***1. Канали витоку інформації ОІД та ТЗПІ;***

В якості елементів каналів витоку інформації найбільший інтерес

представляють ТЗПІ і ДТЗС, котрі мають вихід за межу зони що

контролюється (КЗ). КЗ це зона, де виключена можливість появи суб’єктів

чи транспортних засобів, котрі не мають постійних чи часових перепусток.

Окрім з’єднувальних ліній ТЗПІ і ДТЗС за межу КЗ можуть виходити

дроти та кабелі, котрі не мають до них відношення, але котрі проходять

скрізь приміщення, де встановлені технічні засоби, а також металеві труби

опалення, водопостачання та інші струмопровідні металоконструкції. Такі

дроти, кабелі і струмопровідні елементи називають сторонніми

провідниками.

Зона, де є можливим перехват (за допомогою розвідувального приймача)

побічних електромагнітних хвиль та подальша розшифровка інформації,

котру вони несуть, (це є зона, в межах котрої відношення “сигнал/завада”

вище за декотре нормоване значення) називається (небезпечною) зоною 2.

Простір навкруги ТЗПІ, в межах котрого на випадкових антенах

наводяться інформаційні сигнали вищі за нормований рівень, називають

(небезпечною) зоною 1.

Випадковою антеною є мережа ДТЗС чи сторонні провідники, здатні

приймати побічні електромагнітні сигнали. Випадкові антени можуть бути

зосередженими та розосередженими.

Зосереджена випадкова антена представляє собою компактний технічний

засіб, наприклад телефонний апарат, гучномовець радіотрансляційної

мережі і т. п. До розосереджених випадкових антен відносять випадкові

антени з зосередженими параметрами: кабелі, дроти, металеві труби та

інші струмопровідні комунікації.

Перехоплення інформації, що обробляється на об’єктах ТЗПІ,

здійснюється по технічних каналах.

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.

Сигнали є матеріальними носіями інформації. За своєю фізичною

природою сигнали можуть бути електричними, електромагнітними,

акустичними.

В залежності від природи сигнали поширюються у визначених фізичних

середовищах. Середовищем поширення можуть бути газові, рідинні,

тверді середовища. Наприклад, повітря, конструкції будівель, струмоведучі

кабелі та дроти, земляний грунт тощо.

Для прийому та вимірювання параметрів сигналів використовують

технічні засоби розвідки (ТЗР).

За фізичним принципом технічні канали витоку інформації можуть бути

класифіковані за групами:

- акустичні (включаючи акусто перетворювальні);

- 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

прослуховування телефонних каналів зв’язку, перехоплення факсових та

модемних сеансів зв’язку;

- перехоплення комп’ютерної інформації (у тому числі

радіовипромінювання комп'ютера), несанкціонований доступ до бази

даних;

- прихована фото- та відеозйомка 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.

***2. Захист каналів зв’язку;***

Захист інформації, що обробляється ТЗПІ, здійснюється з використанням пасивних та активних методів та засобів.

***Пасивні методи*** захисту направлені на:

- ослаблення інформаційних сигналів ТЗПІ на межі зони що контролюється до рівнів,

унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

- ослаблення наведених 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, унеможливлюючих

їх виділення засобами розвідки на шумовому фоні;

***Активні методи*** захисту спрямовані на:

- створення просторових маскуючих електромагнітних завад з ціллю зменшення

відношення сигнал/завада на межі зони що контролюється до рівнів,

унеможливлюючих їх виділення засобами 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;

Ослаблення побічних електромагнітних випромінювань ТЗПІ та їх наведень у сторонні

провідники здійснюється шляхом екранування та заземлення ТЗПІ та їх ліній заземлення.

Послаблення просочування інформаційних сигналів ТЗПІ до мереж електроживлення

здійснюється шляхом фільтрації інформаційних сигналів.

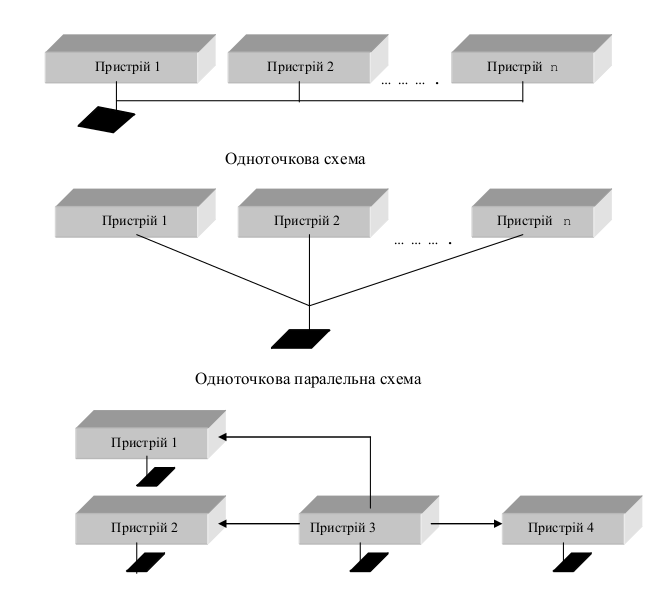
**3. Заземлення ТЗПІ**

Необхідно пам’ятати, що екранування ТЗПІ та з’єднувальних ліній ефективне тільки при умові безпомилкового заземлення.

Використовуються декілька типів заземлення: одноточкові, багатоточкові і комбіновані (гібридні) схеми, а також послідовні та паралельні схеми, та їх комбінації..

На мал. 2 представлені деякі типи заземлення [4]. Одноточкова схема проста, але має недоліки.

Тут зворотні струми протікають від різних електричних кіл по загальному дроту заземлення.



(мал. 2)

Одноточкова паралельна схема цього недоліку не має. Але має інший недолік. Вона потребує великої кількості довгих заземлюючих провідників. Це призводить до зростання електричного опору системи заземлення. Крім того, тут можуть з’являтися небажані взаємні зв’язки, котрі створюють декілька ланцюгів заземлення для кожного пристрою. В результаті можуть з’являтися вирівнюючі струми і різниці потенціалів між пристроями.

Багатоточкова схема вільна від цих недоліків. Але тут треба приймати запобіжні заходи від створення замкнутих електричних контурів.

Основні вимоги до систем заземлення:

- система має включати до себе загальний заземлювач, кабель заземлення, шини та дроти,

котрі з’єднують заземлювач з об’єктом;

- опір системи заземлення має бути мінімальним;

- кожний елемент що заземлюється має підключатися до заземлювача або до заземляючо.

Магістралі за допомогою окремого відгалужувача. Послідовне підключення декількох заземляющих елементів до одного провідника забороняється;

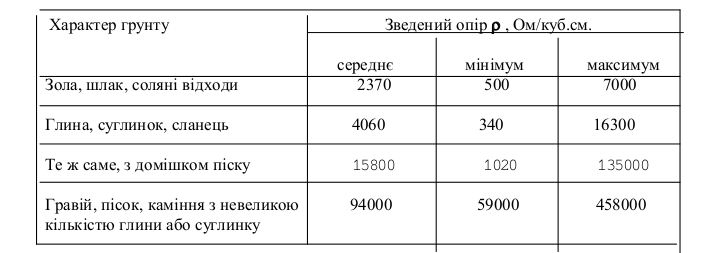
- система має бути вільна від замкнутих контурів;

- не треба використовувати загальний провідник для систем екрануючих заземлень, захисних заземлень та сигнальних кіл.

- контакти мають бути захищені від корозії та утворення оксидних плівок, а також від утворення гальванопар;

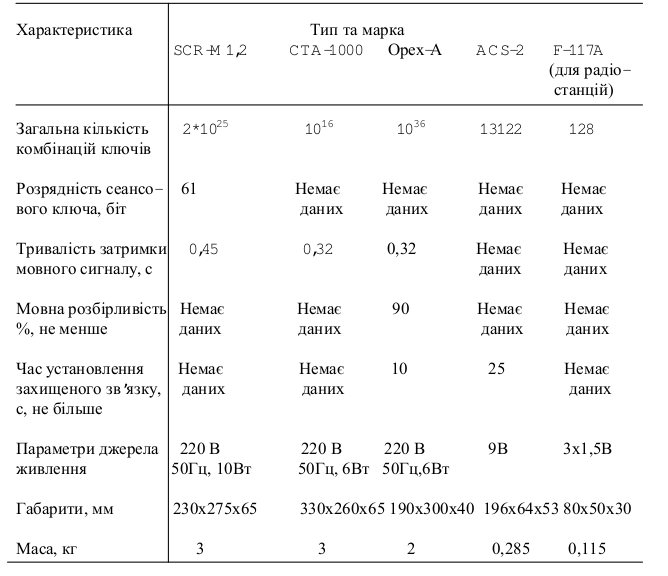
- не можна використовувати в якості заземлення нульові фази електромереж, металеві конструкції будівель, екрани і захисні оболонки підземних кабелів, металеві труби систем опалення, водопостачання тощо.

Якщо якомога краще забезпечений електричний контакт між заземлювачем та грунтом, то опір системи заземлення, в основному, складає опір грунту.

Нормований опір грунту (опір 1 кубічного сантиметра грунту) становить у середньому величини, що приводяться нижче:

**4. Закриття мовних сигналів в телефонних каналах**

Головні характеристики деяких скремблерів.



Для передавання цифрової інформації використовують пристрої серії СМ: кишеньковий телекс-шифратор СМ-11, шифратор для телефаксів СМ-13, радіоперемовний чотириканальний пристрій СМ-21 для діапазону 134....174 мГц, та ін.

Головною метою розробки систем передачі людської мови є збереження тих її характеристик, які найбільш важливі для сприйняття слухачем. Безпека зв'язку при передачі мовних повідомлень грунтується на використанні різних методів закриття, що міняють характеристики мови так, що вона стає нерозбірливо і невпізнанною для особи, що підслуховує мовне повідомлення. Метод закриття залежить від вигляду, конкретного застосування і технічних характеристик каналу передачі.

У мовних системах зв'язку відомі два основні методи закриття мовних сигналів, що відрізняються способом передачі в каналах зв'язку: аналогове скрембліровання і дискретизація мови з подальшим шифруванням (цифрові системи закриття). Кожний з цих методів має свої достоїнства і недоліки.

Рівні, або ступені секретності систем закриття мови вельми умовні, оскільки із цього приводу не вироблено чітких стандартів або правил. Прийнято, що основні рівні захисту можуть бути тактичними і стратегічними.

Тактичний, або низький рівень використовується для захисту інформації від прослуховування сторонніми особами на період часу, вимірювальний хвилинами і днями. Існує велика кількість простих методів, здатних забезпечити такий рівень захисту при прийнятній вартості.

При стратегічному, або високому рівні захисту від перехоплення висококваліфікованому і технічно добре оснащеному фахівцю для дешифрування повідомлення потрібний від декількох місяців до багатьох років.

Під аналоговим скремблювання розуміють таку зміну характеристик мовного сигналу, при якому одержаний модульований сигнал, володіючи властивостями нерозбірливості і невпізнання, займає таку ж смугу частот спектру, як і початковий відкритий сигнал. З аналогових методів практичне застосування одержало частотне і тимчасове скремблювання, а також їх комбінація. Частотне скремблювання буває двох видів — інверсне і смугове.

Інверсний скремблер здійснює перетворення мовного спектру, рівносильне повороту спектру мовного сигналу навколо деякої середньої крапки. При цьому нижні частоти перетворяться у високі і навпаки. Цей спосіб володіє невисоким рівнем закриття, оскільки при перехопленні легко встановлюється частота, відповідна середній точці інверсії в смузі спектру мовного сигналу.

Смуговий скремблер розділяє мовний спектр на декілька смуг з подальшим їх перемішуванням і інверсією за деяким правилом, або ключем (рис. 4.25). Зміна ключа дозволяє підвищити ступінь закриття, але при цьому потрібне введення синхронізації на приймальній стороні системи. Недоліком цього виду скремблювання є те, що основна частина енергії мовного сигналу зосереджена в невеликій області низькочастотного спектру. Тому вибір варіантів перемішування обмежений і багато хто з систем характеризується відносно високою залишковою розбірливістю.

У цифровому закритті мовних сигналів широко поширені системи на базі вокодеров. У таких системах пристрій кодування мови (вокодер), аналізуючи форму мовного сигналу, оцінює параметри змінних компонент моделі генерації мови і передає значення цих параметрів в цифровій формі по каналу зв'язку на синтезатор, де по прийнятих параметрах синтезується мовне повідомлення. Цифрова послідовність параметрів мови з виходу вокодерного пристрою подається на вхід шифратора, де піддається перетворенню по одному з криптографічних алгоритмів, потім поступає через модем в канал зв'язку, на приймальній стороні якого здійснюються зворотні операції по відновленню мовного сигналу. Шифруючі і дешифруючі функції забезпечуються або в окремих пристроях, або в програмно-апаратній реалізації самого вокодера.