Навчально-методичне видання

В.Д. Козюра,
В.О. Хорошко, М.Є. Шелест,
Ю.М. Ткач, Я.Ю. Усов

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Навчальний посібник

В авторській редакції

Відповідальний за випуск – *Лук'яненко В.В.*

Підписано до друку 26.04.2019 р.
Формат 60х 84/16. Папір офсетний. Друк числовий.
Гарнітура Times New Roman. Обл.-вид. арк. 8,32.
Ум. друк. арк. 8,49. Тираж 300 прим.
Зам. № 566.

Віддруковано з оригінал-макету замовника

Видавець - ФОП Лук'яненко В.В. ТПК «Орхідея»

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції серія ДК № 3020 від 02.11.2007 р.

16600, Чернігівська обл., м. Ніжин, вул. Небесної сотні, 13 а.
Тел.: 068 815 06 60
E-mail: holdingvv@ gmail.com

В.Д. Козюра,
В.О. Хорошко, М.Є. Шелест,
Ю.М. Ткач, Я.Ю. Усов

КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Навчальний посібник

Ніжин
2019

УДК 004.891:65.012.8
К -63

Рекомендовано до друку вченою радою Чернігівського національного технологічного університету (протокол № 3 від 25 березня 2019 року)

РЕЦЕНЗЕНТИ:

О.Г. Корченко – завідувач кафедри безпеки інформаційних технологій НАУ д.т.н., професор, лауреат Державної премії України в галузі науки і техніки

Ю.Є.Яремчук – директор Центру інформаційних технологій і захисту інформації Вінницького національного технологічного університету, д.т.н., професор

С.В. Зайцев – завідувач кафедри інформаційних та комп'ютерних систем ЧНТУ д.т.н., доцент

К - 63 **Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах**: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.

ISBN 978-617-7609-30-7

У навчальному посібнику розглядаються основи організації та порядок виконання робіт із захисту інформації в інформаційно-телекомунікаційних системах, порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

УДК 004.891:65.012.8

ISBN 978-617-7609-30-7

Для нотаток

19. Куприянов А.И. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ: учеб. пособие для студ. высш.учеб. заведений / А.И.Куприянов, А.В.Сахаров, В.А.Шевцов. – М.: Изд. центр «Академия», 2006. – 256 с.

20. Ленков С.В. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ТОМ I. НЕСАНКЦИОНИРОВАННОЕ ПОЛУЧЕНИЕ ИНФОРМАЦИИ / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко; под ред. В.А.Хорошко. – К.: Арий, 2008. – 464 с.

21. Ленков С.В. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ. ТОМ II. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / С.В.Ленков, Д.А.Перегудов, В.А.Хорошко; под ред. В.А.Хорошко. – К.: Арий, 2008. – 344 с.

22. Макнамара Д. СЕКРЕТЫ КОМПЬЮТЕРНОГО ШПИОНАЖА: ТАКТИКА И КОНТРМЕРЫ / Д.Макнамара; пер. с англ.; под ред. С.М.Молявко. – М.: БИНОМ. Лаборатория знаний, 2004. – 536 с.

23. Мельников В.П. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ: учеб. пособие для студ. высш. учеб. заведений / В.П.Мельников, С.А.Клейменов, А.М.Петраков; под. ред. С.А.Клейменова. – 3-е изд., стер. – М.: Изд. центр «Академия», 2008. – 336 с.

24. Меньшаков Ю.К. ОСНОВЫ ЗАЩИТЫ ОТ ТЕХНИЧЕСКИХ РАЗВЕДОК: учеб. пособие / Ю.К.Меньшаков; под общ. ред. М.П.Сычева. – М.: Изд. МГТУ им. Н.Э.Баумана, 2011. – 478 с.

25. ОРГАНИЗАЦИЯ И СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ / под общ. ред. С.А.Диева, А.Г.Шаваева. – М.: Концерн «Банковский Деловой Центр», 1998. – 472 с.

26. Соболев А.Н. ФИЗИЧЕСКИЕ ОСНОВЫ ТЕХНИЧЕСКИХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: Учебное пособие / А.Н.Соболев, Кириллов В.М. – М.: Гелиос АРВ, 2004. – 224 с.

27. Торокин А.А. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ: Учебное пособие для студентов высших учебных заведений / А.А.Торокин. – М.: «Гелиос АРВ», 2005. – 960 с.

28. Фейнштайн К. ЗАЩИТА ПК ОТ СПАМА, ВИРУСОВ, ВСПЛЫВАЮЩИХ ОКОН И ШПИОНСКИХ ПРОГРАММ (Самоучитель) / К.Фейнштайн; пер. с англ. О.Б.Вереиной. – М.: НТ Пресс, 2005. – 240 с.

29. Халяпин Д.Б. ЗАЩИТА ИНФОРМАЦИИ. ВАС ПОДСЛУШИВАЮТ? ЗАЩИЩАЙТЕСЬ! – М.: НОУ ШО «Баярд», 2004. – 432 с.

30. Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие / А.А.Хорев. – М.: Гостехкомиссия России, 1998. – 320 с.

31. Шаньгин В.Ф. ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ / В.Ф.Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

32. Ярочкин В.И. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебник для студентов вузов, 2 -е изд. / В.И.Ярочкин. – М.: Академический Проект; Гаудеамус, 2004. – 544 с.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

DoS – *Denial-of-Service*, атака «відмова в обслуговуванні»
DDoS – *Distributed DoS*, розподілена атака «відмова в обслуговуванні»
PDCA – *Plan*, *Do*, *Check*, *Act*, Плануй, Здійснюй, Перевіряй, Дій
АС – автоматизована система
АРМ – автоматизоване робоче місце
БД – база даних
ДБН – державні будівельні норми
ДСТУ – державний стандарт України
ДТ – державна таємниця
ДТЗ – допоміжні технічні засоби
ЕОМ – електронна обчислювальна машина
ЕОТ – електронна обчислювальна техніка
ЕСКД – єдина система конструкторської документації
ЕСПД – єдина система програмної документації
ЗОТ – засоби обчислювальної техніки
ІБ – інформаційна безпека
ІзОД – інформація з обмеженим доступом
ІС – інформаційна система
ІТ – інформаційна технологія
ІТС – інформаційно-телекомунікаційна система
КЗІ – криптографічний захист інформації
КЗЗ – комплекс засобів захисту
КС – комп'ютерна система
КСЗІ – комплексна система захисту інформації
ЛОМ – локальна обчислювальна мережа
НД – нормативний документ
НД ТЗІ – нормативний документ з технічного захисту інформації
НДР – науково-дослідна робота
НСВ – несанкціонований силовий вплив
НСД – несанкціонований доступ
ОІД – об'єкт інформаційної діяльності
ОпС – операційна система
ОС – обчислювальна система
ОТЗ – основні технічні засоби
ПЕМВН – побічне електромагнітне випромінення і наведення
ПЕОМ – персональна електронна обчислювальна машина
ПЗ – програмне забезпечення
ПЗП – постійний запам'ятовуючий пристрій
ПК – персональний комп'ютер
ПМА – програма і методи атестації
ПРД – правила розмежування доступу
РД – керівний документ
РСО – режимно-секретний орган
СлЗІ – служба захисту інформації
СЗІ – система захисту інформації
СРД – система розмежування доступу
СКБД – система керування базами даних
СУІБ – система управління інформаційною безпекою
ТЗ – технічне завдання
ТЗІ – технічний захист інформації
ТР – тимчасові рекомендації
ТС – телекомунікаційна система
ЦП – центральний процесор

ПОЗНАЧЕННЯ ПОСЛУГ
Конфіденційності:
КД – довірча конфіденційність
КА – адміністративна конфіденційність
КО – повторне використання об'єктів
КК – аналіз прихованих каналів
КВ – конфіденційність при обміні
Цілісності:
ЦД – довірча цілісність
ЦА – адміністративна цілісність
ЦО – відкат
ЦВ – цілісність при обміні
Доступності:
ДР – використання ресурсів
ДС – стійкість до відмов
ДЗ – гаряча заміна
ДВ – відновлення після збоїв
Спостереженості:
НР – реєстрація
НИ – ідентифікація и автентифікація
НК – достовірний канал
НО – розподіл обов'язків
НЦ – цілісність КЗЗ
НТ – самотестування
НВ – автентифікація при обміні
НА – автентифікація відправника
НП – автентифікація одержувача

ЛІТЕРАТУРА

1. Андреев В.І. СТРАТЕГІЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: підручник / В.І.Андреев, В.Д.Козюра, Л.М.Скачек, В.О.Хорошко. – К.: Вид. ДУІКТ, 2007. – 277 с.
2. Бармен С. РАЗРАБОТКА ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ / С.Бармен, пер. с англ. – М.: ИД «Вильямс», 202. – 208 с.
3. Белов Е.Б. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебное пособие для вузов / Е.Б.Белов, В.П.Лось, Р.В.Мещеряков, А.А.Шлепанов. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 544 с.
4. Блавацька Н.М. ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ: підручник / Н.М.Блавацька, В.Д.Козюра, В.О.Хорошко. – К.: Вид. ДУІКТ, 2011. – 330 с.
5. Бузов Г.А. ЗАЩИТА ОТ УТЕЧКИ ИНФОРМАЦИИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ: Учебное пособие для студентов высших учебных заведений / Г.А.Бузов, С.В.Калинин, А.В.Кондратьев. – М.: «Горячая линия – Телеком», 2005. – 416 с.
6. Гайворонський М.В. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ / М.В.Гайворонський, О.М.Новиков. - К.: Видавнича група BHV, 2009. - 608 с.
7. Галатенко В.А. СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: курс лекций: учебное пособие. Второе издание / В.А.Галатенко; под ред. академика РАН В.Б.Бетелина. – М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. – 264 с.
8. Грибунин В.Г. КОМПЛЕКСНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ: учеб. пособие для студ. высш. учеб. заведений / В.Г.Грибунин, В.В.Чудовский. – М.: Издательский центр «Академия», 2009. – 416 с.
9. Гришина Н.В. ОРГАНИЗАЦИЯ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ / Н.В.Гришина. – М.: Гелиос АРВ, 2007. – 256 с.
10. Довгань О.Д. МЕТОДОЛОГІЯ ЗАХИСТУ ІНФОРМАЦІЇ: навч.-метод. посіб. / О.Д.Довгань, Г.М.Гулак, А.К.Гринь, С.В.Мельник. – К.: Наук.-вид. центр НА СБ України, 2012. – 184 с.
11. Емельянова Н.З. ЗАЩИТА ИНФОРМАЦИИ В ПЕРСОНАЛЬНОМ КОМПЬЮТЕРЕ: учебное пособие / Н.З.Емельянова, Т.Л.Партыка, И.И.Попов. – М.: ФОРУМ, 2009. – 368 с.
12. Железняк В.К. ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ: учебное пособие / В.К.Железняк. – СПб.: ГУАП., 2006. – 188 с.
13. Завгородний В.И. КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ: Учебное пособие / В.И.Завгородний. – М.: Логос; ПБОЮЛ Н.А.Егоров, 2001. – 264 с.
14. Зайцев А.П. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: Учебное пособие. Изд. 2-е испр. и доп. / А.П.Зайцев, И.В.Голубятников, Р.В.Мещеряков, А.А.Шелупанов. – М.: Машиностроение-1, 2006. − 260 с.
15. Зайцев А.П. ТЕХНИЧЕСКИЕ СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ: Учебник для вузов / А.П.Зайцева, А.А.Шелупанов, Р.В.Мещеряков и др.; под ред. А.П.Зайцева и А.А.Шелупанова. – М.: ООО «Издательство Машиностроение», 2009. – 508 с.
16. Коженевский С.Р. ТЕРМІНОЛОГІЧНИЙ ДОВІДНИК З ПИТАНЬ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ / С.Р.Коженевский, Г.В.Кузнецов, В.О.Хорошко, Д.В.Чирков; за ред. проф. В.О.Хорошка. – К.: Вид. ДУІКТ, 2007. – 365 с.
17. Конахович Г.Ф. ЗАЩИТА ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ / Г.Ф.Конахович, В.П.Климчук, С.М.Паук, В.Г.Потапов. – К.: «МК-Пресс», 2005. – 288 с.
18. Конеев И.Р. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ / И.Р.Конеев, А.В.Беляев. – СПб.: БХВ-Петербург, 2003. – 752 с.

2. Канали витоку інформаціє можуть виникати внаслідок випромінювання інформативних сигналів під час роботи ОТЗ і внаслідок наведення цих сигналів у лініях зв'язку, колах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території. Інформативні сигнали можуть поширюватися на великі відстані і реєструватися засобами технічних розвідок за межами контрольованої зони.

3. Роботи з технічного захисту інформації (ТЗІ) в ІТС передбачають: категоріювання об'єктів електронно-обчислювальної техніки; включення до технічних завдань на монтаж ІТС розділу з ТЗІ; монтаж ІТС відповідно до рекомендацій НД ТЗІ; обстеження (в тому числі технічний контроль) об'єктів ЕОТ; установлення (при необхідності) атестованих засобів захисту; технічний контроль за ефективністю вжитих заходів.

Контрольні питання

1. Що таке виток інформації і за рахунок чого він утворюється?
2. Що є технічним каналом витоку інформації і які види каналів витоку існують?
3. Якими способами і із застосуванням яких засобів реалізується оптичний канал витоку інформації?
4. Якими способами і із застосуванням яких засобів реалізується акустичний канал витоку інформації?
5. За рахунок чого утворюються канали витоку інформації при її обробці в ІТС?
6. Що необхідно виконати на етапі проведення організаційних заходів по технічному захисту інформації?
7. Що в себе включають підготовчі технічні заходи?
8. У чому сенс технічних заходів, пов'язаних із захистом інформації?
9. Як здійснюється контроль за станом технічного захисту інформації?
10. Що визначається в процесі спецдосліджень?

ВСТУП

Будь-яка інформація, незалежно від того, чи є вона власністю держави, всього суспільства або окремих організацій чи фізичних осіб, становить певну цінність. Відтак інформаційні ресурси потребують захисту від різних впливів, які можуть призвести до зниження їхньої цінності.

Здавна люди розв'язували питання захисту інформації, переважно – державних і військових таємниць. Завдання захисту були досить типовими і не змінювалися протягом тисячоліть: забезпечити передавання інформації від достовірного джерела вповноваженій особі так, щоб вона не потрапила до інших осіб. Для цього використовували різні методи захисту. Деякі з них із незначними змінами застосовують і зараз, коли, наприклад, підтверджують справжність документа особистою печаткою.

У XX столітті правила роботи з таємною інформацією, способи її зберігання, передавання, а також методи ведення розвідки з метою здобуття такої інформації не уповноваженими (ворожими) особами зазнали суттєвих змін через бурхливий розвиток технічних засобів, що використовували як для захисту інформації, так і для подолання цього захисту. Наприкінці XX століття було здійснено чергову технічну революцію, яка стосувалася саме технологій підготовки, зберігання, пошуку, оброблення та розповсюдження інформації. Йдеться про масове застосування комп'ютерної техніки, що стала загальнодоступною, а також про об'єднання комп'ютерів у мережі, які досягли глобального масштабу. В результаті виникли і набули поширення розподілені інформаційні системи, які дістали назву інформаційно-комунікаційних систем.

Комп'ютерна технологія оброблення інформації несе в собі певні загрози, які можуть призвести до небажаних втрат або тимчасової недоступності важливих даних. У контексті інформаційно-комунікаційних систем слід згадати системи зберігання даних, надійність яких власники інформації інколи переоцінюють. Але є й менш очевидні проблеми. Зокрема, це можливість існування шкідливого і навіть руйнівного програмного забезпечення. Прикладні програ-

ми можуть містити приховані функції, неописані в документації, що з'явилися в програмному коді через недбалість програмістів або навмисно. Такі функції можуть бути активізовані випадково або за певних умов. Одним із найпоширеніших і найнебезпечніших різновидів шкідливого програмного забезпечення є комп'ютерні віруси, здатні розмножуватись і розповсюджуватись.

Завдяки комплексному підходу можливо знайти компромісне рішення щодо відношення сукупної вартості володіння кінцевою інформаційною системою до комплексу загроз інформації, яка в ній циркулює. Ця мета досягається завдяки збалансованому розвитку технічних засобів захисту у сукупності із вдосконаленням законодавчої та нормативної бази. Отже, задачі захисту інформації в інформаційно-комунікаційній системі є суперпозицією задач двох головних напрямів:

- захист важливої інформації, зокрема державної, військової або комерційної таємниці від цілеспрямованих дій порушників;
- захист інформації від впливів, спричинених некоректним функціонуванням комп'ютерної системи через відмови обладнання, збоїв програмного забезпечення, помилки в реалізації апаратних або програмних засобів, або наявність програмних засобів з прихованими руйнуючими властивостями.

Автори висловлють щиру подяку ….

за уважне та доброзичливе рецензування і висловлені зауваження та поради, які сприяли значному покращенню навчального посібника.

безпечних) сигналів у широкому діапазоні частот навколо апаратури та кабельних з`єднань ОТЗ, наявність інформативних (небезпечних) сигналів у колах, проводах електроживлення та заземленні ТЗОІ та ДТЗС.

Під час спецдосліджень визначається радіус, за межами якого відношення «інформативний сигнал/шум» менше гранично допустимої величини.

Проводяться вимірювання і розрахунок параметрів інформативного (небезпечного) сигналу, виявляється можливість його витоку каналами ПЕМВН, визначаються фактичні значення його параметрів у каналах витоку, проводиться порівняння фактичних параметрів з нормованими.

У випадку перевищення допустимих значень розробляються захисні заходи, використовуються засоби захисту (екранування джерел випромінювання, встановлення фільтрів, стабілізаторів, засобів активного захисту).

Після проведення спецдосліджень, вироблення та впровадження засобів захисту проводиться контроль за ефективністю застосованих технічних засобів захисту.

У процесі роботи технічних засобів і захищеної техніки, у міру необхідності, проводиться оперативний контроль за ефективністю захисту каналів витоку інформативного (небезпечного) сигналу.

Результати контролю (спецдосліджень) оформляються **актом**, складеним у довільній формі, підписуються перевіряючим та затверджуються керівником організації.

Висновки

1. Технічному захисту підлягає інформація з обмеженим доступом, яка обробляється, циркулює, відображається в автоматизованих системах і засобах обчислювальної техніки. Носіями цієї інформації є електричні й електромагнітні поля і сигнали, що утворюються в результаті роботи засобів оброблення ІзОД (основні технічні засоби) або впливу небезпечного сигналу на засоби оброблення відкритої інформації, на засоби і системи життєзабезпечення (допоміжні технічні засоби і системи).

Технічний канал витоку вважається *захищеним*, якщо сигнал не перевищує встановленого нормативною документацією відношення «інформативний сигнал/шум». Пристрої захисту і захищені технічні засоби вважаються справними, якщо їх параметри відповідають вимогам експлуатаційнихдокументів.

Контроль за виконанням організаційних та підготовчих технічних заходів щодо захисту інформації здійснюється візуальним оглядом прокладки проводів і кабелів, що виходять за межі об`єкта захисту, а також технічних засобів захисту та захищеної техніки.

У ході перевірки визначаються:

- наявність електромагнітного зв`язку між лініями ОТЗ та ДТЗС (проходження в одному кабелі або жгуті), між різними видами ТЗОІ та ДТЗС;
- наявність виходів ліній зв`язку, сигналізації, годинофікації, радіотрансляції за межі виділених приміщень;
- наявність незадіяних ТЗОІ, ДТЗС, проводів, кабелів;
- можливість відключення ТЗПІ на період проведення конфіденційних переговорів або важливих нарад;
- рознесення джерел електромагнітних та акустичних полів на максимально можливу відстань у межах виділених приміщень;
- виконання заземлення апаратури, яке виключає можливість утворення петель з проводів та екранів;
- рознесення кабелів електроживлення ОТЗ та ДТЗС з метою виключення наводок небезпечних сигналів;
- виконання розведення кіл електроживлення екранованим або крученим кабелем;
- наявність можливості відключення електроживлення ОТЗ під час обезструмлення мережі; відхилення параметрів електроживлення від заданих норм, під час появи несправностей у колах живлення.

У процесі проведення спецдосліджень, перевірки ефективності технічних заходів захисту підлягають інструментальному контролю ОТЗ і лінії зв`язку.

У ході контролю перевіряються електромагнітні поля інформативних (не-

1. Концепція інформаційної безпеки

Інформація – це відомості про осіб, предмети, факти, події, явища і процеси незалежно від форми їх представлення.

Інформація може мати різну форму (дані, закладені в комп'ютерах, кресленнях, пам'ятних записках, досьє, формулах, діаграмах, моделях продукції, дисертаціях, судових документах тощо).

Інформація має *споживачів*, що потребують її, і тому має певні споживчі якості, а також має і своїх *володарів* або *виробників*.

З точки зору споживача, якість використовуваної інформації дозволяє отримувати додатковий економічний або моральний ефект.

З точки зору власника – збереження в таємниці комерційно-важливої інформації дозволяє успішно конкурувати на ринку виробництва, збуту товарів і послуг. Це природньо вимагає певних дій, спрямованих на захист конфіденційної інформації.

Основні **концептуальні положення** системи захисту інформації:

1. *Забезпечення безпеки інформації не може бути одноразовим актом*. Це безперервний процес, що полягає в обгрунтуванні і реалізації найбільш раціональних методів, способів і шляхів вдосконалення і розвитку системи захисту, безперервному контролі її стану, виявленні її вузьких і слабких місць і протиправних дій.

2. *Безпека інформації може бути забезпечена лише при комплексному використанні усього арсеналу наявних засобів захисту в усіх структурних елементах організації і на усіх етапах технологічного циклу обробки інформації*. Найбільший ефект досягається тоді, коли усі використовувані засоби, методи і заходи об'єднуються в єдиний цілісний механізм – систему захисту інформації (СЗІ). При цьому функціонування системи повинне контролюватися, оновлюватися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов. Ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними усіх встановлених правил, спрямованих на її захист.

Система захисту інформації (СЗІ) – це організована сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Захист інформації має бути:

- *безперервним* (зловмисники тільки і шукають можливість, як би обійти захист інформації, що цікавить їх);
- *плановим* (кожна служба розроблює детальні плани захисту інформації у сфері її компетенції з урахуванням спільної мети організації);
- *цілеспрямованим* (захищається те, що повинно захищатися в інтересах конкретної мети, а не усе підряд);
- *конкретним* (захисту підлягають конкретні дані, що об'єктивно підлягають охороні, втрата яких може заподіяти організації певний збиток);
- *активним* (захищати інформацію необхідно з достатньою мірою наполегливості);
- *надійним* (методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до секретів, що охороняються, незалежно від форми їх представлення, мови вираження і виду фізичного носія на якому вони закріплені);
- *універсальним* (залежно від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати де б він не проявився, розумними і достатніми засобами, незалежно від характеру, форми і виду інформації);
- *комплексним* (для захисту інформації повинні застосовуватися усі види і форми захисту в повному об'ємі. Неприпустимо застосовувати лише окремі форми або технічні засоби).

Комплексний характер захисту виникає з того, що захист – це специфічне явище, що є складною системою нерозривно взаємозв'язаних і взаємозалежних процесів, кожен з яких у свою чергу має безліч різних сторін, які взаємно обумовлюють один одного, властивостей, тенденцій.

Для забезпечення виконання цих вимог безпеки СЗІ повинна задовольнятися певними **умовами**:

Заземлення ОТЗ слід здійснювати від загального контуру заземлення, розміщеного в межах контрольованої території, з опором заземлення за постійним струмом відповідно до вимог стандартів.

Система заземлення повинна бути єдиною для всіх елементів ОТЗ і будуватися за радіальною схемою. Утворення петель і контурів у системі заземлення не допускається.

Екрани кабельних ліній ТЗОІ, що виходять за межі контрольованої території, повинні заземлятися в кросах від загального контуру заземлення в одній точці для виключення можливості утворення петель по екрану та корпусах.

У кожному пристрої повинна виконуватися умова безперервності екрана від входу до виходу. Екрани слід заземляти тільки з одного боку. Екрани кабелів не повинні використовуватися як другий провід сигнального кола або кола живлення.

Екрани кабелів не повинні мати електричного контакту з металоконструкціями. Для монтажу слід застосовувати екрановані кабелі з ізоляцією або одягати на екрани ізоляційну трубку.

У довгих екранованих лініях (мікрофонних, лінійних, звукопідсилювальних) рекомендується ділити екран на ділянки для одержання малих опорів для високочастотних струмів і кожну ділянку заземляти тільки з одного боку.

Результати виконання технічних заходів оформляються **актом приймання робіт**, складеним у довільній формі, підписуються виконавцем робіт і затверджуються керівником організації.

Порядок контролю за станом технічного захисту інформації

Мета контролю:

1) Виявлення можливих технічних каналів витоку інформативного (небезпечного) сигналу (проведення спецдосліджень).
2) Вироблення заходів, що забезпечують його приховування.
3) Оцінка достатності й ефективності вжитих заходів захисту.
4) Оперативний контроль за станом технічного захисту каналів витоку інформативного сигналу.

шувати працездатність технічного засобу і погіршувати його технічні параметри.

Високочастотні автогенератори, підсилювачі (мікрофонні, приймання, пересилання, гучномовного зв`язку) та інші пристрої, що містять активні елементи, рекомендується відключати від ліній електроживлення у «черговому режимі» або «режимі чекання виклику».

Підключення пристроїв захисту слід проводити без порушення або зміни електричної схеми ТЗОІ і ДТЗС.

Захист ІзОД від витоку кабелями та проводами рекомендується здійснювати шляхом:

- застосування екранувальних конструкцій;
- роздільного прокладання кабелів ОТЗ та ДТЗС.

При неможливості виконання вимог щодо рознесення кабелів електроживлення ОТЗ та ДТЗС електроживлення останніх слід здійснювати або екранованими кабелями, або від розділових систем, або через мережеві фільтри.

Не допускається утворення петель та контурів кабельними лініями. Перехрещення кабельних трас різного призначення рекомендується здійснювати під прямим кутом одна до одної.

Електроживлення ОТЗ повинно бути стабілізованим за напругою та струмом для нормальних умов функціонування ОТЗ і забезпечення норм захищеності.

У колах випрямного пристрою джерела живлення необхідно встановлювати фільтри нижніх частот, які повинні мати фільтрацію по симетричних і несиметричних шляхах поширення.

Необхідно передбачити відключення електромережі від джерела живлення ОТЗ під час зникнення напруги в мережі, під час відхилення параметрів електроживлення від норм, заданих в технічних умовах, та під час появи несправностей у колах електроживлення.

Усі металеві конструкції ОТЗ (шафи, пульти, корпуси розподільних пристроїв та металеві оболонки кабелів) повинні бути заземлені.

- охоплювати увесь технологічний комплекс інформаційної діяльності;
- бути різноманітною по використанню засобів, багаторівневою з ієрархічною послідовністю доступу;
- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
- бути нестандартною, різноманітною (при вибиранні засобів захисту не можна розраховувати на непоінформованість зловмисників відносно її можливостей);
- бути простою для технічного обслуговування і зручною для експлуатації користувачами;
- бути надійною (поломки технічних засобів є причиною появи неконтрольованих каналів витоку інформації);
- бути комплексною, мати цілісність, яка означає, що жодна її частина не може бути вилучена без збитку для усієї системи.

До системи безпеки інформації пред'являються також певні **вимоги**:

- чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
- надання користувачеві мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму числа засобів захисту, загальних для декількох користувачів;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;
- забезпечення оцінки ступені конфіденційності інформації;
- забезпечення контролю цілісності засобів захисту і негайне реагування на їх вихід з ладу.

СЗІ повинна мати певні види власного забезпечення, спираючись на які вона виконуватиме свою цільову функцію.

Види забезпечення СЗІ:

- правове;

- організаційне;
- апаратне;
- інформаційне;
- програмне;
- математичне;
- лінгвістичне;
- нормативно-методичне.

Правове забезпечення – нормативні документи, положення, інструкції, вимоги яких є обов'язковими у рамках сфери їх дії.

Організаційне забезпечення – реалізація захисту інформації здійснюється певними структурними одиницями (режимно-секретна служба, служба режиму, служба охорони, служба ТЗІ та ін.), якими треба керувати.

Апаратне забезпечення – використання технічних засобів як для захисту інформації, так і для забезпечення діяльності СЗІ.

Інформаційне забезпечення – відомості, дані, показники, параметри, які лежать в основі рішення завдань, що забезпечують функціонування СЗІ.

Програмне забезпечення – інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінку наявності і небезпеки різних каналів витоку і шляхів НСД до джерел інформації, що захищається.

Математичне забезпечення – використання математичних методів для різних розрахунків, пов'язаних з оцінкою небезпеки дій порушників, зон і норм необхідного захисту.

Лінгвістичне забезпечення – спеціальні мовні засоби спілкування фахівців і користувачів у сфері захисту інформації.

Нормативно-методичне забезпечення – норми і регламенти діяльності органів, служб, засобів, що реалізують функції захисту інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації.

Задовольнити сучасні вимоги по забезпеченню безпеки організації і захист її конфіденційної інформації може тільки комплексна система безпеки (рис 1.1).

До **засобів технічного захисту** відносяться:

- фільтри-обмежувачі та спеціальні абонентські пристрої захисту для блокування витоку мовної ІзОД через двопровідні лінії телефонного зв`язку, системи директорського та диспетчерського зв`язку;
- пристрої захисту абонентських однопрограмних гучномовців для блокування витоку мовної ІзОД через радіотрансляційні лінії;
- фільтри мережеві для блокування витоку мовної ІзОД колами електроживлення змінного (постійного) струму;
- фільтри захисту лінійні (високочастотні) для встановлення в лініях апаратів телеграфного (телекодового) зв`язку;
- генератори лінійного зашумлення;
- генератори просторового зашумлення;
- екрановані камери спеціальної розробки.

Для телефонного зв`язку, не призначеного для пересилання ІзОД, рекомендується застосовувати апарати вітчизняного виробництва, сумісні з пристроями захисту. Телефонні апарати іноземного виробництва можуть застосовуватися за умови проходження спецдосліджень і позитивного висновку компетентних організацій системи ТЗІ про їх сумісність з пристроями захисту.

Вибір методів і способів захисту елементів ТЗОІ та ДТЗС, що мають мікрофонний ефект, залежить від величини їх вхідного опору на частоті 1кГц.

1. Елементи з вхідним опором менше 600 Ом (головки гучномовців, електродвигуни вентиляторів, трансформатори тощо) рекомендується відключати по двох проводах або встановлювати у розрив кіл пристрої захисту з високим вихідним опором для зниження до мінімальної величини інформативної складової струму.

2. Елементи з високим вхідним опором (електричні дзвінки, телефонні капсулі, електромагнітні реле) рекомендується не тільки відключати від кіл, а й замикати на низький опір або закорочувати, щоб зменшити електричне поле від цих елементів, зумовлене напругою, наведеною під час впливу акустичного поля. При цьому слід враховувати, що обраний спосіб захисту не повинен пору-

При невиконанні зазначених вище умов системи повинні відключатися від мережі електроживлення по двох проводах.

Захист ІзОД від витоку через кола електроосвітлення та електроживлення побутової техніки повинен здійснюватися підключенням зазначених кіл до окремого фідера трансформаторної підстанції, до якого не допускається підключення сторонніх користувачів.

У випадку невиконання зазначеної вимоги електропобутові прилади на період проведення закритих заходів повинні відключатися від кіл електроживлення.

3. **Технічні заходи.** Це основний етап робіт з технічного захисту ІзОД і полягає у встановленні ОТЗ, забезпеченні ТЗОІ та ДТЗС пристроями ТЗІ.

Під час вибору, встановлення, заміни технічних засобів слід керуватися:

- паспортами;
- технічними описами;
- інструкціями з експлуатації;
- рекомендаціями з установлення, монтажу та експлуатації, що додаються до цих засобів.

ОТЗ повинні розміщуватися, по можливості, ближче до центру будинку або в бік найбільшої частини контрольованої території. Складові елементи ОТЗ повинні розміщуватися в одному приміщенні або в суміжних.

Якщо зазначені вимоги невиконувані, слід вжити додаткових заходів захисту:

- установити високочастотні ОТЗ в екрановане приміщення (камеру);
- установити в незахищені канали зв`язку, лінії, проводи і кабелі спеціальні фільтри та пристрої;
- прокласти проводи і кабелі в екранувальних конструкціях;
- зменшити довжину паралельного пробігу кабелів і проводів різних систем з проводами та кабелями, що несуть ІзОД;
- виконати технічні заходи щодо захисту ІзОД від витоку колами заземлення та електроживлення.

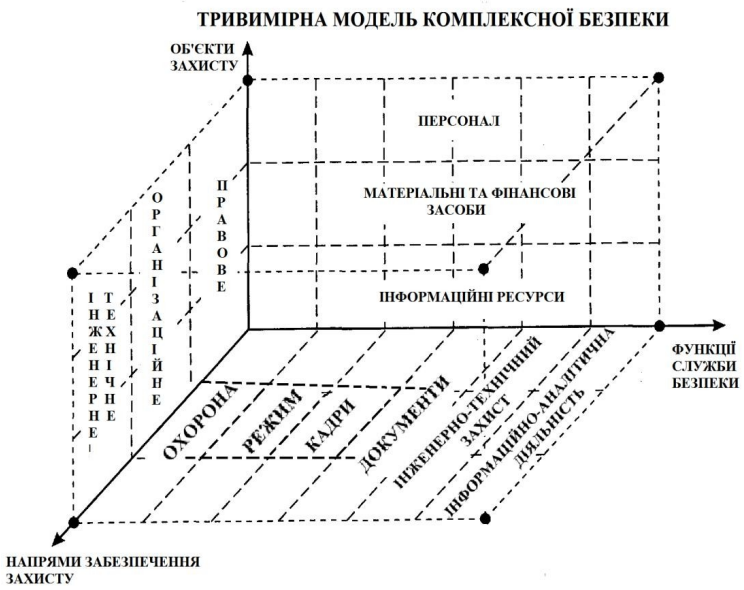

Рис. 1.1 Концептуальна модель інформаційної безпеки

Інформаційна безпека – це стан захищеності інформаційних ресурсів організації і підтримувальної інфраструктури від зовнішніх і внутрішніх загроз, які можуть завдати неприйнятного збитку суб'єктам інформаційних відношень.

Для побудови СЗІ потрібно:

- визначити загрози безпеки інформації, джерела цих загроз, способи їх реалізації і цілі, а також інші умови і дії, що порушують безпеку;
- розглядати заходи захисту інформації від неправомірних дій, що призводять до нанесення збитку.

Для аналізу такого значного набору джерел, об'єктів і дій доцільно використовувати методи моделювання, при яких формується як би «заступник» реальних ситуацій.

Основні компоненти концептуальної моделі безпеки інформації (рис. 1.2):

- об'єкти загроз;
- загрози;
- джерела загроз;

- цілі загроз з боку зловмисників;
- джерела інформації;
- способи неправомірного оволодіння інформацією з обмеженим доступом (ІзОД) (способи доступу);
- напрями захисту інформації;
- способи захисту інформації;
- засоби захисту інформації.

1.2 Концептуальна модель безпеки інформації

Інформаційна безпека – це стан захищеності інформаційних ресурсів, технології їх формування і використання, а також прав суб'єктів інформаційної діяльності.

Концепція безпеки є основним правовим документом, який визначає захищеність організації від внутрішніх і зовнішніх загроз.

Загрози конфіденційної інформації – це потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння відомостями, які охороняються. Такими діями є:

- *ознайомлення* з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;

- установленням у викличних колах вимикачів для розриву кіл;
- установленням на вході гучномовців вимикачів (реле), які дають можливість розривати кола по двох проводах;
- забезпеченням можливості відключення живлення мікрофонних підсилювачів;
- установленням найпростіших пристроїв захисту.

Способи захисту ІзОД від витоку через радіотрансляційну мережу, що виходить за межі виділеного приміщення:

- відключенням гучномовців по двох проводах;
- вмиканням найпростіших пристроїв захисту.

Для служби оповіщення слід виділити чергові абонентські пристрої поза виділеними приміщеннями; кола до цих пристроїв повинні бути прокладені окремим кабелем.

Блокування каналів витоку ІзОД через кола вторинних електрогодинників системи електрогодинофікації здійснюється відключенням їх на період проведення закритих заходів.

Запобігання витоку ІзОД через системи пожежної та охоронної сигналізацій здійснюється відключенням датчиків пожежної та охоронної сигналізації на період проведення важливих заходів, що містять ІзОД, або застосуванням датчиків, які не потребують спеціальних заходів захисту.

З метою виключення можливості витоку ІзОД під час роботи незахищених технічними засобами телевізорів, радіоприймачів, звукопідсилювальної та звуковідтворювальної апаратури необхідно на період проведення важливих заходів зазначені пристрої відключати від мережі електроживлення по двох проводах.

Засоби блокування витоку ІзОД через системи електронної оргтехніки та кондиціонування:

- розташуванням зазначених систем усередині контрольованої території без винесення окремих компонентів за її межі;
- електроживленням систем від трансформаторної підстанції, що знаходиться всередині контрольованої території.

- визначити системи, що підлягають демонтажу, потребують переобладнання кабельних мереж, кіл живлення, заземлення або установлення в них захисних пристроїв.

За результатами обстеження складається **акт** довільної форми **з переліком виконаних заходів** і прикладанням:

- переліку ОТЗ, розміщених у виділених приміщеннях;
- плану виділених приміщень із зазначенням місць установлення ОТЗ, а також схем прокладання кабелів, проводів, кіл;
- переліку технічних засобів, кабелів, кіл, проводів, що підлягають демонтажу.

Акт підписується виконавцем робіт і затверджується керівником організації.

2. **Підготовчі технічнізаходи** включають у себе первинні заходи блокування електроакустичних перетворювачів і ліній зв`язку, які виходять за межі виділених приміщень.

Способи блокування ліній зв`язку:

- відключенням ліній зв`язку ТЗОІ та ДТЗС або встановленням найпростіших схем захисту;
- демонтажем технічних засобів, кабелів, кіл, проводів, що уходять за межі виділених приміщень;
- видаленням за межі виділених приміщень окремих елементів технічних засобів, які можуть бути джерелом виникнення каналу витоку інформації.

Способи блокування каналів можливого витоку ІзОД у системах міського та відомчого телефонного зв`язку:

- відключенням дзвінкових (викличних) ліній телефонного апарата;
- установленням у колі телефонного апарата безрозривної розетки для тимчасового відключення;
- установленням найпростіших пристроїв захисту.

Способи запобігання витоку ІзОД через діючі системи гучномовного диспетчерського та директорського зв`язку:

- *модифікація* інформації в кримінальних цілях як часткова або значна зміна складу і змісту відомостей;
- *руйнування* (*знищення*) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

Ці дії з інформацією призводять до порушення її *конфіденційності*, *цілісності*, *доступності*, що призводить до порушення як режиму управління, так і його якості.

Кожна загроза спричиняє за собою певний збиток – моральний або матеріальний, а захист і протидія загрозі покликані понизити його величину.

1.3 Загрози та їх прояви

Рис. 1.4 Класифікація загроз

Дії, які призводять до неправомірного оволодіння ІзОД

Відношення об'єкта (організація) і суб'єкта (конкурент, зловмисник) в інформаційному процесі з протилежними інтересами можна розглядати з позиції активності в діях, що призводять до оволодіння ІзОД. В цьому випадку можливі такі ситуації:

- *власник не приймає ніяких заходів до збереження ІзОД*, що дозволяє зловмисникові легко отримати ті зведення, що цікавлять його;
- *власник інформації строго дотримується заходів інформаційної безпеки*, тоді зловмисникові доводиться докладати значних зусиль до здійснення доступу до відомостей, що охороняються, використовуючи для цього усю сукупність способів несанкціонованого проникнення: легальне або нелегальне, заходове або без заходове;
- проміжна ситуація – це *виток інформації по технічних каналах*, при

5.2 Захист інформації в ІТС від витоку та руйнування

Організація захисту ІзОД в ІТС від витоку каналами ПЕМВН визначається тимчасовими рекомендаціями **ТР ТЗІ - ПЕМВН-95. Нормативний документ системи технічного захисту інформації. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок**.

Технічному захисту підлягає ІзОД, носіями якої є поля і сигнали, що утворюються в результаті роботи технічних засобів пересилання, оброблення, зберігання, відображення інформації (ТЗОІ), а також допоміжних технічних засобів і систем (ДТЗС).

Роботи із захисту ІзОД від витоку каналами ПЕМВН включають організаційні, підготовчі технічні та технічні заходи, а також організацію контроля за виконанням заходів ТЗІ і оцінки ефективності цих заходів.

Загальні рекомендації з ТЗІ з обмеженим доступом від витоку каналами ПЕМВН

1. **Організаційні заходи:**

- визначити перелік відомостей з обмеженим доступом, що підлягають технічному захисту (визначає власникінформації);
- обгрунтувати необхідність розроблення і реалізації захисних заходів з урахуванням матеріальної або іншої шкоди, яка може бути завдана внаслідок можливого порушення цілісності ІзОД чи її витоку технічними каналами;
- установити перелік виділених приміщень, в яких не допускається реалізація загроз та витік ІзОД;
- визначити перелік технічних засобів, що повинні використовуватися як ОТЗ;
- визначити технічні засоби, застосування яких не обгрунтовано службовою та виробничою необхідністю та які підлягають демонтажу;
- визначити наявність задіяних і незадіяних повітряних, наземних, настінних та закладених у приховану каналізацію кабелів, кіл і проводів, що уходять за межі виділених приміщень;

- закладки, що асоціюються з програмно-апаратним середовищем;
- закладки, що асоціюються з програмами первинного завантаження;
- закладки, що асоціюються із завантаженням драйверів;
- закладки, що асоціюються з ПЗ загального призначення;
- використовувані модулі, що містять тільки код закладки;
- модулі-імітатори, співпадаючі з деякими програмами, що вимагають введення конфіденційної інформації;
- закладки, що маскуються під програмні засоби оптимізаційного призначення (архіватори, прискорювачі і т.д.);
- закладки, що маскуються під програмні засоби ігрового і розважального призначення.

Щоб закладка змогла виконати які-небудь функції, вона повинна отримати управління, тобто процесор повинен почати виконувати інструкції (команди), що відносяться до коду закладки. Це можливо тільки при одночасному виконанні двох умов:

1) закладка повинна знаходитися в оперативній пам'яті до початку роботи програми, яка є метою дії закладки, отже, вона має бути завантажена раніше або одночасно з цією програмою;

2) закладка повинна активізуватися за деякому загальному, як для закладки, так і для програми, події, тобто при виконанні ряду умов в апаратно-програмному середовищі управління має бути передане на програму-закладку.

Це досягається шляхом аналізу і обробки закладкою загальних дій (як правило, переривань). В якості таких переривань можна виділити:

- переривання від системноготаймера;
- переривання від зовнішніх пристроїв;
- переривання від клавіатури;
- переривання при роботі з диском;
- переривання операційного середовища (у тому числі переривання для роботи з файлами і запуску виконуваних модулів).

якій власник ще не знає про це, а зловмисник без особливих зусиль може їх використовувати у своїх інтересах.

Дії, які призводять до незаконного оволодіння ІзОД:

1) *розголошення* – умисні або необережні дії осіб, яким відповідні відомості були довірені в установленому порядку, що привели до ознайомлення з ними осіб, не допущених до них. Виражається в повідомленні, пересилці, публікації та інших способах і реалізується по каналах поширення і засобах масової інформації;

2) *витік* – безконтрольний вихід ІзОД за межі організації або кола осіб, яким вона була довірена. Можливий по різних каналах витоку інформації, у тому числі візуально-оптичним, акустичним, електромагнітним, електричним і матеріально-речовим;

3) *несанкціонований доступ* – протиправне умисне оволодіння ІзОД особою, яка не має права доступу до відомостей, що охороняються. Реалізується різними способами, у тому числі такими, як: співпраця (шпигунство), вивідування, підслуховування, копіювання, підробка, знищення, перехоплення, фотографування та ін. Для реалізації цих дій зловмисникові доводиться часто проникати на об'єкт або створювати поблизу нього спеціальні пости контролю і спостереження, обладнаних найсучаснішими технічними засобами.

Факт отримання зловмисниками або конкурентами відомостей, що охороняються, називають **витоком**.

Витік інформації здійснюється по різних технічних каналах.

1.5 Модель технічного каналу витоку інформації

Технічний канал витоку інформації (рис. 1.5) – це фізичний шлях від джерела конфіденційної інформації до зловмисника, за допомогою якого останній може отримати доступ до відомостей, що охороняються. Для утворен-

ня каналу витоку інформації потрібні певні просторові, енергетичні і тимчасові умови, а також наявність на стороні зловмисника відповідної апаратури прийому, обробки і фіксації інформації.

По фізичній природі можливі наступні шляхи перенесення інформації:

- світлові промені;
- звукові хвилі;
- електромагнітні хвилі,
- матеріали і речовини.
- матеріальноречові.

Типи технічних каналів витоку інформації:

- *радіоканали* (електромагнітні випромінювання радіодіапазону);
- *акустичні канали* (звукові коливання в будь-якому середовищі);
- *електричні канали* (небезпечна напруга і струми в струмопровідних комунікаціях);
- *оптичні канали* (електромагнітні випромінювання в інфрачервоній, видимій і ультрафіолетовій частині спектру);
- матеріально-речові канали (папір, фото, цифрові і магнітні носії, відходи і т.п.).

Висновки

1. Інформація – це ресурс. Втрата ІзОД приносить моральний або матеріальний збиток.
2. Умови, сприяючі неправомірному оволодінню ІзОД, зводяться до її розголошування, витоку і несанкціонованого доступу до її джерел.
3. У сучасних умовах безпека інформаційних ресурсів може бути забезпечена тільки комплексною системою захисту інформації.
4. Комплексна система захисту інформації має бути: безперервною, плановою, цілеспрямованою, конкретною, активною, надійною.
5. Система захисту інформації повинна спиратися на систему видів власного забезпечення, здатного реалізувати її функціонування не лише в повсякденних умовах, але і в критичних ситуаціях.

ний стан за рахунок потайної дії на них спеціальних оптичних і звукових сигналів.

Для протидії подібним загрозам слід враховувати наступні моменти:

- ПрЗ ОС відноситься до специфічного виду радіоелектронного заглушення, який передбачає створення завад ОС не лише через різні види природного, але і штучного середовища передачі даних;
- цілі ПрЗ ОС за своїми масштабами можуть бути набагато вище за традиційні цілі радіоелектронного заглушення;
- ОС є складними об'єктами заглушення, ці системи дуже уразливі від ПрЗ, що відносяться до класу імітуючих завад;
- ПрЗ у відмінності від інших можуть зберігатися в заглушенних системах роками, розмножуватися в них, реалізовувати різні деструктивні функції;
- залежно від наявної вихідної інформації про ОС отримання НСД до її ресурсів системою програмного заглушення і вплив на них ПрЗ можливо на різну глибину;
- ПрЗ ОС передбачає зміщення акцентів у бік обліку властивостей пам'яті ОС, інформації, що зберігається в ній, процедурного характеру створюваних завад, розгляду усього процесу заглушення як програми.

Програмні закладки – це навмисно внесені в ПЗ функціональні об'єкти (програмні коди), які за певних умов ініціюють реалізацію можливостей програмного забезпечення, що не декларується. Як правило, програмні закладки використовують вірусну технологію потайного впровадження, поширення і активізації.

Програмні закладки призначені для несанкціонованого тайного отримання конфіденційній інформації. Типова програмна закладка може, наприклад, зберігати інформацію (у тому числі і паролі), що вводиться з клавіатури, в декількох зарезервованих для цього секторах, а потім пересилати накопичені дані по мережі на комп'ютер порушника.

Програмні закладки класифікуються *за методом і місцем їх впровадження і застосування*:

на програмні завади. У випадку використанні помилкових даних програмою може статися непередбачене переривання її роботи, видача помилкового результату.

Метод впливу ПрЗ на програмне забезпечення ОС. В результаті дії програмних завад змінюються характеристики програмного забезпечення, що знаходиться в пам'яті. Наприклад, окремі програми і дані можуть бути стерті, а інші спотворені. Спотворення програм в пам'яті ОС можливе як зі збереженням властивих їм функцій, так і зі зміною їх.

Рис. 1.51 Методи програмного заглушення обчислювальних систем

Метод впливу ПрЗ на апаратне забезпечення ОС. Спочатку змінюються характеристики апаратних засобів, їх стан. Зокрема, може змінюватися стан дисплея, принтера, клавіатури, інших облаштувань ОС. Створювані програмні завади поповнюють наявне програмне забезпечення.

Метод впливу ПрЗ на операторів ОС. В результаті впливу ПрЗ на ОС змінюється стан її операторів. При цьому можуть бути створені програмні завади, що не лише дезінформують операторів, але і змінюють їх психофізіологіч-

Контрольні питання

1. Що розуміється під інформаційною безпекою?
2. Що таке система захисту інформації в організації?
3. Які цілі і завдання системи захисту інформації?
4. Які забезпечуючи підсистеми включає система захисту інформації і їх призначення?
5. Поясніть призначення основних компонент концептуальної моделі захисту інформації в організації.
6. Що таке загрози інформації з обмеженим доступом і на що вони спрямовані?
7. За якими ознаками класифікуються загрози інформаційної безпеки?
8. Які дії призводять до протиправного опанування інформації з обмеженим доступом?

2. Основні поняття та визначення комплексного захисту інформації

2.1 Комплексна система захисту інформації: цілі, завдання, принципи створення

Володіння інформацією необхідної якості в потрібний час і в потрібному місці є запорукою успіху у будь-якому вигляді господарської діяльності. Монопольне володіння певною інформацією виявляється вирішальною перевагою в конкурентній боротьбі, саме тому власникові необхідно її захищати.

Виділяються два види власної інформації у підприємця:

1) *технічна* (*технологічна*) *інформація* – наприклад, методи виробництва продукції, програмне забезпечення, рецепти ліків і т.п.;

2) *ділова інформація* – наприклад, бізнес-плани підприємства, списки клієнтів, матеріали різних замовлених досліджень.

Забезпечення безпеки інформації є безперервний процес, який полягає в контролі захищеності, виявленні вузьких місць в системі захисту, обґрунтуванні і реалізації найбільш раціональних шляхів вдосконалення і розвитку системи захисту:

- безпека інформації може бути забезпечена лише при комплексному використанні усього арсеналу наявних засобів захисту;
- ніяка система захисту не забезпечить безпеки інформації без належної підготовки користувачів і дотримання ними усіх правил захисту;
- ніяку систему захисту не можна вважати абсолютно надійною, оскільки завжди може знайтися зловмисник, який знайде лазівку для доступу до інформації.

Комплексна система захисту інформації (**КСЗІ**) – це сукупність організаційних та інженерних заходів, програмно-апаратних, криптографічних та інших засобів, які забезпечують захист інформації обмеженого доступу в ІТС.

Цілі створення КСЗІ:

1) захист законних інтересів організації від протиправних посягань;

2) недопущення:

- обробка отриманої інформації;
- прийняття рішення на програмне заглушення;
- формування програмних завад;
- одержання доступу до ресурсів ОС для введення в неї ПрЗ;
- введення ПрЗ в ОС;
- безпосередний вплив ПрЗ наОС.

Отримання НСД до ресурсів ОС і введення в ці системи ПрЗ можливий звичайними радіоканалами, каналами супутникового зв'язку, телефонними лініями міжнародного зв'язку, спеціальними виділеними кабельними лініями, через безпосередній доступ до консолей ОС, до лазерних і магнітних носіїв інформації, використовуваних в системі (рис. 1.50).

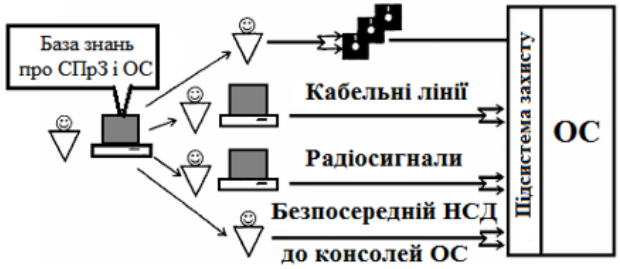

Рис. 1.50 Структура проникнення програм заглушення в ОС

Методи програмного заглушення ОС дуже різноманітні (рис. 1.51).

Метод заглушення ОС процедурними ПрЗ полягає в створенні ПрЗ, що виступать шкідливими управляючими программами, процедурами, командами, на які має бути передане управління ресурсами ОС. Після отримання управління ресурсами ОС процедурні ПрЗ реалізують покладені на них функції: самовідтворюватися, стирати, спотворювати, копіювати цінну інформацію, що знаходиться в оперативній і зовнішній пам'яті, видавати помилкові команди, імітувати роботу істинних програм і т.п.

Метод заглушення ОС декларативними ПрЗ передбачає створення програмних завад, якими виступають помилкові дані, повідомлення, електронні листи. При цьому методі не передбачається передача управління ресурсами ОС

альні заважаючи дії на ОС, які подібні за розпізнавальними параметрами істинним сигналам. Вони відносяться до класу імітуючих завад.

Об'єктами УПрЗ є глобальні і локальні обчислювальні мережі, обчислювальні центри, інформаційно-управляючі системи, окремі ЕОМ, мікропроцесорні пристрої.

Узагальнена мета програмного заглушення ОС – зниження ефективності або зрив функціонування ОС, управління різними процесами.

Слабкі сторони ОС, які ПрЗ використовує для досягнення своїх цілей:

- відкритість ОС як для корисних зовнішніх дій, так і умисних програмних завад;
- недосконаліть організаційно-технічних і логічних структур ОС;
- недосконаліть захисту ОС від програмних завад;
- наявність істотних витрат на усунення наслідків дії ПрЗ наОС;
- можливість тривалого зберігання ПрЗ в пам'яті ОС.

Негативні ефекти в ОС, які викликаються програмними завадами:

- втрата цінної інформації, що зберігається в пам'яті системи;
- непередбачене переривання обчислювального процесу;
- видача на засоби відображення інформації помилкових результатів розрахункових та інформаційних завдань;
- видача помилкової інформації на пристрої управління зовнішніми об'єктами;
- передача на ОС, що взаємодіють, програм і даних з ПрЗ;
- перехоплення циркулюючої в ОС інформації і передача її каналами витоку;
- затримка в часі рішення системних і прикладних завдань;
- поглинання ресурсів пам'яті ОС і у ряді випадків її перевантаження;
- руйнування апаратних засобів;
- дезінформація і зміна психофізіологічного стану операторів ОС та ін.

Операції процесу програмного заглушення ОС:

- добування інформації про заглушення ОС;

- розкрадання фінансових і матеріально-технічних засобів;
- знищення майна і цінностей;
- розголошування, витоку і НСД до ІзОД;
- порушення роботи технічних засобів забезпечення виробничої діяльності (включаючи інформаційні технології).

Завдання створення КСЗІ:

- прогнозування, своєчасне виявлення і усунення загроз безпеки, причин і умов, сприяючих нанесенню збитку організації, порушенню її нормального функціонування і розвитку;
- віднесення інформації до категорії обмеженого доступу, а інших ресурсів – до різних рівнів небезпеки, що підлягають збереженню;
- створення механізму і умов оперативного реагування на загрози безпеки прояву негативних тенденцій у функціонуванні організації;
- ефективне припинення загроз персоналу і посягань на ресурси на основі правових, організаційних і інженерно-технічних заходів і засобів забезпечення безпеки;
- створення умов для максимально можливого відшкодування і локалізації збитку, послаблення негативного впливу наслідків порушення безпеки організації.

Комплексна система захисту інформації **включає**:

1) службу захисту інформації;
2) фізичну охорону об’єктів;
3) інженерно-технічні заходи;
4) комплекс засобів захисту від НСД;
5) комплекс засобів блокування технічних каналів витоку інформації;
6) комплекс засобів криптографічного захисту;
7) регламентацію дій користувачів.

Об’єкти захисту в ІТС:

- *інформаційні ресурси* обмеженого доступу та інші інформаційні ресурси, що підлягають захисту від НСД, в тому числі такі, що містять відкриту інформацію;

- *процеси обробки інформації в ІТС* – інформаційні технології, регламенти та процедури збирання, обробки, зберігання та передачі інформації;

- *інфраструктура ІТС* – системи обробки та аналізу інформації, технічні та програмні засоби її обробки, передачі та відображення, в тому числі канали інформаційного обміну та телекомунікації, системи та засоби захисту інформації, об'єкти та приміщення, в яких розміщено компоненти ІТС;

- *користувачі* і *обслуговуючий персонал* ІТС.

Захисту підлягає вся інформація, що може циркулювати в ІТС:

- *відкрита інформація*, для якої необхідно забезпечити такі властивості, як цілісність та доступність;

- *ІзОД*, для якої необхідно забезпечити захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення;

- *конфіденційна інформація*, доступ до якої обмежено власником у відповідності до прав, наданих Законом України «Про інформацію»;

- *персональні дані*, доступ до яких обмежено у відповідності з Законом України «Про захист персональних даних»;

- *службова інформація*, доступ до якої обмежено у відповідності з Законом України «Про доступ до публічної інформації»;

- *інформація*, що становить *державну* або іншу передбачену законом *таємницю*, відповідно до вимог Закону України «Про державну таємницю» та інших спеціальних законів.

Суб'єкти інформаційних відносин в ІТС:

1) організація як власник інформаційних ресурсів;

2) структурні підрозділи організації, що забезпечують експлуатацію ІТС;

3) посадові особи та співробітники структурних підрозділів організації, як користувачі ІТС у відповідності з службовими обов'язками;

4) підприємства, державні органи та установи – учасники інформаційної взаємодії з ІТС;

Для НСВ дротяними каналами потрібно енергії на декілька порядків нижче, ніж по мережі живлення, і деструктивна дія може бути реалізована за допомогою відносно простих технічних засобів, що забезпечують високу ймовірність виведення об'єкту атаки з ладу. Зокрема, в даному випадку для НСВ може бути використаний будь-який електромагнітний шокер.

3. **Безпровідний силовий вплив.** Найбільш прихованим і найбільш ефективним є канал силової деструктивної дії по ефіру з використанням потужного короткого електромагнітного імпульсу. В цьому випадку стало можливим реалізувати досить компактні електромагнітні технічні засоби НСВ, що розміщуються за межами об'єкту атаки і на достатньому для маскування атаки видалення від комунікацій (рис. 1.49).

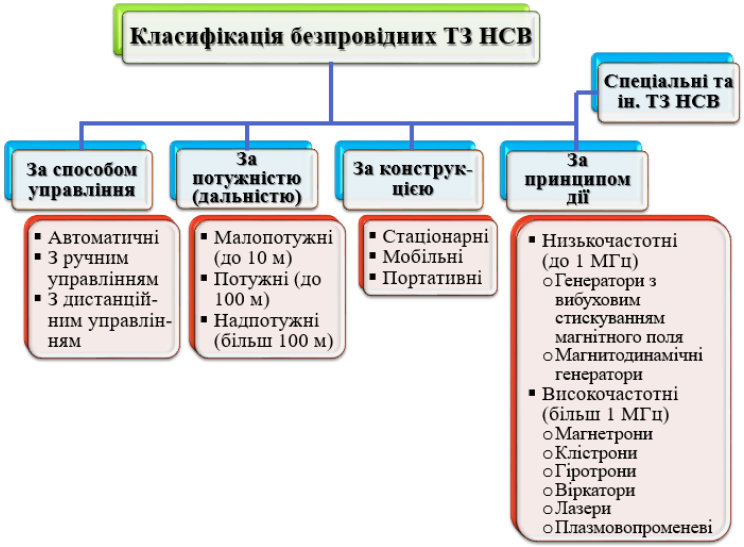

Рис. 1.49 Класифікація безпровідних ТЗНСВ лініями

Програмне заглушення обчислювальних систем (ПрЗ ОС) – це комплекс організаційно-технічних заходів, спрямованих на порушення нормального функціонування ОС шляхом створення їм умисних програмних завад.

Умисні програмні завади (УПрЗ) на логічному рівні є хибними програмами, процедурами, даними. З фізичної точки зору програмні завади – це спеці-

Рис. 1.47 Класифікація технічних засобів НСВ мережами електроживлення

Навмисний силовий вплив дротяними лініями зв'язку. Для проникнення енергії НСВ дротяними лініями необхідно здолати граничну поглинаючу здатність компонентів, які можуть бути використані у вхідних ланцюгах (рис. 1.48). Для виведення із ладу цих компонентів (мікросхем, транзисторів, діодів і т.п.) досить дії імпульсу з енергією 1-1000 мкДж, причому цей імпульс може бути дуже коротким (10-1000 нс). Напруга пробою переходів складає від одиниць до десятків вольт.

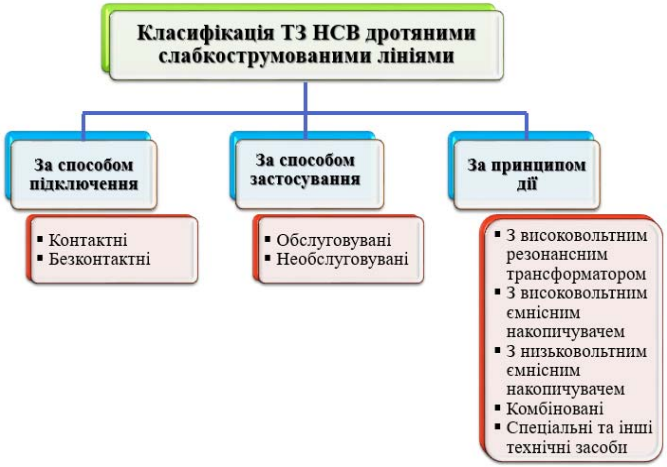

Рис. 1.48 Класифікація ТЗНСВ дротяними слабкострумованими лініями

5) юридичні та фізичні особи, інформація про яких накопичується, зберігається та обробляється в ІТС;

6) юридичні та фізичні особи, задіяні в процесі створення та функціонування ІТС – розробники компонентів ІТС, обслуговуючий персонал, організації, що надають послуги у сфері захисту інформації тощо.

Суб'єкти інформаційних відносин в ІТС зацікавлені в забезпеченні:

- конфіденційності інформації з обмеженим доступом;
- цілісності інформації;
- захисту від нав'язування хибної інформації;
- своєчасного доступу до необхідної інформації;
- розмежування відповідальності за порушення законних прав інших суб'єктів інформаційних відносин та встановлених правил поводження з інформацією;
- можливості здійснення неперервного контролю та керування процесами обробки та передачі інформації.

Рис. 1.6 Принципи створення комплексної системи захисту інформації

1. **Законність.** Забезпечення захисту інформації та створення КСЗІ в ІТС здійснюється відповідно до вимог чинного законодавства в сфері захисту інформації. Користувачі та обслуговуючий персонал ІТС повинні мати уявлення про

відповідальність за неправомірне розголошення інформації з обмеженим доступом та правопорушення в області інформаційних відносин, визначену нормативно-правовими актами України.

2. **Системність.** Системний підхід до створення КСЗІ в ІТС передбачає врахування всіх пов'язаних та взаємодіючих елементів, умов та факторів, суттєва значущих для вирішення проблеми забезпечення захисту інформації в ІТС. При створені КСЗІ необхідно враховувати всі критичні та найбільш вразливі сегменти системи обробки інформації, а також характер, можливі об'єкти та напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи та НСД до інформації. КСЗІ повинна створюватися не лише з врахуванням всіх відомих каналів проникнення та НСД до інформації, але й з врахуванням можливості виникнення принципово нових шляхів реалізації загроз.

3. **Комплексність.** Комплексне використання заходів та механізмів захисту ІТС передбачає узгоджене використання різнорідних засобів при створені цілісної системи захисту, яка перекриває всі значущі канали реалізації загроз та не містить вразливих місць на стиках окремих її компонентів. Захист повинен будуватися ешелоновано. Зовнішній захист має забезпечуватися фізичними засобами, організаційними та правовими заходами. Одними з найбільш стійких до атак повинні бути механізми захисту, реалізовані на рівні операційних систем ПЕОМ, оскільки саме ОС керує використанням ресурсів комп'ютерної системи. Прикладний рівень захисту, який враховує особливості предметної області, забезпечує внутрішню межу захисту.

4. **Неперервність.** Захист інформації – неперервний цілеспрямований процес, який передбачає здійснення відповідних заходів на всіх етапах життєвого циклу ІТС, починаючи з ранніх стадій проектування системи. Більшості технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна адміністративна підтримка – своєчасна зміна та забезпечення коректного режиму зберігання та застосування ідентифікаторів, паролів, ключів шифрування, призначення повноважень тощо. Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу методів та засобів, що вико-

зації перед нападом на об'єкт або для провокації помилкових спрацьовувань сигналізації без проникнення на об'єкт.

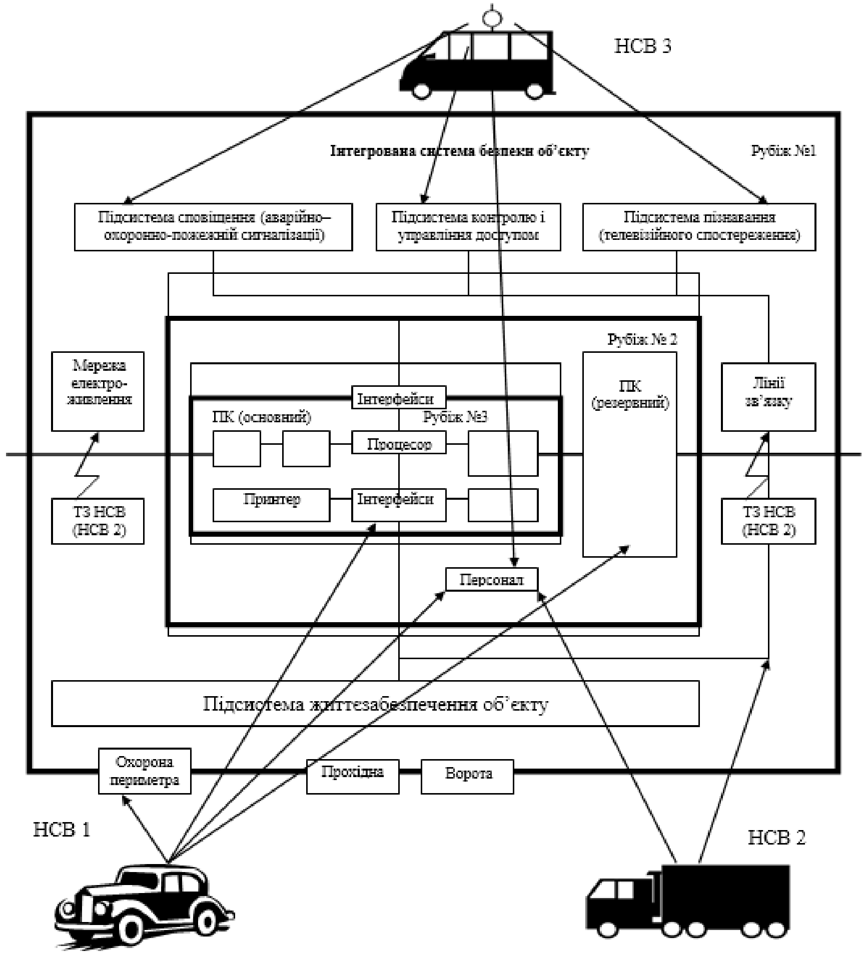

Рис. 1.46 Основні канали навмисного силового впливу

Комп'ютер або інше електронне устаткування ІТС має два важливих канали для проникнення енергії НСВ за мережею живлення:

- кондуктивний шлях через джерело вторинного електроживлення;
- наведення через паразитні ємністі та індуктивні зв'язки, як внутрішні, так і між спільно прокладеними силовими кабелями та інформаційними лініями зв'язку.

- від розрядів електричних зарядів;
- від електромагнітних полів випромінювання.

2. **Навмисний силовий вплив (НСВ)** – це умисне створення різкого сплеску напруги в мережі живлення, по інформаційних дротяних лініях або в ефірі з амплітудою, тривалістю і енергією сплеску, які здатні привести до збоїв в роботі пристрою або до виходу його з ладу.

Технічні засоби НСВ (ТЗНСВ) є *електромагнітною зброєю*, яка здатна дистанційно уразити будь-яку систему. Головне при атаці – забезпечити відповідну потужність електромагнітного імпульсу.

Істотно підвищує скритність нападу та обставина, що аналіз ушкоджень в знищеному пристрою не дозволяє однозначно ідентифікувати причину виникнення ушкодження, оскільки причиною може бути як умисна (напад), так і неумисна (наприклад, індукція від блискавки) силова дія. Ця обставина дозволяє порушникові успішно використовувати ТЗНСВ неодноразово.

ІТС, електронні елементи КСЗІ можуть бути піддані НСВ за трьома основними каналами (рис. 1.46):

- мережею електроживлення (НСВ № 1);
- комунікаційними мережами і каналами (НСВ № 2);
- ефіром з використанням потужних коротких електромагнітних імпульсів (НСВ № 3).

Використання НСВ дозволяє здолати усі стандартні рубежі захисту в системах безпеки. Усе визначається потужністю впливу, вибраними засобами захисту, наявними фінансовими можливостями.

Навмисний силовий вплив мережами живлення – це умисне створення різкого виплеску напруги в мережі живлення з амплітудою, тривалістю і енергією сплеску, які здатні привести до збоїв в роботі пристрою або до виходу його з ладу. Для НСВ використовують спеціальні технічні засоби, які підключаються до мережі безпосередньо за допомогою гальванічного зв'язку, через конденсатор або трансформатор (рис. 1.47).

НСВ може бути використане і для попереднього виведення із ладу сигналі-

ристовуються для забезпечення захисту інформаційних ресурсів ІТС, для встановлення спеціальних програмних та апаратних закладних пристроїв та інших засобів подолання системи захисту після відновлення її функціонування.

5. **Своєчасність.** Процеси визначення задач комплексного захисту ІТС та реалізації заходів забезпечення захисту інформації починають здійснюватися на ранніх стадіях розробки ІТС. Створення КСЗІ повинне проводитись паралельно з розробкою та розвитком самої автоматизованої системи, ресурси якої підлягають захисту. Це дозволить врахувати вимоги щодо забезпечення захисту інформації вже на стадіях проектування архітектури ІТС та створити більш ефективно захищену систему як з точки зору витрат ресурсів, так і стійкості.

6. **Неперервність вдосконалення.** Заходи та засоби захисту інформації, організаційні та технічні рішення, кадровий склад повинен постійно вдосконалюватися з врахуванням змін в методах та засобах перехоплення інформації, нормативних вимог з забезпечення захисту інформації, досягнутого вітчизняного та зарубіжного досвіду.

7. **Достатність.** Рівень витрат на забезпечення захисту інформації в ІТС повинен відповідати цінності інформаційних ресурсів та величині можливих збитків від їх розголошення, втрати, витоку, руйнування та спотворення.

8. **Персональна відповідальність.** Передбачає покладання відповідальності за забезпечення захисту інформації та системи її обробки на кожного співробітника організації в межах його повноважень. Розподіл прав та обов’язків співробітників повинен здійснюватися таким чином, щоб у випадку будь-якого порушення множина винних була чітко відома та мінімальна.

9. **Мінімізація повноважень.** Означає надання користувачам мінімальних прав доступу. Доступ до інформаційних ресурсів ІТС повинен надаватися виключно в тому випадку та об’ємі, якщо це необхідно співробітнику організації для виконання його функціональних обов’язків.

10. **Гнучкість системи захисту.** Прийняті заходи та встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечити як надмірний, так і недостатній рівень захисту. Для забезпечення можливості ва-

ріювання рівнем захищеності, засоби захисту повинні мати необхідну гнучкість. Особливо важливою дана властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснити на систему, що вже експлуатується, без порушення процесу її нормального функціонування. Крім того, зовнішні умови та вимоги з часом змінюються. В таких ситуаціях властивість гнучкості КСЗІ звільняє власників ІТС від необхідності прийняття кардинальних заходів щодо повної заміни засобів захисту на нові.

11. **Простота застосування засобів захисту.** Механізми захисту інформації в ІТС повинні бути інтуїтивно зрозумілими та простими у використанні. Застосування засобів захисту не повинне бути пов'язане з спеціальними знаннями або з виконанням дій, що потребують додаткових навичок при звичайній роботі зареєстрованих за встановленим порядком користувачів.

12. **Обґрунтованість та технічна реалізованість.** Інформаційні технології, технічні та програмні засоби, засоби та заходи захисту інформації в ІТС повинні бути реалізовані на сучасному рівні розвитку науки та техніки, обґрунтовані з точки зору досягнення заданого рівня захищеності інформаційних ресурсів та повинні відповідати встановленим нормам та вимогам з забезпечення захисту інформації.

13. **Спеціалізація та професіоналізм.** Передбачає залучення до розробки засобів та реалізації заходів захисту інформації в ІТС спеціалізованих організацій, які найбільш підготовлені до конкретного виду діяльності з забезпечення захисту інформаційних ресурсів, мають досвід практичної роботи та ліцензію на провадження господарської діяльності з надання послуг у галузі захисту інформації, видану Держспецзв'язку. Реалізація організаційних заходів та налаштування засобів захисту повинні здійснюватися професійно підготовленими спеціалістами організації.

14. **Обов'язковість контролю.** Спроби порушення встановлених правил забезпечення захисту інформації в ІТС повинні бути обов'язково та своєчасно виявлені та припинені. Контроль за діяльністю будь-якого користувача, кожного засобу захисту та відносно будь-якого об'єкта захисту має здійснюватися на

вого зварювання, газорозрядні пристрої, індукційна і перемикальна апаратура та ін.).

За *характером протікання процесу в часі* завади поділяються на:

- *імпульсні* – короткі викиди напруги на фоні більш-менш стабільної основної напруги; амплітуда імпульсної завади може в сотні-тисячі разів перевищувати основну напругу, але тривалість перешкоди дуже коротка (рис. 1.45, *а*);

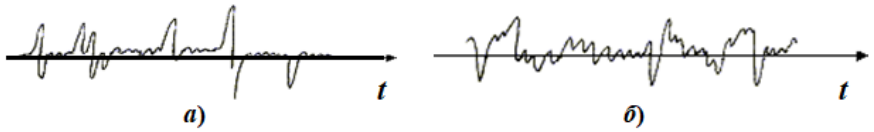

Рис. 1.45 Вид імпульсних (а) та флуктуаційних (б) завад

- *флуктуаційні* – безперервні в часі процеси, що складаються з великого числа короткочасних імпульсів з випадковою амплітудою (рис. 1.45, *б*). Якщо імпульси слідують дуже часто, перехідні процеси в приймачі накладаються один на одного, що і створює безперервний випадковий процес. Характерною особливістю завад цього типу є відсутність значних окремих викидів.

За *результатами дії на корисний сигнал* виділяють такі типи завад:

- *адитивні* – не залежать від сигналу (***s***) і викликається стороннім збуренням поля (***ξ***), яким передається сигнал каналом зв'язку:

$$\chi = s + \xi;$$

- *мультиплікативні* – обумовлени сторонньою зміною коефіцієнта передачі (***V***) каналу зв'язку:

$$\chi = s \times V.$$

У загальнішому випадку при одночасній наявності адитивної і мультиплікативної завад:

$$\chi = s \times V + \xi.$$

Зовнішні завади об'єктам підрозділяються на завади:

- від мережі живлення (імпульсні завади, провали і перенапруження в мережі живлення змінного струму);

- із зовнішніх ліній зв'язку (симетричні і несиметричні імпульсні завади);

За *місцем виникнення* завади поділяються на:

- *внутрішні* (шуми, наведення і перешкоди від розузгодження);
- *зовнішні* (промислові (індустріальні), від радіопередавачів, атмосферні та космічні).

Шум – це флуктуаційний процес, пов'язаний з дискретною природою електричного струму і є послідовністю дуже коротких імпульсів, що з'являються хаотично у великій кількості. Розрізняють різноманітні види шумів:

- *тепловий* – виникає в провідниках за рахунок теплового хаотичного руху електронів;
- *напівпровідниковий* – виникає внаслідок статичного характеру процесу генерації-рекомбінації пар електронів і дірок;
- *дрібний* – виникає внаслідок випадкового характеру подолання носіями струму потенційних бар'єрів, наприклад, електронно-діркових переходів, і т.д.

Наведення (**наведений в струмопровідних лінійних елементах технічних засобів сигнал**; **наведення**) – завада, що виникає внаслідок непередбаченою схемою і конструкцією даного об'єкту передачі паразитними зв'язками напруги, струму, заряду або магнітного потоку з джерела завади в дану частину об'єкту. Струм і напруга в струмопровідних елементах, викликані електромагнітним випромінюванням, ємнісними і індуктивними зв'язками.

Паразитний зв'язок – це зв'язок по електричних і (або) магнітних ланцюгах, поява якого не була передбачена конструктором.

Завада від розузгодження є небажаним перехідним процесом в даному ланцюзі об'єкту, що містить ділянки з розподіленими і зосередженими параметрами, який виникає внаслідок розузгодження між неоднорідними ділянками.

Індустріальні завади формуються пристроями, які генерують відносно регулярні електромагнітні коливання, не призначені для випромінювання (медичні високочастотні установки, різного роду промислові агрегати, системи розгортки та ін.), а також електричними пристроями, що не виробляють періодичних електромагнітних коливань (лінії електропередач, системи запалення двигунів внутрішнього згорання, високочастотна апаратура для дуго-

основі застосування засобів оперативного контролю і реєстрації та повинен охоплювати як несанкціоновані, так і санкціоновані дії користувачів.

Основні **вимоги**, що пред'являються до комплексної системи захисту інформації:

- має бути *прив'язана до цілей і завдань захисту інформації* на конкретному підприємстві;
- має бути *цілісною*, містити усі її складові, мати структурні зв'язки між компонентами, що забезпечують її погоджене функціонування;
- має бути *всеосяжною*, такою, що враховує усі об'єкти і складові, їх компоненти захисту, усі обставини і чинники, що впливають на безпеку інформації, і усі види, методи і засоби захисту;
- має бути *достатньою* для вирішення поставлених завдань і *надійною* в усіх елементах захисту, тобто базуватися на принципі *гарантованого результату*;
- має бути «*вмонтованою*» в технологічні схеми збору, зберігання, обробки, передачі і використання інформації;
- має бути компонентно, логічно, технологічно і економічно *обгрунтованою*;
- має бути такою, що реалізовується, *забезпечується усіма необхідними ресурсами*;
- має бути *простою* і *зручною* в експлуатації і управлінні, а також у використанні законними споживачами;
- має бути *безперервною*;
- має бути досить *гнучкою*, здатною до цілеспрямованого пристосування при зміні компонентів її складових частин, технології обробки інформації, умов захисту.

2.2 Основні терміни та визначення

1. <u>Закон України «Про інформацію»</u> (Відомості Верховної Ради України, 1992, № 48, ст. 650):

❖ **Документ** – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі.

❖ **Захист інформації** – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісності інформації та належний порядок доступу до неї;

❖ **Інформація** – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

2. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» (Відомості Верховної Ради України, 2007, № 12, ст. 102):

❖ **Інформаційна безпека** – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

3. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (Відомості Верховної Ради України, 2006, № 30, ст. 258):

❖ **Об'єкт інформаційної діяльності** – інженерно-технічна споруда (приміщення), де здійснюється діяльність, пов'язана з інформацією, що підлягає захисту.

4. Закон України «Про державну таємницю» (Відомості Верховної Ради України, 1994, № 16, ст. 93)

❖ **Державна таємниця (секретна інформація)** – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

електромагнітного поля для наведення (генерування) в ІТС електромагнітної енергії з рівнем, що викликає порушення нормального функціонування (збій в роботі) технічних і програмних засобів цих систем.

Причини умисного руйнування інформації:

- порушникові не вдається отримати інформацію технічними каналами;
- порушник прагне приховати сліди несанкціонованого доступу до інформації;
- вандалізм.

Основними **методами руйнування інформації** є:

- застосування завад;
- використання умисних силових електромагнітних впливів на інформаційні об’єкти і апаратно-програмне забезпечення ІТС;
- використання шкідливого програмного забезпечення;
- застосування закладних пристроїв (апаратних і програмних).

1. **Завада** (або **перешкода**) – це небажана електрична і (або) магнітна дія на систему або її частину, яка може привести до спотворення інформації, що зберігається, перетворюється, передається або оброблюється.

За *походженням* завади поділяються на:

- *неумисні природного походження* (космічні і атмосферні завади, шуми антених систем, внутрішні шуми приймачів);
- *неумисні штучного походження*;
- *організовані* (активні та пасивні).

Активні завади підрозділяється на:

- *маскуючі* (*загороджувальні*) – створюють шумовий фон у широкій смузі частот, на якому важко виділити корисний сигнал;
- *прицільні* – створюють шумовий фон великої потужності у вузькій смузі часто, енергетично пригнічуючи приймальні пристрої;
- *імітуючі* – підробка корисних сигналів по одному або декількох параметрах.

- перехоплення наведень інформаційних сигналів з ліній електроживлення і заземлення ТЗОІ;
- «високочастотного опромінення» ТЗОІ;
- впровадження в ТЗОІ закладних пристроїв.

Рис. 1.44 Способи перехоплення інформації в ТЗОІ

Методи і засоби руйнування інформації

Несанкціонована дія на інформацію, що захищається, – це дія з порушенням встановлених прав і правил доступу, яка призводить до витоку, спотворення, підробки, знищення, блокування доступу до інформації, а також до втрати, знищення або збою функціонування носія інформації та засобів її оброблення і передачи.

Найбільш небезпечною несанкціонованою дією є **умисна силова електромагнітна дія на інформацію**, здійснювана шляхом застосування джерела

❖ **Гриф секретності** – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації.

❖ **Засекречування матеріальних носіїв інформації** – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації.

❖ **Категорія режиму секретності** – категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях.

❖ **Матеріальні носії секретної інформації** – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо.

❖ **Охорона державної таємниці** – комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв.

❖ **Ступінь секретності** («особливої важливості», «цілком таємно», «таємно») – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

5. <u>Закон України «Про захист інформації в інформаційно- телекомунікаційних системах»</u> (Відомості Верховної Ради України, 1994, № 31, ст. 286):

❖ **Блокування інформації в системі** – дії, внаслідок яких унеможливлюється доступ до інформації в системі.

❖ **Виток інформації** – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

❖ **Доступ до інформації в системі** – отримання користувачем можливості обробляти інформацію в системі.

❖ **Захист інформації в системі** – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі.

❖ **Знищення інформації в системі** – дії, внаслідок яких інформація в системі зникає.

❖ **Інформаційна (автоматизована) система** – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

❖ **Інформаційно-телекомунікаційна система** – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

❖ **Комплексна система захисту інформації** – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

❖ **Криптографічний захист інформації** – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

❖ **Несанкціоновані дії щодо інформації в системі** – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства.

❖ **Обробка інформації в системі** – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів.

❖ **Порушення цілісності інформації в системі** – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст.

❖ **Порядок доступу до інформації в системі** – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації.

❖ **Телекомунікаційна система** – сукупність технічних і програмних за-

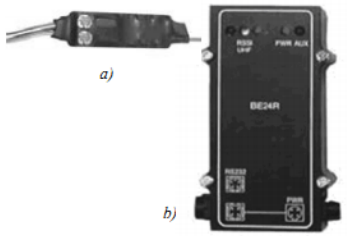

Рис. 1.43 Апаратный кейлоггер BE24 (а) з передачею інформації радіоканалом і приймальний пристрій BE24 СК (в)
(передача перехоплених даних здійснюється на частотах 300 – 306 МГц, потужність передавача складає 1-100 мВт, що забезпечує передачу інформації на дальності від 50 до 500 м і більш)

Апаратні закладки для перехоплення інформації, що виводиться на принтер, встановлюються в корпусі принтера і за принципом роботи аналогічні апаратними кейлогерам.

Апаратні закладки для перехоплення інформації, записуваної на жорсткий диск комп'ютера, є найбільш складними. Вони включають блоки перехоплення, обробки, передачі, управління і живлення, потайно встановлюються в системному блоці комп'ютера і контактно підключаються до інтерфейсу, що сполучає жорсткий диск з материнською платою.

Перехоплювані сигнали поступають в блок спеціальної обробки, що включає спеціалізований процесор, де здійснюється їх обробка за спеціальною програмою. Файли із заданим розширенням (наприклад, *.doc) записуються в оперативну або flash–пам'ять. Командою управління записана в пам'яті інформація в цифровому виді радіоканалом або мережею 220 В передається на приймальний пункт, де у вигляді окремих файлів записується на жорсткий диск для подальшої обробки. Приймальний комплекс складається з радіоприймального пристрою, модему, ноутбука і спеціального програмного забезпечення.

Таким чином, перехоплення інформації, що обробляється технічними засобами, може здійснюватися шляхом (рис. 1.44):

- перехоплення ПЕМВ, що виникають при роботі технічних засобів;
- перехоплення наведень інформаційних сигналів із сполучних ліній ДТЗС і сторонніх провідників;

суватися на жорсткий диск для подальшої обробки.

Блок дистанційного управління призначений для дистанційного включення і виключення закладного пристрою і встановлення параметрів роботи передавального пристрою.

Приймальний комплекс складається з радіоприймального пристрою, модему, ноутбука і спеціального програмного забезпечення.

Апаратні закладки для перехоплення інформації, що вводиться з клавіатури комп'ютера, потайно встановлюються в корпусі клавіатури або усередині системного блоку і підключаються до інтерфейсу клавіатури. Вони призначені, в основному, для перехоплення паролів користувачів і текстових документів і складаються з модуля перехоплення, передавального блоку і блоку управління. Живлення закладок здійснюється від інтерфейсу клавіатури (рис. 1.42).

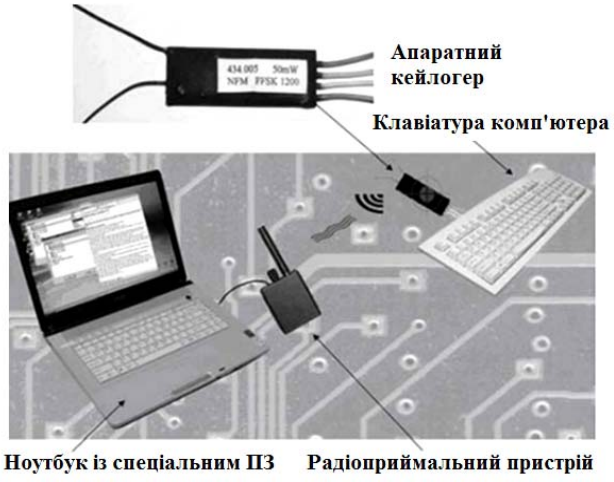

Рис. 1.42 Приклад застосування апаратного кейлогера

Перехоплювана інформація може або передаватися радіоканалом, або записуватися на flash-пам'ять.

Приймальний комплекс складається з радіоприймального пристрою, спеціального модемного модуля (модему), ноутбука і спеціального програмного забезпечення (рис. 1.43).

собів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

❖ **Технічний захист інформації** – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

6. Закон України «Про електронні документи та електронний документообіг» (Відомості Верховної Ради України, 2003, № 36, ст. 275):

❖ **Електронний документ** – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

7. Закон України «Про електронний цифровий підпис» (Відомості Верховної Ради України, 2003, № 36, ст. 276):

❖ **Електронний підпис** – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних.

❖ **Електронний цифровий підпис** – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

8. Закон України «Про ліцензування певних видів господарської діяльності» (Відомості Верховної Ради України, 2000, № 36, ст. 299):

❖ **Ліцензія** – документ державного зразка, який засвідчує право ліцензіа-

та на провадження зазначеного в ньому виду господарської діяльності протягом визначеного строку у разі його встановлення Кабінетом Міністрів України за умови виконання ліцензійних умов.

❖ **Ліцензування** – видача, переоформлення та анулювання ліцензій, видача дублікатів ліцензій, ведення ліцензійних справ та ліцензійних реєстрів, контроль за додержанням ліцензіатами ліцензійних умов, видача розпоряджень про усунення порушень ліцензійних умов, а також розпоряджень про усунення порушень законодавства у сфері ліцензування.

Офіційне тлумачення термінів та визначень, які використовуються при побудові комплексної системи захисту інформації, наводяться в:

- **ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення**;

- **НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу**.

Терміни, регламентовані у цих документах, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації, і рекомендовані для використання у довідковій та навчально- методичній літературі, що належить до сфери технічного захисту інформації.

❖ **Автоматизована система (ІТС)** – організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється. АС (ІТС) класифікується як:

- **АС (ІТС) класу 1** – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності (наприклад, автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів);

- **АС (ІТС) класу 2** – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності (наприклад, локальна обчислювальна мережа). Істотна відміна від попереднього класу – наявність користувачів з різними повноваженнями по доступу і/або те-

Рис. 1.40 Схема технічного каналу витоку інформації, що створюється шляхом впровадження у ТЗОІ закладних пристроїв

Для перехоплення різних видів інформації в ТЗОІ використовуються апаратні закладки (рис. 1.41).

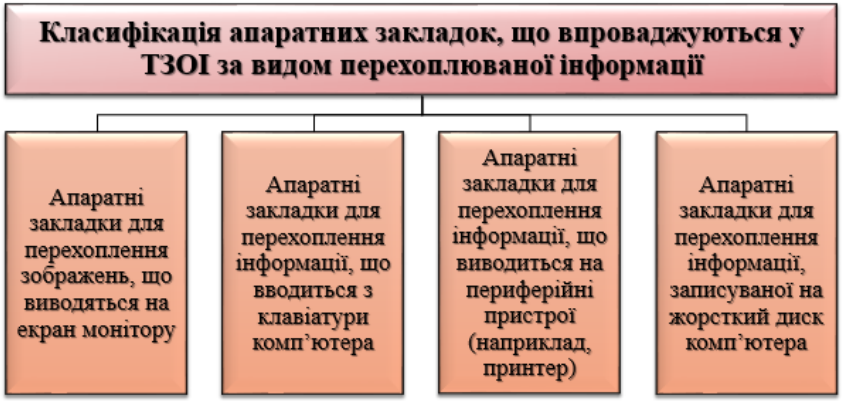

Рис. 1.41 Класифікація апаратних закладних пристроїв

Апаратні закладки для перехоплення зображень, що виводяться на екран монітора, складаються з блоку перехоплення і компресії, передавального блоку, блоку управління і блоку живлення. Вони потайно встановлюються, як правило, в корпусі монітора (можлива установка закладки і в системному блоці комп'ютера) і контактно підключаються до кабелю монітора.

Перехоплене відеозображення в цифровому виді передається радіоканалом, лінії електромережі 220 В або виділеній лінії на приймальний пункт, де відновлюється і відображується на екрані комп'ютера в реальному масштабі часу, створюючи «копію» екрану, а додаткова інформація може запи-

Рис. 1.38 Схема технічного каналу витоку інформації, створюваного шляхом «високочастотного опромінення» ТЗОІ

Для перехоплення інформації, оброблюваною ТЗОІ, можливе використання електронних пристроїв перехоплення інформації (закладних пристроїв), потайно впроваджуваних в технічні засоби і системи.

Рис. 1.39 Приклад перехоплення інформації, оброблюваної ТЗОІ, шляхом установки в них закладних пристроїв

Перехоплена за допомогою закладних пристроїв інформація або безпосередньо передається радіоканалом, або спочатку записується в спеціальний запам'ятовуючий пристрій, а вже потім командою управління передається радіоканалом. Для передачі інформації також можуть використовуватися лінії електроживлення ТЗОІ або оптичний (інфрачервоний) канал.

хнічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності;

- **АС (ІТС) класу 3** – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності (наприклад, глобальна мережа). Істотна відміна від попереднього класу – необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

❖ **Обчислювальна система (ОС)** – сукупність програмно-апаратних засобів, призначених для обробки інформації.

❖ **Комп'ютерна система (КС)** – сукупність програмно-апаратних засобів, яка подана для оцінки.

❖ **Політика безпеки інформації** – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

❖ **Загроза** – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків ІТС.

❖ **Атака** – спроба реалізації загрози.

❖ **Безпека інформації** – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

❖ **Захист інформації в ІТС** – діяльність, яка спрямована на забезпечення безпеки оброблюваної в ІТС інформації та ІТС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

❖ **Комплексна система захисту інформації (КСЗІ)** – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

❖ **Комплекс засобів захисту (КЗЗ)** – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

❖ **Виток інформації** – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї.

❖ **Несанкціонований доступ до інформації (НСД)** – доступ до інформації, здійснюваний з порушенням посадових повноважень співробітника.

❖ **Захист від несанкціонованого доступу** – запобігання або істотне утруднення несанкціонованого доступу до інформації.

❖ **Конфіденційність інформації** – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

❖ **Цілісність інформації** – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

❖ **Доступність** – властивість ресурсу системи (комп'ютерної системи, послуги, об'єкта комп'ютерної системи, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

❖ **Спостереже їсть** – властивість комп'ютерної системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

❖ **Система технічного захисту інформації** – сукупність організаційних структур, нормативно-правових документів та матеріально-технічної бази (основними елементами матеріально-технічної бази системи ТЗІ є технічні засоби із захистом, засоби технічного захисту інформації та засоби контролю за ефективністю технічного захисту інформації).

❖ **Технічний захист інформації** – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформа-

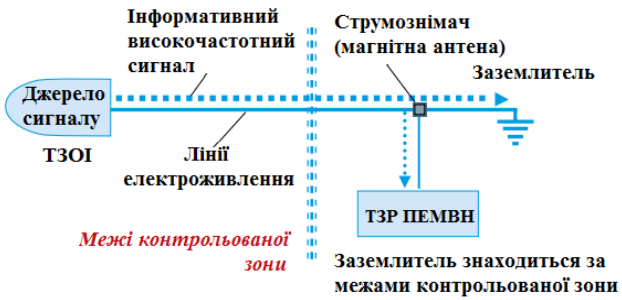

Рис. 1.36 Схема технічного каналу витоку інформації, що виникає за рахунок наведень інформативних сигналів в ланцюгах заземлення ТЗОІ

Спеціально створювані технічні канали витоку інформації. Разом з пасивними способами перехоплення інформації, оброблюваною ТЗОІ, можливе використання і активних способів, зокрема, способу «високочастотного опромінення», при якому ТЗОІ опромінюється потужним високочастотним гармонійним сигналом (для цих цілей використовується високочастотний генератор із спрямованою антеною, що має вузьку діаграму спрямованості) (рис. 1.37). При взаємодії опромінюючого електромагнітного поля з елементами ТЗОІ відбувається модуляція вторинного випромінювання інформативним сигналом. Перевипромінюваний сигнал приймається приймальним пристроєм засобу розвідки і детектується.

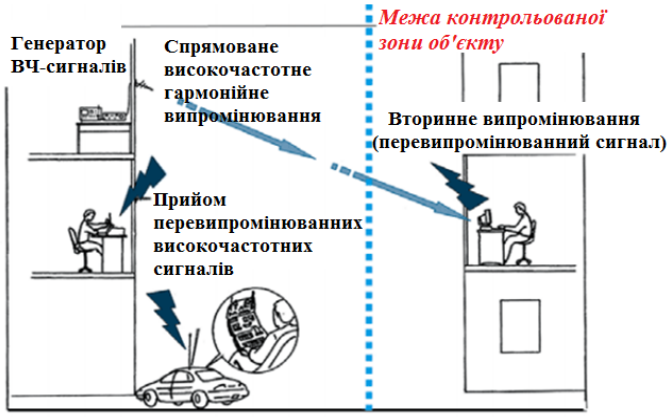

Рис. 1.37 Приклад технічного каналу витоку інформації, створюваного шляхом «високочастотного опромінення» ТЗОІ

2) відстань від ТЗОІ до випадкової зосередженої антени була менш *r*1, а відстань до випадкової розподіленої антени була менш *r*1';

3) була можливість безпосереднього підключення до випадкової антени за межами контрольованої зони об'єкту засобів розвідки ПЕМВН;

4) за межами контрольованої зони повинна існувати можливість безпосереднього підключення до ліній електроживлення і заземлення ТЗОІ, до сполучних ліній ДТЗС або до сторонніх провідників портативних засобів розвідки ПЕМВН.

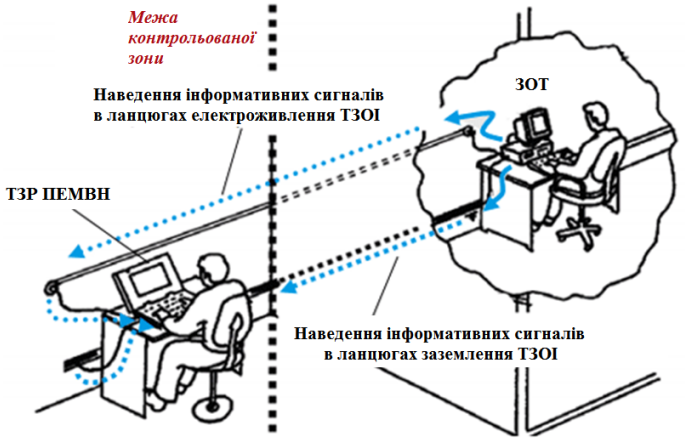

Рис. 1.34 Приклад перехоплення інформативних сигналів при підключенні засобів розвідки ПЕМВН до ліній електроживлення і заземлення ТЗОІ

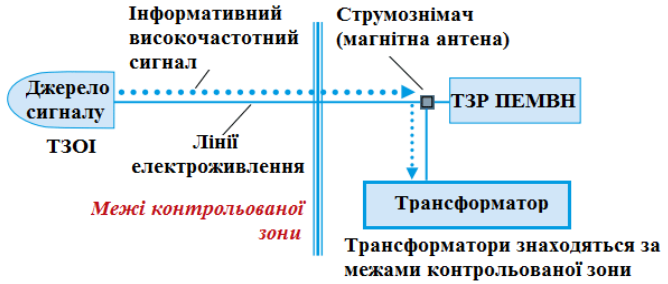

Рис. 1.35 Схема технічного каналу витоку інформації, що виникає за рахунок наведень інформативних сигналів в лініях електроживлення ТЗОІ

ції, порушення цілісності та режиму доступу до інформації.

❖ **Технічний канал витоку інформації** – сукупність носія інформації, середовища його поширення та засобу технічної розвідки.

❖ **Побічне електромагнітне випромінення і наведення (ПЕМВН)** – електромагнітне випромінення та наведення, що є побічним результатом функціонування технічного засобу і може бути носієм інформації.

❖ **Контрольована зона** – територія, допуск осіб на яку обмежений та знаходиться під контролем.

Висновки

1. КСЗІ – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

2. До складу КСЗІ входять: служба захисту інформації, фізична охорона об’єктів, інженерно-технічні заходи, комплекс засобів захисту від НСД, комплекс засобів блокування технічних каналів витоку інформації, комплекс засобів криптографічного захисту, регламенти дій користувачів.

3. Принципи створення КСЗІ: законність, системність, комплексність, неперервність, своєчасність, неперервність вдосконалення, достатність, персональна відповідальність, мінімізація повноважень, гнучкість системи захисту, простота застосування засобів захисту, обґрунтованість та технічна реалізованість, спеціалізація та професіоналізм, обов’язковість контролю.

4. Офіційне тлумачення термінів та визначень КСЗІ наводяться в ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення, НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Терміни, регламентовані у цих документах, обов'язкові для використання.

Контрольні питання

1. Дайте визначення КСЗІ. Які цілі вона переслідує і які завдання вирішує?

2. Визначте склад КСЗІ.
3. Що є об'єктами захисту в КСЗІ?
4. Які види інформації підлягають захисту в ІТС?
5. Визначите склад суб'єктів інформаційних відношень в ІТС.
6. Розкрийте суть принципів системності і комплексності при створенні КСЗІ.
7. У яких цілях реалізується принцип обов'язковості контролю при створенні КСЗІ?
8. Визначите основні вимоги до КСЗІ.
9. У яких документах містяться визначення і основна термінологія КСЗІ?
10. Дайте визначення ІТС. Які існують класи ІТС?

Простір навколо ТЗОІ, на межі і за межами якого рівень напруги наведеного від ТЗОІ інформативного сигналу в зосереджених антенах не перевищує допустимого (нормованого) значення ($U = U_н$), називається **небезпечною зоною 1** ($r1$), а в розподілених антенах – **небезпечною зоною 1'** ($r1'$).

Розмір зони $r1$ ($r1'$) залежить не лише від рівня ПЕМВ ТЗОІ, але і від довжини випадкової антени (від приміщення, в якому встановлене ТЗОІ до місця можливого підключення до неї засобів розвідки).

Зони $r1$ ($r1'$) для кожного ТЗОІ визначаються інструментально-розрахунковим методом без урахування затухання сигналів у випадкових антенах при проведенні спеціальних досліджень технічних засобів на ПЕМВН і вказується в приписі на їх експлуатацію або сертифікаті відповідності, а з урахуванням реального затухання сигналів у випадкових антенах – при атестації об'єкту інформатизації.

Схема електричного каналу витоку інформації, що виникає за рахунок наведень ПЕМВ ТЗОІ у випадкових антенах приведена на рис. 1.33.

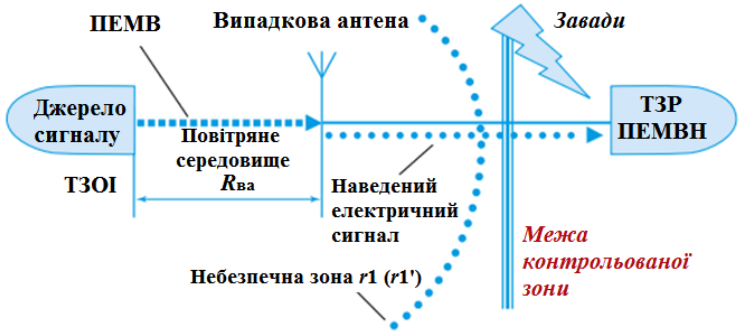

Рис. 1.33 Схема електричного каналу витоку інформації, що виникає за рахунок наведень ПЕМВ ТЗОІ у випадкових антенах

Для виникнення електричного каналу витоку інформації необхідно, щоб:

1) сполучні лінії ДТЗС, лінії електроживлення, сторонні провідники і т.д., що виконують роль випадкових антен, виходили за межі контрольованої зони об'єкту;

- наведення в електричних ланцюгах ТЗОІ, викликані внутрішніми ємнісними і (або) індуктивними зв'язками («просочування» інформативних сигналів в ланцюзі електроживлення через блоки живлення ТЗОІ);

- наведення в ланцюгах заземлення ТЗОІ, викликані інформативними ПЕМВ ТЗОІ, а також гальванічним зв'язком схемної (робочої) землі і блоків ТЗОІ.

Приклад перехоплення наведень інформативних сигналів з інженерних комунікацій технічним засобом розвідки ПЕМВН показан на рис. 1.32.

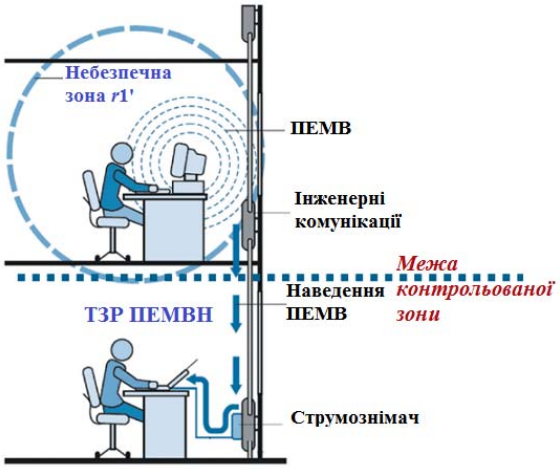

Рис. 1.32 Перехоплення наведень інформативних сигналів з інженерних комунікацій

Випадкові антени можуть бути:

- *зосередженими* – компактні технічні засоби (телефонний апарат, гучномовець радіотрансляційної мережі, датчик пожежної сигналізації і т.д.), підключені до ліній, що виходять за межі контрольованої зони;

- *розподіленими* – випадкові антени з розподіленими параметрами: кабелі, дроти, металеві труби та інші струмопровідні комунікації, що виходять за межі контрольованої зони. Рівень сигналів, що наводяться в них, значною мірою залежить не лише від потужності випромінюваних сигналів, але і відстані до них від ТЗОІ.

3. Правові підстави та основні положення щодо створення КСЗІ та комплексу ТЗІ в Україні

3.1 Структура законодавства України в області захисту інформації

Право – це сукупність загальнообов'язкових правил і норм поведінки, які встановлені або санкціоновані державою по відношенню до певних сфер життя та діяльності державних органів, підприємств (організацій) та населення.

Правовий захист інформації – це спеціальні правові акти, правила, процедури та заходи, які забезпечують захист інформації на правовій основі.

Правовий захист інформації як ресурс признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами (рис. 1.7).

Рис. 1.7 Система нормативно-правових документів в Україні, що регламентують питання захисту інформації

В Україні такими правовими (актами, нормами) є:

- Конституція;
- закони України;
- адміністративне, кримінальне право, викладені у відповідних кодексах.

Відомчі нормативні акти визначаються:

- наказами;
- розпорядженнями;
- положеннями;
- інструкціями, що видаються відомствами, організаціями і підприємствами, діючими у рамках певних структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу і змісту, співвідношення його з усією системою законів і правових актів України.

Рис. 1.8 Структура законодавства України в області захисту інформації

як за рахунок ПЕМВ, так і за наявності внутрішніх паразитних ємнісних і (або) індуктивних зв'язків випрямного облаштування блоку живлення ТЗОІ. Наприклад, в підсилювачі низької частоти струми посилюваних сигналів замикаються через джерело електроживлення, створюючи на його внутрішньому опорі падіння напруги, яка при недостатньому загасанні у фільтрі випрямного пристрою може бути виявлена в лінії електроживлення за наявності магнітного зв'язку між вихідним трансформатором підсилювача і трансформатором випрямного пристрою.

Окрім заземляючих провідників, що служать для безпосереднього з'єднання ТЗОІ з контуром заземлення, гальванічний зв'язок із землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий дріт мережі електроживлення, екрани (металеві оболонки) сполучних кабелів, металеві труби систем опалювання і водопостачання, металева арматура залізобетонних конструкцій і т.д. Усі ці провідники спільно із заземляючим пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали.

Крім того, в грунті навколо заземляючого пристрою виникає електромагнітне поле, яке також є джерелом інформації.

Різні допоміжні технічні засоби, їх сполучні лінії, а також лінії електроживлення, сторонні провідники і ланцюги заземлення грають роль *випадкових антен*, при безпосередньому (через струмознімач або індукційний датчик) підключенні до яких засоби розвідки ПЕМВН можливе перехоплення інформаційних сигналів.

Залежно від причин виникнення наведення інформативних сигналів можна розділити на:

- наведення в електричних ланцюгах ТЗОІ, викликані інформативними побічними і (або) паразитними електромагнітними випромінюваннями ТЗОІ;
- наведення в сполучних лініях ДТЗС і сторонніх провідниках, викликані інформативними побічними і (чи) паразитними електромагніт-ними випроміню-ваннями ТЗОІ;

методом при проведенні спеціальних досліджень ТЗОІ на ПЕМВ і вказується в приписі на їх експлуатацію або сертифікаті відповідності.

Умови для виникнення електромагнітного каналу витоку інформації (рис. 1.31):

1) відстань від ТЗОІ до межі контрольованої зони має бути менш зони $R2$ ($R < R2$);

2) в межах зони $R2$ можливе розміщення стаціонарних або перевозимих (переносимих) засобів розвідки ПЕМВН

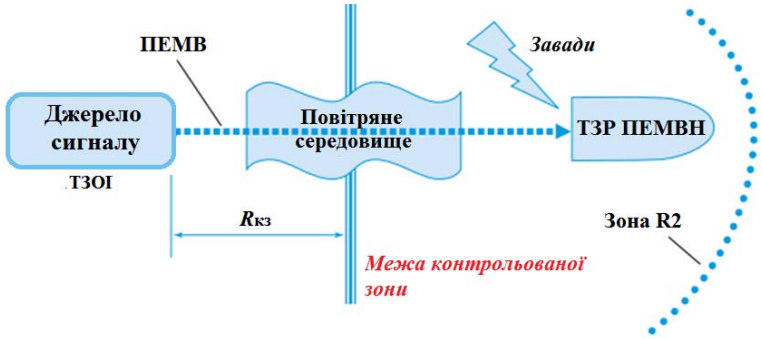

Рис. 1.31 Умови для виникнення електромагнітного каналу витоку інформації

Електричні канали витоку інформації (ЕКВІ). Причинами виникнення ЕКВІ є *наведення інформативних сигналів*.

Наведення інформативних сигналів – це струми і напруга в струмопровідних елементах, викликани побічними електромагнітними випромінюваннями, ємнісними та індуктивними зв'язками елементів електронних схем.

Де виникають наведення інформативних сигналів:

- у лініях електроживлення ТЗОІ;
- у лініях електроживлення і сполучних лініях ДТЗС;
- у ланцюгах заземлення ТЗОІ і ДТЗС;
- у сторонніх провідниках (металевих трубах систем опалювання, водопостачання, металоконструкціях і т.д.).

Поява інформаційних сигналів в ланцюзі електроживлення ТЗОІ можливо

Вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, у тому числі і в (рис. 1.8):

- *конституційне законодавство* – норми, що стосуються питань інформатизації та захисту інформації, які входять до конституційного законодавства як складові елементи;
- *основні загальні закони та кодекси* – норми з питань інформатизації та захисту інформації;
- *закони з організації державної системи управління* – закони стосовно окремих структур господарства, економіки, системи державних органів та визначення їх статусу, які включають окремі норми з питань захисту інформації;
- *спеціальні закони* – сукупність законів, які закладають основи правового забезпечення інформаційної безпеки;
- *підзаконні нормативні акти* – стандарти, загальнодержавні та відомчі нормативні документи, що орієнтовані на забезпечення захисту інформації.

Спираючись на державні правові акти і враховуючи відомчі інтереси на рівні конкретної організації, розробляються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки. До таких документів відносяться:

- положення про збереження конфіденційної інформації;
- перелік відомостей, що становлять конфіденційну інформацію;
- інструкція про порядок допуску співробітників до відомостей, що становлять конфіденційну інформацію;
- положення про спеціальне діловодство і документообіг;
- перелік відомостей, дозволених до публікації в пресі;
- положення про роботу з іноземними фірмами та їх представниками;
- зобов'язання співробітника про збереження конфіденційної інформації;
- пам'ятка співробітникові про збереження комерційної таємниці та ін.

Конфіденційна інформація – інформація з обмеженим доступом, яка містить відомості, що перебувають у володінні, користуванні або розпорядженні фізичних чи юридичних осіб або держави, та порядок доступу до якої обмежується ними. Вона може бути:

- *особиста* – відомості про факти, події і обставини приватного життя громадян, які дозволяють ідентифікувати його особу (персональні дані), за винятком відомостей, що підлягають поширенню в ЗМІ у встановленому Законом порядку;

- *судово-слідча* – відомості, які складають таємницю слідства і судочинства;

- *службова* – службові відомості, доступ до яких обмежений органами державної влади (службова таємниця);

- *професійна таємниця* – відомості, пов'язані з професійною діяльністю, доступ до яких обмежений Законами (лікарська, нотаріальна, адвокатська таємниця, таємниця листування, телефонних переговорів та ін.);

- *комерційна*, *банківська* – відомості, пов'язані з комерційною (банківською) діяльністю, доступ до яких обмежений Законом (комерційна, банківська таємниця);

- *виробнича* – відомості про суть винаходу, моделі або промислового зразка до офіційної публікації інформації про них.

Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Таблиця 1.1 Основні параметри комерційної таємниці

Визначення	Зміст
СУБ'ЄКТ	Підприємства, організації, колективи, громадяни
ОБ'ЄКТ	Поняття застосоване до широкого спектру інтелектуальної і промислової власності
ХАРАКТЕРИСТИКИ	Активний ресурс Конфіденційна інформація Особлива форма власності Товар ринкової новизни

засобами розвідки побічних електромагнітних випромінювань і наведень (ТЗР ПЕМВН).

Типовий комплекс розвідки ПЕМВ включає спеціальний приймальний пристрій, ПЕОМ (або монітор), спеціальне програмне забезпечення і широкодіапазонну спрямовану антену (рис. 1.29).

Рис. 1.29 Комплекс перехоплення ПЕМВ ТЗОІ
(включає спеціальне приймальне облаштування PKI 2715 (дальність перехоплення ПЕМВ від 10 до 50 м) і широкосмугова спрямована антена R&SHЬ 007 (діапазон частот від 80 МГц до 1,3 ГГц, коефіцієнт посилення 5 – 7 дБ)

Перехоплення побічних електромагнітних випромінювань ТЗОІ технічними засобами розвідки показано на рис. 1.30.

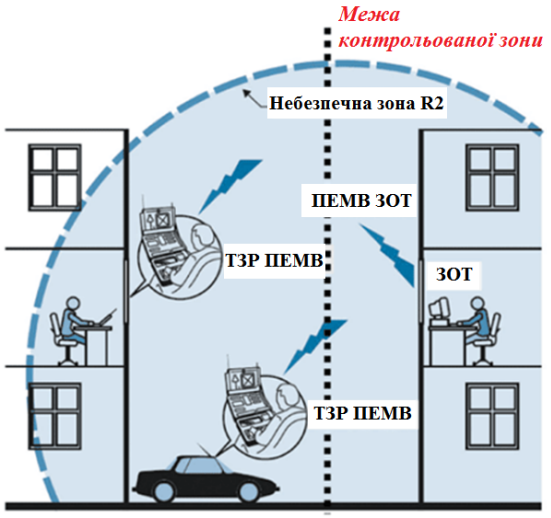

Рис. 1.30 Приклади перехоплення ПЕМВ технічними засобами розвідки

Простір навколо ТЗОІ, на межі і за межами якого напруженість електричної (***E***) або магнітної (***H***) складової електромагнітного поля не перевищує допустимого (нормованого) значення ($\boldsymbol{E} \le \boldsymbol{E}_н$; $\boldsymbol{H} \le \boldsymbol{H}_н$) називається **небезпечною зоною 2** (*R*2).

Зона *R*2 для кожного ТЗОІ визначається інструментально-розрахунковим

- генератори стирання і підмагнічування магнітофонів;
- гетеродини радіоприймальних і телевізійних пристроїв;
- генератори вимірювальних приладів і т.д.

Рис. 1.28 ілюструє можливі режими роботи обчислювальної техніки, в яких виникають ПЕМВ. Діапазон можливих частот ПЕМВ ЗОТ може складати 10 кГц – 2 ГГц.

Рис. 1.28 Режими оброблення інформації в ЗОТ, в яких виникають ПЕМВ

Паразитне електромагнітне випромінювання ТЗОІ – це побічне радіовипромінювання, що виникає в результаті самозбудження генераторних або підсилювальних блоків ТЗОІ із-за паразитних зв'язків. Найчастіше такі зв'язки виникають за рахунок випадкових перетворень негативних зворотних зв'язків (індуктивних або ємнісних) в паразитні позитивні, що призводить до переводу підсилювача з режиму посилення в режим автогенерації сигналів. Частота автогенерації (самозбудження) лежить в межах робочих частот нелінійних елементів підсилювачів (наприклад, напівпровідникових приладів, електровакуумних ламп і т.п.).

У ряді випадків паразитне електромагнітне випромінювання модулюється інформативним сигналом відповідно до змін параметрів інформативного сигналу, що впливають на нього.

Для перехоплення ПЕМВ ТЗОІ використовуються спеціальні стаціонарні, переносимі та перевозимі приймальні пристрої, які називаються **технічними**

ЦІННІСТЬ	Реально (потенційно) створює переваги в конкурентній боротьбі
ВИМОГИ	Потенційно корисна Не загальновідома
ТЕРМІН ДІЇ	Визначається життєвим циклом товару
ЗАХИСТ	Правовий Організаційний Інженерно-технічний

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці (*ст. 505 Цивільного кодексу України*).

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які подальші претензії до недобросовісного співробітника, клієнта, конкурента і посадовця виявляться просто безпідставними.

Якщо перелік відомостей конфіденційного характеру не доведений своєчасно до кожного співробітника (природно, якщо він допущений по посадових обов'язках) письмово, то співробітник, що вкрав важливу інформацію, порушуючи встановлений порядок роботи з нею, швидше за все розведе руками: звідки мені це знать!

В цьому випадку ніякі інстанції, аж до судових, не зможуть допомогти.

Правові норми забезпечення безпеки і захисту інформації на конкретному підприємстві відбиваються в сукупності засновницьких, організаційних і функціональних документів.

Правові вимоги забезпечення безпеки і захисту інформації відбиваються в **Статуті** у вигляді наступних положень:

- підприємство має право визначати склад, об'єм і порядок захисту відомостей конфіденційного характеру, вимагати від своїх співробітників забезпечення їх збереження і захисту від внутрішніх і зовнішніх загроз;
- підприємство зобов'язане забезпечити збереження конфіденційної інформації.

Це дозволяє адміністрації підприємства:

- створювати організаційні структури із захисту конфіденційної інформації;
- видавати нормативні та розпорядливі документи, які визначають порядок виділення відомостей конфіденційного характеру і механізми їх захисту;
- включати вимоги із захисту інформації в угоди з усіх видів господарської діяльності;
- вимагати захисту інтересів підприємства з боку державних і судових інстанцій;
- розпоряджатися інформацією, що являється власністю підприємства, в цілях отримання вигоди і недопущення економічного збитку колективу підприємства і власникові засобів виробництва;
- розробити «Перелік відомостей конфіденційної інформації».

Таким чином, правове регулювання потрібне для:

- вдосконалення механізму попередження протиправних дій по відношенню до інформаційних ресурсів;
- уточнення і закріплення завдань і правомірності окремих суб'єктів у сфері попереджувальної діяльності;
- охорони прав і законних інтересів громадян і організацій.

3.2 Основні положення правових норм щодо створення КСЗІ та комплексів ТЗІ

1. Конституція України (Відомості Верховної Ради України, 1996, № 30, ст. 141): «*Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу*» (ст. 17).

2. Закон України «Про інформацію» (Відомості Верховної Ради України, 1992, № 48, ст. 650) регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Основні **напрями державної інформаційної політики** (ст. 3):

- перехоплення наведень інформативних сигналів із сполучних ліній ДТЗС і сторонніх провідників;
- перехоплення наведень інформативних сигналів з ліній електроживлення і заземлення ЗОТ;
- «високочастотного опромінення» ЗОТ;
- впровадження у ЗОТ закладних пристроїв.

Електромагнітні канали витоку інформації. В електромагнітних каналах витоку інформації (ЕМКВІ) носієм небезпечної інформації є *електромагнітні випромінювання* (ЕМВ), що виникають при обробці інформації ТЗОІ. Причини виникнення цих каналів показані на рис. 1.27.

Рис. 1.27 Причини виникнення електромагнітних каналах витоку інформації

У деяких ТЗОІ (наприклад, системах звукопідсилення) носієм інформації є електричний струм, параметри якого (сила струму, напруга, частота і фаза) змінюються за законом зміни інформаційного мовного сигналу. При протіканні електричного струму струмоведучими елементами ТЗОІ та їх сполучними лініями в просторі, що оточує їх, виникає змінне електричне і магнітне поле. Через це елементи ТЗОІ є випромінювачами електромагнітного поля, яке модулюється за законом зміни інформаційного сигналу.

Ініціаторами виникнення ПЕМВ можуть бути різного роду високочастотні генератори:

- задаючі генератори;
- генератори тактової частоти;

Рис. 1.25 Схема технічного каналу витоку інформації в ТЗОІ

Порушники для перехоплення інформації використовують **технічні засоби розвідки** (ТЗР). Інші зацікавлені суб'єкти (юридичні особи, групи фізичних осіб, окремі фізичні особи) для перехоплення інформації використовують **спеціальні технічні засоби** (СТЗ), пристосовані або допрацьовані для негласного отримання інформації.

Класифікація технічних каналів витоку інформації приведена на рис. 1.26.

Рис. 1.26 Класифікація технічних каналів витоку інформації в ІТС

Перехоплення інформації, що обробляється ЗОТ, може здійснюватися шляхом:

- перехоплення ПЕМВ, що виникають при роботі ЗОТ;

1) забезпечення доступу кожного до інформації;

2) забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

3) забезпечення інформаційної безпеки України;

4) забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;

5) сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору;

6) створення умов для формування в Україні інформаційного суспільства;

7) постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

8) створення інформаційних систем і мереж інформації, розвиток електронного урядування.

Суб'єкти інформаційних відносин (ст. 4)):

- фізичні особи;
- юридичні особи;
- об'єднання громадян;
- суб'єкти владних повноважень.

Об'єкт інформаційних відносин – *інформація* (ст. 4).

1.9 Класифікація інформації за порядком доступу

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів влад-

них повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

3. Закон України «Про державну таємницю» (Відомості Верховної Ради України, 1994, № 16, ст. 93) регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України.

Сфери, у яких інформація може бути віднесена до державної таємниці (ст. 8):

- оборони;
- зовнішніх відносин;
- економіки, науки і техніки;
- державної безпеки та охорони правопорядку.

Основні організаційно-правові заходи щодо охорони державної таємниці (ст. 18):

- єдині вимоги до виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації;
- дозвільний порядок провадження діяльності, пов'язаної з державною таємницею (ДТ);
- обмеження оприлюднення, передачі іншій державі або поширення іншим шляхом секретної інформації;
- обмеження щодо перебування та діяльності в Україні іноземців, осіб без громадянства та іноземних юридичних осіб, їх доступу до ДТ, а також розташування і переміщення об'єктів і технічних засобів, що їм належать;
- режим секретності державних органів, органів місцевого самоврядування, підприємств, установ і організацій, що провадять діяльність, пов'язану з ДТ;
- спеціальний порядок допуску та доступу громадян до ДТ;

меженого доступу, ДТЗС, приміщень або об'єктів (будівель, споруд), в яких вони встановлені.

Виділені приміщення (ВП) – приміщення, призначені для ведення закритих переговорів, що містять відомості з обмеженим доступом.

Приміщення, що захищаються, – приміщення, призначені для ведення конфіденційних переговорів.

Об'єкти інформатизації, що захищаються, виділені приміщення, а також приміщення, що захищаються повинні атестовуватися за вимогами безпеки інформації.

Об'єкти засобів обчислювальної техники (ЗОТ) – об'єкти інформатизації, на яких обробка інформації здійснюється з використанням комп'ютерної техніки.

Об'єкт інформатизації, як об'єкт розвідки з боку порушника, включає ряд джерел (рис. 1.24), що дозволяють дістати доступ до закритих відомостей через перехоплення каналов витоку інформації.

Рис. 1.24 Об'єкт інформатизації, як об'єкт розвідки

Технічний канал витоку інформації (ТКВІ) – сукупність джерела інформативного сигналу (наприклад, ТЗОІ), технічного засобу, що здійснює перехоплення інформації, і фізичного середовища, в якому поширюється інформативний сигнал (рис. 1.25).

Допоміжні технічні засоби і системи (ДТЗС), які можуть знаходитися в приміщеннях розміщення ОТЗ:

- системи і засоби міського автоматичного телефонного зв'язку;
- системи і засоби передачі даних в системі радіозв'язку;
- системи і засоби охоронної і пожежної сигналізації;
- системи і засоби оповіщення і сигналізації;
- контрольно-вимірювальна апаратура;
- системи і засоби кондиціонування;
- системи і засоби дротяної радіотрансляційної мережі та прийому програм радіомовлення і телебачення;
- засоби електронної оргтехніки;
- системи і засоби електрочасофикації та інші технічні засоби і системи.

Сторонні провідники, що проходять через приміщення, в яких встановлені ТЗОІ і ДТЗС:

- дроти і кабелі системи електроживлення ТЗОІ і ДТЗС;
- системи заземлення;
- металеві труби систем опалювання;
- металеві труби водопостачання;
- інші струмопровідні металоконструкції.

Ряд сполучних ліній ДТЗС, сторонніх провідників, а також лінії електроживлення і заземлення можуть виходити за межі контрольованої зони об'єкту.

Контрольована зона (КЗ) – простір (територія, будівля, частина будівлі), в якому виключено неконтрольоване перебування сторонніх осіб (відвідувачів, працівників різних технічних служб, що не є співробітниками організації), а також транспортних засобів.

Межа контрольованої зони – периметр території організації, що охороняється, а також конструкції охороняємої будівлі або частини будівлі, якщо вони розміщені на території, що не охороняється.

Об'єкт інформатизації (ОІ), що захищається, – це сукупність інформаційних ресурсів, що містять відомості обмеженого доступу, ТЗОІ об-

– технічний та криптографічний захисти секретної інформації.

4. Закон України «Про основи національної безпеки України» (Відомості Верховної Ради України, 2003, № 39, ст. 351) визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності.

Загрози національним інтересам і національній безпеці України в інформаційній сфері (ст. 7):

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основні напрями державної політики з питань національної безпеки в інформаційній сфері (ст. 8):

– забезпечення інформаційного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері;

– вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

5. Закон України «Про захист інформації в інформаційно- телекомунікаційних системах» (Відомості Верховної Ради України, 1994, № 31, ст. 286) регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

1.10 Об’єкти та суб’єкти захисту в ІТС

Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинна оброблятися в системі із застосуванням ***комплексної системи захисту інформації*** *з підтвердженою відповідністю* (ст. 8).

Підтвердження відповідності здійснюється за результатами *державної експертизи*.

Для створення комплексної системи захисту інформації використовуються засоби захисту інформації, які мають *сертифікат відповідності* або *позитивний експертний висновок* за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації.

Відповідальність за забезпечення захисту інформації в системі покладається на *власника системи*. Власник системи утворює *службу захисту інформації* або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним (от. 9).

6. Закон України «Про ліцензування видів господарської діяльності» (Відомості Верховної Ради України, 2015, № 23, ст. 158) визначає види господарської діяльності, що підлягають ліцензуванню, порядок їх ліцензування,

розташування, наприклад, дротів в котушках індуктивності (міжвиткової відстані) призводить до зміни їх індуктивності, а, отже, до зміни частоти випромінювання генератора, тобто до частотної модуляції сигналу. Або дія акустичного поля на конденсатори призводить до зміни відстані між пластинами і, отже, до зміни його місткості, що, у свою чергу, також призводить до частотної модуляції високочастотного сигналу генератора. Найчастіше спостерігається паразитна модуляція інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, що знаходяться у виділених приміщеннях і мають конденсатори змінної ємності з повітряним діелектриком в коливальних контурах гетеродинів. Промодульовані інформаційним сигналом високочастотні коливання випромінюються в навколишній простір і можуть бути перехоплені і детектовані засобами радіорозвідки.

Технічні канали витоку інформації, що обробляється технічними засобами обробки інформації

Технічні засоби обробки інформації (ТЗОІ) обмеженого доступу:

- засоби обчислювальної техніки (ЗОТ) – технічні засоби ІТС, ЕОМ та їх окремі елементи;
- засоби виготовлення і розмноження документів;
- апаратура звукопідсилення, звукозапису, звуковідтворення і синхронного перекладу;
- системи внутрішнього телебачення;
- системи відеозапису і відеовідтворення;
- системи оперативно-командного зв'язку;
- системи внутрішнього автоматичного телефонного зв'язку та ін.

З точки зору захисту ці технічні засоби і системи називаються **основними технічними засобами** (**ОТЗ**).

Об'єкт інформатизації – сукупність інформаційних ресурсів, засобів і систем обробки інформації, використовуваних відповідно до заданої інформаційної технології, засобів забезпечення об'єкту інформатизації, приміщень або об'єктів (будівель, споруд, технічних засобів), в яких вони встановлені.

(стіни, стелі, підлоги), труби водопостачання, опалювання, каналізації та інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються контактні мікрофони (стетоскопи). Контактні мікрофони, сполучені з електронним підсилювачем називають *електронними стетоскопами*.

Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні і включають перехоплення акустичних коливань через ДТЗС, що мають «мікрофонний ефект», а також шляхом «високочастотного нав'язування».

Деякі елементи ДТЗС (трансформатори, котушки індуктивності, електромагніти вторинного електрогодинника, дзвінків телефонних апаратів, дроселі ламп денного світла, електрореле і т.п.) мають властивість змінювати свої параметри (місткість, індуктивність, опір) під дією акустичного поля, що створюється джерелом акустичних коливань. Зміна параметрів призводить або до появи на цих елементах електрорушійної сили, що змінюється за законом впливаючого інформаційного акустичного поля, або до модуляції струмів, що протікають по цих елементах, інформаційним сигналом.

Оптико-електронний (лазерний) канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відзеркалювальних поверхонь (стекол вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді і фазі (за законом вібрації поверхні) і приймається приймачем оптичного (лазерного) випромінювання, при демодуляції якого виділяється мовна інформація. Причому лазер і приймач оптичного випромінювання можуть бути встановлений в одному або різних місцях (приміщеннях).

В результаті дії акустичного поля міняється тиск на усі елементи високочастотних генераторів ТЗОІ і ДТЗС. При цьому змінюється (трохи) взаємне розташування елементів схем, дротів в котушках індуктивності, дроселів і т.п., що може привести до змін параметрів високочастотного сигналу, наприклад, до модуляції його інформаційним сигналом. Тому цей канал витоку інформації називається **параметричним**. Це обумовлено тим, що незначна зміна взаємного

встановлює державний контроль у сфері ліцензування, відповідальність суб'єктів господарювання та органів ліцензування за порушення законодавства у сфері ліцензування.

Ліцензуванню підлягають (ст. 7):

8) … *надання послуг у галузі криптографічного захисту інформації* (крім послуг електронного цифрового підпису) та *технічного захисту інформації*, за переліком, що визначається КМ України.

Постановою КМ України **«Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України»** (від 16.11.2016 № 821) визначається перелік послуг у галузі КЗІ (крім послуг електронного цифрового підпису) та ТЗІ, господарська діяльність щодо яких підлягає ліцензуванню:

I. Послуги у галузі КЗІ:

– розроблення і складення конструкторської та іншої технічної документації, виробництво криптосистем і засобів КЗІ (з наданням права провадження діяльності у галузі КЗІ, що становить державну таємницю; з наданням права провадження діяльності у галузі КЗ службової інформації);

– постачання, монтаж (встановлення), налаштування, технічне обслуговування (супроводження), ремонт та/або утилізація криптосистем і засобів КЗІ;

– тематичні та експертні дослідження криптосистем і засобів КЗІ.

II. Послуги у галузі ТЗІ:

– оцінювання захищеності інформації, що не становить державної таємниці;

– оцінювання захищеності інформації усіх видів, у тому числі інформації, що становить державну таємницю.

– виявлення закладних пристроїв.

7. <u>Кодекс України про адміністративні правопорушення</u> (Відомості Верховної Ради Української РСР (ВВР) 1984, додаток до № 51, ст. 1122):

– ст. 188-39 – порушення законодавства у сфері захисту персональних даних;

– ст. 195-5 – незаконне зберігання спеціальних технічних засобів негласного отримання інформації;

– ст. 212-2 – порушення законодавства про державну таємницю;

– ст. 212-5 – порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави;

– ст. 212-6 – здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем.

8. Кримінальний кодекс України (Відомості Верховної Ради України, 2001, № 25-26, ст. 131):

– ст. 114 – шпигунство;

– ст. 163 – порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер;

– ст. 231 – незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю;

– ст. 232 – розголошення комерційної або банківської таємниці;

– ст. 328 – розголошення державної таємниці;

– ст. 329 – втрата документів, що містять державну таємницю;

– ст. 330 – передача або збирання відомостей, що становлять конфіденційну інформацію, яка знаходиться у володінні держави;

– ст. 359 – незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації;

– ст. 361 – несанкціоноване втручання в роботу електронно- обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

Рис. 1.23 Класифікація технічних каналів витоку акустичної інформації

У **вібраційних (структурних) технічних каналах** витоку інформації середовищем поширення акустичних сигналів є конструкції будівель, споруд

пазоні частот від 20-30 Гц до 20-22 кГц.

Приклад можливих каналів витоку акустичної інформації з об'єкту інформаційної діяльності показаний на рис. 1.22.

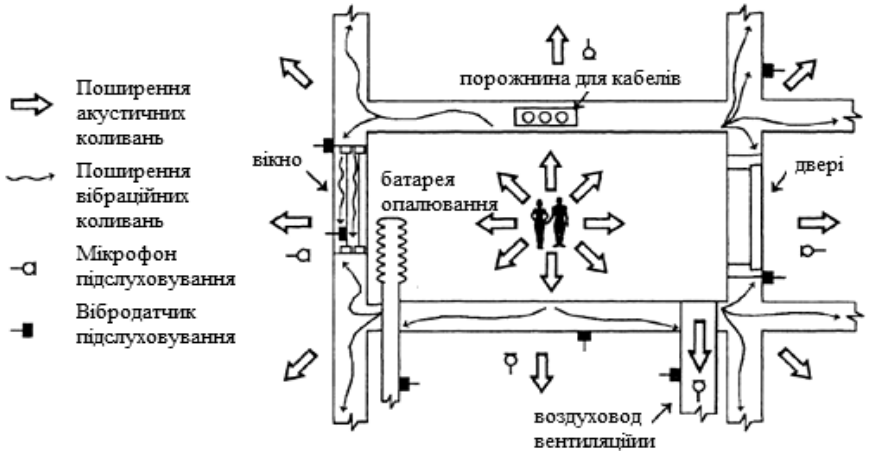

Рис. 1.22 Канали витоку акустичної інформації з ОІД

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплення технічні канали витоку акустичної (мовний) інформації можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронний і параметричні (рис. 1.23).

У **повітряних технічних каналах** витоку інформації середовищем поширення акустичних сигналів є повітря і для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні спрямовані мікрофони. Мініатюрні мікрофони об'єднуються (або з'єднуються) з портативними звукозаписними пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Автономні пристрої, що конструкційно об'єднують мініатюрні мікрофони і передавачі, називають *акустичними закладками*.

– ст. 361-1 – створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут;

– ст. 361-2 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації;

– ст. 361-3 – несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об’єктів національної інформаційної інфраструктури;

– ст. 361-4 – несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що оброблюється в державних електронних інформаційних ресурсах;

– ст. 362 – несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;

– ст. 362-1 – несанкціоновані дії з інформацією, що оброблюється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах критичних об’єктів національної інформаційної інфраструктури, вчинені особою, яка має право доступу до такої інформації;

– ст. 363 – порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється;

– ст. 363-1 – перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку;

– ст. 376-1 – незаконне втручання в роботу автоматизованої системи документообігу суду;

– ст. 422 – розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості.

9. Указ Президента України «Про Положення про технічний захист інформації в Україні» (від 27 вересня 1999 р. № 1229/99). Положення визначає правові та організаційні засади технічного захисту важливої для держави, суспільства і особи інформації, охорона якої забезпечується державою відповідно до законодавства.

Технічний захист інформації здійснюється щодо органів державної влади, органів місцевого самоврядування, органів управління Збройних Сил України та інших військових формувань, утворених згідно із законодавством України, відповідних підприємств, установ, організацій.

Правову основу ТЗІ в Україні становлять:

– Конституція України;

– закони України;

– акти Президента України та КМ України;

– нормативно-правові акти СБ України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України, інших державних органів;

– міжнародні договори України, згода на обов'язковість яких надана ВР України, з питань ТЗІ;

– це Положення.

Державна політика ТЗІ формується згідно із законодавством і реалізується *Державною службою спеціального зв'язку та захисту інформації України* у взаємодії з органами, щодо яких здійснюється ТЗІ.

Організація ТЗІ в органах покладається на їх керівників. Нормативно-правові акти з ТЗІ є обов'язковими для виконання всіма суб'єктами системи ТЗІ.

тепловизори, а також портативні закамуфльовані телевізійні камери високої чутливості, комплексовані з пристроями передачі інформації по радіоканалу.

Характеристика технічних каналів витоку акустичної інформації

Під **акустичною** розуміється інформація, носієм якої є *акустичні сигнали*. У тому випадку, якщо джерелом інформації є людська мова, акустична інформація називається *мовною*.

Акустичний сигнал є обуреннями пружного середовища, що проявляються у виникненні акустичних коливань різної форми і тривалості (рис. 1.21).

Рис. 1.21 Причини створення акустичних каналів витоку інформації

Акустичними називаються механічні коливання часток пружного середовища, що поширюються від джерела коливань в навколишній простір у вигляді хвиль різної довжини.

Первинними джерелами акустичних коливань є механічні коливальні системи, наприклад, органи мови людини, а вторинними – перетворювачі різного типу, у тому числі електроакустичні. Останні є пристроями, призначеними для перетворення акустичних коливань в електричні. До них відносяться пьезоелементи, мікрофони, телефони, гучномовці та інші пристрої.

Залежно від форми акустичних коливань розрізняють прості (тональні) і складні сигнали. *Тональний* – це сигнал, що викликається коливанням, що здійснюється за синусоїдальним законом. *Складний сигнал* включає цілий спектр гармонійних складових. Мовний сигнал є складним акустичним сигналом в діа-

Рис. 1.20. Класифікація способів прихованого видионаблюдения і зйомки

Зйомка об'єктів проводиться для документування результатів спостереження і детальнішого вивчення об'єктів. Для зйомки об'єктів використовуються телевізійні і фотографічні засоби. Причому фотоапарати

Зйомка об'єктів проводиться для документування результатів спостереження і детальнішого вивчення об'єктів з використанням телевізійних і фотографічних засобів. Причому фотоапарати використовуються у разі, коли необхідно отримати окремі зображення, наприклад, зовнішній вигляд об'єкту або фотознімок співробітника, а телевізійні – коли необхідно отримати зображення динамічного процесу, наприклад технологічного циклу, або дій окремих осіб.

Для зйомки об'єктів вдень з великої відстані використовуються фотоапарати і телевізійні камери з довгофокусними об'єктивами або комплексовані з телескопами. Для зйомки об'єктів вдень зблизька використовуються портативні фотоапарати або смартфони, телекамери, комплексовані з пристроями відеозапису і передачі відеозображень по радіоканалу. Зйомка об'єктів вночі проводиться, як правило, зблизька. Для цих цілей використовуються портативні фотоапарати і телевізійні камери, комплексовані з приладами нічного бачення, або

Рис. 1.11 Суб'єкти системи ТЗІ

Основні **завдання органів**, щодо яких здійснюється ТЗІ:

– забезпечення ТЗІ згідно з вимогами нормативно-правових актів з питань ТЗІ;

– видання у межах своїх повноважень нормативно-правових актів із зазначених питань;

– здійснення контролю за станом ТЗІ.

Органи, щодо яких здійснюється ТЗІ, відповідно до покладених на них завдань:

– створюють або визначають підрозділи, на які покладається забезпечення ТЗІ та контроль за його станом, узгоджують основні завдання та функції цих підрозділів;

– видають за погодженням з Адміністрацією Держспецзв'язку України та впроваджують нормативно-правові акти з питань ТЗІ;

– погоджують з Адміністрацією Держспецзв'язку України проведення підприємствами, установами, організаціями тих науково-дослідних, дослідно-конструкторських і дослідно-технологічних робіт, спрямованих на розвиток

нормативно-правової та матеріально-технічної бази системи ТЗІ, які здійснюються за рахунок коштів державного бюджету;

– створюють або визначають за погодженням з Адміністрацією Держспецзв'язку України підприємства, установи та організації, що забезпечують ТЗІ;

– забезпечують підготовку, перепідготовку та підвищення кваліфікації кадрів з ТЗІ;

– надають Адміністрації Держспецзв'язку України за його запитами відомості про стан ТЗІ.

Основні **завдання інших суб'єктів** системи ТЗІ:

– дослідження загроз для інформації на об'єктах, функціонування яких пов'язано з інформацією, що підлягає охороні;

– створення та виробництво засобів забезпечення ТЗІ;

– розроблення, впровадження, супроводження комплексів ТЗІ;

– підвищення кваліфікації фахівців з ТЗІ.

10. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» (від 22 травня 1998 р. № 505/98). Положення визначає порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі.

Державну політику у сфері криптографічного захисту інформації відповідно до закону реалізує *Державна служба спеціального зв'язку та захисту інформації України*.

Ліцензування діяльності, пов'язаної з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації, здійснюється згідно із законодавством України.

Державні органи, підприємства, установи і організації придбавають, вивозять з України, використовують криптосистеми і засоби криптографічного захисту інформації *за погодженням з Адміністрацією Держспецзв'язку України*.

Рис. 1.19 Класифікація техничних каналів витоку інформації

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

Технічні засоби розвідки служать для прийому і виміру параметрів сигналів. Вони використовуються для перехоплення інформації, що обробляється в технічних засобах, акустичної (мовної) інформації, а також як засоби прихованого виденаблюдения і зйомки.

Характеристика способів прихованого відеоспостереження і зйомки

Важливим джерелом конфіденційних відомостей є **видова інформація**, що отримується технічними засобами розвідки порушника у вигляді *зображень об'єктів* або *документів*. Залежно від характеру інформації й її призначення виділяють наступні способи її отримання (рис. 1.20): спостереження за об'єктом, зйомка об'єкту, зйомка (зняття копій) документів.

Спостереження за об'єктом організовується протягом певного (у ряді випадків тривалого) часу. Залежно від умов спостереження і освітлення для спостереження об'єктом можуть використовуватися різні технічні засоби: *для спостереження вдень* – оптичні прилади (монокуляри, підзорні труби, біноклі, телескопи і т.д.), телевізійні системи; *для спостереження вночі* – прилади нічного бачення, телевізійні системи, тепловизоры; *для спостереження з великої відстані* використовуються засоби з довгофокусними оптичними системами, а при спостереженні зблизька – встановлені телевізійні камери, що камуфлюють потайно. Причому відеозображення з телевізійних камер може передаватися на монітори як по кабелю, так і по радіоканалу.

5. Методи, засоби та заходи захисту інформації в ІТС від витоку та руйнування технічними каналами

Захист інформації від витоку технічними каналами – це комплекс організаційно-технічних заходів, що виключають або ослабляють безконтрольний вихід конфіденційної інформації за межі контрольованої зони.

Слід пам'ятати, що:

- безпечних технічних засобів немає;
- джерелами утворення технічних каналів витоку інформації є фізичні перетворювачі;
- будь-який електронний елемент за певних умов може стати джерелом утворення каналу витоку інформації;
- будь-який канал витоку інформації може бути виявлений і локалізований;
- канал витоку інформації легше локалізувати, ніж виявити.

5.1 Технічні канали витоку та руйнування інформації

Витік – це безконтрольний вихід конфіденційної інформації за межі організації або кола осіб, яким вона довірена. Утворюється за рахунок неконтрольованих фізичних полів (акустичних, світлових, електро-магнітних, радіаційних, теплових та ін.)

Технічний канал витоку інформації – фізичний шлях від джерела інформації до порушника, за допомогою якого може бути здійснений НСД до відомостей, що охороняються (див. рис. 1.5). Технічні канали витоку підрозділяються на візуально-оптичні, акустичні, електро-магнітні, матеріально-речові та ін. (рис. 1.19).

Сигнали є *матеріальними носіями інформації*. По своїй фізичній природі сигнали можуть бути електричними, електромагнітними, акустичними і т.д., тобто сигналами, як правило, являються електромагнітні, механічні та інші види коливань (хвиль), причому інформація міститься в їх параметрах, що змінюються.

З метою визначення рівня захищеності від несанкціонованого доступу до інформації з обмеженим доступом проводяться *сертифікаційні випробування* криптосистем і засобів криптографічного захисту.

Для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації.

Зазначені криптосистеми і засоби перебувають у державній власності.

Засоби криптографічного захисту службової інформації та криптосистеми з відповідного дозволу можуть перебувати і в недержавній власності.

Для криптографічного захисту конфіденційної інформації використовуються криптосистеми і засоби криптографічного захисту, які мають *сертифікат відповідності*.

До користування криптосистемами та засобами криптографічного захисту секретної інформації допускаються особи, які у встановленому законодавством України порядку одержали допуск до державної таємниці.

11. <u>Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні»</u> (від 8 жовтня 1997 р. № 1126). Концепція визначає основи державної політики у сфері захисту інформації інженерно-технічними заходами. Технічний захист інформації (ТЗІ) є складовою частиною забезпечення національної безпеки України.

ТЗІ – *це діяльність, спрямована на забезпечення інженерно-технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації з обмеженим доступом, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.*

Загрози безпеці інформації:

1) Перевага технічним засобам оброблення інформації та засобам зв'язку іноземного виробництва, які здебільшого не забезпечують захист інформації.

2) Використання комунікаційного обладнання іноземного виробництва у мережах зв'язку передбачає дистанційний доступ до його апаратних та програ-

мних засобів, що створює умови для несанкціонованого впливу на їх функціонування і контролю за організацією зв'язку та змістом повідомлень, які пересилаються.

3) Створення компактних технічних засобів розвідки, за допомогою яких можна легко підключатись до ліній телекомунікацій та різноманітних технічних засобів оброблення інформації з метою здобування, пересилання та аналізу розвідувальних даних.

4) Створилися можливості витоку інформації, порушення її цілісності та блокування. Витік інформації, яка становить державну та іншу передбачену законом таємницю, службової інформації, – це одна з основних можливих загроз національній безпеці України в інформаційній сфері.

Причини загроз безпеці інформації в Україні:

– не виваженість державної політики в галузі ІТ;

– діяльність інших держав, спрямована на одержання переваги;

– діяльність політичних партій, суб'єктів підприємницької діяльності, окремих фізичних осіб;

– злочинна діяльність, спрямована на протизаконне одержання інформації з метою досягнення матеріальної вигоди;

– використання ІТ низького рівня;

– недостатність документації на засоби забезпечення ТЗІ іноземного виробництва, низька кваліфікація технічного персоналу у сфері ТЗІ.

Стан ТЗІ зумовлюється:

– недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць, конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;

– недостатністю нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення ТЗІ;

– незавершеністю створення системи сертифікації засобів забезпечення ТЗІ;

9. Який порядок створення КСЗІ?
10. У чому полягають принципи управління доступом?
11. У чому сенс концепції матриці доступу?
12. Що є функціями і механізмами захисту?

Висновки

1. Несанкціонований доступ (НСД) - це доступ до інформації з використанням засобів, включених до складу АС, що порушує встановлені ПРД. НСД може здійснюватися з використанням штатних засобів (сукупності програмно-апаратного забезпечення, що входять у затверджену конфігурацію АС, а також з використанням програмно-апаратних засобів, включених до складу АС зловмисником.

2. Основні канали НСД, через які порушник може отримати доступ до компонент ІТС і здійснити розкрадання, модифікацію і/або руйнування інформації: штатні канали доступу до інформації (термінали, засоби відображення інформації; канали зв'язку), технологічні пульти управління, побічні електромагнітні випромінювання від апаратури, ліній зв'язку, мереж електроживлення і заземлення та ін., лінії зв'язку між апаратними засобами ІТС.

3. Захист від несанкціонованого доступу – це діяльність, спрямована на забезпечення додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стані системи заходів із захисту інформації. Основні принципи забезпечення захисту інформації: планування захисту і керування системою захисту, керування доступом, послуги безпеки і гарантії.

Контрольні питання

1. Як класифікуються загрози за результатами їх впливу на інформацію?
2. Що таке НСД і які існують способи його реалізації?
3. Поясніть узагальнену модель способів НСД до джерел конфіденційної інформації.
4. Які існують поширені прийоми НСД?
5. Які існують основні категорії мережевих атак?
6. У чому сенс моделі порушника?
7. Що таке захист від НСД?
8. Які основні принципи забезпечення захисту інформації від НСД?

– недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

– недостатньою узгодженістю чинних в Україні нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України.

Правова основа забезпечення ТЗІ в Україні:

– Конституція України;

– Закони України «Про основи національної безпеки України», «Про інформацію», «Про доступ до публічної інформації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про державну таємницю», «Про науково-технічну інформацію»;

– інші нормативно-правові акти;

– міжнародні договори України, що стосуються сфери інформаційних відносин.

Основні функції організаційних структур системи ТЗІ:

– оцінка стану ТЗІ в державі, визначення пріоритетних напрямів його розвитку;

– розвиток правових засад удосконалення системи ТЗІ;

– виявлення та прогнозування загроз безпеці інформації;

– забезпечення інженерно-технічними заходами захисту інформації, що підлягає технічному захисту;

– створення умов для ТЗІ, що здійснюється суб'єктами інформаційних відносин на власний розсуд;

– формування та забезпечення реалізації державної політики щодо створення та впровадження вітчизняних засобів забезпечення ТЗІ;

– створення національної системи стандартизації та нормування у сфері ТЗІ;

– організація фундаментальних і прикладних науково-дослідних робіт та розробок у сфері ТЗІ;

– забезпечення взаємодії організаційних структур системи ТЗІ з іншими системами захисту інформації, системами забезпечення інформаційної та національної безпеки;

– організація створення та виконання програм розвитку ТЗІ;

– забезпечення ліцензування підприємницької діяльності в сфері ТЗІ;

– організація контролю за якістю засобів забезпечення ТЗІ шляхом їх сертифікації;

– організація контролю за відповідністю вимогам ТЗІ об'єктів, діяльність яких пов'язана з інформацією, що підлягає технічному захисту, шляхом їх атестації;

– організація контролю за ефективністю ТЗІ на об'єктах, діяльність яких пов'язана з інформацією, що підлягає технічному захисту;

– забезпечення підготовки фахівців для роботи у сфері ТЗІ;

– сприяння залученню інвестицій і вітчизняного товаровиробника у сферу ТЗІ;

– організація міжнародного співробітництва в сфері ТЗІ, представлення інтересів України у відповідних міжнародних організаціях;

– забезпечення (кадрове, фінансове, нормативне, матеріально-технічне, інформаційне тощо) життєдіяльності складових організаційних структур системи ТЗІ.

Державна політика у сфері ТЗІ визначається *пріоритетністю національних інтересів*, має на меті унеможливлення реалізації загроз для інформації та здійснюється шляхом виконання положень Концепції, а також програм розвитку ТЗІ.

Основні напрями державної політики у сфері ТЗІ:

1) Нормативно-правове забезпечення.

2) Удосконалення чинних та розроблення нових нормативних документів з питань ТЗІ.

3) Організаційне забезпечення.

- не повинно існувати можливості одержати доступ до об'єктів ІТС в обхід КЗЗ;
- КЗЗ, що реалізує політику безпеки, має бути безперервно захищений від злому і несанкціонованої модифікації;

- КЗЗ повинен *мати модульну структуру*:
  - КЗЗ має бути реалізований як набір відносно незалежних частин;
  - кожна з частин повинна взаємодіяти з іншими тільки через добре визначені інтерфейси;
  - КЗЗ має бути спроектовано як набір груп функцій (шарів), що взаємодіють тільки з сусідніми нижнім і верхнім шарами.

3. **Концепція диспетчера доступу**. При реалізації КЗЗ використовується концепція диспетчера доступу. Атрибути диспетчера доступу повинні забезпечити безперервний і повний захист від НСД, мати невеликі розміри і бути захищеними від модифікації.

Головна мета диспетчера доступу – забезпечення відомої точки проходження всіх запитів всередині ІТС і досягнення гарантії того, що потоки інформації між об'єктами-користувачами, об'єктами-процесами і пасивними об'єктами відповідають вимогам політики безпеки.

Диспетчер доступу має бути завжди активним і повинен контролювати всі запити на доступ до будь-якого захищеного об'єкта, який піддається впливу. Він служить бар'єром між інформацією, до якої хоче одержати доступ користувачів, і самим користувачем. Диспетчер доступу дозволяє або забороняє доступ відповідно до того, чи є запит *авторизованим*. Рішення приймається на підставі перевірки атрибутів доступу користувача, процесу і пасивного об'єкта.

Узагальненням концепції диспетчера доступу є ідея *герметизації*, коли кожний об'єкт як би герметизовано диспетчером доступу, що утворює навкруги нього непроникну оболонку.

Найбільш широке розповсюдження одержала реалізація класичного погляду на диспетчер доступу, яка називається «**ядром захисту**».

В *процесі розробки* гарантії забезпечуються діями розробника щодо забезпечення правильності (коректності) розробки.

В *процесі оцінки* гарантії забезпечуються шляхом перевірки додержання розробником вимог критеріїв, аналізу документації, процедур розробки і постачання, а також іншими діями експертів, які проводять оцінку.

Основні **принципи реалізації програмно-технічних засобів захисту інформації** в ІТС від НСД:

1. *Функції і механізми захисту*. Завдання засобів захисту:

- ізоляція об'єктів КС всередині сфери керування;
- перевірка всіх запитів доступу до об'єктів;
- реєстрація запитів і результатів їх перевірки і/або виконання.

Елементарна функція будь-якої з послуг, що реалізуються засобами захисту, може бути віднесена:

- до функцій *ізоляції*, *перевірки* або *реєстрації*;
- до функцій забезпечення *конфіденційності*, *цілісності* і *доступності* інформації або *керованості* ІТС і *спостереженості* дій користувачів.

Кожна функція може бути реалізована одним або більше внутрішніми механізмами, що залежать від конкретної ІТС. Водночас одні й ті ж самі механізми можуть використовуватись для реалізації кількох послуг.

Для реалізації функцій захисту можуть використовуватись:

- програмні засоби;
- апаратні засоби;
- криптографічні перетворення;
- різні методи перевірки повноважень і т.д.

Вибір методів і механізмів практично завжди залишається за розробником.

Функції захисту мають бути реалізовані відповідно до декларованої політики безпеки і вимог гарантій.

2. *Реалізація комплексу засобів захисту*. До реалізації КЗЗ пред'являється ряд **вимог**:

- КЗЗ повинен *забезпечувати безперервний захист* об'єктів ІТС:

4) Науково-технічна та виробнича діяльність.

12. <u>ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації</u>. Стандарт установлює об’єкт, мету, основні організаційно-технічні положення забезпечення ТЗІ, неправомірний доступ до якої може завдати шкоди громадянам, організаціям та державі, а також категорії нормативних документів системи ТЗІ.

Технічний захист інформації здійснюється **поетапно**:

1) визначення й аналіз загроз;
2) розроблення системи захисту інформації;
3) реалізація плану захисту інформації;
4) контроль функціонування та керування СЗІ.

Нормативні документи системи ТЗІ:

1) нормативні документи із стандартизації у галузі ТЗІ;
2) державні стандарти та прирівняні до них нормативні документи;
3) нормативні акти міжвідомчого значення, що реєструються у Міністерстві юстиції України;
4) нормативні документи міжвідомчого значення технічного характеру, що реєструються уповноваженим Кабінетом Міністрів органом;
5) нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

13. <u>ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт</u>. Стандарт установлює вимоги до порядку проведення робіт з ТЗІ. Зміст та послідовність робіт з протидії загрозам або їхньої нейтралізації полягає в:

– проведення обстеження підприємства, установи, організації;
– розроблення і реалізації організаційних, первинних технічних, основних технічних заходів з використанням засобів забезпечення ТЗІ;
– приймання робіт з ТЗІ;
– атестації засобів (систем) забезпечення ІД на відповідність вимогам нормативних документів з ТЗІ.

14. <u>ДБН А.2.2-2-96. Проектування. Технічний захист інформації. Загальні вимоги до організації проектування і проектної документації для будівництва</u>. Норми встановлюють вимоги до забезпечення технічного захисту інформації під час організації проектування будівництва (нового будівництва, розширення, реконструкції та капітального ремонту) підприємств, будівель та споруд.

15. <u>Нормативні документи з технічного захисту інформації</u>:

– ТР ЕОТ-95 Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок;

– ТР ТЗІ – ПЕМВН-95 Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок;

– НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 1.1-005-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу ТЗІ. Основні положення;

– НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі;

– НД ТЗІ 1.6-005-2013 Захист інформації на об’єктах інформаційної діяльності. Положення про категорювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці;

– НД ТЗІ 2.1-002-2007 Захист інформації на об’єктах інформаційної діяльності. Випробування комплексу ТЗІ. Основні положення;

– НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (зі зміною №1);

Система повинна надавати користувачам, що мають адміністративні повноваження, можливість проглядати та аналізувати дані реєстрації, що представляються у вигляді журналів реєстрації, виявляти небезпечні з точки зору політики безпеки події, встановлювати їх причини і користувачів, відповідальних за порушення політики безпеки.

Послуги безпеки. З точки зору забезпечення безпеки інформації ІТС або КЗЗ можна розглядати як *набір функціональних послуг*, кожна з яких є набіром функцій, що дозволяють протистояти деякій множині загроз.

Вимоги до функціональних послуг розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз конфіденційності, цілісності, доступності та спостереженості. Кожна послуга включає декілька рівнів. Чим вище рівень послуги, тим повніше забезпечується захист від певного виду загроз.

Для кожної послуги повинна бути розроблена політика безпеки, яка буде реалізована ІТС. **Політика безпеки** має визначати, до яких об'єктів застосовується послуга. Ця визначена підмножина об'єктів називається *захищеними об'єктами* відносно даної послуги.

Критерії гарантій дозволяють оцінити коректність реалізації послуг і включають вимоги до:

- архітектури КЗЗ;
- середовища розробки;
- послідовності розробки;
- випробування КЗЗ;
- середовища функціонування;
- експлуатаційної документації.

В критеріях вводиться сім рівнів гарантій, ієрархія яких відбиває поступово наростаючу міру упевненості в тому, що послуги, які надаються, дозволяють протистояти певним загрозам.

Гарантії забезпечуються як в процесі розробки, так і в процесі оцінки.

хисту дозволяють управляти потоками інформації між користувачами і об'єктами тільки спеціально авторизованим користувачам. Наприклад, механізм, коли у вигляді атрибутів доступу використовуються мітки, що відображають міру конфіденційності інформації (об'єкта) і рівень допуску користувача.

КЗЗ на підставі порівняння міток об'єкта і користувача може визначити, чи є користувач, що запитує інформацію, авторизованим користувачем.

Система, що реалізує адміністративне керування доступом, повинна гарантувати, що потоки інформації всередині системи установлюються адміністратором і не можуть бути змінені звичайним користувачем.

З іншого боку, система, що реалізує довірче керування доступом, дозволяє звичайному користувачеві модифікувати, в тому числі створювати нові потоки інформації всередині системи.

Створення додаткових потоків інформації може бути зумовлене:

- модифікацією атрибутів доступу користувача, процесу або пасивного об'єкта;
- створенням нових об'єктів (включаючи копіювання існуючих);
- експортом або імпортом об'єктів.

Забезпечення персональної відповідальності. Кожний співробітник з персоналу ІТС має бути ознайомлений з необхідними положеннями політики безпеки і нести персональну відповідальність за їх додержання.

Політика безпеки повинна установлювати обов'язки співробітників, особливо тих, що мають адміністративні повноваження, і види відповідальності за невиконання цих обов'язків. Як правило, це забезпечується в рамках організаційних заходів безпеки.

Коли користувач працює з ІТС, то система розглядає його не як фізичну особу, а як об'єкт, якому притаманні певні атрибути і поводження.

Комплекс засобів захисту ІТС повинен забезпечувати реєстрацію дій об'єктів-користувачів щодо використання ресурсів системи, а також інших дій і подій, які так або інакше можуть вплинути на дотримання реалізованої ІТС політики безпеки.

– НД ТЗІ 2.5-008-2002 Вимоги із захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу «2»;

– НД ТЗІ 3.1-001-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексів технічного захисту інформації. Перед проектні роботи;

– НД ТЗІ 3.3-001-2007 Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації;

– НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

– НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

– НД ТЗІ 3.7-003-2005 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Висновки

1. Правовий захист – спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі.

2. Вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, у тому числі і в конституційне законодавство, основні загальні закони, закони по організації державної системи управління, спеціальні закони, відомчі правові акти та інші.

3. Спираючись на державні правові акти і враховуючи відомчі інтереси на рівні конкретної організації, розробляються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки.

4. Правове регулювання потрібне для вдосконалення механізму попере-

дження протиправних дій по відношенню до інформаційних ресурсів, для уточнення і закріплення завдань і правомочності окремих суб'єктів у сфері попереджувальної діяльності, охорони прав і законних інтересів громадян і організацій.

5. Правові заходи забезпечення безпеки і захисту інформації є основою порядку діяльності і поведінки співробітників підприємства і визначають заходи їх відповідальності за порушення встановлених норм.

Контрольні питання

1. Поясніть систему нормативно-правових документів в Україні, що регламентують питання захисту інформації.
2. Яка структура законодавства України у сфері захисту інформації?
3. Що таке конфіденційна інформація? Які її основні види?
4. Що таке комерційна таємниця? Які її параметри?
5. Які правові вимоги забезпечення безпеки і захисту інформації вказуються в Статуті організації?
6. Як підрозділяється інформація за режимом доступу?
7. Хто є суб'єктами стосунків, пов'язаних із захистом інформації в ІТС?
8. Які загрози інформації визначені в Концепції технічного захисту інформації в Україні?

Концепція матриці доступу. Матриця доступу – таблиця, уздовж кожного виміру якої відкладені ідентифікатори об'єктів ІТС, а в якості елементів матриці виступають дозволені або заборонені режими доступу (рис. 1.18).

	O_1	O_2	…	O_j	…	O_m
S_1	R	R,W	…	E	…	R
S_2	R,A	-	…	R	…	E
…	…	…	…	…	…	…
S_i	R	-	…	-	…	R
…	…	…	…	…	…	…
S_n	R,W	-	…	E	…	E

Рис. 1.18 Матриця доступу

Тут S_i – суб'єкт доступу; O_j – об'єкт доступу; режими: R – читання, W – запису, E – виконання програми, A – дописування.

Матриця доступу може бути:

- двомірною (наприклад, користувачі/пасивні об'єкти або процеси/пасивні об'єкти);
- тримірною (користувачі/процеси/пасивні об'єкти);
- повною, тобто містити вздовж кожної з осей ідентифікатори усіх існуючих на даний час об'єктів ІТС даного типу;
- частковою.

Повна тримірна матриця доступу дозволяє точно описати:

- хто (ідентифікатор користувача);
- через що (ідентифікатор процесу);
- до чого (ідентифікатор пасивного об'єкту);
- який вид доступу може одержати.

Довірче і адміністративне керування доступом. *Довірче керування доступом* – керування, при якому засоби захисту дозволяють звичайним користувачам управляти потоками інформації між іншими користувачами і об'єктами свого домену (наприклад, на підставі права володіння об'єктами), тобто призначення і передача повноважень не вимагають адміністративного втручання.

Адміністративне керуванням доступом – керування, при якому засоби за-

- довірче і адміністративне керування доступом;
- наявність атрибутів доступу;
- забезпечення персональної відповідальності.

Безперервний захист. Захист інформації повинен забезпечуватись протягом всього періоду її існування – з моменту створення об'єкта ІТС або його імпорту до системи і до його знищення або експорту з системи всі запити на доступ до об'єкта і об'єкта на доступ до інших об'єктів мають контролюватися КЗЗ:

- необхідно, щоб абсолютно всі запити на доступ до об'єктів контролювались КЗЗ і не існувало можливості обминути цей контроль (для захисту об'єктів КЗЗ повинен, в першу чергу, забезпечувати свою цілісність і керованість);
- особливе значення набуває визначення діючих за умовчанням правил, які визначають початкові умови, за яких починається існування об'єкта всередині ІТС.

Атрибути доступу. КЗЗ повинен забезпечити ізоляцію об'єктів всередині сфери управління і гарантувати розмежування запитів доступу і керування потоками інформації між об'єктами. Для цього з об'єктами ІТС має бути пов'язана інформація (атрибути доступу), що дозволяла б КЗЗ ідентифікувати об'єкти і перевіряти легальність запитів доступу:

- кожний об'єкт ІТС (користувач, процес або пасивний об'єкт) повинен мати певний набір атрибутів доступу (унікальний ідентифікатор та іншу інформацію, що визначає його права доступу і/або права доступу до нього).
- відповідність атрибутів доступу і об'єкта може бути як явною, так і неявною.
- атрибути доступу об'єкта є частиною його представлення в ІТС.

Використовуючи набір атрибутів доступу відповідно до прийнятої політики безпеки, можна реалізувати:

- довірче керування доступом;
- адміністративне керування доступом;
- контроль за цілісністю та інші види керування доступом.

4. Методи, засоби та заходи захисту інформації в ІТС від НСД

4.1 Несанкціонований доступ до інформації і способи його здійснення

Несанкціонований доступ (НСД) – це доступ до інформації з використанням засобів, включених до складу ІТС, що порушує встановлені правила розмежування доступу (ПРД). НСД може здійснюватися:

– з використанням штатних засобів (сукупності програмно-апаратного забезпечення), що входять у затверджену конфігурацію ІТС;

– з використанням програмно-апаратних засобів, включених до складу ІТС порушником.

Способи здійснення НСД дуже різноманітні (рис. 1.12).

Рис. 1.12 Суб'єкти системи ТЗІ

1. **Ініціативна співпраця** проявляється в певних діях осіб, чимось незадоволених або гостро потребуючих коштів для існування, з числа працюючих в організації або просто пожадливих і жадібних, готових заради наживи на будь-які протиправні дії. Відомо досить прикладів ініціативної співпраці з політичних, моральних або фінансових міркувань. Фінансові затруднення, політичні

або наукові розбіжності, незадоволення просуванням по службі, образи від начальства і влади, незадоволення своїм статусом штовхають володарів конфіденційної інформації на співпрацю із злочинними угрупуваннями та іноземними розвідками.

Наявність такої людини у сфері виробництва і управління підприємства дозволяє порушникам отримувати необхідні відомості про діяльність фірми і дуже для них вигідно, оскільки інформатор економить час і витрати на впровадження свого агента, представляє свіжу і достовірну інформацію, яку звичайним шляхом було б складно отримати.

2. **Схилення до співпраці** – це, як правило, насильницька дія з боку зловмисників. Схилення або вербування може здійснюватися шляхом підкупу, залякування, шантажу. Схилення до співпраці реалізується у вигляді реальних загроз, переслідування та інших дій, що виражаються в переслідуванні, образі і т.д. Деякі конкуренти використовують рекет. По інтенсивності насильства це один з найбільш агресивних видів діяльності, де за зовні мирними візитами і переговорами криється готовність діяти навмисно жорстоко з метою залякування. Дуже близько до схилення лежить і переманювання фахівців фірми конкурента на свою фірму з метою подальшого володіння його знаннями.

3. **Вивідування, випитування** – це прагнення під виглядом наївних питань отримати певні відомості. Випитувати інформацію можна і помилковими працевлаштуваннями, і створенням помилкових фірм, іншими діями.

4. **Підслуховування** – спосіб ведення розвідки і промислового шпигунства, вживаний агентами, спостерігачами, інформаторами, спеціальними постами підслуховування. В інтересах підслуховування порушники використовують спеціальних людей, співробітників, сучасну техніку, різні прийоми її застосування. Підслуховування може здійснюватися безпосереднім сприйняттям акустичних коливань особою при прямому сприйнятті мовної інформації або за допомогою технічних засобів.

5. **Спостереження** – візуальний спосіб ведення розвідки про стан і діяльність супротивника за допомогою оптичних приладів. Як правило, ведеться ці-

Основні **принципи забезпечення захисту інформації від НСД**:

- планування захисту і керування системою захисту;
- керування системою доступу;
- забезпечення послуг безпеки і гарантій.

Планування захисту і керування системою захисту. Для забезпечення безпеки інформації під час її обробки в ІТС створюється КСЗІ, процес управління якою повинен підтримуватись протягом всього життєвого циклу ІТС.

На *стадії розробки* мета процесу управління КСЗІ є створення засобів захисту, які могли б ефективно протистояти ймовірним загрозам і забезпечували б надалі дотримання політики безпеки під час обробки інформації.

На *стадії експлуатації* ІТС мета процесу управління КСЗІ є оцінка ефективності створеної КСЗІ і вироблення додаткових (уточнюючих) вимог для доробки КСЗІ з метою забезпечення її адекватності при зміні початкових умов (характеристик ОС, оброблюваної інформації, фізичного середовища, персоналу, призначення ІТС, політики безпеки і т.д.).

При плануванні дій слід враховувати порядок створення КСЗІ:

- *аналіз об'єкта захисту і можливих загроз* – визначення ресурсів ІТС, що підлягають захисту, при цьому загрози визначаються в термінах ймовірності їх реалізації і величини можливих збитків;
- *оцінка ризиків* (на підставі аналізу загроз, існуючих в системі вразливостей, ефективності вже реалізованих заходів захисту);
- *вироблення заходів захисту*, перетворення яких в житті дозволило б знизити рівень остаточного ризику до прийнятного рівня;
- *формулювання або коригування політики безпеки*;
- *розробка плану захисту* (опис послідовності і змісту всіх стадій і етапів життєвого циклу КСЗІ).

Слід пам'ятати, що вартість заходів щодо захисту інформації має бути адекватною розміру можливих збитків.

Керування системою доступу. Основні принципи керування доступом:

- безперервний захист;

2) Спостерігатиметься поступове зміщення вектору мережевих атак у бік атак через широко затребувані файлообменні мережі.

3) Шкідливі програми стануть ще складнішими.

4) Звичайними стануть атаки на портативні пристрої.

5) Слід бути готовим до повторної хвилі поширення фальшивих антивірусних продуктів.

Модель порушника

Порушник – це особа, яка може одержати доступ до роботи з включеними до складу ІТС засобами (апаратними і програмними).

Порушники класифікуються за чотирма рівнями можливостей (табл. 1.4), що надаються їм штатними засобами ІТС. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього. Припускається, що в своєму рівні порушник – це фахівець вищої кваліфікації, який має повну інформацію про ІТС і КЗЗ.

Таблиця 1.4 Можливості порушників

Рівень	Можливості порушника
1	Запуск фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації
2	Створення і запуск власних програм з новими функціями обробки інформації
3	Управління функціонуванням ІТС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування
4	Увесь обсяг можливостей осіб, що здійснюють проектування, реалізацію і ремонт апаратних компонентів ІТС, аж до включення до складу ІТС власних засобів з новими функціями обробки інформації

4.2 Методи, засоби та заходи захисту інформації в ІТС від НСД

Захист від несанкціонованого доступу – це діяльність, спрямована на забезпечення додержання правил розмежування доступу шляхом створення і підтримки в дієздатному стану системи заходів із захисту інформації.

леспрямовано, в певний час і в потрібному місці спеціально підготовленими людьми,. ведеться потайно. До технічних засобів спостереження відносяться оптичні прилади (біноклі, труби, перископи), телевізійні системи (для звичайної освітленості і низькорівневої), прилади спостереження вночі і при обмеженій видимості.

6. **Розкрадання** – умисне протиправне заволодіння чужим майном, засобами, документами, матеріалами, інформацією. Викрадають усе, що погано лежить, включаючи документи, продукцію, дискети, ключі, коди, паролі та шифри.

7. **Копіювання** – це створення дублікатів. Копіюють документи, які містять відомості, що цікавлять порушника; інформацію, що обробляється в ІТС; продукцію.

8. **Підробка** – це модифікація, фальсифікація довірчих документів, що дозволяють отримати певну інформацію, листів, рахунків, бухгалтерських і фінансових документів, ключів, пропусків, паролів і т.д.

9. **Знищення** – у частині інформації особливу небезпеку представляє її знищення в ІТС, в якій накопичуються на технічних носіях величезні об'єми відомостей різного характеру, причому багато з них дуже важко виготовити у вигляді немашинних аналогів. Знищуються і люди, і документи, і засоби обробки інформації, і продукція.

10. **Незаконне підключення** – це контактне або безконтактне підключення до різних ліній і дротів з метою несанкціонованого доступу до інформації. Підключення можливо як до дротяних ліній телефонного і телеграфного зв'язку, так і до ліній зв'язку іншого інформаційного призначення: лініям передачі даних, сполучним лініям периферійних облаштувань великих і малих ЕОМ, лініям диспетчерського зв'язку, конференц-зв'язку, живлення, заземлення тощо.

11. **Перехоплення** – це отримання розвідувальної інформації за рахунок прийому сигналів електромагнітної енергії пасивними засобами прийому, розташованими, як правило, на достатній відстані від джерела конфіденційної інформації. До перехоплення переговорів схильні будь-які системи радіозв'язку,

переговори, що ведуться з рухливих засобів телефонного зв'язку (радіотелефон), переговори усередині приміщення за допомогою безпровідних систем установського зв'язку та інші.

12. **Негласне ознайомлення** – спосіб отримання інформації, до якої порушник не допущений, але за певних умов він може отримати можливість дещо упізнати (відкритий документ на столі під час бесіди з відвідувачем, спостереження екрану ПК зі значної відстані у момент роботи із закритою інформацією і т.д.). До негласного ознайомлення відноситься і люстрації поштових відправлень, установського і особистого листування.

13. **Фотографування** – спосіб отримання видимого зображення об'єктів кримінальних інтересів на фотоматеріалі. Особливість способу – документальність, що дозволяє при дешифруванні фотознімків по елементах і демаскуючих ознаках отримати дуже цінні, детальні відомості про об'єкт спостереження.

14. **Збір і аналітична обробка** – це завершаючий етап вивчення і узагальнення здобутої інформації з метою отримання достовірних і охоплюючих відомостей по аспекту діяльності об'єкту його інтересів, що цікавить порушника. Повний об'єм відомостей про діяльність конкурента не може бути отриманий яким-небудь одним способом. Чим більші інформаційні можливості має порушник, тим більше успіхів він може добитися. На успіх може розраховувати той, хто швидше і повніше збере необхідну інформацію, переробить її і прийме правильне рішення.

Загрози НСД до оброблюваної в ІТС інформації залежать від:

– характеристик апаратно-програмних компонентів ІТС;
– фізичного середовища функціонування ІТС;
– персоналу (користувачів і обслуговуючого ІТС персоналу);
– інформації, що оброблюється, і технологій її обробки.

Узагальнена модель способів несанкціонованого доступу до джерел конфіденційної інформації наведена в табл. 1.2.

Атаки типу «людина-в-середині» виконуються на безпровідних мережах набагато простіше, ніж на дротяних, оскільки до дротяної мережі вимагається реалізувати певний вид доступу. Вони використовуються для порушення конфіденційності та цілісності сеансу зв'язку. Порушник зазвичай підміняє ідентифікацію одного з мережевих ресурсів і використовує можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту, необхідного для задоволення деяких своїх цілей, наприклад для спуфінга IP-адресів, зміни MAC-адреси для імітування іншого хоста і т.д.

Анонімний доступ в Інтернет. Незахищені безпровідні ЛОМ забезпечують хакерам найкращий анонімний доступ для атак через Інтернет. Хакери можуть використовувати незахищену безпровідну ЛОМ організації для виходу через неї в Інтернет, де вони здійснюватимуть протиправні дії, не залишаючи при цьому своїх слідів. Організація з незахищеною ЛОМ формально стає джерелом атакуючого трафіку, націленого на іншу комп'ютерну систему, що пов'язано з потенційним ризиком правової відповідальності за заподіяний збиток жертві атаки хакерів.

Тенденції розвитку ІТ-загроз:

- загрози інсайдерів;
- загрози від шкідливих програм;
- неавторизований доступ з боку зовнішніх порушників;
- DoS- і DDoS-атаки;
- електронне шахрайство;
- фішинг та фарминг атаки;
- спам;
- загроза фізичної втрати носія інформації;
- електронний вандалізм і саботаж.

Сценарії розвитку ІТ-загроз на найближчий час:

1) Таргетовані (цільові) атаки на об'єкти критичної інфраструктури і критичної інформаційної інфраструктури.

Виявлення WLAN. Для виявлення безпровідних мереж WLAN використовується, наприклад, утиліта *NetStumber* спільно з супутниковим навігатором глобальної системи позиціонування GPS. Ця утиліта ідентифікує SSID мережі WLAN, а також визначає, чи використовується в ній система шифрування WEP. Застосування зовнішньої антени на портативному комп'ютері робить можливим виявлення мереж WLAN під час обходу потрібного району або поїздки по місту. Надійним методом виявлення WLAN є обстеження офісної будівлі з переносним комп'ютером в руках.

Підслуховування ведуть для збору інформації про мережу, яку передбачається атакувати згодом. Перехоплювач може використовувати здобуті дані для того, щоб отримати доступ до мережевих ресурсів. Устаткування, використовуване для підслуховування в мережі, може бути не складніше того, яке застосовується для звичайного доступу до цієї мережі. Безпровідні мережі за своєю природою дозволяють сполучати з фізичною мережею комп'ютери, що знаходяться на деякій відстані від неї, начебто ці комп'ютери знаходилися безпосередньо в мережі. Це дозволяє підключитися до безпровідної мережі, розташованої у будівлі, людини, що сидить в машині на стоянці поряд з ним. Атаку за допомогою пасивного прослуховування практично неможливо виявити.

Фальшиві точки доступу вмережу. Досвідчений атакуючий може організувати фальшиву точку доступу з імітацією мережевих ресурсів. Абоненти, нічого не підозрюючи, звертаються до цієї точки доступу і повідомляють їй свої важливі реквізити, наприклад, автентифікаційну інформацію. Цей тип атак іноді застосовують у поєднанні з прямим глушенням, щоб заглушити істинну точку доступу в мережу.

Відмова в обслуговуванні. Повну паралізацію мережі може викликати атака типу «відмова в обслуговуванні» (*DoS*). Безпровідні системи особливо сприйнятливі до таких атак. Фізичний рівень у безпровідній мережі – абстрактний простір навколо точки доступу. Зловмисник може включити пристрій, що заповнює увесь спектр на робочій частоті перешкодами і нелегальним трафіком, таке завдання не викликає особливих труднощів.

Таблиця 1.2 Модель способів НСД до джерел інформації

Джерела	Способи														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	Σ
Люди	⊗	⊗	⊗	⊗	⊗	⊗		⊗	⊗			⊗	⊗		10
Документи					⊗	⊗	⊗	⊗	⊗		⊗	⊗	⊗	⊗	9
Публікації								⊗				⊗		⊗	3
Технічні носії						⊗	⊗	⊗	⊗					⊗	5
Технічні засоби ПД				⊗					⊗	⊗	⊗				4
Технічні засоби ІТС				⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗		10
Продукція					⊗	⊗	⊗	⊗	⊗			⊗	⊗		7
Відходи						⊗								⊗	2
РАЗОМ	1	1	1	3	4	6	4	6	6	2	3	5	4	4	50

Аналіз моделі показує, що з точки зору уразливості від атак НСД найважливішими джерелами є люди, технічні засоби ІТС і документація, а найбільш універсальними способами НСД є розкрадання, копіювання і підробка.

Звідси витікає, що основними напрямами заходів щодо НСД до джерел ІзОД за допомогою технічних засобів є захист від:

– спостереження і фотографування;
– підслуховування;
– незаконного підключення;
– перехоплення;
– подолання системи розмежування доступу (СРД);
– несанкціонованого дослідження і копіювання.

Основні **задачі НСД**:

– безпосереднє звертання до об'єктів з метою одержання певного виду доступу;

– створення програмно-апаратних засобів, що виконують звертання до об'єктів в обхід засобів захисту;

– модифікація засобів захисту, що дозволяє здійснити НСД;

– впровадження в ІТС програмних або апаратних механізмів, що порушують структуру і функції ІТС і дозволяють здійснити НСД.

Класифікація загроз безпеки ІТС (можливостей впливу на ІТС, які прямо або непрямо завдають збитку її безпеки):

1. За *аспектом інформаційної безпеки*, проти якої вони спрямовані:

– **загрози доступності** (відмова в обслуговуванні) – спрямовані на створення таких ситуацій, коли певні дії або блокують доступ до деяких ресурсів ІТС, або знижують її працездатність;

– **загрози цілісності інформації**, яка зберігається в комп'ютерній системі або передається каналом зв'язку – спрямовані на зміну інформації або її спотворення, що призводить до порушення її якості або повного знищення;

– **загрози конфіденційності** – спрямовані на розголошування конфіденційної або секретної інформації. Інформація стає відомою особам, які не повинні мати до неї доступу. Загроза порушення конфіденційності має місце всякий раз, коли отриманий НСД до деякої закритої інформації, що зберігається в ІТС або передаваний від однієї системи до іншої;

– **загрози спостереженості та керованості ІТС** – спрямовані на порушення властивостей ІТС, які дозволяють фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

2. За *природою виникнення*:

– **природні загрози**, викликані діями на ІТС об'єктивних фізичних процесів або стихійних природних явищ;

– **штучні загрози** безпеки ІТС, викликані діяльністю людини.

3. За *ступенем навмисності прояву*:

– **загрози, викликані помилками або халатністю персоналу**, наприклад некомпетентне використання засобів захисту, введення помилкових даних і т.п.;

– **загрози умисної дії**, наприклад дії зловмисників.

Fi, в межах якої усі абоненти, забезпечені безпровідними адаптерами, дістають доступ до мережі.

У точки доступу є **ідентифікатор набору сервісів SSID** (Service Set IDentifier) – 32-бітовий рядок, використовуваний в якості імені безпровідної мережі, з якою асоціюються усі вузли. Ідентифікатор SSID потрібний для підключення робочої станції до мережі.

Головна відмінність між дротяними і безпровідними мережами пов'язана з наявністю неконтрольованої області між кінцевими точками безпровідної мережі. Це дозволяє тим, що атакують, знаходяться у безпосередній близькості від безпровідних структур, проводити цілий ряд нападів, які неможливі у дротяному світі.

Основні уразливості і загрози безпровідних мереж приведені на рис. 1.17.

Мовлення радіомаяка. Точка доступу включає з певною частотою широкомовний «радіомаяк», щоб оповіщати навколишні безпровідні вузли про свою присутність. Ці широкомовні сигнали містять основну інформацію про точку безпровідного доступу (включаючи SSID) і запрошують зареєструватися безпровідні вузли в цій області. Будь-яка робоча станція, що знаходиться в режимі очікування, може отримати SSID і додати себе у відповідну мережу.

Мовлення радіомаяка є природженою патологією безпровідних мереж. Багато моделей дозволяють відключати SSID частину цього мовлення, що містить, щоб дещо утруднити безпровідне підслуховування, але SSID проте посилається при підключенні, тому все одно існує невелике вікно уразливості.

Рис. 1.17 Уразливості і загрози безпровідних мереж

безпечують конфіденційність і цілісність передаваних повідомлень;

- автентифікація відправника здійснюється за його IP-адресом (процедура автентифікації виконується тільки на стадії встановлення з'єднання, а надалі достовірність пакетів, що приймаються, не перевіряється);
- відсутність можливості контролю за маршрутом проходження повідомлень в мережі Інтернет, що робить видалені мережеві атаки практично безкарними.

Загрози при безпровідному доступі до локальної мережі

Безпровідні локальні мережі WLAN (*Wireless Local Area Network*) включають (рис. 1.16):

- точки безпровідного доступу;
- робочі станції для кожного абонента.

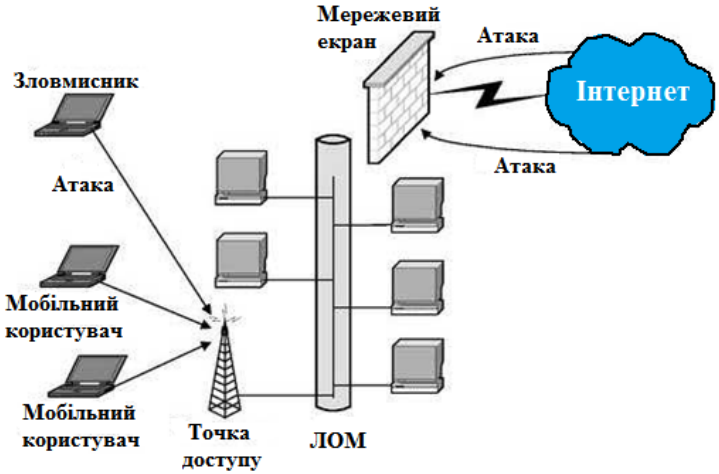

Рис. 1.16 Структура безпровідної локальної мережі WLAN

Точки доступу AP (*Access Point*) виконують роль концентраторів, що забезпечують зв'язок між абонентами і між собою, а також функцію мостів, що здійснюють зв'язок з кабельною локальною мережею і з Інтернетом.

Дещо близько розташованих точок доступу утворюють зону доступу Wi-

4. За *безпосереднім джерелом загроз*:

– **природне середовище**, наприклад стихійні лиха, магнітні бурі тощо;

– **людина**, наприклад вербування шляхом підкупу персоналу, розголошування конфіденційних даних і т.п.;

– **санкціоновані програмно-апаратні засоби**, наприклад видалення даних, відмова в роботі операційної системи;

– **несанкціоновані програмно-апаратні засоби**, наприклад зараження комп'ютера вірусами з деструктивними функціями.

5. За *ступенем залежності від активності ІТС*:

– **незалежно від активності ІТС**, наприклад розкриття шифрів криптозахисту інформації;

– **тільки в процесі обробки даних**, наприклад загрози виконання і поширення програмних вірусів.

6. За *положенням джерела загроз*:

– **поза контрольованої зони ІТС**, наприклад перехоплення даних, що передаються каналами зв'язку, перехоплення електромагнітних, акустичних та інших випромінювань пристроїв;

– **в межах контрольованої зони ІТС**, наприклад застосування підслуховуючих пристроїв, розкрадання роздруківок, записів, носіїв інформації і т.п.;

– безпосередньо в ІТС, наприклад некоректне використання ресурсів ІТС.

7. За *ступенем дії на ІТС*:

– **пасивні загрози**, які при реалізації нічого не міняють в структурі і змісті ІТС, наприклад загроза копіювання секретних даних;

– **активні загрози**, які при дії вносять зміни в структуру і зміст ІТС, наприклад впровадження троянських коней і вірусів.

8. За *етапами доступу користувачів або програм до ресурсів ІТС*:

– **загрози, що проявляються на етапі доступу до ресурсів ІТС**, наприклад загрози несанкціонованого доступу в ІТС;

– **загрози, що проявляються після дозволу доступу до ресурсів ІТС**, наприклад загрози несанкціонованого або некоректного використання ресурсів ІТС.

9. За *способом доступу до ресурсів ІТС*:

– **загрози з використанням стандартного шляху доступу** до ресурсів ІТС, наприклад незаконне отримання паролів та інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача;

– **загрози з використанням прихованого нестандартного шляху доступу** до ресурсів ІТС, наприклад несанкціонований доступ до ресурсів ІТС шляхом використання недокументованих можливостей операційної системи.

Причинами випадкових дій при експлуатації ІТС можуть бути:

– аварійні ситуації із-за стихійних лих і відключень електроживлення;

– відмови і збої апаратури;

– помилки в програмно-апаратном забезпеченні;

– помилки в роботі обслуговуючого персоналу і користувачів;

– перешкоди в лініях зв'язку із-за дій зовнішнього середовища.

Умисні загрози пов'язані з цілеспрямованими діями порушника (порушником можуть виступати службовець, відвідувач, конкурент, найманець і т.д.). Тут слід враховувати наступні чинники:

– порушником може бути як стороння особа, так і законний користувач системи – інсайдер;

– порушник, як правило, вибирає найбільш слабку ланку в захисті;

– кваліфікація порушника може бути на рівні розробника ІТС;

– порушникові відома інформація про принципи роботи системи.

Інсайдер – це людина, допущена до роботи з інформацією, яка призначена для строго обмеженого кола осіб. Використовуючи своє положення, інсайдери крадуть інформацію. Вони можуть пересилати її по електронній пошті, копіювати на різні USB-пристрої і КПК, записувати в ноутбуки, роздруковувати і виносити на папері, викладати на всілякі файлообмінні ресурси.

ливість збору адрес електронної пошти на заражених машинах. Вкрадені адреси продаються спамерам або використовуються при розсилці спаму самими хазяями ботнета. При цьому зростаючий ботнет дозволяє отримувати нові і нові адреси.

- **Анонімний доступ в Мережу** – зловмисники можуть звертатися до серверів в Мережі, використовуючи зомбі-машини, і від імені заражених машин здійснювати кіберзлочини, наприклад зламувати веб-сайти або переказувати вкрадені грошові кошти.

- **Продаж і оренда ботнетів** – один з варіантів незаконного заробітку за допомогою ботнетів ґрунтується на здачі ботнета в оренду або продажі готової мережі. Створення ботнетів для продажу є окремим напрямом кіберзлочинного бізнесу.

- **Крадіжка конфіденційних даних** – цей вид кримінальної діяльності постійно притягає кіберзлочинців, а за допомогою ботнетів «улов» у вигляді різних паролів (для доступу до електронної пошти, FTP-ресурсам, веб-сервісам) та інших конфіденційних цих користувачів збільшується в тисячі разів!

Бот, яким заражені комп'ютери в зомбі-мережі, може викачати іншу шкідливу програму, наприклад троянську програму, що краде паролі. У такому разі інфікованими троянською програмою виявляться усі комп'ютери, що входять в цю зомбі-мережу, і зловмисники зможуть дістати паролі з усіх заражених машин. Вкрадені паролі перепродаються або використовуються, зокрема, для масового зараження веб-сторінок (наприклад, паролі для усіх знайдених FTP-акаунтів) з метою подальшого поширення шкідливої програми-бота і розширення зомбі-мережі.

Основні причини атак на IP-мережі:

- використання загальнодоступних каналів передачі даних (найважливіші дані передаються мережею в незашифрованому виді);

- уразливості в процедурах ідентифікації, реалізованих в стеку TCP/IP (ідентифікуюча інформація на рівні IP передається у відкритому виді);

- відсутність у базовій версії стека протоколів TCP/IP механізмів, що за-

аферисти дістають доступ у кращому разі до його поштової скриньки, а в гіршому – до електронного рахунку.

- **Фарминг** (*Pharming*) – вид шахрайства, що ставить метою отримати персональні дані користувачів, але не через пошту, а прямо через офіційні вебсайти. Фармери замінюють на серверах DNS цифрові адреси легітимних вебсайтів на підробні, внаслідок чого користувачі перенаправляються на сайти шахраїв. Цей вид шахрайства ще небезпечніше, оскільки помітити підробку практично неможливо.

- **Застосування ботнетів. Ботнет** (*зомбі-мережа*) – це мережа комп'ютерів, заражених шкідливою програмою *Backdoor*, яка дозволяє порушникам видалено управляти зараженими машинами (кожній окремо, частиною комп'ютерів, що входять в мережу, або усією мережею цілком) без відома користувача. Такі програми називаються **ботами**. Ботнети мають потужні обчислювальні ресурси, є грізною кіберзброєю і хорошим способом заробляння грошей для зловмисників. При цьому зараженими машинами, що входять в мережу, хазяїн ботнета може управляти звідки завгодно: з іншого міста, країни або навіть з іншого континенту, а організація Інтернету дозволяє робити це анонімно.

Управління комп'ютером, який заражений ботом, може бути:

- *прямим* – порушник може встановити зв'язок з інфікованим комп'ютером і керувати ним, використовуючи вбудовані в тіло програми-бота команди;
- *опосередкованим* – бот сам з'єднується з центром управління або іншими машинами в мережі, посилає запит і виконує отриману команду.

- **Розсилка спаму** – це найбільш поширене і один з найпростіших варіантів експлуатації ботнетів. За експертними оцінками, нині більше 80% спаму розсилається із зомбі-машин. Спам з ботнетів необов'язково розсилається власниками мережі. За певну плату спамери можуть взяти ботнет в оренду. Багатотисячні ботнети дозволяють спамерам здійснювати із заражених машин мільйонні розсилки впродовж короткого часу. Ще одна «перевага» ботнетів – мож-

Основні канали НСД, через які порушник може отримати доступ до компонентів ІТС і здійснити розкрадання, модифікацію і/або руйнування інформації приведені на рис. 1.13, а поширені прийоми НСД – на рис. 1.14.

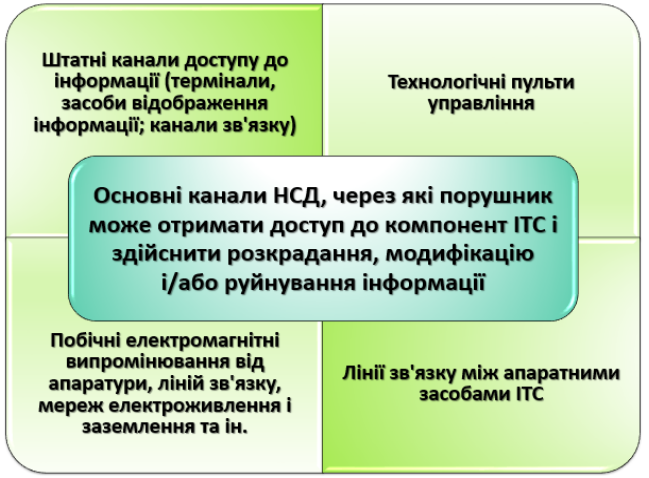

Рис. 1.13 Основні канали НСД до компонентів ІТС

Рис. 1.14 Поширені прийоми НСД

Перехоплення паролів здійснюється спеціально розробленими програмами. При спробі законного користувача увійти до системи програма- перехоплювач імітує на екрані введення імені та пароля користувача, які відразу пересилаються власникові програми-перехоплювача, після чого на екран виводиться повідомлення про помилку і управління повертається операційній системі. Ко-

ристувач припускає, що допустив помилку при введенні пароля. Він повторює введення і дістає доступ в систему. Власник програми- перехоплювача, що отримав ім'я і пароль законного користувача, може тепер використовувати їх у своїх цілях.

Маскарад – виконання яких-небудь дій одним користувачем від імені іншого користувача, що має відповідні повноваження. Метою маскараду є приписування яких-небудь дій іншому користувачеві або присвоєння повноважень і привілеїв іншого користувача. Приклади реалізації маскараду:

– вхід в систему під ім'ям і паролем іншого користувача (цьому маскараду передує перехоплення пароля);

– передача повідомлень в мережі від імені іншого користувача.

Незаконне використання привілеїв – системи захисту встановлюють певні набори привілеїв для виконання заданих функцій. Кожен користувач отримує свій набір привілеїв:

– звичайні користувачі – мінімальний;

– адміністратори – максимальний.

Несанкціоноване захоплення привілеїв, наприклад, за допомогою маскараду, призводить до можливості виконання порушником певних дій в обхід системи захисту. Незаконне захоплення привілеїв можливе або за наявності помилок в системі захисту, або через халатність адміністратора при управлінні системою і призначенні привілеїв.

Шкідливі програми. До таких програм відносяться:

- **комп'ютерний вірус** – це програмний код, який може заражати інші програми, модифікуючи їх за допомогою включення в них свої, можливо, змінені копії, причому остання зберігає здатність до подальшого розмноження;

- **мережевий черв'як** є шкідливою програмою, яка поширюється локальними або глобальними мережами;

- **троянський кінь** – програма, яка разом з діями, описаними в її документації, виконує деякі інші дії, що ведуть до порушення безпеки системи і деструктивних результатів.

ршим етапом діяльності псевдоантивіруса є «сканування» системи користувача. По ходу «сканування» псевдоантивірус виводить повідомлення, послідовність яких добре продумана: наприклад, помилка Windows, виявлення шкідливих програм, необхідність встановити антивірус. Фальшивий антивірус пропонує виправити нібито виявлені помилки і вилікувати систему, але вже за гроші. Чим достовірніше імітація дій серйозного легального ПЗ, тим більше у шахраїв шансів отримати плату за «роботу» лжеантивіруса.

Псевдоантивіруси практично неможливо виявити за допомогою євристичних сигнатур, які засновані на поведінковому аналізі.

- **Фішинг** (*Phishing*) – це вид інтернет-шахрайства, мета якого – отримати ідентифікаційні дані користувачів. Сюди відносяться крадіжки паролів, номерів кредитних карт, банківських рахунків, PIN-кодів та іншій конфіденційній інформації, що дає доступ до грошей користувача.

Фішинг використовує не технічні недоліки ПЗ, а легковірність користувачів Інтернету. Сам термін *phishing* (рибний лов), розшифровується як *password harvesting fishing* – вивуджування пароля. Зловмисник закидає в Інтернет «приманку» і «виловлює» усіх «рибок» – користувачів Інтернету, – які клюнуть на цю «приманку». Зловмисник створює практично точну копію сайту вибраного банку (електронної платіжної системи, аукціону і т.п.); потім за допомогою спам-технології по електронній пошті розсилається лист, складений так, щоб бути максимально схожим на справжній лист від вибраного банку. При складанні листа використовуються логотипи банку, імена і прізвища реальних керівників банку; у такому листі, як правило, повідомляється про те, що із-за зміни ПЗ в системі інтернет-банкінга користувачеві необхідно підтвердити або змінити свої облікові дані. В якості причини для зміни даних можуть бути названі вихід з ладу ПЗ банку або ж напад хакерів. В усіх випадках мета таких листів одна – змусити користувача клацнути по приведеному посиланню, а потім ввести свої конфіденційні дані (пароль, номер рахунку, PIN-код) на помилковому сайті банку (електронної платіжної системи, аукціону); зайшовши на помилковий сайт, користувач вводить у відповідні рядки свої конфіденційні дані, а далі

- *запитів DNS* – які допомагають зрозуміти, хто володіє тим або іншим доменом і які адреси цьому домену присвоєні;
- *ехо-тестування адрес* (*Ping Sweep*), розкритих за допомогою DNS, дозволяє побачити, які хости реально працюють в цьому середовищі;
- *сканування портів* використовується, щоб скласти повний список послуг, підтримуваних цими хостами. В результаті добувається інформація, яку можна використовувати для злому.

- **Зловживання довірою** – цей тип дій є зловмисним використанням стосунків довіри, існуючих в мережі. Типовим прикладом такого зловживання є ситуація в периферійній частині корпоративної мережі. У цьому сегменті зазвичай розташовуються сервери DNS, SMTP і HTTP Оскільки усі вони належать до одного сегменту, злом одного з них призводить до злому і усіх інших, оскільки ці сервери довіряють іншим системам своєї мережі. Ризик зловживання довірою можна понизити за рахунок суворішого контролю рівнів довіри в межах своєї мережі. Системи, розташовані із зовнішнього боку міжмережевого екрану, ніколи не повинні користуватися абсолютною довірою з боку систем, захищених міжмережевим екраном. Стосунки довіри повинні обмежуватися певними протоколами і по можливості автентифікуватися не лише по IP-адресам, але і по інших параметрах.

- **Псевдоантивіруси** – це шахрайські програми, що є фальшивими антивірусами. Хоча псевдоантивіруси виводять повідомлення про виявлення шкідливих програм, але насправді вони нічого не знаходять і не лікують. Їх завдання полягає зовсім в іншому: переконати користувача в наявності загрози (насправді неіснуючої) для комп'ютера і спровокувати його сплатити гроші за активацію «антивірусного продукту». Такий вид шахрайських програм називається *Fraud Tool* і відноситься до класу *RiskWare*.

Для поширення фальшивих антивірусів використовуються способи, вживані для поширення більшості шкідливих програм, наприклад приховане завантаження за допомогою *Trojan-Downloaded*, експлуатація вразливостей зламаних/заражених сайтів. Шахраї використовують також рекламу в Інтернеті. Пе-

Градації доступу до інформації, що зберігається, оброблюється і захищається в ІТС:

- *рівень носіїв інформації* (інформація для зручності маніпулювання найчастіше фіксується на матеріальному носії);

- *рівень засобів взаємодії з носієм* (якщо спосіб представлення інформації такий, що вона не може бути безпосередньо сприйнята людиною, виникає необхідність в перетворювачах інформації);

- *рівень змісту інформації* (людині має бути доступний сенс представленої інформації, її семантика);

- *рівень представлення інформації* (інформація може бути охарактеризована способом свого представлення, або тим, що називається мовою).

У табл. 1.3 перераховані методи реалізації загроз НСД залежно від рівня доступу до інформації в ІТС, а також від спрямованості загроз.

Основні **напрями реалізації порушником інформаційних загроз** в ІТС:

- безпосереднє звернення до об'єктів доступу;

- створення програмних і технічних засобів, що виконують звернення до об'єктів доступу в обхід засобів захисту;

- модифікація засобів захисту, що дозволяє реалізувати загрози інформаційної безпеки;

- впровадження в технічні засоби ІТС програмних або технічних механізмів, що порушують передбачувану структуру і функції ІТС.

Таблиця 1.3 Основні методи реалізації загроз НСД

Рівень доступу до інформації в ІТС	**Методи реалізації загроз НСД**			
	Загроза розкриття параметрів системи	*Загроза порушення конфіденційності*	*Загроза порушення цілісності*	*Загроза відмови служб (відмови доступу до інформації)*
Рівень носіїв інформації	- Визначення типу і параметрів носіїв інформації	- Розкрадання (копіювання) носіїв інформації	- Знищення машинних носіїв інформації	- Виведення з ладу машинних носіїв інформації
Рівень засобів взаємодії з носієм	- Отримання інформації про програмно-апаратне середо-	- НСД до ресурсів ІТС - Здійснення ко-	-Внесення користувачем несанкціонованих змін в програми і дані	- Прояв помилок проектування і розробки програмно- апаратних

	вище - Отримання детальної інформації про функції, що виконуються ІТС - Отримання даних про вживані системи захисту	ристувачем несанкціонованих дій - Несанкціоноване копіювання ПЗ - Перехоплення даних, що передаються каналами зв'язку	-Установка і використання нештатного ПЗ -Зараження шкідливим ПЗ	компонентів ІТС - Обхід механізмів захисту ІТС
Рівень представлення інформації	- Визначення способу представлення інформації	- Візуальне спостереження - Розкриття представлення інформації (дешифрування)	- Внесення спотворення в представлення даних - Знищення даних	- Спотворення відповідності синтаксичних і семантичних конструкцій мови
Рівень змісту інформації	- Визначення змісту даних на якісному рівні	- Розкриття змісту інформації	- Впровадження дезінформації	- Заборона на використання інформації

Аналіз загроз корпоративних мереж

Для організації комунікації в неоднорідному мережевому середовищі застосовується набір протоколів TCP/IP, що забезпечує сумісність між комп'ютерами різних типів. Крім того, протоколи TCP/IP надають доступ до ресурсів глобальної мережі Інтернет.

Завдяки своїй популярності TCP/IP став стандартом де-фактор для міжмережевої взаємодії. Проте повсюдне поширення стека протоколів TCP/IP оголило і його слабкі сторони. Створюючи своє дітище, архітектори стека TCP/IP не бачили причин особливо турбуватися про захист мереж, що будуються на його основі. Тому в специфікаціях ранніх версій протоколу IP були відсутні вимоги безпеки, що привело до первинної уразливості реалізації цього протоколу.

Проблеми забезпечення інформаційної безпеки в корпоративних комп'ютерних мережах обумовлені загрозами безпеки для локальних робочих станцій, локальних мереж і атаками на корпоративні мережі, що мають вихід в загальнодоступні мережі передачі даних.

Порушник, здійснюючи атаку, зазвичай ставить перед собою наступні цілі:

- порушення конфіденційності передаваної інформації;
- порушення цілісності і достовірності передаваної інформації;
- порушення працездатності системи в цілому або окремих її частин.

цей користувач має значні привілеї доступу, порушник може створити для себе «прохід» для майбутнього доступу, який діятиме, навіть якщо користувач змінить свої пароль і логін;

- **Вгадування ключа** – криптографічний ключ є кодом або числом, необхідним для розшифрування захищеної інформації. Хоча упізнати ключ доступу важко і такі спроби вимагають великих витрат ресурсів, проте це можливо. Зокрема, для визначення значення ключа може бути використана спеціальна програма, що реалізовує метод повного перебору. Ключ, до якого дістає доступ порушник, що атакує, називається *скомпрометованим*. Той, що атакує, використовує скомпрометований ключ для діставання доступу до захищених передаваних даних без відома відправника і одержувача. Ключ дає можливість розшифровувати і змінювати дані.

- **Атаки на рівні застосувань** – ці атаки можуть проводитися декількома способами. Найпоширеніший з них полягає у використанні відомих слабкостей серверного програмного забезпечення (FTP, HTTP, веб-сервера). Головна проблема з атаками на рівні додатків полягає в тому, що порушники часто користуються портами, яким дозволений прохід через міжмережевий екран. Хакери постійно відкривають і публікують на своїх сайтах в Інтернеті усі нові вразливі місця прикладних програм.

- **Аналіз мережевого трафіку** – метою атак подібного типу є прослуховування каналів зв'язку і аналіз передаваних даних і службової інформації з метою вивчення топології і архітектури побудови системи, отримання критичної призначеної для користувача інформації (наприклад, паролів користувачів або номерів кредитних карт, що передаються у відкритому виді). До атак цього типу схильні такі протоколи, як FTP і Telnet, особливістю яких є те, що ім'я і пароль користувача передаються у рамках цих протоколів у відкритому виді.

- **Мережева розвідка** – це збір інформації про мережу за допомогою загальнодоступних даних і додатків. При підготовці атаки проти якої-небудь мережі порушник, як правило, намагається отримати про неї якомога більше інформації. Мережева розвідка проводиться у формі:

ристовуються сніфери пакетів, транспортні протоколи і протоколи маршрутизації. Атаки «людина-в-середині» проводяться з метою крадіжки інформації, перехоплення поточної сесії і діставання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення передаваних даних і введення несанкціонованої інформації в мережеві сесії.

- **Атака експлойта** (*exploit* – експлуатувати) – це експлуатація комп'ютерної програми, фрагмента програмного коду або послідовності команд, що використовують уразливості в ПЗ і вживані для проведення атаки на комп'ютерну систему. Метою атаки може бути, як захоплення контролю над системою, так і порушення її функціонування (DoS-атака). Залежно від методу діставання доступу до уразливого ПЗ, експлойти поділяються на видалені і локальні:
  - *видалений експлойт* працює через мережу і використовує уразливість в захисті без якого-небудь попереднього доступу до уразливої системи;
  - *локальний експлойт* запускається безпосередньо в уразливій системі, вимагаючи попереднього доступу до неї. Зазвичай використовується для отримання порушником прав суперкористувача.
- **Парольні атаки** – метою цих атак є заволодіння паролем і логіном законного користувача. Порушники можуть проводити парольні атаки, використовуючи такі методи, як:
  - підміна IP-адреси (IP-спуфинг);
  - підслуховування (сніфинг);
  - простий перебір.

Часто хакери намагаються підібрати пароль і логін, використовуючи для цього численні спроби доступу. Такий підхід носить назву **«Атака повного перебору»** (*Brute Force Attack*). Для цієї атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті порушникові вдається підібрати пароль, він дістає доступ до ресурсів на правах звичайного користувача. Якщо

Рис. 1.15 Типи мережевих атак

Розподілені системи характеризуються наявністю *видалених атак*, оскільки компоненти розподілених систем зазвичай використовують відкриті канали передачі даних і порушник може не лише проводити пасивне прослуховування передаваної інформації, але і модифікувати передаваний трафік (активна дія) (рис. 1.15).

Атака доступу – це спроба отримання порушником інформації, на ознайомлення з якою у нього немає дозволу. Атаки доступу спрямовані на порушення конфіденційності інформації і підрозділяються на:

- **підслуховування** (*Sniffing*) – снифер пакетів є програмою, яка перехоплює усі мережеві пакети, що передаються через певний домен у відкритому виді;
- **перехоплення** (*Hijacking*) – це активна атака – порушник захоплює інформацію в процесі її передачі до місця призначення і дістає доступ до ресурсу на системному рівні;

- **перехоплення сеансу** (*Session Hijacking*) – після закінчення процедури автентифікації з'єднання, встановлене законним користувачем, перемикається порушником на новий хост, а початковому серверу видається команда розірвати з'єднання. В результаті «співрозмовник» законного користувача виявляється непомітно підміненим.

Атака модифікації – це спроба неправомочної зміни інформації. Така атака можлива скрізь, де існує або передається інформація; вона спрямована на порушення цілісності інформації:

- **зміна даних** – порушник, що отримав можливість прочитати дані, зможе зробити і наступний крок – змінити їх. Дані в пакеті можуть бути змінені, навіть якщо порушник нічого не знає ні про відправника, ні про одержувача;
- **додавання даних** – порушник додає нові дані, які дозволять йому зробити якісь неправомірні дії, наприклад, зломщик виконує операцію у банківській системі, внаслідок чого кошти з рахунку клієнта переміщаються на його власний рахунок;
- **видалення даних** – це переміщення існуючих даних, наприклад анулювання запису про операцію з балансового звіту банку, внаслідок чого зняті з рахунку грошові кошти залишаються на нім.

Атака «відмова в обслуговуванні» (*Denial-of-Service*, *DoS*) робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми.

Якщо атака проводиться одночасно через множину пристроїв, говорять про **розподілену атаку «відмову в обслуговуванні»** (*DDoS*, *Distributed DoS*).

Виділяються наступні різновиди цього виду атак:

- **відмова в доступі до інформації** – DoS-атаки, спрямовані проти інформації, яка стає непридатною для використання. Інформація знищується, спотворюється або переноситься в недоступне місце;
- **відмова в доступі до програм** – DoS-атаки, спрямовані на програми обробки або відображення інформацію, або на комп'ютерну систему, в якій ці

програми виконуються. У разі успіху подібної атаки рішення завдань, що виконуються за допомогою такої програми, стає неможливим;

- **відмова в доступі до системи** – загальний тип DoS-атак ставить своєю метою виведення із ладу ІТС, внаслідок чого сама система, встановлені на ній програми і уся збережена інформація стають недоступними;
- **відмова в доступі до засобів зв'язку** – метою атаки є комунікаційне середовище. Цілісність комп'ютерної системи й інформації не порушується, проте відсутність засобів зв'язку позбавляє користувачів доступу до цих ресурсів.

Комбіновані атаки – полягають в застосуванні порушником декількох взаємопов’язаних дій для досягнення своєї мети:

- **Підміна довіреного суб'єкта** – підміна IP-адреса відправника іншою адресою – такий спосіб атаки називають *фальсифікацією адреси* (*IP-спуфингом*, **IP-spoofing**). IP-спуфинг має місце, коли порушник, що знаходиться усередині корпорації або поза нею, видає себе за законного користувача. Порушник може:
  - скористатися IP-адресою, що знаходиться в межах діапазону санкціонованих IP-адресів, або авторизованою зовнішньою адресою, яка дозволяє доступ до певних мережевих ресурсів;
  - використовувати спеціальні програми, формувальні IP-пакети так, щоб вони виглядали як витікаючі з дозволених внутрішніх адрес корпоративної мережі.
- **Посередництво** – атака має на увазі активне підслуховування, перехоплення передаваних даних невидимим проміжним вузлом і управління ними. Коли комп'ютери взаємодіють на низьких мережевих рівнях, вони не завжди можуть визначити, з ким саме вони обмінюються даними.
- **Посередництво в обміні незашифрованими ключами** (атака **Man-in-the-Middl** – «*людина-в-середині*») – для проведення атаки порушникові потрібний доступ до пакетів, що передаються по мережі. Такий доступ до усіх пакетів, що передаються від провайдера ISP у будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак цього типу часто вико-