МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ»

Я.Ю. Дорогий, А.О. Нікітенко

Методи та засоби технічного захисту інформації. ПРАКТИКУМ

Електронний навчальний посібник

Рекомендовано Державним вищим навчальним закладом
«Донецький національний технічний університет»
Міністерства освіти і науки України
як навчальний посібник для здобувачів освіти
галузі знань 12 «Інформаційні технології» всіх форм навчання

Луцьк
ДВНЗ «ДонНТУ»
2024

УДК 004.056-049.65
Д 69

Рекомендовано Вченою Радою Державного вищого навчального закладу «Донецький національний технічний університет» Міністерства освіти і науки України як навчальний посібник для здобувачів освіти галузі знань 12 «Інформаційні технології» всіх форм навчання (Протокол № 4 від 28.03.2024 р).

Автори:

Я.Ю. Дорогий, д-р техн. наук, доцент, професор кафедри прикладної математики та інформатики (Державний вищий навчальний заклад «Донецький національний технічний університет»).

А.О. Нікітенко, асистент кафедри прикладної математики та інформатики (Державний вищий навчальний заклад «Донецький національний технічний університет»).

Рецензенти:

В.В. Цуркан, кандидат технічних наук, доцент, доцент Спеціальної кафедри №5 Інституту спеціального зв'язку та захисту інформації (Національний технічний університетУкраїни «Київський політехнічний інститут ім. Ігоря Сікорського»).

В.Я. Воропаєва, к.т.н., доцент, Проректор з науково-педагогічної роботи ДонНТУ, професор кафедри автоматики та телекомунікацій (Державний вищий навчальний заклад «Донецький національний технічний університет»).

Дорогий Я.Ю. Методи та засоби технічного захисту інформації. Практикум: електрон. навч. посіб. / *Я.Ю.Дорогий, А.О. Нікітенко*. – Луцьк : ДонНТУ, 2024. – 241 с.

В посібнику зібрано матеріали для здобуття навичок з технічного захисту інформації, у тому числі – з проєктування комплексу ТЗІ, створення підсистем фізичного захисту джерел інформації, отримання характеристик технічних засобів захисту, засобів контролю й спостереження. Наведено теоретичні відомості з навчальної дисципліни, контрольні запитання, завдання для практичного та самостійного опрацювання, перелік літератури. Отримання практичних навичок пропонується організувати у вигляді ділової гри.

Навчальний посібник призначений для здобувачів освіти, які навчаються за спеціальностями 12 галузі «Інформаційні технології», зокрема, спеціальності 125 «Кібербезпека», але може бути застосований студентами споріднених спеціальностей й буде корисним практикуючим фахівцям з інформаційних та інформаційно-вимірювальних технологій.

ISBN 000-000-000-000-0

© Дорогий Я.Ю., Нікітенко А.О., 2024

ЗМІСТ

ВСТУП

Розвиток людства на тлі показного добробуту в розвинених країнах та декларацій про необхідність захисту людських цінностей характеризується загостренням конкуренції між державами, організаціями та людьми за "життєвий" простір, ринки збуту та якість життя. Це спричинене зростанням чисельності людства, зменшенням природних ресурсів Землі, погіршенням екології та побічними негативними процесами технічного прогресу.

Основу будь-якої діяльності людей становить її інформаційне забезпечення. Інформація стає одним із основних засобів вирішення проблем та завдань держави, політичних партій та діячів, різних комерційних структур та окремих осіб. Оскільки отримання інформації шляхом проведення власних досліджень стає все більш витратним, то розширюється сфера здобування інформації дешевим, але незаконним шляхом.

У зв'язку з цими обставинами неперервно зростає актуальність завдань захисту інформації в усіх сферах діяльності людей: на державній службі, у бізнесі, у науковій діяльності та навіть у особистому житті. Постійна конкуренція між методами та засобами здобування та захисту інформації призвела до появи на ринку різноманітних пристроїв та приладів у цій предметній області, що створює проблему раціонального вибору та застосування заходів захисту.

Серед заходів захисту інформації все більшу вагу об'єктивно набуває технічний захист інформації, що ґрунтується на використанні різноманітних технічних засобів забезпечення безпеки інформації. Така тенденція обумовлена наступними причинами:

1. Постійним і неперервним впровадженням у інформаційні процеси в різних сферах життя суспільства безпаперової технології. При цьому йдеться не лише про широке використання обчислювальної техніки, але й про засоби масової інформації, освіти, торгівлі, зв'язку тощо.

2. Величезними досягненнями в області мікроелектроніки, що створюють технічну та технологічну базу для масового виробництва доступних звичайному покупцеві засобів нелегального здобування інформації з мінімальним ризиком. Зменшення ж ризику та загрози покарання збільшує число любителів легкого збагачення на протиправні дії. Доступність мініатюрних та камуфльованих засобів здобування інформації перетворює задачу по нелегальному здобуванню інформації з унікальної та ризикованої операції в прибутковий бізнес.

3. Оснащення службових та житлових приміщень, а також в останні часи автомобілів, різноманітною електро- та радіоелектронною апаратурою сприяє випадковому неконтрольованому витоку конфіденційної інформації з приміщень та автомобілів, зумовленому фізичними процесами у цій апаратурі.

Очевидно, що ефективний захист інформації державних та комерційних структур, а також окремих фізичних осіб з урахуванням цих тенденцій можливий лише за більш широкого використання технічних засобів захисту. Значне зростання зацікавленості у проблемі захисту інформації з боку не лише фахівців, але і комерційних структур та окремих громадян України стимулювало зростання кількості публікацій з даної тематики. Різноманіття, іноді поверхових, думок з питань захисту інформації, відсутність єдиного понятійного апарату, слабкість теоретичної та методологічної бази, яка враховує специфіку захисту інформації в умовах ринку, викликає необхідність в систематизації та структуруванні накопичених у цій області знань та створення основ технічного захисту інформації.

Рішенню деяких практичних задач й присвячений цей навчальний посібник. Він призначений для студентів галузі знань 12 Інформаційні технології та інших, які вивчають питання, пов’язані з тематикою технічного захисту інформації, а також для фахівців, що займаються питаннями організації та управління захистом інформації, та інших осіб, які цікавляться питаннями захисту інформації.

1 НОРМАТИВНО-ПРАВОВА БАЗА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Діяльність державної системи захисту інформації регламентується документами, що становлять нормативно-правову базу технічного захисту інформації. Основу її складають документи, класифікація яких наведена на рис. 1.1.

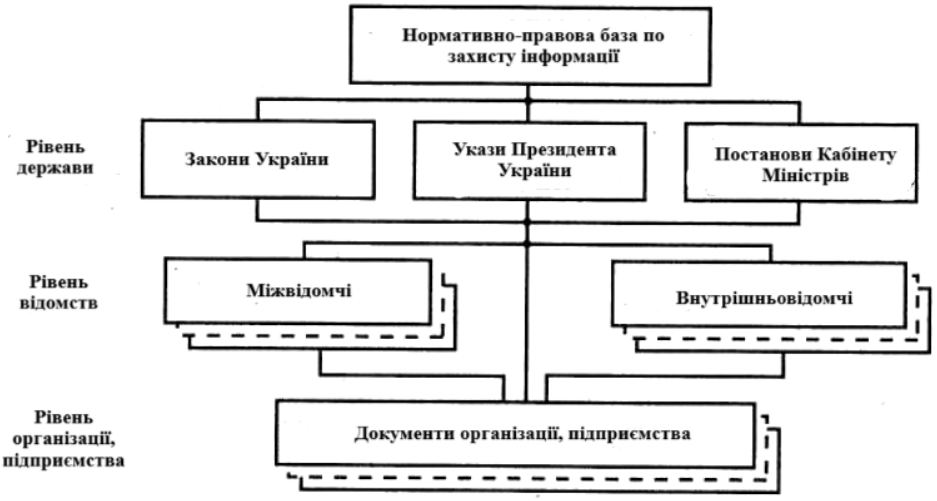


Рисунок 1.1 – Класифікація документів нормативно-правової бази захисту інформації

За призначенням документи поділяються на:

- керівні;
- нормативні;
- методичні.

Керівні документи визначають структуру, права та обов'язки органів і людей, які забезпечують технічний захист інформації на різних рівнях державної системи. Керівні документи розробляються на всіх рівнях державної системи захисту, причому документи на нижчому рівні конкретизують документи вищого рівня.

Будь-яка діяльність з виконання керівних документів супроводжується прийняттям рішень з того чи іншого питання. Основу прийняття рішень становить ідентифікація поточних факторів або ознак з еталонними. Сукупність еталонних факторів або ознак є сутністю поняття «норма» і змістом нормативних документів. Поняття норми широко використовують у всіх сферах діяльності людей. Наприклад, у суспільстві існують норми поведінки, частина яких законодавчо закріплена в Цивільному кодексі. Грубі відхилення від норм поведінки – злочини та шкала покарань залежно від рівня відхилення від норми розглянуті у Кримінальному кодексі. Норми в людському суспільстві можуть змінюватися еволюційно в процесі його розвитку і трансформуватися окремими групами людей, які володіють силами та засобами психологічного впливу на населення.

Нормативи в галузі технічного захисту інформації визначені фахівцями в нормативних документах. В результаті порівняння поточних показників захисту інформації з необхідними нормативами приймається рішення про рівень безпеки інформації, що захищається.

Так як поточні показники ефективності захисту інформації залежать від великої кількості факторів, то **методики** їх визначення різними органами та фахівцями і, отже, отримані результати в загальному випадку можуть відрізнятися. Наприклад, якщо не збігаються методики вимірювання рівнів небезпечних сигналів у контролюючого та контрольованого органів, то фахівцям контрольованого органу важко довести достатність використовуваних ходів захисту. Тому, як правило, одночасно розробляються нормативи та **методики** їх визначення, які поєднуються в нормативно-методичні документи.

Основні закони України, укази Президента України та Постанови КМУ у галузі технічного захисту інформації зазначені в табл. 1.1.

Основу міжвідомчих документів становлять рішення, керівні та нормативно-методичні документи Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). У них розглядаються основи концепції захисту інформації від технічної розвідки, типові положення про

органи захисту інформації, вимоги та методичні рекомендації щодо захисту інформації від витоку технічних каналів, керівні документи з різних аспектів захисту інформації в автоматизованих системах, нормативно-методичні документи щодо протидії різним видам технічної розвідки.

Таблиця 1.1 – Основні документи у галузі технічного захисту інформації

№	Рівень документа	Назва документа	Дата прийняття
1	ЗУ	Про захист інформації в інформаційно-телекомунікаційних системах	05.07.1994
2	ЗУ	Про основні засади державного нагляду (контролю) у сфері господарської діяльності"	05.04.2007
3	ЗУ	Про доступ до публічної інформації	13.01.2011
4	ЗУ	Про ліцензування видів господарської діяльності	02.03.2015
5	ЗУ	Про Державну службу спеціального зв’язку та захисту інформації України	23.02.2006
6	Укази Президента України	Про положення про технічний захист інформації в Україні	27.09.1999
7	Постанова Кабінету Міністрів	Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах	29.03.2006

У кожному відомстві держави, що є власником або користувачем інформації, що містить державну таємницю, розробляються та конкретизуються керівні та нормативно-методичні документи та створюються органи, які

забезпечують захист інформації як у самому відомстві, так і підлеглих під поділами (організаціями, підприємствами).

До керівних документів, що розробляються в організації (на підприємстві), належать:

• керівництво (інструкція) із захисту інформації в організації (на підприємстві);

• положення про підрозділ організації, на який покладаються завдання щодо забезпечення безпеки інформації;

• інструкції із захисту окремих джерел інформації, насамперед інформації про вироби, що розробляються, та продукції.

У різних організаціях ці документи можуть мати різні назви, від зазначених. Але сутність цих документів залишається незмінною, оскільки потреба в них об'єктивна.

Порядок захисту в організації визначається відповідним керівництвом (інструкцією). Воно може містити такі розділи:

• загальні положення;

• перелік відомостей, що охороняються;

• демаскуючі ознаки об'єктів організації;

• оцінки можливостей органів та засобів добування інформації;

• організаційні та технічні заходи щодо захисту інформації;

• порядок планування робіт служби безпеки;

• порядок взаємодії з державними органами, які вирішують завдання щодо захисту матеріальної та інтелектуальної власності, державної та комерційної таємниці.

Але в цьому посібнику не можна врахувати всіх особливостей захисту інформації в конкретних умовах. У будь-якій організації постійно змінюється ситуація з джерелами та носіями конфіденційної інформації, загрозами її безпеці. Наприклад, появі нового товару на ринку передує велика робота, що включає різні етапи та стадії: проведення досліджень, розробка лабораторних та діючих макетів, створення дослідного зразка та його доопрацювання за

результатами випробувань, підготовка виробництва (документації та додаткового обладнання), виготовлення дослідної серії виявлення попиту товар, масовий випускати продукцію.

На кожному етапі та стадії до роботи підключаються нові люди, розробляються нові документи, створюються вузли та блоки з інформативними для них демаскуючими ознаками. Створенню кожного виробу або самостійного документа супроводжує свій набір інформаційних елементів, їх джерел та носіїв, загроз і каналів витоку інформації, що виявляються в різні моменти часу.

Для захисту інформації про виріб на кожному етапі його створення розробляється відповідна інструкція. Інструкція повинна містити відомості, необхідні для забезпечення безпеки інформації, у тому числі: загальні відомості про зразок, відомості про нього, що захищаються, та його демаскуючі ознаки, потенційні загрози безпеці інформації, задум і заходи щодо захисту, порядок контролю (завдання, органи контролю, мають право на перевірку, засоби контролю, допустимі значення контрольованих параметрів, умови та методики, періодичність та види контролю), прізвища осіб, відповідальних за безпеку інформації.

Нормативно-методичну базу становлять:

- державні стандарти (ДСТУ);
- загальні вимоги (ЗВ), загальні технічні вимоги (ЗТВ), тактико-технічні вимоги (ТТТ), керівні документи (КД) та інші документи;
- моделі;
- норми, методики та інструкції;
- експлуатаційно-технічна документація;
- навчально-методична та наукова література.

Перелік основних державних стандартів на технічні засоби охорони зазначено у табл. 1.2.

Таблиця 1.2 – Перелік основних державних стандартів на технічні засоби охорони

№ п/п	Номер ДСТУ	Найменування ДСТУ
1	ДСТУ 3396 0-96	Технічний захист інформації. Основні положення
2	ДСТУ 3396 1-96	Технічний захист інформації. Порядок проведення робіт.
3	ДСТУ 4145-2002	Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка
4	ДСТУ ISO/IEC TR 13335-1:2003	Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина 1. Концепції й моделі безпеки IT (ISO/IEC TR 13335-1:1996, IDT
5	ДСТУ ISO/IEC 14888-2:2015	Інформаційні технології. Методи захисту. Цифрові підписи з доповненням. Частина 2. Механізми, що ґрунтуються на факторизації цілих чисел (ISO/IEC 14888-2:2008, IDT)

Основним нормативним документом є перелік відомостей, що становлять державну, військову, комерційну або будь-яку іншу таємницю. Перелік відомостей, що містять державну таємницю, ґрунтується на положеннях Закону «Про державну таємницю». Переліки відомостей цього закону, що підлягають захисту, конкретизуються відомствами стосовно тематики конкретних організацій. У комерційних структурах, що виконують державні замовлення, переліки поширюються на інформацію, що стосується цього замовлення. Переліки відомостей, що становлять комерційну таємницю, складаються керівництвом фірми за участю співробітників служби безпеки.

Інші нормативні документи визначають максимально допустимі значення рівнів сигналів з інформацією, що захищається, і концентрації демаскуючих

речовин на межах контрольованих зон, не перевищення яких забезпечує необхідний рівень безпеки інформації. Ці норми розробляються з відповідними відомствами, а для комерційних структур, які виконують недержавні замовлення, є фахівцями цих структур. Крім того, нормативні документи поєднані з методиками виміру параметрів норм.

Робота з захисту інформації в організації проводиться всіма його співробітниками, але ступінь участі різних категорій суттєво відрізняється. Будь-який співробітник, який підписав зобов'язання про нерозголошення таємниці, бере участь у захисті інформації хоча б шляхом виконання керівних документів про захист інформації.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5. Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Основні завдання державної системи захисту інформації від технічної розвідки.

2. Сутність категорій порушень вимог щодо захисту інформації.

3. Структура державного захисту інформації від технічної розвідки.

4. Завдання та структура Державної служби спеціального зв’язку та захисту

інформації (ДССЗЗІ).

5. Завдання та структура органів захисту інформації Служби безпеки України (СБУ).

6. Завдання органів із забезпечення захисту інформації відомств.

7. Види та органи ліцензування продукції, діяльності та послуг із захисту інформації.

8. Завдання та структура захисту інформації в організаціях (установах, на підприємствах).

9. Класифікація документів нормативно-правової бази щодо захисту інформації.

10. Призначення керівних та нормативно-методичних документів щодо захисту інформації.

2 ПІДСИСТЕМА ФІЗИЧНОГО ЗАХИСТУ ДЖЕРЕЛ ІНФОРМАЦІЇ

Основні складові систем ТСО: датчики, прилади візуального спостереження, системи збирання та обробки інформації, засоби зв'язку, живлення та тривожно-викличної сигналізації

Підсистема фізичного захисту створюється для протидії навмисним загрозам впливу зловмисника і стихійним силам, насамперед пожежі. Засоби цієї підсистеми реалізують методи фізичного захисту за допомогою інженерних конструкцій та технічних засобів охорони. Необхідність та ефективність інженерного захисту та технічної охорони об'єктів підтверджується статистикою, відповідно до якої понад 50% вторгнень здійснюється на комерційні об'єкти з вільним доступом персоналу та клієнтів і лише 5% – на об'єкти з посиленим режимом охорони, із застосуванням спеціально навченого персоналу та складних технічних систем охорони.

Основу засобів інженерного захисту та технічної охорони об'єктів складають механічні засоби та інженерні споруди, що перешкоджають фізичному руху зловмисника) до місця знаходження об'єктів захисту, технічні засоби, що інформують співробітників служби безпеки (охорону) про проникнення зловмисника(-ів) у контрольовану зону та що дозволяють спостерігати обстановку в них, а також засоби та люди, які усувають загрози.

Проникнення зловмисників може бути потайливим, з механічним руйнуванням інженерних конструкцій та засобів охорони за допомогою інструменту або вибуху, а в окремих випадках у вигляді збройного нападу з нейтралізацією охоронців. Відповідно до принципу багатозональності та багаторубіжності захисту інформації рубежі захисту створюються, перш за все, на межах контрольованих (охоронюваних) зон.

Склад підсистеми фізичного захисту може істотно відрізнятися: від дерев'яних дверей з простим замком для більшості житлових квартир до автоматизованої системи охорони з групою швидкого реагування великої

організації (підприємства). У випадку структура підсистеми фізичного захисту представлена на рис. 2.1.

Рисунок 2.1 – Структура підсистеми фізичного захисту

Сучасну підсистему фізичного захисту організації (підприємства, фірми) по вирішуваним завданням можна поділити на комплекс інженерного захисту джерел інформації та комплекс технічної охорони.

Інженерний захист інформації забезпечують:

• природні та штучні перепони (бар'єри) на можливому шляху руху зловмисників та поширення стихійних сил до джерел інформації (або іншим цінностям);

• запобіжні пристрої систем контролю та управління допуском.

До **природних перешкод** належать важкопрохідні ділянки місцевості, що примикають або знаходяться на території організації (рви, яри, скелі, річки, густі ліс і чагарник), які доцільно використовувати для зміцнення кордонів.

Штучні перешкоди створюються людьми і суттєво відрізняються за конструкцією та стійкістю до дії зловмисника. Ними є паркани, стіни, міжповерхові перекриття (підлоги, стелі), вікна будівель та приміщень, тобто інженерно-архітектурні конструкції, що є перепоною на шляху руху зловмисника. Найбільш важкопереборні перешкоди для зловмисника

створюють капітальні (бетонні та цегляні) високі (вище зростання людини) паркани, стіни та міжповерхові перекриття будівель.

Найменш стійкими перешкодами є **двері** та **вікна будівель** (приміщень), особливо на першому та останньому поверхах будівель та у місцях близького розташування вікон від парканів, будівель, на рушниць і дерев. Зі статистики квартирних крадіжок, яка відображає слабкі місця інженерного захисту приміщень, випливає, що більшість крадіжок відбувається шляхом вибивання дверей, зриву петель, підбору ключів, проникнення через вікна, кватирки та балкони.

Вікна зміцнюють застосуванням спеціальних, стійких до механічних ударів стекол і встановленням у віконних отворах металевих грат.

Двері та ворота — традиційні конструкції для пропуску людей або транспорту на територію організацію або в приміщення . Міцність дверей визначається товщиною, видом матеріалу та конструкцією дверного полотна та дверної рами, а також міцністю кріплення та кріплення рами до стіни та надійністю замків. Вимоги до міцності дверей вказані у ДСТУ EN 14351-1:2020.

Останні рубежі захисту створюють металеві шафи, сейфи та сховища. Тому до їх механічної міцності пред'являються підвищені вимоги. Металеві шафи призначені для зберігання документів з невисоким грифом конфіденційності, цінних речей, невеликої суми грошей. Надійність шафи визначається лише міцністю металу та секретністю замків.

Для зберігання особливо цінних документів, речей, великих сум грошей застосовуються **сейфи** та **сховища.** До сейфів і сховищ належать двостінні металеві шафи з важкими наповнювачами простору між стінками, якими використовуються армовані бетонні склади, композити, багатошарові заповнювачі з різних матеріалів.

Традиційно для проходу людей і проїзду транспорту на територію організації використовуються хвіртки в паркані, двері будівлі та ворота для автотранспорту, що закриваються на замок. Для забезпечення санкціонованого допуску людей і транспорту в контрольовані зони створюється **система**

контролю та управління доступом (СКУД) людей та транспорту**.** Структурна схема контрольно-пропускного пункту (КПП) СКУД наведена на рис. 2.2.

Рисунок 2.2 – Структура системи контролю та управління доступом
Позначення: ДП – ознаки, що демаскують, ІСБ – інтегральна система безпеки

Для виявлення людини або автомашини необхідно виміряти їх ознаки, що демаскують, що використовуються для ідентифікації, утворити поточні ознакові структури, порівняти їх з еталонними і за результатами порівняння прийняти рішення про допуск або заборону на допуск об'єкта. Процедура ідентифікації (порівняння поточної ознакової структури з еталонною) проводиться в контролері (пристрої ідентифікації). Контролер може використовуватися в автономному режимі або у складі локальної мережі інтегральної системи безпеки. Пропуск об'єкта в контрольовану зону або його недопущення здійснює виконавчий пристрій.

Очевидно, чим більш інформативні ознаки використовуються для ідентифікації, то менші значення помилок. Якщо допускається об'єкт, що не має на це право, то виникає з ймовірністю $P_{лд}$ помилка помилкового допуску (помилка 1-го роду), якщо не допускається об'єкт, що має допуск, то з ймовірністю $P_{лз}$ виникає помилка помилкової заборони на допуск або помилка 2-го роду. З погляду інформаційної безпеки, ймовірність помилкового допуску більшою мірою характеризує надійність СКУД, ніж заборони на допуск. Імовірність помилки 2-го роду зменшує пропускну здатність СКУД, яка оцінюється кількістю ідентифікованих об'єктів в одиницю часу. Зрештою, всі об'єкти, що мають допуск, після додаткової процедури ідентифікації будуть

допущені у відповідну контрольовану зону. Пропущені ж зловмисники можуть завдати інформації і не тільки їй непоправної шкоди. Тому для забезпечення необхідного рівня безпеки інформації від загроз навмисного впливу ймовірність помилкового допуску має бути не більш допустимою, а ймовірність помилкового заборони — мінімально можливою.

Помилки допуску визначаються насамперед інформативністю поточної та еталонної ознакових структур ідентифікаторів. Ідентифікатор являє собою носій демаскуючих знаків, які використовуються для ідентифікації і належать суб'єкту або об'єкту ідентифікації, що має допуск.

Для ідентифікації застосовуються **атрибутні** та **біометричні ідентифікатори.** Як атрибутні ідентифікатори використовуються автономні носії ознак суб'єкта або об'єкта. Наприклад, ключ, що відкриває двері або ворота, дозволяє вхід людині або в'їзд водію, які володіють ключем на момент допуску. Як атрибутні ідентифікатори застосовуються також: спецодяг (форма працівника МВС, халат лікаря або сестри), документ, що засвідчує особу, або технічний паспорт автомобіля, перепустка, ідентифікаційні картки, в яких іменні ознаки записуються на магнітній смузі, у штрих-коді, у структурі перевипромінюючого картою «Віганда» зовнішнього магнітного поля, кодової послідовності радіо сигналу, випромінюваного «Proximty» картою.

Помилки ідентифікації виникають у разі помилкової ідентифікації і якщо ідентифікатор з ознаками одного об'єкта (суб'єкта) потрапляє до іншого суб'єкта (об'єкта). Зменшення помилок ідентифікації людини чи автотранспорту досягається:

• підвищенням інформативності та кількості демаскуючих ознак ідентифікаторів;

• надійною прив'язкою ідентифікаторів до об'єкта ідентифікації.

Помилковий допуск об'єкта ідентифікації в контрольовану зону виникає не тільки за рахунок помилок пристроїв ідентифікації, а й у результаті підробки ідентифікаторів. Одна з оборотних сторін технічного прогресу — проблема захисту атрибутних ідентифікаторів від підробки. Сучасні ідентифікаційні

картки (штрихові, магнітні, «Віганда», Proximty) забезпечують дуже малі помилки ідентифікації. Деякі з них (карти «Віганда» та «Proximty») дуже складно підробити. Однак ідентифікаційні карти слабо прив'язані до об'єкта ідентифікації. Їх можуть викрасти, купити та відібрати. У цьому відношенні навіть найзахищеніші карти не відрізняються від ідентифікаторів часів громадянської війни-мандатів. Мандати являли собою аркуш паперу, на якому були надруковані або навіть написані від руки реквізити (прізвище, ім'я, по батькові представника влади, посада або виконувані функції) і завірені підписом особи, що видала мандат, і печаткою установи. Єдиним доказом приналежності мандата (так само як і безконтактної «Proximty» карти) конкретної людини була наявність мандата або картки у цієї людини.

Для прив'язки атрибутного ідентифікатора до суб'єкта (об'єкту) вживаються різні заходи. Наприклад, до відповідальності притягуються люди, які привласнили неналежний їм атрибут — що наділи для виконання протизаконних дій форму військовослужбовця або співробітника правоохоронних органів. Найчастіше для прив'язки ідентифікатора до конкретної людини в ідентифікатор вносяться ознаки цієї людини. До винаходу фотографії ознаки (прикмети) людини (зростання, характер статури, тип обличчя, форма носа, колір очей і волосся та інші прикмети) словами вписувалися в атрибутний ідентифікатор, зараз використовується фотографія його обличчя. Фотографія особи — найпоширеніший засіб прив'язки ідентифікатора до конкретної людини. Але фотографію можна замінити або навіть змінити обличчя за допомогою пластичної операції , що досить часто спостерігається у кримінальному світі.

Радикальним вирішенням проблеми виключення підробки та крадіжки атрибутних ідентифікаторів є застосування біометричних ідентифікаторів. Як біометричні ідентифікатори використовуються іменні ознаки людини, втратити які можна тільки разом з відповідним органом. Поряд із традиційними відбитками пальців використовуються фізіологічні та динамічні характеристики людини та її окремих органів: малюнки райдужної оболонки очей та кровоносних судин на її сітківці, термографія (теплове зображення обличчя),

геометрія пензля, динаміка підпису або друку на клавіатурі, спектральні характеристики мови людини. Значення показників біометричних ідентифікаторів значно різняться. Малюнки папілярних ліній пальців, райдужної оболонки та кровоносних судин сітківки ока забезпечують ймовірності несанкціонованого пропуску, близькі до 0, але реалізуються дорогою апаратурою. При використанні інших ознак помилки вищі, але кошти дешевші. Крім того, населення поки що психологічно не готове до широкого впровадження СКУД. Наприклад, малюнок райдужної оболонки очей містить конфіденційну інформацію про стан здоров'я людини, яку використовує медицина для діагностики його здоров'я, у разі використання для СКУД, стан може стати відомим стороннім людям. Але складність, ціна радіоелектронних засобів та психологічна готовність користувачів до їх застосування — мінливі фактори, а переваги біометричних ідентифікаторів очевидні та постійні.

У найпростішому варіанті ідентифікацію людей за атрибутними ідентифікаторами проводить на КПП охоронець, який натисканням педалі розблокує турнікет, що обертається, для проходу допущеної людини. Така організація пропускного режиму, яка застосовується ще в багатьох держустановах і на промислових підприємствах, має малу пропускну здатність і низьку достовірність селекції, особливо в умовах дефіциту часу. Коли перед очима співробітника охорони безперервно проходить потік людей, які поспішають на роботу, то в умовах психологічного тиску черги різко зростає ймовірність помилкової ідентифікації людини по фотографії на пропуску.

При застосуванні ідентифікаційних карток і біометричних ідентифікаторів цю процедуру виконують автомати, які здійснюють зчитування демаскуючих ознак з карточки або з людини, порівнюють їх з еталонними, попередньо занесеними в пам'ять пристрою, і за результатами порівняння видають сигнал управління виконавчому пристрою. Для зчитування інформації магнітні карти або карти зі штрих-кодом проводяться через передбачений у зчитувальному пристрої проріз або вставляються у відповідну щілину, що вимагає від об'єкта, що ідентифікується, уважності та акуратності. Більш зручними є ідентифікаційні

карти з можливістю дистанційного зчитування ознак — карти «Віганда» та «Proximity». Для зчитування ознак людини він повинен попередньо ввести з пульта свій ідентифікаційний номер, а потім докласти палець або кисть руки до віконця оптичного зчитувального пристрою, направити погляд на телевізійну камеру, написати певне слово, ввести його з клавіатури або вимовити вголос. Дані, що зчитуються, перетворюються процесором комп'ютера або мікропроцесором спеціального пристрою ідентифікації в поточну ознакову структуру, яка порівнюється з еталонною, викликаною з бази еталонів попередньо вводиться ідентифікаційним номером.

Фізичний допуск людини або автотранспорту в контрольовану зону здійснює **виконавчий пристрій (керований запобіжний пристрій).** Найпростішим пристроєм є двері. Якщо ідентифікатор — ключ не відповідає еталону в замку, двері не відчиняються і забороняють прохід у приміщення. В організаціях і громадських місцях (на транспорті, стадіонах та ін.) широко застосовуються **двері, що обертаються, розсувні і обертові три- або чотиришгангові турнікети висотою** до пояса і на повне зростання. Турнікети мають механізм блокування обертання, який при дозволі допуску розблокується педаллю контролера (вахтера, охоронця) або автоматично за сигналом керування. Найбільш досконалими виконавчими пристроями СКУД людей є шлюзові тамбури, які представляють кабіну з двома дверима. При проході людини в шлюз вхідні двері зачиняються, а після проходження процедури ідентифікації за роздільною командою контролера (вахтера) або автоматичного пристрою ідентифікації відчиняються вихідні двері. При відмові в допуску шлюзовий тамбур дозволяє затримати людину, яка перебуває в ньому, для з'ясування особистості. Передбачено також режим аварійного виходу людей у разі несправності виконавчого пристрою або знеструмлення СКУД. Для спостереження за людиною, що знаходиться в тамбурі, його стіни виконані з ударомічного скла (бронескла) або пластику. Усередині шлюзу встановлюються пристрої визначення атрибутних або біометричних ідентифікаційних ознак, а також можуть бути встановлені детектори металевих предметів для виявлення

зброї або радіоелектронних засобів, не дозволених для пронесення на контрольовану територію, а також телевізійна камера спостереження.

Контрольно-пропускний пункт на вході організації включає:

- зал із засобами контролю та управління доступом для проходу людей;
- бюро перепусток;
- камеру зберігання речей персоналу та відвідувачів, не дозволених для пронесення в організацію;
- приміщення для начальника охорони, чергового контролера, розміщення охоронної сигналізації та зв'язку та інші;
- засоби контролю та управління доступом транспорту.

Конструкція, склад та кількість КПП визначаються розмірами території організації та кількістю персоналу. КПП повинні забезпечувати необхідну пропускну спроможність людей та транспорту. Запасні входи та проїзди для пропуску людей та транспорту в аварійній ситуації в нормальних умовах закриваються , пломбуються або опечатуються.

Підкомплекс виявлення повинен сповіщати співробітників служби безпеки, насамперед охоронців, органи позавідомчої охорони, поліцію, пожежну охорону про проникнення зловмисників на територію, що охороняється, про пожежу або інші стихійні лиха, захист від яких передбачений завданнями системи.

Для виявлення спроб подолання зловмисником бар'єрів та механічних перешкод, а також пожежі застосовуються **технічні засоби охорони** об'єктів **(ТЗО),** побудовані на різних фізичних принципах.

Сукупність ТЗО, призначених для вирішення **певної групи** задач виявлення джерел навмисних загроз, утворює підкомплекс ТЗО, що є варіантом підкомплексу виявлення джерел загроз (рис. 2.1). Структура типового підкомплексу ТЗО автономного комплексу охорони представлена на рис. 2.3.

Рисунок 2.3 – Структура підкомплексу ТЗО

Сповіщувач (датчик) охоронний (охоронно-пожежний, пожежний) є технічним пристроєм, що формує електричний сигнал тривоги при впливі на нього механічних сил і полів від зловмисника та пожежі. Так як виявити зловмисника і пожежу можна за їх демаскуючою ознакою, то сповіщувач призначений для виявлення цих демаскуючих ознаках і формування у разі їх виявлення сигналу тривоги, що сповіщає про загрози або управляє в автоматичному режимі засобами нейтралізації загроз. Так як створити ефективні універсальні датчики або сповіщувачі не можна, то розроблено велику кількість типів сповіщувачів, що реагують на окремі ознаки зловмисника та пожежі або їх комбінації. За призначенням сповіщувачі поділяються на сповіщувачі для блокування окремих об'єктів охорони, закритих приміщень, відкритих просторів, периметрів та виявлення пожежі. Залежно від зони виявлення сповіщувачі поділяються на **точкові, лінійні, поверхневі** та **об'ємні.** За видом ознак і способів їх виявлення сповіщувачі поділяються на **контактні, акустичні, оптико-електронні, радіохвильові, вібраційні, ємнісні, теплові, вібраційні** та **комбіновані.** Чим вища чутливість сповіщувача, тим вища ймовірність виявлення зловмисника і пожежі, але водночас вища ймовірність помилкової тривоги, відповідної ймовірності спрацьовування сповіщувача від перешкод. Для зменшення ймовірності помилки сповіщувача ускладнюють еталонну ознакову структуру. В акустичних і радіохвильових сповіщувачах для селекції сигналів, відбитих від зловмисника, що рухається, використовується ефект Доплера. Сигнал тривоги у сповіщувачі формується лише при

перевищенні відхилення частоти відбитого сигналу від частоти випромінюваного сигналу на величину не менш заданої, відповідної частоті сигналу від зловмисника, що рухається. В оптичному діапазоні відхилення довжин хвиль випромінюваного і відбитого світла настільки малі, що виміряти їх достатньо просто не вдається. Тому для селекції сигналів від зловмисника від перешкод використовуються інші рішення. Наприклад, приймачі пасивних оптико-електронних сповіщувачів мають широку діаграму напрямленості. Сигнал тривоги виникає, якщо інфрачервоне випромінювання від зловмисника послідовно приймається з різних напрямків (променів діаграми спрямованості), що можливо, якщо зловмисник рухається перпендикулярно до напрямку променів.

Для зниження помилок підвищують кількість використовуваних прийняття рішень ознак, вводячи їх у пам'ять мікропроцес сміття. Наприклад, для виявлення розбиття скла вікна або вітрини в якості еталона використовуються спектральні та динамічні характеристики сигналів, що виникають при його руйнуванні. Ознаки акустичних перешкод, у тому числі утворюються при ударі по склу без його руйнування, відрізняються від еталонних ознак. В результаті цього вдається з більшою ймовірністю розпізнати акустичні сигнали при розбитті скла на тлі численних акустичних перешкод.

Значне зменшення помилок виявлення досягається в комбінованих сповіщувачах за рахунок прийняття рішення в ньому про вторгнення зловмисника за даними різних датчиків, наприклад, оптичних та радіохвильових.

Шлейф сигналізації (охоронний, пожежний, пожежноохоронний) утворює електричний ланцюг, що забезпечують електричний зв'язок сповіщувачів та приймально-контрольного приладу. З метою економії з'єднувальних проводів сповіщувачі групуються, а шлейфи з'єднують групу сповіщувачів із приймально-контрольним приладом. Наприклад, охоронні та пожежні сповіщувачі, встановлені в одному приміщенні, передають у разі спрацьовування сигнали тривоги по одному шлейфу. Сповіщувачі, підключені до одного шлейфу, повинні мати однотипні вихідні ланцюги — з нормально

замкнутими або нормально розімкненими контактами. Еквівалентна схема шлейфу, що з'єднує сповіщувачі з нормально замкнутими контактами, наведено на рис. 2.4.

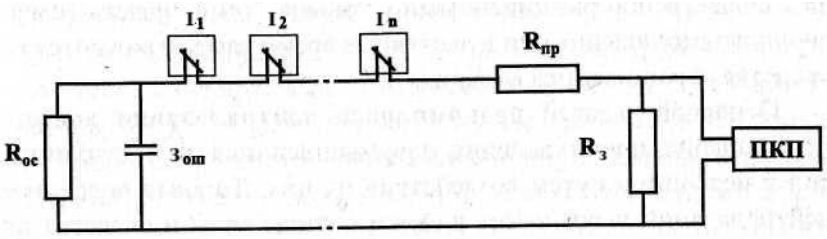


Рисунок 2.4 – Еквівалентна схема шлейфу

Позначення: I_n – n-й сповіщувач; ПКП - приймально-контрольний прилад; $R_{\text{пр}}$ – опір проводів шлейфу; $R_{\text{з}}$ – опір ізоляції проводів шлейфу; $R_{\text{ос}}$ – узгоджуючий опір; $З_{\text{ош}}$– електрична ємність шлейфу

Чим більше використовується шлейфів, тим точніше локалізовані місця встановлення сповіщувачів і тим точніше визначають сили тралізації загроз місце вторгнення їх джерел. Але при цьому зростають витрати на встановлення ТЗО. Крім того, доцільно мати різні шлейфи охоронної та пожежної сигналізації. В цьому випадку можна забезпечити цілодобову пожежну охорону, а засоби охоронної сигналізації у робочий час відключати.

Приймально-контрольні прилади (ПКП) призначені для прийому та обробки сигналів, що надходять від сповіщувачів, сповіщення звуковим та світловим сигналом співробітників охорони про надходження сигналів тривоги, порушення роботи сповіщувачів та шлейфів.

Усе ширше застосовувані телевізійні засоби спостереження становлять основу **підкомплексу спостереження (підкомплексу охоронного телебачення).** У нього входять також засоби чергового освітлення, що забезпечують необхідний рівень освітленості території, що охороняється в нічний час. Підкомплекс спостереження забезпечує можливість візуального дистанційного контролю за територією, що охороняється, і діями зловмисників і, що важливо для подальшого криміналістичного розслідування, за запис

зображень надзвичайних подій. Крім того, можливості сучасних засобів спостереження дозволяють автоматично виявляти проникнення зловмисника в контрольовані зони і вирішувати завдання охорони, конкуруючи в деяких випадках із засобами підкомплексу виявлення. У зв'язку з істотно розширеними можливостями засобів телевізійного спостереження вони в даний час розглядаються як засоби охоронного телебачення.

Основним завданням **підкомплексу нейтралізації** є припинення проникнення зловмисника чи стихійних сил джерела шляхом на них. Типова підсистема нейтралізації загроз має у своєму складі сили та засоби для фізичного та психологічного впливу на зловмисників, які проникли на територію, що охороняється, а також засоби гасіння пожежі. Оскільки комплекс охорони стає непрацездатним при виключенні електроживлення, то одними з основних засобів підкомплексу нейтралізації є засоби аварійного та резервного електроживлення, джерела якого автоматично підключаються замість основного мережевого. Нейтралізація загроз є необхідною функцією будь-якого комплексу охорони, оскільки за її відсутності неможливо в принципі забезпечити безпеку джерел інформації, як і будь-яких інших об'єктів захисту. Можливості нейтралізації погроз визначають час реакції підсистеми фізичного захисту інформації.

Основною силою підкомплексу нейтралізації є людина – охоронець. Він може перебувати в штаті підрозділу охорони організації або бути співробітником державної або приватної охоронної структури. Найменший час реакції сил нейтралізації загроз забезпечується, коли організація сама себе охороняє. У цьому випадку чергова зміна або сили швидкого реагування розміщуються на території організації, недалеко від місць проникнення. Крім того, під час періодичного обходу території охоронці можуть помітити вторгнення або початок пожежі до спрацювання технічних засобів та оперативно розібратися в обстановці. У деяких організаціях у нічний час для охорони залучаються також сторожові собаки, що перевершують за чутливістю та надійністю кращі зразки засобів охорони.

Але експлуатація **комплеску автономної охорони** потребує великих витрат. Справді, для забезпечення цілодобової охорони мінімальний штат співробітників підрозділу охорони становить 7 осіб: по 2 особи у кожній із 3 змін плюс одна людина для заміни хворих та відпускників. Заробітна плата охоронців протягом кількох років може перевищити разові витрати на технічні засоби охорони. Бюджет далеко не багатьох, навіть досить великих комерційних структур може ви тримати таке фінансове навантаження. Тому дедалі ширше застосовуються комплекси **централізованої охорони,** у яких сили нейтралізації зловмисників є спільними для кількох організацій. Структурну схему комплексу централізованої охорони показано на рис. 2.5.

Рисунок 2.5 – Комплекс централізованої охорони

Позначення: Р - ретранслятор; ПЦН – пульт централізованого спостереження

Прикладом охорони централізованого комплексу є охорона відділень філій ощадного банку, дрібних фірм, приватних будинків, дач, квартир. Деякі територіально розташовані фірми, наприклад, в одній будівлі, можуть мати загальний підрозділ охорони. Ефективну централізовану охорону забезпечують підрозділи позавідомчої охорони МВС.

У комплексах централізованої охорони сповіщення (сигнали перевірки працездатності комплексів охоронно-пожежної сигналізації та тривоги від них) передаються після взяття об'єкта під охорону по провідних або радіоканалах на

пульт централізованого спостереження пункту централізованої охорони, який інформує оператора світловими та звуковими сигналами та тривозі. Як провідні лінії зв'язку для передання сповіщень у більшості випадках використовуються лінії телефонів, встановлених на об'єкті охорони. У найпростіших випадках на час охорони телефонні лінії підключаються до засобів охорони. Для забезпечення спільного телефонного зв'язку та передачі повідомлень на кінцях телефонної лінії встановлюється апаратура ущільнення, наприклад частотного, яка забезпечує передачу повідомлень без перешкод телефонного зв'язку. За відсутності телефонного зв'язку повідомлення передаються по радіоканалу за допомогою передатчика в УКХ діапазоні на об'єкті охорони та приймача на пункті централізованої охорони.

Після надходження сигналу тривоги за командою оператора на об'єкт охорони виїжджає озброєна група співробітників. Незважаючи на досить жорсткі вимоги за часом (5-7 хвилин) прибуття групи охорони час реакції системи централізованої охорони більше, ніж автономної, особливо якщо об'єкт, що охороняється, знаходиться далеко від місця знаходження машини мобільної групи охорони. Крім того, цей час може бути в ряді випадків неприпустимо збільшено внаслідок порушення радіозв'язку, «пробок» і ремонту на дорогах або шляхом, наприклад, випадкової або створеної дорожньо-транспортної пригоди з машиною охорони, яка прямувала до об'єкта. Але централізовані комплекси мають великі можливості щодо нейтралізації загроз, особливо у вигляді збройного нападу.

Нейтралізація дій зловмисників та пожежі в комплексах охорони здійснюється співробітниками служби безпеки та засобами, що функціонально об'єднуються в підкомплекс нейтралізації загроз. Він може містити:

- підрозділ охорони автономного чи централізованого комплексу;
- тривожну звукову та світлову сигналізацію;
- штатного чи позаштатного пожежника;
- засоби пожежогасіння;
- джерела резервного (аварійного) електроживлення.

Підрозділ охорони, що включає в найбільших і найбагатших організаціях групу швидкого реагування, становить основу підкомплексу нейтралізації загроз. В автономному комплексі охорони підрозділ охорони є елементом структури організації, у централізованій використовується підрозділ охорони, загальний для кількох організацій, або підрозділ позавідомчої охорони.

Тривожна сигналізація призначена для психологічного впливу на потайно проникаючого в зони організації порушника з метою змусити його відмовитися від наміру.

Донедавна для ліквідації пожежі в будь-якій організації в легко доступних місцях розміщувалися традиційні **засоби пожежогасіння:** піноутворювальні вогнегасники, механічні засоби (багри, сокири) для руйнування вогнища пожежі, бочка з піском, пожежні рукави та ін.

Наприкінці у XX ст. відбулися серйозні, якісні зміни у засобах пожежогасіння, для яких характерні:

• витіснення трудомістких в експлуатації та ненадійних кислотних пінних вогнегасників більш надійними та довговічними;

• автоматизація процесів пожежогасіння.

Для гасіння пального середовища різних класів застосовують речовини, які включають у себе: воду, піну, газ, порошок, аерозолі та їх комбінації. Однак не всі вказані вогнегасні речовини придатні для ефективного гасіння різних горючих речовин. Деякі поєднання пального та вогнегасних речовин не тільки малоефективні, а й можуть погіршити ситуацію. Наприклад, при гасінні пожежі водою, спричиненої коротким замиканням електричних проводів, можуть виникнути нові осередки загоряння.

Джерела **резервного (аварійного) електроживлення** забезпечують працездатність основного елемента системи захисту інформації при виключенні основного джерела електроживлення.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали

магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Склад системи технічного захисту інформації.
2. Основні функції комплексів підсистеми фізичного захисту джерел інформації.
3. Що належить до комплексу технічної охорони джерел інформації?
4. Типи технічних засобів підсистеми фізичного захисту джерел інформації.
5. Призначення та склад засобів системи контролю та управління доступом.
6. Типи ідентифікаторів. Переваги та недоліки біометричних ідентифікаторів у порівнянні з атрибутними.
7. Типи технічних засобів охорони.
8. Кошти, що застосовуються для нейтралізації загроз.
9. Склад комплексу централізованої охорони.

3 КЛАСИФІКАЦІЯ МЕТОДІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Класифікація методів технічного захисту інформації

Як випливає з факторів, що впливають на ефективність технічного захисту інформації, її методи повинні забезпечити реалізацію наступних напрямів технічного захисту інформації:

• запобігання та нейтралізацію навмисних та випадкових впливів на джерело інформації;

• приховування інформації та її носіїв від органу розвідки (зловмисника) на всіх етапах добування інформації.

Крім того, враховуючи, що для добування інформації зловмисник може використовувати різні спеціальні засоби (заставні пристрої, диктофони та ін.), третій напрямок включає методи виявлення, локалізації та знищення цих засобів, а також придушення їх сигналів.

Перший напрямок об'єднують методи, при реалізації яких:

• утруднюється рух зловмисника чи розповсюдження стихійних сил до джерела інформації;

• виявляється вторгнення зловмисника чи стихійних сил у контрольовану зону та його нейтралізація.

Класифікація напрямів та методів технічного захисту інформації наведена на рис. 3.1.

Утруднення руху джерел загроз впливу до джерел інформації забезпечується в рамках напрямку, що називається фізичним **захистом.** Фізичний захист забезпечується методами інженерного захисту та технічної охорони. Інженерний захист створюється за рахунок використання **природних** і **художніх перешкод** на маршрутах можливого поширення джерел загроз впливу. Штучні перешкоди створюються за допомогою різних інженерних конструкцій, основними з яких є паркани, ворота, двері, стіни, міжповерхові перекриття, вікна, шафи, ящики столів, сейфи, сховища. Оскільки будь-які природні та штучні перепони можуть бути подолані, то для забезпечення надійного захисту

інформації, як і інших матеріальних цінностей, необхідні методи виявлення вторгнень у контрольовані зони та їх нейтралізації.

