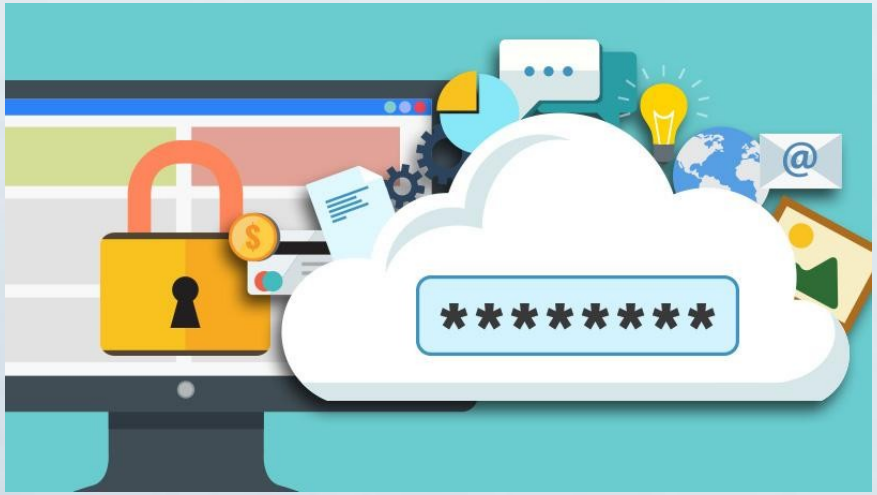
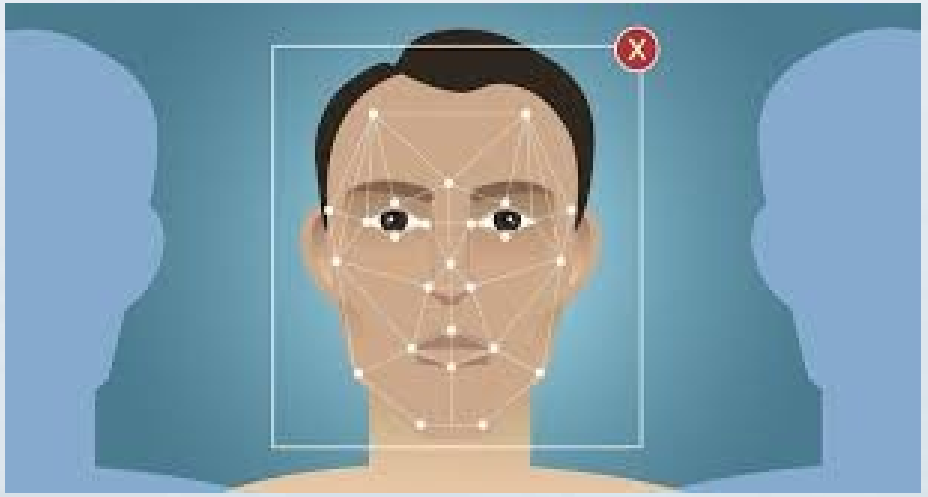
Урок № 40
Тема “Основні захисні механізми. Ідентифікація та аутендифікація користувачів”





Захист інформації від несанкціонованого доступу

Для захисту інформації на рівні **прикладного та системного ПЗ** використовуються:			
системи розмежування доступу до інформації;	системи ідентифікації, аутентифікації;	системи аудиту та моніторингу;	системи антивірусного захисту.

Для захисту інформації на рівні **апаратного забезпечення** використовуються:

апаратні ключі	системи сигналізації	засоби блокування пристроїв та інтерфейс вводу-виводу інформації.

Методи, що забезпечують санкціонованим особам доступ до об'єктів

Авторизація - в інформаційних технологіях це надання певних повноважень особі або групі осіб на виконання деяких дій в системі обробки даних. ("Чи має право виконувати цю діяльність?")

Аутентифікація - це метод незалежного від джерела інформації встановлення автентичності інформації на основі перевірки достовірності її внутрішньої структури ("це той, ким назвався?").

Ідентифікація - це метод порівняння предметів або осіб за їх характеристиками шляхом розпізнавання з предметів або документів, визначення повноважень, пов'язаних з доступом осіб в приміщення, до документів і т.д. ("Це той, ким назвався і має право виконувати цю діяльність?")

Що таке ідентифікація?

Ідентифікація - це процедура розпізнавання суб'єкта за його ідентифікатором (простіше кажучи, це визначення імені, логіна або номера).

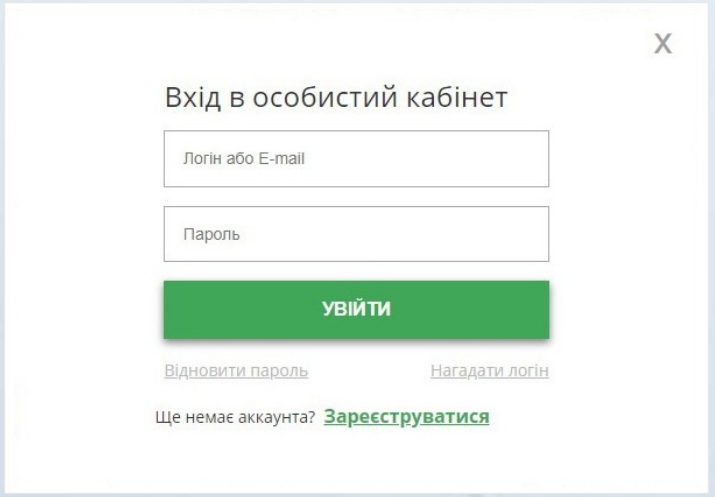
Ідентифікація виконується при спробі увійти в будь-яку систему (наприклад, в операційну систему або в сервіс електронної пошти). Мета ідентифікації — перевірити, чи відомий індивід системі

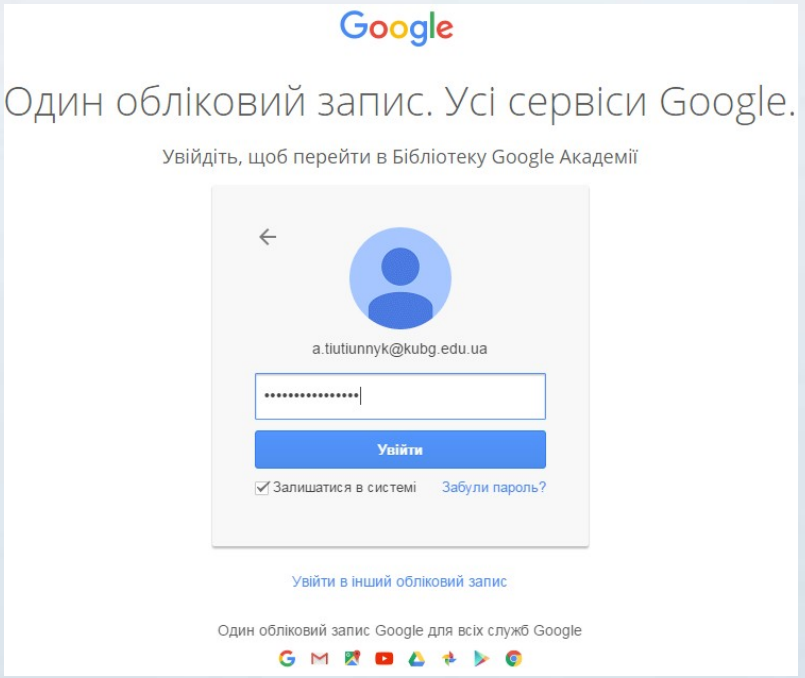
Ідентифікатором може бути:

- номер телефону
- номер паспорта
- e-mail
- номер сторінки в соціальній мережі і т.д.

Що таке ідентифікація?

Коли нам дзвонять з невідомого номера, що ми робимо?
Запитуємо "Хто це", тобто дізнаємося ім'я.
Ім'я в даному випадку і є ідентифікатор, а відповідь вашого співрозмовника - це буде ідентифікація.





Що таке аутентифікація?

- Після ідентифікації проводиться аутентифікація:
- **Аутентифікація (з англ.)** - буквально «встановлення автентичності, справжності».

Аутентифікація — це процес розпізнавання користувача системи і надання йому певних прав та повноважень. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає.

Якщо пояснювати ще простіше, **аутентифікація** – перевірка відповідності імені входу і пароля (введені облікові дані звіряються з даними, що зберігаються в базі даних) .

Аутентифікація схожа, припустимо, з перевіркою на КПП, або коли вахтер порівнює ваше обличчя з фотографією в пропуску, встановлюючи вашу особистість.

