МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва і архітектури

ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ

Конспект лекцій

Для студентів з галузі знань 12 «Інформаційні технології»
за спеціальністю 125 «Кібербезпека та захист інформації»

Київ 2025

Конспект лекцій для студентів з галузі знань 12 «Інформаційні технології» за спеціальністю 125 «Кібербезпека та захист інформації» з дисципліни «Програмно-апаратні засоби захисту»/ Уклад. А.М. Котенко, Ю. І. Хлапонін, В. М. Трофимчук – К.:КНУБА, 2025. – 154 с.

Укладач:

А.М. Котенко, канд. техн. наук, доцент

Ю.І. Хлапонін, д.т.н, професор

В. М. Трофимчук

Відповідальний за випуск д.т.н, професор Ю.І. Хлапонін

Рецензент Симоненко О.А. - канд. техн. наук, доцент

Конспект лекцій затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії протокол № 5 від 13 січня 2025 р.

Конспект лекцій розглянуто та рекомендовано до друку на засіданні групи забезпечення спеціальності, протокол № 7 від 28 лютого 2024 р.

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1. **Лекції** з дисципліні «Програмно-апаратні засоби захисту» у студентів спеціальності 125 «Кібербезпека та захист інформації» охоплюють розділи курсу, що пов'язані з розглядом причин втрати інформації та методами і засобами захисту інформації від втрат.

2. Мета лекційних занять полягає у ознайомленні студентів з існуючими програмно-апаратними методами та засобами захисту інформації.

3. Основною метою курсу є формування у студентів теоретичного розуміння та відповідних практичних навичок, необхідних для забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності.

Дотримуючись принципу причинно-наслідкового зв'язку, перед вивченням програмних та апаратних засобів захисту інформації, необхідно розглянути причини – фізичні явища, шо призводять до втрати інформації.

Інформаційно-комунікаційні системи, що використовуються для обробки інформації та інформаційного обміну, знаходяться у спеціалізованих приміщеннях – об'єктах інформаційної діяльності (ОІД). Тому в даному конспекті лекцій розглянуто фізичні причини виникнення радіоканалу (побічні електромагнітні випромінення (ПЕВМ) технічних засобів) та електричного (наведення ПЕВМ та просочування інформаційних сигналів в електричні лінії) витоку інформації. Розглянути активні та пасивні методи та засоби протидії витоку інформації через електричний та радіоканал.

Акустичний канал витоку інформації з ОІД виникає під час озвучування секретної інформації на ОІД. В даному конспекті лекцій розглянуто фізичні причини виникнення акустичного каналу як то – за рахунок вібрації інженерних конструкцій ОІД, акустоелектричних та параметричних перетворювань тощо. Розглянуто активні та пасивні методи та засоби протидії витоку акустичної інформації з ОІД.

Розглянуто причини виникнення матеріально-речового каналу витоку інформації з ОІД, та методи і засоби протидії даній загрозі інформації.

2. ЛЕКЦІЙНИЙ МАТЕРІАЛ

Лекція №1

Тема: Вступ до дисципліни. Термінологія

ПЛАН ЛЕКЦІЇ

1. Поняття інформації, її види.
2. Вимоги до захисту інформації.
3. Термінологія технічного захисту інформації.

1. Поняття інформації, її види

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (*Закон України Про інформацію № 2657-XII від 2 жовтня 1992 року).*

За змістом інформація поділяється на такі види:

інформація про фізичну особу;

інформація довідково-енциклопедичного характеру;

інформація про стан довкілля (екологічна інформація);

інформація про товар (роботу, послугу);

науково-технічна інформація;

податкова інформація;

правова інформація;

статистична інформація;

соціологічна інформація;

інші види інформації.

Інформація про фізичну особу (персональні дані) - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

Інформацією з обмеженим доступом є: конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за

бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

Інформація довідково-енциклопедичного характеру - систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище. Правовий режим інформації довідково-енциклопедичного характеру визначається законодавством та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Інформація про стан довкілля (екологічна інформація) - відомості та/або дані про:

- стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;

- фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми).

Інформація про стан довкілля, крім інформації про місце розташування військових об'єктів, не може бути віднесена до інформації з обмеженим доступом.

Інформація про товар (роботу, послугу) - відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги). Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Науково-технічна інформація - будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Правовий режим науково-технічної інформації визначається Законом України "Про науково-технічну інформацію", іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. Науково-технічна інформація є відкритою за режимом доступу, якщо інше не встановлено законами України.