Рисунок 3.1 – Класифікація напрямів і методів інженерно-технічного захисту інформації

Ці методи називаються **технічною охороною об'єктів захисту.** Під об'єктами захисту розуміються як люди і матеріальні цінності, так і носії інформації, локалізовані в просторі. До таких носіїв відносяться папір, машинні носії, фото і кіно плівка, продукція, матеріали тощо, тобто все, що має чіткі розміри та вагу. Носії інформації у вигляді електромагнітних та акустичних полів, електричного струму не мають чітких меж і для захисту інформації на цих носіях методи інженерного захисту не прийнятні — електромагнітне поле з інформацією не можна зберігати, наприклад, у сейфі. Для захисту інформації на таких носіях застосовують методи приховання інформації.

Приховування інформації (хования, приховування) поєднує групу методів захисту інформації, основу яких становлять умови та дії, що ускладнюють пошук та виявлення об'єктів захисту, розпізнавання та вимірювання їх ознак, зняття з носіїв інформації з якістю, достатнім для її використання. Воно

передбачає такі зміни місцезнаходження, часу передачі повідомлення або прояви демаскуючих ознак, структури інформації, структури та енергії носіїв, за яких зловмисник не може безпосередньо або за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах. Приховувати від зловмисника можна як інформацію, так і її носій. Розрізняють просторове, тимчасове, структурне та енергетичне приховування.

Просторове приховування ускладнює пошук та виявлення зловмисником джерела інформації у просторі. Воно досягається розміщенням джерела інформації в місцях, розташування яких апріорі зловмиснику не відоме. Такі місця зберігання називаються **тайниками.** Перед зловмисником постає додаткове завдання – пошук джерела. Чим більша область пошуку, тим важче знайти об'єкт. Підводні човни становлять велику загрозу, перш за все, тому, що забезпечується їхня висока просторова скритність. При створенні схованок їх автори часто не враховують шаблонність мислення більшості людей. Цим користуються квартирні злодії, які легко знаходять місця, де господарі зберігають свої цінності.

До просторових можна віднести стеганографічні способи захисту інформації, які передбачають потайливе розміщення інформації, що захищається, що відображається в символьній формі, в так званих контейнерах. Контейнери – вільні частини носія, що містить іншу інформацію.

Найбільш древнім стеганографічним способом приховування інформації є написання повідомлення симпатичними (безбарвними без спеціальної теплової або хімічної обробки) чорнилами між рядками листа або іншого документа. Відомо багато способів запису даних, що реалізують просторове приховування інформації: запис наколом літер на зворотному боці етикеток флаконів, банок або пляшок, на внутрішній стороні сірникової коробки, всередині яйця та ін. У роки розквіту фототехніки для потайної передачі повідомлень використовувалася «мікроточка», винайдена німецьким ученим Е. Голдбергом. «Мікроточка» являла собою мікрозображення розвідувального повідомлення розміром 0,01-1мм^2 , яке наклеювалося як точка тексту листа, листівки, під

марку та інші місця невинної кореспонденції або предметів. Величина зменшених символів у «мікроточці» досягала 1 мікрона. Великі можливості щодо реалізації стеганографічних способів приховування інформації надають комп'ютерні технології запису інформації. Комп'ютерна стеганографія ґрунтується на тому, що файли, що містять оцифроване зображення або звук, можуть бути певною мірою видозмінені без втрати якості зображення або звуку. Така можливість обумовлена нездатністю органів чуття людини розрізняти незначні зміни в кольорі зображення або в частотах звуку. Тому як контейнери використовуються графічні та звукові файли, що містять оцифроване зображення та звук. Молодші (1-4) розряди використовуваних багаторозрядних кодів можуть бути змінені без погіршення якості зображення або звуку, в них можна записати секретну та конфіденційну інформацію та забезпечити її ефективне приховування. Наприклад, якість еталонного зображення у форматі bmp об'ємом 243 Кбайт непомітно відрізняється від того самого зображення у файлі якого вміщена інша інформація об'ємом 119 Кбайт.

Відсутність у зловмисника даних про час передачі спілкування з інформацією, що цікавить, або часу прояву демаскуючих ознак об'єкта захисту змушує зловмисника витрачати великі ресурси на забезпечення безперервності розвідки. Цим досягається **тимчасове приховування.** Десятки тисяч операторів і технічних засобів Агентства національної безпеки США постійно і безперервно «слухають» ефір у різних точках простору в різних частотних діапазонах, щоб не пропустити і перехопити інформативне повідомлення в каналах зв'язку свого ймовірного супротивника. Чим коротше за часом повідомлення, тим складніше його виявити. Тому одним із методів тимчасового приховання є передача з великою швидкістю повідомлення, накопиченого за час, що значно перевищує час його передачі.

З іншого боку, якщо відомий час можливої роботи засобів добування, то значно легше приховати інформацію. Хоча розвідка ведеться потайливо, але поява тих чи інших носіїв засобів розвідки (літаків, кораблів, космічних апаратів, автомобілів з дипломатичними номерами) біля контрольованої зони в більшості

випадків виявляється засобами відповідних служб, що дозволяє вжити заходів щодо приховання інформації. Наприклад, «ахіллесовою п'ятою» найефективнішою у мирний час космічної розвідки є завчасне знання контррозвідкою точного часу прольоту низькоорбітального розвідувального космічного апарату. Службі безпеки часом достатньо для забезпечення ефективного захисту на короткий час (хвилини) прольоту припиняти інформативні випромінювання і зачохляти об'єкти, що захищаються, що спостерігаються зверху.

Структурне приховування досягається зміною або створенням помилкового інформаційного портрета семантичного повідомлення, фізичного об'єкта або сигналу.

Інформаційним портретом можна назвати сукупність елементів та зв'язків між ними, що відображають зміст повідомлення (мовного або даних), ознаки об'єкта чи сигналу. Елементами дискретного семантичного повідомлення, наприклад, є букви, цифри або інші знаки, а зв'язки між ними визначають їх послідовність. Інформаційними портретами об'єктів спостереження, сигналів і речовин є їх еталонні ознакові структури.

Можливі такі способи зміни інформаційного портрета:

- видалення частини елементів та зв'язків, що утворюють інформаційний вузол (найбільш інформативну частину) портрета;
- зміна частини елементів інформаційного портрета при зберіганні незмінності зв'язків між елементами, що залишилися;
- видалення чи зміна зв'язків між елементами інформаційного портрета за збереження їх кількості.

Зміна інформаційного портрета об'єкта викликає зміну зображення його зовнішнього вигляду (видових ознак, що демаскують), характеристик випромінюваних ним полів або електричних сигналів (ознак сигналів), структури та властивостей речовин. Ці зміни спрямовані на зближення ознакових структур об'єкта та навколишнього його фону, внаслідок чого

знижується контрастність зображення об'єкта по відношенню до фону та погіршуються можливості його виявлення та розпізнавання.

Але за зміни інформаційного портрета інформація сприймається як зловмисником, а й її санкціонованим одержувачем. Отже, для санкціонованого одержувача інформаційний портрет повинен бути відновлений шляхом додаткової передачі віддалених елементів і зв'язків або алгоритму (ключа) цих змін.

В умовах ринку, коли виробник змушений рекламувати свій товар, найбільш доцільним способом інформаційного приховування є виключення з реклами або відкритих публікацій найбільш інформативних відомостей або ознак — інформаційних вузлів, що містять таємницю, що охороняється.

До **інформаційних** вузлів відносяться принципово нові технічні, технологічні та образотворчі рішення та інші досягнення, які становлять ноу-хау. Вилучення з технічної документації інформаційних вузлів не дозволить конкуренту скористатися інформацією, що міститься в рекламі або публікаціях.

Цей метод, що широко застосовується, дозволяє:

• істотно зменшити обсяг інформації, що захищається, і тим самим спростити проблему захисту інформації;

• використовувати у рекламі нової продукції інформацію про неї, не побоюючись розголошення.

Наприклад, замість захисту інформації, що міститься в сотнях і тисячах аркушів технічної документації, що розробляється для виробництва нової продукції, захисту підлягають всього кілька десятків аркушів з інформаційними вузлами.

Структурне приховування, в результаті якого інформаційний портрет змінюється під інформаційний портрет фону, називається маскуванням **.** Методи маскування відрізняються для різних видів повідомлення. Маскування семантичної інформації, що подається у вигляді набору певним чином пов'язаних символів, забезпечується криптографічними методами і називається **шифруванням.** Фоном для повідомлення, що маскується, є випадковий набір

символів. Тому що менше зашифроване повідомлення відрізняється менше від випадкового, воно представляє вищий рівень приховування інформації.

Маскування ознакової інформації досягається зміною інформаційних ознак об'єкта захисту під ознаки об'єктів фону. Залежно від виду ознакової інформації маскуються ознаки об'єктів спостереження, сигналів або речовин, що демаскують. Фон при спостереженні утворює інші об'єкти, зокрема предмети місцевості. Фоном для сигналів є інші сигнали – перешкоди. Але перешкоди на відміну від об'єктів фону при спостереженні можуть змінювати параметри сигналів, що несуть інформацію, що захищена. Якщо енергія перешкод вища за енергію сигналів, то ці зміни настільки значні, що структура сигналів наближається до структури перешкод. Отже, перешкоди маскують сигнал. Так як ступінь впливу перешкод і відповідно маскувальний ефект залежать від відношення потужності сигналу і перешкод, то метод маскування сигналу перешкодами можна назвати енергетичним прихованням інформаційних сигналів.

Енергетичне приховування досягається зменшенням відношення енергії (потужності) сигналів, тобто носіїв (електромагнітного або акустичного полів та електричного струму) з інформацією, і перешкод. Зменшення відношення сигнал/перешкода (слово «потужність», як правило, опускається) можливе двома методами: зниженням потужності сигналу або збільшенням потужності перешкоди на вході приймача.

Дія перешкод призводить до зміни інформаційних параметрів носіїв: амплітуди, частоти, фази. Якщо носієм інформації є амплітудно-модульована електромагнітна хвиля, а в середовищі поширення каналу присутня перешкода у вигляді електромагнітної хвилі, що має однакову з носієм частоту, але випадкову амплітуду і фазу, то відбувається інтерференція цих хвиль. В результаті цього значення інформаційного параметра (амплітуди сумарного сигналу) випадково змінюються і інформація спотворюється. Чим менше відношення потужностей, а отже, амплітуд, сигналу та перешкоди, тим значніше

значення амплітуди сумарного сигналу відрізнятимуться від вихідних (встановлюваних при модуляції) і тим більше спотворюватиметься інформація.

Природні та промислові перешкоди, які постійно присутні у середовищі поширення носія інформації, мають найбільший вплив на амплітуду сигналу, у меншому ступені — на його частоту. Але ЧС-сигнали мають ширший спектр частот. Тому у функціональних каналах, що допускають передачу більш широкосмугових сигналів, наприклад, в УКХ-діапазоні, передачу інформації здійснюють, як правило, ЧС-сигналами як більш завадостійкими, а у вузькосмугових ДВ-, СВ- і КВ-діапазонах – АМ-сигналами .

У загальному випадку якість інформації, що приймається, погіршується зі зменшенням відношення сигнал/перешкода. Характер залежності якості інформації від відношення сигнал/ перешкода відрізняється для різних видів інформації (аналогової, дискретної), носіїв і перешкод, способів запису на носій (виду модуляції), параметрів засобів прийому та обробки сигналів.

Найбільш жорсткі вимоги до якості інформації пред'являються при передачі даних (міжмашинний обмін): ймовірність помилки знака за плановими завданнями, завданнями статистичного та бухгалтерського обліку оцінюється порядку 10^{-5}-10^{-6}, за грошовими даними – 10^{-8}-10^{-9}. Для порівняння, в телефонних каналах гарна складова розбірливість мови забезпечується при 60-80%, тобто вимоги до якості інформації, що приймається, істотно менш жорсткі. Ця різниця обумовлена надмірністю мови, яка дозволяє при пропуску окремих звуків і навіть складів відновлювати мовленнєве повідомлення. Можливість помилки знака 10^{-5} досягається при його передачі двійковим АМ сигналом і відношенні потужності сигналу до потужності флуктуаційного шуму на вході приймача приблизно 20, при передачі ЧС сигналом – близько 10. Для забезпечення розбірливості мови порядку 85% перевищення амплітуди сигналу над шумом має становити близько 1 отримання задовільної якості факсимільного зображення — приблизно 35 дБ, якісного телевізійного зображення — понад 40 дБ.

У загальному випадку при зменшенні відношення сигнал/перешкода до одиниці і менш якість інформації настільки погіршується, що вона не може

практично використовуватися. Для конкретних видів інформації та модуляції сигналу існують граничні значення відношення сигнал/перешкода, нижче за які забезпечується енергетичне приховування інформації.

Оскільки розвідувальний приймач у принципі може бути наближений до кордонів контрольованої зони організації, то значення відношення сигнал/перешкода вимірюються, перш за все, на межі цієї зони. Забезпечення на межі зони значень відношення сигнал/перешкода нижче мінімально допустимої величини гарантує безпеку інформації, що захищається від витоку за межами контрольованої зони.

Маскування ознак речовин забезпечується перетворенням ознак речовин під ознаки інших речовин, що не цікавлять зловмисника. Наприклад, для контрабанди наркотиків іноді їх перетворять на іншу хімічну речовину, яка пропускається митною службою і відновлюється після проведення до початкового складу.

Інший метод структурного приховання полягає в трансформації вихідного інформаційного портрета в новий, що відповідає помилковій семантичній інформації або помилковій ознаковій структурі, і «нав'язуванні» нового портрета органу розвідки (зловмиснику). Такий метод захисту називається **дезінформуванням.** Дезінформування найефективніше при приховуванні семантичної інформації, коли у здобутому повідомленні міститься хибна інформація. При приховуванні ознакової інформації межа між маскуванням та дезінформуванням розмита. Принципова відмінність між ними полягає в тому, що маскування спрямоване на утруднення виявлення об'єкта захисту серед інших об'єктів фону, а дезінформування – створення помилкового об'єкта прикриття. При пошуку орган розвідки (зловмисник) не знаходить замаскований об'єкт, при дезінформуванні він виявляє інший об'єкт замість істинного, ознаки якого неможливо змінити під ознаки фону. Наприклад, якщо в глухому місці без будов розміщується шахта стратегічної ракети, то неможливо приховати під'їзні шляхи автотранспорту до неї. У цьому випадку структурне приховування

інформації про місце знаходження ракетної установки забезпечується не тільки маскуванням її конструкції, а й імітацією функціонування цього об'єкта.

Дезінформування належить до найбільш ефективних методів захисту інформації з наступних причин:

• створює у власника інформації, що захищається, запас часу, обумовлений перевіркою розвідкою достовірності отриманої інформації;

• наслідки прийнятих конкурентом на основі хибної інформації рішень можуть бути для нього гіршими в порівнянні з рішеннями, що приймаються за відсутності інформації, що добувається.

Остання причина обумовлена тим, що при недостатності інформації збільшується в просторі можливих рішень область прийняття рішень, усередині якої знаходиться оптимальне рішення. Прийняті рішення за недостатності інформації відрізнятимуться від оптимального. При використанні дезінформації може утворитися інша сфера прийняття рішень на значній відстані від оптимального рішення. У цьому випадку можуть виникнути для користувача помилковою інформацією катастрофічні наслідки.

Дезінформування здійснюється шляхом припасування ознак інформаційного портрета об'єкта, що захищається, під ознаки інформаційного портрета помилкового об'єкта, що відповідає заздалегідь розробленій версії, — **об'єкта прикриття.** Від ретельності підготовки версії та бездоганності її реалізації багато в чому залежить правдоподібність дезінформації. Версія має передбачати комплекс розподілених у часі та у просторі заходів, спрямованих на імітацію ознак помилкового об'єкта. Причому чим менше при дезінформації використовується хибних відомостей та ознак, тим важче розкрити її хибний характер.

Розрізняють такі способи дезінформування:

• заміна реквізитів інформаційних портретів, що захищаються в тому випадку, коли інформаційний портрет об'єкта захисту схожий на інформаційні портрети інших «відкритих» об'єктів і не має специфічних інформативних ознак. У цьому випадку обмежуються розробкою і підтримкою

версії про інший об'єкт, видаючи в якості його ознак ознаки об'єкта, що захищається. Наприклад, в даний час велика увага приділяється розробкам продукції подвійного застосування: військового та цивільного. Поширення інформації про виробництво продукції суто цивільного використання є надійним прикриттям для варіантів військового призначення;

• підтримка версії з ознаками, запозиченими з різних інформаційних портретів реальних об'єктів. Застосовується у випадках, як у організації одночасно виконується кілька закритих тем. Шляхом різних поєднань ознак, що належать до різних тем, можна нав'язати протилежній стороні хибне уявлення про роботи, що ведуться, без імітації додаткових ознак;

• поєднання істинних і хибних ознак, причому хибними замінюється незначна, але найцінніша частина інформації, що відноситься до об'єкта, що захищається;

• зміна лише інформаційних вузлів із збереженням незмінної решти інформаційного портрета.

Як правило, використовуються різні комбінації цих варіантів.

Однак, цей метод захисту практично складно реалізувати. Основна проблема полягає у забезпеченні достовірності хибного інформаційного портрета. Дезінформування тільки в тому випадку досягне мети, коли у розвідки (зловмисника) не виникнуть сумніви в істинності хибної інформації, що підсовується йому. В іншому випадку може бути отриманий протилежний ефект, так як при розкритті розвідкою факту дезінформування отримана помилкова інформація може звузити область пошуку істинної інформації. Враховуючи, що споживачі інформації чітко представляють збитки від дезінформації і за найменших сумнівів перевірятимуть ще раз інформацію з використанням інших джерел, дезінформування в більшості випадків потребує хорошої організації та значних витрат.

Основу третього напряму технічного захисту інформації становлять методи пошуку, виявлення та тралізації джерел небезпечних сигналів. Так як ці джерела виявляються за їх демаскуючими ознаками, то ці методи містять

процедури ідентифікації джерел випадкових небезпечних сигналів за їх ознаками, що демаскують.

Знання конкретних загроз інформації, що захищається, створює можливість постановки завдань щодо **визначення раціональних заходів захисту інформації,** що запобігають загрозам або знижують до допустимих значень ймовірність їх реалізації. Заходи захисту інформації з позиції системного підходу розглядаються як результати функціонування системи захисту. Вони можуть являти собою конкретні дії персоналу, пропозиції щодо придбання та встановлення технічних та програмних засобів, вимоги до співробітників, визначені у відповідних правових документах, і т.д. У принципі для запобігання або, принаймні, суттєвого зниження рівня конкретної загрози безпеці інформації можна запропонувати кілька заходів щодо її захисту. Однак їх ефективність може істотно відрізнятися. Вибір будь-якого заходу захисту інформації, як і в будь-якій сфері, проводиться за показниками оцінки ефективності, які враховують ступінь виконання завдання та витрати ресурсу на її вирішення. Різноманітність загроз безпеки інформації породжує різноманітність заходів її захисту. Ефективність кожного заходу захисту інформації оцінюється своїми **локальними (приватними) показниками ефективності.** Їх можна поділити на **функціональні (оперативні)** та **економічні.** Функціональні показники характеризують рівень безпеки інформації, економічні — витрати на її забезпечення. Оскільки рівень безпеки інформації визначається величиною потенційної шкоди від реалізації загроз, то як локальні функціональні показники ефективності захисту інформації використовуються як показники кількості та якості інформації, яка може потрапити до зловмисника, так і характеристики реально виникаючих загроз безпеки інформації.

Ефективність системи захисту в цілому визначається глобальними функціональним та економічним критеріями чи показниками. Як функціональний глобальний критерій часто використовується «зважена» сума функціональних локальних показників. Якщо позначити через w_i значення і-го

локального показника, то глобальний показник визначається як $W_r = \sum a_i w_i$, причому $\sum a_i = 1$. Коефіцієнт a_i характеризує «вагу» локального показника. Фізичного сенсу такий показник не має. Глобальний економічний показник є мірою сумарних витрат за інформацію.

Ефективність тим вища, чим нижчі витрати при однаковому рівні безпеки інформації, або чим більший рівень безпеки інформації при однакових витратах. Перший підхід до оцінки ефективності використовується в умовах відсутності жорстких обмежень на ресурс, який виділяється для захисту інформації, тоді як другий враховує даний ресурс.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Основні напрямки технічного захисту інформації.
2. Методи технічного захисту інформації.
3. Чим відрізняється інженерний захист об'єктів від їхньої технічної охорони?
4. Умова ефективного забезпечення тимчасового приховування об'єктів

захисту.

5. Що являє собою інформаційна модель об'єкта захисту?
6. Наведіть приклади інформаційних портретів спостереження.
7. Чим маскування відрізняється від дезінформування?
8. Перелічити способи дезінформування.
9. Умови ефективного енергетичного приховування.

4 ПРОЕКТУВАННЯ КОМПЛЕКСУ ТЗІ

Алгоритм проектування (удосконалення) системи захисту інформації. Основні етапи проектування системи захисту інформації технічними засобами

Завдання проектування (розробки, вдосконалення) системи захисту інформації та її елементів виникає тоді, коли створюється нова організація із закритою (секретною, конфіденційною) інформацією або чинна система не забезпечує необхідний рівень безпеки інформації.

Проектування системи захисту, що забезпечує досягнення поставлених перед технічним захистом інформації цілей і розв'язання задач, проводиться шляхом системного аналізу чинної та розробки варіантів необхідної. Побудова нової системи або її модернізація передбачає:

- визначення джерел інформації та опис факторів, що впливають на її безпеку;
- виявлення та моделювання загроз безпеці інформації;
- визначення слабких місць чинної системи захисту інформації;
- вибір раціональних заходів запобігання загрозам;
- порівняння варіантів за приватними показниками та глобальним критерієм, вибір одного або кількох раціональних варіантів;
- обґрунтування обраних варіантів у доповідній записці або проекті для керівництва організації;
- доопрацювання варіантів або проекту з урахуванням зауважень керівництва.

Так як відсутні формальні способи синтезу системи захисту, то її оптимізація при проектуванні можлива шляхом поступового наближення до раціонального варіанту в результаті ітерацій.

Алгоритм проектування системи захисту інформації представлений на рис. 4.1.

Послідовність проектування (модернізації) системи захисту включає три основні етапи:

- моделювання об'єктів захисту;
- моделювання погроз інформації;
- вибір заходів захисту.

Основним методом дослідження систем захисту є моделювання. Моделювання передбачає створення моделі та її дослідження (аналіз). Опис або фізичний аналог будь-якого об'єкта, у тому числі системи захисту інформації та її елементів, що створюються для визначення та дослідження властивостей об'єкта, є його моделлю. У моделі враховуються суттєві для розв'язуваної задачі елементи, зв'язки та властивості досліджуваного об'єкта.

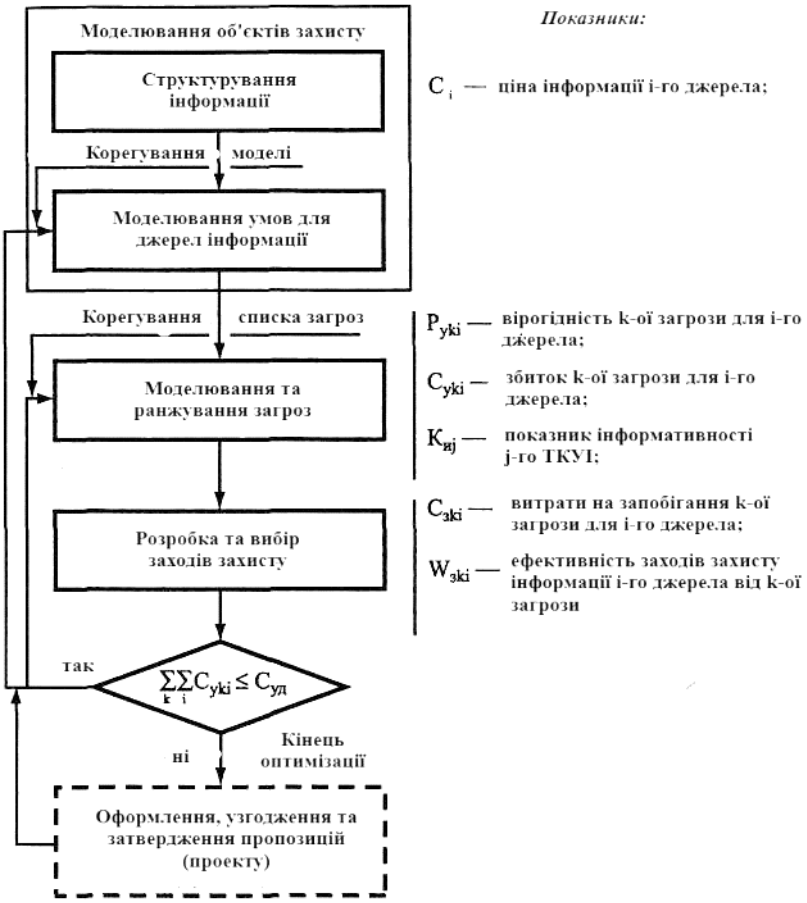


Рисунок 4.1 – Алгоритм проектування системи захисту інформації

Моделювання становить основу діяльності живих істот, у тому числі людини. В основі багатьох хвороб психіки людини лежать порушення механізму

моделювання навколишнього середовища. У крайніх її проявах у хворому мозку створюються моделі, що мають мало подібності із загальноприйнятими або об'єктивно існуючими моделями навколишнього світу. У цьому випадку вчинки хворої людини на основі спотвореної моделі не відповідають моделям інших людей, а поведінка такої людини класифікується як ненормальна. Поняття «норми» є досить умовним і суб'єктивним і може змінюватися у значних межах. Творчі люди здатні у своїй уяві створювати моделі, що відрізняються від реальності, і ці моді певною мірою впливають на їхню поведінку, яка іншим людям видається дивною. Образ такого дивака-вченого Паганеля намалював Жюль Верн у своєму романі «Діти капітана Гранта».

Оскільки основу життя людини складають хімічні та електричні процеси в його організмі, то моделі навколишнього середовища можуть спотворюватися під дією хімічних наркотичних речовин. Люди постійно користуються наркотиками, щоб підкоригувати свої моделі зовнішнього світу з метою зменшення рівня негативних емоцій, що виникають при інформаційній недостатності або невідповідності життєвих реалій завданням і цілям людини. Наркотичні речовини (алкоголь, тютюн, кофеїн, кола), що викликають слабкий наркотичний вплив на організм людини, узаконені. Інші – опіум, героїн, ЛСД тощо настільки згубні, що наркоманія розглядається людством як одна з найбільш страшних загроз його існуванню.

Розрізняють **вербальні, фізичні** та **математичні моделі** та відповідне **моделювання.**

Вербальна модель описує об'єкт національною та професійною мовами. Людина постійно створює вербальні моделі навколишнього середовища і керується ними при прийнятті рішень. Чим точніше модель відображає світ, тим вона ефективніша за інших рівних умов діяльність людини. На здібності різних людей до адекватного моделювання навколишнього світу впливають як природні (генетичні) дані, так і виховання, навчання, в тому числі на основі власного досвіду, фізичний і психічний стан людини, а також світоглядні моделі суспільства, в якому живе конкретна людина.

На природній чи професійній мові можна описати будь-який об'єкт чи явище. Складні моделі минулого, теперішнього чи майбутнього життя людей створюють письменники. Але вербальні моделі дозволяють аналізувати зв'язки між її елементами лише на якісному рівні.

Фізична модель представляє матеріальний аналог реального об'єкта, який можна піддавати в ході аналізу різним впливам і отримувати кількісні співвідношення між цими впливами та результатами. Часто як фізичні моделі досліджують зменшені копії великих об'єктів, для вивчення яких відсутній інструментарій. Моделі літаків і автомобілів продувають в аеродинамічних трубах, макети будинків для сейсмічних районів випробовують на вібростендах і т. д. Але можливості фізичного моделювання об'єктів захисту і загроз обмежені, оскільки важко і дорого створити фізичні аналоги реальних об'єктів. Справді, щоб отримати фізичну модель каналу витоку, необхідно відтворити його елементи, зокрема середовище, і навіть апріорі невідомі засоби та дії зловмисника.

У міру розвитку обчислювальної математики та техніки розширюється сфера застосування **математичного моделювання.** Математичне моделювання передбачає створення та дослідження математичних моделей реальних об'єктів і процесів. Математичні моделі можуть розроблятися у вигляді аналітичних залежностей виходів системи від входів, рівнянь для моделювання динамічних процесів у системі, статистичних характеристик реакцій системи на впливи випадкових факторів. Математичне моделювання дозволяє найбільш економно і глибоко досліджувати складні об'єкти, чого, в принципі, не можна досягти за допомогою вербального моделювання або що надмірно дорого при фізичному моделюванні. Можливості математичного моделювання обмежуються рівнем формалізації опису об'єкта і ступенем адекватності математичних виразів реальним процесам в модельованому об'єкті.

Подібні обмеження виникають при моделюванні складних систем, елементами яких є люди. Різноманітність поведінки конкретної людини поки що

не піддається опису мовою математичних символів. Однак у статистичному сенсі поведінка людини більш прогнозована та стійка.

Для моделювання складних систем дедалі ширше застосовується метод математичного моделювання, який називається **імітаційним моделюванням.** Воно передбачає визначення реакцій моделі системи на зовнішні дії, які генерує ЕОМ як випадкові числа. Статистичні характеристики (математичні очікування, дисперсія, вид і параметри розподілу) цих випадкових чисел повинні з прийнятною точністю відповідати характеристикам реальних впливів. Функціонування системи при випадкових зовнішніх впливах описується як алгоритм дій елементів системи та його характеристик у відповідь кожен вплив на вході. Таким чином імітується робота складної системи в реальних умовах. Шляхом статистичної обробки вихідних результатів при досить велику вибірку вхідних впливів виходять достовірні оцінки роботи системи. Наприклад, досить об'єктивна оцінка ефективності системи захисту інформації при різноманітті дій зловмисників, які з погляду служби безпеки мають випадковий характер, можлива, як правило, на основі імітаційного моделювання системи захисту.

Інший перспективний напрямок математичного моделювання, який представляє інтерес для моделювання об'єктів захисту та загроз інформації – **комп'ютерні ділові ігри.** Комп'ютерні ділові ігри – аналог ділових ігор людей, що застосовується для вирішення проблем в організаційних структурах. Ділова гра імітує процес прийняття рішення у складних умовах недостатності достовірної інформації людьми, які грають роль певних посадових осіб. Учасниками комп'ютерної гри є дві особи або комп'ютер та людина. Причому за співробітника служби виступає людина, а зловмисника — комп'ютер чи людина. Наприклад, зловмисник — комп'ютер встановлює у випадковому місці заставний пристрій, а інший гравець — людина здійснює пошук заставного пристрою за допомогою різних вибраних засобів за показаннями віртуальних приладів моделей цих засобів.

Комп'ютерні ігри захисту інформації можуть застосовуватися як для аналізу конкретних об'єктів, загроз і заходів захисту, так і як тренажерів для підготовки співробітників служби безпеки.

У чистому вигляді кожен вид моделювання використовується рідко. Як правило, застосовуються комбінації вербального, фізичного та математичного моделювання. З вербального моделювання починається сам процес моделювання, тому що не можна створити фізичні або математичні моделі, не маючи образного уявлення про об'єкт і його словесного опису. Якщо є можливість досліджувати властивості об'єкта на фізичній моделі, то найточніші результати забезпечуються при фізичному моделюванні. Таким чином перевіряють аеродинаміку літаків та автомобілів шляхом продування зменшених фізичних моделей літаків та автомобілів в аеродинамічних трубах. Коли створення фізичної моделі з тих чи інших причин неможливо або надмірно дорого, то проводять математичне моделювання, іноді доповнюючи його фізичним моделюванням окремих вузлів, деталей, тобто тих частин об'єкта, опис яких не піддається формалізації.

Оскільки створення і дослідження універсальних моделей (які дозволяють проводити всебічні дослідження) є дорогою і складною справою, то з метою спрощення моделей у них деталізуються тільки елементи та зв'язки між ними, які необхідні для вирішення конкретної поставленої задачі. Інші, менш суттєві для вирішення конкретного завдання елементи та зв'язки, укрупнюються або не враховуються зовсім. Через відмову від такого підходу економляться ресурси та досліджуються з допомогою диференційованих моделей окремі властивості об'єкта, які цікавлять дослідника.

Моделювання об'єктів захисту передбачає визначення джерел з інформацією, що захищається, і розробку моделей матеріальних об'єктів захисту. До об'єктів захисту відносяться джерела інформації, що захищається, і контрольовані зони, в яких знаходяться ці джерела.

В результаті цього етапу визначаються:

- моделі об'єктів захисту із зазначенням усіх джерел інформації з описом

факторів, що впливають на їхню безпеку;

• Ціна С та і-та інформація, що захищається для кожного окремого джерела і.

На основі отриманих результатів на етапі **моделювання** загроз виявляються загрози безпеці інформації, проводиться оцінка очікуваної від їх реалізації потенційної шкоди та ранжування загроз за потенційною шкодою. При моделюванні загроз визначаються ризик (імовірність) загрози P_y та збитки C_yу разі її реалізації. Знання шкоди дозволяє також визначити кількість загроз, нейтралізація яких забезпечить допустимий рівень безпеки інформації $C_{уд}$. Для цього достатньо зробити послідовно складання шкоди від загроз, починаючи з останньої у списку, і порівняти отриману суму з допустимим збитком. Риса під загрозами списку за умови приблизної рівності сумарної шкоди від не запобігання загроз допустимому для власника інформації значенню розділить список на 2 частини. Верхня, більша частина списку погроз включає загрози, які необхідно нейтралізувати для забезпечення допустимого рівня безпеки інформації, нижня — малоістотні загрози.

Послідовність ранжованих загроз визначає послідовність **вибору заходів захисту** на 3-му етапі. Цей етап починається з визначення заходів захисту з нейтралізації першої, найбільш небезпечної загрози, далі — другої загрози тощо. Тобто з декількох варіантів, що забезпечують приблизно рівну безпеку, вибирається варіант з меншими витратами. Як ефективність варіанта найчастіше використовується відношення величини зменшення шкоди при обраній мірі захисту витрат на реалізацію цього варіанта. З варіантів вибирається той, для якого це ставлення більше.

Для кожної обраної міри захисту розраховуються необхідні витрати на її життєвому циклі (від її реалізації до припинення). Якщо позначити витрати на нейтралізацію к-ї загрози інформації i-го джерела через C_{ykj}, то процедура вибору заходів захисту умовно завершується при виконанні умови $\sum_{k=1}\sum_{i=1} C_{yki} \geq C_{рз}$, де $C_{рз}$ – ресурс, що виділяється на захист інформації. Умовність означає, що після виконання цієї умови доцільно продовжити вибір з

метою визначення та оцінки витрат для заходів, використання яких перевищує виділений ресурс. Ці результати дозволять визначити загрози, що залишилися, і необхідні для їх нейтралізації додаткові витрати.

Такий підхід дозволяє ефективніше використовувати наявні ресурси для запобігання найбільш значущим загрозам, ніж розподіл ресурсів на всі можливі загрози. По-друге, знання конкретних непопереджених загроз дозволяє власнику інформації зробити вибір: збільшити виділені ресурси або прийняти ризик.

Вибором заходу захисту, що запобігає одній загрозі, завершується одна ітерація проектування системи захисту. Після її завершення відповідно до вказаного на рис. 4.1 зворотнього зв'язку коригуються моделі об'єктів захисту та загроз інформації. Коригування моделей об'єктів захисту полягає у внесенні до них вибраних заходів. Ці заходи віртуально змінюють захищеність інформації та, відповідно, характеристики її загроз. Крім того, при коригуванні список загроз скорочується зверху на одиницю.

Доцільність коригування обумовлена зв'язком між факторами, що впливають на безпеку інформації та загрозами. Наприклад, запропоноване встановлення заходів для усунення загрози безпеці інформації шляхом встановлення протишумових дверей одночасно знижує ризик підслуховування.

Ітерації продовжуються до досягнення допустимого рівня безпеки або при перевищенні виділеного на захист інформації ресурсу. При виконанні зазначених умов процес побудови (удосконалення) необхідної системи завершується або продовжується з метою визначення додаткового ресурсу.

Після розгляду керівництвом запропонованих варіантів (краще двох для надання вибору), обліку пропозицій та зауважень, найкращий, з погляду особи, яка приймає рішення, варіант (проект, пропозиції) фінансується та реалізується шляхом проведення необхідних закупівель матеріалів та обладнання, проведення будівельно-монтажні роботи, налагодження засобів захисту та здачі в експлуатацію системи захисту або її додаткових елементів.

Слід наголосити, що спеціаліст із захисту інформації повинен при обґрунтуванні запропонованих керівництву організації варіантів захисту

враховувати психологію особи (керівника), яка приймає рішення про реалізацію пропозицій, а також не достатню інформованість її про загрози безпеці інформації в організації.

Психологічним фактором, що стримує прийняття рішення керівником про виділення досить великих ресурсів на захист інформації, є та обставина, що в умовах скритності добування інформації загрози їй апріорі не надаються досить серйозними, а набувають деякого абстрактного характеру. До існування потенційних загроз керівники звикають і їх не помічають так само, як люди не помічають безлічі загроз їх здоров'ю. Крім того, керівник через власне уявлення про погрози, способи та засоби їх нейтралізації може перебільшувати значущість одних заходів захисту та применшувати інші. Внаслідок цих обставин думка керівника щодо необхідності та сутності заходів захисту інформації може не співпадати з пропозиціями фахівців з інформаційної безпеки. Однак така розбіжність не повинна зменшувати ентузіазм і наполегливість фахівця, оскільки вона характерна для будь-якого виду діяльності, а вміння обґрунтовувати свої пропозиції є необхідною якістю будь-якого фахівця.

Слід зазначити, що розглянута послідовність у вигляді близька до чинних підходів. Наприклад, процес організації захисту США відповідно до концепцією «Opsec» (Operation Security) включає 7 етапів: від аналізу об'єкта захисту на першому етапі до доведення персоналу фірми заходів щодо безпеки інформації та здійснення контролю на останньому. Зміст низки процедур методу Opsec близько розглянутим. Проте в ній недостатньо місця та уваги відведено моделюванню загроз, а більше — аналізу заходів щодо захисту інформації керівними особами організації (фірми, компанії, установи).

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.
2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Етапи алгоритму проектування (модернізації) системи захисту інформації.
2. Умови завершення оптимізації та функції зворотного зв'язку в алгоритмі проектування (модернізації) системи захисту інформації.
3. Види моделей, що застосовуються під час проектування системи захисту інформації.
4. Що представляє собою вербальна модель?
5. Що представляє собою фізична модель?
6. Що представляє собою математичне моделювання?
7. Особливості імітаційного моделювання.

5 ПАРАЗИТНІ ЗВ’ЯЗКИ ТА НАВЕДЕННЯ

Паразитні зв'язки та наведення

У будь-якому радіоелектронному засобі або електричному приладі поряд з струмопроводами (проводами, провідниками друкованих плат), передбаченими їх схемами, виникають численні побічні шляхи, якими поширюються електричні сигнали, у тому числі небезпечні сигнали акустоелектричних перетворювачів. Ці шляхи створюються внаслідок паразитних зв'язків і наведень. Першопричиною їх є поля, створювані електричними зарядами та струмами в ланцюгах радіоелектронних засобів та приладів.

Постійні електричні заряди та електричний струм в елементах і ланцюгах радіозасобів та електричних приладів створюють відповідні електричні та магнітні поля, а заряди та струм змінної частоти — електромагнітні поля. Поля поширюються у просторі та впливають на елементи та ланцюги інших технічних засобів та систем. Крім того, для функціонування засобів та систем необхідно забезпечити гальванічне з'єднання їх елементів. Через гальванічні з'єднання виникають додаткові шляхи поширення сигналів одних вузлів і блоків по ланцюгах інших. В результаті впливу побічних полів і впливу через провідники і резистори сигналів одних вузлів і блоків на сигнали інших блоків і вузлів виникають паразитні зв'язки та наведення як усередині радіоелектронних засобів, так і між розташованими засобами. Ці зв'язки та на горілки погіршують роботу вузлів, блоків та засобів загалом. Тому при проектуванні радіоелектронних засобів рівні цих паразитних зв'язків та наведень знижують до допустимих значень. Чим вище вимоги до характеристик засобів, тим потрібні великі зусилля, а отже, і витрати для нейтралізації паразитних зв'язків і наведень. Основна частина високої ціни (десятки тисяч доларів) високоточних контрольно-вимірювальних приладів фірм Hewlett Packard , Ronde & Scwarz та ін. припадає на заходи щодо зменшення паразитних зв'язків та наведень.

Однак, незважаючи на заходи щодо зниження рівня паразитних зв'язків і наведень для забезпечення необхідних характеристик радіоелектронного засобу,

залишковий їх рівень створює загрози для інформації, що міститься в інформаційних параметрах сигналів, що циркулюють в радіоелектронному засобі. **Тому будь-який радіоелектронний засіб або електричний прилад слід з погляду інформаційної безпеки розглядати як потенційне джерело загрози безпеці інформації.**

Відомі три види паразитних зв'язків:

- ємнісна;
- індуктивна;
- гальванічна.

Ємнісний зв'язок утворюється в результаті впливу електричного поля, індуктивний - впливу магнітного поля, гальванічний зв'язок - через загальний активний опір.

Модель ємнісного паразитного зв'язку представлена на рис. 5.1.

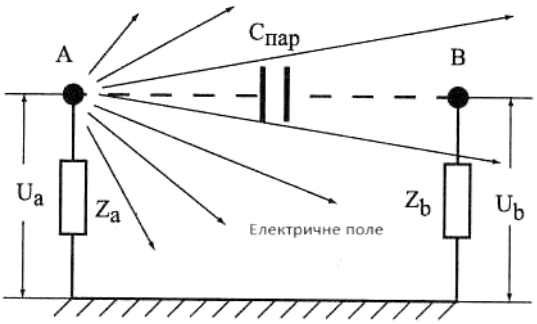


Рисунок 5.1 – Паразитний ємнісний зв'язок

На цьому рисунку U_{a} — потенціал заряду точки А щодо корпусу, що створює електричне поле. В результаті впливу цього поля в точці В виникає заряд протилежного знака . Величина потенціалу заряду (наведеної напруги) U_b точки відносно корпусу визначається співвідношенням ємнісного опору $\text{C}_{\text{п}}$, і опорів Z_b:

$$U_b = U_a \frac{Z_b}{Z_b + Z_{\text{п}}},$$

де $Z_{\text{п}} = 1/j\omega C_{\text{п}}$ – ємнісний опір між точками А і В, ω – кругова частота зміни потенціалу заряду точки А.

Ємність $\text{C}_{\text{п}}$ є паразитною і створює ємнісний паразитний зв'язок між точками А і В. Відношення:

$$\beta_{\text{с}} = \frac{U_b}{U_a} = \frac{Z_b}{Z_b + Z_{\text{п}}},$$

називається **коефіцієнтом паразитного ємнісного зв'язку.**

У більшості реальних випадках $Z_{\text{п}} \gg Z_b$, тому $\beta_c \approx Z_b j\omega C_{\text{п}}$. Отже, коефіцієнт паразитного ємнісного зв'язку пропорційний величині паразитної ємності та частоті коливань електричного поля.

Ємнісний паразитний зв'язок виникає між будь-якими елементами схеми: проводами, радіоелементами схеми та корпусом (шасі). Величина паразитної ємності на одиницю довжини проводів, паралельно розташованих на віддаленні b один від одного, визначається за формулою:

$$C_{\text{п}} = \frac{\pi\varepsilon_{\text{а}}}{\ln\left(\frac{2b}{d} + \sqrt{\left(\frac{b}{d}\right)^2 - 1}\right)},$$

де d — діаметр проводів; $\varepsilon_{\text{а}}$ — абсолютне значення діелектричної постійної.

З цієї формули випливає, що величина ємності пропорційна діелектричної проникності середовища, діаметру проводів і обернено пропорційна відстані між проводами. Максимальна паразитна ємність виникає між проводами котушок, у яких витки проводів намотуються впритул один до одного ($b \approx d$) і просочуються лаком ($\varepsilon_{\alpha} \approx 4{,}5 \cdot 10^{-11}$ Ф/м). Ця ємність становить $4{,}4 \cdot 10^{-10}$ Ф/м або 44 пФ/м. Ємність між двома паралельними проводами довжиною 100 мм та діаметром 0,1 мм зменшується з 0,75 пф до 0,04 пф зі збільшенням відстані між ними з 2 до 50 мм. Для проводів діаметром 2 мм ця ємність за тих самих умов більша і становить 5-0,07 пф.

Так як між рядом розташованими основними і допоміжними засобами існує паразитний ємнісний зв'язок, що сприяє передачі сигналів з інформацією, що захищається від ОТСС до ВТСС, то для визначення величини наведення треба знати їх паразитні ємності. Ці ємності називаються **власними ємностями** радіоелектронного засобу та електричного приладу. Обчислити власну ємність можна тільки для найпростіших конфігурацій типу штир, куля, диск. Наприклад, для штиря довжиною L паразитна ємність становить $\text{С}_{\text{п}} \approx 0{,}1\text{L}$, для диска $З_{\text{п}} \approx 0{,}35D$, кулі - $З_{\text{п}} \approx 0{,}56D$ де D — діаметр кулі і диска. Для реальних

радіоелектронних засобів складної конфігурації власна ємність $C_п$ визначається експериментально шляхом розміщення засобу в однорідному електричному полі і вимірюванням наведеної напруги на його виході $U_н$. Попередньо вимірюється наведена еталонна напруга $U_{не}$ в найпростішому пристрої (диску, кулі та інших) з відомою (еталонною) власною ємністю $C_{пє}$, поміщеному в це поле. На основі отриманих даних власна ємність досліджуваного засобу визначається методом заміщення, відповідно до якого $C_п = C_{пє} U_н / U_{не}$.

Паразитний індуктивний зв'язок ілюструється на рис. 5.2.

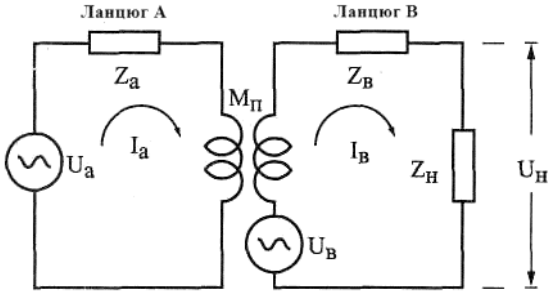


Рисунок 5.2 – Паразитний індуктивний зв'язок

Змінний струм, що протікає по ланцюгу А, створює магнітне поле, силові лінії якого досягають провідників іншого ланцюга В і наводять у ньому ЕРС величиною:

$$U_B = I_a \omega M_п = U_a \omega M_п / Z_a,$$

де ω – кругова частота змінного струму в ланцюзі A ; Z_a – повний опір ланцюга А ; $M_п$ – паразитна взаємна індуктивність між ланцюгами А і В.

ЕРС величиною U створює в ланцюгу В струм I зворотно пропорційний сумарному опору Z ланцюга В і опору навантаження $Z_н$. Цей струм викликає навантаження напруги наведення $U_н = UZ_н /(Z_В + Z_Н) = U_a \omega M_п Z_н / Z_а(Z_В + Z_Н)$. Відношення $\beta_i = U_н / U_а = \omega M_п Z_н / Z_а (Z + Z_н)$ називається **коефіцієнтом паразитного індуктивного** зв'язку **.** Він, як випливає з наведеного виразу, пропорційний частоті змінного струму і величині паразитної взаємної індуктивності і обернено пропорційний опору ланцюгів.

Взаємна індуктивність замкнутих ланцюгів залежить від взаємного розташування та конфігурації провідників. Вона тим більше, чим більша частина

магнітного поля струму в одному ланцюгу пронизує провідники іншого ланцюга.

Слід розрізняти взаємну індуктивність між провідниками різних ланцюгів від індуктивності провідника. Індуктивність характеризує властивість провідника перешкоджати зміні струму, що проходить через нього, яка обумовлена явищем самоіндукції. Вона виникає, коли силові лінії змінного магнітного поля пронизують провідники, якими протікає струм, що створює це магнітне поле.

Гальванічний паразитний зв'язок ще називають зв'язком через загальний опір, що входить до складу декількох ланцюгів. Такими загальними опорами можуть бути опір з'єднувальних проводів та пристроїв живлення та керування. Наприклад, вузли та блоки комп'ютера, що здійснюють обробку інформації, з'єднані з напругою +5 В блоку живлення. Для встановлення «0» тригерів дискретних пристроїв на відповідні їх входи одночасно подається відповідний сигнал управління. На рис. 5.3 наведена спрощена схема, що ілюструє виникнення гальванічного зв'язку.

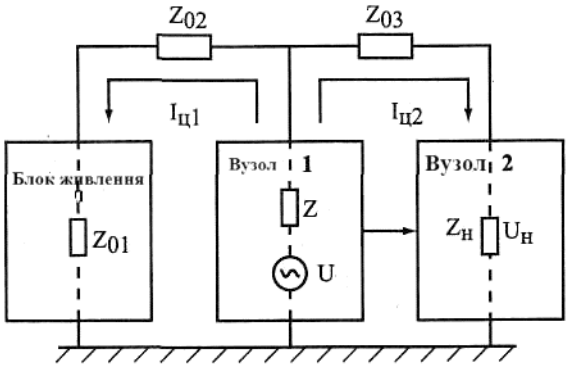


Рисунок 5.3 – Паразитний гальванічний зв'язок

Відповідно до нього до блоку живлення через загальні опори Z_{01}, Z_{02} і Z_{03} підключені вузол 1 і вузол 2 радіоелектронного засобу. Сигнал напругою U і 1-го вузла створює струми $I_ц1$ і $I_ц2$, в результаті яких на еквівалентному опорі N2 вузла виникає напруга наведення U. Відношення $\beta_г = U_н / U$ і називається коефіцієнтом **паразитного гальванічного зв'язку.**

Якщо побічні поля та електричні струми є носіями інформації, що захищається, то паразитні наведення та зв'язки можуть призводити до витоку інформації. Отже, паразитні зв'язки та наведення являють собою побічні фізичні процеси та явища, які можуть призводити до витоку інформації, що захищається.

Можливість витоку інформації через паразитні зв'язки і наведення носить імовірнісний характер і залежить від багатьох факторів, у тому числі від конфігурації, розмірів (щодо періоду коливань струмів, що протікають) і взаємного положення випромінюючих і приймаючих струмопровідних елементів засобів. На відміну від передбачених для зв'язку функціональних антен, конструкція та характеристики яких визначаються при створенні радіопередавальних та радіоприймальних засобів, ці елементи можна назвати **випадковими антенами.**

Випадковими антенами можуть бути монтажні проводи, з'єднувальні кабелі, струмопроводи друкованих плат, виводи радіо деталей, металеві корпуси засобів та приладів та інші елементи засобів. Параметри випадкових антен істотно гірші за функціональні. Але через невеликі відстані між передавальними та приймальними випадковими антенами (у радіоелектронному засобі або одному приміщенні) вони створюють загрози витоку інформації.

Випадкові антени мають складну і часто апріорі невизначену конфігурацію, досить точно розрахувати значення їх електричних параметрів, що збігаються з вимірюваними, дуже складно. Тому реальну випадкову антену замінюють її моделями у вигляді дротяної антени – відрізка дроту (вібратора) та рамки.

У ближній зоні вібратор створює переважно електричне поле. Властивості дротяної антени перетворюють електричний сигнал у полі (радіосигнал) і навпаки характеризуються параметром антени, названим **діючою висотою** $h_д$ і вимірюваним у м. Діюча висота передавальної антени являє собою параметр, що зв'язує напруженість електричного поля, створюваного антеною в напрямку з рівнем сигналу у самій антені. Діюча висота приймальної антени дорівнює відношенню ЕРС до приймальної антени до напруженості електричного поля,

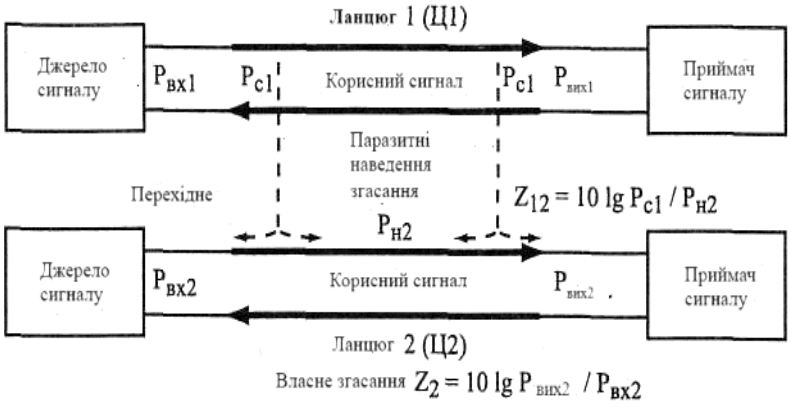
що викликає її: $h_д = U_a / E_a$. При цьому передбачається, що приймальна антена орієнтована в просторі відповідно до поляризації електромагнітного поля і прийом здійснюється з напрямку максимального рівня поля. Оскільки відношення напруженостей електричної та магнітної складових електромагнітного поля біля випадкової антени дорівнює хвильовому опору середовища ($Z = E_а / H_а$), то $h_д = U_а / H_а Z_в$.

Коефіцієнт посилення випадкової антени у вигляді замкнутого ланцюга (рамки) оцінюється за допомогою параметра, названого **довжиною антени, що діє,** $L_д = U_a / H_а$. За аналогією зі способами визначення власної ємності засобу діюча висота (довжина) випадкової антени знаходиться методом заміщення.

Паразитні зв'язки можуть викликати витік інформації з проводів та створювати умови для виникнення побічних електромагнітних випромінювань. За рахунок паразитних зв'язків виникають небезпечні сигнали у проводах кабелів різних ліній і ланцюгів, у тому числі в ланцюгах заземлення та електроживлення, а також виникають паразитні коливання в підсилювачах, дискретних пристроях та ін.

Серйозну загрозу безпеці інформації створюють наведення сигналів ОТСС на дроти та кабелі, що виходять за межі контрольованої зони (рисунок 4.4). Коли струм проходить провідниками першого ланцюга (Ц1), навколо них створюється магнітне поле, силові лінії якого пронизують провідники другого ланцюга (Ц2). В результаті цього ланцюгом Ц2 потече крім основного ще й перехідний струм, що створює перешкоду основному. Захищеність від взаємних перешкод оцінюється так званим **перехідним загасанням** $Z_{12} = 10\, lg P_{с1} / P_{н2}$, де $P_{с1}$ та $P_{н2}$ – потужність сигналів в 1-му ланцюгу і наведення від них у 2-му ланцюгу. Для надійного захисту інформації перехідне згасання має бути не менше величини $10\, lg P_с / P_{пр}$, де $P_с$ і $P_{пр}$ — потужність сигналу з інформацією та чутливість приймача зловмисника, що перехоплює наведений сигнал. Так як кабелі в будівлі укладаються в спеціальних колодязях і нішах, то між кабелями за рахунок їх досить близького і паралельного на великій відстані розташування виникають досить великі паразитні зв'язки між кабелями внутрішніх і міської АТС, інших

інформаційних ліній зв'язку, ланцюгами електроживлення та заземлення. Оскільки співробітники організації при розмові по телефонах внутрішньої АТС частіше допускають порушення режиму секретності (конфіденційності), ніж під час розмови по міській АТС, то при регулярному підслуховуванні розмов по внутрішній АТС можна видобути цінну інформацію. Власне згасання $Z_1 = 10\ lg\ P_{вих1} / P_{вх2}$.



¶ Рисунок 5.4 – Паразитні наведення

Сучасна архітектура службових приміщень передбачає створення між міжповерховими перекриттями і стелею (підлогою) вільного простору для прокладання різних кабелів (електроживлення, внутрішньої та міської АТС, трансляції , оперативного та диспетчерського зв'язку, мереж передачі даних та ін.). Це створює додаткові можливості виникнення між проводами кабелів паразитних зв'язків і появи небезпечних сигналів, що поширюються межі контрольованої зони.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Види побічних електромагнітних випромінювань та наведень.

2. Чим відрізняються активні акустоелектричні перетворювачі пасивних?

3. Які загрози створюють випадкові акустоелектричні перетворювачі ?

4. Види паразитних зв'язків. Фізичні явища, що викликають ємнісні та індуктивні паразитні зв'язки.

5. Коли виникає паразитний гальванічний зв'язок?

6. Фізичний сенс діючої висоти та довжини антени, що діє.

7. Джерела побічних низькочастотних та високочастотних випромінювань.

8. Умови виникнення паразитних коливань у підсилювачі.

9. Характер поширення електромагнітної хвилі у ближній зоні.

10. Характер випромінювання електромагнітного поля симетричного та несиметричного кабелів.

11. Причини, що спричиняють появу небезпечних сигналів у ланцюгах електроживлення.

12. Фізичні процеси, що призводять до витоку інформації щодо ланцюгів заземлення.

6 НИЗЬКОЧАСТОТНІ ТА ВИСОКОЧАСТОТНІ ВИПРОМІНЮВАННЯ ТЕХНІЧНИХ ЗАСОБІВ

Низькочастотні та високочастотні випромінювання технічних засобів

Велику загрозу безпеці інформації створюють також побічні випромінювання радіо- та електротехнічними засобами електромагнітних полів, що містять інформацію, що захищається. Джерелами випромінювань можуть бути ланцюги, що містять статичні або динамічні заряди (електричний струм), в інформаційні параметри яких тим чи іншим способом записується інформація, що захищається. Носії інформації, що захищаються у вигляді статичних або динамічних зарядів, можуть потрапляти в ці ланцюги безпосередньо, якщо ці ланцюги беруть участь в обробці, передачі та зберіганні інформації, що захищається, або самі елементи ланцюгів мають властивості акустоелектричних перетворювачів, або опосередковано, коли небезпечні сигнали проникають у випромінюючі ланцюги. паразитні зв'язки.

Вид випромінювання та характер поширення електромагнітного поля у просторі залежить від частоти коливань поля та виду випромінювача. Розрізняють **низькочастотне та високочастотні небезпечні випромінювання.**

Під низькочастотними випромінюваннями розуміються випромінювання електромагнітних полів, частоти яких відповідають звуковому діапазону. Джерелами таких випромінювань є пристрої та ланцюги звукопідсилювальної апаратури (мікрофони, підсилювачі потужності, аудіомагнітофони, гучномовці та їх узгоджувальні трансформатори, кабелі між мікрофонами і підсилювачами, підсилювачами і гучномовцями, ланцюги, що містять випадкові акустоелектричні перетворювачі).

Найбільшу загрозу створюють засоби звукофікації приміщень для озвучування акустичної інформації, що містить державну або комерційну таємницю. Ці засоби включають мікрофони, підсилювачі потужності, гучномовці, що встановлюються на стінах великих приміщень (залів для нарад, конференц-залів) або в спинки крісел, а також з'єднувальні кабелі . Причому

часто підсилювачі потужності розміщуються в технічному приміщенні, віддаленому на значній відстані від конференц-залу. По проводах кабелів звукопідсилювальної апаратури протікають великі струми, що становлять частки та одиниці ампер. Ці струми створюють потужні магнітні поля, які, по-перше, можуть поширюватися за межі виділеного приміщення, будівлі і навіть організації, а по-друге, наводити ЕРС у будь-яких струмопровідних конструкціях, у тому числі в ланцюгах електроживлення та металевої арматури будівель.

До **високочастотних небезпечних випромінювань** відносяться електромагнітні поля, що випромінюються ланцюгами радіоелектронних засобів, якими поширюються високочастотні (вище звукового діапазону) сигнали з секретною (конфіденційною) інформацією . Можна стверджувати, що якщо не вжито спеціальних додаткових заходів, то джерелами подібних небезпечних побічних ВЧ-випромінювань можуть бути будь-які ланцюги радіо- та електричних засобів. До основних джерел побічних випромінювань з потужністю, достатньою для поширення електромагнітного поля за межі контрольованої зони, наприклад приміщення, відносяться:

- гетеродини радіо- та телевізійних приймачів;
- генератори підмагнічування та стирання аудіо- та відеомагнітофонів;
- підсилювачі та логічні елементи в режимі паразитної генерації;
- електронно-променеві трубки засобів відображення інформації, що захищається (моніторів, телевізорів);
- елементи ВЧ-нав'язування;
- монітори, клавіатура, принтери та інші пристрої комп'ютерів, у яких циркулюють сигнали в паралельному коді.

Гетеродини радіо- і телевізійних приймачів є генераторами гармонійних коливань, необхідними для перетворення частоти сигналу, що приймається в проміжну частоту. Гармонічне коливання з гетеродина подається на змішувач, на нелінійному елементі (діоді або транзисторі) якого здійснюється перетворення вхідного сигналу, що приймається, в сигнал проміжної частоти. Частоти сигналів гетеродинів відрізняються на величину проміжної частоти (465

кГц - для ДВ-, СВ-і КВ-діапазонів, 10 МГц - для УКХ-діапазонів) від прийнятих сигналів і можуть мати значення від сотень кГц до десятків ГГц. Якщо елементи контуру (індуктивність і ємність) гетеродина мають властивості акустоелектричних перетворювачів або в нього проникають небезпечні сигнали від інших перетворювачів, то можлива амплітудна або частотна модуляція сигналів гетеродина. Потужність випромінювання модульованих сигналів гетеродина тим більша, чим ближче значення довжини хвилі гармонійного коливання до довжини ланцюгів, якими протікають сигнали гетеродинів. Часто вона буває достатньою для підслуховування мовної інформації в кабінеті керівника з увімкненим радіо- або телевізійним приймачем за допомогою побутових радіоприймачів у сусідніх приміщеннях або навіть будинках.

Генератори сигналів високочастотного підмагнічування та стирання магнітофонів створюють гармонійні коливання на частотах сотні кГц. Генератори сигналів високочастотного підмагнічування необхідні для забезпечення аналогового аудіо- і відеозапису з малими нелінійними спотвореннями. Залежність залишкової намагніченості магнітної плівки від напруженості магнітного поля в голівці запису є нелінійною, що призводить до спотворень у записаному сигналі. Шляхом подачі в магнітну голівку поряд із струмом запису додаткового струму підмагнічування з частотою близько 100 кГц і амплітудою, що в 6-8 разів перевищує максимальну амплітуду струму запису, встановлюється робоча точка для струму запису на лінійній ділянці кривої намагнічування. В результаті вибору оптимального струму підмагнічування вдається зменшити нелінійні спотворення сигналів запису до одиниць відсотків.

Генератор високочастотного стирання забезпечує стирання записаної на магнітну стрічку інформації шляхом розмагнічування її магнітного шару практично до нуля. Для цього в стиральну головку аудіомагнітофона подається струм із частотою 50-100 кГц. При такій частоті струму стирання і зменшенні напруженості магнітного поля головки внаслідок видалення стирається елементарна ділянка рухомої магнітної стрічки від зазору стиральної магнітної

головки, що призводить до багаторазового перемагнічування ділянки з намагніченістю, що зменшується до нуля. На відміну від високочастотного стирання і знищення інформації шляхом впливу на магнітний шар магнітним полем постійного магніту, який застосовується як стиральна головка в спеціальних диктофонах, намагнічування магнітного шару стрічки до насичення забезпечується.

Паразитна генерація може виникнути за певних умов у підсилювачах та логічних елементах дискретної техніки. Логічний елемент у даному контексті розглядається як підсилювач з дуже високим коефіцієнтом посилення.

Математичну модель підсилювача незалежно від числа каскадів посилення можна представити у вигляді комплексної передатної функції:

$$К_{ус}\ (\omega)\ e^{j\varphi_{ус}(\omega)},$$

де $К_{ус}\ (\omega)$ і $\varphi_{ус}(\omega)$ – коефіцієнт посилення та фаза вихідного сигналу відносно вхідного від частоти $\omega = 2\pi f$. В підсилювачі напруги фаза вихідного сигналу для непарного числа каскадів посилення змінюється на 180°, а при парному числі каскадів збігається з фазою вхідного сигналу.

Оскільки між елементами підсилювача завжди існують кісткові, індуктивні і гальванічні паразитні зв'язки, то на вході підсилювача поряд з посиленим зовнішнім сигналом присутні сигнали, що проникли у вхідні ланцюги через паразитний зворотний зв'язок, у тому числі з виходу підсилювача. Паразитний зворотний зв'язок можна також представити математичною моделлю $К_{ос}\ (\omega)\ e^{j\varphi_{ос}(\omega)}$. Узагальнена математична модель підсилювача із зворотним зв'язком представлена на рис. 6.1.

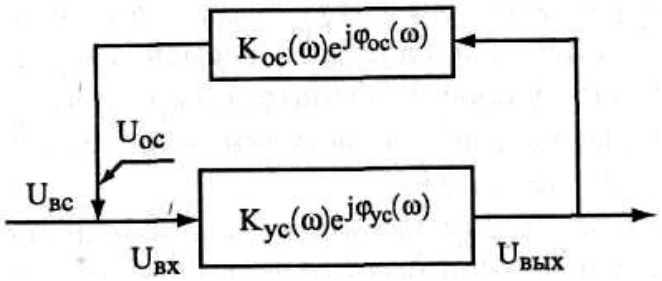


Рисунок 6.1 – Модель підсилювача із зворотним зв'язком

Зв'язок між виходом і входом підсилювача описується рівнянням:

$$U_{\text{вих}} = (U_{\text{вс}} + U_{\text{ос}})\,\text{К}_{\text{ус}}(\omega)\text{e}^{j\varphi_{\text{ус}}(\omega)} = [U_{\text{вс}} + U_{\text{вих}}\text{К}_{\text{ос}}\,(\omega)\text{e}^{j\varphi_{\text{ос}}(\omega)}]\,\text{К}_{\text{ус}}(\omega)\text{e}^{j\varphi_{\text{ус}}(\omega)}$$

Після перетворення:

$$U_{\text{вих}} = U_{\text{вс}}\frac{\text{К}_{\text{ус}}(\omega)\text{e}^{j\varphi_{\text{ус}}(\omega)}}{1 - \text{К}_{\text{ус}}(\omega)\text{e}^{j[\varphi_{\text{ус}}(\omega)+\varphi_{\text{ос}}(\omega)]}}$$

Режим посилення переходить у режим генерації, коли вихідний сигнал досягає максимального значення і підтримується на цьому рівні незалежно від U_x . Ця умова виконується за нульового значення знаменника зазначеного вище виразу. Отже, режим генерації виникає при $1 - \text{К}_{\text{ус}}(\omega)\,\text{К}_{\text{ос}}\,(\omega)\text{e}^{j[\phi_{\text{ус}}(\omega)+\phi_{\text{ос}}(\omega)]} \approx 0$. Для цього необхідно виконати дві умови:

1) $\varphi_{\text{ос}}\,(\omega) = 1/K_{\text{вус}}(\omega)$;

2) $\varphi_{\text{ос}}(\,\omega\,) = -\,\varphi_{\text{ос}}\,(\omega)$.

Перша умова визначає мінімально необхідну для виникнення паразитної генерації величину коефіцієнта паразитного зворотного зв'язку. Чим вище коефіцієнт посилення підсилювача, тим менший коефіцієнт паразитного зворотного зв'язку створює передумови для виникнення генерації. Наприклад, якщо $\text{К}_{\text{ос}} = 10$, то для виникнення генерації необхідно проникнення 0,1 частини вихідного сигналу на вхід підсилювача. Для підсилювача з $K_{\text{ус}} = 100$ достатньо надходження на його вхід 0,01 частини вихідного сигналу. Ця залежність пояснює можливість паразитної генерації у логічних елементах дискретної техніки. Високий коефіцієнт посилення логічного елемента та висока частота спектральних складових фронту дискретного сигналу створюють сприятливі умови для виникнення паразитної генерації в логічних елементах.

Друга умова передбачає, що зміна фази сигналу зворотного зв'язку має бути протилежною величині фазового зсуву підсилювача. Це означає, що фази зовнішнього сигналу і сигналу зворотного зв'язку повинні бути приблизно рівними. Зворотний зв'язок, при якому фаза сигналу на вході підсилювача збігається з фазою сигналу зворотного зв'язку, називається **позитивною ,** а коли фази цих сигналів протилежні - **заперечною.** Якщо позитивний зворотний

зв'язок сприяє паразитної генерації, то негативна, навпаки, підвищує стабільність роботи підсилювача, але за рахунок деякого зниження напруги на виході підсилювача. Тому в підсилювачах з високим коефіцієнтом посилення для виключення паразитної генерації створюють між каскадами негативний зворотний зв'язок, а також застосовують комплекс заходів для зменшення паразитних зв'язків. З цією метою при монтажі використовують короткі екрановані дроти, елементи вхідних і вихідних ланцюгів розносять на максимально можливу відстань, екранують трансформатори підсилювачів, в ланцюзі живлення попередніх каскадів встановлюють RC - фільтри низьких частот, підсилювальні каскади розміщують в одну лінію та ін.

Небезпека паразитної генерації полягає також у тому, що вона часто виникає на частотах вище робочого діапазону і без спеціальних досліджень не виявляється. Справді, зі зростанням частоти оброблюваних сигналів зменшуються значення паразитних ємнісних та індуктивних опорів між каскадами. В результаті цього збільшуються $К_{ос}$ і зсув фази сигналів, що пройшли через паразитні зв'язки. Тому можливість виконання умов генерації в підсилювачі на частотах, що перевищують верхню частоту робочого діапазону частот підсилювача, підвищується. Хоча на цій частоті корисні сигнали на вхід підсилювача не подаються, але на його вході присутні сигнали, обумовлені тепловим шумом і проникли через паразитний зворотний зв'язок. Будь-яка шумова реалізація на вході посилюється підсилювачем та частково повертається через паразитний зворотний зв'язок на його вхід. При рівні фаз величина сумарного сигналу на вході підсилювача підвищується, що призводить до зростання сигналу на виході підсилювача. Наслідком цього є збільшення сигналу $U_{ос}$ і подальше збільшення сигналу на вході підсилювача і т.д. Відбувається лавиноподібний процес наростання амплітуди сигналу на вході і виході підсилювача, що завершується процесом безперервної генерації на частоті $f_{рез}$. Тому не рекомендується, наприклад , застосовувати в підсилювачах низької частоти високочастотні транзистори, які посилюють шуми з частотами вище за верхню межу робочого діапазону частот.

Паразитна генерація підсилювача або логічного елемента створює загрозу інформації, якщо вона записується в інформаційні параметри паразитного коливання, тобто відбувається його модуляція інформаційними сигналами. Це явище виникає у випадку, якщо ланцюги паразитного генератора містять акустоелектричні перетворювачі або в них потрапляють небезпечні сигнали від інших випадкових акустоелектричних перетворювачів підсилювача.

Люмінофор електронно-променевих трубок засобів відображення під дією електронів випромінює, крім світла, електромагнітне поле в широкому діапазоні радіочастот з напруженістю, що забезпечує можливість перехоплення сигналів на віддаленні в десятки метрів. Враховуючи, що сигнали керування електронним променем трубки подаються послідовно в часі, їх побічні ВЧ-випромінювання створюють серйозну загрозу для трубки інформації, що відображається на екрані.

Пристрої комп'ютера, в яких поширюються сигнали в послідовному коді (монітори, клавіатура, принтери та інші), також є джерелом небезпечних сигналів. Заміна монітора комп'ютера на електронно-променевій трубці на рідкокристалічний монітор не усуває проблему захисту інформації, що відображається на екрані. Хоча екран рідкокристалічного монітора не створює небезпечні випромінювання, але у пристрої керування значеннями пікселів рядки монітора присутні послідовні інформаційні сигнали. Спектр цих сигналів має широкий спектр діапазоні сотень МГц. У результаті їх перехоплення можливе відновлення зображення.

До **випромінюючих елементів ВЧ-нав'язування** відносяться радіо- і механічні елементи, які забезпечують модуляцію зовнішніх електричних і радіосигналів, що підводяться до них. До таких елементів відносяться:

1) нелінійні елементи, на які одночасно надходять низькочастотний електричний сигнал з інформацією, що захищається (небезпечний сигнал) і високочастотний гармонійний сигнал;
2) струмопровідні механічні конструкції, що змінюють свій розмір і перетворюють зовнішнє електромагнітне поле.

Якщо на нелінійний елемент (діод, транзистор) подаються 2 сигнали: низькочастотний сигнал $u_c(t)$, в інформаційні параметри яких записана інформація, і високочастотний (сотні кГц-одиниці МГц) гармонійний сигнал $u_{вч}$ від зовнішнього генератора, то в струмі через нелінійний елемент з'являться високочастотні складові, модульовані по амплітуді небезпечним сигналом. Дійсно, струм, що протікає в нелінійному елементі в момент часу t визначається сумою напруг цих сигналів і опором ланцюга, в якій знаходиться нелінійний елемент. У загальному випадку залежність струму від напруг сигналів має вигляд $i_{нє} = f[u_c(t) + u_{вч}(t)]$. Через нелінійність функції $f(x)$ в струмі виникають складові, що представляють різні комбінації її аргументів. Справді, якщо функція $f(x)$ описується квадратичною залежністю, то $i_{нє} = k\,[u_c\,(t) + u_{вч}\,(t)]2 = k\,[\,u_c\,(t)^2 + 2u_c(t)\,u_{вч}(t) + u_{вч}\,(t)^2]$, де k – нормуючий коефіцієнт. Якщо уявити високочастотний сигнал як $u_{вч}(t) = A_{вч}\,sin\,\omega_{вч}\,t$, а небезпечний сигнал – у вигляді ряду Фур'є

$$u_c(t) = C_0 + \sum_{k=1}^{n} C_k \sin\,(k\,\omega_{10} t + \varphi_k),$$

той твір

$$2u_c(t)u_{вч}(t) = 2A_{вч}C_0 sin\omega_{вч}t + A_{вч}\sum_{k=1}^{n} C_k \cos\,[(\omega_{вч} - k\omega_{10})t - \varphi_k].$$

З цього виразу випливає наявність у спектрі струму високочастотних гармонік небезпечного сигналу, що несуть інформацію, що захищається . Цей струм створює електромагнітне поле, потужність якого залежить не тільки від потужності сигналів, але і від співвідношення довжини його хвилі і довжини ланцюга, по якій протікає струм. Такий варіант реалізується шляхом подачі зовнішнього високочастотного електричного сигналу до телефонної провідної лінії. Розглянутий варіант реалізується шляхом подачі зовнішнього електричного сигналу до телефонної провідної лінії.

Іншим видом випромінювача ВЧ-нав'язування є механічні конструкції, здатні змінювати свій розмір під дією акустичної хвилі та перевідбивати зовнішнє

електромагнітне поле. Такі конструкції, як правило, утворюють замкнуту порожнину зі струмопровідними поверхнями, одна з яких — тонка і здатна коливатися відповідно до акустичного сигналу мембрана. При коливанні мембрани змінюються геометричні розміри порожнини. Порожниною є коливальний контур, власна частота якого визначається її геометричними розмірами. При опроміненні конструкції електромагнітним полем з частотою коливання, що дорівнює власній частоті контуру, виникають резонансні явища і перевідбивається максимум енергії поля, що опромінюється. При коливаннях мембрани змінюються частота та напруженість перевідбитого поля. Після прийому перевідбитого поля з нього можна виділити шляхом демодуляції електричний сигнал, що відповідає акустичному. Такий випромінювач ВЧ-нав'язування по суті являє собою пасивний акустоелектричний перетворювач енергії, що підводиться.

Дальність поширення випромінюваного ВЧ-електромагнітного поля залежить від його потужності, частоти коливання, величини загасання поля в середовищі та характеру поширення поля.

Характер поширення електромагнітного поля у вільному просторі описується 4-ма рівняннями Максвелла, наведеними їм в 1873 році у праці «Трактат про електрику та магнетизм». Ці рівняння з'явилися узагальненням відкритих раніше законів електричного та магнітного полів.

Відповідно до першого рівняння, будь-яке магнітне поле створюється електричними струмами і зміною в часі електричного поля. Друге рівняння узагальнює закон електромагнітної індукції, відкритий Фарадеєм в 1831 році, і вказує на те, що в результаті зміни магнітного поля в будь-якому середовищі з'являється електричне поле. З третього рівняння Максвелла випливає, що потік вектора електричної індукції через будь-яку замкнуту поверхню дорівнює сумі зарядів в об'ємі, обмеженому цією поверхнею. Четверте рівняння дозволяє зробити висновок про те, що кількість силових ліній магнітного поля, що входять в середовище деякого об'єму, дорівнює кількості силових ліній, що

виходять з цього обсягу. Це можливо за умови відсутності в природі магнітних зарядів.

З рівнянь Максвелла також випливає, що автономно (незалежно) у природі можуть існувати лише постійні електричні та магнітні поля. Поле, що випромінюється зарядами та струмами змінної частоти, є електромагнітним. У ньому присутні електромагнітні та електричні компоненти, які описуються взаємно перпендикулярними векторами. Залежно від виду випромінювача та відстані від нього до точки вимірювання характер зміни та співвідношення між цими компонентами відрізняються та змінюються. Характер поширення електромагнітного поля піддається точному математичному опису для моделей випромінювачів як елементарних вібраторів. Як елементарний вібратор розглядається модель випромінювача, розміри якої істотно менше довжини хвилі випромінюваного електромагнітного поля і відстані від випромінювача до точки вимірювання. Для такої моделі параметри випромінювання у всіх точках приймаються рівними. Розрізняють елементарні електричний вібратор та магнітну рамку. Електричний вібратор збуджується джерелом змінної електрорушійної сили (джерелом зарядів), магнітна рамка – струмом, що протікає по рамці.

У реальних умовах, з урахуванням пере відображення електромагнітних хвиль від численних перешкод (будівель, стін приміщень, автомобілів і т. д.), характер поширення настільки складний, що в загальному випадку не піддається строгому аналітичному опису .

Залежно від співвідношення геометричних розмірів джерел випромінювань і відстані від них до точки вимірювання поля розрізняють **зосереджені та розподілені джерела.** Зосереджені джерела мають розміри, істотно менші, ніж відстань від джерела до точки спостереження. До зосереджених джерел належить більшість радіоелектронних засобів та його вузлів, і навіть головки гучномовців. Для розподілених джерел їх геометричні розміри співмірні або більше відстані до них. Типові розподілені джерела електромагнітного випромінювання — проводи кабелів ліній зв'язку.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів,

виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Що являють собою низькочастотні небезпечні випромінювання?
2. Наведіть приклад джерел низькочастотних небезпечних випромінювань.
3. Що являють собою високочастотні небезпечні випромінювання?
4. Наведіть приклад джерел високочастотних небезпечних випромінювань.
5. Які засоби створюють найбільшу загрозу безпеці інформації?
6. Що таке паразитна генерація?
7. Який зворотний зв'язок є позитивним?
8. Який зворотний зв'язок є негативним?
9. Що таке ВЧ-нав'язування?
10. Наведіть приклад із **зосереджених** джерел електромагнітного поля.
11. Наведіть приклад **розподілених** джерел електромагнітного поля.

7 ЗАСОБИ ТЕЛЕВІЗІЙНОГО СПОСТЕРЕЖЕННЯ

Дистанційне спостереження об'єктів, що рухаються, здійснюється за допомогою засобів телевізійного спостереження. Схема комплексу засобів телевізійного спостереження показано на рис. 7.1.

Рисунок 7.1 – Схема комплексу засобів телебачення

При телевізійному спостереженні зображення об'єктивом проектується на світлочутливий шар фотокатода вакуумної передавальної трубки або мішені твердотільного перетворювача. Фотокатод містить речовини, з атомів якої кванти світлової енергії вибивають електрони, кількість яких пропорційна енергії світла (яскравості елемента зображення). На фотокатоді утворюється зображення $Q(x, y, t)$ у вигляді електричних зарядів, еквівалентне оптичному $B\ (x, y, t)$ зображенню, де Q і В – значення відповідно величини зарядів і яскравості в точках з координатами х і у в момент часу t.

У вакуумних телевізійних передавальних трубках проводиться зчитування величини заряду за допомогою електронного променя трубки, що відхиляється по горизонталі та вертикалі магнітними полями. Ці поля створюються відхиляючими котушками, що надягаються на горловину телевізійної трубки.

За час розвитку телебачення розроблено багато типів передаючих телевізійних трубок, що відрізняються чутливістю фотокатода і роздільною здатністю. Поява простих ТВ-трубок типу «відикон» дозволило створити компактні телекамери. Мініатюрні відикони з діаметром до 15 мм забезпечують чіткість 400-600 ліній. На основі відео розроблені різні варіанти телевізійних

передаючих трубок: плюмбікон, кремнікон, суперортикон, ізокон та ін., які забезпечують якісне світлоелектричне перетворення в широкому діапазоні довжин хвиль і освітленості.

На початку 70-х років було відкрито та реалізовано новий принцип побудови безвакуумних твердотільних перетворювачів «світлоелектричний сигнал», т.з. **приладів із зарядовим зв'язком (ПЗЗ).** В основу таких приладів покладено властивості структури метал-оксид-напівпровідник, званої МОП-структурою (рис. 7.2).

Фотокатод або мета ПЗЗ представляє лінійку або матрицю з осередків з МОП-структурами, утворену горизонтальними та вертикальними струмопровідними прозорими електродами. Розміри кожного осередку відповідають розмірам елемента зображення. Роздільна здатність ПЗЗ визначається кількістю осередків, що розміщуються в полі зображення.

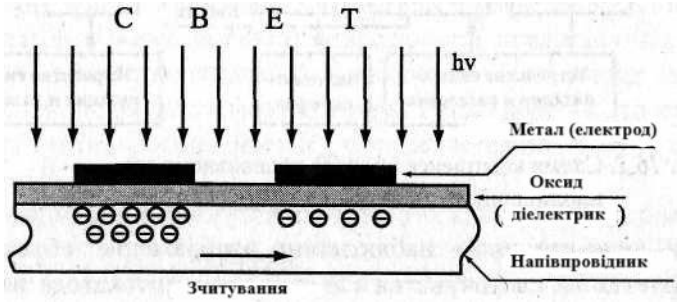


Рисунок 7.2 – Схема фрагмента ПЗЗ

Зчитування зарядів, що утворюються в кожному осередку ПЗЗ під дією світла точок зображення, проводиться шляхом послідовного перекачування зарядів з осередку на осередок під дією сигналів, що подаються на електроди. В результаті цього на виході ПЗЗ утворюється послідовність електричних сигналів, амплітуда яких відповідає величині заряду на осередках мішені на ПЗЗ

Типова **телевізійна передаюча камера** містить електронну плату з елементами електронної схеми, плату зі світлоелектричним перетворювачем та об'єктив. У малогабаритній камері для прихованого спостереження об'єктив та світлоелектричний перетворювач зміцнюються на єдиній електронній платі.

Електронна схема електронної плати телевізійної камери виконує такі функції:

• генерація сигналів управління світлоелектричним перетворювачем з метою зчитування з нього сигналів, еквівалентних яскравості об'єктів зображення;

• посилення сигналів зображення з виходу світлоелектричного перетворювача;

• формування сигналів (імпульсів) синхронізації за рядками та кадрами зображення на екрані монітора;

• формування повного колірного сигналу, що містить сигнали зображення, малі та кадрові синхронізуючі їм пульси.

Світлочутливі матриці сучасних телевізійних камер виконуються на приладах із зарядовим зв'язком (ПЗЗ), які порівняно з вакуумними телевізійними передаючими трубками мають неспівмірно малі розміри та енергоспоживання. Розмір світлочутливої області матриці називається оптичним **форматом.** Для систем відеоспостереження застосовують формати: 1/4, 1/3, 1/2, 2/3 та 1 дюйм. Слід зазначити, що розмір діагоналі матриці менший за величину, що дорівнює добутку формату на еквівалент дюйма (2,54 мм). Наприклад, розмір матриці 1/2" складає 6,4 × 4,8 мм з діагоналлю 7,8 мм замість 0,5 × 25,4 = 12,7 мм цього формату.

Чим більший формат матриці, тим вище можна забезпечити роздільну здатність камери. Матриці оптичного формату 1/2, 2/3 і 1 дюйм застосовують у камерах середнього та високого класу, а 1/3 та 1/4 – у малогабаритних камерах і для прихованого спостереження. На основі матриць формату 1/4 дюйма розміром 3,4 × 2,4 мм компанією Watec (Японія) створені надмініатюрні камери WAT-660 (29 × 29 × 16 мм) та WAT-704 R (циліндричної форми діаметром 18 мм).

Для отримання кольорового зображення світлочутливий елемент ПЗЗ матриці складається з 3-4 світлочутливих осередків, перед якими встановлені світлофільтри червоного, синього та зеленого кольорів. У варіанті 4 осередків дві

з них чутливі до зелених променів (перед ними встановлені світлофільтри зеленого кольору). Такий варіант наближає спектральну характеристику ПЗЗ матриці до спектральної характеристики ока, найбільш чутливого до зеленого кольору. Через технологічні та схемотехнічні проблеми та меншу освітленість кожного осередку елемента матриці роздільна здатність і чутливість кольорових камер гірша за чорно-білі. Для забезпечення високої роздільної здатності кольорових камер світловий потік від об'єктива за допомогою призм направляють на 3 ПЗЗ-матриці з відповідними світлофільтрами, що істотно ускладнює конструкцію камери. Камери з ПЗЗ-матрицями називаються також CCD - камерами.

Об'єктив телевізійної камери може бути змінним і вбудованим, з постійною і змінною фокусною відстанню . Основні характеристики об'єктива: **фокусна відстань f** та **світлосила.** Фокусна відстань об'єктива визначає кут зору телевізійної камери. Об'єктиви з малою фокусною відстанню (біля 2,8 мм) забезпечують перегляд просторів великої площі, але зображення, що отримуються, мають дрібний масштаб. Крім того, ширококутні об'єктиви вносять суттєві спотворення у зображення. Довгофокусні об'єктиви з f до 350 мм створюють чіткіше зображення, але з малою глибиною різкості. Для спостереження за вхідними дверима, приміщенням, відкритими майданчиками застосовуються ширококутні камери з кутом зору 60-90°. Залежність кута зору об'єктива α і камери від фокусної відстані об'єктива f в мм описується виразом $\alpha = arctg\,(h/2f)$, де h – розмір матриці по горизонталі мм. Отже, камери з малим оптичним форматом мають широкий кут зору.

Можливості спостереження з різними кутами зору створюють варіооб'єктиви (об'єктиви зі змінною фокусною відстанню), фокусна відстань яких може змінюватися вручну або сервоприводом.

Для прихованого спостереження застосовують мініатюрні телевізори заходи з об'єктивами pin-hole (з винесеною вхідною зіницею) або спеціальні насадки. У об'єктивів pin-hole площина апертури діафрагми збігається із вхідною зіницею (див. рис. 7.3).

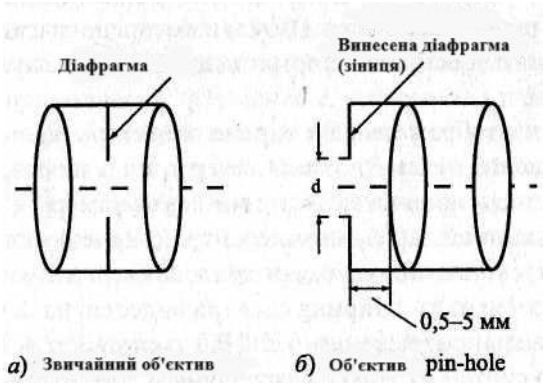


Рисунок 7.3 – Особливості об'єктиву pin-hole

Таке розташування діафрагми дозволяє істотно зменшити зовнішній діаметр d вхідної зіниці без помітного зниження світлосили об'єктива. Наприклад, японська мініатюрна камера «WAT-660» має чутливість 0,8 лк, роздільну здатність 380 ліній. При використанні об'єктивів pin-hole з діаметром зіниці від 0,9 до 2 мм камери можна вбудовувати в двері, стіну під шпалери, настінний годинник, в корпус сповіщувача та ін. предмети. Для прихованого спостереження через невеликий отвір використовується також на садочку у вигляді оптоволоконного кабелю діаметром близько 2 мм і довжиною 50 см і більше з об'єктивом на кінці.

У камерах із змінними об'єктивами застосовують два типи стандартних конструкцій вузлів приєднання:

• тип "C" ("C - mount") з різьбленням 2,54 × 0,8 і відстанню до площини ПЗЗ матриці 17,5 мм (старий стандарт);

• тип "CS" ("CS - mount") з різьбленням 2,54 × 0,8 і відстанню до площини ПЗЗ матриці 12,5 мм (новий стандарт).

Основними світлоелектричними показниками камери є роздільна **здатність** і **чутливість.**

Роздільна здатність (дозвіл) телевізійної камери визначається кількістю телевізійних ліній (ТВЛ), що формують зображення. Телевізійні мовні стандарти SECAM і PAL передбачають дозвіл 625 ТВЛ, NTSC (у США, Японії, Канаді та деяких країнах Латинської Америки) – 525 ТВЛ. Для телевізійних камер відеоспостереження систем охорони необхідний дозвіл нижче або вище в

залежності від розв'язуваних завдань. У майбутньому передбачається перехід телевізійного мовлення на формат високої чіткості з подвоєним дозволом.

Чіткість зображення на екрані монітора залежить не тільки від роздільної здатності телевізійної камери, але й від роздільної здатності монітора і смуги пропускання лінії зв'язку камери з монітором. Для безперервної передачі відеосигналу телевізійної камери смуга пропускання лінії зв'язку повинна бути не менше ширини спектра відеосигналу. Ширина спектру відеосигналу мовного стандарту при роздільній здатності 625 ТВЛ становить 6,5 МГ, чорно-білих камер систем охорони з роздільною здатністю 300 ТВЛ - 2,75 МГц і кольорових - 3,8 МГц.

Здатність телевізійної камери працювати при різній освітленості оцінюється двома показниками: **чутливістю** і **мінімальною освітленістю об'єкта спостереження.**

Чутливість камери характеризується мінімальною обумовленістю ПЗЗ-матриці, при якій забезпечується задана якість зображення. Для отримання зображення хорошої якості необхідно забезпечити відношення сигнал/шум на виході камери близько 50 дБ. При відношенні сигнал/шум близько 30 дБ на екрані монітора видно перешкоди у вигляді безладних точок (сніга), мінімально-допустиме відношення сигнал/шум - 20-24 дБ. Відповідно до цього мінімально-допустимим відношенням сигнал/шум визначається реальна чутливість телевізійної камери на відміну від граничної, коли розмах сигналу дорівнює розмаху шумової реалізації. В цьому випадку на зображенні практично, крім шумів, нічого не видно. Реальна і гранична чутливість телевізійної камери різняться приблизно в 10 разів. Звичайною вважається чутливість порядку часток лк (для чорно-білих камер) та одиниць лк (для кольорових). Телевізійні камери високої чутливості є працездатними при освітленості близько 0,01 лк.

Яскравість зображення на ПЗЗ-матриці пропорційна освітленості об'єкта спостереження, коефіцієнту відображення його поверхні та світлосилі об'єктива. Тому при позначенні чутливості камери в одиницях освітленості об'єкта спостереження вказується крім його освітленості також коефіцієнт відображення

і F-число об'єктива. Зазвичай мінімальна освітленість розглядається для об'єктів з коефіцієнтом відображення 0,75 та об'єктивів камери з F = 1,4. За цих умов освітленість ПЗЗ матриці буде приблизно в 10 разів менше, ніж у об'єкта спостереження.

Оскільки телевізійна камера має власні шуми, то при зменшенні освітленості об'єкта знижується відношення сигнал/шум на виході камери. Підвищення чутливості телевізійної камери, що розширює можливості застосування камери для прихованого спостереження, проводиться за наступними принципами:

• застосування високочутливих ПЗЗ-матриць та світлосильних об'єктивів;

• застосування електронно-оптичних перетворювачів-підсилювачів (ЕОП) яскравості зображення;

• використання адаптивних режимів накопичення та зчитування заряду в ПЗЗ-матрицях.

Підвищення чутливості ПЗЗ-матриць досягається зменшенням втрат світла через малу площу світлочутливих елементів, які займають лише близько 10% площі ПЗЗ-матриці. Решту її площі займають канали переносу зарядів при їх зчитуванні. Застосування мікролінз перед поверхнею ПЗЗ-матриці дозволяє в 3-4 рази підвищити чутливість ПЗЗ-матриці без лінз. До інших заходів підвищення чутливості відноситься пошук матеріалів з більш високою чутливістю у видимому діапазоні, з меншим рівнем шуму зчитування, який зменшує шуми відеосигналу, а також зниження впливу світіння транзисторів вихідного пристрою ПЗЗ-матриці, що створює засвічення зображення на ній.

Електронно-оптичні перетворювачі, що застосовуються в приладах нічного бачення, посилюють у десятки тисяч разів світло від об'єкта спостереження і дозволяють наблизити чутливість телевізійної камери до чутливості зорової системи людини (близько 10^{-4} лк). Їх широке використання стримується високою вартістю і низькою надійністю.

Для підвищення чутливості використовується також можливість ПЗЗ-матриці накопичувати енергію світлового сигналу між моментами зчитування еквівалентних електричних сигналів. При накопиченні η однакових сигналів відношення сигнал/шум збільшується в $\sqrt{\eta}$ разів. ПЗЗ-матриці з накопиченням досягають чутливості (4-5) 10^{-5} лк, тобто дозволяють спостерігати об'єкти в нічних умовах.

Телевізійна камера, так само як і фото- або кінокамера, містить пристрої, що забезпечують необхідну витримку і глибину різкості, а також пристрої електронного перетворення відеосигналу, що забезпечують підвищення якості зображення. Основними такими пристроями є **електронний затвор, автоматична діафрагма, пристрій автоматичного регулювання посилення відеосигналу.**

Електронний затвор визначає час витримки (тривалість накопичення зарядів ПЗЗ-приладами при проекції на них оптичного зображення) електронним способом. Електронний затвор забезпечує зміну витримки від часток секунд до 1/100000 с., що дозволяє спостерігати об'єкти, що швидко рухаються, в широкому діапазоні освітленості. Автоматичний електронний затвор автоматично змінює витримку при зміні освіченості.

Автоматична діафрагма змінює відносний отвір об'єктива в залежності від освітленості об'єкта спостереження та необхідної глибини різкості, що особливо важливо для забезпечення чіткості зображень відкритих майданчиків, коридорів та довгих приміщень.

Автоматичне регулювання посилення в електронній схемі камери підтримує необхідний рівень сигналу на виході підсилювача відео при зміні на 15-20 дБ і більше рівня сигналу на виході ПЗС матриці- вході відеопідсилювача.

Застосовувана у відеопідсилювачі **гамма-корекція (γ-корекція) відеосигналу** покращує якість зображення на екрані приймальної електронно-променевої трубки. Необхідність корекції викликана нелінійною залежністю яскравості світіння люмінофора екрану від амплітуди відеосигналу, яка апроксимується параболічною функцією з показником γ = 2,2. Гамма-корекція

передбачає запровадження нелінійності коефіцієнта посилення відеопідсилювача з γ = 0,25-0,45.

Яскравість різних ділянок зображення може істотно відрізнятись, а автоматичний затвор і пристрій АРУ реагують на усереднені значення яскравості зображення. При попаданні в поле зору камери, наприклад, електричної лампочки, що горить, темні ділянки зображення стають на екрані монітора ще темніше, а яскраві створюють засвітку зображення. У камерах з **компенсацією засвітлення («світла ззаду»)** опорна освітленість для автоматичної установки витримки та регулювання посилення оцінюється за яскравістю центральної частини зображення на ПЗЗ-матриці.

Електричний сигнал з виходу вакуумної передавальної трубки або ПЗЗ посилюється і передається по кабелю або у вигляді радіосигналів до телевізійного приймача. Останній виконує зворотні функції, перетворюючи електричний сигнал на зображення, яскравість кожного елемента якого еквівалентна амплітуді відповідного сигналу. Формування зображення проводиться на екрані приймальної вакуумної маскової трубки (кінескопа) або плоских панелей.

У вакуумній приймальній телевізійній трубці (кінескопі) зображення створюється на її екрані з люмінофором електронним променем, що модулюється електричним сигналом зображення і відклоняється по горизонталі (рядку) і вертикалі (по кадру) синхронно з траєкторією відхилення променя передавальної трубки або зчитування з ПЗС. Синхронність забезпечується шляхом передачі синхронізуючих сигналів у вигляді груп імпульсів, моменти формування яких відповідають кордонам рядків і кадрів. Синхроімпульси спільно з сигналом зображення утворюють повний телевізійний сигнал. У приймачі з повного телевізійного сигналу виділяються синхроімпульси, які синхронізують роботу пристроїв кадрової та малої розгортки. Ці пристрої формують сигнали, при проходженні яких по котушках відхилення, надіти на горловину кінескопа, створюються магнітні поля, що відхиляють електронний промінь.

Але вакуумні приймальні телевізійні трубки громіздкі, важкі, крихкі, потребують високовольтного (20-25 кВ) джерела постійного струму, пристрої розгортки споживають досить велику потужність, створювані трубкою поля, не нешкідливі для людини. Майбутнє за панелями.

Відомо кілька типів плоских панелей для телевізійних приймачів, але найбільш успішно розвиваються **газорозрядні** та **рідкокристалічні панелі.**

Газорозрядну панель утворюють два плоскопаралельних скла, між якими розміщені мініатюрні газорозрядні елементи. В інертному газі газорозрядного елемента під дією керуючих сигналів, що формуються мікропроцесором пристрою синхронізації і подаються на прозорі електроди одного або обох стекол, виникає розряд з ультрафіолетовим випромінюванням. Це випромінювання викликає свічення нанесеного на переднє або заднє скло люмінофора одного кольору чорно-білої панелі або люмінофорів червоного, зеленого або синього кольорів кольорової панелі. Наприклад, газорозрядна панель японської фірми NHK має формат екрану 874 × 520 мм, 1075200 елементів з кроком 0,65 мм, товщину 6 мм та вагу 8 кг. Газорозрядні панелі мають високу яскравість, що дозволяє створювати контрастне зображення навіть за сонячного світла.

Основою рідкокристалічної панелі є також дві плоскопаралельні скляні пластини. На одну з них нанесені прозорі горизонтальні та вертикальні струмопровідні електроди. У місцях їхнього перетину укріплені плівкові транзистори, два виведення яких з'єднані з електродами на склі, а третій утворює обкладку конденсатора. Другу пластину конденсатора представляє прозорий металізований шар на другій скляній пластині, розташованої паралельно першої на відстані, що вимірюється мікронами. Між пластинами розташована органічна речовина (рідкий кристал), яка під дією електричного поля змінює кут поляризації світла, що проходить через неї. З двох сторін панелі укріплені поляроїдними плівками, кути поляризації яких повернені на 90° відносно один одного.

Растр телевізійного зображення формується сигналами, що генеруються пристроєм синхронізації та подаються на електроди скляних пластин. При подачі на ці електроди напруги в точці їх перетину конденсатор заряджається і виникає електричне поле між відповідними обкладками конденсатора. Залежно від величини напруги, змінюється кут поляризації рідкого кристала між обкладками конденсатора. За відсутності напруги і, відповідно, електричного поля рідкий кристал повертає кут поляризації світла від лампи підсвічування на 90°, у результаті світло вільно проходить через поляроїдні плівки. Залежно від напруги на обкладках конденсатора кут поляризації може змінюватися від 90° до 0°, а прозорість комірки панелі — від максимальної до непропускання світла. Панель кольорового телевізора містить червоний, зелений та синій світлофільтри, що утворюють тріаду елемента розкладання зображення.

Роздільна здатність, яскравість, контрастність рідкокристалічних моніторів наближаються до аналогічних характеристик моніторів на електронно-променевих трубках, РК-монітори поступаються за інерційністю, але суттєво перевищують монітори на електронно-променевих трубках за масо-габаритними характеристиками, енергоспоживанням та екологічними показниками.

Широкополосність аналогового телевізійного сигналу та великий обсяг значень пікселів цифрового телебачення створюють проблеми при їх консервації. При записі відеосигналу на магнітну стрічку швидкість переміщення стрічки щодо записуючої головки відеомагнітофона повинна становити 5-6 м/с, що неприйнятно при реалізації принципів запису, що застосовуються в аудіомагнітофонах.

У відеомагнітофоні реалізовано комплекс заходів, що забезпечують якість зображення, близьке до телевізійного, при прийнятних споживчих показниках відеомагнітофона і відео касети (габаритах, вазі, часу запису на касеті). З цією метою скорочують смугу частот до 4-6 МГц, а для зменшення лінійної швидкості переміщення магнітної стрічки проводиться поперечно-рядкова (поперек стрічки) і похило-рядкова (під гострим кутом до напрямку руху стрічки) запис

відеосигналів на магнітну стрічку за допомогою обертової однієї або кількох (до 4) головок. Сигнали звукового супроводу та управління записуються на бічних краях магнітної стрічки.

Такі методи запису відеосигналів дозволяють при збереженні високої швидкості руху стрічки щодо головки значно зменшити її поздовжню швидкість і забезпечити прийнятний час запису на одній касеті. Для зменшення впливу паразитної амплітудної модуляції через змінний контакт головки зі стрічкою застосовують частотну модуляцію зі змінним індексом модуляції для різних частот і записують на стрічку частотно-модульований сигнал. Крім того, збереження необхідних тимчасових співвідношень досягається застосуванням високоточного стрічкопротяжного механізму, систем автоматичного регулювання електродвигунами і цифрових коректорів тимчасових спотворень.

Відеомагнітофони з поперечно-рядковим записом забезпечують високу якість зображення та звукового супроводу, але вони громіздкі та складні в експлуатації. Конструктивно більш простими є професійні та побутові відеомагнітофони з похило-рядковим записом.

Залежно від вимог до якості запису та відповідної швидкості «стрічка-головка» застосовують стрічки шириною 50,8, 25,4, 19, 12,65 мм і менше. Широка стрічка використовується у професійних відеомагнітофонах, 12,65 мм і менше – у побутових. Різноманітність значень ширини стрічки у поєднанні з різними способами запису спричинила безліч форматів запису: для стрічки шириною 50,6 мм — Q, 25,4 мм — B, C, 19,05 мм — U, 12,65 мм — L, МП, VHS, Beta та інші. Відеофонограми формату VHS для вітчизняної побутової апаратури мають такі параметри:

- швидкість голівки щодо стрічки – 4,85 м/с;
- поздовжня швидкість стрічки – 23,39 мм/с;
- ширина відеорядка – 0,04 мм;
- ширина доріжки звуку – 0,3 мм;
- ширина доріжки управління – 0,75 мм;
- кут нахилу рядки щодо краю стрічки – близько 6 град.

Мала поздовжня швидкість стрічки дозволяє на стандартній касеті з розмірами 188 × 104 × 25 мм робити безперервний запис зображення протягом 3-5 годин (залежно від товщини та довжини стрічки).

З метою підвищення якості зображення розвивається цифровий відеозапис у форматах D1 - D5, а в інтересах скорочення розмірів і ваги, що важливо для вирішення завдань з добування інформації – перехід на малогабаритні касети. На базі широко застосовуваного формату VHS запропоновані формати VHS - C (для касети з розмірами 92 × 59 × 22,5 мм), S - VHC, Video 8 (95 × 62,5 × 15 мм, ширина стрічки 8 мм) та малогабаритна касета МК (102 × 63 × 12 мм із шириною стрічки 3,8 мм). Формат S - VHC забезпечує роздільну здатність 440 ТВЛ замість 330 для формату VHC. У сучасних відеомагнітофонах вдається також знизити швидкість перемотки стрічки до 1 см/с і менше з відповідним збільшенням часу запису. Наприклад, у цифровому відеомагнітофоні EV-A80 (Sony) досягнуто швидкість стрічки 0,6/0,3 см/с, час запису у форматі V-8-540/1120 хв. з роздільною здатністю 250 рядків.

Аналогові відеомагнітофони поступово замінюються на цифрові, як вторинні носії інформації в яких використовуються жорсткі диски або енергонезалежна пам'ять.

При існуючих стандартах на параметри телевізійних засобів спостереження їх дозвіл на порядок гірший за роздільну здатність фотографій. Для підвищення чіткості зображення збільшують у 2 рази роздільну здатність та частоту кадрів. Але при цьому відповідно збільшується ширина спектра телевізійного сигналу з усіма недоліками, що з цього випливають. Для зменшення смуги зображення попередньо стискають. Для телевізійного спостереження в ІЧ-діапазоні застосовують телевізійні камери з ПЗЗ, чутливими до ІЧ-променів.

Для спостереження в оптичному діапазоні застосовують також лазери, промені яких у видимому або ІЧ-діапазонах підсвічують об'єкти в умовах низького природного освітлення. Для цієї мети промінь лазера за допомогою дзеркал, що коливаються, сканує простір з об'єктами, що спостерігаються, а

відбиті від них сигнали приймаються фотоприймачем так само, як при природному освітленні.

Відеопередавачі систем прихованого спостереження працюють у діапазоні частот від 60 МГц до 2,3 ГГц та вище. Їхня потужність становить від 40 мВт до 50 Вт, при цьому забезпечується дальність передачі від декількох метрів до 20 км. Наприклад, дальність передачі мініатюрного передавача РК5115 при потужності 15 Вт на частоті 236 МГц становить 400 м. Для збільшення дальності передачі використовують спеціальні ретранслятори.

Для прийому телевізійних радіосигналів використовуються як телевізійні приймачі широкого застосування, так і спеціальні. Наприклад, аудіо- та відеоприймач РК 625 забезпечує прийом аудіо- та відео-сигналів у діапазоні від 60 МГц до 1,2 ГГц, а відеоприймач RX 100 – у діапазоні 1,2-2,3 ГГц. Відеоприймачі мають вбудовані мікропроцесори, що автоматизують операції з пошуку та прийому сигналів. Наприклад, відеоприймач РК 6625 має 100 програмованих каналів пам'яті, 24-годинний таймер та автоматичний режим пошуку відеосигналів.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з

добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Склад та технічні характеристики типового комплексу засобів телевізійного спостереження.

2. Перерахуйте оптичні формати, що використовуються в системах відеоспостереження.

3. Типи передаючих телевізійних трубок, що використовуються в телебаченні.

4. Перерахуйте заходи , що підвищують чутливість телевізійної камери.

5. Переваги та недоліки аналогових відеомагнітофонів у порівнянні з цифровими.

6. Принципи запису широкосмугових сигналів магнітну стрічку.

7. Принципи роботи приладів із зарядовим зв'язком.

8. Принципи формування зображень на газорозрядних та рідкокристалічних панелях. Їх переваги в порівнянні з електроннопроменеві трубки.

9. Які алгоритми компресії відео ви знаєте?

8 ДИКТОФОНИ. ЗАКЛАДНІ (ЗАСТАВНІ) ПРИСТРОЇ. ЛАЗЕРНІ ЗАСОБИ ПІДСЛУХОВУВАННЯ. ЗАСОБИ ВИСОКОЧАСТОТНОГО НАВ'ЯЗУВАННЯ

Диктофони

Для прихованого підслуховування мовної інформації та її реєстрації широко застосовуються диктофони з вбудованими та винесеними мікрофонами. Прихований запис інформації проводиться з метою:

• «документування» розмови чи телефонної розмови задля економії часу під час складання звіту чи наступного аналізу розмови;

• реєстрації важко запам'ятовуються під час розмови інформації;

• використання запису для надання впливу на співрозмовника або надання його як доказ будь-яких його обіцянок і висловлювань, збору матеріалів про конкурентів, зловмисників та ін.;

• отримання голосового зразка співрозмовника для подальшої ідентифікації під час підслуховування;

• реєстрації власних пропозицій їхнього наступного аналізу;

• записи розмови у приміщенні під час відсутності власника диктофона.

Диктофони за принципами роботи діляться на кінематичні (зі стрічкопротяжним механізмом для забезпечення запису на магнітну стрічку або металевий дріт) та цифрові.

Кінематичні диктофони для потайливого підслуховування відрізняються від побутових або професійних (які використовуються журналістами) демаскуючими ознаками зі зниженою форматністю і можливістю потайливого управління режимами роботи. Це досягається:

• зменшенням в результаті прецизійного виготовлення механічних вузлів акустичних шумів стрічкопротяжного механізму;

• мінімізацією побічних електромагнітних випромінювань за рахунок виключення з електричної схеми генераторів підмагнічування та стирання;

• екранування електромагнітного випромінювання колекторного

двигуна;

• можливістю підключення виносного мікрофона;

• можливістю розміщення диктофона та його компонентів в одязі людини та потайливого управління режимами роботи диктофона;

• високою автоматизацією роботи диктофона - установкою акустоавтомата, лічильника стрічки, автореверса, індикатора роботи та іншими елементами.

Запис мови в диктофонах здійснюється на мікрокасеті зі швидкістю 2,4 або 1,2 см/с, тривалість запису в залежності від швидкості та типу касети становить від 15 хв. до 3 годин.

Автономне електроживлення більшості диктофонів забезпечується 1-2 елементами хімічного джерела струму типу АА і ААА, вага їх з батарейками становить десятки і сотні г (Olimpus L400, наприклад 90 г), а габарити диктофонів дозволяють їх розміщувати у внутрішній кишені піджака.

Металеві корпуси диктофона та додаткові шари екрану значно зменшують електромагнітне випромінювання колекторного двигуна, але не повністю елімінують його виявлення на короткі відстані, в десятках сантиметрів.

У цифрових диктофонах стрічкопротяжний механізм відсутній, а запис мовленнєвої інформації проводиться в цифровій формі на напівпровідникових пристроях, що запам'ятовують. Відсутність у цифрових диктофонах стрічкопротяжного механізму виключає акустичні шуми, але як його демаскуючої ознаки проявляються високочастотні випромінювання, що створюються імпульсами тактової частоти аналого-цифрового перетворювача та напівпровідникової пам'яті.

Заставні пристрої

З метою суттєвого підвищення дальності підслуховування широко застосовуються заставні пристрої (закладки, радіомікрофони, жучки, клопи). Ці пристрої перед підслуховуванням потай розміщуються в приміщенні зловмисниками або залученими до цього співробітниками організації, які

проникають під різними приводами до приміщення. Такими приводами можуть бути відвідування керівництва або фахівців сторонніми особами з різними пропозиціями, участь у нарадах, прибирання, ремонт приміщення та технічних засобів тощо.

Заставні пристрої в силу великої різноманітності конструкцій та оперативного застосування створюють серйозні загрози безпеці мовної та іншої інформації, що захищається в місцях з обмеженим доступом.

У загальному випадку заставний пристрій є ретранслятором, на вхід якого надходить первинний сигнал, що несе інформацію, а на виході — сигнал, узгоджений з характеристиками середовища, в якому він буде поширюватися. Різноманітність заставних пристроїв породжує різноманіття варіантів їхньої класифікацій. Варіант класифікації вказано на рис. 8.1.

Рисунок 8.1 – Класифікації заставних пристроїв

За виглядом носія інформації, що розповсюджується від закладних пристроїв, їх можна поділити на дротові та випромінюючі заставні пристрої. Носієм інформації від провідних закладок є електричний струм, який

розповсюджується по електричних дротах, а випромінюючі заставні пристрої передають інформацію за допомогою радіо- та ІЧ-сигналів.

Залежно від виду первинного сигналу провідні та випромінюючі заставні пристрої ділять на акустичні та апаратні. Акустичні заставні пристрої містять мікрофон, що перетворює акустичні сигнали на електричні. Апаратні закладки встановлюються в телефонних апаратах, ПЕОМ та інших радіоелектронних засобах. Вхідними сигналами для них є електричні сигнали, що несуть мовленнєву інформацію (у телефонних апаратах), або інформаційні послідовності , що циркулюють в ПЕОМ при обробці конфіденційної інформації. У таких закладках відсутній мікрофон, що спрощує їх конструкцію, і є можливість використовувати для електроживлення енергію засобу, в якому встановлена закладка. Інформацію апаратні закладки можуть передавати з проводів — дротові апаратні або за допомогою радіосигналів — випромінюючі апаратні. Широко застосовуються дротові телефонні заставні пристрої, що ретранслюють радіосигналом мовленнєву інформацію в телефонних лініях.

Провідні акустичні закладки є:

• субмініатюрні мікрофони, потай встановлені в побутових радіо- та електроприладах, у предметах меблів та інтер'єру та з'єднані тонким проводом з мікрофонним підсилювачем або диктофоном, що розміщуються в інших приміщеннях;

• мініатюрні пристрої, що містять мікрофон, підсилювач і формувач сигналу, що передається, як правило, по телефонних лініях і ланцюгах електроживлення.

Дротові акустичні закладки мають високу чутливість і завадостійкість, але наявність додаткового проводу демаскує закладки і ускладнює їх установку, особливо в умовах дефіциту часу. Тому такі закладки можуть встановлюватися під час ремонту або у приміщеннях з можливістю досить простого та тривалого доступу до них людей, наприклад, у номери готелів.

Закладки, що використовують санкціоновано прокладені дроти (ланцюги електроживлення та інформаційні лінії), позбавлені цього недоліку. Тому вони

все ширше застосовуються для передачі в межах будівлі інформації в місця знаходження зловмисника або його засоби для запису або ретрансляції сигналу радіоканалом. Ці закладні пристрої встановлюються в місцях підключення проводів електроживлення до вимикачів і мережевих розеток, у телефонних апаратах або їх розетках, а також усередині інших радіозасобів.

Випромінювальні заставні пристрої позбавлені недоліків про водних, але у них проявляється інша інформативна демаскуюча ознака — випромінювання в радіо- та оптичному діапазонах.

Найбільш широко застосовуються акустичні радіозакладки, що дозволяють порівняно просто та потай встановлювати їх у різних місцях приміщення. Найпростіша акустична радіо закладка містить (див. рис. 8.2) такі основні пристрої: мікрофон, мікрофонний підсилювач, генератор несучої частоти, модулятор, підсилювач потужності, антену та джерело електроживлення.

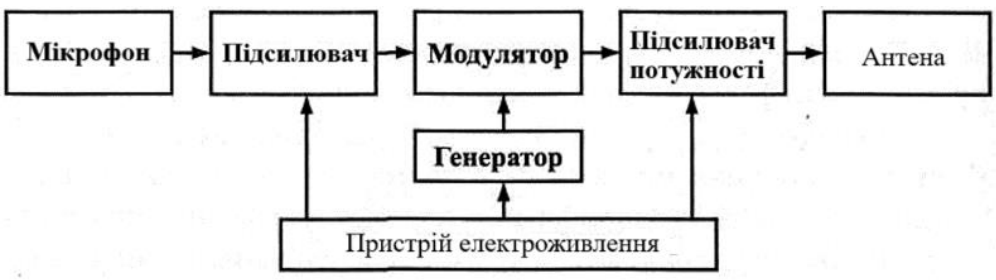


Рисунок 8.2 – Схема акустичної закладки

Мікрофон перетворює акустичний сигнал, що містить інформацію, на електричний сигнал, який посилюється до рівня входу модулятора. У модуляторі проводиться модуляція коливання несучої частоти посиленим сигналом з мікрофона, тобто інформація переписується з низькочастотного носія на високочастотний носій. Для забезпечення необхідної потужності випромінювання модульований сигнал посилюється в підсилювачі потужності. Електрична схема сучасних заставних пристроїв все частіше доповнюється пристроями, що забезпечують тактичне закриття переданої інформації.

Випромінювання радіосигналу у вигляді електромагнітної хвилі здійснюється антеною, як правило, у вигляді відрізка дроту. Для телефонних випромінюючих заставних пристроїв як антена використовуються дроти телефонних ліній. Так як антени у вигляді шматків дроту (диполів) або дротів ліній погано погоджуються довжинами хвиль генерованих передавачем коливань, то лише невелика частина потужності електричних сигналів випромінюється в ефір.

З метою зменшення ваги, габаритів та енергоспоживання, функції в радіозакладці реалізуються технічно за допомогою мінімальної кількості активних та пасивних елементів. Найпростіші закладки можуть містити лише один транзистор.

Встановлення заставних пристроїв можливе із заходом зловмисника до приміщення, де проводиться їхнє розміщення, або без заходу. Перший варіант дозволяє раціональніше розмістити закладку як з точки зору енергетики, так і скритності, але пов'язаний з підвищеним ризиком для зловмисника. Тому у випадках, коли створюються передумови для дистанційної (без заходової) установки закладки, їх закидають у приміщення або ними вистрілюють з пневматичної рушниці або пращі. Наприклад, комплект PS фірми Sipe Electronic складається зі спеціального безшумного пневматичного пістолета з прицільною відстанню 25 м і радіозакладкою, укріпленою на стрілі. Стріла після пострілу надійно прикріплюється за допомогою присоски до поверхонь з металу, дерева, пластмаси, бетону та інших гладких будівельних та облицювальних матеріалів. Мікрофон забезпечує знімання мовної інформації з відстані до 10 м, а передавач — її передачу на відстань до 100 м.

За діапазоном частот заставні пристрої відрізняються великою різноманітністю. На ранніх етапах використання заставних пристроїв частоти випромінювань прив'язували їх до частот побутових радіоприймачів в УКХ-діапазоні. При масовій появі у населення побутових радіоприймачів збільшилася небезпека випадкового перехоплення сигналів радіозакладок сторонніми

особами. Тому більшість типів сучасних закладок мають вищі частоти в УВЧ-діапазоні.

Для більш 96% радіозакладок робочі частоти зосереджені в інтервалі 88-501 МГц, причому більша частина (52%) з них має частоти 373-475 МГц, близько 42% - 92-169 МГц. Найбільш інтенсивно використовується діапазон частот 450-475 МГц, в якому зосереджено робочі частоти 36% наявних на ринку радіо заставних пристроїв.

Продовжується тенденція подальшого підвищення частот, у тому числі з переходом до ГГц-діапазону. Зі збільшенням частоти передавача зменшується рівень перешкод, що дозволяє знизити потужність передавача і, відповідно, його габарити, а також довжину антени. Крім того, залізобетонні стіни приміщень сучасних будівель екранують випромінюване заставним електромагнітне поле тим більше, чим більша довжина хвилі по відношенню до лінійних розмірів осередку залізної арматури стіни. Тому з підвищенням частоти передавача заставного пристрою (зменшенням довжини хвилі) екранувальний ефект арматури залізо тонної стіни знижується, хоча згасання поля в бетоні дещо збільшується.

В інтересах підвищення скритності для випромінюючих закладних пристроїв освоюється ІЧ-діапазон. Проте в силу більшого порівняно з радіохвилями загасання ІЧ-променів у середовищі поширення та необхідністю забезпечення прямої видимості між випромінювачем ІЧ-закладки та фотоприймачем зловмисника застосування подібних заставних пристроїв обмежене.

Крім діапазону частот на умови передачі закладкою інформації впливає стабільність частоти її передавача. Для простих схемних рішень передавача закладки значення його частоти змінюються у значних межах залежно від температури та напруги живлення. Величина дрейфу робочої частоти радіозакладок може досягати одиниць МГц. Внаслідок цього радіоприймач, налаштований на частоту радіозакладки, через деякий час втрачає радіосигнал. Ця обставина має важливе значення для забезпечення автоматичного прийому

сигналів радіозакладок, наприклад, у разі, коли підслуховування проводиться апаратурою в автомобілі за відсутності в ньому оператора. Частоти близько половини пропонованих на ринку радіозакладок стабілізуються.

Підвищення стабільності частоти випромінювання забезпечується шляхом застосування в коливальному контурі генератора елементів зі слабкою температурною залежністю, температурної компенсації, стабілізації напруги живлення, включення в коливальний контур елементів, що стабілізують його частоту.

Розрізняють «м'яку» та «жорстку» стабілізацію. У закладних пристроях «м'яка» стабілізація зі стабільністю часто досягається 10^{-3}-10^{-4} схемотехнічними рішеннями (стабілізацією напруги температурною компенсацією та ін.). Для більшої стабільності частоти передавача («жорсткої», зі стабільністю 10^{-5}-10^{-6}) як стабілізуючі елементи використовуються пластини кристала кварцу. При встановленні кварцу паралельно контуру генератора в ньому виникають стабільні механічні коливання, частота яких залежить від виду зрізу кристала кварцу, товщини та розмірів його пластини. Резонансні електричні коливання в контурі існують при рівності частот коливань кварцу та контуру. Стабілізація частоти випромінювання радіозакладки ускладнює її схему і збільшує габарити передавача, але суттєво покращує зручність роботи.

Іншою проблемою, що виникає при застосуванні заставних пристроїв, є забезпечення їх енергією протягом підслуховування. Можливості сучасної мікроелектроніки зі створення мініатюрних заставних пристроїв обмежуються переважно масогабаритними характеристиками автономних джерел живлення (хімічних елементів). Мікрогабаритні джерела струму, що широко застосовуються в електронному годиннику, забезпечують роботу заставних пристроїв протягом короткого часу (десятків годин при мінімально-допустимій потужності випромінювань для дальності до сотні метрів). Для закладних пристроїв використовуються гальванічні елементи (батареї та акумулятори) з високою питомою ємністю. Усереднені характеристики таких елементів наведено у табл. 8.1.

Таблиця 8.1 – Характеристики гальванічних елементів

Тип елемента	Напруга, У	Питома ємність, Втч/кг	Саморозряд, % в місяць
Нікель-кадмієвий (Ni-Cad)	1,25	40-80	20
Нікель-гідридний (Ni-MH)	1,25	60-120	30
Літій-іонний (Li-Ion)	3,6	110-160	до 10
Літій-полімерний (Li-Pol)	3,6	100-130	до 10

Місткість гальванічного елемента пропорційна його габаритам та вазі. Найбільш широко поширені циліндричні гальванічні елементи розміром АА і ААА з діаметром 10,5 і 8,2 мм, висотою 44,5 і 40,2 мм відповідно. Кнопкові (у вигляді таблетки) гальванічні елементи мають діаметр 7,86-16 мм і висоту 3,56-16,8 мм. Плоскі елементи мають габарити: довжина 14,2-31 мм, висота 14-21,4 мм. У великогабаритних заставних пристроях застосовують ядерні джерела електроживлення з часом роботи в десятки років, але вони потребують товстих і важких екранів для захисту від радіоактивного випромінювання.

Радикально проблема електроживлення заставних пристроїв і, відповідно, тривалість їх роботи вирішується підключенням заставних пристроїв до зовнішніх джерел електроживлення – до мережі та ланцюгів РЕМ та інших приладів, в які встановлюються заставні пристрої. Широко застосовуються подібні заставні пристрої в телефонних апаратах, закамуфльовані під їх елементи (конденсатори, телефонні капсулі та ін.), у трійниках для підключення кількох приладів до однієї розетки електромережі. У 75% заставних пристроїв використовується автономне (батарейне) живлення, 8% – живлення від мережі та 17% – живлення від телефонної лінії. Крім того, енергія може підводитися ззовні шляхом опромінення заставних пристроїв зовнішнім електромагнітним полем. Можливість їхньої безперервної роботи до моменту виявлення та вилучення пояснює все ширше їх поширення.

Збільшення часу експлуатації та підвищення скритності роботи заставного пристрою досягаються також шляхом автоматичного підключення до автономного джерела живлення найбільш енергоємного вузла радіозакладки — передавача тільки в період передачі мовної інформації. Така можливість реалізується у двох варіантах. У першому варіанті в закладці встановлюється спеціальний пристрій – акустичний автомат (акустоавтомат), що підключає до джерела живлення передавач при прийомі закладкою акустичного сигналу.

У тиші, у нічний час у включеному стані (в «черговому» режимі) знаходиться лише мікрофонний підсилювач із виконавчим електронним реле. При появі в приміщенні акустичних сигналів від людей, що розмовляють, реле по сигналу від мікрофонного підсилювача підключає передавач і заставний пристрій випромінює радіосигнали з інформацією. Після припинення розмови вихідний стан реле відновлюється і випромінювання припиняється.

У другому варіанті дистанційно керовані заставні пристрої включаються на випромінювання по зовнішньому радіосигналу, що дається зловмисником. Ці заставні пристрої забезпечують підвищену скритність і триваліший час роботи. Однак для їх ефективного застосування треба мати додатковий канал витоку відомостей про час циркулювання конфіденційної інформації в приміщенні, де встановлено заставний пристрій. Наприклад, треба досить точно знати час, коли вестимуться в приміщенні конфіденційні розмови. Так як дистанційно керовані закладки містять пристрій для прийому радіосигналів, що управляють, то вони найбільш складні і, отже, дорогі.

З метою додаткового підвищення скритності роботи закладних пристроїв все ширше застосовують перетворення сигналів, що ускладнюють їх виявлення. За цією ознакою закладні пристрої ділять на незакриті та з технічним закриттям.

Жорсткі вимоги до габаритів, маси, енергоспоживання заставних пристроїв обмежують потужність випромінювання їх передавачів. Найчастіше (понад 80%) застосовуються радіомікрофони, потужність випромінювання яких знаходиться в інтервалі 3-11 мВт, закладки з більш високою потужністю – до 22

мВт складають менше 10%. Зустрічаються закладки і більшої потужності випромінювання (до 200 мВт і більше), проте їхня частка вкрай незначна. Мала потужність випромінювання передавачів радіозакладок визначає відносно невелику дальність прийому їх сигналів. Близько 75% зразків забезпечує функціонування каналу на відстанях 50-350 м, 16% – на відстанях 460-600 м, 7% – на відстанях 740- 800 мі лише близько 2% – на відстані до 1000 і більше метрів. Зазначені пропорції згодом змінюються, та його характер зберігається.

У загальному випадку технічні дані заставних пристроїв знаходяться в межах:

- частотний діапазон – 27-900 МГц;
- потужність – 0,2-500 мВт;
- дальність – 10-1500 м;
- час безперервної роботи – від кількох годин до кількох років;
- габарити – 1-8 $дм^3$;
- вага – 5-350 г.

Основна проблема оперативного застосування заставних пристроїв полягає в раціональному розміщенні їх у приміщенні або в радіоелектронному засобі. Раціональність досягається при забезпеченні:

• надходження на вхід закладки сигналу з характеристиками, необхідні для якісної передачі звукової або іншої інформації;

• скритності розміщення та роботи закладки, принаймні, протягом часу підслуховування інформації, що цікавить зловмисника.

Ефективність виконання цих умов залежить від віддаленості місця встановлення закладки від джерел звуку та наявності між ними звукопоглинаючих і звукоізолюючих екранів, від чутливості мікрофона, розмірів і параметрів акустики, перш за все, від часу реверберації приміщення і часу, який має зловмисник для встановлення. Чутливість сучасних малогабаритних мікрофонів забезпечує досить якісний прийом акустичних сигналів на видаленні до 10- 5 м за відсутності екранів на шляху

розповсюдження акустичної хвилі. На якість мови, що ретранслюється закладним пристроєм, впливають:

— співвідношення сигнал/шум на вході мікрофонного підсилювача закладного пристрою;

— час реверберації приміщення, в якому встановлено заставний пристрій.

При малому часі реверберації на мікрофон закладки надходить пряма акустична хвиля, ослаблена відстанню та екранами, що маскують закладку. При великому часі рівень сигналу на мембрані збільшується за рахунок енергії перевідбитих хвиль, але внаслідок складання на мембрані хвиль, що відповідають різним звукам, погіршується розбірливість ретранслюваної мови. Ці фактори впливають на якість сприйняття такої мови людиною, але меншою мірою, ніж при ретрансляції її заставними пристроями.

Незважаючи на порівняно малі розміри та вагу заставних пристроїв, вони можуть бути виявлені при ретельному візуальному огляді приміщення. З метою продовження часу їх оперативного використання, а також наближення мікрофонів до джерела звуку заставні пристрої камуфлюють під предмети, які не викликають підозри у оточуючих людей. Важко знайти предмети особистого користування, засоби оргтехніки та побутової радіоелектроніки, до яких не можна було б підключити різноманітні пристрої для підслуховування. Деякі з таких засобів підслуховування наведено у табл. 8.2.

Таблиця 8.2 – Засоби підслуховування

Найменування засобу	Тип, фірма	Характеристики засобу
Радіопередавачі в:	ELECTRONIC:	
склянці	РК535	65 × 100 мм, 210 г, сонячні батареї
попільничці	РК565-S	90 × 45 мм, 480 г, сонячні батареї
свічнику	РК580	100 × 175 мм, 650 г, сонячні батареї

Продовження таблиці 8.2

калькулятор	РК620-S	135 × 100 мм, радіус дії 150-200 м
розетці електроживлення	РК55О	140 × 60 × 40 мм, 380 г, дальність до 600 м
настільна запальничка	РК575	80 × 32 × 52 мм 150 г, час роботи до 80 год
цвяху	РК520	35 × 6 мм, 96 г, 36 годин, до 200 м
кульковій ручці	РК585	135 × 11 мм, 25 г, 6 годин, до 300 м
годинник	РК1025-S	88-108 або 130-150 МГц, 6 годин
ремені	РК850-S	139 МГц, до 800 м
Радіопередавач в запонках, шпильці для краватки	STG4140, STG	15-150 МГц, потужність 5 мВт
Радіопередавач у відеокасеті	UM 007.3, SMIRAB ELEC TRONIC	136-146 МГц, до 300 м, час безперервної роботи 3 діб
Магнітофон у книзі	РК660, ELECTRONIC	200 × 250 × 65 мм 1200 г, час запису 2 × 90 хв.
Магнітофон у пачці сигарет	РК1985, ELECTRONIC	55 × 87 × 21 мм, 160 г, час роботи 11 год.

Лазерні засоби підслуховування

Підслуховування за допомогою лазерних засобів є порівняно новим способом (перші робочі зразки з'явилися в 60-ті роки) і призначене для знімання акустичної інформації з плоских поверхонь, що вібрують під дією акустичних хвиль. До таких поверхонь відносяться, перш за все, шибки закритих вікон.

Система лазерного підслуховування складається з лазерного передавача в інфрачервоному діапазоні та оптичного приймача. Лазерний промінь за допомогою оптичного прицілу направляється на вікно приміщення, в якому ведуться розмови, що цікавлять зловмисника. При відображенні лазерного

променя від поверхні, що вібрує, відбувається його частотна, кутова і фазова модуляція.

Частотна модуляція обумовлена ефектом Доплера внаслідок коливальних рухів шибки під впливом акустичного мовного сигналу. Але цей вид модуляції через проблему вимірювання змін частоти (довжини хвилі) для добування інформації не використовується.

Зміна кута відбиття лазерного променя, тобто кутова модуляція, відбувається через викривлення поверхні скла під час його коливання. Відбитий промінь приймається оптичним приймачем, розміщеним у точці прийому відбитого променя. Зміни напрямку відбитого променя при коливаннях скла викликають відповідні зміни положення плями світла на світлочутливому елементі (фотодіод, фототранзистор) оптичного приймача. В результаті цього змінюється освітленість світлоочисного елемента приймача і амплітудна модуляція електричного сигналу на виході елемента. Сигнал після посилення прослуховується і записується на аудіомагнітофон. Юстування положення світлочутливого елемента оптичного приймача проводиться за оцінкою оператором розбірливості мови.

Інший варіант побудови системи лазерного підслуховування передбачає реалізацію в оптичному приймачі фазової демодуляції шляхом порівняння фаз опромінювального і відбитого променів. З цією метою вихідний промінь за допомогою напівпрозорого дзеркала розщеплюється на два промені. Одним з них опромінюється скло, інший прямує до приймача як опорний сигнал. В оптичному приймачі створюється електричний сигнал з рівнем, що відповідає різниці фаз опорного і відбитого променів або коливань скла вікна. Цей варіант забезпечує вищу чутливість системи підслуховування, але складний у реалізації.

Прикладом засобу лазерного підслуховування є система РК-1035 фірми РК Electronic. Система складається з лазерних передавача та приймача, магнітофона для запису перехопленої інформації. Передавач та приймач системи встановлюються на тринозі. Лазерний передавач має розміри 65 × 250 мм, вага 1,6 кг, потужність — 5 мВт, довжина хвилі випромінювання — 850 мкм.

Лазерний приймач має розміри 65 × 260 мм, вага 1,5 кг. Електроживлення – від мережі та автономне.

Дані щодо можливостей систем лазерного підслуховування суперечливі. У рекламних матеріалах дальність вказується для різних систем від сотень метрів до км. Однак без посилання на рівень зовнішніх акустичних шумів ці величини можна розглядати як потенційно досяжні в ідеальних умовах. У міських умовах коливання зовнішнього скла вікна з подвійним склінням під дією шуму вулиці можуть перевищувати амплітуду його коливання від акустичного мовного сигналу. Слід також мати на увазі складність практичної установки випромінювача та приймача, при якій забезпечується попадання дзеркально відбитого від скла невидимого лазерного променя на фотоприймач. Оптимальний варіант застосування — забезпечення перпендикулярності лазерного променя по відношенню до поверхні скла, що опромінюється. У цьому випадку відбитий промінь повернеться до фотоприймача, встановленого поруч (в одному приміщенні) з випромінювачем. Однак реалізувати такий варіант можна лише в окремих випадках.

Рівні ж дифузно відбитих від скла променів настільки малі, що їх вдається прийняти і натомість міських акустичних шумів. Крім того, слід зазначити, що співвідношення між вартістю систем лазерного підслуховування і витрат на ефективний захист від них не на користь розглянутого методу добування інформації.

Отже, системи лазерного підслуховування, незважаючи на їх досить високі гіпотетичні можливості, мають обмежене застосування, особливо розвідкою комерційних структур.

Засоби високочастотного нав'язування

Видобування мовної інформації шляхом високочастотного нав'язування досягається за допомогою модуляції зовнішніх високогодинних радіо- або електричного сигналів первинним електричним сигналом, що несе мовну інформацію. Для забезпечення такої модуляції необхідно дистанційно подавати

зовнішнє електромагнітне поле або високочастотні електричні сигнали на елементи, параметри яких або струми, що протікають по них, змінюються під дією мовних сигналів.

В якості таких елементів можуть використовуватися різні порожнини з електропровідною поверхнею, що представляють собою високочастотні контури з розподіленими параметрами і обсяг яких змінюється під дією акустичної хвилі. Якщо частота такого контуру збігається з частотою нав'язування високочастотного, а поверхня порожнини знаходиться під впливом акустичної інформацією, то еквівалентний контур перевипромінює і модулює зовнішнє поле.

Найчастіше в якості модулюючого елемента застосовується нелінійний елемент, зокрема у схемах телефонного апарату. У цьому випадку високочастотне нав'язування забезпечується підведенням до телефонного апарату гармонійного високочастотного сигналу шляхом підключення до телефонного кабелю високочастотного генератора. В результаті взаємодії високочастотного коливання з мовними сигналами на нелінійних елементах телефонного апарату відбувається модуляція високочастотного коливання мовним низькочастотним сигналом і випромінювання промодульованого високочастотного коливання проводами телефонного апарату. Так як частота високочатотного нав'язування зловмиснику відома, то високочастотні модульовані сигнали можуть бути перехоплені його приймачем.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Особливості диктофонів для прихованого запису мовленнєвої інформації.
2. Переваги та недоліки цифрових диктофонів порівняно зі стрічкопротяжними диктофонами.
3. Класифікація заставних пристроїв.
4. Способи підвищення скритності заставних пристроїв.
5. Способи збільшення тривалості роботи заставних пристроїв.
6. Навести приклади технічної реалізації заставних пристроїв.
7. Принципи роботи засобів лазерного підслуховування, обмеження - при їх застосуванні.
8. Пояснити принцип високочастотного нав'язування.
9. Способи та засоби високочастотного нав'язування.

9 ХАРАКТЕРИСТИКИ РАДІОПРИЙМАЧІВ. ТЕХНІЧНІ ЗАСОБИ АНАЛІЗУ СИГНАЛІВ. ЗАСОБИ ВИЗНАЧЕННЯ КООРДИНАТ ДЖЕРЕЛ РАДІОСИГНАЛІВ. ЗАСОБИ ПЕРЕХОПЛЕННЯ ОПТИЧНИХ ТА ЕЛЕКТРИЧНИХ СИГНАЛІВ

Характеристики радіоприймачів

Можливості радіоприймача визначаються такими технічними характеристиками:

- діапазоном частот, що приймаються;
- чутливістю;
- вибірковістю;
- динамічним діапазоном;
- якістю відтворення сигналу (рівнями нелінійних і фазових спотворень);
- експлуатаційними параметрами.

Діапазон прийнятих частот забезпечується шириною смуги пропускання селективних елементів вхідних фільтрів та інтервалом частот гетеродина. Налаштування приймача на потрібний діапазон або піддіапазон частот здійснюється шляхом перемикання елементів вхідних контурів і контуру гетеродина, а налаштування на частоту всередині діапазону (піддіапазону) — шляхом зміни частоти гетеродина. У радіоприймачах все ширше як гетеродина використовується пристрій — синтезатор частот, що створює безліч (сітку) гармонічних коливань на стабілізованих фіксованих частотах з інтервалом, що відповідають кроку налаштування частоти приймача.

Чутливість радіоприймача оцінюється мінімальною потужністю або напругою сигналу на його вході, за якої рівень сигналу і відношення сигнал/шум на виході приймача забезпечують нормальну роботу кінцевих пристроїв (індикації та реєстрації). Така чутливість називається реальною. Гранична чутливість відповідає потужності (напрузі) вхідного сигналу, рівного потужності (напрузі) шумів вхідних ланцюгів радіоприймача. Інформація корисного сигналу потужністю менш потужності шумів радіоприймача

настільки сильно ними спотворюється, що передача інформації можлива тільки при кодуванні її спеціальними завадостійкими кодами.

У діапазонах дециметрових і більш коротких хвиль чутливість вимірюють у ватах або децибелах по відношенню до рівня 1 мВт (дБм), спектральної щільності в Вт/Гц або децибелах (стосовно Вт/Гц), на метрових і довших у мікровольтах (мкВ). Реальна чутливість сучасних професійних супергетеродинних приймачів дециметрових і сантиметрових хвиль становить 10^{-12} -10^{-15} Вт або -180 ... -200 дБ по відношенню до Вт/Гц, приймачів метрових і довших хвиль - 0,1-10 мкВ.

Вибірковість приймача оцінюється параметрами амплітудно-частотної характеристики (АЧХ) його селективних ланцюгів, що визначає залежність коефіцієнта посилення приймального тракту від частоти. Вибірковість приймача максимальна, коли його амплітудно-частотна характеристика повторює форму спектра сигналу, що приймається. У цьому випадку буде прийнято всі його спектральні складові, але не пропущено спектральні складові інших сигналів (перешкод). Практично реалізувати цю вимогу надзвичайно важко, оскільки спектр сигналів з окремою інформацією має порізану форму, що постійно змінюється, і існують великі технічні проблеми при формуванні амплітудно-частотної характеристики складної заданої форми. Як ідеальна АЧХ розглядається П-подібна форма з шириною, що дорівнює середній ширині спектра сигналу.

Вибірковість реального приймача оцінюється двома основними показниками: шириною смуги пропускання та коефіцієнтом прямокутності АЧХ радіоприймача, реальна форма якої має дзвоноподібний вигляд.

Ширина смуги пропускання вимірюється на рівні 0,7 за напругою, а коефіцієнт прямокутності оцінюється відношенням смуги пропускання на рівні 0,1 до смуги пропускання на рівні 0,7. Чим більш пологою є АЧХ радіоприймача, тим ширша смуга пропускання на рівні 0,1 по відношенню до рівня 0,7 і тим більша величина коефіцієнта прямокутності. Коефіцієнт пропускання дозволяє кількісно оцінити пологий характер амплітудно-частотної характеристики

радіоприймача . Чим ближче коефіцієнт прямокутності АЧХ до 1, тим крутіше її скати і тим менше перешкод «пролізе» по краях смуги пропускання. З метою зменшення потужності перешкод, що пройшли в тракт приймача, ширину його смуги пропускання встановлюють відповідною шириною спектра сигналу. У приймачах для прийому сигналів, що істотно відрізняються за шириною, наприклад мовлення і телеграфа, ширину смуг пропускання різних селективних ланцюгів змінюють шляхом комутації селективних елементів (котушок індуктивності, конденсаторів).

Так як активні елементи підсилювальних каскадів радіоприймача (транзистори, діоди та ін.) мають досить вузький інтервал значень вхідних сигналів, при яких забезпечується їх лінійне перетворення, то при обробці сигналів з амплітудою поза цими інтервалами виникають їх нелінійні спотворення, в результаті яких спотворюється інформація. Можливість приймача обробляти з допустимим рівнем нелінійних спотворень вхідні радіосигнали, що відрізняються за амплітудою, характеризується динамічним діапазоном. Величина динамічного діапазону оцінюється відношенням у децибелах максимального рівня до мінімального рівня сигналу, що приймається.

Для підвищення динамічного діапазону в сучасних радіоприймачах застосовується пристрій автоматичного регулювання посилення (АРУ) приймального тракту, що змінює його коефіцієнт посилення відповідно до рівня прийнятого сигналу.

Невідповідність амплітудно-частотної та фазової характеристик, динамічного діапазону радіоприймача поточним характеристикам сигналу призводять до його частотних, фазових і нелінійних спотворень і втрати інформації.

Частотні спотворення радіоприймачів викликаються неоднаковими змінами складових спектра вхідного сигналу. Через частотні спотворення сигнал на вході демодулятора спотворюється, що призводить до зміни інформації, що міститься в ньому.

Фазові спотворення сигналу виникають через порушення фазових співвідношень між окремими спектральними складовими сигналу при проходженні його ланцюгами тракту приймача.

Спотворення, що виявляються в появі в частотному спектрі вихідного сигналу додаткових складових, відсутні у вхідному сигналі, називаються нелінійними. Нелінійні спотворення викликають елементи радіоприймача, що мають нелінійну залежність між виходом і входом. Вони виникають при перевищенні відношення значень максимальної та мінімальної напруги сигналу на вході приймача до його динамічного діапазону. Ці види спотворень призводять до зміни інформаційних параметрів сигналу на вході демодулятора і, як наслідок, спотворення інформації після демодуляції.

Крім зазначених електричних характеристик можливості радіоприймачів оцінюються також за їх надійністю, оперативністю управління, видами електроживлення і споживаної потужності, маса-габаритним показниками.

Традиційні аналогові радіоприймачі поступово витісняються цифровими, в яких сигнал перетворюється на цифровий вигляд з подальшою його обробкою засобами обчислювальної техніки.

Великі можливості перехоплення радіосигналів у широкому діапазоні частот надають приймачі, що сканують. Особливостями цих радіоприймачів є:

• дуже швидка (електронна) перебудова частоти налаштування приймача в широкому діапазоні частот;

• наявність пристроїв (блоків) «пам'яті», яка запам'ятовує введені апріорі, а також у процесі пошуку, частоти радіосигналів, які не становлять або, навпаки, становлять інтерес для оператора;

• інформаційно-технічне сполучення на базі, як правило, інтерфейсу R – 232 S , приймача з комп'ютером, що забезпечує можливість передачі сигналів в комп'ютер для їх обробки та управління приймачем.

«Пам'ять» радіоприймача дозволяє запам'ятовувати частоти виявлених радіосигналів і не витрачати час на їх аналіз при подальшому скануванні

діапазону частот. У результаті різко скорочується час перегляду широкого діапазону частот.

У багатьох приймачах (AR-2700, AR-3000 A , AR-5000, AR-8000, IC-R 10, ICR-8500 та інші) передбачені інтерфейси сполучення з ПЕОМ, що дозволяє автоматизувати пошук сигналів за ознаками, що задаються, в тому числі, що використовують прості види технічного закриття.

На основі приймачів, що сканують та ПЕОМ створено автоматичні комплекси радіоконтролю (радіомоніторингу) приміщень. Комплекс працює під управлінням ПЕОМ, в реальному масштабі часу забезпечує відображення на екрані монітора амплітудно-частотних характеристик сигналів, їх реєстрацію на жорсткий диск з можливістю подальшої обробки. Прискорений перегляд діапазону частот забезпечується за допомогою програмно-апаратних засобів швидкого панорамного аналізу (на основі швидкого перетворення Фур'є).

Для перехоплення радіосигналів зі складною структурою, що застосовуються в стільниковому, пейджинговому та інших видах мобільного зв'язку, створюються спеціальні приймальні комплекси.

Перехоплення найбільш інформативних радіовипромінювань підсилювача та екрана монітора ПЕОМ можливе за допомогою телевізійного приймача широкого застосування з переробленими блоками рядкової та кадрової синхронізації. Прикладом спеціального засобу перехоплення побічних випромінювань ПЕОМ в діапазоні частот 25-2000 МГц може служити комплекс 4625-COM-INT , який має 100 каналів пам'яті для накопичення перехопленої інформації. Після обробки інформація відновлюється у вигляді, що відображається на екрані монітора ПЕОМ. Комплекс має високу чутливість (0,15 мкВ), має розміри 25 × 53 × 35 см і вагу 18 кг. Слід зазначити, що хоча при перехопленні радіовипромінювань від інших джерел побічних радіовипромінювань ПЕОМ (системного блоку, дисководів, принтера) не виникають серйозні проблеми, можливість добування інформації з перехоплених сигналів цих джерел перебільшена. Достовірні факти про реалізацію такої потенційної можливості відсутні.

Технічні засоби аналізу сигналів

Технічні засоби вимірювання ознак сигналу включають великий набір різних програмно-апаратних пристроїв і приладів, у тому числі пристрої панорамного огляду та аналізу спектра сигналу, селективні вольтметри, вимірювачі часових параметрів дискретних сигналів, визначники видів модуляції коду та ін.

Портативні аналізатори спектра при порівняно невеликих габаритах і вазі (9,5-20 кг) дозволяють приймати сигнали всіх діапазонів частот (30 Гц-40 ГГц) і аналізувати їхню тонку структуру з високою точністю. Похибка вимірювання частоти сигналу становить 15-210 Гц для частоти 1 Гц і 1-1,2 кГц – для частоти 10 ГГц, а похибка вимірювання амплітуди сигналу 1-3 дБ. Наприклад, цифрові аналізатори спектру HP8561E фірми «Hewlett Packard» вимірюють параметри сигналу в діапазоні частот 30 Гц-6,5 ГГц, а аналізатори спектру 2784 фірми «Tektonix» – у діапазоні 9 кГц-40 ГГц.

Селективні мікровольтметри дозволяють вимірювати амплітуди з похибкою 1 дБ і частоту з похибкою 10-100 Гц в діапазоні частот до 1-2 ГГц. Характеристики деяких із них наведені у табл. 9.1.

Таблиця 9.1 – Характеристики селективних мікровольтметрів

Тип приладу	Діапазон частот, МГц	Чутливість
SMV-8	26-1000	1 мкВ
SMV-11	0,01-30	0,1 мкВ
STV-401	26-300	2мкВ
ESH2	0,009-30	-30 дБ/мкВ
ESV	20-1300	-10 дБ/мкВ

Високоефективними та компактними засобами технічного аналізу є спеціальні прилади контролю радіозв'язку (радіотестери). До них відносяться "Stabilock 4015" (1,45-1000 МГц), "Stabilock 4032" (2-1000 МГц), HP 8920 A / D (0,4-1000 МГц) та ін. Чутливість зазначених приладів не більше 2 мкВ , а вага 13, 18,5 та 20 кг відповідно.

У складі радіотестера конструктивно об'єднані різні пристрої прийому та аналізу сигналів: аналізатор спектру, генератор сигналів, запам'ятовуючий осцилограф, пристрої демодуляції та декодування службових сигналів, інтерфейси поєднання з ПЕОМ і з принтером для реєстрації результатів вимірювань.

Засоби визначення координат джерел радіосигналів

Інформативними ознаками джерела радіосигналів є його координати. Для визначення координат застосовується радіоприймач з антеною, що повертається, діаграма спрямованості якої має гострий максимум або мінімум. Повертаючи антену у напрямі досягнення максимуму (мінімуму) сигналу на виході антени, визначають напрямок на джерело радіосигналу. Цей процес називають пеленгуванням, значення кутів між напрямками північ і джерело — пеленгами, а засіб пеленгування — радіопеленгатором, чи пеленгатором.

Координати джерела радіовипромінювань на місцевості розраховуються по двох або більше пеленгах з різних точок або по одному пеленгу і дальності від пеленгатора до джерела. Для розрахунку координат джерела радіовипромінювань необхідні також координати пеленгаторів.

Принципи пеленгування джерела радіосигналів двома пеленгаторами або одним рухомим з двох точок А і В ілюструються схемою на рис. 9.1.

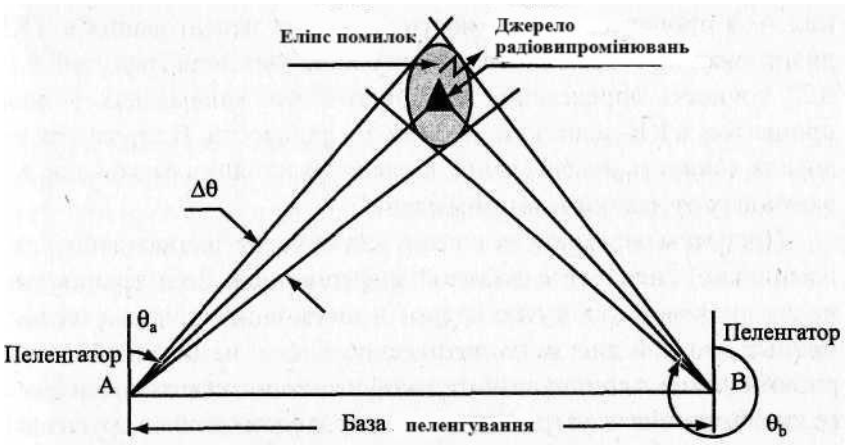


Рисунок 9.1 – Принципи пеленгування

Відстань між двома точками, з яких визначаються пеленги, називається базою пеленгування. Координати джерела відповідають точці перетину пеленгів на топографічній карті або розраховуються в результаті розв'язання тріангуляційної задачі.

Інструментальні помилки пеленгаторів, зміни умов поширення радіохвиль, вплив об'єктів поблизу джерел радіосигналів, відображення від яких спотворюють електромагнітне поле в антен пеленгаторів, похибки зчитування пеленгів викликають систематичні та випадкові помилки пеленгування. Кутові помилки пеленгування утворюють еліпс помилок (див. рис. 6.1), що окреслює межі площі на місцевості, всередині яких знаходиться джерело радіовипромінювань.

Для підвищення точності координат застосовують антени пеленгаторів з більшою крутизною зміни діаграми спрямованості від кута повороту антени, зменшують систематичні помилки пеленгаторів і похибки вимірювань, при розрахунках враховують умови поширення радіохвиль від джерела до пеленгаторів, збільшують кількість пеленгів. Більш високу точність пеленгування забезпечують фазові методи пеленгування на основі порівняння фаз, що припадають від джерела радіохвиль на рознесені в просторі антени пеленгаторів. Помилки пеленгування вимірюють у градусах, точність пеленгування — у відсотках від дальності. Точність пеленгування в УКХ діапазонах на відкритій місцевості становить частки градусів: 0,1°, 0,2°; точність визначення координат у цих діапазонах – частки відсотків, у КВ-діапазоні – 3-5% від дальності. У міських умовах точність пеленгування нижче через вплив радіохвиль, відбитих від будівель та автомобілів.

Процеси перехоплення включають також реєстрацію (запис, за споминання) сигналів з здобутою інформацією. Реєстрація сигналів здійснюється шляхом аудіо- та відеозапису, запису на магнітні стрічку та диски, на оптичні диски, на звичайному, електрохімічному, термочутливому та світлочутливому папері , запам'ятовування в пристроях напівпровідникового та

інших видів пам'яті, фотографування зображень на екранах моніторів ПЕОМ, телевізійних приймачів, осцилографів та спектроаналізаторів.

Засоби перехоплення оптичних та електричних сигналів

Видобування інформації на носіях у вигляді електричних та оптичних сигналів, що розповсюджуються по напрямних лініях (проводах та світлопроводах), здійснюється шляхом знімання сигналів з цих напрямних. Перехоплення здійснюється контактними та безконтактними способами. При контактному способі перехоплення частина енергії сигналу відводиться через фізичний контакт проводу або світлопроводу приймача зловмисника з проводом або світлопроводом, по яких поширюється сигнал з інформацією.

Підключення засобу перехоплення електричних сигналів до електричних дротів кабелю може бути послідовним або паралельним (рис. 9.2 а) та 9.2 б)).

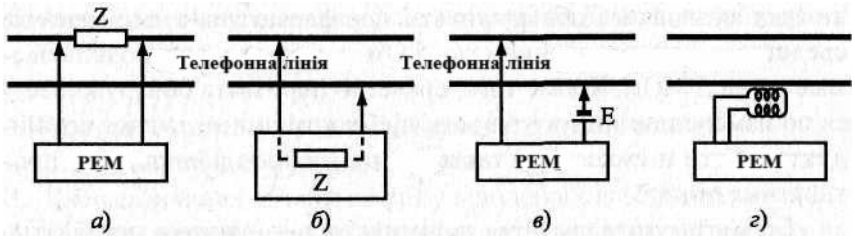


Рисунок 9.2 – Варіанти підключення засобів підслуховування (РЕМ) до телефонної лінії

При послідовному підключенні в розрив проводу лінії включається елемент приймача перехоплення — опір, сигнал з якого посилюється і відтворюється у формі, доступній для людини, аналізу або запису на аудіо- або відеомагнітофон. При паралельному способі засіб перехоплення підключається до дротів лінії паралельно. Найбільш простим засобом перехоплення сигналу з метою підслуховування мовної інформації в телефонних лініях зв'язку є трубка, яка підключається до проводів зі знятою ізоляцією телефонної лінії за допомогою контактів типу «крокодил». Послідовно або паралельно підключаються засоби перехоплення, які можна подати у вигляді

еквівалентного комплексного (активного і реактивного) опору Z. Тому контактне підключення зменшує енергію сигналу та змінює електричні параметри лінії, до якої підключено засіб перехоплення. Ці зміни є демаскуючими ознаками засобу перехоплення, за якими воно може бути виявлено. Імовірність виявлення залежить від величини зміни параметрів лінії та їх стабілізації.

Для зниження впливу підключеного засобу перехоплення зменшують величину включеного послідовно опору до одиниць Ома або збільшують вхідний опір, який паралельно підключається до одиниць Мома (мегаома). Зменшення напруги в лінії можна компенсувати подачею зовнішньої до додаткової напруги протилежного знака, як показано на рис. 9.2 в).

Сучасні засоби захисту інформації в провідних лініях дозволяють виявляти засоби, що послідовно включаються, з опором до 5 Ом і паралельно підключаються – до 5 МОм. Крім того, засіб перехоплення виявляється зі зміни індуктивності та ємності лінії за рахунок його індуктивності та ємності, а також зі зміни хвильового опору лінії.

Безконтактні засоби підключення – датчики перехоплюють сигнали, які випромінюють дроти при протіканні по них електричного струму. В цьому випадку засоби перехоплення не відбирають у сигналів енергію і виявляються значно гірше. Варіант підключення безконтактного диференціального індуктивного датчика показано на рис. 6.2 г). У котушках датчика наводять ЕРС поля, що випромінюються струмами в провідниках лінії, так і інших зовнішніх полів. З метою компенсації однакових за рівнем ЕРС зовнішніх полів котушки включені зустрічно. Оскільки одна з котушок знаходиться ближче до проводу лінії ЕРС, наведеної в ньому, її ЕРС більша за величиною, ніж ЕРС у котушці, що знаходиться подалі від проводу. Чутливість сучасних індуктивних пристроїв знімання інформації настільки велика, що з допомогою вдається зняти інформацію з броньованих кабелів.

Оскільки світло, що розповсюджується в оптичних кабелях, не виходить при дотриманні умов експлуатації за межі оболонки, то перехоплення оптичних сигналів можливе у двох варіантах:

- у місцях входу (виходу) оптичних сигналів у (із) кабелю;
- при деформації оптичного кабелю, при якій кут його вигину перевищує кут граничного відбиття променів світла в кабелі.

Перший варіант може бути реалізований шляхом заміни стандартних роз'ємів, що з'єднують кабелі із засобами або кабелі один з одним, на роз'єм з додатковим відведенням, до якого підключається оптичний приймач зловмисника. Під час отримання інформації за другим варіантом оптичний кабель згинається, поверхня місця вигину світло волокна захищається від ізоляції, і до нього притискається світлодіод. Хоча такий варіант теоретично можливий, практична його реалізація важка через, перш за все, складнощі у визначенні потрібного тонкого світло волокна серед безлічі інших волокон оптичного кабелю.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з

добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Типи радіоприймачів. Переваги супергетеродинних радіоприймачів як засобу перехоплення радіосигналів.

2. Параметри радіоприймачів. Відмінності граничної чутливості від реальної чутливості.

3. Особливості радіоприймачів.

4. Відмінності портативних аналізаторів спектру та радіоприймачів, що сканують.

5. Навести приклади використання селективних вольтметрів.

6. Методи визначення координат джерел радіовипромінювань.

7. Заходи, спрямовані на підвищення точності визначення координат джерел радіовипромінювань.

8. Варіанти підключення пристроїв, що підслухують, до телефонної лінії.

9. Способи добування інформації зі світло волокон.

10 ДЕМАСКУЮЧІ ОЗНАКИ СИГНАЛІВ. ДЕМАСКУЮЧІ ОЗНАКИ РЕЧОВИН

Демаскуючі ознаки сигналів

Поняття «сигнал» досить ємне і в загальному випадку позначає змінну фізичну величину, що однозначно відображає повідомлення. Часто люди під час передачі конфіденційної інформації обмінюються умовними сигналами, використовуючи при цьому різні предмети, написи, слова, звуки. Наприклад, незнайомі люди під час зустрічі обмінюються умовними фразами. У радіоелектроніці під сигналом розуміється змінна фізична величина.

По суті сигнал є носієм інформації, що поширюється в просторі, що міститься в значеннях його фізичних параметрів. До сигналів відносяться: власні (обумовлені тепловим рухом електронів, радіоактивні) випромінювання об'єктів, відображені від об'єктів поля та хвилі, електромагнітні поля та електричний струм від створених людиною джерел сигналів. **Інформація, що міститься у будь-якому сигналі, представлена значеннями його інформаційних параметрів.**

Класифікація сигналів представлена на рис. 10.1.

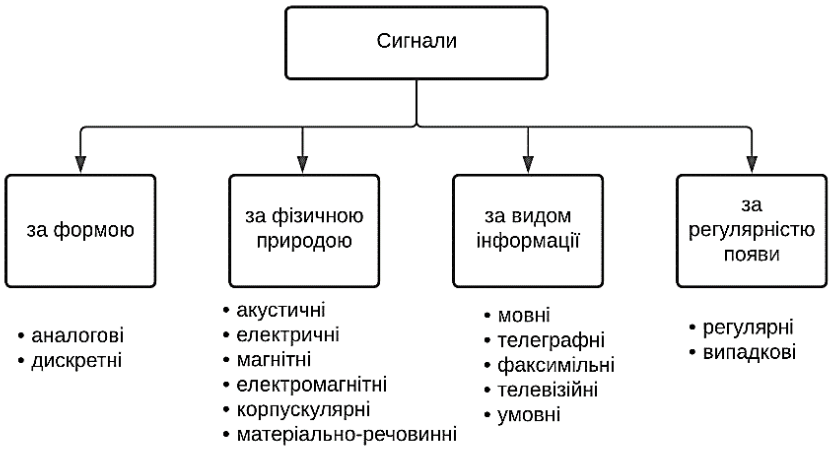


Рисунок 10.1 – Класифікація сигналів

До аналогових сигналів відносяться сигнали, рівень (амплітуди) яких може приймати довільні значення в певному для сигналу інтервалі.

Амплітуда простого і досить поширеного в природі гармонійного сигналу змінюється за синусоїдальним законом:

$$s(t) = Asin(\omega t + \varphi),$$

де A – амплітуда;

$\omega = 2\pi f$ – кругова частота коливання;

φ – фаза коливання.

Частота f вимірюється Гц і називається лінійною.

Більшість аналогових сигналів мають складнішу форму. Періодичні (повторювані через час $T_п$ – період) сигнали довільної форми можуть бути представлені відповідно до формули Фур'є у вигляді суми гармонійних коливань:

$$s(t) = C_0 + \sum_{.}^{n} C_k \cos(k\omega_1 t - \varphi_k),$$

де C_0 – постійна складова сигналу; C_k – амплітуда k-ї гармоніки сигналу (k = 1, 2, ..., n); $k\omega_1$ і φ_k – частота і фаза k-ї гармоніки сигналу; ω_1 – основна (1-ї гармоніки) частота.

Параметри ряду Фур'є обчислюються за відповідними формулами, наприклад. Ряд Фур'є є математичною моделлю періодичного сигналу, так само як будь-який колір може бути розкладений на складові червоного, зеленого і синього кольорів. Сукупність гармонійних (спектральних) складових сигналу утворює його **спектр.**

Амплітуда кожної спектральної складової характеризує енергію відповідної гармоніки основної частоти сигналу. Чим швидше змінюється амплітуда сигналу, то більше в його спектрі високочастотних гармонік. Різниця між максимальною і мінімальною частотами спектра сигналу, між якими зосереджена основна частина, наприклад 95% енергії, називається шириною **спектра** ΔF. Приклад графічного зображення спектра періодичного сигналу представлений на рис. 10.2.

Частоти складових спектру неперіодичного аналогового сигналу безперервно змінюються. При спостереженні спектра такого сигналу на екрані аналізатора спектра положення та рівень різних спектральних складових безперервно змінюються і спектр виглядає як суцільний.

Дуже зручною і широко застосовуваною є комплексна форма запису ряду Фур'є, яка відповідно до формули Ейлера визначає тригонометричні функції через показові: $\cos(x) = (e^{jx} + e^{-jx})/2$ і $\sin(x) = (e^{jx} - e^{-jx})/2j$. Подання сигналу у вигляді ряду Фур'є в комплексній формі має вигляд:

$$s(t) = \sum_{k=-n}^{k=n} C_k^* e^{jk\omega_1 t^X} = (e^{jx} - e^{-jx})/2j,$$

Як випливає з наведеного виразу, спектр у комплексній формі, що називається лінійчастим, симетричний щодо 0, а $C_k^* = \frac{1}{2} C_k$ для $k \neq 0$.

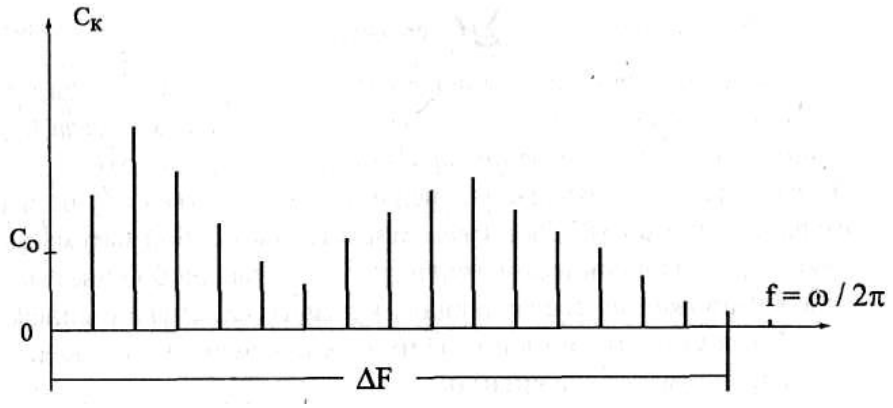


Рисунок 10.2 – Приклад спектра періодичного аналогового сигналу

Відповідно до зміни амплітуди аналогового сигналу змінюється його енергія або потужність, пропорційна квадрату амплітуди. Залежно від часу вимірювання енергії сигналу розрізняють **середню** та **миттєву потужність.** Десятковий логарифм відношення максимальної миттєвої потужності сигналу до мінімальної називається **динамічним діапазоном сигналу.** Динамічний діапазон промови диктора радіо і телебачення становить 25-30 дБ, вокального ансамблю - 45-65 дБ, а симфонічного оркестру досягає 70-95 дБ.

Аналоговий сигнал описується набором параметрів, що є його ознаками. До них відносяться:

- частота чи діапазон частот;
- амплітуда чи потужність сигналу;
- фаза сигналу;
- тривалість сигналу;
- вид модуляції;
- ширина діапазону сигналу;
- динамічний діапазон сигналу.

У дискретних сигналів амплітуда має кінцевий, наперед визначений набір значень. Найбільш широко застосовується двійковий (бінарний) дискретний сигнал: в ЕОМ, в телеграфії, при передачі даних. Інформаційні сигнали, що циркулюють в ЕОМ IBM PC, мають два рівні амплітуди: низький (L-рівень - 0 В) і високий (Н-рівень - 5 В). Осцилограма бінарного сигналу показано на рис. 1.3.

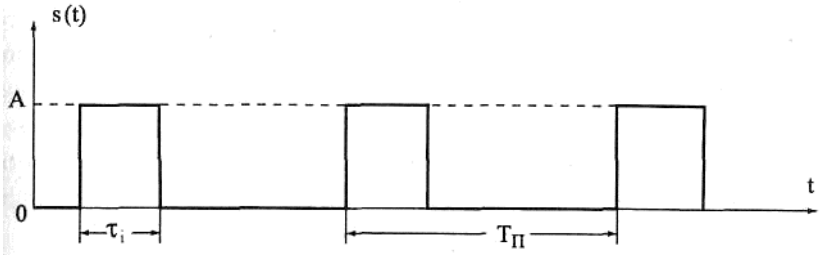


Рисунок 10.3 – Осцилограма бінарного сигналу

Дискретний сигнал характеризується наступними параметрами: амплітудою А і потужністю Р, тривалістю імпульсу τ_i , періодом $T_п$ або частотою $F_п = 1/T_п$ повторення імпульсів (для періодичних дискретних сигналів), шириною спектра сигналу $\Delta F_с$, шпаруватістю імпульсів $\alpha = T_п/\tau_і$.

Спектр дискретного періодичного сигналу містить нескінченну кількість гармонійок, що спадають за амплітудою. Вигляд спектру для бінарного періодичного сигналу ілюструється на рисунку 10.4.

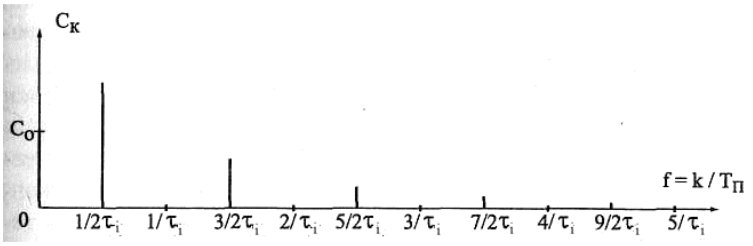


Рисунок 10.4 – Приклад спектру бінарного періодичного сигналу

Він характеризується такими властивостями:

- форма огинальної спектра описується функцією | $sinf\ /\ f$ |;
- амплітуда гармонік C_k має нульове значення у точках $k\ /\ \tau_i$, k =1, 2,…;
- в області частот спектра $(0\ -\ 1/\ \tau_i)$ розташовуються $\alpha\ -1$ гармонік;
- постійна складова сигналу дорівнює A/ α .

Враховуючи, що більша частина енергії сигналу зосереджена в області частот $0\ -\ 1/\ \tau_i$, ширина спектра бінарного періодичного сигналу приблизно оцінюється за формулою: $F_i\ \approx\ 1/\ \tau_i$. Ширина спектра телеграфного сигналу у вигляді двійкової послідовності , обмеженого третьою гармонікою , оцінюється величиною $\Delta F_{\text{Т}}$. Наприклад, ширина спектра телеграфного сигналу, що передається зі швидкістю 50 Бод, приблизно дорівнює 75 Гц.

При проходженні дискретних сигналів по реальних електричних ланцюгах радіотехнічних засобів у силу їх частотно-виборчих властивостей та обмеженої смуги пропускання спектр сигналів змінюється, внаслідок чого спотворюється їх форма та зменшується крутість імпульсів. Прямокутний імпульс набуває дзвоноподібної форми. В результаті цього розмивається межа між формами аналогового і дискретного сигналів. Спотворення форми та зменшення амплітуди імпульсних сигналів у проводах кабелів обмежують дальність їх передачі, наприклад, для забезпечення міжмашинного обміну даними в локальних мережах.

За фізичною природою сигнали можуть бути акустичними, електричними, магнітними, електромагнітними (у радіодіапазоні – радіосигнали), корпускулярними (у вигляді потоків елементарних частинок) і речовинними, наприклад, ароматні добавки в газ подають сигнал про його витік.

Сигнали по виду інформації, що передається, поділяються на мовні, телеграфні, телекодові, факсимільні, телевізійні, про радіоактивні випромінювання та умовні. Телеграфні та телекодові сигнали використовуються для передачі буквено-цифрової інформації з низькою та високою швидкістю відповідно. Факсимільні та телевізійні сигнали забезпечують передачу нерухомих та рухомих зображень. Сигнали радіоактивних випромінювань є ознаками радіоактивних речовин, що демаскують. Умовні сигнали несуть інформацію, зміст якої попередньо визначено між її джерелом і одержувачем, наприклад горщик з квіткою на підвіконні в літературних творах про розвідників — про провал явки.

Вигляд інформації, що міститься в сигналі, змінює його демаскуючі ознаки: форму, ширину спектра, частотний та динамічний діапазон. Наприклад, стандартний мовний сигнал, що передається по телефонній лінії, має ширину спектра 300-3400 Гц, звуковий - 16-20000 Гц, телевізійний - 6-8 МГц і т.д. Твір $B = \Delta F_c T_c$ називається **базою сигналу**. Якщо У ≈ 1, то сигнал вузькосмуговий, при > 1 — сигнал широкосмуговий .

За часом прояви сигнали можуть бути регулярними, час появи яких одержувачу інформації відомо, наприклад сигнали точного часу, і випадкові, коли цей час не відомий. Статистичні характеристики прояву випадкових сигналів у часі можуть являти собою досить інформативні ознаки джерел, що демаскують, насамперед, про їх належність і режими функціонування. Наприклад, поява в приміщенні радіосигналу під час ведення в ньому розмов може з досить високою ймовірністю служити демаскуючою ознакою заставного пристрою з акустичним автоматом .

За аналогією з демаскуючим об'єктом і з такою самою метою доцільно ввести поняття демаскуючий сигнал, факт виявлення якого може бути інформативною ознакою об'єкта захисту. Наприклад, побічні випромінювання на певній частоті конкретної радіостанції можуть служити її прямою, а іноді іменною ознакою. Під час війни за «почерком» роботи на ключі впізнавали радиста і виявляли радіогру, затіяну противником.

Демаскуючі ознаки речовин

Споживчі властивості продукції залежать не тільки від конструктивних і схемотехнічних рішень, а й від властивостей матеріалів (речовин), у тому числі з яких вона створюється. Тому склад, властивості та технологія отримання речовин із цими властивостями викликають великий інтерес у фахівців, а інформація про них може бути надзвичайно дорогою.

Речовиною називають матеріальні об'єкти в твердому, рідкому або газоподібному стані, що складаються з частинок одного або декількох хімічних елементів, що мають масу та об'єм. Класифікацію речовин наведено на рисунку 10.5.

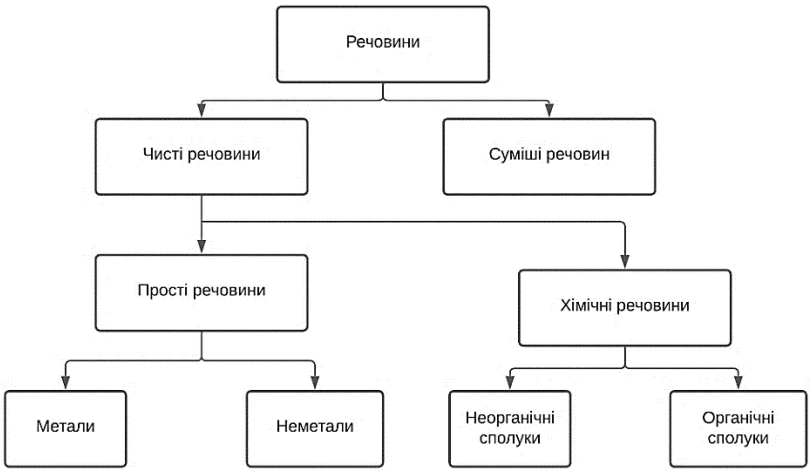


Рисунок 10.5 – Класифікація речовин

Речовини поділяються на прості та хімічні сполуки (складні). **Прості речовини** складаються з атомів одного хімічного елемента, **хімічні сполуки** — із різних елементів. Хімічний елемент утворюють атоми з однаковим позитивним зарядом ядра (з однаковим порядковим номером у періодичній системі Д. І. Менделєєва). Атоми хімічних елементів можуть існувати у вільному стані за дуже високої температури або у складі простих речовин. Властивості хімічних сполук не збігаються з властивостями хімічних елементів, що його утворюють.

За властивостями хімічні елементи умовно поділяються на **метали та** неметали. До металів відносяться прості речовини, що мають у звичайних умовах кристалічну структуру (крім ртуті), хорошу теплопровідність та електропровідність. У свою чергу метали за щільністю діляться на легкі (зі щільністю до 5 г/см^3) і важкі, за температурою плавлення – на легкоплавкі (з температурою плавлення до 1000°С) і тугоплавкі, за хімічною стійкістю до кислот - благородні (срібло , золото) і не благородні. Прості речовини, що не мають ознак металів, відносяться до неметалів.

Більшість сполук, до складу яких входить елемент вуглець, відносять до органічних. Але найпростіші сполуки вуглецю (оксиди — сполуки з вуглецю та кисню, вугільна кислота та її солі, деякі інші), а також не містять вуглець — до неорганічних сполук.

Для забезпечення безпеки інформації про речовини з новими властивостями важливо представляти ознаки, за якими зловмисник може відтворити речовину з новими властивостями. Класифікація основних ознак речовин представлена на рис. 10.6.

За фізичним складом речовини можуть бути однорідними **твердими** (кусковими, порошковими), **рідкими, газоподібними та неоднорідними,** у вигляді суспензій, емульсій тощо.

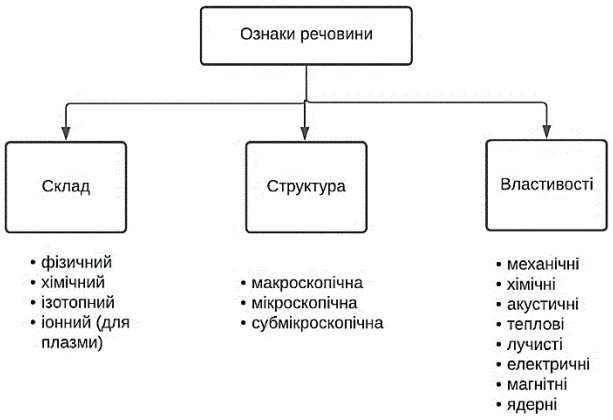


Рисунок 10.6 – Класифікація ознак речовин

За хімічним складом речовини поділяються на **органічні та неорганічні.** У свою чергу органічні речовини — на вуглеводні, кисневмісні та азотовмісні, неорганічні — на оксиди, кислоти, основи та солі.

Ізотопний склад характеризує стабільність або нестабільність ядер речовин або, іншими словами, наявність радіоактивних ізотопів у речовини, що розглядається.

Іонний склад речовини визначається при знаходженні його в іонізованому стані, що називається плазмою і виникає під дією високої температури або газового розряду (для газоподібних речовин).

Будова речовин описують на **макроскопічному, мікроскопічному та субмікроскопічному рівнях.** Воно може являти собою кристалічну решітку, набір макромолекул, молекул, субатомних частинок та атомів.

Механічні властивості речовин характеризують їхню міцність на стиск і розтяг, твердість, в'язкість, щільність, пористість, пластичність, змочуваність, непроникність і т.д.

Хімічні властивості речовини визначаються за наслідками взаємодії його з іншими речовинами.

Акустичні властивості визначають швидкість передачі та поглинання звуку в речовині.

Теплові властивості оцінюються за температурою фазових переходів з одного стану в інший, теплопровідності, теплоємності та ін.

Променисті (оптичні, рентгенівські та ін.) властивості речей описуються коефіцієнтами та спектральними характеристиками пропускання, відображення, заломлення, можливостями по дифракції, поляризації та інтерференції променів світла в інфрачервоному , видимому та ультрафіолетовому діапазонах, а також гамма-випромінювань.

Електропровідність, величини термо-ЕРС, окислювально-відновлювальні потенціали, потенціали іонізації, діелектрична та магнітна проникність тощо характеризують **електричні та магнітні** властивості речовини.

Ядерні властивості речовини оцінюються за масою ізотопів, масою та періодом напіврозпаду радіоактивних частинок та ін.

Ознаки, за якими можна виявити і розпізнати речовину , тобто визначити його склад, структуру та властивості, у суміші інших речовин, є **демаскуючими.** Демакскуючі ознаки нової речовини та технології її виготовлення містяться не тільки в кінцевому продукті, а й у вихідних і проміжних продуктах технологічного процесу, що застосовуються для отримання цієї речовини. Речовину, що містить демаскуючі речові ознаки об'єкта захисту або технологію його виготовлення, називають **демаскуючою речовиною.** Наприклад, нові парфуми відрізняються від прототипів складом. Демаскуючими ознаками нових парфумів є характеристики запаху, а демаскуючими речовинами — компоненти парфумів у певному співвідношенні. Оригінальні парфуми відрізняються від підробки також рядом ознак, у тому числі стійкістю збереження запаху. Стійкість запаху надають спеціальні дорогі добавки, що є демаскуючими речовинами оригіналу. В результаті фізико-хімічного аналізу демаскуючих речовин видобувається інформація про склад, структуру, властивості і технологію виготовлення продукції, яка може містити державну та комерційну таємницю.

Потенційні можливості виявлення та розпізнавання демаскуючих речовин залежать від їх концентрації в суміші до речовин, що бувають. Мінімально допустимі значення концентрації демаскуючих речовин, що виключають отримання зловмисниками інформації, що захищається, використовуються як норми при забезпеченні безпеки інформації про ознаки речовин .

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи, доведення порядку проведення заняття (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Сутність ознакового підходи до інформації.
2. Що є мовою ознак?
3. Чим первинні джерела інформації відрізняються від вторинних ?
4. Чим відрізняються джерела ознак інформації від джерел семантичної інформації?
5. Джерелом якого виду інформації є комп'ютер?
6. Навіщо створюються професійні мови? Відмінності мов національного спілкування від професійних.
7. Математична інтерпретація інформативності ознаки.
8. Відмінності ознак аналогових та дискретних сигналів.
9. Відмінність цінності інформації від ціни. Складові ціни інформації.
10. Чи старіють історичні документи?
11. Чому не можна об'єктивно виміряти кількість інформації? Чим вимірюють кількість інформації?
12. Чому кажуть, що якщо таємниця відома більш ніж одній людині , вона відома всім?
13. Первинні та вторинні носії інформації. До якого носія інформації належить людина?
14. Чому телефонний апарат не можна розглядати як джерело семантичної інформації? Які якості має мати джерело семантичної інформації?
15. Чим відрізняються прямі та непрямі джерела інформації?
16. Види модуляції гармонійного вагання.
17. Що знати для демодуляції сигналу?

11 ЗАСОБИ КОНТРОЛЮ ПРИМІЩЕНЬ НА ВІДСУТНІСТЬ ЗАКЛАДНИХ ПРИСТРОЇВ

Засоби контролю приміщень на відсутність заставних пристроїв

Для забезпечення безпеки інформації в приміщенні необхідний постійний контроль відсутності в ньому заставних пристроїв — «чистка» приміщень. Доцільними є такі види «чистки»:

- оперативний візуальний огляд приміщення;
- профілактичний періодичний контроль з використанням технічних засобів пошуку та локалізації заставних пристроїв;
- разовий контроль приміщення перед проведенням у ньому нарад з високим грифом секретності;
- перевірка приміщення після проведення капітального ремонту у ньому;
- перевірка різних нових предметів, що розміщуються в приміщенні представницьких подарунків, предметів інтер'єру, радіоелектронних засобів та інше;
- радіомоніторинг приміщення протягом робочого часу, особливо під час наради.

Частота та способи перевірки приміщень з метою виявлення в них заставних пристроїв залежать від їхньої категорії та порядку допуску в них сторонніх осіб. Найбільшої уваги служби безпеки заслуговують кабінети керівника та його найближчих заступників. Вони, з одного боку, часто ведуть розмови на конфіденційні теми, з другого — ці приміщення відвідують як співробітники організації, так і сторонні особи.

Сутність пошуку закладки шляхом візуального огляду полягає в ретельному огляді приміщення, предметів меблів (книжкової шафи та полиць, столів, стільців, крісел, дивана, та ін.), комп'ютера, радіо- та електропобутових пристроїв, телефонних апаратів, пристроїв гучномовного та диспетчерського зв'язку, картин на стінах , портьєр і жалюзі, інших предметів у приміщенні, в яких

у принципі можна заховати малогабаритний заставний пристрій. Огляд проводиться без розбирання предмета, що розглядається.

З метою забезпечення повноти візуального контролю доцільно проводити його за певною схемою, аналогічною схемою огляду місця події криміналістами: від дверей по або проти годинникової стрілки від периферії до центру приміщення. Під час огляду звертається увага на свіжі подряпини на шпалерах, біля мережевих та телефонних розеток та вимикачів освітлення, на стінах, гвинтах корпусу телефонного апарату, на пилові сліди зміщення картини або інших предметів, на відрізки проводів та інші сліди або незрозумілі на перший погляд предмети.

Для візуального огляду пошуку закладних пристроїв застосовують різне допоміжне устаткування. Це обладнання дозволяє підвищити ймовірність виявлення закладки під час візуального огляду приміщення. До такого обладнання належать ліхтарі, оглядові дзеркала та технічні ендоскопи.

Ліхтарі застосовуються для огляду місць, що погано освітлюються. Для вирішення цього завдання можуть використовуватися малогабаритні побутові ліхтарі. Але зручнішими є ліхтарі з покращеними світловими характеристиками.

Доглядові дзеркала застосовуються для огляду важкодоступних місць (меблевих ніш, вентиляційних отворів, під шафою, диваном і т. д.). Оглядовий комплект дзеркал «Джміль-2» включає 2 змінні дзеркала різних розмірів і конфігурації, телескопічну штангу з 5 колін сумарною довжиною 1550 мм і ліхтар підсвічування.

Дзеркала «CEM і CEM/ ILL» встановлюються на телескопічній рукоятці з 6 секцій завдовжки 140 см у розгорнутому та 35 см у закритому станах. Шнур на кінці рукоятки дозволяє варіювати кут огляду. На ручці закріплюється ліхтар. Вага доглядового дзеркала без ліхтаря — 519 г, з ліхтарем — у 2 рази більша.

Для пошуку малогабаритних закладок у місцях, які не проглядаються за допомогою дзеркал, можна застосовувати волоконно-оптичні технічні ендоскопи, які використовуються для спостереження важкодоступних місць.

Ефективність візуального огляду підвищується при контролі важкодоступних місць за допомогою індикаторів поля. Для забезпечення випромінювання радіозакладки з акустоавтоматом під час перевірки необхідно увімкнути радіо, телевізор або голосно розмовляти.

Візуальний оперативний огляд кабінету керівника організації перед початком або після завершення робочого дня цілі відповідно доручити його секретареві, оскільки він (вона) може виявити найшвидше нові предмети, що з'явилися в кабінеті, аж до появи нової авторучки на столі. Якщо перевірка проводиться ввечері, то кабінет має бути закритий на ніч, а запасні ключі перебувати під наглядом охорони.

Періодичний контроль передбачає поглиблену перевірку приміщення на наявність у ньому всіх видів закладок. За розв'язуваними завданнями періодичний контроль повинен забезпечувати виявлення та локалізацію заставних пристроїв, які не можуть бути виявлені під час візуального огляду. До таких закладок відносяться камуфльовані та малогабаритні некамуфльовані закладки, у тому числі закладки, що передають сигнали з проводів. Періодичність такого чищення встановлює керівник виходячи з цінності інформації, що захищається, яка залежить як від виду діяльності, так і етапу роботи. У типовому варіанті періодичний контроль може проводитися кілька разів на місяць, а також після кожного ремонту із залученням сторонніх осіб, за роботою яких важко організувати постійне спостереження. Набір технічних засобів, які використовуються при такому контролі, визначається можливістю організації щодо їх придбання.

Одним із найважливіших завдань служби безпеки при підготовці до відповідальної наради є перевірка приміщення, в якому вона повинна проводитись. Необхідність такої перевірки викликана потенційною можливістю визначення конкурентом або зловмисником часу та тематики наради та проведення ними операції з встановлення в кімнаті наради заставного пристрою, у тому числі дистанційно керованого.

Глибина «чистки» кімнати наради залежить від характеру використання приміщення в процесі функціонування організації. Якщо організація виділяє спеціальне приміщення для проведення нарад, яке постійно закрито на ключ, опечатане печаткою відповідальної особи, здається щодобово під охорону з відповідним записом у журналі, то контроль приміщення перед нарадою проводиться шляхом візуального огляду з використанням засобів аналізу випромінювань. Якщо нарада проводиться у службовому приміщенні (кабінеті керівника або його заступників, у робочих кімнатах співробітників), то обсяг перевірки відповідає обсягу періодичної «чистки».

Крім того, не можна виключити можливість пронесення закладки одним із учасників наради. Тому ефір біля виділеного приміщення доцільно контролювати і в ході наради за допомогою автоматизованих комплексів радіомоніторингу.

Проведення капітального ремонту приміщення пов'язане з загрозою встановлення в конструктивних або спеціально створених порожнинах у стінах (для проводів прихованої електропроводки, вимикачів та розеток електроживлення, виведення проводів для підключення люстри та ін.). Постійно контролювати працівників, які проводять ремонт, практично неможливо. Тому після капітального ремонту необхідно провести ретельний технічний контроль порожнього (до розміщення меблів та приладів) приміщення на відсутність у ньому заставних пристроїв. Доцільно меблі та прилади, що знаходяться в кабінеті, на час ремонту винести в інше приміщення, що закривається і опечатується. Якщо меблі і прилади залишені в приміщенні, що ремонтується, або винесені в коридор та приміщення не закривається, то перевіряється кожен предмет.

Достовірне виявлення закладок можливе при комплексному застосуванні апаратури, що виявляє прямі та непрямі демаскуючі ознаки: радіовипромінювання, порожнечі у стіні, металеві та нелінійні елементи. Враховуючи високу вартість набору такої апаратури та порівняно малу частоту

проведення такого ремонту, для перевірки приміщення після ремонту доцільно залучати спеціалізовані організації.

Виявлені заставні пристрої вилучаються або залишаються на місці передачі дезінформації. Якщо вилучення виявленої закладки пов'язане з необхідністю проведення досить серйозних будівельних робіт, то закладки, підключені до телефонної лінії або ланцюгів електроживлення, дешевше «спалити» високовольтними імпульсами, від'єднавши від лінії, що перевіряється, всі радіоелектронні засоби. Крім того, дроти телефонної лінії необхідно від'єднати від розподільної коробки.

Розпізнавання виявлених предметів з підозрою на закладення, а також перевірку представницьких та інших подарунків або виробів, що купуються за попереднім замовленням або з доставкою до місця експлуатації фірмою посередником, проводиться:

• шляхом механічного розбирання, якщо така допускається за умовами експлуатації або не передбачається подальше використання виявленого предмета;

• просвічуванням рентгенівськими променями нерозбірливих предметів;

• опроміненням полем нелінійного локатора предметів, які за своїм прямим функціональним призначенням не можуть містити напівпровідникові елементи;

• проведенням спеціальних досліджень радіоелектронної апаратури, насамперед ПЕОМ.

Розпізнати виявлений предмет незрозумілого на вигляд призначення, а не просто його викинути, важливо тому, що факт виявлення закладки представляє цінну інформацію про активні дії зловмисника і переходу загроз безпеки інформації зі стану потенційних у стан реальних.

Різного роду подарунки досліджуються без порушення їх товарного вигляду, що можливо шляхом виявлення випромінювань, дистанційного виявлення напівпровідникових елементів або просвітлення подарунка.

Спеціальні дослідження можуть проводитись фахівцями за наявності відповідної апаратури. Якщо не вдається виявити закладку по сигналу, що випромінюється нею, то проводиться неруйнівне розбирання досліджуваного засобу і аналіз кожного з його вузлів. Зовнішніми ознаками наявності закладки можуть бути:

- відмінності у технології монтажу однієї з деталей;
- відмінності у складі та розміщенні деталей досліджуваного вузла та ідентичного вузла іншого перевіреного засобу.

Оскільки виробництво сучасної радіоелектронної та обчислювальної техніки ґрунтується на високих технологіях, вимоги яких важко виконати на неспеціалізованому підприємстві, то порушення технології можуть бути виявлені фахівцями в процесі зовнішнього огляду. Наприклад, встановлення на друкованій платі засобу закладки у вигляді мікросхеми або камуфльованої деталі вимагатиме зміни топології або монтажу плати, відновлення її захисного покриття, що важко зробити без появи помітної межі шару лаку, зруйнованого при пайці.

У разі відсутності помітних порушень технології монтажу надійне виявлення сторонніх елементів забезпечує порівняння досліджуваного вузла або блоку з еталоном. Як зразок застосовують аналогічні вузли інших виробів, наприклад, відповідної плати засобу такого ж типу. Цей метод пов'язаний з додатковими витратами на придбання ідентичних засобів по інших торгових каналах. Тому доцільно при оснащенні організації технікою купувати однотипні кошти у різних продавців з подальшим порівнянням. Найбільш трудомістким є процес виявлення закладок на основі технічної документації досліджуваного засобу, отримання якої може представляти досить складне завдання.

Різноманітність технічних засобів виявлення та локалізації заставних пристроїв ставить перед службою безпеки організації проблему їх вибору при купівлі та ефективної експлуатації.

Вибір раціонального складу коштів для «чистки» приміщень визначається:

- цінністю інформації, що захищається у виділених приміщеннях;
- кількістю виділених приміщень;
- періодичністю проведення нарад та інших заходів з циркуляцією інформації, що захищається;
- фінансовим становищем організації.

"Існує велика кількість варіантів складання набору засобів для прибирання приміщень, які придбаває організація. Раціональний вибір передбачає такий склад коштів, придбання яких окупається протягом певного часу (наприклад, до 5 років) по відношенню до витрат на «чистку» приміщень з використанням орендованих коштів або залучення спеціалізованих організацій.

Склад засобів для виявлення заставних пристроїв у загальному випадку доцільно розділити на три варіанти: мінімальний, середній та максимальний.

Мінімальний набір включає:

- ліхтар для освітлення темних місць під час візуального пошуку;
- індикатор поля;
- портативний приймач, що сканує;
- керуючу програму;
- комп'ютер, встановлений у контрольованому приміщенні;
- аналізатор провідних ліній;
- ручний металодетектор.

Такий набір забезпечує:

- візуальний огляд приміщень з освітленням та контролем рівня електромагнітного поля у важкодоступних місцях;
- виявлення приймачем, що сканує, випромінювань закладок з локалізацією місць встановлення з допомогою індикатора поля;
- виявлення невипромінюючих закладок у місцях, що не містять металу (цегляних стінах, предметах меблів, шафах і т. д.).

Враховуючи, що у виділених приміщеннях зазвичай встановлюються ПЕОМ, доцільно поєднати її з приймачем, що сканує і, використовуючи

відповідне програмне забезпечення, проводити автоматизований аналіз радіообстановки в приміщенні. У цьому випадку досягається вища ймовірність виявлення радіозаставних пристроїв.

Але такий набір не забезпечує надійного виявлення заставних пристроїв, насамперед закладок дистанційно керованих, підключених до електромережі або розміщених у порожнинах залізобетонних стін.

Середній набір містить:

- електричний ліхтар;
- оглядовий комплект дзеркал;
- індикатор поля – частотомір;
- автоматизований комплекс радіомоніторингу приміщення;
- нелінійний локатор;
- аналізатор провідних ліній;
- ручний металодетектор;
- генератор перешкод у радіодіапазоні.

Такий склад забезпечує вищу ймовірність виявлення заставних пристроїв порівняно з можливістю попереднього варіанта (за рахунок радіомоніторингу приміщення).

У комплект **максимального набору,** крім зазначених для середнього варіанта, доцільно включити технічний ендоскоп та рентгенотелевізійну установку. Просвічування виявлених предметів невідомого призначення через високу вартість рентгенівських установок і рідкість таких подій можна проводити в спеціалізованих організаціях або взятим в оренду апаратом. Однак мати в організації власну рентгенівську установку корисно не тільки для розпізнавання заставних пристроїв, але й для просвічування кореспонденції, посилок чи інших предметів невідомого походження та призначення з метою виявлення вибухових речовин.

Класифікація засобів виявлення та локалізації закладних підслуховуючих пристроїв

Внаслідок постійної конкуренції між виробниками заставних пристроїв та засобів їх виявлення та локалізації на ринку існує безліч видів та типів технічних засобів, як тих, так і інших. Класифікація технічних засобів виявлення та локалізації заставних пристроїв наведена на рис. 11.1.

Рисунок 11.1 – Класифікація засобів виявлення та локалізації заставних пристроїв

Засоби радіоконтролю приміщення призначені для виявлення закладних пристроїв, що випромінюють радіохвилі під час їх пошуку. Для виявлення не випромінюючих при пошуку закладок — дистанційно керованих і передаючих сигналів по проводах застосовуються засоби, що реагують не на радіовипромінювання, а на інші ознаки закладок, що демаскують. Зрештою, засоби придушення заставних пристроїв забезпечують енергетичне приховування їх сигналів, порушення працездатності закладок або їхнє фізичне руйнування.

Враховуючи, що радіовипромінний закладки переважають на ринку заставних пристроїв, існують різноманітні засоби радіоконтролю обстежуваних приміщень: від найпростіших індикаторів електромагнітного поля до складних автоматизованих комплексів. Класифікація виявників радіовипромінювань закладних пристроїв вказано на рис. 11.2.

Рисунок 11.2 – Класифікація засобів виявлення випромінювань заставних пристроїв

Найпростішими та найдешевшими виявниками радіовипромінювань заставних пристроїв є **виявники електромагнітних полів.** Найбільш прості з них — індикатори поля, які світловим або звуковим сигналом інформують оператора про наявність у місці розташування антени індикатора електромагнітного поля з напругою вище фонової. Більш складні з них – частотоміри забезпечують, крім того, вимірювання частоти коливань поля. Але чутливість виявителей поля мала, тому з їх допомогою можна виявляти поля радіозакладок в безпосередній близькості від джерела випромінювання.

Істотно більшу чутливість мають **супергетеродинні побутові приймачі.** Однак можливості використання побутових радіоприймачів для пошуку радіозакладок обмежені радіомовним діапазоном та видами модуляції, що застосовуються в радіомовленні (АМ та ЧС). За допомогою перетворювачів (конверторів) можна перебудувати частотний діапазон побутового радіоприймача на частоту радіозакладки, якщо вона відома. Проте для пошуку радіозв'язкових пристроїв з невідомою частотою ті перебудовані побутові радіоприймачі є неефективними, оскільки вони здатні виявляти лише частоту закладення в обмеженому діапазоні частот.

Широкі можливості з виявлення радіозакладок мають **спеціальні приймачі.** Вони забезпечують пошук у діапазоні частот, що перекриває частоти багатьох застосовуваних радіозакладок — від часток МГц до одиниць ГГц.

Час перегляду діапазону частот вдається значно скоротити в радіоприймачах з електронною перебудовою часто ти і блоками пам'яті в так званих **приймачах, що сканують.** Блоки пам'яті цих приймачів дозволяють запам'ятовувати часто ти сигналів, про які достовірно відомо, що вони не належать до закладних пристроїв.

Інформаційно-технічне сполучення приймачів, що сканують з переносними комп'ютерами послужило технічною основою для створення **автоматизованих комплексів** для швидкого і надійного пошуку радіовипромінювальних пристроїв, що підслуховують. Час перегляду діапазону частот вдається значно скоротити в радіоприймачах з електронною перебудовою та блоками пам'яті. Блоки пам'яті цих приймачів дозволяють запам'ятати частоти сигналів, про які достовірно відомо, що вони не належать до закладних пристроїв. Для подальшого скорочення часу перегляду діапазону частот та підвищення ймовірності виявлення сигналів заставних пристроїв застосовують такі додаткові заходи:

- підвищують швидкість сканування до 100 МГц/с та більше;
- здійснюють аналогово-цифрову обробку сигналів на базі процесора швидкого перетворення Фур'є;
- виробляють автоматичний панорамний аналіз сигналів у діапазоні шириною до 15-20 МГц використовуючи ідентифікацію спектрограм поточних сигналів порівняно зі спектрограмами сигналів заставних пристроїв;
- використовують як ознаку ідентифікації сигналу заставного пристрою тестові акустичні сигнали, що випромінюються спеціальним акустичним генератором комплексу і ретранслюються заставним пристроєм;
- автоматично визначають координати заставного пристрою за часом запізнення на мембрані мікрофона тестових акустичних сигналів від акустичних колонок комплексу.

Але радіозакладки і закладки, що дистанційно керуються, передають інформацію по проводах, не виявляються апаратурою радіоконтролю. Для їх пошуку використовуються демаскуючі ознаки матеріалу конструкції та

елементів схеми заставного пристрою, а також ознаки сигналів, що розповсюджуються по проводах. З метою виявлення та локалізації таких закладок застосовуються або створюються спеціальні технічні засоби, класифікація яких наведена на рис. 11.3.

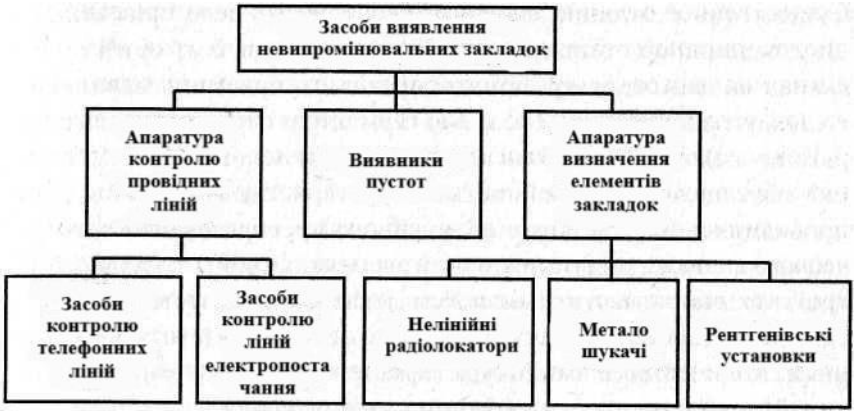


Рисунок 11.3 – Класифікація засобів виявлення закладок, що не випромінюють

Апаратура для контролю провідних ліній призначена для виявлення в них небезпечних сигналів та їх джерел, у тому числі заставних пристроїв. Оскільки основними напрямними лініями, якими передаються від заставних пристроїв електричні сигнали з інформацією, є телефонні лінії та ланцюги електроживлення, то відповідні засоби контролю включають прилади контролю телефонних ліній та ліній електроживлення.

Виявники порожнеч дозволяють виявляти можливі місця встановлення заставних пристроїв у порожнинах стін або інших дерев'яних чи цегляних конструкціях.

Велику групу утворюють засоби виявлення або локалізації заставних пристроїв за фізичними властивостями елементів електричної схеми або конструкції. Такими елементами є: напівпровідникові прилади, що застосовуються в будь-яких заставних пристроях, металеві деталі конструкції, елементи, що поглинають рентгенівські промені.

З цих засобів найбільш достовірні результати забезпечують засоби для виявлення напівпровідникових елементів за їх нелінійними властивостями — **нелінійні радіолокатори.** Принципи роботи нелінійних радіолокаторів близькі до принципів роботи радіолокаційних станцій, що широко застосовуються для радіолокаційного спостереження різних об'єктів. Істотна відмінність полягає в тому, що якщо приймач радіолокаційної станції приймає відбитий від об'єкта ехо-сигнал на частоті сигналу, що випромінюється, то приймач нелінійного локатора приймає 2-ю і 3-ю гармоніки перевипромінюваного (відбитого) сигналу. Поява у відбитому сигналі цих гармонік обумовлена нелінійністю характеристик вихід/вхід підлозі провідників. В результаті нелінійного перетворення електричного сигналу, що індукується в елементах схеми заставного пристрою високочастотним полем локатора, утворюється сигнал, у спектрі якого присутні крім основної частоти її гармоніки. Кількість і амплітуда гармонік залежить від характеру не лінійності і потужності електромагнітного поля.

Металодетектори (металошукачі) реагують на наявність у зоні пошуку електропровідних матеріалів, насамперед металів, і дозволяють виявляти корпуси або інші металеві елементи закладки.

Переносні рентгенівські установки застосовуються для просвітлення предметів, призначення яких не вдається виявити без їх розбирання, насамперед тоді, коли розбирання неможливе без руйнування знайденого предмета.

Апаратура радіоконтролю

Принципи роботи та основні характеристики засобів радіоконтролю полягають у наступному.

Виявник поля є широкосмуговим приймачем прямого посилення (у найпростішому випадку — детекторним) з телескопічною штиревою антеною. Посилені сигнали, що перевищують за рівнем вручну порогове значення, що встановлюється, подаються на світловий і звуковий індикатори, що інформують оператора про наявність у місці знаходження антени електромагнітного поля з

потужністю, що перевищує порогове значення. Перед пошуком закладки індикатор поля налаштовується на рівень фону в обстежуваному приміщенні. З цією метою оператор, перебуваючи в точці приміщення на відстані декількох метрів від можливих місць розміщення закладок, встановлює регулятор чутливості в таке положення, при якому індикатор знаходиться на межі спрацьовування. При наближенні індикатора поля до випромінюючої закладки напруженість електромагнітного поля зростає, підвищується рівень сигналу в антені і, відповідно, на вході індикатора поля. При перевищенні рівня порогового значення, що визначається положенням регулятора чутливості, індикатор спрацьовує, оповіщуючи про появу в наступній зоні електромагнітного поля потужністю, що перевищує потужність фону. З метою більшої інформативності світлових індикаторів їх виконують у сучасних виявниках поля у вигляді лінійки із 4-10 світлодіодів. Кожен наступний світлодіод випромінює світло у разі підвищення рівня електромагнітного поля.

У силу широкої смуги детекторного приймача, що істотно перевищує ширину спектра сигналу, чутливість цих засобів невелика і становить одиниці мВ. Крім того, в приміщенні за рахунок багаторазових перевідображень електромагнітних хвиль різних джерел утворюються «стоячі» хвилі, які можуть маскувати випромінювання заставного пристрою невеликої потужності та пучності яких можуть виявляти індикатори поля. Для підвищення можливостей індикатори поля доповнюються лічильниками частоти сигналу максимальної амплітуди, індикаторами рівня, малогабаритними гучномовцями для забезпечення «акустичної зав'язки». Остання досягається подачею посиленого демодульованого сигналу на гучномовець. При наближенні індикатора поля з гучномовцем, що випромінює шумовий акустичний шум, до скритно встановленого закладного пристрою цей акустичний сигнал ним перевипромінюється і після детектування і посилення озвучується гучномовцем. Виникає позитивний акустичний зворотний зв'язок, який призводить до різкого зростання гучності шумового акустичного сигналу в міру наближення до заставного пристрою. Такий індикатор поля дозволяє не тільки приблизно

визначити місцезнаходження джерела випромінювання підвищеної потужності, але й з високою достовірністю ідентифікувати заставний пристрій. Хоча ймовірність виявлення заставного пристрою за допомогою виявника поля невелика, простота схеми, низька вартість, малі розміри і маса виявників поля забезпечують їх широке застосування як засоби пошуку заставних радіовипромінюючих під час візуального огляду приміщення, особливо у важкодоступних місцях (під плінтусом, за картиною), у книжковій шафі та ін.).

У результаті подальшого розвитку індикаторів поля створено широкосмугові радіоприймальні пристрої — **інтерсептори з** автоматичним налаштуванням їх селективних елементів на радіосигнал з найбільшим рівнем. Чутливість інтерсепторів вища за чутливість детекторних індикаторів поля. Наприклад, інтерсептор AS 104 фірми Optoelectronics забезпечує прийом радіосигналів у смузі 10-1000 МГц, має активний преселектор зі смугою 4 МГц і посилення 30 дБ.

Принцип «захоплення» частоти радіосигналу з максимальним рівнем та подальшим аналізом його характеристик мікропроцесором покладено основою роботи сучасних **частотомірів.** Мікропроцесор записує сигнал з максимальним рівнем у внутрішню пам'ять, здійснює його цифрову фільтрацію, перевірку на стабільність та когерентність сигналу та вимірювання його частоти з точністю до одиниць кГц (2 кГц, 0,01% від номінального значення). Значення частоти у цифровій формі індукується на рідкокристалічному екрані.

Знання частоти дозволяє оператору грубо класифікувати радіосигнал, що приймається, за можливими його джерелами (радіо- або телевізійне мовлення, службовий зв'язок, стільниковий радіотелефонний зв'язок і т.д.) і підвищити оперативність «чистки» приміщення.

Побутові приймачі як засоби виявлення заставних пристроїв мають істотно більш високу чутливість, ніж індикатори поля та частотоміри, і дозволяють впевнено приймати радіосигнал закладки, якщо тільки його частота відповідає діапазону частот радіоприймача. Діапазони частот побутових радіоприймачів стандартизовані та становлять: для України та країн СНД 65,8-74 Мгц (УКВ1)

та 100-108 Мгц (УКВ2), відповідно до Міжнародного регламенту радіозв'язку 41-68 Мгц (УКВ1) та 87,5-108 МГц (УКХ2). Більшість сучасних побутових радіо приймачів випускаються у так званому розширеному діапазоні 65-108 МГц. Частка закладок з частотами випромінювань, що потрапляють у ці діапазони, мала і постійно зменшується. Враховуючи це, деякі побутові радіоприймачі оснащуються вбудованими або підключаються конверторами (перетворювачами) на діапазон зон випромінювань радіозакладок до 450-480 МГц. До таких приймачів належать, наприклад, AE 1490, Sony CFM-145. Вони мають додатковий діапазон робочих частот 460-480 МГц, чутливість їх становить 2-3 мкВ, що забезпечує прийом високочастотних ЧМ-сигналів радіозакладок.

Наочне уявлення про завантаження радіодіапазону, що полегшує пошук радіозаставних пристроїв, забезпечують **аналізатори спектру.** Широкий діапазон частот мають аналізатори спектру виробництва фірми Rohde & Schwarz ZWOB 2 (100 кГц-1,6 кГц), ZWOB 6 (100 кГц-2,7 ГГц), ZWOB 4 (100 кГц-2,3 ГГц), ZRMD (10 МГц-18 ГГц). Дещо меншими можливостями володіють аналізатори спектру виробництва країн СНД: СК4-61 (100 МГц-15 ГГц), С4-42 (40 МГц-17 ГГц), СК4-59 (10 кГц-0,3 ГГц), С4-47 (100 МГц-39,6 ГГц), СК4-83 (10 Гц-0,3 Гц), С4-9 (50 МГц-1,4 МГц),

Все більш широко для пошуку заставних пристроїв застосовуються **радіоприймачі, що сканують.** Ці приймачі мають високі електричні параметри в широкому діапазоні частот будівництва, що перекриває частоти радіовипромінювань наявних на ринку закладок. Приймачі, що сканують, автоматично послідовно налаштовуються на частоти радіосигналів у всьому діапазоні. Оператор, прослуховуючи звукові сигнали на виході приймача на кожній із частот, приймає рішення про продовження або припинення пошуку. Для продовження пошуку він натискає відповідну кнопку, подаючи пристрою управління приймача команду про перебудову на наступну частоту. У приймачах, що сканують, з пам'яттю в ній запам'ятовуються частоти радіосигналів, які не цікавлять оператора, що прискорює процес після пошуку.

Очевидно, що для того, щоб оператор міг виявити радіосигнал закладки, вона повинна передавати відомий акустичний сигнал. Для цього при пошуку закладок за допомогою побутових та радіоприймачів, що сканують, необхідно в приміщенні, що обстежується, випромінювати акустичний сигнал. Акустичний сигнал, крім того, «провокує» заставні пристрої, що автоматично включаються від голосів розмовляючих.

В умовах великого діапазону випромінювань радіозаставних пристроїв, що постійно розширюється, частота його послідовного перегляд навіть за допомогою приймачів, що сканують, займає кілька годин. В результаті тривалого пошуку оператор стомлюється і підвищується ймовірність пропуску їм випромінювання закладки. Для оперативного пошуку закладок застосовуються **спеціальні приймачі,** які містять крім приймача, що сканують, випромінювач акустичного тестового сигналу та мікропроцесор. Випромінювач акустичного сигналу імітує джерело акустичної інформації. Мікропроцесор виявляє радіо сигнали, на які налаштовується приймач, що сканує, за критерієм «свій-чужий» і швидко виявляє радіосигнал за кладки, якщо такий є. Наприклад, приймач РК 855 S генерує звуковий сигнал на частоті 2,1 кГц. Після виявлення свого сигналу він послідовно автоматично перевіряє його 4 рази, після чого подається сигнал оператору про виявлення закладки. Сканування всього діапазону частот займає близько 3-4 хвилин. Щоб уникнути перевантаження чутливих мікрофонів і надійно виявляти радіозакладки різних типів, гучність тестового акустичного сигналу поступово змінюється: 1,5-2 хв він випромінюється на повній гучності, потім той же час на половинній потужності. Апаратура розміщується в портфелі типу "дипломат", важить 4,9 кг.

Подальший розвиток спеціальних приймачів призвів до появи на ринку **автоматизованих програмно-апаратних комплексів** для пошуку засобів негласного знімання акустичної інформації. Типовий комплекс включає:

- радіоприймач, що сканує із широкосмуговими антенами;
- комутатор антен для комплексів, що контролюють декілька приміщень;
- комп'ютер типу Notebook чи мікропроцесор;

• спеціальне математичне та програмне забезпечення комплексу;

• контролер введення інформації з виходу радіоприймача в комп'ютер та формування тестового сигналу;

• перетворювач спектру;

• акустичний корелятор;

• блок живлення.

Комплекс за мінімальної участі оператора визначає і запам'ятовує рівні і частоти радіосигналів у контрольованому приміщенні, виявляє в результаті кореляційної обробки спектрограм випромінювання, що з'явилися, з використанням тестового акустичного сигналу розпізнає потайно встановлені в приміщенні радіомікрофони. Можливості комплексів розширюють також включенням до їх складу блоку контролю провідних ліній, що дозволяє виявляти підслуховувальні пристрої, підключені до проводів кабелів.

У комплект сучасних автоматизованих комплексів радіомоніторингу входить генератор прицільних перешкод. Він забезпечує можливість оперативно налаштовуватися на частоту виявленого заставного пристрою і придушувати його сигнали в умовах, коли немає часу на пошук і нейтралізацію заставного пристрою, наприклад, під час наради.

З метою скорочення часу перегляду діапазону частот за кілька хвилин аналіз сигналів у перспективних комплексах проводиться з урахуванням швидкого перетворення Фур'є.

Створення та застосування автоматизованих комплексів для безперервного радіомоніторингу приміщень з конфіденційною інформацією є найефективнішим напрямом розвитку засобів для комплексного захисту інформації від витоку радіоелектронним каналом.

Таке твердження ґрунтується на наступних передумовах :

• при безперервному контролі накопичується великий обсяг інформації про електромагнітну обстановку в захищеному приміщенні, що полегшує і прискорює процес виявлення нових джерел випромінювання;

• виявляються не тільки безперервно випромінюючі або включаються за

акустичним сигналом закладки, але і радіовипромінювання дистанційно керованих закладок в період їх активної роботи, тобто створюються передумови для боротьби із заставними пристроями в реальному масштабі часу;

• виявляються інформативні побічні випромінювання різних радіоелектронних засобів, для виявлення яких у зв'язку з більшою невизначеністю їх прояву та малою потужністю випромінювань потрібно провести більш ретельний аналіз радіообстановки в приміщенні.

Можливості автоматизованих комплексів визначаються не стільки технічними параметрами апаратури (більшість комплексів мають близькі параметри, оскільки комплектуються в основному однотипними радіоприймачами і ПЕОМ), скільки програмним забезпеченням. Програмні комплекси сучасних комплексів мають великі можливості: дозволяють накопичувати дані про радіоелектронну обстановку, аналізувати завантаження і спектральний склад радіосигналів у діапазоні частот радіоприймача, виявляти інформативні електромагнітні випромінювання від будь-яких РЕМ, оцінювати ефективність використання радіотехнічних засобів захисту інформації завдання.

Подальший розвиток автоматизованих комплексів передбачає:

• розширення видів закладних пристроїв;

• створення та включення до складу програмного забезпечення комплексу бази даних про заставні пристрої з інформаційними портретами випромінюваних сигналів для їх автоматичного виявлення та розпізнавання;

• розробку на базі програмно-апаратних засобів комплексів експертної системи з виявлення джерел витоку інформації в радіоелектронному каналі.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Класифікація засобів виявлення, локалізації та придушення заставних пристроїв.

2. Методи пошуку заставних радіовипромінюючих пристроїв.

3. Методи пошуку закладних пристроїв, що не випромінюють.

4. Методи пошуку дротових телефонних заставних пристроїв.

5. Види засобів, що використовуються для виявлення радіовипромінюючих закладних пристроїв.

6. Типовий склад автоматизованих комплексів радіомоніторингу.

7. Типовий склад засобів виявлення закладних пристроїв.

8. Види "чисток" приміщення від заставних пристроїв.

9. Основні ознаки заставних пристроїв, що використовуються для виявлення.

12 ДЖЕРЕЛА ЗАГРОЗ ВИПАДКОВИХ ВПЛИВІВ. ЧИННИКИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВІД ЗАГРОЗ ВПЛИВУ. ЧИННИКИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ЗАГРОЗ ВИТОКУ

Джерела загроз випадкових впливів

Джерела загроз випадкових впливів можуть бути:

• стихійні сили (пожежа, повінь, ураган, землетрус та ін.) та дії щодо їх нейтралізації;

• інженерні конструкції, ланцюги електропостачання, труби водо- та теплопостачання та інші елементи інфраструктури місць встановлення засобів інформаційного забезпечення, що прийшли в непридатний стан;

• технічні засоби збирання, обробки, передачі та зберігання інформації, що містять несправні елементи;

• програми, що містять помилки та віруси;

• некваліфіковані або погано виконуючі свої обов'язки оператори та персонал, що обслуговує програмно-апаратні засоби;

• гризуни та комахи у місцях розміщення інформаційних засобів.

Теоретичні питання протиборства двох сторін розглядаються теорією ігор. У ній розрізняють ігри людей між собою та ігри людей із природою. Якщо в іграх людей протиборчі сторони є активними і кожна з них вибирає стратегію , що погіршує положення протилежної сторони, то природа представляє пасивну сторону, дії якої розглядаються як випадкові.

Серед стихійних сил, які можуть у разі виникнення вплинути на носій інформації, найбільшу загрозу створює пожежа. Вона відбувається найчастіше, може повністю знищити носії інформації, його гасіння може супроводжуватися залитим місць пожежі водою та піною з не менш руйнівними для носія інформації наслідками.

Відповідно до статті 2 Кодексу цивільного захисту України пожежа – неконтрольований процес горіння, внаслідок якого знищується або пошкоджується майно, природні ресурси, а також виникають небезпечні

чинники, що створюють загрозу життю та здоров’ю людей, тварин, негативно впливають на навколишнє природне середовище;. Для виникнення горіння необхідна наявність «трикутника горіння»: пального середовища, джерела запалювання та окислювача.

Пальним середовищем можуть бути речовини в твердому, рідкому та газоподібному стані, у тому числі:

• горючі елементи несучих, що огороджують та інші конструктивні елементи частини будівлі (решетування горищ, віконні палітурки, двері);

• горючі елементи обладнання (шланги, дроти та ін.);

• сировина, матеріали, та горюча готова продукція;

• горюча начинка будівлі (меблі, матеріали та ін.).

Джерела запалювання - це гарячі або розжарені тіла, електричні розряди, що мають запас енергії і мають температуру, достатні для виникнення горіння. Типовими джерелами запалювання є:

• відкрите полум'я від багать, сірників, технологічного обладнання , паяльних ламп, газових пальників, ізоляції та ін.;

• тління горючих речовин (тютюну, торфу, бавовни в упаковці та ін.);

• нагріті поверхні технологічного обладнання, димових труб, нагрівальних елементів електроплит або електрочайників, струмопровідних жил кабелів при перевантаженні, опалювальних приладів та обладнання та ін.;

• екзотермічні процеси, що призводять до теплового, мікробіологічного та хімічного займання;

• малорозмірні сильно нагріті тіла у вигляді розпечених частинок, що виникають при електрогазозварювальних роботах і короткому замиканні ланцюгів електроживлення, тліючі тютюнові вироби, іскри від вогнищ, труб, автотранспорту та ін.;

• електричні іскри та дуги, що виникають в електрообладнанні при вимкненні, у нещільних контактах електричних з'єднань, статичної електрики, блискавки.

Окислювачем горіння є кисень повітря. Його зниження у замкнутому просторі (приміщенні) уповільнює процес горіння, а при зниженні кисню у повітрі нижче 15% горіння припиняється. Цю обставину покладено основою гасіння по жару шляхом зменшення доступу кисню до джерела горіння. Однак для ефективного гасіння пожежі необхідно, щоб вогнегасна речовина не вступала в реакції з пальним і не сприяла розвитку пожежі. Залежно від горючого середовища пожежі поділяються на такі класи:

- A — тверді горючі речовини (деревина, бавовна, торф, гумотехнічні вироби, пластмаси);
- B – вуглеводні, спирти, ефіри, альдегіди та кетони (нафта, бензин, жири, смоли, ацетон та ін.);
- C – горючі гази (метан, пропан, водень, ацетилен та ін.);
- D — легкі та лужні метали та їх сполуки (магній, калій, натрій, алюміній та ін.);
- E — радіо- та електричне обладнання під електричною напругою.

Джерелами загроз пожежі, повені, механічних руйнувань можуть бути не лише природні явища, а й плоди не сумлінної діяльності людини, яка своєчасно не ремонтує будівлі, приміщення та їхню інфраструктуру. Найчастішою причиною пожежі в будівлях називають коротке замикання між проводами електропроводки, яке виникає передусім через руйнування внаслідок старіння ізоляції проводів.

Проржавілі труби водо- і теплопостачання у разі їх прориву можуть спричинити повінь, особливо руйнівну у разі гарячої води.

Зворотною стороною ускладнення технічних засобів обробки, передачі та зберігання інформації, що постійно впроваджуються у всі сфери діяльності та життя людей, є проблема їх надійності. Приховані дефекти в елементах, повільно поточні хімічні процеси в місцях контакту та інші фактори все частіше проявляються зі зростанням складності радіоелектронних засобів. Хоча вживаються досить серйозні заходи щодо забезпечення їхньої діяльності, виявити всі приховані дефекти неможливо. Достатньо послатися на досвід

природи, яка для підтримки життя живої істоти постійно оновлює його клітини і створила в його організмі потужну імунну систему для боротьби з чужорідними вторгненнями. Але навіть ці заходи, недосяжні для технічних засобів, далеко не завжди рятують живу істоту від хвороб з тяжкими або трагічними наслідками.

Проблема ускладнюється ще тією обставиною, що спричинені несправностями збої в роботі складних радіоелектронних засобів не завжди оперативно виявляються, а можуть проявитися у вигляді відкладених помилок у роботі. Наприклад, збої в роботі процесора, викликані надмірним підвищенням його температури, можна помітити лише збільшення частоти його зависання. Враховуючи, що збій в апаратурі — це зміна електричного сигналу, зміна інформаційного сигналу призводить до зміни або навіть до знищення інформації, а зміна службового сигналу — до блокування інформації.

Аналогічна картина спостерігається із програмним забезпеченням. Витрачені зусилля на виправлення помилок у великих програмах можна порівняти з затратами на її розробку. Тому виробники програм підключають до їх тестування користувачів програм, збираючи від них виявлені ними помилки і вносячи виправлення в чергову версію. Крім помилок у програмі зміни та знищення інформації викликають віруси, які зі зростанням їх різновидів створюють серйозні загрози безпеці інформації.

Некваліфікований або недбайливий працівник є постійною загрозою для обслуговуваної ним апаратури та інформації, що циркулює в ній. Хоча він не має поганих намірів, але своїми діями він може завдати шкоди, не меншої, ніж від дій ворога. Приказка «добрими намірами вимощена дорога в пекло» відноситься і до таких людей. Досить згадати, що найстрашніша в історії людства чорнобильська катастрофа сталася через добрі наміри підвищити ефективність атомного реактора людьми, які не розглянули всі можливі наслідки експерименту.

Гризуни, що живуть у приміщеннях, де знаходяться засоби обробки інформації, можуть привести їх у такий стан, при якому знищується або

видозмінюється інформація, що зберігається в них. З історії перебудови відомі факти, коли щури, об'їдаючи ізоляцію проводів, перетворювали на металобрухт кораблі та літаки. Збої в роботі апаратури викликають навіть таргани, які із задоволенням влаштовують свої колонії в темних і теплих порожнечах радіоелектронної апаратури, змінюючи своїми тілами параметри її елементів і ланцюгів.

Так як витік інформації по акустичному, оптичному і радіоелектронному технічних каналах відбувається за допомогою сигналів, в інформаційні параметри яких записується інформація, що захищена, то джерелами загроз витоку є, перш за все, джерела сигналів у цих каналах.

Витік інформації на носіях у вигляді матеріальних тіл виникає при їх несанкціонованому та ненавмисному перенесенні до зловмисника. Слід відрізняти витік інформації на матеріальних тілах від несанкціонованого, але навмисного перенесення таких носіїв, що здійснюється зловмисником (агентом розвідки або завербованим нею співробітником). Наприклад, лист документа, забракований секретаркою під час друкування та викинутий нею в кошик для паперів, може бути перенесений прибиральницею в бак для відходів, вивезений на звалище за межі організації. На сміттєзвалищі він може бути виявлений зловмисником, який стежить за відходами організації. Цей процес поширення носія можна розглядати як витік інформації. Якщо ж цей документ цілеспрямовано виноситься з організації з метою добування з нього інформації, то інформація видобувається агентурними методами.

Чинники забезпечення захисту інформації від загроз впливу

Випадкові та навмисні впливи на джерела інформації, що охороняються системою технічного захисту інформації, можна подати у вигляді моделі, наведеної на рис. 12.1.

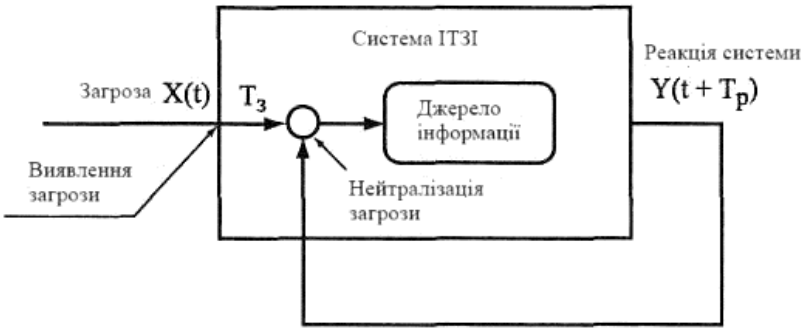


Рисунок 12.1 – Загрози впливу та реакція на них системи ІТЗІ

У поточний момент часу на вхід системи інформаційної технології захисту інформації (ІТЗІ) надходить k-я загроза впливу, яка у разі виявлення викликає через час реакції системи τ_p міру по нейтралізації цієї загрози. Нейтралізація загрози можлива лише в тому випадку, якщо джерело загрози за час реакції не досягне джерела інформації. В іншому випадку джерело загрози встигне вплинути на джерело інформації, внаслідок чого зміниться, буде знищена або викрадена інформація, що міститься в ньому. Те саме станеться, якщо загроза не буде виявлена. Можливий також варіант, коли виникне хибний сигнал про загрозу за її фактичної відсутності. Очевидно, що на безпеці інформації такий варіант відобразиться, але збільшаться витрати на заходи захисту, що знизить ефективність захисту.

Тимчасові показники системи ІТЗІ (час реакції та затримки) у загальному випадку величини випадкові, оскільки вони залежать від великої кількості факторів. Якщо загрозу, наприклад, створює зловмисник, який прагне проникнути до місця зберігання джерела інформації, то час його руху залежить від багатьох різних факторів. До них відносяться апріорні знання зловмисника про систему захисту (про кількість і міцність перешкод на шляху його руху, засоби охорони, нейтралізації вторгнень та ін.), кваліфікація зловмисника, можливості його технічних засобів, що використовуються для подолання цих перешкод і т. д.

Час реакції системи визначається організацією охорони, віддаленістю місця проникнення зловмисника від місця розміщення сил і засобів

нейтралізації загрози, часом виявлення зловмисника на території організації, швидкістю руху їх до місця знаходження зловмисника і т.д. апроксимувати нормальним законом.

Для забезпечення безпеки інформації необхідно або зменшувати час реакції системи до значення, меншого часу затримки зловмисника, або зміцнювати перешкоди шляхом збільшення часу затримки до значення, більшого часу реакції.

Оскільки час реакції людей залежить від їхньої психологічної установки на нейтралізацію загроз, то при підвищенні ймовірності помилкових тривог засобів охорони час реакції може також збільшитися, а ймовірність $P(\tau_p < \tau_з)$ — зменшитися.

З урахуванням розглянутих міркувань ймовірність $P_{ур}$ реалізації загрози впливу визначається як:

$$P_{ур} = P_{нв} + P_{ов}P(\tau_p < \tau_з),$$

де $P_{ов}$ і $P_{нв}$ — ймовірності виявлення та невиявлення джерела загрози відповідно.

Сумарна ймовірність впливу джерела загрози інформації на її джерело може бути оцінена відповідно до виразу:

$$P_{ур} = P_{ву}[P_{нв} + P_{ов}P(\tau_p < \tau_з)],$$

де $P_{ву}$ – ймовірність виникнення загрози впливу.

З аналізу цього виразу випливає, що для ефективного захисту інформації необхідно:

• збільшувати можливість виявлення загрози впливу;

• зменшувати ймовірність появи хибного сигналу про загрозу;

• зменшувати час реакції системи на загрозу з моменту виявлення її джерела;

• збільшувати час затримки джерела небезпеки.

Чинники забезпечення захисту інформації від загроз витоку інформації

Загрози витоку інформації з'являються, коли створюються передумови несанкціонованого поширення носія інформації від її джерела до зловмисника. Процес витоку можна розділити на два послідовні етапи: утворення каналу витоку і поширення по ньому інформації, що захищається. Так як у загальному випадку характеристики носіїв небезпечних сигналів каналів витоку інформації зловмиснику невідомі, то для зняття з них інформації він повинен виявити ці носії, встановити з ними контакт та отримати (зняти) з них інформацію. На ефективність захисту від витоку впливають такі фактори:

- умови утворення технічного каналу витоку інформації;
- час і витрати на пошук носія з інформацією, що захищається;
- ймовірність виявлення та розпізнавання носія інформації;
- відношення сигнал/шум на вході приймача сигналів (контраст зображення, концентрація демаскуючої речовини в пробі), що визначає якість інформації, що видобувається;
- ймовірність розпізнавання об'єкта захисту за ознаками, що здобуваються.

Умови утворення технічних каналів витоку інформації можуть бути для зловмисника випадковими або створюваними. Наприклад, побічне високочастотне випромінювання радіоелектронного засобу, розміщеного у виділеному приміщенні, не залежить від зловмисника. Тому частота випромінювання для зловмисника не відома і йому з метою використання цього випромінювання для підслуховування доведеться її шукати. Якщо зловмисник організує канал витоку інформації, наприклад, шляхом встановлення в приміщенні заставного пристрою, то частота відома, але невідомий час ведення закритих переговорів.

Пошук носія з інформацією залежно від його виду може бути у просторі та за частотою. Час і витрати на пошук носія інформації залежать від апріорних даних про його місце розташування та частоту. Якщо ці дані відсутні, пошук здійснюється шляхом сканування частини простору і діапазону частот, в межах

яких може знаходитися носій. Таким чином здійснюють сканування повітряного простору засобу ППО країни або частотного діапазону за позовом службою контролю ефіру незареєстрованого передавача. Очевидно, що тимчасові та інші витрати залежать від обсягу простору та діапазону частот, в яких здійснюється пошук, а також характеристик засобів пошуку. Наприклад, час пошуку випадкового небезпечного сигналу з мовленнєвою інформацією, що генерується побічним високочастотним випромінюванням в діапазоні від одиниць МГц до одиниць ГГц, може становити години. Пошук завершується виявленням та розпізнаванням носія.

Імовірність виявлення об'єкта розвідки визначається значенням твору безумовної ймовірності виявлення його ознак та умовної (після виявлення) ймовірності ідентифікації об'єкта за виявленими ознаками. Коли час прояву ознак менший за час пошуку об'єкта, то під час пошуку об'єкт може бути пропущений. Наприклад, якщо під час будівництва приймача зловмисник отримує сигнал побічного випромінювання на частоту з кабінету керівника організації, де відсутня мовна інформація, він може сприйняти цей сигнал як перешкоду і переорієнтувати радіоприймач. Імовірність виявлення ознак об'єкта розвідки $P_{оп}$ приблизно можна оцінити як відношення часу прояви ознак $\tau_{пп}$ до часу пошуку $T_{по}$, тобто $P_{оп} \approx \tau_{пп} / T_{по}$.

Виявлення об'єкта за його ознаками є процес порівняння безлічі поточних ознакових структур з еталонною ознаковою структурою об'єкта розвідки (об'єкта на дотримання, сигналу, речовини), а розпізнавання – шляхом порівняння поточної ознакової структури виявленого об'єкта з безліччю ознак, що описують його характеристики - тип, призначення, структуру, параметри та ін. (див. рис. 12.2).

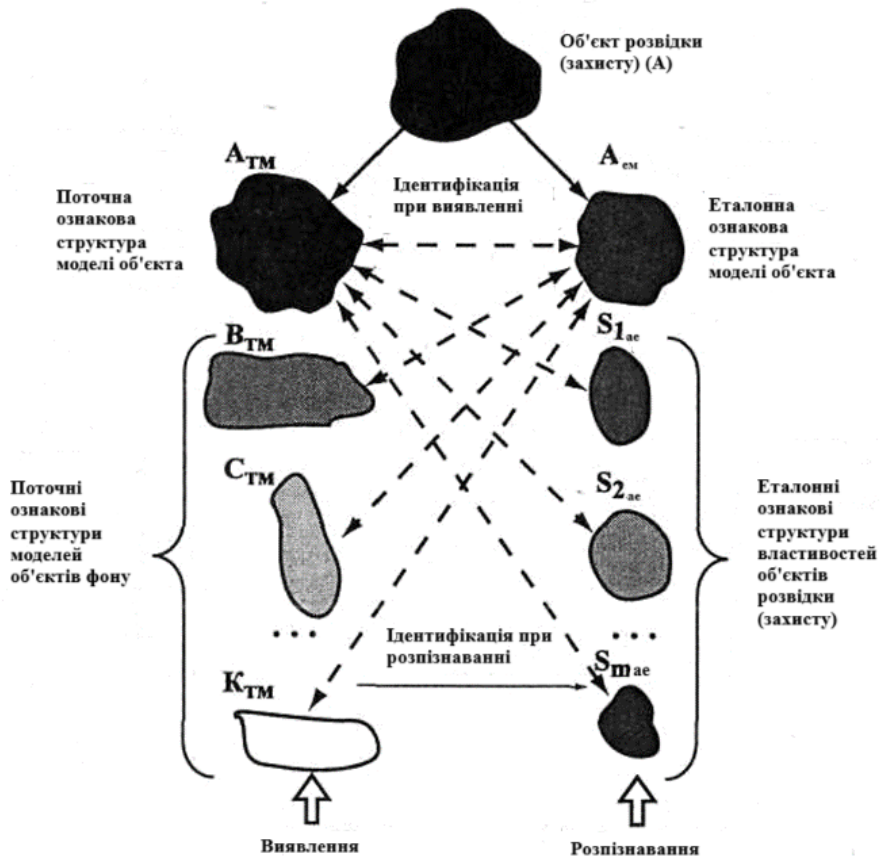


Рисунок 12.2 – Схема процедур виявлення та розпізнавання об'єктів

Об'єкт або його характеристики ідентифікуються по максимуму близькості поточних і еталонних ознакових структур аналізованих об'єктів та їх властивостей. Основу процесів виявлення та розпізнавання становить процедура **ідентифікації ознакових структур.**

Ідентифікація є процедурою визначення близькості двох ознакових структур (поточної та еталонної) з урахуванням інформативності їх ознак. Представимо інформаційну ємність поточної ознакової структури через $S_{\text{іт}}$, а інформаційну ємність еталонної структури через $S_{\text{іе}}$. Графічно близькість двох структур можна представити у вигляді перетину діаграм Венна із загальною областю $S_{\text{іте}}$. Коли діаграми Венна, що відповідають поточній та еталонній ознаковим структурам перетинаються, то міру їх близькості (коефіцієнт ідентичності) можна характеризувати як $К_{\text{ін}} = S_{\text{іте}} /(S_{\text{іт}} + S_{\text{іе}} - 2S_{\text{іте}})$ (рис. 5.3). Якщо всі ознаки структур збігаються, то структури ідентичні за ознаками, що розглядаються. Якщо всі ознаки однієї структури з меншою інформаційною

ємністю збігаються з ознаками іншої структури, що має велику інформаційну ємність, то міра близькості (коефіцієнт ідентичності $К_{ін}$) оцінюється відношенням меншої інформаційної ємності до більшої.

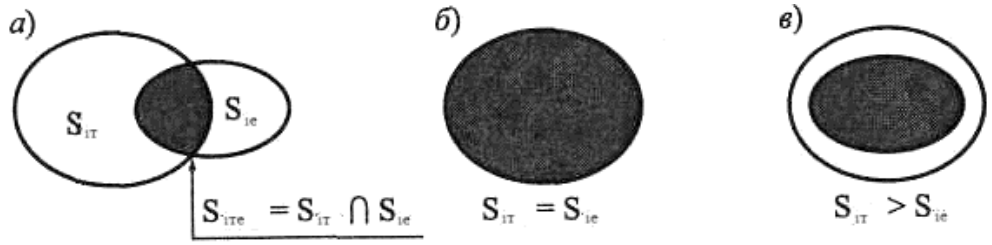


Рисунок 12.3 – Діаграми Венна поточної та еталонної ознакових структур

Отже, ймовірність ідентифікації структур залежить від кількості та інформативності загальних для них ознак, що демаскують. Позначимо ймовірність присутності до-го ознаки в еталонній ознаковій структурі через $Р_{ек}$, а через $Р_{тк}$ – ймовірність виявлення цієї ознаки при формуванні поточної ознакової структури. Імовірність наявності к-ї ознаки в обох структурах дорівнює добутку ймовірностей $Р_{ек}Р_{тк}$.

Інформативність к-ї ознаки ознакової структури залежить від помилки Δk її вимірювання на моделі об'єкта щодо значення цієї ознаки у реального об'єкта. При наближенні до першого залежність $I_к(\Delta k)$ можна подати у вигляді $I_к(\Delta k) = I_{ок} \exp(-\alpha_k \Delta k)$, де $I_{ок}$ – інформативність к-го ознаки об'єкта , α_k – коефіцієнт, що враховує вплив точності вимірювання ознаки на його інформативність. При нульовій помилці вимірювання ознаки інформативність ознаки ознакової структури відповідатиме інформативності цієї ознаки об'єкта. При збільшенні помилки виміру інформативність ознака прагне межі до нульового значення. Так як на ймовірність ідентифікації об'єкта впливає інформативність к-ї ознаки в еталонній і поточній ознакових структурах, то інформативність загальної для цих структур к-ї ознаки можна оцінити величиною $I_{ок} \exp[\alpha_k(\Delta_{ек} + \Delta_{тк})]$.

Отже, в загальному випадку ймовірність ідентифікації об'єкта за к-ою ознакою можна представити у вигляді функції, яка залежить від ймовірності $Р_{ек}$

включення до k-ї ознаки в еталонну ознакову структуру об'єкта, ймовірності $P_{тк}$ його виявлення та включення в поточну ознакову структуру, інформативності цього ознаки з урахуванням точності його вимірювання при утворенні еталонних та поточних ознакових структур:

$$Q_k = P_{ек} P_{тк} I_{ок} \exp\left[-\alpha_k(\Delta_{ек} + \Delta_{тк})\right],$$

Точність вимірювання ознак залежить від роздільної здатності засобу добування та співвідношення потужності носія у вигляді сигналу та потужності інших носіїв — перешкод. У теорії зв'язку визначені залежності ймовірності виявлення та розпізнавання сигналів від відношення сигнал/шум на вході приймача.

Імовірність ідентифікації об'єкта за m ознаками еталонної та поточної структур оцінюється відповідно до виразу :

$$Q_{\text{і}} \leq 1 - \prod_{k=1}^{m}(1 - Q_k),$$

де m – кількість загальних ознак для еталонної та поточної структур моделей об'єкта.

Знак враховує залежність ознак. Максимальне значення ймовірність ідентифікації набуває для незалежних ознак; мінімальна, рівна ймовірності ідентифікації за однією ознакою при коефіцієнті кореляції між ознаками, що дорівнює 1. Керуючи розглянутими факторами, можна забезпечити необхідний рівень безпеки інформації, при якому ймовірність ідентифікації об'єкта органом розвідки менша за нормативне значення.

Після виявлення та ідентифікації носія з інформацією, що захищається, її витік можливий, якщо відношення потужності (амплітуди) носія і потужності (амплітуди) перешкод на вході приймача зловмисника перевищує певне значення, що залежить від виду інформації та її носія, методу запису інформації на носій , вимог до якості інформації, що добувається, та ін. У явному вигляді це відношення визначається для акустичних і радіосигналів. Для оптичних сигналів ця величина відповідає абсолютному контрасту зображення об'єкта по відношенню до зображення тла. У речовому каналі витоку інформації, наприклад, після отримання проби з демаскуючою речовиною можливість

визначення речових ознак залежить від концентрації демаскуючої речовини в суміші проби.

Оскільки інформація, що добувається міститься в ознаках об'єкта, то можливість витоку інформації залежить від ймовірності розпізнавання цих ознак.

Таким чином, ризик (ймовірність) витоку інформації по технічному каналу можна оцінити у вигляді добутку ймовірностей наступних подій:

- утворення технічного каналу витоку інформації;
- виявлення внаслідок пошуку носія з інформацією;
- необхідного перевищення потужності носія стосовно потужності перешкод;
- розпізнавання об'єкта захисту (розвідки).

Отже, для запобігання витоку інформації по технічному каналу необхідно:

- усунути умови, що сприяють утворенню технічних каналів витоку інформації;
- приховати демаскуючі ознаки носія інформації в каналах витоку;
- зменшити потужність носія у місці можливого розміщення приймача зловмисника;
- зменшити інформативність ознакової структури об'єктів захисту.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.
2. Скласти термінологічний словник.
3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Основні фактори, що впливають на ефективність захисту інформації від загроз впливу.

2. Умови, які потрібно виконати для виявлення та розпізнавання об'єкта розвідки.

3. Чим відрізняються процедури виявлення від процедур розпізнавання ?

4. Основні напрямки технічного захисту інформації.

5. Методи технічного захисту інформації.

6. Чим відрізняється інженерний захист об'єктів від їхньої технічної охорони?

7. Умова ефективного забезпечення тимчасового приховування об'єктів - захисту.

8. Що являє собою інформаційна модель об'єкта захисту ?

9. Чим маскування відрізняється від дезінформування?

10. Умови ефективного енергетичного приховання.

13 ЗАСОБИ КОНТРОЛЮ ТЕЛЕФОННИХ ЛІНІЙ ТА ЛАНЦЮГІВ ЕЛЕКТРОЖИВЛЕННЯ

Засоби контролю телефонних ліній та ланцюгів електроживлення

Враховуючи поширення телефонів як засобів комунікацій та підвищений інтерес зловмисників до підслуховування телефонних розмов, велика увага при забезпеченні захисту інформації приділяється способам та засобам контролю телефонних ліній.

Способи контролю телефонних ліній засновані на тому, що будь-яке підключення до них викликає зміну електричних параметрів ліній і сигналів у них: напруги та струму в лінії, значень ємності та індуктивності лінії, активного та реактивного її опорів. Залежно від способу підключення пристрою, що підслуховує до телефонної лінії (послідовного — у розрив проводу телефонного кабелю або паралельного) вплив пристрою, що підслуховує може істотно відрізнятися. Оскільки заставний пристрій використовує енергію телефонної лінії, величина відбору потужності закладкою з телефонної лінії залежить від потужності передавача закладки та його коефіцієнта корисної дії. Найкращі можливості виявлення цих відхилень існують при опущеній трубці телефону. Це обумовлено тим, що в цьому стані в телефонну лінію подається постійна напруга 60 + 10% (для вітчизняних телефонних ліній) і 25-36 (для зарубіжних АТС). При піднятті трубки в лінію надходять від АТС дискретний сигнал, що перетворюється в телефонній трубці в довгий звук, а напруга в лінії зменшується до 12 В.

Для контролю телефонних ліній застосовуються такі пристрої:

• пристрої оповіщення світловим та звуковим сигналом про зменшення напруги в телефонній лінії, викликаному несанкціонованим підключенням засобів підслуховування до телефонної лінії;

• вимірники параметрів телефонних ліній (напруги, струму, ємнісного опору, хвильового опору та ін.), при відхиленні яких від номінального значення формується сигнал тривоги;

• «кабельні радари», що дозволяють виявляти неоднорідності телефонної лінії та вимірювати відстань до неоднорідності (асиметрії постійного струму в місцях підключення пристроїв, що підслуховують, обриву, короткого замикання та ін.).

Найпростіший пристрій контролю телефонних ліній є вимірювач напруги з індикацією зміни його значення від номінального, яке фіксується оператором в режимі налаштування обертанням регулятора на лицьовій панелі пристрою. Передбачається, що під час встановлення номінальної напруги до телефонної лінії пристрою, що підслуховує не підключено. Наприклад, аналізатор провідних ліній АПЛ-1 («Іній», асоціація «Конфідент») дозволяє виявляти підключення пристроїв, що підслуховують, включених послідовно і мають опір не менше 5 Ом, і підключених паралельно з опором не більше 1,5 мОм. На деяких подібних пристроях, наприклад ST 1, встановлюється стрілочний вимірювач напруги (вольтметр), в інших (АТ-23, Атол, АТЛ-2 та ін.) передбачено цифрове відображення значень напруги і струму на РК-дисплеї.

Як правило, подібні пристрої містять також фільтри для захисту від прослуховування за рахунок «мікрофонного ефекту» в елементах телефону та високочастотного нав'язування.

Але пристрої контролю телефонної мережі зі зміни напруги або струму в ній не забезпечують надійного виявлення підключаючих паралельно до лінії сучасних засобів підслуховування з вхідним опором більше одиниць МОм. Підвищення реальної чутливості пристроїв контролю обмежено нестабільністю параметрів лінії, коливаннями напруги джерел електроживлення на АТС та перешкодами в лінії. Для зниження ймовірності помилкових тривог у складніших подібних пристроях збільшують кількість вимірюваних характеристик лінії, передбачають можливість накопичення та статистичної обробки результатів вимірювань протягом досить тривалого часу як контрольованої лінії, так і близько розташованих. Наприклад, портативний аналізатор ССТО-1000 фірми CCS Commucation Control дозволяє проводити 6 типів контрольних перевірок телефонної лінії і може бути використаний для одночасної перевірки 25

телефонних пар, а аналізатор АТЛ-2 інформує про розмикання телефонної лінії на час більше 20 секунд, яке виникає при послідовному підключенні до неї пристрою, що підслуховує.

Так як будь-яке фізичне підключення до кабелю телефонної лінії створює в ній неоднорідність, від якої відбивається сигнал, що посилається в лінію, то за характером відображення і часу запізнення відбитого сигналу оцінюють вид неоднорідності і розраховують довжину ділянки лінії до неоднорідності (місця підключення). У приладі АПЛ-1 («Амулет») характер схеми пристрою, що підслуховує оцінюється по фігурі Лісажу, вид якої визначається зсувом фаз між напругою і струмом сигналу, що подається на вертикальні і горизонтальні пластини електронно-променевої трубки. Для виявлення неоднорідностей застосовують також випробувачі кабельних ліній Р5-А, Р5-5, Р5-8, Р5-9, Р5-10, Р5-13 та ін.

Засобами та програмним забезпеченням для виявлення та аналізу сигналів заставних пристроїв у провідних лініях оснащуються також перспективні автоматизовані комплекси. Наприклад, у мобільному автоматизованому комплексі «Крона 5» («Нелк») встановлений багатофункціональний конвертор, що дозволяє виявляти витік акустичної інформації по електромережі, телефонним та іншим провідним лініям в діапазоні частот 0,01-5 МГц, а також по інфрачервоному каналу.

Найбільш раціональним варіантом є поєднання в одному приладі функції виявлення несанкціонованого підключення до телефонної лінії та протидії підслуховуванню . Активна опір здійснюється шляхом лінійного зашумлення телефонної лінії.

Технічні засоби придушення сигналів заставних пристроїв

Іншу групу засобів активної боротьби із закладками утворюють генератори перешкод. Класифікація цих коштів наведено на рис. 13.1.

Виходи генератора лінійного зашумлення з'єднуються з проводами телефонної лінії та електромережі і в них подаються електричні сигнали, що

перекривають небезпечні сигнали за спектром та потужністю. Генератори просторового шуму підвищують рівень електромагнітних перешкод у приміщенні і, отже, на вході приймача зловмисника. Для ефективного придушення сигналу закладки рівень перешкоди у смузі спектра сигналу має у кілька разів перевищувати рівень сигналу.

Рисунок 13.1 – Класифікація засобів придушення заставних пристроїв

Енергетичне приховування інформації шляхом придушення (зниження відношення сигнал/шум нижче порогового значення) електричних і радіосигналів дозволяє забезпечити превентивний захист інформації без попереднього виявлення та локалізації заставних пристроїв. Можливі три способи придушення:

• зниження відношення сигнал/шум до безпечних для інформації значень шляхом просторового та лінійного зашумлення;

• впливу на заставні пристрої радіо- та електричними сигналами, що порушують задані режими роботи цих пристроїв;

• впливу на заставні пристрої, що викликають їх руйнування.

Для придушення сигналів заставних пристроїв застосовуються **загороджувальні** та **прицільні перешкоди.** Загороджувальні перешкоди мають ширину спектра, що перекриває частоти випромінювань переважної кількості заставних пристроїв, від часток до тисячі МГц. Потужність випромінювання вбирається у 20 Вт («Гном-3»).

Однак подібні генератори перешкод ефективно пригнічують радіосигнали закладки, якщо відношення потужності перешкоди і сигналу закладки в кілька

разів вище відношення ширини спектра перешкоди та сигналу. Ця вимога обумовлена тим, що потужність перешкоди «розмазується» по діапазону частот генератора перешкод, що в середньому становить близько 1000 МГц, і частку вузькосмугового сигналу закладки припадає лише незначна частина енергії перешкоди, якої не вистачає для ефективного спотворення інформаційних параметрів сигналу. Наприклад, один із пристроїв активного захисту інформації з підвищеною вихідною потужністю забезпечує максимальну потужність шуму в смузі ЧС-сигналу (150-200 кГц) близько 40 мВт при інтегральному значенні вихідної потужності генератора до 20 Вт. Але для вузькосмугового ЧС-сигналу потужність перешкоди в смузі сигналу становить частки і одиниці мВт, що недостатньо для придушення сигналів закладки . Враховуючи значну частку на ринку радіозакладок з потужністю випромінювання порядку 10-20 мВт і тенденцію звуження смуги їх кварцованих частот, застосування навіть досить потужних генераторів перешкод не гарантує запобігання витоку інформації. Нарощування потужності загороджувальної перешкоди обмежується вимогами з екологічної безпеки та електромагнітної сумісності випромінювань перешкод і сигналів радіомовлення та зв'язку в зашумлюваному просторі.

Проблеми електромагнітної сумісності немає при лінійному зашумленні. Завдання придушення сигналів закладок, що передаються по ланцюгах електроживлення, вирішується простим перевищенням спектральної щільності перешкоди над спектральною щільністю сигналу. Для придушення телефонних радіозакладок шляхом лінійного зашумлення спектр перешкоди не повинен співпадати зі спектром мовного сигналу, інакше перешкода заважатиме розмові абонентів. Як такі перешкоди застосовують аналогові та дискретні перешкодні сигнали, спектр яких вищий за спектр мовного сигналу. Найпростішим дискретним перешкодовим сигналом є меандр — послідовність прямокутних імпульсів зі шпаруватістю 2. Частоти сигналів підбираються такими, щоб вони проходили через селективні ланцюги мікрофонного підсилювача та модулятора заставного пристрою, але не сприймалися слуховою системою людини.

Сигнали-перешкоди з частотою вище 20 кГц змінюють режими роботи підключених до телефонної лінії заставних пристроїв, внаслідок чого змінюється частота та розширюється спектр їх випромінювань. Внаслідок цього погіршується перебірливість приймає мій зловмисником мови і зменшується в кілька разів дальність підслуховування.

Вплив перешкоди на паралельно підключений до телефонної лінії заставний пристрій проявляється в основному у зміні частоти випромінювання передавача, в результаті чого приймач , налаштований на номінальну частоту передавача закладки , не зможе прийняти сигнал. Наприклад, пристрій захисту телефонних ліній УЗТ-02 фірми «Нелк» генерує перешкодовий сигнал з максимальною амплітудою 35 В, який, впливаючи на елементи електронної схеми телефонної закладки, призводить до «розмивання» спектра сигналу, що випромінюється, і зниження співвідношення сигнал/шум на вході приймача зловмисника. Вплив перешкод порушує також роботу пристроїв автоматичного регулювання рівня запису та автоматичного включення диктофона голосом.

Один із способів фізичного пошкодження закладок, підключених до телефонної лінії та ліній електроживлення, подача до лінії коротких імпульсів великої амплітуди. Так як в схемах закладок застосовуються мініатюрні низьковольтні деталі (транзистори, конденсатори), то високовольтні імпульси їх пробивають і схема закладки виводиться з ладу. Наприклад, так званий руйнівник «жучків» РК 3320 (РК Electronic) посилає в лінію імпульси амплітудою до 4000 В і протягом 2-4 хв призводить до непрацездатного стану заставного пристрою. Вітчизняний випалювальник телефонних заставних пристроїв ПТЛ-1500 виводить з ладу заставні пристрої шляхом подачі в телефонну лінію імпульсів напругою 1600 В. Однак метод фізичного руйнування апаратних закладок не можна використовувати без відключення від телефонної лінії всіх радіоелектронних засобів, сучасних електронних телефонних апаратів факсів і т.д.).

Нелінійні локатори

На ринку є великий вибір моделей вітчизняних та зарубіжних нелінійних локаторів. Залежно від режиму випромінювання їх ділять на локатори з безперервним та імпульсним випромінюванням. Проникаюча глибина електромагнітної хвилі залежить від потужності та частоти випромінювання. Так як з підвищенням частоти коливань збільшується згасання електромагнітної хвилі в середовищі поширення, то рівень потужності перевідбитого сигналу тим вищий, чим нижча частота локатора. Але при більш низькій частоті погіршуються можливості локатора по локалізації місця знаходження нелінійності, так як при прийнятних розмірах його антени розширюється діаграма спрямованості.

Очевидно, що чим вище потужність випромінювання локатора, тим глибше проникає електромагнітна хвиля і тим більша ймовірність виявлення закладки, що вміщена в стіну. Але велика потужність випромінювання надає шкідливий вплив на оператора. Для забезпечення його безпеки максимальна потужність випромінювання локатора в безперервному режимі має перевищувати 3-5 Вт. При імпульсному режимі роботи локатора потужність імпульсу досягає 300 Вт при середній потужності, що не перевищує часток і одиниць Вт. Приймачі нелінійних локаторів забезпечують дальність виявлення напівпровідникових елементів 0,5-2 і більше метрів і точність визначення їх місцезнаходження — кілька см (наприклад, у локаторі «Джерельце» — 2 см). Максимальна глибина виявлення об'єктів у середовищі, що маскує становить десятки см, наприклад локатор «Циклон» виявляє радіоелектронні засоби в залізобетонних стінах завтовшки 50 см, в цегляних та дерев'яних стінах – до 70 см.

Вітчизняні локатори за своїми характеристиками не поступаються, а деякі зразки перевищують показники зарубіжних, а за вартістю в кілька разів дешевше. Локатор «Об» є повним аналогом зарубіжних зразків. Радіолокатори «Джерельце-ПМ», «Перехід», «Енвіс» мають додатковий режим аналізу за прийнятого від об'єкта сигналу, у тому числі можливість слухання модульованих

сигналів локатора, відображених від напівпровідникових елементів закладок. Принцип модуляції аналогічний до модуляції при високочастотному нав'язуванні. Локатор «Циклон» надає можливість роботи у двох режимах: у режимі пошуку та у режимі «сторожа». В останньому режимі дві антени встановлюються у проході контрольно-пропускного пункту організації або у дверному отворі приміщення, наприклад зали засідання. Цей локатор дозволяють дистанційно контролювати прихований внесення або винесення радіоелектронних засобів.

Нелінійні радіолокатори забезпечують високу ймовірність виявлення заставних пристроїв всіх типів, але є досить складними і дорогими засобами перевірки приміщення на відсутність в них заставних пристроїв.

Виявники порожнин, металодетектори та рентгенівські апарати

Ця група приладів використовує фізичні властивості середовища, в якому може розміщуватися заставний пристрій, або властивості елементів заставних пристроїв, незалежні від режиму їх роботи.

Так як у порожнечах суцільних середовищ (цегляних і бетонних стінах, дерев'яних конструкціях та ін.) можуть встановлюватися довгострокові дистанційно-керовані заставні пристрої, то виявлення та обстеження порожнеч проводиться при «чистці» приміщень.

У найпростішому випадку порожнечі в стіні або будь-якому іншому суцільному середовищі виявляються шляхом їх простукування. Порожнечі в суцільних середовищах змінюють характер поширення структурного звуку, внаслідок чого спектри звуків, що сприймаються слуховою системою людини, в суцільному середовищі і в порожнечі відрізняються.

Технічні засоби **виявлення порожнин** дозволяють підвищити достовірність виявлення порожнин. Як такі засоби можуть застосовуватися як різні ультразвукові прилади, зокрема медичного призначення, і спеціальні

виявники порожнеч. Спеціальні технічні засоби для виявлення порожнин використовують:

• відмінності у значеннях діелектричної проникності середовища та порожнечі;

• відмінності у значеннях теплопровідності повітря та суцільного середовища:

• відображення акустичних хвиль в ультразвуковому діапазоні від меж розділу "тверде середовище - повітря").

У порожнечі (повітря) діелектрична постійна близька до одиниці, для бетону, цегли, дерева вона значно більша. Діелектрики з різними значеннями діелектричної постійної по-різному деформують електричне поле, що створюється винахідником порожнечі. За зміною діелектричної індукції локалізується порожнеча. Так виявник порожнин «Кайма» виявляє порожнини в цегляних або бетонних стінах розміром 6×6×12 см та 6×6×25 см.

За допомогою ультразвукового томографа Д 1230 виявляються порожнечі об'ємом від 30 $см^3$ на глибині до 1м, ультразвукового товщинометра Д 1220 – глибиною до 50 см.

Ефективним засобом виявлення порожнин у стінах, нагрітих на кілька градусів вище температури повітря в приміщенні, є тепловізори. Чутливість тепловізорів, що охолоджуються, досягає 0,01 градуса за Цельсієм, неохолоджуваних — на порядок гірше. За рахунок різниці теплопровідності бетону або цегли стін і повітря межі порожнин з повітрям при нагріванні або охолодженні приміщення можуть спостерігатися на екрані тепловізору.

Переносний тепловізор ТН-3 («Спектр»), що не охолоджується, з вбудованим цифровим процесором забезпечує можливість спостереження на екрані зображень в ІЧ-діапазоні (8-13 мкм) об'єкта при мінімальній різниці температури елементів його поверхні 0,15 град. Комплект тепловізора містить камеру розміром 110×165×455 мм і масою 6 кг, малогабаритний монітор та блок живлення.

Металодетектори виявляють заставні пристрої за магнітними та електричними властивостями їх елементів. Будь-яка закладка містить струмопровідні елементи: резистори, індуктивності, з'єднувальні струмопровідники у навісному або мікромініатюрному виконанні, антену, корпус елементів живлення, металевий корпус закладки.

За принципом дії розрізняють **параметричні (пасивні)** та **індукційні (активні) металодетектори.** За конструкцією — **стаціонарні** та **ручні.** Для виявлення малих струмопровідних елементів застосовують в основному ручні металодетектори, які можна наблизити впритул до струмопровідного елемента.

У **параметричних металодетекторах** струмопровідні елементи, що потрапляють у зону дії пошукової рамки (котушки) діаметром 250-300 мм, змінюють її індуктивність. Ця котушка є індуктивністю коливального контуру пошукового генератора частота коливань якого становить 50-500 кГц. Чим вище частота коливань генератора, тим більше відхилення частоти генератора, тобто тим вище чутливість металодетектора, але одночасно сильніше позначається вплив середовища, особливо ґрунту землі. Тому в деяких типах металодетектора позовну котушку запитують негармонічним сигналом з частою тою 15-50 кГц, а для вимірювання відхилення частоти використовуються гармоніки коливання на частотах 500-1000 кГц.

Для вимірювання відхилення частоти коливань генератора параметричного металодетектора широко застосовується метод «бій» — явища, що виникає при складанні двох коливань з близькими частотами. Одне коливання із частотою, що змінюється, створюється пошуковим генератором, інше — еталонним генератором зі стабілізованою частотою. Частоти цих коливань встановлюються рівними за відсутності в зоні дії пошукової рамки сторонніх предметів. Частота биття надходить у вигляді тональної частоти на навушники та світловий індикатор. За частотою тону звукового сигналу та миготіння світлового індикатора можна локалізувати область, усередині якої знаходиться металевий предмет.

Перевагою параметричних металодетекторів є їх магнітна селективність — здатність розділяти метали за магнітними властивостями. Відомо, що чорні метали (чавун, сталь, кобальт, сплави) мають питому магнітну проникність μ » 1. У кольорових парамагнітних металів (титану, алюмінію, олова, платини та ін.) цей показник трохи більше 1, у діамагнітних металів (золота, міді, срібла, свинцю, цинку та ін.) — трохи менше 1. Отже, за знаком і величиною відхилення частоти пошукового генератора від номінального (нульового) значення можна судити про тип рамки металевого предмета, що потрапив у зону дії. Ця можливість розширила сферу застосування ручних металодетекторів, у тому числі для пошуку скарбів та активізувала дослідження щодо їх удосконалення в середині 90-х років XX ст.

Однак чутливість пасивних параметричних металодетекторів недостатня для виявлення металевих предметів, що знаходяться в не однорідному середовищі. Глибину виявлення збільшують **індукційні металодетектори.** Вони за допомогою спеціального генератора і випромінюючої пошукової рамки (котушки) створюють магнітне поле. Воно індукує в токопровідних предметах вихрові струми, що створюють вторинне поле. Це поле приймається іншою, вимірювальною, котушкою металодетектора. Сигнал, що наводиться в ньому, фільтрується, обробляється, посилюється і подається на звуковий і світловий індикатор металодетектора.

Розрізняють аналогові та імпульсні індукційні металодетектори. У аналогових металодетекторах на пошукову котушку надходить від генератора гармонійний сигнал із частотою 3-20 кГц. В імпульсних металодетекторах вдається за рахунок потужного короткого імпульсу, що подається в пошукову котушку, сформувати магнітне поле з напруженістю 100-1000 А/м, що на порядок перевищує напруженість поля аналогового металодетектора і проникає до 2 м ґрунту землі.

Оскільки магнітне поле пошукової котушки пронизує вимірювальну котушку, то основною технічною проблемою індукційних металодетекторів є компенсація сигналів, що водяться цим полем у вимірювальній котушці.

Компенсація сигналів у вимірювальній котушці досягається за рахунок взаємно перпендикулярного просторового розташування осей пошукової та вимірювальної котушок, використання компенсаційної котушки з параметрами, ідентичними параметрам вимірювальної, але з протилежним напрямком намотування проводу, а також шляхом відповідної обробки.

Характеристики сигналу у вимірювальній котушці залежать від розмірів струмопровідної поверхні об'єкта, її електропровідності магнітної проникності матеріалу та частоти поля. Виділення дуже слабких сигналів, що наводяться у вимірювальній котушці металодетектора вторинним полем дрібних металевих предметів, на тлі різних перешкод, а також компенсація перешкод потребує досить складних алгоритмів оптимальної обробки, що реалізуються мікропроцесорною технікою.

Для виявлення закладок застосовуються в основному ручні металодетектори. Вимірювальна та пошукова котушки в них можуть виконуватися у вигляді тороїда діаметром порядку 140-150 мм, укріпленого на корпусі ручки (АКА 7202) або безпосередньо в корпусі металодетектора (Мініскан). Металодетектор має звуковий та світловий індикатори, регулятор налаштування чутливості, живлення ручних металодетекторів від хімічних джерел струму. Проблема автоматичного підстроювання коефіцієнта посилення металодетектора під параметри середовища вирішується мікропроцесором. Максимальна чутливість металодетектора характеризується уламком голки довжиною 5 мм, що знаходиться в полі дії вимірювальної котушки. Вага ручних металодетекторів невелика: від 260 г до кількох кг.

Для інтерскопії предметів незрозумілого призначення застосовують переносні **рентгенівські установки.** Переносні рентгенівські установки бувають двох видів:

- флюороскопи з відображенням зображень на екрані перегляду приставки;
- рентгенотелевізійні установки.

Переносні флюороскопи складаються з випромінювача, пульта дистанційного керування, переглядової приставки з люмінесцентним екраном, акумуляторного блоку, зарядного пристрою, з'єднувальних кабелів та сумок для перенесення установки (транспортної упаковки). Обстежуваний предмет розміщується між випромінювачем і переглядовою приставкою на відстані біля 50 см від випромінювача та впритул до переглядової приставки.

Проникаюча здатність рентгенівських променів пропорційна анодній напрузі на рентгенівській трубці, яка досягає у деяких переносних флюороскопів 250 кВ. Наприклад, оглядова рентгенівська установка «Джміль-90/К» фірми «Флеш Електронікс» для забезпечення високої проникаючої здатності має анодну напругу 90 кВ. Вона просвічує сталеву пластину товщиною 2 мм, бетонну стіну товщиною до 100 мм, дозволяє розрізнити за перешкодою з алюмінію товщиною 3 мм два мідні дроти діаметром 0,2 мм, розташовані на відстані 1 мм один від одного. Робоче поле екрана приставки — коло діаметром 255 мм.

З метою підвищення безпеки оператора в сучасних переносних рентгенівських флюороскопах (наприклад, у флюороскопі Яуза-1 фірми «Novó») використовується люмінесцентний екран із запам'ятовуванням, що дозволяє розглядати зображення після вимкнення високої напруги. До складу таких комплексів включається спеціалізований термоконтейнер для стирання зображення із люмінесцентних екранів.

Зменшення потужності рентгенівського випромінювання та маса-габаритних характеристик установки досягається посиленням яскравості зображення екрану. Переносний рентгенівський флюороскоп ФП-1 («Спектр») з коефіцієнтом посилення яскравості екрана не менше 30000 має малі розміри (270×240×920 мм) та масу (3 кг). У той самий час розміри його флюороскопічного екрану становлять 250×250 мм. Додатково до нього постачається фото- або відеоприставка для документування зображень.

Для просвічування тонких предметів з неметалевими корпусами застосовують установки з радіоактивними ізотопами низької активності. Такі

установки компактні, прості в керуванні та безпечні. Наприклад, рентгенівська мікроустановка РК-990 з габаритами 220 × 210 мм і масою 1,7 кг просвічує об'єкт з розмірами до 63 × 87 мм.

У **рентгенотелевізійних** установках тіньове зображення перетворюється на телевізійне зображення на екрані віддаленого від випромінювача монітора. Наприклад, рентгенівський апарат «Джміль-експрес» забезпечує можливість спостереження зображення об'єкта як на екрані монітора, віддаленого до 2 м від рентгенівської установки, так і на екрані переглядової приставки комплексу «Джміль-90К». Розмір екрана рентгенотелевізійного перетворювача 360х480 мм. Ця установка дозволяє запам'ятовувати до 1000 зображень та забезпечує інформаційно-технічне сполучення з ПЕОМ.

Застосування рентгенівських установок для дослідження заставних пристроїв обмежується порівняно їх високою вартістю.

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Переваги та недоліки індикаторів поля.
2. Типовий склад автоматизованих комплексів радіомоніторингу.
3. Типи апаратури контролю провідних ліній.
4. Принципи роботи виявників порожнин.
5. Особливості нелінійних локаторів. Типи нелінійних локаторів.
6. Види та типи рентгенівських апаратів.
7. Принципи роботи параметричних та індукційних металодетекторів.
8. Типи засобів, що порушують роботу заставних пристроїв.

14 ЗАПОБІГАННЯ ВИТОКУ ІНФОРМАЦІЇ З ЛАНЦЮГІВ ЕЛЕКТРОЖИВЛЕННЯ ТА ЗАЗЕМЛЕННЯ

Запобігання витоку інформації з ланцюгів електроживлення та заземлення

Заходи щодо запобігання витоку інформації, що захищається, по ланцюгах електроживлення повинні:

• усунути проникнення сигналів з інформації, що захищається через блоки електроживлення основних технічних засобів і систем у ланцюзі електроживлення;

• знизити до допустимого рівня наведення НЧ і ВЧ випромінювань з інформацією, що захищається, на проводи ланцюгів електроживлення;

• придушити електричні сигнали у ланцюгах електроживлення до виходу їх із контрольованої зони.

Гальванічний зв'язок блоку живлення з інформаційними блоками РЕМ забезпечується через фільтр низької частоти, який зменшує до прийнятних значень рівень змінної складової напруги з виходу блоку живлення РЕМ. Чим менше величина змінної складової (пульсацій), тим вища якість блоку живлення. Однак зниження коефіцієнта пульсації зв'язано з різким зростанням витрат і збільшенням маса-габаритних характеристик блоку живлення. Для допустимих значень пульсації напруги типових блоків живлення смуга його пропускання ΔF становить близько 30 Гц. При такому значенні можливе пропускання оминаючого мовного сигналу в ланцюзі електроживлення. Зменшення ΔF досягається за допомогою:

- додаткових стабілізаторів у блоці живлення;
- мотор-генератору;
- автономних джерел живлення (акумуляторів, дизель-генераторів).

Мотор-генератор являє собою генератор електричного струму, обертання ротора якого забезпечується електричним двигуном, що живиться від первинного джерела змінного струму. Смуга пропускання мотор-генераторів становить частки Гц, що унеможливлює проникнення інформації від споживача

електроживлення до первинного джерела. Потужність мотор-генераторів становить від 8 до 75 кВА.

Для усунення проникнення небезпечних сигналів у ланцюзі електроживлення через ємнісні та індуктивні зв'язки блоку живлення застосовують способи, спрямовані на зниження значень цих паразитних зв'язків. З цією метою змінюють компонування (взаємне розташування) деталей блоку живлення таким чином, щоб мінімізувати довжину струмопровідних паралельних елементів та збільшити між ними відстань, а також екранують випромінюючі поля деталі. Найбільші паразитні зв'язки виникають між первинною і вторинною обмотками силового трансформатора, що перетворює напруги первинного джерела живлення на напруги живлення елементів схеми радіоелектронного засобу. З метою зниження їх до допустимих значень застосовують такі способи:

• первинну і вторинну обмотку розташовують на різних частинах магнітопроводу сердечника трансформатора;

• між первинною та вторинною обмотками, що розміщуються на одній котушці, встановлюється заземлений екран з мідної фольги товщиною не менше 0,2 мм;

• первинна обмотка розміщується у заземленому екрані;

• обмотки трансформатора розміщуються в індивідуальних заземних екранах, між якими також встановлюється заземлений екран.

У першому варіанті знижується ККД трансформатора через додаткове розсіювання магнітного поля первинної обмотки в повітрі. Екран перетворює паразитну ємність між проводами обмоток на паразитні ємності між цими проводами та заземленим екраном. Щоб виключити утворення навколо магнітопроводу короткозамкнутого витка з екрана, в якому в результаті магнітної індукції поля первинної обмотки виникнуть великі вихрові струми, між кінцями екрану залишають повітряний зазор з дуже високим опором.

З метою активного придушення небезпечних сигналів, що проникають через блоки живлення та наведені у проводах силових кабелів, ланцюги

електроживлення зашумлюють. Для цього подається на провід силових кабелів мовний шумовий сигнал, який формується з білового шуму за допомогою відповідних фільтрів.

Для виключення поширення високочастотних небезпечних сигналів по ланцюгах електроживлення при їх виведенні з виділених приміщень встановлюються фільтри живлення, лінійні та розв'язуючі мережеві фільтри. Фільтри живлення забезпечують затухання небезпечних сигналів смуги 20 кГц-1 ГГц щонайменше 60 дБ. Вони випускаються на робочу напругу 127-500 В і робочий струм 1-70 А. Так як у фільтрах, що пропускають великий струм, застосовуються індуктивності (котушки) з товстого дроту, то вага їх може досягати десятки кг.

Крім зазначених технічних заходів для запобігання витоку інформації з ланцюгів електроживлення необхідно забезпечити такі вимоги та рекомендації до системи електроживлення організації:

• електричні установки та кабелі повинні бути встановлені в межах контрольованої зони;

• на об'єктах 1-ї категорії електроживлення здійснюється від пристроїв, що забезпечують електромагнітну розв'язку мережі електроживлення від промислової електромережі, у тому числі сертифіковані агрегати безперебійного живлення, 4-провідні мережеві перешкодні фільтри, системи двигун-генератор;

• на об'єктах 2-ї категорії електроживлення проводиться через сертифіковані мережеві перешкододавлюючі фільтри та (або) проводиться активне зашумлення ланцюгів електроживлення;

• на об'єктах 3-ї категорії електроживлення може здійснюватися від підстанції в контрольованій зоні без додаткових заходів;

• на об'єктах 2-ї та 3-ї категорій допускається електроживлення від трансформаторної підстанції, розміщеної за межами контрольованої зони, але при використанні сертифікованих 4-провідних перешкододавлюючих фільтрів або систем активного зашумлення;

• подача електроенергії від трансформаторної підстанції до силових щитів проводиться екранованим силовим кабелем, а розподільні пристрої та силові щити закриваються на замок і опечатуються.

Заходи щодо запобігання витоку інформації щодо ланцюгів заземлення спрямовані на зниження величини паразитного гальванічного зв'язку між заземлюваними радіоелектронними засобами та зменшенням площі магнітних рамок, що утворюються ланцюгами заземлення. При цьому ці заходи не повинні збільшувати опір ланцюгів заземлення.

При виборі схеми заземлення слід враховувати, що найбільш часто використовуване послідовне заземлення (рис. 14.1 а)) має найбільший коефіцієнт гальванічного паразитного зв'язку. Низькочастотні засоби, розміщені на невеликій відстані один від одного, рекомендується заземлювати в одній точці (рис. 14.1 б)), в інших випадках доцільно застосовувати багатоточкове заземлення (рис. 14.1 в)).

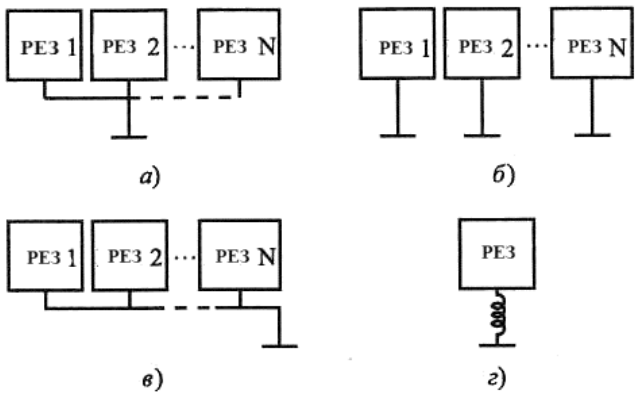


Рисунок 14.1 – Типи заземлення радіоелектронних засобів

З метою виключення зняття інформації з струмів, що розтікаються в землі, заземлювачі розміщуються всередині контрольованої зони на видаленні не менше 2-3 м від її кордону (огорожі).

Засоби запобігання витоку інформації через ПЕМІН

Засоби захисту інформації від витоку через побічні електромагнітні випромінювання та наведення повинні задовольняти наступним вимогам:

а) Небезпечні сигнали, які можуть містити конфіденційну інформацію, повинні бути ослаблені до рівня, що виключає знімання з них інформації на межі контрольованої зони. Враховуючи, що чутливість сучасних приймачів становить частки мкВ, то рівень небезпечних сигналів на вході приймача, розташованого на межі контрольованої зони, не повинен перевищувати ці значення. Якщо рівні небезпечних сигналів на виході пристроїв, що створюють їх, наприклад акустоелектричних перетворювачів, складають одиниці і десятки мВ, то засоби захисту повинні забезпечити послаблення амплітуд небезпечних сигналів на 100-120 дБ.

б) Засоби захисту не повинні вносити помітних спотворень у роботу функціональних пристроїв, які використовуються співробітниками організації та ускладнювати процес користування ними.

Оскільки небезпечні сигнали є побічним продуктом роботи різних радіоелектронних засобів і виникають випадковим чином, а до їх джерел, як правило, відсутній прямий доступ (без порушення конструкції), то можливості застосування способів технічного закриття або шифрування мови в цих електромагнітних каналах витоку відсутні. Основний спосіб захисту інформації в них – енергетичне приховування.

Засоби придушення небезпечних сигналів акустоелектричних перетворювачів

Засоби придушення небезпечних сигналів розміщуються в радіоелектронному засобі або частіше включаються між захищеним засобом і проводами відповідних інформаційних ліній. Найпростішим пристроєм відключення від лінії є вимикач (тумблер), що додатково встановлюється на телефонному апараті. Більш складні пристрої відключення містять електромагнітні реле, які підключають телефонний апарат тільки при піднятті трубки або надходженні на апарат з покладеною трубкою сигналу виклику від іншого абонента.

Найпростішим фільтром є конденсатор, що встановлюється у дзвінковий ланцюг телефонних апаратів застарілої (з електромеханічним дзвінком) конструкції (рис. 14.2). Ємність конденсатора вибирається такої величини, щоб зашунтувати небезпечні сигнали, що виникають в обмотці котушки якоря дзвінкового ланцюга в результаті впливу на якір акустичних хвиль у звуковому діапазоні частот. Цей конденсатор надає сигнали виклику частотою 25 Гц слабкий вплив, так як частоти мовного сигналу значно вище.

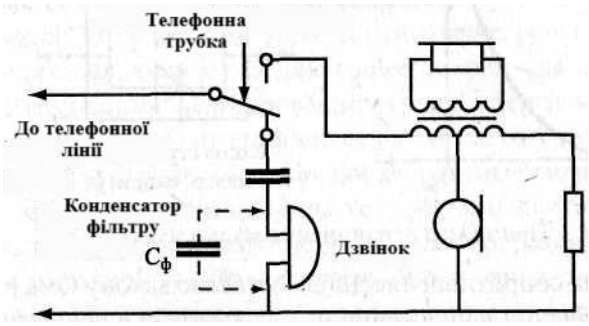


Рисунок 14.2 – Фільтрування небезпечного сигналу у дзвінковому ланцюзі

Більш складний фільтруючий пристрій являє собою багатоланковий фільтр низької частоти на LC-елементах, що пригнічує більш високі частоти акустоелектричних перетворювачів у порівнянні з корисними сигналами годин єдиного часу, охоронних і пожежних сповіщувачів та ін. Дволанковий П-подібний фільтр забезпечує згасання небезпечних сигналів вторинному годиннику за рахунок акустоелектричних перетворень, приблизно на 85 дБ. Подібні фільтри забезпечують захист інформації в телефонних апаратах від високочастотного нав'язування, не пропускаючи до них високочастотні електричні сигнали від генератора, підключеного зловмисником до відповідної телефонної лінії. Корисні сигнали в діапазоні частот проходять через фільтр без помітного послаблення.

Можливість обмеження небезпечних сигналів ґрунтується на нелінійних властивостях напівпровідникових елементів (діодів, транзисторів, диністорів, тиристорів). Вольтамперна характеристика (залежність значення

протікає по нелінійному елементу електричного струму від прикладеного до нього напруги джерела струму) напівпровідникового діода показана на рис. 14.3.

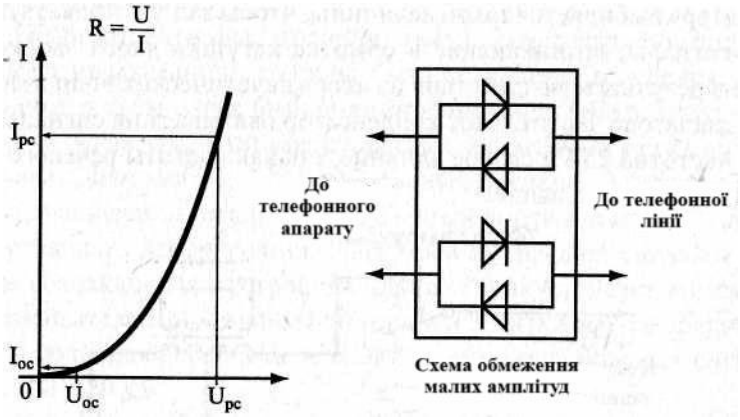


Рисунок 14.3 – Принципи обмеження малих амплітуд

Оскільки опір діода згідно із законом Ома дорівнює відношенню значення напруги на його висновках до величини струму, що протікає по діоду, то з цього рисунка випливає, що діод створює високий (сотні тисяч Ом) опір для сигналів з низьким (частки і одиниці мВ) напругою і мале (сотні Ом) — для корисних сигналів у телефонних лініях завбільшки десятки вольт. Тому небезпечні сигнали, що виникають в радіоелектронних засобах, що захищаються і мають малу амплітуду в порівнянні з корисним сигналом, додатково послаблюються в тисячі разів, а корисні сигнали проходять через напівпровідниковий обмежувач практично без згасання. Наприклад, пристрій «Граніт-VIII» забезпечує ослаблення вхідного сигналу амплітудою не більше 0,1 близько 65 дБ, а сигналу амплітудою понад 10 В всього на 3 дБ. Розглянутий спосіб захисту інформації реалізований у пристроях «Корунд», «Граніт-VIII МП -1», МП-1 (для аналогових ТА), МП-1ЦА (для цифрових ТА з автономним живленням), МП-1ЦЛ (для цифрових ТА з живленням від міні-АТС).

Поєднання фільтра та обмежувача широко використовується в пристроях комплексного захисту інформації шляхом придушення небезпечних побічних сигналів та сигналів високочастотного нав'язування (Грань-300, МП-1А та ін.).

Засоби захисту від небезпечних сигналів у гучномовцях не застосовуються через незначні відмінності в характеристиках корисних та небезпечних сигналів, незважаючи на те, що їх частоти збігаються в межах звукового діапазону. Так як котушка динамічної головки гучномовця має малий опір порядку 4-8 Ом, то для виключення перегорання її тонкого дроту величина напруги сигналу, що подається на котушку невелика, частки В. З цією метою сигнал ретрансляційної мережі, що має для мережі міста напруга 15 В, а області 30, подається на гучномовець через понижувальний трансформатор. Внаслідок цього співвідношення рівнів небезпечного та корисного сигналів у котушці гучномовця недостатнє для ефективного використання обмежувачів малих амплітуд. Тому для придушення небезпечних сигналів гучномовця застосовують пристрій, що відрізняє небезпечні сигнали від корисних за їх напрямком. Таким пристроєм є буферний пристрій у вигляді одного або декількох послідовно з'єднаних емітерних повторювачів. Емітерний повторювач є каскадом підсилювача потужності із загальним емітером (див. рис. 14.4), у якого коефіцієнт посилення сигналу за напругою близький до 1.

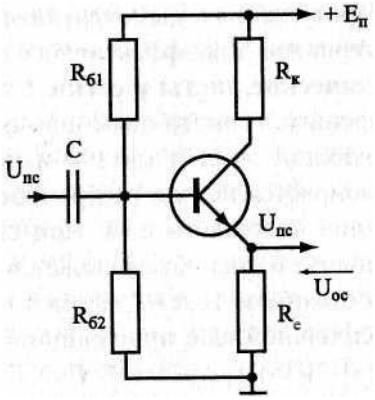


Рисунок 14.4 – Емітерний повторювач буферного пристрою

Емітерний повторювач має високий вхідний і малий вихідний опори і застосовується для узгодження взаємодіючих радіотехнічних пристроїв з вихідними і вхідними опорами, що істотно відрізняються.

Корисний сигнал $U_{\text{пс}}$ ззовні проходить до гучномовця через емітерний повторювач без помітних змін, а внутрішній небезпечний сигнал $U_{\text{ос}}$

пригнічується до 1000 разів (60 дБ за напругою). Враховуючи високий рівень небезпечного сигналу гучномовця, для його гарантованого придушення в буферному пристрої з'єднують послідовно 3 емітерних повторювача із загальним коефіцієнтом придушення до 180 дБ.

Засоби екранування електромагнітних полів

Для екранування електромагнітних полів застосовуються спеціальні конструкції та різноманітні матеріали. Спеціальні конструкції включають екрановані споруди, приміщення та камери. Вони можуть бути стаціонарними, збірно-розбірними та мобільними. Виконуються із сталевих листів товщиною 2-3 мм та забезпечують згасання електромагнітного поля 60-120 дБ. Для забезпечення нормальної роботи вони обладнуються захищеними дверима, воротами, отворами з пристроями сигналізації про щільне закриття, різноманітними завадними фільтрами, засобами вентиляції та кондиціювання, пожежної сигналізації, пожежогасіння та димоуловлювання.

Як матеріали для ефективного екранування використовуються **металеві листи та сітки.** Сталеві листи товщиною 2-3 мм, зварені герметичним швом, забезпечують найбільший ефект, що екранує (до 100 і більше дБ). Товщина сталевого листа вибирається виходячи з міцності конструкції та можливості створення суцільного шва. При зварюванні змінним струмом товщина суцільного шва забезпечується при товщині листів 1,5-2 мм, на постійному струмі близько 1 мм, газове зварювання дозволяє створити суцільний шов при товщині листів, що зварюються до 0,8 мм.

Однак металеві листи мають високу ціну, а виготовлення з них екранів та їх експлуатація вимагають великих витрат. Корозія і напруження зварювальних швів, що з'являється під час монтажу, знижують надійність і довговічність екранів, а необхідність їх періодичної перевірки і усунення дефектів підвищують експлуатаційні витрати.

Дешевші та зручніші, але менш ефективні екрани з **металевої сітки.** Застосовують для екранування сітки з лудженого сталевого та латунного дроту

з осередками розмірами від часток (0,25) мм до одиниць (3-6) мм. Екрануючі властивості сітки в основному визначаються відображенням електромагнітної хвилі від її поверхні. Ефективність захисту від електромагнітного випромінювання екрану з лудженого низьковугільного сталевого каркасу з осередками розміром 2,5-3 мм становить 55-60 дБ при частотах 50 Гц, тоді як ефективність подвійної сітки з відстанню між шарами 100 мм досягає рівня близько 90 дБ. За співвідношенням радіуса r дроту сітки та кроку сітки s розрізняють густі та рідкісні сітки. До густих відносяться сітки, у яких $s/r \leq 8$, у рідкісних – $s/r > 8$. Ефективність екранування рідкісної сітки визначається за формулою:

$$S_{\text{с}} = \frac{\lambda}{2s[\ln(\frac{2\pi r}{s})}.$$

Для густих сіток більш точний результат виходить за заміни величини $ln(2\pi r/s)$ у цій формулі на $2\pi r/s$.

Поряд із розглянутими традиційними засобами для електромагнітного екранування останнім часом все ширше застосовуються **фольгові** та **металізовані матеріали, токопровідні фарби** та **клеї, радіопоглинаючі будівельні матеріали.**

Як **фольгові матеріали** використовується фольга товщиною 0,01-0,08 мм, що наклеюється на екрановану поверхню, і фольга на непровідній підкладці, наприклад на фольгоізолі. Фольга виготовляється із алюмінію, латуні, цинку.

Металізація різних матеріалів застосовується для електромагнітного екранування завдяки універсальності методів і розпилення розплавленого металу струменем стисненого повітря. Розпилені частинки металу, що рухаються з великою швидкістю, ударяються об поверхню підкладки, деформуються і стикаються один з одним. При цьому забезпечується міцний зв'язок з підкладкою та безперервна провідність покриття. Цей метод дозволяє нанести металевий шар практично на будь-яку поверхню: щільний папір, тканину, дерево, скло, пластмасу, бетон та ін. Товщина шару, що наноситься, залежить від фізико-хімічних властивостей підкладки. Для щільного паперу шар

металу характеризується величиною не більше 0,28 кг/м^2 , для тканини — 0,3 кг/м^2 , для жорсткої підкладки товщина не обмежується. Як метал покриття частіше використовується цинк, рідше алюміній. Алюмінієве покриття має більший (приблизно не 20 дБ) коефіцієнт екранування, але воно менш технологічне.

Ефективність екранування металізованої цинком поверхні оцінюється за емпіричною формулою:

$$S_{\text{мет}} = 97 + 5lgd_0 - 20lgf,$$

де d_0 – кількість розпиленого металу, кг/м2, f - частота поля, Мгц.

З металізованих матеріалів найбільш широко застосовуються металізовані **тканини** та **плівки (скла).** Тканини металізуються як шляхом вплетення в неї металізованих або металевих ниток пряжі, так і шляхом нанесення на поверхню тканини шару металу. При цьому у тканин зберігаються не тільки її первісні властивості (гнучкість, повітропроникність, легкість) і зовнішній вигляд, але з'являються додаткові стійкість до агресивних середовищ і протипожежна стійкість. Тканину можна зшивати, склеювати і навіть паяти. Ефективність екранування металізованих тканин у високочастотному діапазоні (сотні МГц) досягає 50-70 дБ. Їх застосовують для екранування стін та віконних отворів (у вигляді штор), корпусів продукції, антенних відбивачів, чохлів на об'єкти радіолокаційного спостереження.

Електричні та оптичні властивості стекол з струмопровідним покриттям залежать від складу струмопровідної плівки, її товщини , методів її нанесення та властивостей скла. Допустимі зниження прозорості плівки не більше 20% і електропровідність забезпечуються при товщині плівки 5-3000 нм. Найбільше поширення отримали плівки з окису олова.

