**Питання 2** :

Метою введення категорювання є використання і облік всіх факторів, котрі дозволяють, не допускаючи витоку інформації, спростити і подешевіти захист ОІД та ТЗПІ, котрі входять до їх складу. Категорування встановлює диференційовані норми на рівні маскуючих завад, на граничне відношення сигнал/завада, на величини НС в КВ. Головними факторами, котрі визначають конкретні вимоги при розробці категорованих норм на первинні параметри, є:

- характер оброблюваної інформації;  
- вірогідність присутності паразитних КВ;  
- умови розміщення об’єктів, котрі підлягають захисту.  
З аналізу властивостей оброблюваної інформації, її важливості, ступеня секретності, детальності зображень при їх передаванні і т.д., визначаються допустимі вірогідності помилок при перехопленні НС і гранично допустимі відношення сигнал/завада.

Під **технічним каналом витоку інформації (ТКВІ)** розуміють сукупність об’єкту розвідки, технічного засобу розвідки (ТЗР), за допомогою котрого отримується інформація про цей об’єкт, та фізичне середовище, по котрій розповсюджується інформаційний сигнал. По суті, під ТКВІ розуміють **спосіб отримання за допомогою ТЗР розвідувальної інформації** про об’єкт розвідки. При цьому форма представлення інформації може бути довільна.

За фізичним принципом технічні канали витоку інформації можуть бути класифіковані за групами:

- акустичні (включаючи акустоперетворювальні);  
- візуально-оптичні (спостереження, фотографування і т.п.);  
- електромагнітні (а також з розподілом на електричні і магнітні окремо);  
- матеріальні (папір, фото, магнітні носії, відходи різного характеру та ін.).

За способом отримання інформації класифікації можуть підлягати методи несанкціонованого доступу до неї:

- акустичний контроль приміщень, автомобіля, людини, контроль та прослуховуван-ня телефонних каналів зв’язку, перехоплення факсових та модемних сеансів зв’язку;

- перехоплення комп’ютерної інформації (у тому числі радіовипромінювання комп’юте- ра), несанкціонований доступ до бази даних;

- прихована фото- та відеоз’омка з застосуванням спеціальної оптики;  
- візуальне спостереження за об’єктом;  
- несанкціоноване ознайомлення з документами;  
- аналітичне обстеження процесу діяльності підприємства, його корисного продукту та

відходів, в тому числі хімічний аналіз зовнішніх викидів;  
- аналітичне ознайомлення з публікаціями та рекламними матеріалами підприємства;

- несанкціоноване отримання інформації про особу шляхом підкупу та шантажу службовців, оточення та родичів.

**Основними об’єктами захисту інформації є**:  
**1**- інформаційні ресурси, котрі несуть у собі відомості, що можуть відноситись до

державної таємниці та конфіденційної інформації:  
**2**- системи та засоби інформатизації (засоби обчислювальної техніки, інформаційно-

обчислювальні комплекси, мережі та системи); програмні засоби (операційні системи, системи керування базами даних та інше загальносистемне та прикладне програмне забезпечення), автоматизовані системи керування, системи зв’язку та передачі даних, технічні засоби отримання, передавання та обробки інформації з обмеженим доступом (звукозапис, звукопідсилення, звукосупроводження, переговорні та телевізійні пристрої, засоби тиражування та виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та змістовної інформації), їх інформативні фізичні поля. Ці засоби часто називають **технічними засобами прийому, обробки, зберігання та передавання інформації (ТЗПІ).**

**3** - технічні засоби і системи, котрі не відносять до засобів та систем автоматизації (ТЗПІ), але розташовані в приміщеннях де оброблюється таємна і конфіденційна інформація. Такі засоби і системи називають **допоміжними технічними засобами і системами (ДТЗС)**. До них відносяться технічні засоби відкритого телефонного, гучномовного зв’язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, системи часофікації, енергопобутові прилади і т.д., а також самі приміщення, де оброблюється інформація обмеженого поширення.

**Питання 1 :**