

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
Харківський національний університет внутрішніх справ
Факультет № 6
Кафедра інформаційних технологій та захисту інформації

ТЕКСТ ЛЕКЦІЇ

З дисципліни МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ
(шифр, назва навчальної дисципліни)

за темою Класифікація та характеристика технічних каналів витоку інформації

Галузь знань 1701 "Інформаційна безпека"
(шифр, назва галузі)

Напрямок підготовки 6.170102 "Системи технічного захисту інформації"
(код, назва напрямку підготовки)

Освітньо-кваліфікаційний рівень бакалавр
(назва ОКР)

Харків
2016 рік

Передмова

Текст лекції із дисципліни " Методи та засоби захисту інформації" для студентів за напрямом підготовки 6.170102 "Системи технічного захисту інформації" на _____ арк.

СХВАЛЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ

_____ Протокол № _____
(дата, місяць, рік)

ЗАТВЕРДЖЕНО

Вченою радою факультету № 6 ХНУВС

_____ Протокол № _____
(дата, місяць, рік)

_____ (підпис) _____ (П.І.Б.)

ПОГОДЖЕНО

Секцією науково-методичної ради
ХНУВС з технічних дисциплін

_____ Протокол № _____
(дата, місяць, рік)

_____ (підпис) _____ (П.І.Б.)

ЗАТВЕРДЖЕНО

На засіданні кафедри інформаційних
технологій та захисту інформації факультету
№ 6 ХНУВС

_____ Протокол № _____
(дата, місяць, рік)

_____ (підпис) _____ (П.І.Б.)

Рецензент:

Носов В.В., професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ к.т.н., доцент.

" Методи та засоби захисту інформації" : тексти лекцій

Розробник: Тулупов В.В. – м. Харків

Харківський національний університет внутрішніх справ, 2016

План лекції

1. Загальна характеристика технічного каналу витоку інформації.
 - 1.1. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ.
2. Електромагнітні канали витоку інформації.
3. Електричні канали витоку інформації.
4. Параметричний канал витоку інформації.
5. Класифікація методів та засобів захисту інформації від витоку технічними каналами.

Література:

Основна:

1. Зайцев, А.П., Шелупанов, А.А. Технические средства и методы защиты информации [Текст]: учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов. – М.: Горячая линия-Телеком, 2009. – 616 с, ил.
2. Хорев, А.А. Способы и средства защиты информации [Текст] / А.А. Хорев. – М.: МО РФ, 2000. – 316 с.
Носов, В.В., Манжай, А.В. Організація та забезпечення безпеки інформації [Текст]: навчальний посібник / В.В. Носов, А.В. Манжай. – Харків: ХНУВС, 2007. – 216 с., іл.

Додаткова :

3. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: <http://www.dsszzi.gov.ua/>.
4. Перелік нормативно-методичних документів в галузі захисту інформації [Електронний ресурс]. – Режим доступу: http://www.nics.com.ua/images/price/price09_10.doc.

Текст лекції

1. Загальна характеристика технічного каналу витоку інформації

Під технічним каналом витоку інформації (ТКВІ) розуміють сукупність об'єкта розвідки, технічного засобу розвідки (ТЗР), за допомогою якого добувається інформація про цей об'єкт, із фізичного середовища, у якому поширюється інформаційний сигнал.

ТКВІ – це спосіб одержання за допомогою ТЗР розвідувальної інформації про об'єкт. Під розвідувальною інформацією звичайно розуміються відомості або сукупність даних про об'єкти розвідки незалежно від форми їхнього подання.

Сигнали є матеріальними носіями інформації. По своїй фізичній природі *сигнали* бувають *електричними, електромагнітними, акустичними, і т.д.* Тобто *сигналами є електромагнітні, механічні й інші види коливань (хвиль)*, причому інформація втримується в їхніх параметрах, що змінюються.

Залежно від природи сигнали поширюються в певних фізичних середовищах. У загальному випадку середовищем поширення можуть бути газові (повітряні), рідинні (водні) і тверді середовища. Наприклад повітряний простір, конструкції споруд, сполучні лінії й струмопровідні елементи, ґрунт (земля) і т.п.

Технічні засоби розвідки служать для прийому й вимірювання параметрів сигналів.

1.1. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ

Згідно з Державним стандартом України (ДСТУ 3396.2-96) «Технічний захист інформації. Терміни та визначення», *технічний канал витоку інформації* – сукупність носіїв інформації, середовища їх поширення та засобів технічної розвідки.

Канал витоку інформації – неконтрольований фізичний шлях від джерела інформації за межі організації чи кола осіб, що володіють охоронюваними відомостями, за допомогою якого можливо неправомірне оволодіння зловмисником інформацією.

З технічних каналів витоку інформації найбільшу небезпеку представляє такий НСД, як знімання інформації за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВН).

Для перехоплення, обробки й аналізу інформації в КВІ можуть використовуватися різноманітні технічні засоби (ТЗ), а також люди (порушники). Тоді існуючі КВІ в залежності від джерел і одержувачів інформації утворюють чотири основних типи каналів: «людина – людина», «людина – ТЗ», «ТЗ – ТЗ» і «ТЗ – людина».

Сказане визначає напрямки потоків інформації. Якщо інформаційний потік поширюється в напрямку від носія до одержувача, то утвориться *узагальнений канал витоку*, якщо ж інформаційний потік у виді явного чи схованого впливу спрямований по вищевказаним чотирьох типах каналів від порушника до носія інформації, то виникає так називаний *узагальнений канал інформаційного впливу* на носій інформації.

У залежності від того, на який параметр носія інформації задумано здійснити вплив, порушником можуть бути застосовані психічні, фізичні, програмно-математичні, радіоелектронні й інші способи і засоби. Параметрами, на які задумано здійснити вплив можуть мати різні характеристики матеріальних носіїв, у тому числі й особистісні характеристики головного прямого носія інформації на об'єкті захисту – людини.

Найбільший потенціал інформативності мають КВІ, у яких для добування конфіденційної інформації використовуються різні технічні засоби. Такі канали одержали назву технічних (ТКВІ). Структура будь-якого ТКВІ, що утворюється в результаті перехоплення, може бути представлена у вигляді системи передачі інформації (рис. 6). При цьому процес передачі повідомлень розбивається на три основні етапи. На початку кожне повідомлення $a(t)$ перетворюється передавачем у небезпечний (інформаційний) сигнал $b(t)$. Небезпечний сигнал переміщується по тракту його поширення, де на нього діє завада $p(t)$, внаслідок чого він частково згасає. Далі одержаний на приймальній стороні небезпечний сигнал $b'(t)$ перетворюється приймачем порушника в повідомлення $a'(t)$. Оскільки завади в загальному випадку мають випадковий характер, сигнал на вході приймача $b'(t)$ буде випадковим чином відрізнятися від $b(t)$ і повідомлення $a(t)$ може відрізнятися від $a'(t)$.

ТКВІ може бути утворений як за допомогою спеціальних закладних пристроїв (мініатюрні передавачі) та приймачів, так і з допомогою тільки приймачів, які приймають небезпечні сигнали, утворені несанкціонованим перетворенням сигналів з ІПЗ у технічних засобах обробки інформації.

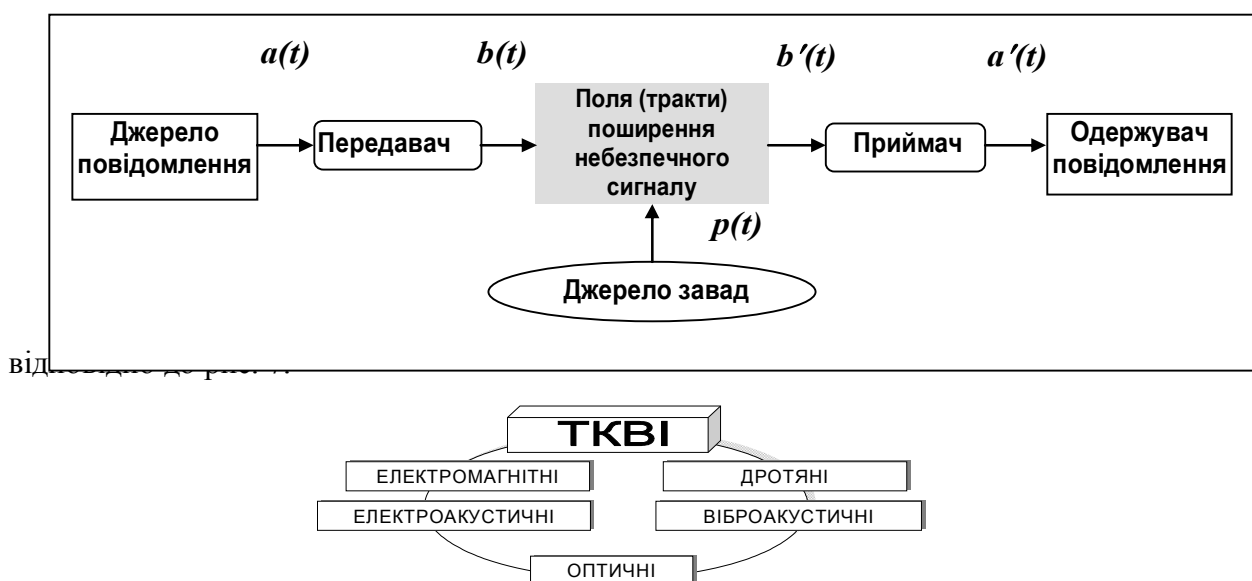


Рис. 7. Класифікація ТКВІ

Схема можливих каналів витоку і несанкціонованого доступу до інформації в типовому одноповерховому приміщенні показана на рис. 8.

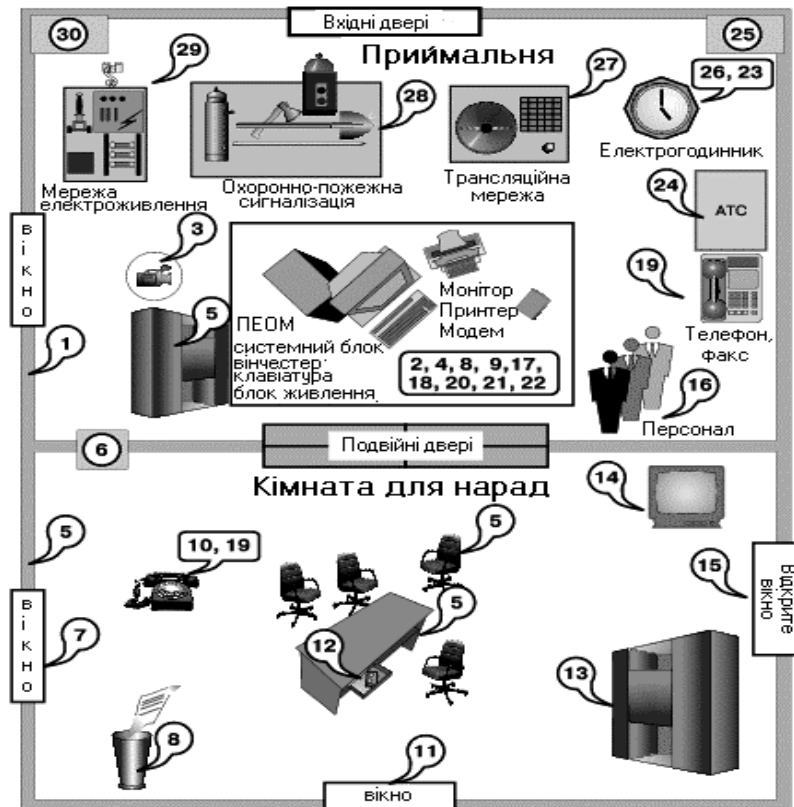


Рис. 8. Можливі КВІ і НСД:

1 – витік за рахунок структурного звуку в стінах і перекриттях; 2 – зняття інформації із стрічки принтера, погано стертих дискет і т.п.; 3 – зняття інформації з використанням відеозапису; 4 – програмно-апаратні закладки в ПЕВМ; 5 – радіозаписи у стінах і меблях; 6 – зняття інформації із системи вентиляції; 7 – лазерне зняття акустичної інформації з вікон; 8 – виробничі й технологічні відходи; 9 – комп'ютерні віруси, логічні бомби і т.п.; 10 – зняття інформації шляхом наведень і "нав'язування"; 11 – дистанційне зняття відеоінформації (оптика); 12 – зняття акустичної інформації з використанням диктофонів; 13 – крадіжка носіїв інформації; 14 – високочастотний канал витоку в побутовій техніці; 15 – зняття інформації напрямленим мікрофоном; 16 – внутрішні канали витоку інформації (через обслуговуючий персонал); 17 – несанкціоноване копіювання; 18 – витік за рахунок побічного випромінювання терміналу; 19 – зняття інформації за рахунок використання "телефонного вуха"; 20 – зняття з клавіатури і принтера по акустичному каналу; 21 – зняття з монітора по електромагнітному каналу; 22 – візуальне зняття з монітора і принтера; 23 – наведення на лінії комунікацій і сторонні провідники; 24 – витік через лінії зв'язку; 25 – витік по ланцюгах заземлення; 26 – витік по мережі електрогодинника; 27 – витік по трансляційній мережі та гучномовному зв'язку; 28 – витік по охоронно-пожежній сигналізації; 29 – витік по мережі електроживлення; 30 – витік по мережі опалювання, газо- і водопостачання.

Виходячи з фізичної природи утворення, технічні канали витоку інформації класифікують як:

– *візуально-оптичні канали* – це, як правило, візуальне спостереження: безпосереднє чи віддалене із застосуванням технічних засобів. Переносником інформації виступає світло, що випускається джерелом конфіденційної інформації, або відбите від нього у видимому, інфрачервоному чи ультрафіолетовому діапазонах;

– *віброакустичні канали*. В акустичних каналах переносником інформації (мова, шуми) виступає звук, що лежить у смузі ультразвуку (понад 20000 Гц), чутного та інфразвукового (до 16 Гц) діапазонів. Діапазон звукових частот, які чує людина, лежить у межах від 16 до 20000 Гц, а як таких, що містяться в людському мовленні, – від 100 до 6000 Гц. Середовищем поширення

звуку є повітря, земля, вода, будівельні конструкції (цегла, залізобетон, металева арматура та ін.);

– *радіоелектронний канал*. Переносником інформації є або електромагнітні хвилі в радіочастотному діапазоні, або струм, що проходить через загальне джерело живлення або по колу заземлення;

– *матеріально-дійсними каналами витоку* виступають найрізноманітніші матеріали у твердому, рідкому чи газоподібному або корпускулярному (радіоактивні елементи) вигляді.

Пошуки шляхів підвищення дальності добування мовної інформації призвели до появи складених каналів витоку інформації, що містять в собі сполучення вищевказаних каналів, наприклад *радіоакустичний, акустооптичний* тощо.

Технічні засоби прийому, обробки, зберігання й передачі інформації (ТЗПІ) – це технічні засоби, що безпосередньо обробляють конфіденційну інформацію.

До таких засобів відносяться:

- електронно-обчислювальна техніка, режимні АТС;
- системи оперативно-командного й гучномовного зв'язку;
- системи звукопідсилення;
- звукового супроводу і звукозапису і т.д.

При виявленні технічних каналів витоку інформації ТЗПІ необхідно розглядати як систему, що включає основне (стаціонарне) устаткування, кінцеві пристрої, сполучні лінії (сукупність проводів і кабелів, що прокладаються між окремими ТЗПІ і їхніми елементами), розподільні й комутаційні пристрої, системи електроживлення, системи заземлення.

Окремі технічні засоби або група технічних засобів, призначених для обробки конфіденційної інформації, разом із приміщеннями, у яких вони розміщуються, становлять *об'єкт ТЗПІ*. Під *об'єктами ТЗПІ* розуміють також виділені приміщення, призначені для проведення закритих заходів.

Поряд із ТЗПІ в приміщеннях установлюються технічні засоби й системи, що безпосередньо не беруть участь в обробці конфіденційної інформації, але використовуються разом із ТЗПІ і перебувають у зоні електромагнітного поля, створюваного ними. Такі технічні засоби й системи називаються *допоміжними технічними засобами й системами (ДТЗС)*.

До них відносяться:

- технічні засоби відкритого телефонного, гучномовного зв'язку;
- системи пожежної й охоронної сигналізації, електрофікації, радіофікації, часофікації, електропобутові прилади і т.д.

Як канал витоку інформації найбільший інтерес представляють ДТЗС, що мають вихід за межі контрольованої зони (КЗ), тобто зони, у якій виключена поява осіб і транспортних засобів, які не мають постійних або тимчасових пропусків.

Крім з'єднувальних ліній ТЗПІ й ДТЗС за межі контрольованої зони можуть виходити кабелі, які для цих ліній не застосовуються, але проходять через приміщення, де встановлені технічні засоби, а також металеві труби систем опалення, водопостачання й інші струмопровідні металоконструкції. Такі з'єднувальні лінії, кабелі й струмопровідні елементи називаються *сторонніми провідниками*.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їхнього поширення й способів перехоплення, технічні канали витоку інформації можна розділити на електромагнітні, електричні й параметричний.

Основні технічні заходи спрямовані на блокування каналів витоку інформації і ґрунтуються на одному з показаних на рис. 9 принципів.

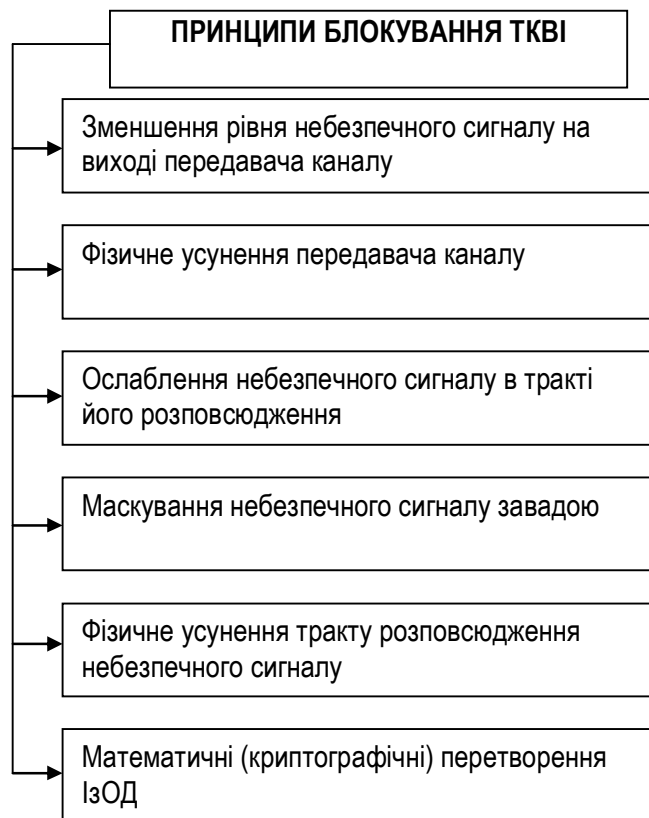


Рис. 9. Принципи блокування ТКВІ

Успіх реалізації вказаних принципів захисту залежить від багатьох чинників. Основними з них є: механізм утворення конкретного ТКВІ; принцип дії та технічні характеристики спеціальних засобів знімання інформації; особливості побудови і функціонування елементів ІС та їх територіального розташування; обраний критерій ефективності/вартість захисту і т.д.

Спеціальні засоби ТЗІ, використовувані під час реалізації основних технічних заходів, можна розділити на засоби ТЗІ і засоби спеціального контролю (рис. 10).

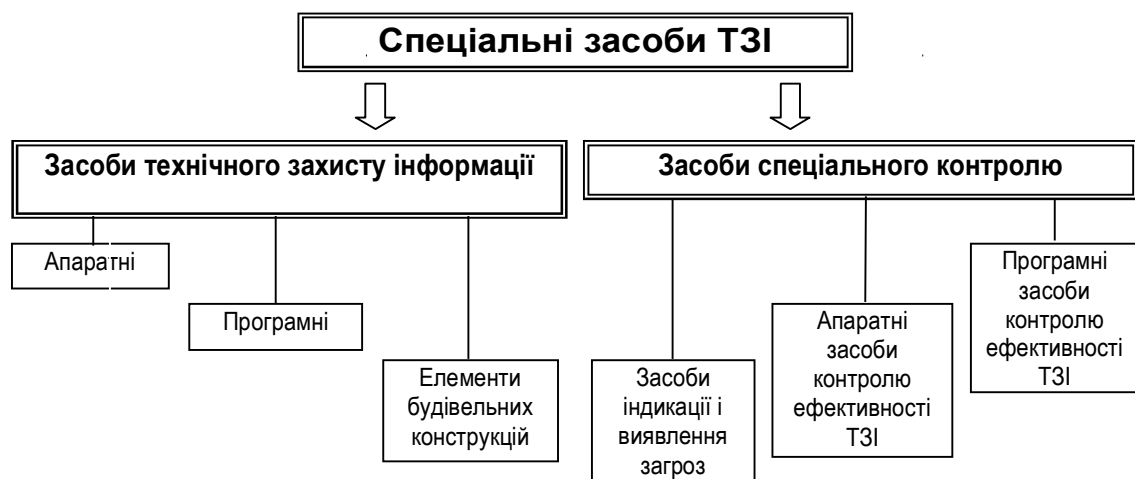


Рис.10 Класифікація спеціальних засобів ТЗІ

Основні технічні заходи передбачають:

1. Заходи щодо блокування ТКВІ з використанням *пасивних засобів* [42]:
 - контроль і обмеження доступу на об'єкти ТСПІ та у виділені приміщення:

- установка на об'єктах ТСПІ та у виділених приміщеннях технічних засобів і систем обмеження і контролю доступу;
- *локалізація випромінювань*:
 - екранування ТСПІ та їх сполучних ліній;
 - заземлення ТСПІ та екранів їх сполучних ліній;
 - звукоізоляція виділених приміщень.
- *розв'язування інформаційних сигналів*:
 - установка смугових фільтрів у допоміжних технічних засобах і системах, у яких спостерігається «мікрофонний ефект» і які мають вихід за межі контрольованої зони (рис. 2.14);
 - установка спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання і каналізації, що мають вихід за межі контрольованої зони;
 - установка автономних або стабілізованих джерел електроживлення ТСПІ;
 - установка пристроїв гарантованого живлення ТСПІ (наприклад, генераторів мотора);
 - установка в ланцюгах і лініях електроживлення ТСПІ та виділених приміщень спеціальних заглушуючих фільтрів.

2. Заходи щодо блокування ТКВІ з використанням *активних засобів* [42]:

- *просторове зашумлення*:
 - просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних завад (у випадках виявлення і визначення частоти випромінювання закладного пристрою або побічних електромагнітних випромінювань ТСПІ) з використанням засобів створення прицільних завад (рис. 2.18 і 2.19);
 - створення акустичних і вібраційних завад з використанням генераторів акустичного шуму (рис. 2.20 і 2.21);
 - заглушення диктофонів у режимі запису з використанням відповідних пристроїв;
- *лінійне зашумлення*:
 - лінійне зашумлення ліній електроживлення (рис. 2.22);
 - лінійне зашумлення сторонніх провідників і сполучних ліній ДТСЗ, що мають вихід за межі контрольованої зони (рис. 2.23);
- *знищення закладних пристроїв*:
 - знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (випалювачів "жучків").

2. Електромагнітні канали витоку інформації

Електромагнітні канали витоку інформації виникають за рахунок різного виду побічних електромагнітних випромінювань (ЕМВ) ТЗПІ :

- випромінювань елементів ТЗПІ;
- випромінювань на частотах роботи високочастотних (ВЧ) генераторів ТЗПІ;
- випромінювань на частотах самозбудження підсилювачів низької частоти (ПНЧ) ТЗПІ.

Електромагнітні випромінювання елементів ТЗПІ. У ТЗПІ носієм інформації є електричний струм, параметри якого (сила струму, напруга, частота й фаза) змінюються за законом інформаційного сигналу. При проходженні електричного струму по струмопровідних елементах ТЗПІ навколо них (у навколишньому просторі) виникає електричне й магнітне поле. У силу цього елементи ТЗПІ можна розглядати як випромінювачі електромагнітного поля, модульованого за законом зміни інформаційного сигналу.

Електромагнітні випромінювання на частотах роботи ВЧ-генераторів ТЗПІ й ДТЗС. До складу ТЗПІ й ДТЗС можуть входити різного роду високочастотні генератори, а саме:

- генератори тактової частоти;
- генератори стирання й підмагнічування магнітофонів;
- гетеродини радіоприймальних і телевізійних пристроїв;

– генератори вимірювальних приладів і т.д.

У результаті зовнішніх впливів інформаційного сигналу (наприклад, електромагнітних коливань) на елементах ВЧ-генераторів наводяться електричні сигнали. Приймачем магнітного поля можуть бути котушки індуктивності коливальних контурів, дроселі в ланцюгах електроживлення і т.п. Приймачем електричного поля є проводи високочастотних ланцюгів і інші елементи. Наведені електричні сигнали можуть викликати ненавмисну модуляцію власних ВЧ-коливань генераторів. Ці промодельовані ВЧ-коливання випромінюються в навколишній простір.

Електромагнітні випромінювання на частотах самозбудження ПНЧ ТЗП. Самозбудження ПНЧ ТЗП (наприклад, підсилювачів систем звукопідсилення й звукового супроводу, магнітофонів, систем гучномовного зв'язку т.п.) можливо за рахунок випадкових перетворень негативних зворотних зв'язків (індуктивних або ємнісних) у паразитні позитивні, що приводить до переведення підсилювача з режиму посилення в режим автоматичної генерації сигналів. Частота самозбудження лежить у межах робочих частот нелінійних елементів ПНЧ (наприклад, напівпровідникових приладів, електровакуумних ламп і т.п.). Сигнал на частотах самозбудження, як правило, виявляється інформаційним сигналом, який промодульований. Самозбудження спостерігається, в основному, при перекладі ПНЧ у нелінійний режим роботи, тобто в режим перевантаження.

Перехоплення побічних електромагнітних випромінювань ТЗП здійснюється засобами радіо-, радіотехнічної розвідки, розміщеними поза контрольованою зоною.

Зона, у якій можливі перехоплення (за допомогою розвідувального приймача) побічних електромагнітних випромінювань і наступна розшифровка інформації, що міститься в них (тобто зона, у межах якої відношення «інформаційний сигнал/перешкода» перевищує припустиме нормоване значення), називається (небезпечною) зоною 2.

3. Електричні канали витоку інформації

Причинами виникнення електричних каналів витоку інформації можуть бути :

- наведення електромагнітних випромінювань ТЗП на сполучні лінії ДТЗС і сторонні провідники, що виходять за межі контрольованої зони;
- витік інформаційних сигналів у ланцюги електроживлення ТЗП;
- витік інформаційних сигналів у ланцюги заземлення ТЗП.

Наведення електромагнітних випромінювань ТЗП виникають при випромінюванні елементами ТЗП (у тому числі і їхніми сполучними лініями) інформаційних сигналів, а також при наявності гальванічного зв'язку з'єднувальних ліній ТЗП та сторонніх провідників або ліній ДТЗС. Рівень сигналів, що наводяться, у значній мірі залежить від потужності випромінюваних сигналів, відстані до провідників, а також довжини спільного пробігу сполучних ліній ТЗП й сторонніх провідників.

Простір навколо ТЗП, у межах якого на випадкових антенах наводиться інформаційний сигнал вище припустимого (нормованого) рівня, називається (небезпечною) зоною 1.

Випадковою антеною є ланцюг ДТЗС або сторонні провідники, здатні приймати побічні електромагнітні випромінювання.

Випадкові антени можуть бути зосередженими й розподіленими. *Зосереджена випадкова антена* являє собою компактний технічний засіб, наприклад телефонний апарат, гучномовець радіотрансляційної мережі й т.д. До *розподілених випадкових антен* відносять випадкові антени з розподіленими параметрами: кабелі, проводи, металеві труби й інші струмопровідні комунікації.

Витік інформаційних сигналів у ланцюзі електроживлення можливо при наявності магнітного зв'язку між вихідним трансформатором підсилювача (наприклад, ПНЧ) і трансформатором випрямного пристрою. Крім того, струми посилюваних інформаційних сигналів замикаються через джерело електроживлення, створюючи на його внутрішньому опорі спад напруги, що при недостатньому загасанні у фільтрі випрямного пристрою може бути виявлене в лінії електроживлення. Інформаційний сигнал може проникнути в ланцюги

електроживлення також у результаті того, що середнє значення споживаного струму в кінцевих каскадах підсилювачів у більшому або меншому ступені залежить від амплітуди інформаційного сигналу, що створює нерівномірне навантаження на випрямляч і приводить до зміни споживаного струму за законом зміни інформаційного сигналу.

Витік інформаційних сигналів у ланцюги заземлення. Крім заземлюючих провідників, що служать для безпосереднього з'єднання ТЗП з контуром заземлення, гальванічний зв'язок із землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносять нульовий провід мережі електроживлення, екрани (металеві оболонки) сполучних кабелів, металеві труби систем опалення і водопостачання, металеві арматури залізобетонних конструкцій і т.д. Усі ці провідники разом із заземлюючим пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали. Крім того, у ґрунті навколо заземлюючого пристрою виникає електромагнітне поле, що також є джерелом інформації.

Перехоплення інформаційних сигналів по електричних каналах витоку можливе шляхом безпосереднього підключення до сполучних ліній ДТЗС і стороннім провідникам, що проходять через приміщення, де встановлені ТЗП, а також до їхніх систем електроживлення й заземлення. Для цих цілей використовуються спеціальні засоби радіо- і радіотехнічної розвідки, а також спеціальна вимірювальна апаратура.

Знімання інформації з використанням апаратних закладок. В останні роки почастишали випадки знімання інформації, оброблюваної в ТЗП, шляхом установки в них електронних пристроїв перехоплення інформації – закладних пристроїв.

Електронні пристрої перехоплення інформації, установлені в ТЗП, іноді називають *апаратними закладками*. Вони являють собою міні-передавачі, випромінювання яких модулюється інформаційним сигналом. Найбільше часто закладки встановлюються в ТЗП іноземного виробництва, однак можлива їхня установка й у вітчизняних засобах.

Перехоплена за допомогою закладних пристроїв інформація або безпосередньо передається по радіоканалі, або спочатку записується на спеціальний запам'ятовувальний пристрій, а вже потім по команді передається на об'єкт, що її запросив. Схема каналу витоку інформації з використанням заставних пристроїв представлена на Рис. 10.

4. Параметричний канал витоку інформації

Перехоплення оброблюваної в технічних засобах інформації може здійснюватися шляхом їх «високочастотного опромінення». При взаємодії електромагнітного поля, що опромінює, з елементами ТЗП відбувається перевипромінювання електромагнітного поля. У ряді випадків це вторинне випромінювання модулюється інформаційним сигналом. При зніманні інформації для виключення взаємного впливу випромінюваного й перевипроміненого сигналів може використовуватися їх тимчасова або частотна розв'язка.¹

При перевипромінюванні параметри сигналів змінюються. Тому даний канал витоку інформації часто називають параметричним.

Для перехоплення інформації з даного каналу необхідні спеціальні високочастотні генератори з антенами, що мають вузькі діаграми спрямованості і спеціальні радіо пристрої. Схема параметричного каналу витоку інформації представлена на Рис. 11.

¹ Наприклад, для опромінювання ТЗП можуть використовуватися імпульсні сигнали.

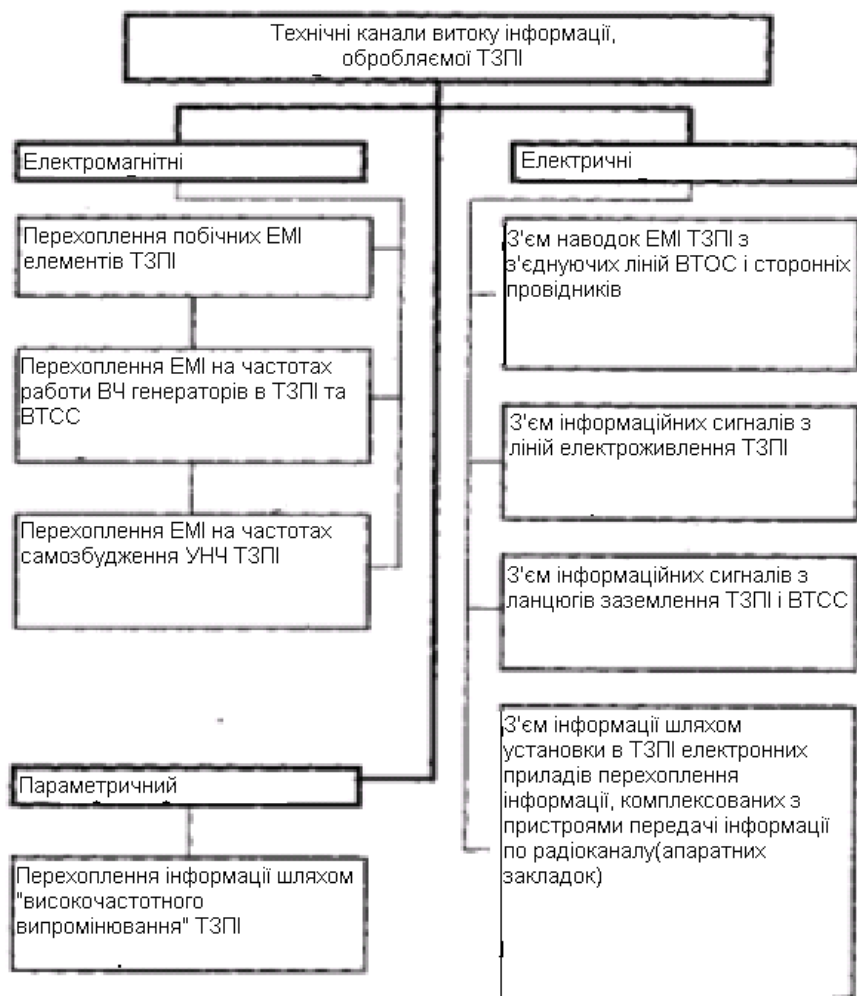


Рис. 1.1.

1. Класифікація методів та засобів захисту інформації від витоку технічними каналами

1. Організаційні методи захисту.

2. Технічні методи захисту.

1. *Організаційний захід* – це захід захисту інформації, проведення якого не вимагає застосування спеціально розроблених технічних засобів.

Захист інформації від витоку по технічних каналах досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних електронних пристроїв перехоплення інформації (заставних пристроїв).

До основних організаційних і режимних заходів відносяться:

- залучення до проведення робіт по захисту інформації організацій, що мають ліцензію на діяльність в області захисту інформації, видану відповідними органами;
- категоріювання і атестація об'єктів ТСПІ і виділених для проведення закритих заходів приміщень (далі виділених приміщень) по виконанню вимог забезпечення захисту інформації при проведенні робіт з відомостями відповідної міри
- секретності;
- використання на об'єкті сертифікованих ТСПІ у ВТСС;
- встановлення контрольованої зони навколо об'єкту;
- залучення до робіт по будівництву, конструкції об'єктів ТСПІ, монтажу апаратури організацій, що мають ліцензію на діяльність в області захисту інформації за відповідними пунктами;

- організація контролю і обмеження доступу на об'єкти ТСП і у виділені приміщення;
- введення територіальних, частотних, енергетичних, просторових і тимчасових обмежень в режимах використання технічних засобів, що підлягають захисту;
- відключення на період закритих заходів технічних засобів, що мають елементи, що виконують роль електроакустичних перетворювачів, від ліній зв'язку і так далі.

2. *Технічний захід* – це захід по захисту інформації, який передбачає застосування спеціальних технічних засобів, а також реалізацію технічних рішень.

Технічні заходи спрямовані на закриття каналів витоку інформації шляхом послаблення рівня інформаційних сигналів або зменшення відношення сигнал/шум в місцях можливого розміщення портативних засобів розвідки або їх датчиків до величин, що забезпечують неможливість виділення інформаційного сигналу засобом розвідки, і проводяться з використанням активних і пасивних засобів.

До технічних заходів з використанням пасивних засобів відносяться :

- *контроль і обмеження доступу на об'єкти ТСП та у виділені приміщення:*
- встановлення на об'єктах ТСП і у виділених приміщеннях технічних засобів і систем обмеження і контролю доступу.
- *локалізація випромінювань :*
- екранування ТСП та їх ліній з'єднання;
- заземлення ТСП і екранів їх ліній з'єднання;
- звукоізоляція виділених приміщень.
- *розв'язування інформаційних сигналів:*
- встановлення спеціальних засобів захисту типу «Граніт» у допоміжних технічних засобах і системах, що мають «мікрофонний ефект» та вихід за межі контрольованої зони;
- встановлення спеціальних діелектричних вставок в обплетення кабелів електроживлення, труб систем опалювання, водопостачання і каналізації що мають вихід за межі контрольованої зони;
- встановлення автономних або стабілізованих джерел електроживлення ТСП;
- встановлення облаштувань гарантованого живлення ТСП (наприклад, мотор-генераторів);
- встановлення в ланцюгах електроживлення ТСП, а також в лініях освітлювальної і розеткової мереж виділених приміщень перешкодоподавляючих фільтрів типу Ф11.

До технічних заходів з використанням активних засобів відносяться:

- *просторове зашумлення:*
- просторове електромагнітне зашумлення з використанням генераторів шуму або створення прицільних перешкод (при виявленні і визначенні частоти випромінювання заставного пристрою або побічних електромагнітних випромінювань) з використанням засобів створення прицільних перешкод;
- створення акустичних і вібраційних перешкод з використанням генераторів акустичного шуму;
- *пригнічення диктофонів в режимі запису з використанням пригнічувачів диктофонів;*
- *лінійне зашумлення:*
- лінійне зашумлення ліній електроживлення;
- лінійне зашумлення сторонніх провідників і сполучних ліній ВТСС, що мають вихід за межі контрольованої зони;
- *знищення закладних пристроїв, підключених до лінії, з використанням спеціальних генераторів імпульсів (спалювачів жучків).*

Виявлення портативних електронних облаштувань перехоплення інформації (заставних пристроїв) здійснюється проведенням спеціальних обстежень, а також спеціальних перевірок об'єктів ТСП і виділених приміщень.

Спеціальні обстеження об'єктів ТСП і виділених приміщень проводяться шляхом їх візуального огляду без застосування технічних засобів.

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

- виявлення закладних пристроїв з використанням пасивних засобів:
 - пошук заставних пристроїв з використанням індикаторів поля, інтерцепторів, частотомірів, приймачів і програмно-апаратних комплексів контролю;
 - організація радіоконтролю (постійно або на час проведення конфіденційних заходів) і побічних електромагнітних випромінювань ТСПП.
- виявлення заставних пристроїв з використанням активних засобів:
 - спеціальна перевірка виділених приміщень з використанням нелінійних локаторів;
 - спеціальна перевірка виділених приміщень, ТСПП і допоміжних технічних засобів з використанням рентгенівських комплексів;
 - установка у виділених приміщеннях засобів і систем виявлення лазерного опромінення (підсвічування) вікон;
 - установка у виділених приміщеннях стаціонарних шукачів диктофонів