Способи аутентифікації

Щоб визначити чиюсь справжність, можна скористатися трьома факторами:

Пароль - то, що ми знаємо (слово, PIN-код, код для замка, графічний ключ)

Пристрій (токен) - то, що ми маємо (пластикова карта, ключ від замка, USB-ключ)

Б а - то, що є частиною нас (відбиток ртрет, сітківка ока)

Виходить, що кожен раз, коли ви вставляєте ключ в замок, вводите пароль або прикладаєте палець до сенсора відбитків пальців, ви проходите аутентифікацію.

Парольна аутентичність

Парольна аутентичність (здійснюється на основі володіння користувачем певної конфіденційної інформації)

- Перевірка автентичності користувача звичайно здійснюється операційною системою.
- Користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль.

Більшість мережевих систем на даний час продовжують використовувати парольну аутентифікацію, оскільки вона простіше і дешевше. *Недоліком* парольної ідентифікації є значна залежність надійності ідентифікації від обраних ними паролів.

Апаратна ідентифікація

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Наприклад, спеціальні електронні ключі.

Найбільш надійними вважаються **смарт-карти** - аналоги звичних багатьом людям банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом і т.д.

Іншим типом ключів є так звані ***токени.*** Ці пристрої мають власну захищену пам’ять і підключаються безпосередньо до одного з портів комп’ютера (USB, LPT).

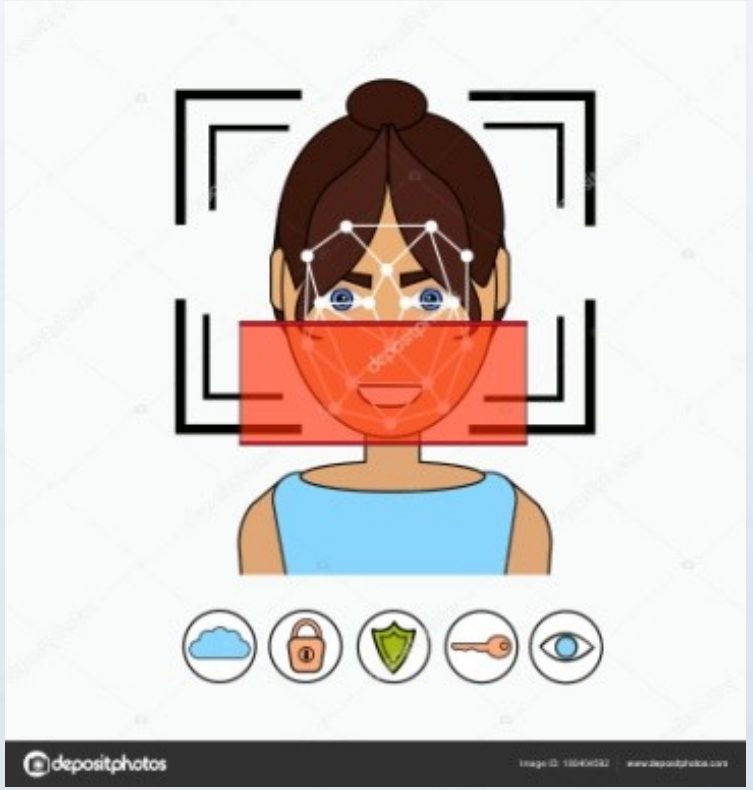
Головною *перевагою* застосування апаратної ідентифікації є досить висока надійність. *Недоліком* апаратної ідентифікації є висока ціна.

Біометрична аутентифікація

Біометрична (електронна) - основана на унікальності певних антропометричних (фізіологічних) характеристик людини.

Системи біометричного захисту використовують унікальні для кожної людини вимірювані характеристики для перевірки особи індивіда.

Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів.

