Урок № 7.

Тема уроку: Інструктаж з БЖД. Ідентифікація та аутентифікація користувачів. Розмежування доступу зареєстрованих користувачів до ресурсів автоматизованих систем.

Сьогодні ти ознайомишся з методами, що забезпечують санкціонованим особам доступ до об'єктів АС, дізнаємося, що таке ідентифікація, аутентифікація, авторизація і в чому різниця між цими поняттями.

Правила поведінки за комп'ютером:

Пам’ятай:

- Робоче місце за комп'ютером потрібно тримати у порядку.
- Не клади зайвих речей на стіл біля комп'ютера.
- Прибирай пил з комп'ютера спеціальною ганчіркою, коли він вимкнений.

Виконуй:

- Слідкуй за осанкою (спина повинна бути прямою).
- Очі мають бути на відстані 50 – 60 см від екрану монітору.
- Кожні 30 хвилин роби перерву в своїй роботі.

Одним з напрямків захисту інформації в інформаційних системах є **технічний захист інформації (ТЗІ)**. У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захист інформації від витоку технічними каналами.

Під *НСД* мається на увазі *доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу*. Під технічними каналами розуміються канали сторонніх електромагнітних випромінювань і наведень, акустичні канали, оптичні канали й ін.

Захист від НСД може здійснюватися в різних складових інформаційної системи: на прикладному і програмному рівні, на апаратному та на мережевому рівні.

Для захисту інформації на рівні **прикладного** та системного ПЗ використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації;
- 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.

Розглянемо методи, що забезпечують санкціонованим особам доступ до об'єктів та інформаційних ресурсів. До них відносять аутентифікацію та ідентифікацію користувачів.

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

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?") За допомогою авторизації встановлюються і реалізуються права доступу до ресурсів.

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?")

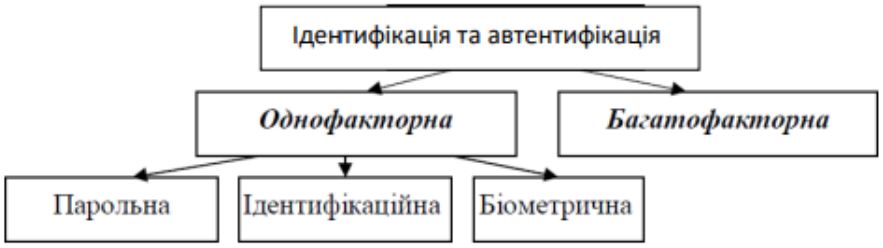

Рис.1.1. Система технологій ідентифікації та автентифікації

Способи Автентифікації:

✓ Парольна (здійснюється на основі володіння користувачем певної конфіденційної інформації);

✓ Біометрична (основана на унікальності певних антропометричних характеристик людини).

Щоб визначити чиюсь справжність, можна скористатися трьома факторами:

• Пароль - то, що ми знаємо (слово, PIN-код, код для замка, графічний ключ): об'єкт може продемонструвати знання якого-небудь загального для сторін секрету;

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

• Біометрика - то, що є частиною нас (відбиток пальця, портрет, сітківка ока).

Біометрична аутентифікація.

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.

До біометричних засобів захисту інформації відносять системи аутентифікації за:

✓ Параметрами голосу.

✓ Візерунком райдужної оболонки ока і карта сітчатки ока.

✓ Рисами обличчя.

✓ Формою долоні.

✓ Відбитками пальців.

✓ Формою і способом підпису.

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення, наприклад: