1. Поєднання технічних та організаційних заходів для захисту ОІД;

Захист інформації з обмеженим доступом при автономному використанні на ОІД пристроїв обробки інформації здійснюється шляхом створення комплексу ТЗІ, який складається із сукупності:

- організаційних заходів захисту від несанкціонованих дій з інформацією (для захисту конфіденційної інформації, що є власністю держави або вимога щодо захисту якої встановлена законом);

- організаційних заходів захисту від несанкціонованих дій з інформацією та технічних засобів захисту інформації від витоку технічними каналами за наявності можливості створення таких каналів (для захисту інформації, що становить державну таємницю).

У залежності від умов розташування об’єктів встановлені категорії норм за визначеними

для кожного виду технічних засобів (ТЗ) каналах витоку інформації:

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.

2. Засоби захисту телефонних ліній зв’язку.

Для захисту телефонних апаратів від “високочастотного нав’язування” застосовуються загороджувальні фільтри, що встановлюються між телефонним апаратом і АТЛ. Амплітудно-частотна характеристика таких фільтрів має забезпечувати “прозорість” в інтервалі каналу тональної частоти (300 – 3400 Гц) і якомога більше згасання сигналів на частотах позазвукового діапазону.

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.