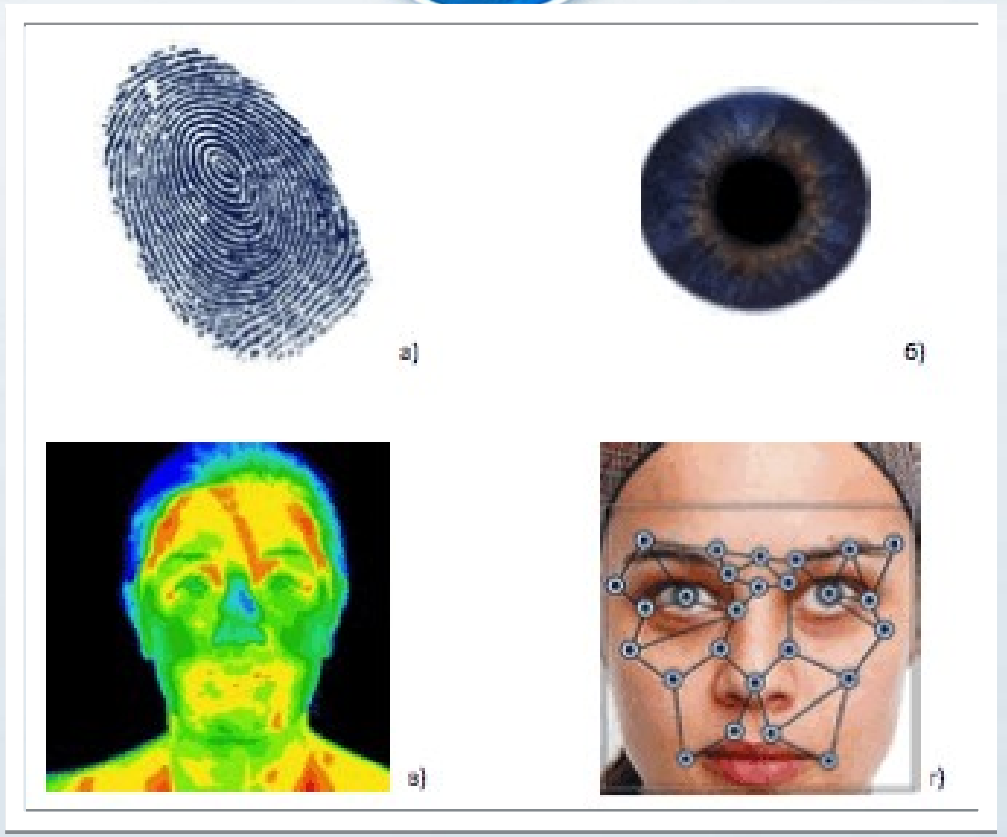


Головною *перевагою* біометричних технологій є найвища надійність. Основним *недоліком* біометричної ідентифікації є вартість устаткування.

Види біометричних аутентифікаторів

До біометричних засобів захисту інформації відносять :

- Параметри голосу.
- Візерунок райдужної оболонки ока і карта сітчатки ока.
- Риси обличчя.
- Форма долоні.
- Відбитки пальців.
- Форма і спосіб підпису.



Біометрична система захисту

Для того, щоб біометрична система змогла надалі аудентифікувати користувача, в ній необхідно спочатку зареєструвати відомості про його ідентифікатори. Під час процедури реєстрації в базу даних системи заносяться характеристики користувачів, необхідні для встановлення їх автентичності.

Біометричні системи

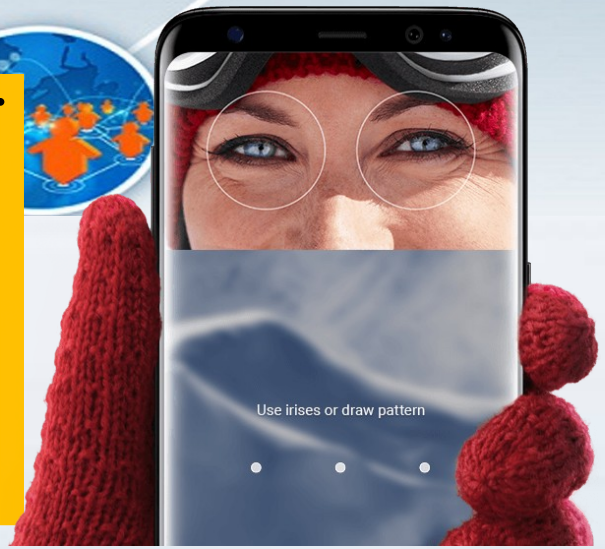
Апаратні засоби: біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютера.

Програмні засоби
Обробляють дані, співвідносять з базою даних і виносять рішення, хто постав перед сканером.

Аутентифікація по райдужній оболонці ока

Райдужна оболонка ока є унікальною для кожної людини біометричної характеристикою.

Зображення ока виділяється з зображення особи і на нього накладається спеціальна маска штрих-кодів. Результатом є матриця, індивідуальна для кожної людини.

