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 *Технічні канали витоку інформації*

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

Напрям підготовки *6.170102 "Системи технічного захисту інформації"*
(код, назва напряму 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
2. Класифікація та характеристика технічних каналів витоку інформації, що обробляється ТЗПІ
3. Особливості витоку інформації технічними каналами
4. Типова структура та види технічних каналів витоку інформації

Література:

Основна:

1. Зайцев, А.П., Шелупанов, А.А. Технические средства и методи 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.
3. 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.
4. Торокин, А.А. Инженерно-техническая защита информации [Текст] / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.
5. Хорев, А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации [Текст]: учебное пособие / А.А. Хорев. – М.: ГТК России, 1998. – 320 с.
6. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс]: НД ТЗІ 1.1-002-99 введений в дію наказом ДСТСЗІ Наказ від 28.04.1999 № 22. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/doccatalog/document?id=41651.
7. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/.
8. Перелік нормативно-методичних документів в галузі захисту інформації [Електронний ресурс]. – Режим доступу: http://www.nics.com.ua/ images/price/price09_10.doc.
9. Законодавство України [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?user=a#Find.

Додаткова:

1. Кузнецов, В.И. Радиосвязь в условиях радиоэлектронной борьбы [Текст] / В.И. Кузнецов. – Воронеж: Воронежский НИИ Связи, 2002. – 403 с.: ил.
2. Каландин, А.П., Герасименко, В.Г., Войналович, В.Ю. Информационная безопасность и защита информации /Сборник терминов и определений [Текст] / А.П. Каландин, В.Г. Герасименко, В.Ю. Войналович. – М., Гостехкомиссия, 2001. – 141 с.
3. Вартанесян, В.А. Радиоэлектронная разведка [Текст] / В.А. Вартанесян. – М.: Воениздат, 1975. – 255 с.

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.

2. 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 електромагнітний 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 утворять чотири основних типи каналів: «людина – людина», «людина – ТЗ», «ТЗ – ТЗ» і «ТЗ – людина».

Сказане визначає напрямок 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.

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 мовлені, – 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'язка;
- 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 розміщаються, 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 (Рис. 6).

3. Особливості витоку інформації технічними каналами

Під *витоком інформації* розуміється несанкціонований перенесення інформації від її джерела до зловмисника. Витік інформації шляхом її розголошення людьми, втратою ними носіїв з інформацією, перенесенням інформації, потоків елементарних часток, речовин в газоподібному, рідкому або твердому вигляду. Витік інформації порівняно з розкраданням матеріальних об'єктів має ряд особливостей, які треба враховувати при організації захисту інформації:

- при витоку інформації не виконується закон збереження матерії, в наслідок чого витік не може бути виявлений в результаті зменшення кількості інформації джерела;
- витік інформації може відбуватися лише при попаданні до зацікавленого в ній несанкціонованого одержувача (зловмисника), на відміну;
- при витоку інформації внаслідок розширення кола її споживачів ціна інформації

зменшується.

При витоку інформації можуть бути відсутні явні ознаки її розкрадання:

– документи в наявності, відбитки печаток на сейфі не порушенні, слідів проникнення в приміщення сторонніх осіб немає. Однак поява непрямих ознак (раптова поява на ринку конкурентного товару з ідентичними споживчими властивостями, зрив з незрозумілих причин виконання договору) змушує причину цих подій розглядати, як витік інформації. Через істотне запізнення виявлення ознак по відношенню до часу витоку інформації завдання хоча б часткової нейтралізації її наслідків стає вельми проблематичною;

– самі по собі факти втрати документу, розголошення відомостей, поширення носіїв за межі контрольованої зони та інші дії далеко не завжди призводять до витоку інформації.[1]

У загальному випадку можна говорити про витік інформації, як факту порушення її безпеки тільки в тому випадку, якщо вона потрапляє до зловмисника незалежно від того, знає або не знає про це власник інформації.

Під *витоком* слід розуміти не процес поширення носія, а *варіант розповсюдження, що закінчується потраплянням інформації до зловмисника.* Вихід же носія за межі заданої області створює передумови для витоку інформації і підвищує загрозу її безпеці. Зауваження про несанкціонованого одержувача має принципове значення. Якщо одержувач інформації санкціонований, то мова йде не про витік, а про передачу інформації по так званому функціональному каналу зв'язку, спеціально створеному для забезпечення комунікацій в людському суспільств.

Можливість витоку інформації характеризується *ризиком витоку,* а цілеспрямована діяльність зі зміни можливості витоку називається *управлінням ризиком.*

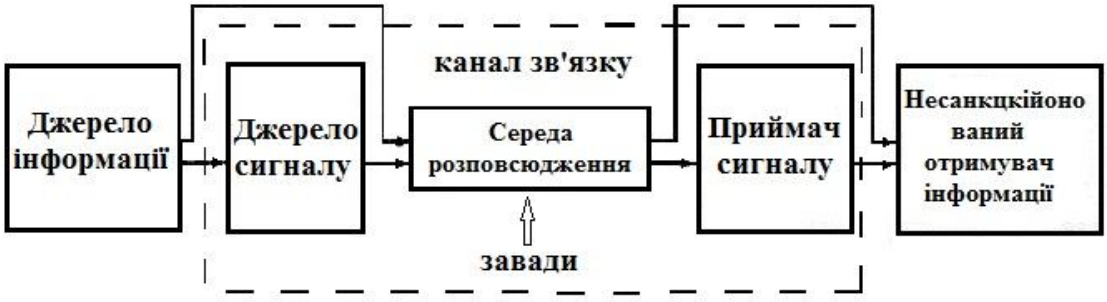
Часто розкрадання і витік інформації розглядають, як автономні процеси. Якщо під розкраданням і витоком інформації розуміти умисне привласнення чужої власності без дозволу її законного власника, то несанкціоноване отримання інформації в результаті її витоку являє собою один із способів її розкрадання. Коли зловмисник знаходить загублений документ з грифом « таємно» і свідомо, розуміючи що наноситися власнику інформації збиток, продасть його зарубіжній спецслужбі, то він може бути притягнутий до кримінальної відповідальності за розкрадання держтаємниці.

4. Типова структура та види технічних каналів витоку інформації

Фізичний шлях несанкціонованого розповсюдження носія інформації до зловмисника утворює канал витоку інформації.

Узагальнена структура типового технічного каналу витоку інформації наведена на рис. 7

[1] Наприклад, якщо приватну розмову під година наради в кабінеті керівника організації чути в приймальню через нещільно закриті двері, а в приймальні немає сторонніх осіб, то витоку інформації немає, хоча носій інформації(акустична хвиля) виходить за межі контрольованої зони - кабінету. Тільки в тому випадку, коли в приймальні буде знаходитись співробітник організації або відвідувач, який скористається інформацією з почутого розмови в особистих або інших цілях або поділитися нею з іншими зацікавленими в ній людьми, відбувається витік інформації з кабінету керівника.



Мал. 6.1 Структура технічного каналу витоку інформації

Інформація, що переноситься, може міститися як на носіях, що є одночасно її джерелами, так і носіях-переносниках, на яких вона переписується з джерел. Наприклад, відходи діловодства, що є джерелами інформації, можуть переноситися людьми або стихійними силами в просторі від місця знаходження джерела до зловмисника, утворюючи канал просочування інформації. Тому канал витоку інформації на макротілах містить джерело інформації, середовище поширення носія і несанкціонованого одержувача. Інформація, що переноситься динамічними носіями у вигляді полів (акустичних і електромагнітних) і електричного струму, заздалегідь переписується в джерелі сигналів в їх інформаційні параметри. Середовище її поширення і приймач сигналу утворюють в сукупності канал зв’язку. Завдання каналу зв’язку полягає в передачі вхідної інформації санкціонованому одержувачеві з мінімальними спотвореннями, тимчасовими, енергетичними і іншими витратами.

Канал просочування інформації на носіях у вигляді нулів і елементарних часток містить ті ж елементи, що і канал зв’язку. І відмінність між ними умовна – залежно від одержувача формації. У каналу зв’язку одержувач інформації санкціонований, у каналу витоку — несанкціонований.[2]

На вхід каналу зв'язку поступає інформація у вигляді первинного сигналу або саме джерело може бути джерелом інформації. Первинний сигнал є носієм з інформацією від це джерела або з виходу попереднього каналу. В якості джерел сигналів можуть бути:

- об’єкт спостереження, що відбиває електромагнітні хвилі, у тому числі світло;
- об’єкт спостереження, випромінюючий власні електромагнітні хвилі в оптичному і радіодіапазонах, викликані тепловим рухом електронів;
- механізми, що рухаються, і машини, створюють акустичні сигнали;
- передавачі функціональних каналів звязку;
- ретранслятори, наприклад заставні пристрої;
- джерела побічних електромагнітних випромінювань і наведень (ПЕМІН);
- радіоактивні матеріали.

Більшість джерел сигналу є одночасно джерелами інформації про видові, сигнальні або мовні ознаки. Тільки у разі, коли передається семантична інформація, вона поступає на вхід джерела сигналу на носії у вигляді первинного сигналу.

Вказані на малюнку стрілками шляху входу і виходу інформації означають вхід і вихід первинних сигналів з інформацією. Оскільки інформація від джерела поступає на вхід каналу на мові джерела (у вигляді буквено-цифрового тексту, символів, знаків, звуків, сигналів і т. д.), то передавач робить перетворення цієї форми представлення інформації у форму, що забезпечує запис її на носій інформації, що відповідає середовищу поширення.

---

[2] Наприклад, зловмисник, впроваджуючи заставний пристрій, створить канал зв'язку, який по відношенню до її джерела є каналом просочування інформації. Слід також відмітити, що наявність каналу витоку є необхідним, але недостатньою умовою просочування інформації. За відсутності джерела інформації і її одержувача просочування інформації немає. Аналогічно, наприклад, канал телефонного зв'язку існує постійно, але передача інформації відбувається тоді, коли абоненти на кінцях каналу зв'язку починають розмовляти.

У загальному випадку джерело сигналу виконує наступні функції:

– створює (генерує) поле (акустичне, електромагнітне) або електричний струм, які переносять інформацію;

– робить запис інформації на носій (модуляцію інформаційних параметрів носія);

– посилює потужність сигналу (носія з інформацією);

– забезпечує передачу (випромінювання) сигналу в середовище поширення в заданому секторі простору.

Запис інформації робиться шляхом зміни параметрів носія відповідно до рівня первинного сигналу, що поступає на вхід. Якщо носіями інформації є суб'єкти і матеріальні тіла (мікрочастки), то передавач відповідає первинному значенню цього слова — передавати або переносити, т. е. виконує функцію носія. У разі коли інформацію переносять сигнали(поля, електричний струм і елементарні частки), то передавачі є джерелами сигналів.

Середовище поширення носія – частина простору, в якій переміщається носій від джерела сигналу до його приймача. Середовище поширення може бути у вигляді вільного простору і направляючих ліній. В якості ліній передачі використовуються електричні дроти різної конфігурації, хвилеводи, волоконно-оптичні кабелі, звукопроводи та інші конструкції. Їх просторове положення визначає маршрут руху носія в просторі. При передачі інформації по направляючих лініях функціональних каналів зв'язку забезпечуються менші втрати енергії носія на даремне опромінення простору і велика безпека інформації, чим при поширенні носіїв у вільному просторі. Проте при цьому різко зростають витрати на створення і експлуатацію таких каналів зв'язку.

Приймач сигналу виконує функцію, зворотну функції передавача, а саме:

– вибір (селекцію) носія з потрібною одержувачеві інформацією;

– посилення прийнятого сигналу-носія до значень, що забезпечують знімання інформації;

– знімання інформації з носія (демодуляцію, декодування);

– перетворення інформації у форму сигналу, доступну одержувачеві (людині, технічному пристрою), і посилення первинних сигналів до значень, необхідних для їх сприйняття людиною і технічним пристроєм.

Якщо одержувач інформації людина, то інформація з виходу приймача має бути представлена на мові спілкування людей. Якщо технічний пристрій, то форма представлення інформації має бути зрозуміла цьому пристрою.

У середовищі можуть поширюватися носії з іншою інформацією, які по відношенню до носія з даною інформацією є перешкодами. Чим ближче ознаки носія з інформацією, що захищається, і перешкод, тим складніше приймачу їх розрізнити і тим сильніше вплив перешкод на інформацію. Наприклад, якщо частоти перешкоди і радіосигналу відрізняються на величину більше за смугу пропускання приймача, то перешкода буде пригнічена селективними ланцюгами приймача. Якщо їх частоти перетинаються, то після демодуляції перешкода накладається на сигнал, що приведе до зміни інформаційних параметрів сигналу, аж до повного руйнування інформації. Постійно зростаюча кількість сигналів в радіодіапазоні породила досить серйозну проблему їх електромагнітної сумісності.

Для санкціонованих джерел ця проблема вирішується організаційними заходами:

– законодавчим розподілом шкали радіодіапазону між різними джерелами;

– контролем за дисципліною зв'язку.

Але ці заходи погано працюють стосовно джерел перешкод. Наприклад, зростання парку автомобілів в місті підвищує насиченість ефіру перешкодами від їх систем запалення, які повністю не пригнічуються встановленими в них фільтрами. Класифікація каналів просочування інформації за різними класифікаційними ознаками дана на рис.8.

Мал. 6.2. Класифікація технічних каналів витоку інформації

Основною класифікаційною ознакою технічних каналів просочування інформації є фізична природа носія. За цією ознакою вони діляться на:

– оптичні;
– радіоелектронні;
– акустичні;
– речові.

Носієм інформації в *оптичному каналі* є електромагнітне поле (фотони) в діапазоні 0,46-0,76 мкм (видиме світло) і 0,76-13 мкм (інфрачервоні випромінювання).

У *радіоелектронному каналі* носіями витоку інформації є електричні, магнітні і електромагнітні поля в радіодіапазоні, а також електричний струм, що поширюється по металевих дротах. Діапазон коливань носія цього виду надзвичайно великий: від звукового діапазону до десятків ГГц.

Відповідно до видів носіїв інформації радіоелектронний канал доцільно розділити на 2 підвиди:

– електромагнітний *канал, носіями* інформації в якому є електричне, магнітне і електромагнітне поля;
– електричний *канал, носій* інформації в якому – електричний струм.

Носіями інформації в *акустичному каналі* є пружні акустичні хвилі в інфразвуковому (менше 16 Гц), звуковому (16 Гц-20 кГц) і ультразвуковому (понад 20 кГц) діапазонах частот, що поширюються в атмосфері, воді і твердому середовищі.

У *речовому каналі* витік інформації здійснюється шляхом несанкціонованого поширення носіїв з інформацією, що захищається, у вигляді речовини, чернеток документів і використаного копіювального паперу, забракованих деталей і вузлів, що передусім викидаються, демаскуючих речовин та ін. Демаскуючі речовини у вигляді твердих, рідких і газоподібних відходів або проміжних продуктів дозволяють визначити склад, структуру і властивості нових матеріалів або відновити технологію їх отримання. До витоку по цьому каналу віднесено несанкціоноване поширення продуктів розпаду радіоактивних речовин, виявлення і розпізнавання яких зловмисником забезпечують можливість визначення наявності і ознак радіоактивних речовин.

Коли йдеться про поширення за межі організації відходів виробництва, слід відрізняти технічний канал витоку від агентурного, у рамках якого винесення носія з інформацією робиться зловмисником, що проник до джерела, завербованим співробітником організації або співробітником, прагнучим продати інформації будь-якому її покупцеві. Межа між агентурним і каналом витоку досить умовна, проте у разі витоку інформації в агентурному каналі носієм інформації є особа, свідома виконуюча протиправні дії, а в технічному речовому каналі носії вивозяться з організації з метою

звільнення її від відходів або відходи поширюються в результаті дії природних сил. У якості таких сил можуть бути повітряні потоки, що розносять газоподібні відходи, що викидаються трубами, або водні потоки річок або водойм, куди скидаються недостатньо очищені рідкі або зважені у воді тверді частки демаскуючих речовин.

