1. **Поєднання технічних та організаційних заходів для захисту ОІД**

Організаційні заходи – це заходи до захисту інформації, проведення котрих не потребує використання спеціально розроблених технічних засобів.

До основних організаційних заходів відносяться:

- залучення до проведення робіт для захисту інформації організацій, що мають ліцензію на діяльність в області ТЗІ, що надається відповідними органами;

- категоріювання і атестація об’єктів ТЗПІ і виділених для проведення секретних

заходів приміщень (далі **виділених приміщень**) до виконання вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідного ступеня секретності;

- використання на об’єкті сертифікованих ТЗПІ і ДТЗС;

- встановлення контрольованої зони навкіл об’єкту;

- залучення до роботи по будуванню, реконструкції об’єктів ТЗПІ, монтуванню апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

- організація контролю та обмеження доступу на об’єкти ТЗПІ та у виділені приміщення;

- введення територіальних, частотних, енергетичних, просторових і часових обмежень в режимах використання технічних засобів, що підлягають захисту;

- відключення, на період проведення секретних заходів технічних засобів, що мають елементи з якостями електроакустичних перетворювачів, від ліній зв’язку і т.і.;

***+: можливо побудувати ідеальну систем захисту***

***-: буль-яка інстррукція не змінює фізичних законів***

Технічні заходи – це заходи з захисту інформації, котрі передбачають використання спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи направлені на зачинення каналів витоку інформації за рахунок ослаблення рівня інформаційних сигналів , або зменшення співвідношення сигнал/завада в місцях можливого розміщення засобів розвідки або їх датчиків до рівнів, унеможливлюючих виділення інформаційних сигналів засобами розвідки, і провадяться з використанням активних та пасивних засобів.

До технічних заходів з використанням **пасивних засобів** відносяться:

\*контроль та обмеження доступу на об’єкти ТЗПІ та виділені приміщення:

- встановлення на об’єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу.

\*локалізація випромінювання:

- екранування ТЗПІ та з’єднувальних ліній;

- заземлення ТЗПІ і екранів їх з’єднувальних ліній;

- звукоізолювання виділених приміщень.

\*розв’язування інформаційних сигналів:

- встановлення спеціальних засобів захисту типу “Граніт” у допоміжних технічних засобах та системах, що мають “мікрофонний ефект” і таких, що мають вихід за межі КЗ;

- встановлення спеціальних діелектричних вставок в оплітення кабелів електроживлення, труб систем опалення, водозабезпечення і каналізації, що мають вихід за межі КЗ;

- встановлення автономних або стабілізованих пристроїв електроживлення ТЗПІ (наприклад, мотор-генераторів);

- встановлення в мережах електроживлення ТЗПІ, а також в лініях освітлювальної

та розеточної мережі виділених приміщень завадопоглинаючих фільтрів типу ФП.

То технічних заходів з використанням активних засобів відносяться:

\*просторове зашумлення:

- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад (при умові виявлення та з’ясування частоти випромінювання закладного пристрою або ПЕМВ ТЗПІ) з використанням засобів створення прицільної завади;

- створення акустичних і вібраційних завад з використанням генераторів акустичного шуму – шумотронів.

- придушення диктофонів в режимі запису з використанням придушуючих пристроїв.

\*лінійне зашумлення:

- лінійне зашумлення ліній електроживлення;

- лінійне зашумлення сторонніх дротів та з’єднувальних ліній ДТЗС, що виходять за межі КЗ.

\*знешкодження закладних пристроїв:

- знешкодження закладних пристроїв, що підключені до лінії, з використанням спеціальних генераторів імпульсів (випалювачів “жучків”).

Спеціальні дослідження виділених приміщень та об’єктів ТЗПІ провадяться шляхом іх візуального огляду без залучення технічних засобів.

Спеціальна перевірка провадиться з використанням технічних засобів. При цьому здійснюється:

\**виявлення закладних пристроїв з використанням пасивних засобів:*

- встановлення засобів і систем виявлення лазерного випромінювання (підсвітлення) віконних стекол;

- встановлення стаціонарних виявителів диктофонів;

- розшук закладних пристроїв з використанням індикаторів поля, інтерсепторів, частотомірів, скануючих приймачів та програмно-апаратних комплексів контролю.

- організація радіоконтролю (постійно, або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТЗПІ.

\**виявлення закладних пристроїв з використанням активних засобів*:

- спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;

- спеціальна перевірка виділених приміщень, ТЗПІ та допоміжних технічних засобів з використанням рентгенівських комплексів.