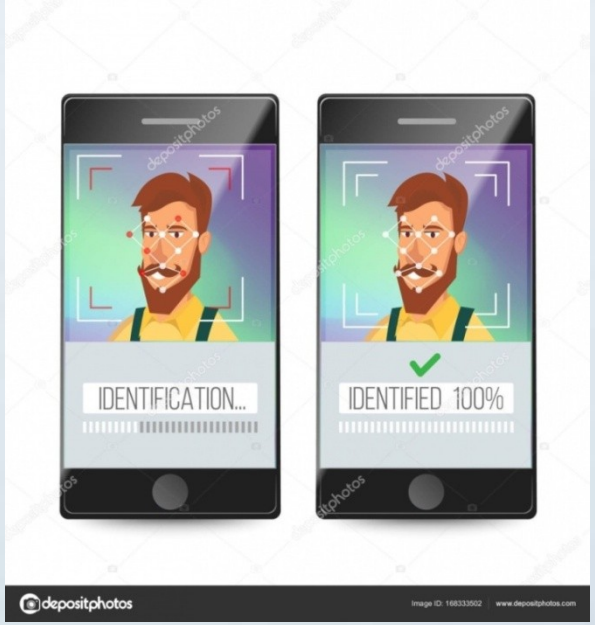


Технологія сканування райдужної оболонки ока була представлена ще в 36-му році минулого століття офтальмологом на ім'я Франк Бурш. Він першим заговорив про унікальність цієї частини організму. Ймовірність збігу цього параметра навіть нижче, ніж у випадку з дактилоскопічними відбитками.

Аутентифікація по зображенню особи

Для ідентифікації особи часто використовуються технології розпізнавання по обличчю. Розпізнавання людини відбувається на відстані. Ідентифікаційні ознаки враховують форму особи, його колір, а також колір волосся. До важливих ознак можна віднести також координати точок особи в місцях, відповідних зміні контрасту (брови, очі, ніс, вуха, рот і овал).

Алгоритм функціонування системи розпізнавання : Зображення особи зчитується звичайною відеокамерою і аналізується. Програмне забезпечення порівнює введений портрет з еталоном, що зберігаються. Важливо також те, що біометричні системи цього класу здатні виконувати безперервну аутентифікацію користувача комп'ютера протягом всього сеансу його роботи



Аутентифікація по долоні руки

У біометриці з метою аудентифікації використовується проста геометрія руки, заснована на аналізі тривимірного зображення кисті руки - розміри і форма, а також деякі інформаційні знаки на тильній стороні руки (образи на згинах між фалангами пальців, візерунки розташування кровоносних судин).

Сканери ідентифікації по долоні руки встановлені в деяких аеропортах, банках і на атомних електростанціях.

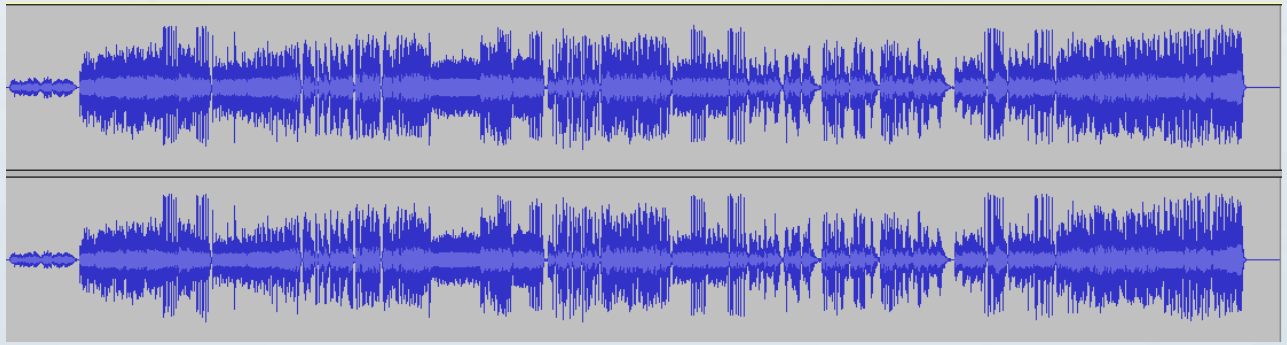
Недоліки: форма кисті руки є параметром, який досить сильно схильний до змін в часі; сканери великого розміру, що веде до подорожчання системи