Кожен з технічних каналів має свої особливості, які необхідно знати і враховувати для забезпечення ефективного захисту інформації від її витоку.

Технічний канал витоку інформації складається з передавача, середовища поширення і приймача, є простим або одноканальним.

Проте можливі варіанти, коли витік інформації відбувається складнішим шляхом – по декількох послідовних або паралельних каналах. У цьому випадку канал можна назвати складним. При цьому використовується властивість інформації переписуватися з одного носія на інший. Наприклад, якщо в кабінеті ведеться конфіденційна розмова, то витік можливий не лише по акустичному каналу через стіни, двері, вікна, але і по оптичному – шляхом знімання інформації лазерним променем із скла вікна або по радіоелектронному з використанням встановленої в кабінеті радіозакладки. У двох останніх варіантах утворюється складний канал, створений з послідовно сполучених акустичного і оптичного (на лазерному промені) або акустичного і радіоелектронного (радіозакладка – середовище поширення радіоприймач) каналів. Такі канали коректно назвати акустооптичним і акусторадіоелектронним відповідно. Для підвищення дальності каналу витоку може також використовуватися ретранслятор, що поєднує функції приймача одного каналу витоку інформації і передавача наступного каналу. Наприклад, для підвищення дальності підслуховування з використанням радіозакладки можна розмістити ретранслятор слабкого сигналу заставного пристрою в портфелі, що здається нібито на зберігання в камеру схову закритого підприємства, а приймати і реєструвати потужніший сигнал ретранслятора на видаленні в декілька кілометрів у безпечному місці. Такий складний канал називається *акустично-радіо, електронно-радіоелектронний*.

По *частоті прояву канали* діляться на постійні і епізодичні. У *постійному каналі витік інформації носить регулярний характер.* Наприклад, наявність в кабінеті джерела небезпечного сигналу може привести до передачі мовної інформації до моменту виявлення цього джерела. Регулярність отримання інформації через такий канал робить його дуже цінним. Тому розвідка дорожить регулярним джерелом інформації і захищає його від контррозвідки. До *епізодичних каналів відносяться канали, витік інформації в яких має короткочасний, часто випадковий характер.*

За *способом створення канали витоку* можуть бути спеціально організовані і випадкові. *Організовані канали* створюються зловмисником для регулярного добування інформації. Наприклад, для підслуховування на великій відстані від джерела мовної інформації організовується канал витоку з приміщення шляхом розміщення в ньому заставного пристрою. Характеристики (частота випромінювання, вид модуляції, потужність передавача та ін.) цього каналу відомі зловмисникові. Ці знання дозволяють йому безперервно або в певний час прослуховувати усі розмови, що ведуться в приміщенні.

Побічні електромагнітні випромінювання і наведення створюють передумови для утворення випадкових каналів просочування інформації, параметри яких апріорі зловмисникові не відомі. Якщо йому вдасться настроїти свій приймач на частоту побічного випромінювання, то виникає випадковий канал витоку інформації. Такий канал може бути дуже інформативним, але випадковий характер його освіти і часу роботи (коли включений випромінюючий технічний засіб) знижує його корисність для зловмисника.

По технічному каналу витоку інформація може передаватися не лише у відкритому виді, вона може бути і закритою. З метою підвищення скритності сигнал на виході перспективних заставних пристроїв закривається, а канал витоку, що використовує ці пристрої, є технічно закритим. При перехопленні функціональних каналів зв'язки, по

яких передається шифрована інформація, утворюється шифрований канал просочування інформації.

Можливості передачі інформації по технічних каналах залежить від багатьох чинників: енергії сигналу, міри його послаблення в середовищі поширення, чутливості і роздільної здатності приймача зловмисника, рівня перешкод в каналі та ін.