1. Поєднання технічних та організаційних заходів для захисту ОІД;

Інформація з обмеженим доступом захищається за допомогою деяких організаційних заходів таких як розділ такої інформації за правовим режимом на конфіденційну та таємну(Держтаємниця або прередбачена іншим законом таємниця)та категоріювання норм .

1 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює

інформація що складає відомості з грифом (ОВ);

2 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює

інформація що складає відомості з грифом (ЦТ);

3 категорія – встановлюється для об’єктів інформаційної діяльності (ОІД) де циркулює

інформація що складає «таємні» відомості.

Також використовуються технічні засоби для захисту ОІД

Основними об’єктами захисту інформації є інформаційні ресурси, котрі несуть у собі відомості, що можуть відноситись до державної таємниці та конфіденційної інформації ,

системи та засоби інформатизації , програмні засоби , автоматизовані системи керування, системи зв’язку та передачі даних. Їх також наз-ть технічними засобами прийому інформації (ТЗПІ) та технічні засоби і системи, котрі не відносять до засобів та систем автоматизації (ТЗПІ) але розташовані в приміщеннях де оброблюється таємна і конфіденційна інформація.

2. Захист каналів зв’язку;

3. Активні засоби. Постановка завад. Види завадових сигналів. Приклади приладів та їх характеристики;

4. Віброакустичне маскування — активний метод захисту, який використовується для зниження відношення сигнал\завада. Найбільш ефективний для захисту від витоку по прямому акустичному каналу.

Для формування акустичних завад використовують спец генератори з кінцевим пристроєм — гучномовцем або вібраційним випромінювачем. Найчастіше використовують генератор шуму. В якості ел-та формування шумових сигналів вик-ють вакуумні, газорозрядні, напівпроводникові та інші ел-ти , а також цифрові пристрої.