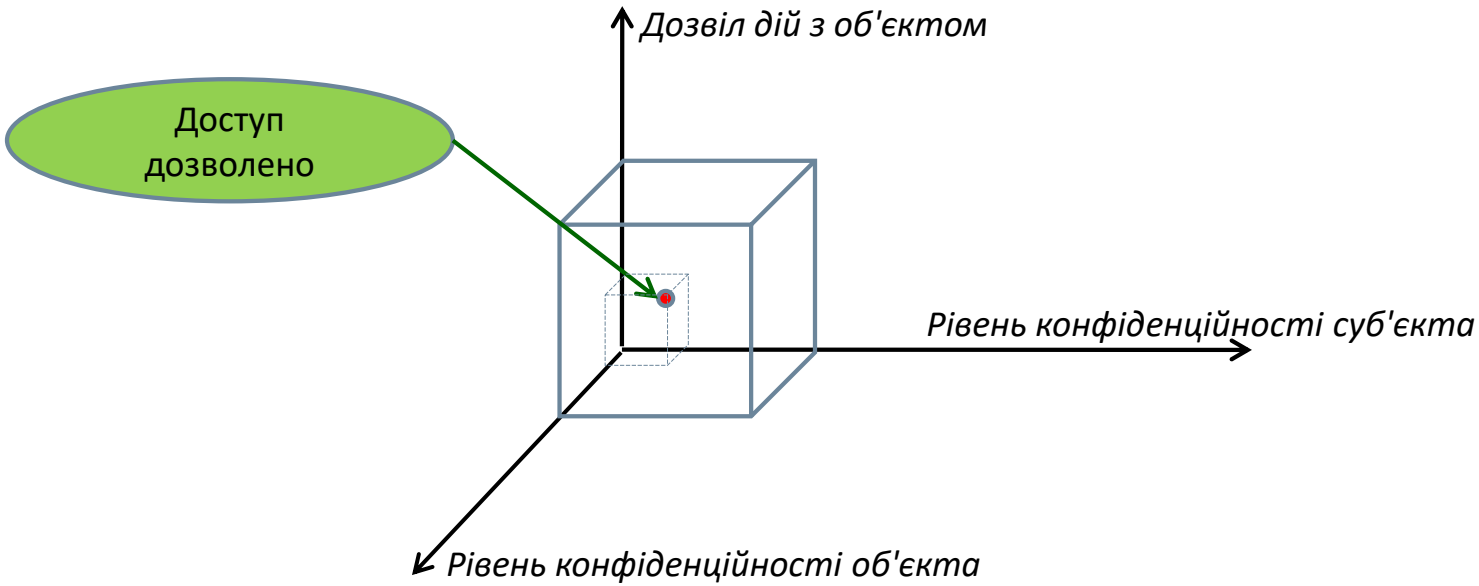
Підходи до організації розмежування доступу

повноважний (мандатний - англ. ***mandatory access control - MAC).***

матричний (дискреційний - англ. **discretionary access control - DAC**

Класичні моделі розмежування доступу

2 Побудова простору безпеки



Модель Хартсона (п'ятимірний простір безпеки):

- ***встановлення повноважень;***
- ***користувачі;***
- ***операції;***
- ***ресурси;***
- ***стан.***

Класичні моделі розмежування доступу

3 Модель Лемпсона – Грехема – Деннінга (побудова матриці доступу)

Обєкти доступа

Суб'єкти доступа

	O_1	O_2	…	O_n
S_1	T_{11}	T_{12}	…	T_{1n}
S_2	T_{21}	T_{22}	…	T_{2n}
…	…	…	…	…
S_m	T_{m1}	T_{m2}	…	T_{mn}

Елемент T_{ij} визначає привілеї суб'єкту доступа S_i по відношенню до об'єкту доступу O_j

Види доступа: виконання, виділення (пам'яті), читання, запис.

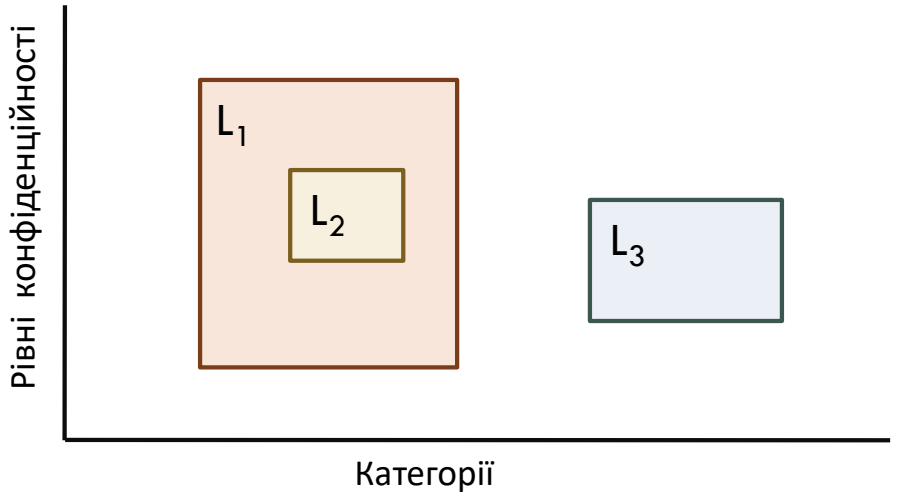
Коли суб'єкт S_i ініціюють доступ видуT_k до объекту O_j, монітор звернень перевіряє наявність T_k в елементі матриці звернень $A[S_i,O_j]$.

Доступ дозволено, якщо $T_k \leq T_{ij}$

Класичні моделі розмежування доступу

4 Модель Белла – Ла Падула

Об'єкти та суб'єкти доступу характеризуються рівнями конфіденційності та категоріями (предметною областю)



L – рівні безпеки

L_1 домінує над L_2; L_1 и L_3 (L_2 и L_3) незрівняні

Класичні моделі розмежування доступу

4 Модель Белла – Ла Падула

Види доступу

Тільки читання → Рівень безпеки суб'єкта повинен домінувати над рівнем безпеки об'єкта

Тільки запис → Рівень безпеки об'єкта повинен домінувати над рівнем безпеки суб'єкта

Читання та запис → Рівень безпеки об'єкта повинен бути рівним над рівнем безпеки суб'єкта

Ні читання, ні запис → Рівні безпеки суб'єкта та об'єкта незрівняні

Висновок з питання 3

Підводячи підсумки розгляду двох класів моделей захисту інформації, відзначимо, що *перевага матричних моделей* полягає в легкості представлення широкого спектра правил забезпечення безпеки інформації. Головний недолік цих моделей - велика розмірність матриць доступу в реальних системах, що веде до неможливості практичної адекватної її реалізації.

Головним *недоліком багаторівневих моделей* є неможливість управління доступом до конкретних об'єктів на основі обліку індивідуальних особливостей кожного з суб'єктів.

Отже, два підходи ніби передбачають пошук різних компромісів між ефективністю, гнучкістю і безпекою. Вочевидь, оптимальне вирішення питань безпеки повинне вироблятися з застосуванням двох видів моделей захисту.