Аутентифікація за відбитками пальців

- Оптичні сканери зчитування відбитків пальців встановлюються на ноутбуки, миші, клавіатури, флеш-диски, а також застосовуються у вигляді окремих зовнішніх пристроїв і терміналів (наприклад, в аеропортах і банках) .
- Якщо візерунок відбитка пальця не збігається з візерунком допущеного до інформації користувача, то доступ до інформації неможливий

Аутентифікація по характеристикам мови

- Ідентифікація людини по голосу - один з традиційних способів розпізнавання, інтерес до цього методу пов'язаний і з прогнозами впровадження голосових інтерфейсів в операційні системи.
- Існують системи обмеження доступу до інформації на підставі і частотного аналізу мови.



Що таке авторизація?

- Коли визначили ідентифікатор, перевірили справжність, вже можна надати і доступ, тобто, виконати авторизацію.
- **Авторизація** (від санкціонувати — «давати авторитет, вплив, влада») — привласнення прав користувачу на вчинення будь-яких дій в системі.
- **Авторизація** - це визначення прав доступу до ресурсів і управління цим доступом.

Приклади авторизації

- Відкриття двері після провертання ключа в замку
- Доступ до електронної пошти після введення пароля
- Розблокування смартфона після сканування відбитку пальця
- Видача коштів в банку після перевірки паспорта та даних про вашому рахунку

Чим відрізняється авторизація від аутентифікації?

Авторизація - це не те ж саме що ідентифікація та аутентифікація

Ідентифікація - це називання себе системі; процедура розпізнавання суб'єкта за його ідентифікатором та визначення прав об’єкта стосовно системи

Аутентифікація - це встановлення відповідності особи, призначеному ним самим ідентифікатору (доказ об’єктом своєї дійсності системі, процес упізнавання особи системою)

Авторизація – це надання цій особі можливостей у відповідність до покладених йому прав, тобто наданні користувачеві доступу до певних ресурсів залежно від його особи, тобто після аутентифікації .

Приклад

Ви заходите в свою квартиру відкриваючи замок ключем. І якщо двері таки відчинилися, то значить ви успішно пройшли аутентифікацію.

- **Ключ від замку** - це ваш ідентифікатор (вставили і повернули - пройшли ідентифікацію). У комп'ютерному світі це аналог того, що ви повідомили системі своє ім'я (нік, нікнейм).
- **Процес відкривання** (збіги ключа і замка) - це аутентифікація. У комп'ютерному світі - це аналог проходження етапу перевірки автентичності (перевірка введеного пароля).
- **Відкривання дверей і вхід в квартиру** - це вже авторизація (отримання доступу). В мережі - це вхід на сайт, сервіс, програму або додаток.

Взаємозв'язок ідентифікації, аутентифікації і авторизації

- Напевно, ви вже здогадалися, що всі три процедури взаємопов'язані:
- Спочатку визначають ім'я (логін або номер) - ідентифікація
- Потім перевіряють пароль (ключ або відбиток пальця) - аутентифікація і в кінці надають доступ - авторизація

Ідентифікація	***Аутентифікація***	***Авторизація***
Визначення	***Перевірка***	***Доступ***
Хто там?	*Чим доведеш?*	*Відкриваю!*

Обговорюємо

1. Вкажіть переваги і недоліки біометричної системи захисту даних
2. Чому біометричні системи захисту інформації є найбільш надійними?
3. Як ви думаєте, які недоліки ідентифікації людей за характеристиками голосу? Наведіть приклади застосування даного методу ідентифікації.
4. Чому райдужка краще за інших біометрічних технологій?
5. Вкажіть проблеми ідентифікації особистості по обличчю.

Працюємо в парах

Які умови дозволяють не встановлювати пароль на комп'ютері?

Діємо

Завдання 1

Ознайомитися з основними правилами створення надійного пароля на сайті https://cyberukraine.in.ua/ (#ПарольГраєРоль)

Завдання 2

Здійсніть перевірку пароля на сайті Проверка пароля - Zillya! https://zillya.ua/ru/check-password

Завдання додому:

- Опрацювати конспект , знайти означення та пояснити термін “двоетапна аутентифікація»
- За матеріалами Інтернету підготуйте бюлетень “Як придумати надійний пароль і де його зберігати”. Розмісіть роботу на Google-диску, наддайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів