Завдання №5

# Об’єкти захисту інформації (ЗІ) та технічні канали її витоку

**Основними об’єктами захисту інформації є**:

**1**- інформаційні ресурси, котрі несуть у собі відомості, що можуть відноситись до державної таємниці та конфіденційної інформації:

**2**- системи та засоби інформатизації (засоби обчислювальної техніки, інформаційно-обчислювальні комплекси, мережі та системи); програмні засоби (операційні системи, системи керування базами даних та інше загальносистемне та прикладне програмне забезпечення), автоматизовані системи керування, системи зв’язку та передачі даних, технічні засоби отримання, передавання та обробки інформації з обмеженим доступом (звукозапис, звукопідсилення, звукосупроводження, переговорні та телевізійні пристрої, засоби тиражування та виготовлення документів та інші технічні засоби обробки графічної, алфавітно-цифрової та змістовної інформації), їх інформативні фізичні поля. Ці засоби часто називають **технічними засобами прийому, обробки, зберігання та передавання інформації (ТЗПІ).**

**3** - технічні засоби і системи, котрі не відносять до засобів та систем автоматизації (ТЗПІ), але розташовані в приміщеннях де оброблюється таємна і конфіденційна інформація. Такі засоби і системи називають **допоміжними технічними засобами і системами (ДТЗС)**. До них відносяться технічні засоби відкритого телефонного, гучномовного зв’язку, системи пожежної та охоронної сигналізації, система енергопостачання, радіотрансляційна мережа, системи часофікації, енергопобутові прилади і т.д., а також самі приміщення, де оброблюється інформація обмеженого поширення.

# Захист каналів зв’язку

При організації захисту інформації ТЗПІ слід розглядати як систему, що включає до свого складу основне (стаціонарне) обладнання, кінцеві пристрої, з’єднувальні лінії (сукупність дротів та кабелів, що прокладені між окремими ТЗПІ та їх елементами), розподіляючі та комунікаційні пристрої, системи електроживлення, заземлення.

Окремі технічні засоби або група технічних засобів, що призначаються для обробки конфіденційної інформації, разом з приміщенням, де вони розташовані, складають **об’єкт ТЗПІ**. Під об’єктом ТЗПІ розуміють також виділені приміщення, що призначені для проведення секретних заходів.

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 розсередженими.

**Зосереджена випадкова антена** представляє собою компактний технічний засіб, наприклад телефонний апарат, гучномовець радіотрансляційної мережі і т. п. До **розсереджених випадкових антен** відносять випадкові антени з розсередженими 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 гасові, 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).

Захист інформації від витоку по технічних каналах досягається проектно-архітектурними рішеннями, **проведенням організаційних і технічних** заходів, а також **виявленням портативних закладних пристроїв**.

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.;

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”).

Виявлення закладних пристроїв здійснюється проведенням спеціальних досліджень та спеціальних перевірок об’єктів ТЗПІ та виділених приміщень.

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.

# Пасивні та активні методи ЗІ

**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 наведень 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;

# Принципи витоку інформації по телефонних каналах зв’язку

В *вібраційних (віброакустичних) технічних каналах витоку інформації* середовищем розповсюдження акустичних сигналів є конструктивні елементи споруд і будівель (стіни, перетини, підлога), труби водопостачання, каналізації та інші тверді тіла.

Для перехоплення акустичних коливань в цьому випадку використовують засоби розвідки з контактними мікрофонами:

- електронні стетоскопи;

**-** радіостетоскопи з передаванням інформації по радіоканалу**.**

Телефонний канал витоку інформації для підслуховування телефонних переговорів (в рамках промислового шпигунства) можливий:

гальваничний зйом телефонних переговорів (шляхом контактного підключення підслуховуючих пристроїв в будь-якому місці абонентської телефонної мережі). Визначається шляхом погіршення чутності і появи перешкод, а також за допомогою спеціальної апаратури; телефонно-локаційних спосіб (шляхом високочастотного нав'язування). По телефонній лінії подається високочастотний сигнал, який впливає на нелінійні елементи телефонного апарату (діоди, транзистори, мікросхеми) на які також впливає акустичний сигнал. В результаті в телефонній лінії формується високочастотний модульований сигнал. Виявити підслуховування можливо за наявністю високочастотного сигналу в телефонній лінії. Однак дальність дії такої системи через загасання ВЧ сигналу в двухпровідній лінії не перевищує ста метрів. Можлива протидія: придушення в телефонній лінії високочастотного сигналу;

індуктивний і ємнісний спосіб негласного знімання телефонних переговорів (безконтактне підключення).

Індуктивний спосіб — за рахунок електромагнітної індукції, що виникає в процесі телефонних переговорів уздовж дроту телефонної лінії. В якості приймального пристрою знімання інформації використовується трансформатор, первинна обмотка якого охоплює один або два дроти телефонної лінії.

Ємнісний спосіб — за рахунок формування на обкладках конденсатора електростатичного поля, що змінюється відповідно до зміни рівня телефонних переговорів. В якості приймального пристрою телефонних переговорів використовується ємнісний датчик, виконаний у вигляді двох пластин, щільно прилеглих до дротів телефонної лінії.

Підслуховування розмов в приміщенні з використанням телефонних апаратів можливо наступними способами: низькочастотний і високочастотний спосіб знімання акустичних сигналів і телефонних переговорів. Даний спосіб заснований на підключенні до телефонної лінії підслуховуючих пристроїв, які перетворені мікрофоном звукові сигнали передають по телефонній лінії на високій або низькій частоті. Дозволяють прослуховувати розмову як при піднятою, так і при опущеною телефонній трубці. Захист здійснюється шляхом відсікання в телефонній лінії високочастотної і низькочастотної складової; використання телефонних дистанційних підслуховуючих пристроїв. Даний спосіб ґрунтується на установці дистанційного пристрою для підслуховування в елементах абонентської телефонної мережі шляхом паралельного підключення його до телефонної лінії і дистанційним включенням. Пристрій має дві властивості, за якими можна його визначити: в момент підслуховування телефонний апарат абонента вимкнений від телефонної лінії, а також при встановленій телефонній трубці і включеному підслуховуючому пристрої напруга живлення телефонної лінії становить менше 20 Вольт, в той час як вона повинна складати 60.