Скло зі струмопровідними покриттями має поверхневий електричний опір порядку 5-10 Ом при незначному (не більше 20%) погіршенні прозорості. **Струмопровідні плівки,** що наклеюються на шибки вікон, дозволяють підвищити екрануючий ефект вікон без погіршення їх зовнішнього вигляду та прозорості на 18-22 дБ на частотах у сотні МГц і на 35-40 дБ на частотах одиниці

ГГц. Залежно від виду металу, що напилюється на плівку, вони мають золотистий (мідне напилення) або сріблястий (алюмінієве напилення) колір.

Струмопровідні фарби створюються шляхом введення в фарби токопровідних матеріалів: колоїдного срібла, графіту, сажі, оксидів металу, порошкової міді, алюмінію та інших металів. Найкращі результати забезпечує фарба, у якої як струмопровідний пігмент застосовується ацетиленова сажа і графіт. Наприклад, фарба, що представляє композицію лаку 9-32 і 300% олівцевого графіту, має поверхневий опір 7-7,6 Ома при товщині покриття 0,15 0,17 мм і опір 5-6 Ом при товщині покриття 0,2-0,21 мм.

Струмопровідні фарби в силу гіршої електропровідності та малої товщини забезпечують меншу в порівнянні з металізованими тканинами екрануючу ефективність, але не менше 30 дБ у широкому діапазоні частот. Але через простоту нанесення на поверхню емалі широко застосовуються для:

- екранування огорож (стін, стель, дверей);
- захисту контактних поверхонь від окиснення;
- фарбування внутрішньої поверхні корпусів апаратури;
- проведення профілактичних та ремонтних робіт, у тому числі для закладення щілин, отворів, виводів труб зі стін, для покращення контакту між металізованими плівками та металевими екранами стін.

Електропровідні клеї застосовуються замість паяння та болтових з'єднань елементів електромагнітних екранів, а також для заповнення щілин та малих отворів у них. Основу електропровідного клею складає суміш епоксидної смоли та тонкодисперсних порошків заліза, кобальту або нікелю. За міцністю до 500 кг/ $см^2$ такий клей має низьку питому електропровідність.

Для підвищення екрануючої здатності стель, стін, підлог приміщень застосовуються **феритодіелектричні облицювальні матеріали,** що поглинають електромагнітні поля. Цим поглиначем є панель зі склеєних металевої підкладки, феритового та діелектричного матеріалів. Феритодіелектричний поглинач електромагнітних хвиль екологічно чистий, має стабільні радіотехнічні характеристики в широкому діапазоні частот, забезпечує

коефіцієнт відображення -12-(-40) дБ в діапазоні частот 0,03-40 ГГц, стійкий до впливу вогню.

Шляхом добавки в бетон будівельних конструкцій струмопровідних матеріалів вдається також підвищити екрануючі властивості стін і перекриттів будівель.

Металізовані тканини і плівки, фольговий матеріал, токопровідні емалі ефективно екранують слабкі побічні електромагнітні випромінювання і наведення, але їхня екрануюча здатність недостатня для енергетичної скритності потужніших сигналів, наприклад випромінювань передавачів заставних пристроїв, не кажучи вже про випромінювання у дослідних лабораторіях створюваних випромінюючих радіоелектронних засобів.

Для гарантованого ослаблення небезпечних сигналів при жорстких вимогах до рівня безпеки інформації джерела випромінювань розміщують в екранованих приміщеннях (екранних кімнатах), огородження яких покриті сталевими листами або металевими сітками. Розміри екранованого приміщення вибирають з його призначення та вартості екранування. Існують екрановані обчислювальні центри площею в багато десятків $м^2$, але зазвичай екранні кімнати для проведення вимірювань радіовипромінювальних блоків і антен мають невелику площу в 6-8 $м^2$ при висоті 2,5-3 м. Металеві листи або полотнища сітки, що покривають стіни, стелю та підлогу, повинні бути міцними, з малим електричним опором, з'єднані між собою по периметру. Для суцільних екранів це з'єднання забезпечується зварюванням або паянням, для сітчастих екранів повинен бути забезпечений точковим зварюванням або пайкою хороший електричний контакт між полотнищами не рідше ніж через 10-15 мм.

Двері мають бути також екрановані. При їх закриванні необхідно забезпечити надійний електричний контакт із металевими листами або сіткою стін по всьому периметру дверей. Для цього застосовують пружинний гребінець із фосфористої бронзи, який зміцнюють по внутрішньому периметру дверної рами.

При наявності в екранній кімнаті вікон останні повинні бути затягнуті одним або двома шарами сітки, відстань між шарами подвійної сітки не менше 50 см. Шари сітки повинні мати хороший електричний контакт із екраном стін по всьому периметру віконної рами. Екран, виготовлений з лудженої низьковуглецевої сталевої сітки з коміркою розміром 2,5-3 мм, зменшує рівень випромінювань на 55-60 дБ, а з такою ж подвійною (з відстанню між зовнішньою і внутрішньою сітками 100 мм) приблизно на 90 дБ. Сітки для забезпечення можливості миття скла зручно робити знімними, а металеве обрамлення знімної частини повинно мати пружні контакти у вигляді гребінки з фосфористої бронзи.

При проведенні робіт з ретельного екранування подібних приміщень необхідно одночасно забезпечити нормальні умови для людини, що працює в ньому, насамперед, вентиляцію повітря і освітлення. Це тим більше важливо, тому що у людини в екранній кімнаті може погіршитися самопочуття через екранування магнітного поля Землі.

Для ефективного електромагнітного екранування вентиляційні отвори на частотах менше 1000 МГц закриваються металевими сітками з прямокутними, круглими або шестигранними осередками. Для забезпечення ефективного електромагнітного екранування необхідно, щоб розміри осередків екрана не перевищували 0,1 довжини хвилі поля. Але на високих частотах розміри осередків можуть бути такими малими, що погіршиться вентиляція через них повітря. Тому на частотах вище 1000 МГц застосовують спеціальні електромагнітні пастки у вигляді конструкції з матеріалів, що поглинають електромагнітні поля, що вставляється у вентиляційні отвори.

Величини згасання радіосигналу в екранованому приміщенні в залежності від конструкції екрана вказані в табл. 14.1.

Таблиця 14.1 – Величини згасання радіосигналу в екранованому приміщенні в залежності від конструкції екрана

Тип конструкції екрану	Згасання радіосигналу, дБ
Одиночний екран із сітки з одиночними дверима, обладнаною затискними пристроями	40
Подвійний екран із сітки з подвійними дверима-тамбуром та затискними пристроями	80
Суцільний сталевий зварний екран з одними дверима-тамбуром із затискними пристроями	100

Завдання до практичного опрацювання

1. Скласти логічну схему бази знань із змісту блоку.

2. Скласти термінологічний словник.

3. Виконати всі пункти, перелічені в розділі підготовчого етапу до практичного заняття.

Практичне заняття (ділова гра)

Цілі:

1. Закріпити і поглибити матеріал, що вивчається студентами.

2. Вміти викласти свою точку зору з проблемних питань та технічного захисту інформації.

Учасники: Студенти розподілені на 3 підгрупи:

1-а підгрупа – співробітники технічної групи служби безпеки;

2-я підгрупа – фахівці з добування інформації у різний спосіб (зокрема і незаконними);

3-я підгрупа – експертна група.

Час: 90 хвилин.

Підготовчий етап (домашня робота)

1. Підготувати матеріал за раніше виданою на поточне заняття (наприкінці попереднього заняття) викладачем теми:

- скласти план блоку;

- скласти термінологічний словник: виписати терміни, що зустрічаються в тексті блоку, і дати їм розшифровку;

- вибрати одне з підприємств (сховища та депозитарії банків; підприємства з виробництва або сховища хімічно небезпечних, наркотичних і вибухових речовин, боєприпасів ядерних матеріалів; підприємства оборонного профілю; урядові установи; енергетичні комплекси, касові зали банків; під'їзди інкасаторських машин, приміщення для зберігання та роботи з важливою інформацією, що захищається, торгові центри з продажу цінних товарів, виробничі приміщення для виготовлення цінної продукції, торгові зали магазинів, службові приміщення установ, офіси середнього та малого бізнесу, виробничі приміщення загального значення; житлові приміщення тощо);

2. Виходячи зі змісту блоку, скласти стосовно обраного об'єкта до десяти питань:

а) співробітникам технічної групи служби безпеки щодо забезпечення безпеки об'єкта;

б) фахівцям з добування інформації різними способами (зокрема незаконними), що стосуються способів несанкціонованого вторгнення на об'єкт, підслуховування, перехоплення тощо.

3. Бути готовими відповісти на будь-які поставлені питання з боку підгрупи співробітників технічної групи служби безпеки, підгрупи спеціалістів з добування інформації різними способами (у тому числі й незаконними. Вміти оцінити питання та відповіді учасників у підгрупі експертів);

4. Бути готовими відповісти на запитання, розміщені в кінці блоку;

5. Оформити домашню роботу у вигляді звіту.

Порядок проведення практичного заняття

1. Організація заняття (перевірка присутніх та готовності до занять, оголошення теми виходячи із змісту поточного заняття). (5 хвилин);

2. Розподіл на підгрупи та доведення порядку проведення заняття. (5 хвилин);

3. Присвоєння підгрупам початкових ролей (співробітники технічної групи служби безпеки, фахівці з добування інформації у різний спосіб (зокрема і незаконними), експертна група). (5 хвилин);

4. Обговорення студентами підгруп питань, винесених на практичне заняття з метою вироблення спільних позицій:

4.1. Питання з боку підгрупи співробітників технічної групи служби безпеки, що виступають у ролі. (15 хвилин);

4.2. Питання з боку підгрупи фахівців з добування інформації, що виступають у ролі. (15 хвилин);

4.3. Запитання з боку підгрупи експертів. (15 хвилин);

4.4. Відповіді та дискусії. (10 хвилин);

4.5.Вироблення спільної позиції та загального підходу до питань, що розглядаються на поточному занятті відповідно до його теми. (5 хвилин);

5. Обговорення викладачем та старшими груп оцінок учасників заняття. (5 хвилин);

6. Підбиття підсумків заняття з оголошенням остаточних оцінок учасників практичного заняття. (5 хвилин);

7. Оголошення теми та змісту наступного практичного заняття. (5 хвилин).

Контрольні запитання

1. Заходи щодо запобігання витоку інформації, що захищається по ланцюгах електроживлення.

2. Вимоги до засобів електроживлення об'єктів 1-3 категорій.

3. Яким чином запобігають витоку інформації щодо ланцюгів

заземлення радіоелектронних засобів?

4. Вимоги до засобів захисту інформації від витоку через побічні електромагнітні випромінювання та наведення.

5. Типи засобів придушення небезпечних сигналів акустоелектричних перетворювачів.

6. Що являють собою спеціальні конструкції для екранування полів?

7. Які матеріали використовуються для екранування електромагнітних полів?

8. Переваги та недоліки плівок, фарб та клею, що застосовуються для електромагнітного екранування.

15 ОЦІНКА ЗАГРОЗ РАДІОЕЛЕКТРОННИХ ТА РЕЧОВИХ КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ

Методичні рекомендації щодо оцінки загроз радіоелектронних каналів витоку інформації

Витік інформації можливий по радіоканалу та проводам. Умови запобігання витоку радіоелектронним каналом:

• напруженість електромагнітного поля на межі контрольованої зони менша за нормативне значення;

• напруга електричного струму в лінії (ланцюгах електроживлення) на межі контрольованої зони меншого значення.

а) Оцінка витоку інформації з радіоканалу

Джерелами радіосигналів з мовленнєвою інформацією, що циркулює у приміщенні, є:

• передавальні пристрої заставних пристроїв;

• джерела побічних електромагнітних випромінювань.

Напруженість електромагнітного поля на межі контрольованої зони залежить від:

• потужності джерела радіовипромінювань;

• характеру зміни напруженості електромагнітного поля при його поширенні джерела випромінювання до приймача сигналів;

• величини згасання енергії поля серед поширення до межі контрольованої зони;

• відстань джерела випромінювання до межі контрольованої зони.

Потужність передавачів заставних пристроїв коливається у межах: від одиниць мВт до одиниць Вт. Максимальна дальність поширення радіосигналів оцінюється за такою формулою:

$$D \leq \frac{\lambda}{4\pi}\sqrt{\frac{P_{\text{іс}} G_{\text{іс}} G_{\text{пр}} \gamma_{\text{п}}}{\text{Р}_{\text{пр}} q_{\text{пр}}}},$$

де P_{ic} – потужність джерела (передавача); $P_{пр}$ – гранична чутливість приймача; G_{ic} і $G_{пр}$ – коефіцієнти посилення антен передавача та приймача; $\gamma_{п}$ – коефіцієнт, що враховує розбіжність кутів поляризації передавальної та приймальної антен; $q_{пр}$ – відношення сигнал/шум на вході приймача, при якому забезпечується необхідна якість інформації на його виході.

Приклад. Для заставного пристрою з P_{ic} = 10 мВт і G_{ic} = 0,05, приймача з $P_{пр}$ = 10^{-13} Вт, $G_{пр}$ = 0,1 і $q_{пр}$ = 10q , а також для $\gamma_{п}$ = 0,5 і λ = 6 м (f = 500 МГц) $D \leq 2500$ м (без урахування згасання електромагнітної хвилі в середовищі поширення та зовнішніх перешкод).

Електромагнітна хвиля з приміщення згасає в основному в елементах будівлі (табл. 15.1).

Таблиця 15.1 – Елементи будівлі

Тип будівлі	Ослаблення радіосигналу у дБ на частоті		
	100 МГц	500 МГц	1 ГГц
Дерев'яна будівля з товщиною стін20 см	5-7	7-9	9-11
Цегляна будівля з товщиною стін в 1,5 цегли	13-15	15-17	16-19
Залізобетонна будівля з осередком арматури 15 х 15 смі завтовшки16 см	20-25	18-19	15-17

Примітка. У будівлях, що розглядаються, 30% площі займають віконні отвори.

Зменшення згасання електромагнітної хвилі в залізобетонних стінах із підвищенням її частоти викликано зниженням екрануючого ефекту металевої арматури залізобетону. На частоті 1 ГГц довжина хвилі дорівнює 30 см, порівнянна з розмірами осередків арматури.

При ослабленні електромагнітної хвилі стінами будівлі на 20 дБ дальність її розповсюдження зменшується на 1 порядок. Для розглянутого прикладу вона становитиме одиниці сотень і десятки метрів.

Оцінка загрози витоку інформації, спричиненої побічними випромінювання ОТСС і ВТСС, здійснюється шляхом порівняння радіусів зон потенційного перехоплення небезпечних радіосигналів із розмірами контрольованих зон організації. Як критерій застосовується енергетичний критерій - рівень поля чи електричного сигналу.

Розрізняють 2 види зон (див. рис. 15.1):

• зона 1 з радіусом R_1 — простір навколо ОТСС, у межах якого не допускається розміщення ВТСС, через яке може відбуватися витік інформації за межі контрольованої зони;

• зона 2 з радіусом R_2 в межах якої рівень сигналу, випромінюваного ОТСС, перевищує норматив.

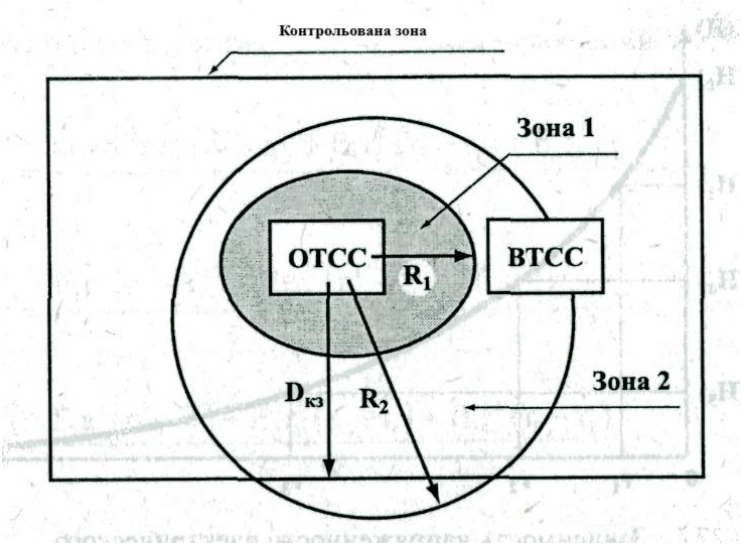


Рисунок 15.1 – Зони безпеки інформації

Так як діаграма спрямованості навколо джерела випромінювання, як правило, нерівномірна, радіуси визначаються на напрямках максимальної напруженості сигналу.

Інформація, що міститься в інформаційних параметрах радіосигналів, захищена поза межами контрольованої зони, якщо $R_{з2} < D_{кз}$, а $R_{з1}$ менше відстані між ОТСС і ВТСС. Тут $D_{кз}$ – відстань від ОТСС до межі контрольованої зони.

Радіус зони 2 більше радіуса зони 1, так як в якості засобу перехоплення використовується спеціальний приймач з істотно вищими характеристиками, ніж ВТСС.

Для оцінки рівня захищеності необхідно оцінити радіуси зон 1 та 2. Для цього визначається характер зміни напруженості поля від відстані до джерела випромінювання. Як відомо, цей характер залежить від того, в якій зоні (ближній або дальній) вимірюється.

У загальному випадку напруженість поля змінюється у вигляді $E(H) = E_0(H_0)/r_{1,2}{}^q$, де q = 1,2,3. Характер зміни оцінюється в результаті вимірювання напруженості Е в двох точках (див. рис 15.2).

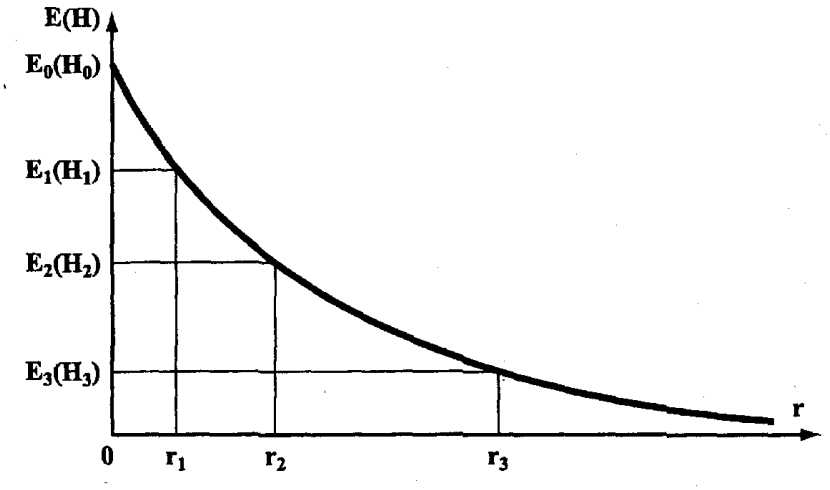


Рисунок 15.2 – Залежність напруженості електричного (магнітного) полів від відстані до їх джерел

Вимірявши E(H) у двох точках, можна приблизно оцінити показник q ступеня зміни напруженості полів за формулою:

$$q = \frac{\ln (E_1/E_2)}{\ln (r_1/r_2)}.$$

За значенням q визначаються розміри зони 2:

$$R_{з2} = r_1 \sqrt[q]{E_1(H_1)/E_{\text{н}}(\text{Н}_{\text{н}})}.$$

Більш точна апроксимація $\text{Е}(\text{Н}) = f(r)$ забезпечується за трьома точками: $\text{Е}(\text{Н}) = \frac{x}{r^3} + \frac{y}{r^2} + \frac{z}{r}$. Невідомі x, y і z визначаються із системи лінійних рівнянь:

$$\begin{cases} \frac{x}{r_1^3} + \frac{y}{r_1^2} + \frac{y}{r_1} = E_1(H_1), \\ \frac{x}{r_2^3} + \frac{y}{r_2^2} + \frac{y}{r_2} = E_2(H_2), \\ \frac{x}{r_3^3} + \frac{y}{r_3^2} + \frac{y}{r_3} = E_3(H_3). \end{cases}$$

В результаті розв'язання цієї системи рівнянь за правилом Крамера:

$$x = \frac{r_1 r_2 r_3 [E_1 r_1^2 (r_2 - r_3) + E_2 r_2^2 (r_3 - r_2) + E_3 r_3^2 (r_1 - r_2)}{w},$$

$$y = \frac{E_1 r_1^3 (r_3^2 - r_2^2) + E_2 r_2^3 (r_1^2 - r_3^2) + E_3 r_3^2 (r_2^2 - r_1^2)}{w},$$

$$z = \frac{E_1 r_1^3 (r_2 - r_3) + E_2 r_2^3 (r_3 - r_1) + E_3 r_3^3 (r_1 - r_2)}{w},$$

$$w = r_1^2 r_2 - r_1 r_2^2 + r_1 r_3^2 - r_2 r_3^2.$$

Допустимі напруженості полів $E_{\text{н}}$ і $\text{Н}_{\text{н}}$ зазначаються у нормативно-методичних документах для різних категорій приміщень.

Нормативні значення напруженості поля з інформацією, що захищається, визначаються зі співвідношення $\text{Е}_{\text{н}} = \text{Е}_{\text{ш}} \delta_i$, де $\text{Е}_{\text{ш}}$— напруженість електричного поля шумів, δ_i— нормативне (максимальне) відношення сигнал/шум, при якому забезпечується безпека інформації. Так як рівень шумів приймача залежить від його смуги пропускання Δf, то вводять такий показник, як рівень $\text{Е}_{\text{шн}}$ нормованого шуму (наведений до одиниці смуги). З огляду на це $\text{Е}_{\text{ш}} = \text{Е}_{\text{шн}} * \sqrt{\Delta f}$.

б) Оцінка загрози витоку мовної інформації з проводів

Джерелами небезпечних сигналів у дротах є:

• ЕРС, що наводяться електромагнітними полями у дротах;

• сигнали випадкових акустоелектричних перетворювачів.

Еквівалентна схема ланцюга, що містить джерело небезпечних сигналів U і наведена на рис. 15.3.

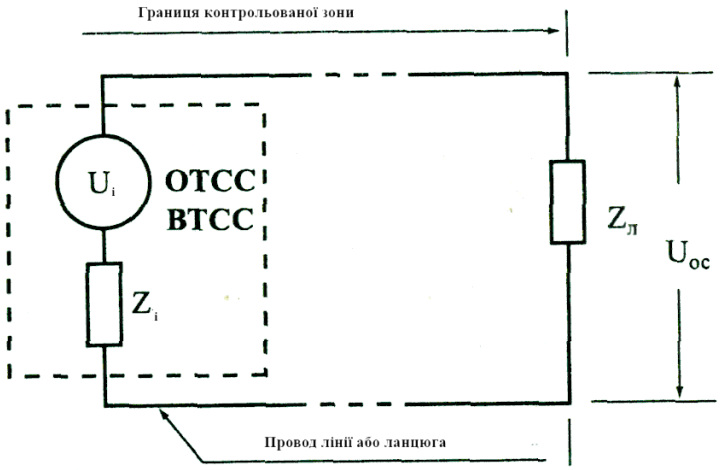


Рисунок 15.3 – Еквівалентна схема провідної лінії

Напруга небезпечного сигналу $U_{\text{ос}}$ у лінії (провідних ланцюгах) на межі контрольованої зони дорівнює величині $U_{\text{ос}} = \frac{U_i Z_i}{Z_i + Z_{\text{л}}}$, де Z_i $Z_{\text{л}}$ – комплексні опори джерела небезпечних сигналів і лінії відповідно.

Безпека мовної інформації забезпечується від витоку по провідних лініях під час умови $U_{\text{ос}} < U_{\text{н}}$, де $U_{\text{н}}$ — нормативне значення небезпечного сигналу.

Якщо джерелом небезпечних сигналів у ВТСС є поля ОТСС напруженістю E, $U_i = \text{E} \cdot \text{h}_{\text{д}}$, де $\text{h}_{\text{д}}$ – висота випадкової антени технічного засобу, що діє. Діюча висота $\text{h}_{\text{д}}$ ВТСС, розташованого у приміщенні, вимірюється як відстань від середини висоти ВТСС до середини перекриття підлоги. Вплив електричного поля на ОТСС на ВТСС здійснюється через паразитний ємнісний зв'язок із Z_{i}. Якщо прийняти $U_{\text{ос}} = U_{\text{н}}$ то власну ємність ВТСС вимірюють методом заміщення. З цією метою ВТСС заміщають моделлю (кулькою або диском) з відомою ємністю C і вимірюють напругу, що індукується в ній U_{e}. Місткість ВТСС оцінюється за формулою: $\text{C}_i = \text{C}_e * U_i / U_e$, де U_i – напруга, що індукується у ВТСС.

Методичні рекомендації щодо оцінки загроз речових каналів витоку інформації

Рівень загрози речового каналу залежить від виду інформації та її носія. Оскільки відходи виробництва, що містять інформацію, що захищається, створюються співробітниками організації (підприємства), то на ціну цієї інформації опосередковано впливає посадовий (науковий) статус співробітника — автора відходів. Ціна інформації в чернетці документа, що диктується керівником, у загальному випадку вища, ніж чернетка рядового виконавця. Оскільки основні заходи захисту від витоку по речовинному каналу відносяться до організаційних, значення показників цього каналу залежить від пунктуальності виконання заходів захисту. Порушення режиму роботи організації або технології виробництва нової продукції, що містить інформацію, що захищається, збільшують ризик витоку інформації по цьому каналу.

Визначити в загальному випадку кількісні значення ризику витоку на основі інструментальних вимірювань у речовому каналі неможливо. Однак можна якісно оцінити потенційну загрозу внаслідок аналізу реальності можливих порушень режиму та технології. Як такі порушення, наприклад, можуть розглядатися факти, зазначені в актах попередніх перевірок рівня безпеки інформації. Крім того, у будь-якій системі існують слабкі місця, рівень захисту яких важко піддається контролю. Наприклад, вимоги про необхідність запису з питань закритої інформації лише в врахованих зошитах або на врахованих аркушах співробітниками організації далеко не завжди виконуються неухильно, а забезпечити безперервний контроль за всіма співробітниками неможливо. Тому існує, хоч і малий, ризик витоку інформації за рахунок порушень цих вимог.

Методичні рекомендації щодо оцінки значень показників моделювання

Одним з найважчих завдань, що виникають у процесі моделювання, є визначення значень показників: ціни інформації, рівня загрози та ймовірності її реалізації, витрат на запобігання загрозам. Така проблема виникає при вирішенні

будь-яких проблем, що слабо формалізуються. Тому їй приділяється постійна увага, хоч до її вирішення ще далеко. Відсутність однозначної залежності результату розв'язання задачі, що слабо формалізується, від вихідних даних, їх невизначеність і недостовірність істотно ускладнюють використання традиційного математичного апарату. Ба більше, часто цього не слід робити, оскільки за недостовірних вихідних даних можна отримати результат, далекий від реального.

Так як люди у повсякденному житті вирішують слабо формалізовані завдання частіше, ніж точні, то в процесі еволюції створено механізм їх вирішення з прийнятною для виживання точністю. Алгоритм їх вирішення на несвідомому рівні поки що не відомий, але отримано корисні евристичні рекомендації.

Оскільки рішення слабо формалізованих завдань виробляє людина, надалі — особа, яка приймає рішення (ЛПР), то методи, що використовуються, об'єктивно повинні ґрунтуватися на здібностях і можливостях ЛПР щодо вирішення таких завдань. Вони враховують такі емпіричні положення:

• точність розв'язання ЛПР слабо формалізованих завдань обернено пропорційна їх складності, причому ЛПР може в середньому оперувати одночасно з 5-9 поняттями;

• об'єктивність оцінок ЛПР показників процедур розв'язання слабоформалізованих завдань в умовах недостатньої та недостовірної інформації вище за використання ним якісних шкал, ніж кількісних;

• при обмеженості ресурсу його доцільно використовувати, перш за все, для запобігання загрозам з максимальною шкодою;

• ефективність використання ресурсу вища при його комплексному застосуванні, коли ті самі заходи запобігають декільком загрозам.

З цих досить загальних положень випливає, що для підвищення точності та об'єктивності ЛПР вибору доцільно:

• деталізувати алгоритм розв'язання задачі, що слабо формалізується, розбиваючи його на етапи і процедури, при визначенні показника яких виникає менше помилок;

• при оцінці показників окремих етапів та процедур використовувати якісні шкали з числом градацій (значень) у межах 5-9;

• проранжувати загрози безпеці інформації щодо потенційних збитків та витрачання ресурсу на запобігання загрозам виробляти послідовно, починаючи з заходів запобігання загрози з максимальною шкодою;

• при розробці заходів захисту враховувати вплив попередніх заходів на зниження шкоди цієї загрози.

Справді, якщо людина не знає точного кількісного значення будь-якого показника, він замінює його якісним заходом: висока людина, велика ціна, довгий шлях, мала ймовірність та ін. При цьому її якісні оцінки можуть бути дуже точними і однозначними.

В даний час робляться численні спроби використовувати для обробки нечітко визначеної інформації апарат нечітких множин Заде. Суть підходу Заде полягає у заміні якісних понять, наприклад, таких як «ціна інформації, «загроза безпеки інформації» та ін., названих лінгвістичними змінними, на кількісні аналоги та подальшу обробку числової інформації за допомогою запропонованого Заде математичного апарату. З цією метою вводяться функції належності чи сумісності кількісних значень лінгвістичної змінної. На рис. 15.4 у графічній формі представлені функції приналежності $\mu_в(h)$ лінгвістичних змінних «висока жінка» та «високий чоловік».

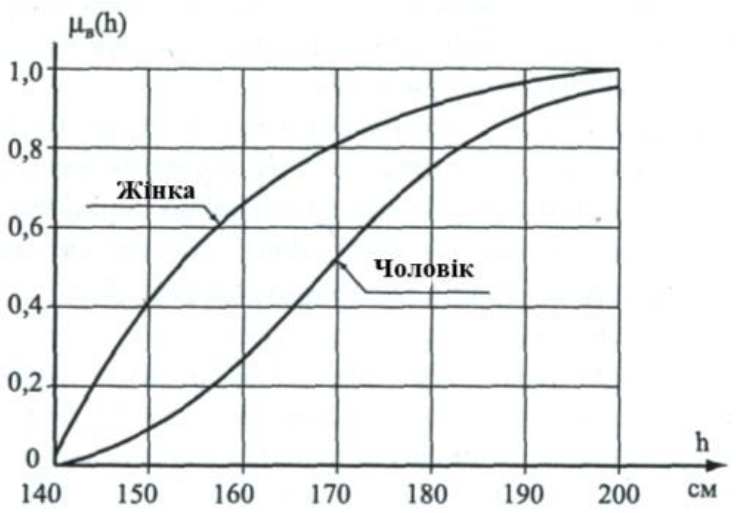


Рисунок 15.4 – Графічне представлення функції власності

На цьому малюнку по осі абсцис вказані значення росту людини в см, а по осі ординат — числа в інтервалі [0-1], відповідні ступеня належності значення росту жінки або чоловіка змінної лінгвістичної «високий(а)».

Функції приладдя можуть бути визначені в графічній або табличній формі, а також у вигляді суми алгебри значень $\mu_{\text{в}}(h)$. Наприклад, функція приналежності лінгвістичної змінної «високий чоловік», графічне уявлення якої наведено на рис. 15.4, має вигляд:

$$\mu_{\text{в}} = 0/140 + 0{,}1/150 + 0{,}3/160 + 0{,}53/170 + 0{,}75/190 + 0{,}95/200.$$

Кожний доданок цієї функції відповідає значенню функції приналежності певного значення зростання людини.

Запропонований математичний апарат теорії нечітких множин дає змогу проводити операції складання, об'єднання, множення, що забезпечує обробку цифрового масиву функцій контексті їхніх властивостей. Незважаючи на привабливість апарату нечітких множин при його застосуванні виникають проблеми, насамперед психологічного плану, які стримують його впровадження. Суть цих проблем полягає в тому, що в ході обробки функцій приналежності виходять результати у вигляді числових матриць, що важко піддаються осмисленому зворотному перетворенню на значення лінгвістичних змінних.

Для оцінки показників пропонується апарат, який краще узгоджується з логікою людини, яка оперує якісними поняттями. Він ґрунтується як на поняттях

апарату нечітких множин, так і психологічних засадах обробки інформації людиною. Принципи його ілюструють рис. 15.5.

Суть пропозицій полягає у наступному.

1. Людина приймає рішення шляхом порівняльного аналізу невеликої кількості альтернативних варіантів, у середньому близько 7. Альтернативи оцінюються якісними значеннями порядкової чи рангової шкали, або в термінології Заде – термами лінгвістичної змінної. Враховуючи здатність людини одночасно оперувати в середньому 5-9 словами та числами, кількість градацій лінгвістичної шкали слід обирати такого ж порядку.

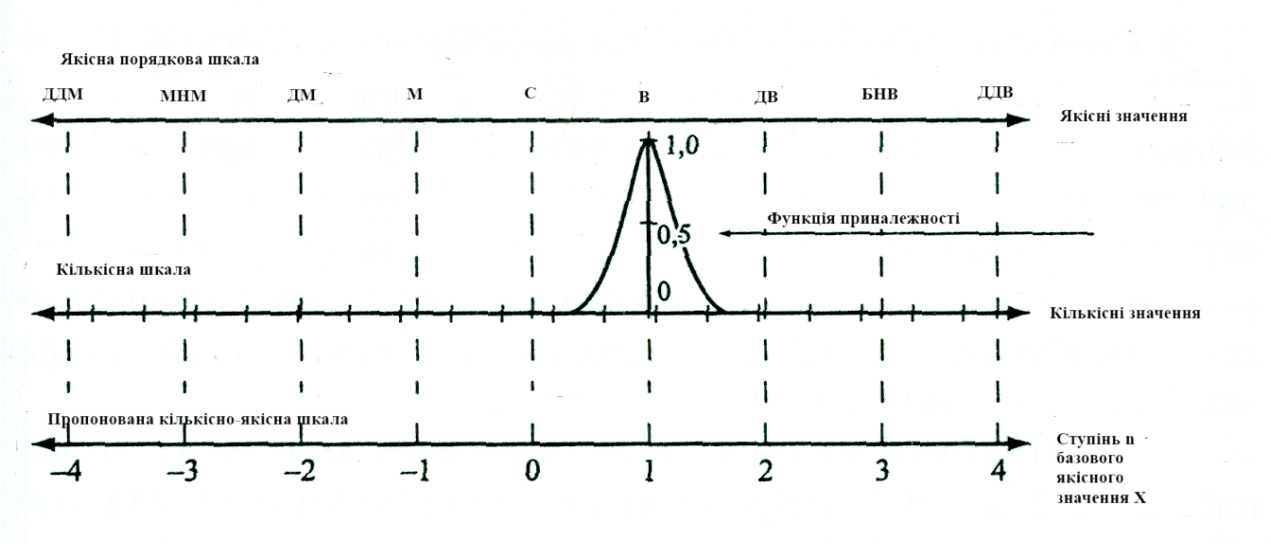


Рисунок 15.5 – Шкали для оцінки показників у галузі інформаційної безпеки. Позначення: ДДМ – дуже, дуже малий (а); МНМ – менш ніж дуже малий; ДМ – дуже малий; М – малий; С – середній; В – великий; ДВ – дуже великий; БНВ – більш ніж дуже великий; ДДВ – дуже, дуже великий.

2. Значення лінгвістичних змінних «ціна інформації», «ризик загрози», «збитки від реалізації загрози»: дуже велика, дуже велика, велика, середня, мала, дуже мала, дуже мала лінгвістичних змінних утворюють якісну шкалу з 7 градаціями. Для інших лінгвістичних змінних градацій шкали будуть характеризуватись іншими поняттями. Але спільними для них є базові значення «великий», «малий» і модифікатори «дуже».

3. Над якісною шкалою розташовується кількісна шкала, значення якої відповідають значенням показника якісної шкали. Значення "великий" або "малий" ідентичні цим значення в першому ступені, тобто великий = великий, а малий = малий.

4. Враховуючи здатність людини до дихотомії (розбиття лінійного розміру навпіл), точка відліку (умовний нуль) відповідає значенню «середня (середня)» лінгвістичної змінної якісної шкали або 0 кількісної шкали. Значення «середній» можна інтерпретувати як «маленький і малий», «не високий і низький». Приймемо, що середній відповідає великому чи малому в нульовому ступені, тобто середній = великий = малий.

5. Праворуч від нуля розташовується підмножина великих значень лінгвістичних змінних з базовим значенням "великий" ("високий"). Інші великі значення утворюються за допомогою модифікаторів "дуже": дуже великий, дуже, дуже великий (надмірно великий) і т. д. Психологічно модифікатор "дуже" відповідає концентрації значення лінгвістичної змінної шляхом зведення її в ступінь 2. Отже, дуже великий = великий; дуже, дуже великий = (дуже великий) = великий.

6. Зліва від нуля знаходиться область підмножини малих значень лінгвістичної змінної чи негативних чисел кількісної шкали. Значення лінгвістичної змінної, менші «середнього», відповідають «малий», «дуже малий» і т. д. або «низький», «дуже низький» тощо. Враховуючи, що психологічно твір «великий» на «малий» як «середній», то малий = середній / великий = великий/ великий = великий, дуже малий = великий і т. д.

Отже, всі значення лінгвістичної змінної можна виразити через одне базове значення "великий", "малий", "високий", "низький" у відповідній мірі.

З урахуванням введених позначень будь-яка лінгвістична змінна може бути записана у вигляді алгебраїчного виразу: yx^n, де y – найменування лінгвістичної змінної (ціна, ймовірність, ризик, збитки та ін), x – базове значення лінгвістичної змінної, n – позитивні числа. Наприклад, показник "дуже велика ціна інформації" = x^2y, де x – велика, y – ціна інформації.

Для підвищення об'єктивності оцінки показників необхідно виявити фактори, що впливають на їхню величину, та встановити зв'язки між значеннями цих факторів та показників. Основні з цих факторів наведені в табл. 15.2.

Таблиця 15.2 – Основні фактори, які впливають на значення величин

№ п/п	Лінгвістична змінна (показник процедур оптимізації)	Умовні позначення показника	Фактори, які враховуються при оцінці показника
1	Ціна інформації і-го джерела	C_i	Гриф секретності
2	Вірогідність k-ої загрози інформації і-го джерела	P_{yki}	$P_{yki} = P^{(\text{пу})}{}_{yki} * P^{(\text{еу})}{}_{yki} * P^{(\text{ву})}{}_{yki}$
3	Збиток від к-ої загрози інформації і-го джерела	C_{yki}	$C_{yki} = C_{\text{ии}} * P_{yki}$
4	Витрати на запобігання k-ої загрози інформації і-го джерела	C_{eki}	Витрати на проектування, закупку, встановлення та експлуатацію технічних засобів та реалізацію організаційних заходів
5	Ефективність заходів на запобігання k-ої загрози інформації і-го джерела	W_{eki}	$W_{eki} = C_{yki}/C_{eki}$

Примітка: $P^{(\text{пу})}{}_{yki} * P^{(\text{еу})}{}_{yki} * P^{(\text{ву})}{}_{yki}$ *– вірогідності виконання просторового, енергетичного та часових вимог розвідувального контакту.*

На ціну інформації, що захищається, впливають власні витрати організації при її отриманні, очікуваний прибуток від застосування інформації, збитки при попаданні цієї інформації до зловмисника. У першому наближенні ціна інформації, що захищається, пропорційна грифу її секретності. Але значення грифа секретності утворюють порядкову шкалу. У кожної людини формується

власне опорне уявлення про кількісну міру якісного значення лінгвістичної змінної. Наприклад, для однієї людини ціна одного й того самого товару дуже мала, для іншої — дуже велика. Враховуючи, що завдання оптимізації системи захисту вирішується в конкретній організації для зменшення суб'єктивізму, як опорний захід доцільно використовувати експертну оцінку в організації кількісної міри базового значення "велика" ціна або "великі" витрати.

Потрапляння до противника інформації, що становить таємницю організації, може завдати їй шкоди, який у випадку оцінюється залежно від потужності організації як середній чи великий. Наприклад, якщо грифу «таємно» можна зіставити значення (х) ціни інформації як більша — x^1, то «цілком таємно» — надзвичайно (дуже, дуже) велика — x^2 , «особливої важливості» — (дуже, дуже велика) – x^4.

Ще більша невизначеність виникає щодо значень ймовірності загрози. Єдина можливість підвищить достовірність оцінки — розчленування цього показника на складові та визначення значень цих складових, що зазвичай простіше, ніж оцінити значення інтегрального показника. Для отримання інформації зловмисником необхідно виконати низку етапів та процесів, які можна звести до трьох умов розвідувального контакту зловмисника з джерелом інформації:

- пошук та виявлення джерела інформації;
- розміщення технічного засобу добування на віддаленні від джерела, при якому забезпечується прийнятне відношення сигнал/шум на вході засобу;
- збіг часу та прояви демаскуючих ознак об'єкта захисту або передачі семантичної інформації та роботи засобу добування.

Загроза реалізується за одночасного виконання цих умов, а ймовірність її дорівнює добутку відповідних ймовірностей.

З урахуванням розглянутих пропозицій значення показників алгоритму проектування системи захисту вказані в табл. 15.3.

Таблиця 15.3 – Значення показників алгоритму проектування системи захисту

№ п/п	Лінгвістичні змінні	Значення показників	Алгебраїчні вирази для обчислення значень показників
1	Ціна інформації	$x^n y_{\text{і}}$	-
2	Вірогідність виконання просторової умови	$x^p y_{ny}$	-
3	Вірогідність виконання енергетичної умови	$x^r y_{ey}$	-
4	Вірогідність виконання тимчасової умови	$x^g y_{\text{ву}}$	-
5	Вірогідність загрози	$x^m y_y$	$x^m y_y = x^{p+r+g}(y_{ny} y_{ey} y_{\text{ву}})$
6	Збиток від загрози	$x^s y_{yy}$	$x^s y_{yy} = x^{n+m}(y_{\text{і}} y_{\text{у}})$
7	Витрати на заходи захисту	$x^1 y_{\text{з}}$	-
8	Ефективність заходів по захисту	$x^h y_e$	$x^h y_e = x^{s-j}(y_{yy}/y_{\text{з}})$

Примітка 1. У виразах таблиці опущені для спрощення записи індексів і та k позначення і-го джерела та k-ої загрози; 2. $y_{ny} y_{ey} y_{\text{ву}} \rightarrow y_{yy}$; $y_{\text{і}} y_y \rightarrow y_{yy}$; $y_{\text{уу}}/y_{\text{з}}\text{т} \rightarrow y_{\text{е}}$;

Приклад 1. Вихідні дані:

• ціна інформації - дуже велика (x^2y_i);

• ймовірність виконання просторової умови – мала ($\text{x}^{-1}\text{y}_{\text{пу}}$);

• ймовірність виконання енергетичної умови – мала ($\text{x}^{-1}\,\text{y}_{\text{еу}}$);

• ймовірність виконання тимчасової умови - середня ($\text{x}^0\,\text{y}_{\text{ву}}$)

• витрати на міру захисту - малі ($x^{-1}\,y_3$).

2. Похідні показники:

• ймовірність загрози – $x^{-1-1+0}y_y = x^{-2}y_y$– дуже мала загроза;

• шкода від загрози – $x^{2-2}y_{yy} = x^0 y_{yy}$ – середня;

• ефективність захисту – $x^{0+1}y_e$ – висока.

Для ціни інформації «велика» за тих же інших вихідних даних:

. збитки від загрози – $x^{1-2}yy = x_y^{-1}yy$ – малий;

• ефективність захисту – $x^{-1+1}y_e = x^0 y_e$ – середня.

Таким чином, розглянутий апарат дозволяє проводити найпростіші операції безпосередньо зі значеннями лінгвістичних змінних без проміжного переведення їх у числові значення. Для однакового сприйняття значень лінгвістичних змінних різними людьми необхідно базове значення прокоментувати відповідним на думку особи, яка здійснює оптимізацію, числовим значенням.

Розглянутий апарат може знайти застосування не тільки для вирішення завдань захисту інформації, але й будь-яких інших проблем, що слабо формалізуються, при вирішенні яких застосовуються якісні шкали.

Контрольні запитання

1. Розрахунок максимальної дальності розповсюдження радіосигналів.
2. Оцінка загрози витоку інформації, спричиненої побічними випромінюваннями ОТСС та ВТСС.
3. Оцінка загрози витоку мовної інформації з проводів.
4. Оцінка потенційної загрози витоку інформації речовими каналами.
5. Чинники що впливають точність прийняття рішень.
6. Сутність математичного апарату нечітких множин Заде.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна література

1. Грайворонський М.В. Безпека інформаційно-комунікаційних систем : підручник / М.В. Грайворонський, О.М. Новіков. – Київ : Видавнича група BHV, 2009. – 698 с.

2. Методи та засоби технічного захисту інформації: Опорний конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського / уклад. В.М. Луценко, Д.О. Прогонов. – Електронні текстові дані (файл:1,80 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.

Додаткова література

1. ДСТУ 3396.0-96. Захист інформації Технічний захист інформації. Основні положення [Електронний ресурс]. – [Чинний від 01.01.1997 р.]. — Режим доступу : https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf . – Назва з екрана.

2. ДСТУ 3396.1-96. Захист інформації Технічний захист інформації. Порядок проведення робіт [Електронний ресурс]. – [Чинний від 01.07.1997 р.]. – Режим доступу: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf . – Назва з екрана.

3. ДСТУ 3396.2-97. Захист інформації.Технічний захист інформації. Терміни та визначення [Електронний ресурс]. - [Чинний від 11.04.1997 р.] – Київ : Держстандарт України, 1997. - Режим доступу: https://usts.kiev.ua/wp-content/uploads/2020/07/dstu-3396.2-97.pdf . – Назва з екрана.

4. НД ТЗІ 3.7-003-2023. Про затвердження переліків документів нормативно-правової бази, що забезпечує надання відповідного виду послуг у галузі криптографічного та технічного захисту інформації [Електронний ресурс].

- [Чинний від 19.07.2023 р.] – Режим доступу: https://cip.gov.ua/services/cm/api/attachment/download?id=60391. – Назва з екрана.

5. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення [Електронний ресурс]. – [Чинний від 12.12.2007 р.] – Режим доступу: https://studfile.net/preview/9384738/ . – Назва з екрана.

6. НД ТЗІ 3.1-001-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи [Електронний ресурс]. – [Чинний від 12.12.2007 р.]. - Режим доступу: https://tzi.com.ua/downloads/3.1-001-07.pdf . – Назва з екрана.

7. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації. [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/3.3-001-07.pdf

8. НД ТЗІ 2.1-002-07 «Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення». [Електронний ресурс]. – [Чинний від 12.12.2007 р.]. – Режим доступу: https://tzi.com.ua/downloads/2.1-002-07.pdf. – Назва з екрана.

9. ТПКО-95 Тимчасове положення про категоріювання об’єктів [Електронний ресурс]. – Режим доступу: https://duikt.edu.ua/uploads/l_1038_96225311.pdf . – Назва з екрана.

10. Про затвердження Положення про державний контроль за станом технічного захисту інформації : наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 16.05.2007 №87 [Електронний ресурс]. – Режим доступу: https://ips.ligazakon.net/document/view/re14052?an=15. – Назва з екрана.

Інформаційні ресурси

1. Технічний захист інформації – інформаційна безпека та захист інформації [Електронний ресурс] : сайт. – Режим доступу: https://tzi.ua/ua/tz.html. - (дата звернення: 19.02.24 р.).

Навчальне видання

ДОРОГИЙ Ярослав Юрійович

НІКІТЕНКО Андрій Олександрович

МЕТОДИ ТА ЗАСОБИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ. ПРАКТИКУМ

Електронний навчальний посібник

Робота друкується в авторській редакції Дизайн обкладинки Є.Єгорова

Формат 60х84/16. Ум. друк. арк. 00,0. Обл.-вид. 00,0.
Тираж __0__ прим. Замовлення № 000/00.

Видавець: Державний вищий навчальний заклад «Донецький національний технічний університет». пл. Шибанкова, 2, м. Покровськ, Донецької обл., 85300, Україна; тел.: (0623) 52-17-90

Свідоцтво про державну реєстрацію суб'єкта видавничої справи:серія ДК № 4911 від 09.06.2015 р.