2.4. Ідентифікація і аутентифікація користувачів

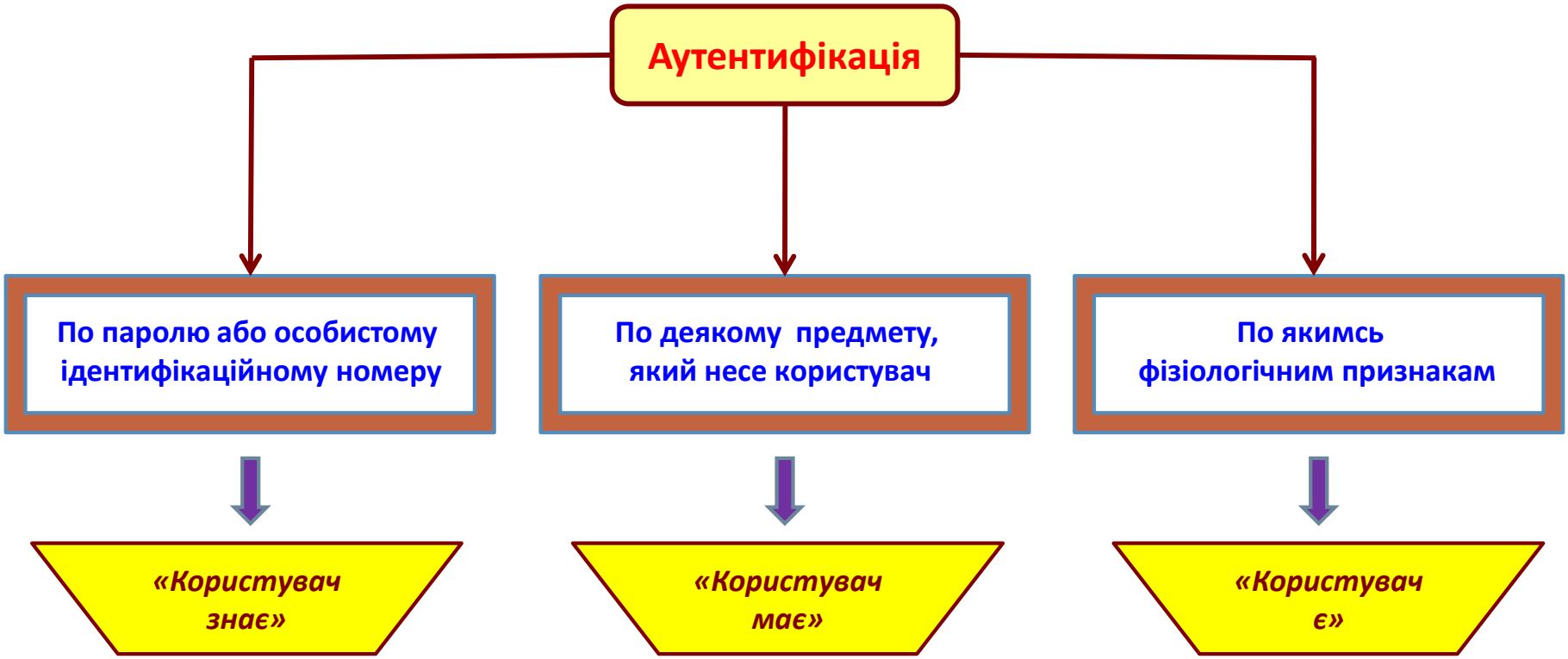
Ідентифікація і аутентифікація користувачів

Визначення

Ідентифікація користувача – встановлення та закріплення за кожним користувачем унікального ідентифікатора у вигляді номера, шифру, коду і т.д. (аналог підпису)

Аутентифікація користувача – перевірка справжності користувача по заявленому ідентифікатору

Ідентифікація і аутентифікація користувачів



Аутентифікація по типу «Користувач знає»

Основа – використання парольної системи доступу

Недолік – більшість паролів легко розкриваються або обходяться

Підвищення надійності:

- ❖зберігання списків паролів користувачів в зашифрованому вигляді;
- ❖використання паролів однократного використання;
- ❖використання для формування паролю вибірки символів;
- ❖використання взаємної аутентифікації користувача та системи (процедура «запит-відповідь)

Необхідність взаємної аутентифікації мережевих процесів підтверджено міжнародними стандартами взаємодії відкритих систем

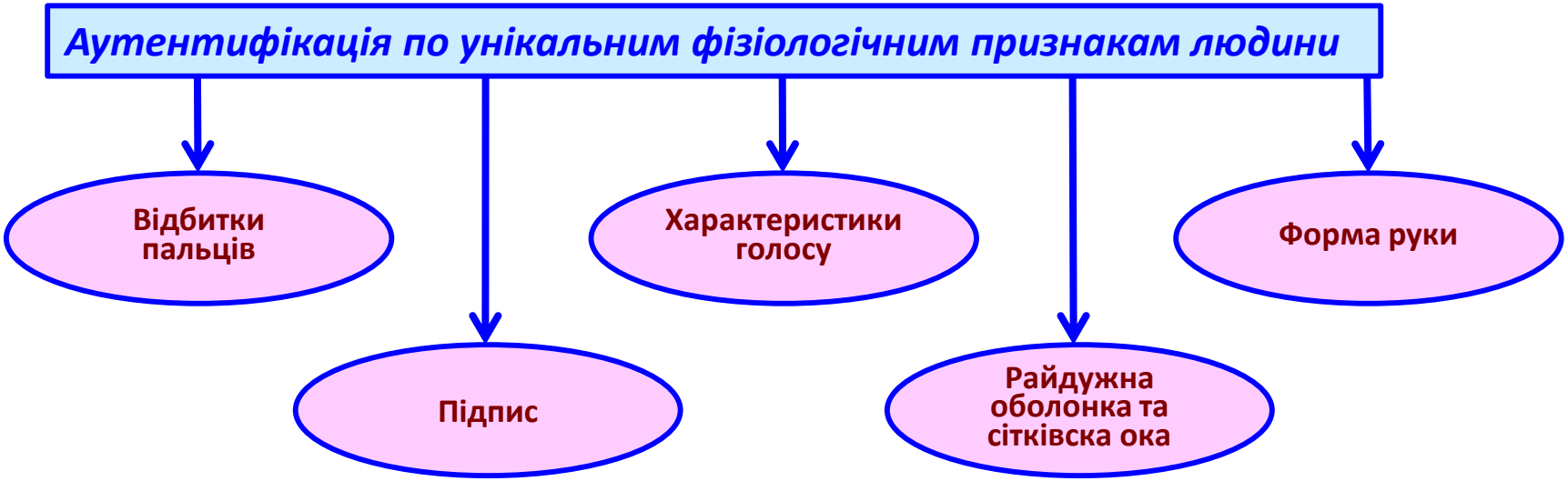
Аутентифікація по типу «користувач має»

Як суб'єкт доступні для користувача Ідентифікаційні картки (s)

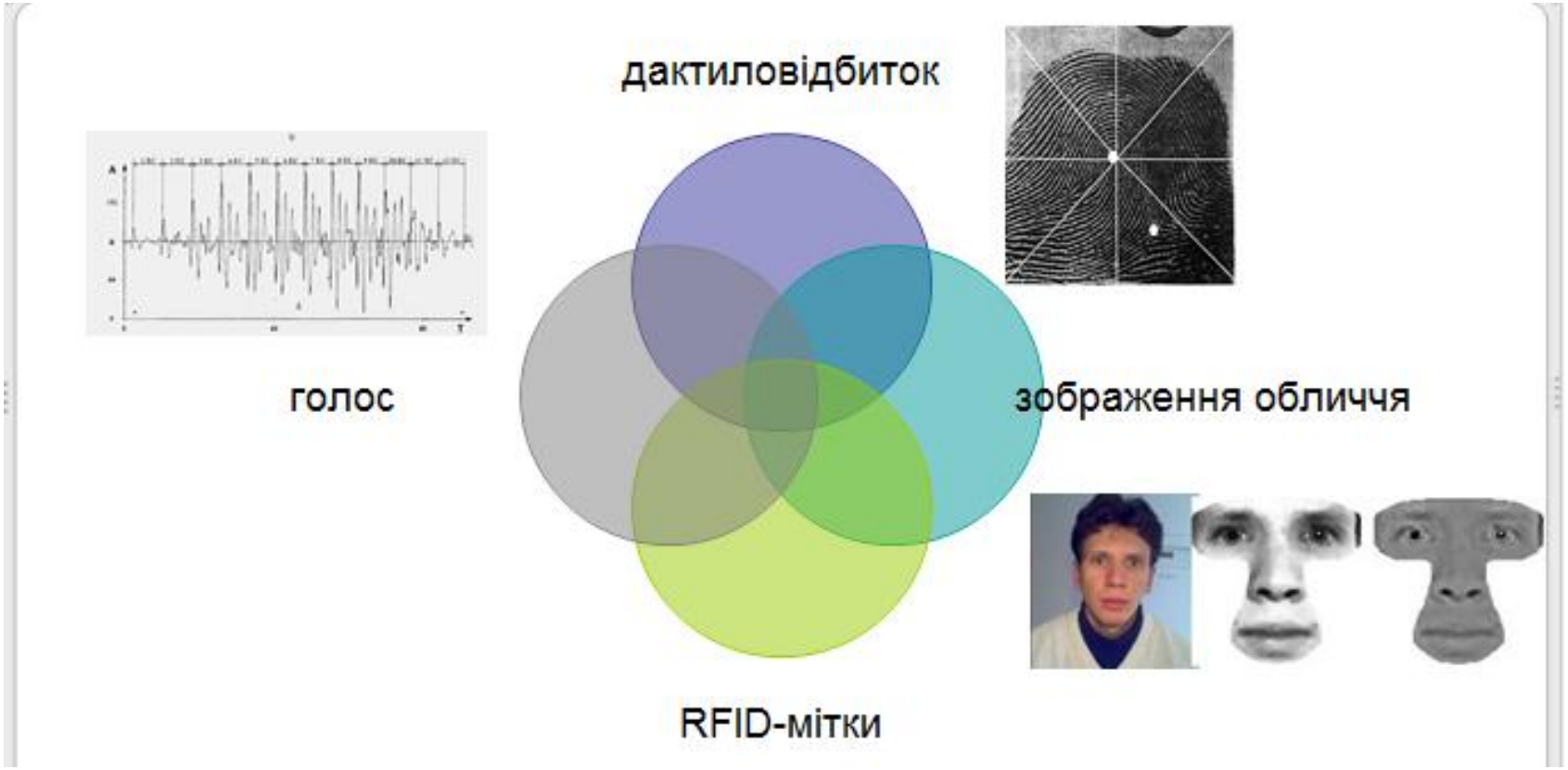
Способи запису та зчитування інформації з карти (можлива комбінація декількох способів):

1. Інформація записується на магнітній полосі
2. В ІК монтується мікросхема, що містить секретний код. Живлення схеми і обмін інформацією з пристроєм розпізнавання здійснюється, як правило, з використанням індуктивного зв'язку
3. На поверхню наноситься покриття, що дозволяє бачити зображення або текст тільки в інфрачервоному або ультразвуковому діапазоні
4. Над текстом або зображенням розміщується рідкокристалічна матриця, прозора тільки при певній орієнтації кристалів
5. На ІК наноситься «мікротекст» або «мікроузор», який не може бути «прочитаний» звичайним обладнанням

Аутентифікація по типу «Користувач є»



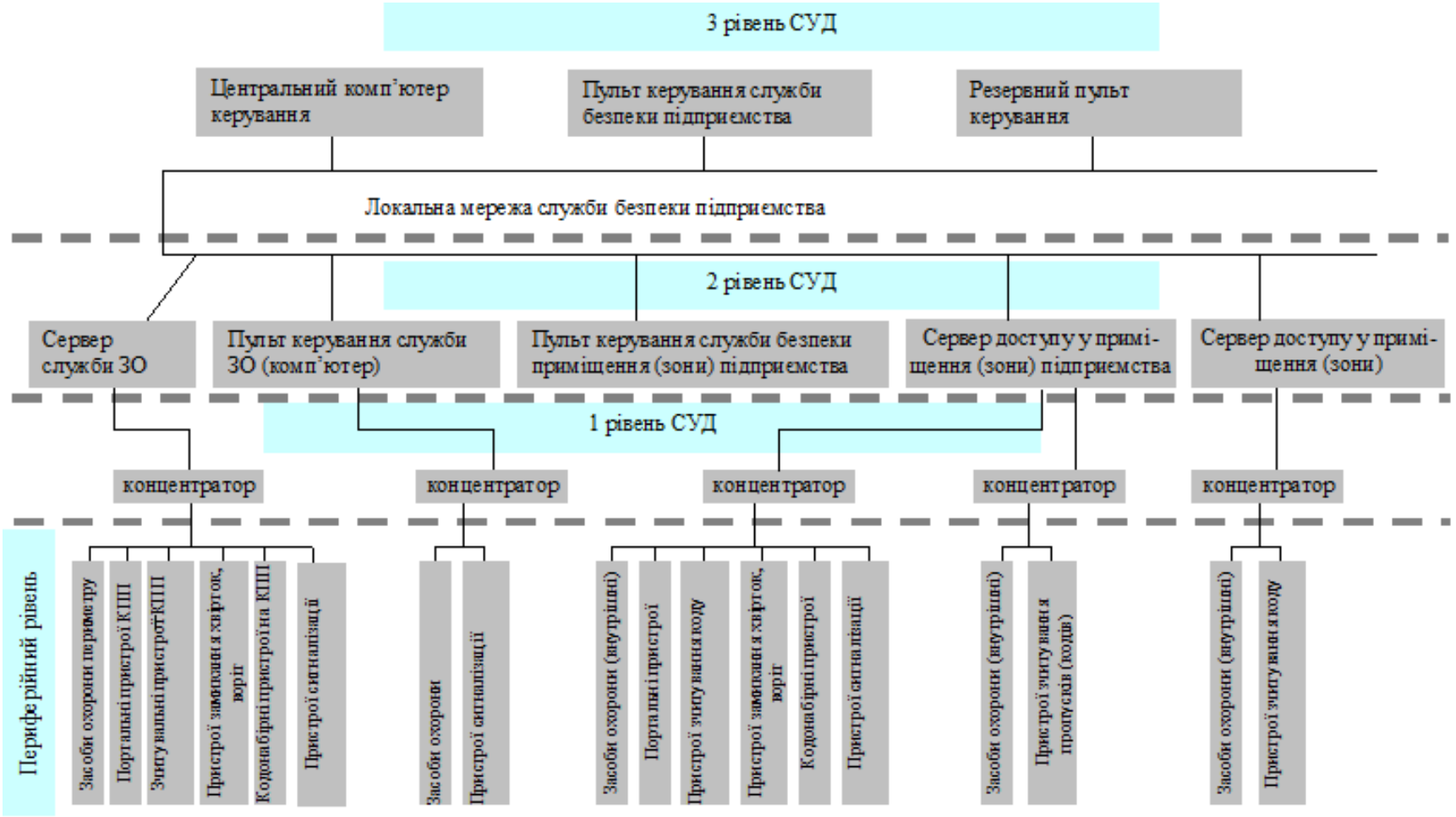
Блок ідентифікації особистості:



Методи контролю доступу

Характеристика елементів систем управління доступом

Елементи систем управління доступом підрозділяються на:
обов'язкові, без яких система непрацездатна,
додаткові, які покращують функціональні і сервісні характеристики системи, а також їх надійність.


3 рівень СУД
Центральний комп'ютер керування
Пульт керування служби безпеки підприємства
Резервний пульт керування
Локальна мережа служби безпеки підприємства
2 рівень СУД
Сервер служби ЗО
Пульт керування служби ЗО (комп'ютер)
Пульт керування служби безпеки приміщення (зони) підприємства
Сервер доступу у приміщення (зони) підприємства
Сервер доступу у приміщення (зони)
1 рівень СУД
концентратор
концентратор
концентратор
концентратор
концентратор
Периферійний рівень
Засоби охорони периметру
Портальні пристрої КПП
Зчитувальні пристрої КПП
Пристрої замикання хвірток, воріт
Кодонабірні пристрої на КПП
Пристрої сигналізації
Засоби охорони
Пристрої сигналізації
Засоби охорони (внутрішні)
Портальні пристрої
Пристрої зчитування коду
Пристрої замикання хвірток, воріт
Кодонабірні пристрої
Пристрої сигналізації
Засоби охорони (внутрішні)
Пристрої зчитування пропусків (кодів)
Засоби охорони (внутрішні)
Пристрої зчитування коду

Висновок за питанням 4

Узагальнивши результати для методів, можна сказати, що для середніх і великих об'єктів, а також для об'єктів із максимальними вимогами безпеки слід використовувати райдужну оболонку як біометричний доступ і, можливо, розпізнавання за венами рук. Для об'єктів із кількістю персоналу до кількох сотень працівників оптимальним буде доступ за відбитками пальців. Системи розпізнавання за 2Б-зображенням обличчя вельми специфічні. Вони потрібні у випадках, коли розпізнавання відбувається без фізичного контакту, але встановити систему контролю за райдужною оболонкою при необхідності ідентифікації людини без її присутності (прихованою камерою або камерою зовнішнього спостереження) неможливо, оскільки це можна зробити лише за малої кількості суб'єктів у базі і невеликого потоку людей, які знімаються на камеру.

Розглянуті методи аутентифікації в разі непідтвердження достовірності повинні здійснювати тимчасову затримку перед обслуговуванням наступного запиту. Це необхідно для зниження загрози підбору ідентифікуючих ознак (особливо паролів) в автоматичному режимі. При цьому всі неуспішні спроби отримання доступу повинні реєструватися з метою забезпечення ефективного контролю безпеки системи

Дякую за увагу!!!