1. Об’єкти захисту інформації (ЗІ) та технічні канали її витоку;

Основними об’єктами захисту інформації є:

1. Інформація з обмеженим доступом.
2. ТЗПІ -технічні засоби передавання/приймання інформації .
3. ДТЗС - допоміжні технічні засоби та системи (буль-які технічні засоби, які розташовані поруч із ТЗПІ, але не здійснюють обробку ІзОД).
4. Виділені приміщення (тільки для акустичних та віброакустичних КВ).

Технічний канал витоку – середовище, об’єкт розвідки і засіб, за допомогою яких можна отримати інформацію про цей об’єкт.

Технічні канали її витоку (фізичний принцип):

* акустичні;
* візуально-оптичні;
* електромагнітні;
* матеріальні

2. Захист каналів зв’язку;

-

3. Пасивні та активні методи ЗІ;

Цілі пасивних методів:

- ослаблення інформаційних сигналів ТЗПІ до рівнів не помітних для засобів розвідки на шумовому фоні;

- ослаблення побічних електромагнітних випромінювань ТЗПІ на сторонні провідники та з’єднувальні лінії ДТЗС, що виходять за межі зони що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- виключення (ослаблення) просочування інформаційних сигналів ТЗПІ до мереж живлення що виходять за межі зони що контролюється до рівнів, не помітних для засобів розвідки на шумовому фоні;

Активні методи захисту спрямовані на:

- створення маскуючих електромагнітних завад з ціллю зменшення відношення сигнал/завада на межі зони що контролюється до рівнів, не помітних засобам розвідки на шумовому фоні;

- створення маскуючих електромагнітних завад у сторонніх провідниках та з’єднувальних лініях ДТЗС з ціллю зменшення відношення сигнал/завада на межі зони, що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

4. Принципи витоку інформації по телефонних каналах зв’язку.

Від’єднанння телефонних апаратів або встановлених телефонних закладок від АТЛ при веденні в приміщенні конфіденційних розмов є найефективнішим методом захисту інформації. Найпростіший спосіб реалізації цього методу захисту полягає у встановленні в корпусі телефонного апарата або телефонної лінії звичайного тумблера, що вмикається і вимикається вручну. Зручнішим в експлуатації є встановлення в телефонній лінії спеціального пристрою захисту – електронного комутатора, який автоматично (без участі оператора) від’єднує телефонний апарат від лінії, коли покладена слухавка.

Дія активних засобів полягає у накладанні захисного шуму на небезпечний сигнал. Розрізняють низькочастотні маскувальні сигнали в діапазоні від 100 Гц до 10 кГц та високочастотні широкосмугові – від 20 кГц до 30 МГц. Внаслідок ефекту маскування не вдається засобами технічної розвідки виділити інформативні параметри сигналів витоку. Активні засоби блокування технічних каналів витоку абонентськими телефонними лініями часто називають засобами лінійного зашумлення, а їхня дія ґрунтується на створенні і «закачуванні» в лінію при покладеній трубці шумового сигналу. Генератори шуму ГШ під’єднуються в розрив телефонної лінії і монтуються, як правило, безпосередньо в корпусі телефонного апарата (рис. 6). Шумовий сигнал подається в лінію в режимі, коли телефонний апарат не використовується (трубка покладена). При піднятті трубки телефонного апарата подавання в лінію шумового сигналу припиняється.

До широко вживаних пасивних методів захисту відносяться: обмеження чи фільтрація небезпечних сигналів за допомогою пристроїв «Скеля–1Ф», «ФЗП–103–2»; захист мовної інформації від витоку абонентськими телефонними лініями внаслідок акустоелектричного перетворення в телефонному апараті у режимі «очікування виклику» — «Рікас–1», «Рікас–2», «Базальт–3»; відключення з використанням пристроїв «Скеля–1К», TS2, «Р5055» фірми «Ренар» джерел таких сигналів — телефонного апарату — за умови покладеної телефонної трубки. Визначити наявність несанкціонованого підключення до каналу зв’язку можна з використанням індикаторних пристроїв «Скеля–1А», «Рікас–4», що фіксують зміну параметрів телефонної лінії, порівняно з відповідними їх значеннями для «чистої» лінії (контроль сталої напруги живлення, струму короткого замикання, навантажувальної характеристики, зміни рівня сигналу на вході приймача контролю у момент підняття трубки, а також низькочастотних сигналів телефонних закладок та сигналів високочастотного нав’язування і накачки, сигналізатор обриву ТЛ тощо)

Скремблер — это малогабаритное устройство, предназначенное для изменения речевого сообщения при передаче и его восстановления при приеме с помощью определенных алгоритмов и ключей. В результате аналоговых криптографических преобразований телефонных сообщений по кабелю или радиоканалу речь становится неузнаваемой и неразборчивой или превращается просто в низкочастотный шум (в зависимости от типа скремблера). Сложность устройства определяет уровень защищенности передаваемой информации.