1. **Засоби захисту телефонних ліній зв’язку.**

Безпосередньо в телефонному апараті варто контролювати і захищати дзвінковий і мікрофонний ланцюги. Як відомо, акустичні коливання, викликані розмовами в приміщеннях, де є телефонні апарати, через маятник дзвоника впливають на якір електромагнітного реле, мікроколивання якого, у свою чергу, викликають мікроструми в котушках і які можуть бути записані при підключенні до абонентської лінії.

Для захисту телефонних апаратів як правило використовуються пристрої типу “Экран”, “Гранит-8”, “Корунд”, “Грань-300” і т. ін. Найбільш ефективним методом захисту інформації при веденні в приміщенні конфіденційних переговорів є відключення телефонних апаратів від лінії. До типових пристроїв, що реалізують даний метод відноситься “Барьер-МІ”.

Активним методом захисту від витікання інформації по електроакустичному каналу передбачається зашумлення телефонної лінії. Шумовий сигнал подається в лінію, коли трубка покладена, а при піднятті трубки телефонного апарата подача шумового сигналу припиняється. До таких засобів відносяться пристрої МП-1А (захист аналогових телефонних апаратів) та МП-1ЦП-1А (захист цифрових телефонних апаратів).

Велику можливість доступу до інформації, що циркулює по телефонній мережі, дає лінія телефонного зв’язку, оскільки вона може також використовуватись як джерело живлення акустичних закладок, а також для передачі інформації, отриманої цими закладками.

Для захисту телефонних ліній використовуються як прості пристрої, що реалізують один з методів захисту, так і складні, що забезпечують комплексний захист ліній різними методами. На вітчизняному ринку є велика кількість різноманітних засобів захисту, серед яких “БР 17/Т”, “КТЛ-3”, “КТЛ-400”, “Ком-3”, “Прокруст” (ПТЗ-ООЗ), “Прокруст-2000”, “Гром-ЗИ-6”, “Протон” та інші. Для виведення з ладу засобів несанкціонованого підключення до телефонної лінії використовуються пристрої типу “ПТЛ- 1500”, “КС-1300”, “КС-1303”, “Кобра” та ін. Разом із засобами активного захисту використовуються пристрої, що дозволяють контролювати деякі параметри телефонних ліній та встановлювати факт несанкціонованого підключення до них. Наприклад, контролери телефонних ліній “КТЛ-2”, “КТЛ-31” ТА “КТЛ-400” за декілька хвилин дозволяють виявити закладки із живленням від телефонної лінії незалежно від способу, місця та часу їх підключення.

Простим методом захисту телефонних ліній є метод **обмеження шкідливих сигналів**. Метод грунтується на нелінійності вольт-амперної характеристики напівпровідників (частіше діода) при малих значеннях струмів та напруг. Зустрічно-паралельне підключення двох діодів послідовно до дзвінково-визовного пристрою телефону дозволяє створити умови, перешкоджаючі проникненню у дзвінково-визовний пристрій сигналів з малою амплітудою, або від генераторів з великим внутрішнім опором.

**Фільтрація небезпечних сигналів** використовується для захисту телефонних апаратів від “ВЧ нав’язування”. Як правило, для захисту телефонних апаратів використовують пристрої, котрі об’єднують фільтр та обмежувач. Це пристрої типу “Экран”, “Гранит-8” і “Гранит-10”, “Корунд”, “Грань-300” та ін.

**Відключення апарату від лінії** при проведенні конфіденційних переговорів є найбільш радикальним методом захисту. Для автоматичного відключення при покладанні слухавки використовують виріб типу “Барьер-М1” . До його складу входять:

- електронний комутатор;

- схема аналізу стану телефонного апарату, наявність сигналів виклику та управління комутатором;

- схема захисту телефонного апарата від високовольтних імпульсів;

Пристрій працює у режимах: черговому, передавання сигналів виклику та робочому. В режимі чергування апарат розв’язує лінію з опором 20 мОм. Напруга на виході пристрою у черговому прийомі складає 5…7 В.

До сертифікованих засобів лінійного зашумлення відносяться пристрої МП-1А (захист аналогових телефонних апаратів) та МП-1ЦП-1А (захист числових телефонних апаратів) та ін.

Низка активних методів захисту телефонних ліній складає функціональні можливості сукупних можливостей трьох пристроїв захисту, таких як “Прокруст”, “Протон”, “Цикада-М”. Основні функціональні характеристики цих пристроїв можна звести до такої таблиці

Окрім зазначених пристроїв широко використовують пристрої моделей “Sel SP-17/P”, “Гром-3И-6”, “Кзот-06” та інші. Ефективність пристроїв активного захисту телефонних ліній оцінюють за їх спроможністю протистояти тим чи іншим методам інформаційної атаки.