завдання №5

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

Канали витоку інформації — методи та шляхи витоку інформації з інформаційної системи; паразитний (небажаний) ланцюжок носіїв інформації, один або кілька з яких є (можуть бути) правопорушником або його спеціальною апаратурою.

Відіграють основну роль у захисті інформації, як фактор інформаційної безпеки.

Технічні канали витоку інформації

2.1 Акустичний канал

2.2 Канал акустичної потужності

2.3 Віброакустичний канал (телефонний)

2.4 Оптичний канал

Приклади непрямих каналів витоку:

основними об’єктами захисту інформації є:

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

- системи та засоби інформатизації; програмні засоби, автоматизовані системи керування, системи зв’язку та передачі даних, технічні засоби отримання, передавання та обробки інформації з обмеженим доступом, їх інформативні фізичні поля.

- технічні засоби і системи, котрі не відносять до засобів та систем автоматизації, але розташовані в приміщеннях де оброблюється таємна і конфіденційна інформація.

при організації захисту інформації тзпі слід розглядати як систему, що включає до свого складу основне обладнання, кінцеві пристрої, з’єднувальні лінії, тощо

Технічні засоби промислового шпигунства

засоби акустичного контролю;

апаратура для знімання інформації з вікон;

спеціальна звукозаписуюча апаратура;

мікрофони різного призначення і виконання;

електромережеві підслуховуючі пристрої;

прилади для знімання інформації з телефонної лінії зв'язку і стільникових телефонів;

спеціальні системи спостереження і передачі відеозображень;

спеціальні фотоапарати;

прилади спостереження в денний час і прилади нічного бачення;

спеціальні засоби радіоперехоплення і прийому побічного електромагнітного випромінювання і наведення;

Технічні засоби знімання інформації можуть бути впроваджені «противником» наступними способами:

установка засобів знімання інформації в захисні конструкції приміщень під час будівельних, ремонтних і реконструкційних робіт;

установка засобів знімання інформації в предмети меблів, інші предмети інтер'єру та побуту, різні технічні засоби як загального призначення, так і призначені для обробки інформації;

установка засобів знімання інформації в предмети побуту, які вручаються в якості подарунків, а згодом можуть використовуватися для оформлення інтер'єру службових приміщень;

установка засобів знімання інформації в ході профілактики інженерних мереж і систем. При цьому в якості виконавця можуть бути використані навіть співробітники ремонтних служб.

# захист каналів зв’язку

Правові

Захист інформації від витоку по технічним каналам здійснюється на основі конституцій і законів, а також захист забезпечується наявністю авторських свідоцтв, патентів, товарних знаків.

В Україні існує стандарт, який встановлює класифікацію і перелік факторів, що впливають на конфіденційну інформацію, в інтересах обґрунтування вимог захисту інформації на об'єкті інформатизації. Цей стандарт поширюється на вимоги щодо організації захисту інформації при створенні та експлуатації об'єктів інформатизації, які використовуються в різних галузях діяльності (оборони, економіки, науки та інших областях).

Організаційні

Забезпечується сукупністю положень про Службу безпеки і планами роботи цієї служби. Плани заходів служби безпеки охоплюють широке коло питань, зокрема: а) на ранній стадії при проектуванні приміщень і будівництві Служба безпеки розглядає наступні питання: виділення приміщень для нарад і переговорів (в такому приміщенні робиться спеціальні перекриття і канали повітряної вентиляції, окремі кімнати екранують і так далі); зручність контролю приміщень, людей, транспорту; створення виробничих зон за типом конфіденційності робіт з самостійним додатковим допуском;

б) служба безпеки бере участь в підборі персоналу з перевіркою їх якостей на підставі особистих бесід (вивчення трудової книжки, отримання інформації з інших місць роботи; потім приймається на роботу ознайомлюється з правилами роботи з конфіденційною інформацією і порядком відповідальності);

в) служба безпеки готує положення і здійснює: організацію пропускного режиму; організацію охорони приміщень і територій; організацію зберігання і використання документів, порядок обліку, зберігання, знищення документів, планові перевірки.

Інженерно-технічні

Захист включає в себе: апаратні засоби захисту; програмні засоби захисту — це використання спеціальних програм в системах, засобах і мережах обробки даних; математичні методи захисту — застосування математичних і криптографічних методів з метою захисту конфіденційної інформації (без знання ключа неможливо дізнатися і розшифрувати вкрадену інформацію).

# пасивні та активні методи зі

Пасивні засоби особистої безпеки

1. Різні накладки (шоломи, каски, наколінники і т.д.)

2. Бронежилети

3. Індивідуальні пояси безпеки або "пояса вірності ".

Активні засоби самозахисту

У наш час з'явилося багато різних засобів захисту, але для щоб з їхньою допомогою реально убезпечити себе й своїх близьких треба орієнтуватися в типах, видах, перевагах і недоліках існуючих засобів захисту, тому що пропоновані засоби можуть бути

- неефективними

- забороненими

- не сертифікованими

- ненадійними

- просто підробками

- незручними (складними в застосуванні) і т.д.

# принципи витоку інформації по телефонних каналах зв’язку

в *вібраційних 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.