Правова інформація - будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо. З метою забезпечення доступу до законодавчих та інших нормативних актів фізичним та юридичним особам держава забезпечує офіційне видання цих актів масовими тиражами у найкоротші строки після їх прийняття.

Соціологічна інформація - будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Для практичного використання більш важливою є класифікація інформації за режимом правового доступу до неї (рис. 1.1).

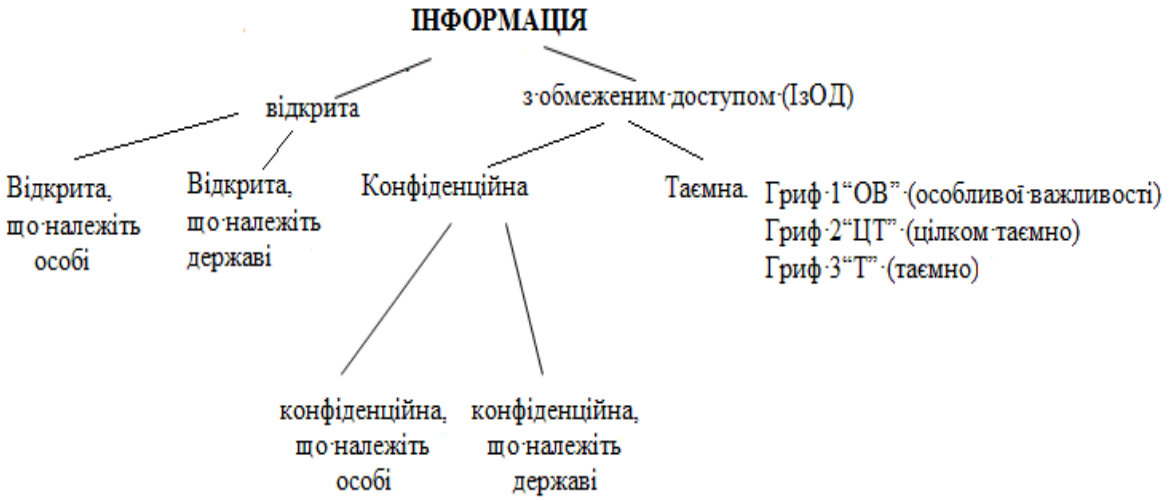


Рис. 1.1 Класифікації інформації за режимом правового доступу

Відкрита інформація – вся інформація окрім віднесеної законом до інформації з обмеженим доступом (п. 2 ст. 20 Закону Про інформацію).

Інформація з обмеженим доступом це інформація яка за своїм правовим режимом поділяється на *конфіденційну* і *таємну*.

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов. Стосовно інформації, що є власністю держави і знаходиться в користуванні органів державної влади чи органів місцевого самоврядування, підприємств, установ та організацій усіх форм власності, з метою її збереження може бути відповідно до закону встановлено обмежений доступ - надано статус конфіденційної.

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

Перелік посад, які дають право посадовим особам, що їх займають, надавати матеріальним носіям секретної інформації грифи секретності, затверджується керівником органу державної влади, органу місцевого самоврядування, підприємства, установи, організації, що провадить діяльність, пов'язану з державною таємницею.

Після закінчення встановлених строків засекречування матеріальних носіїв інформації та у разі підвищення чи зниження визначеного державним експертом з питань таємниць ступеня секретності такої інформації або скасування рішення про віднесення її до державної таємниці керівники органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, у яких здійснювалося засекречування матеріальних носіїв інформації, або керівники органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, які є їх правонаступниками, чи керівники вищого рівня зобов'язані протягом шести місяців забезпечити зміну грифа секретності або розсекречування цих матеріальних носіїв секретної інформації та письмово повідомити про це керівників органів державної влади, органів місцевого самоврядування, підприємств, установ, організацій, яким були передані такі матеріальні носії секретної інформації.

Об’єкт інформаційної діяльності – інженерно-технічна споруда, де здійснюється діяльність пов’язана з інформацією, яка підлягає захисту. (Закон України Про Державну службу спеціального зв’язку та захисту інформації України (ст.1) м. Київ, 23 лютого 2006 року №3475-IV).

2. Вимоги до захисту інформації.

Критерії інформаційної безпеки**:**

Цілісність — властивість інформації бути захищеною від несанкціонованого знищення, модифікації.

Конфіденційність — властивість інформації бути захищеною від несанкціонованого ознайомлення.

Доступність — властивість інформації бути захищеною від несанкціонованого блокування.

ПРАВИЛА
забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах

1. Ці Правила визначають загальні вимоги та організаційні засади забезпечення захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - система).

2. Дія цих Правил не поширюється на захист інформації в системах урядового та спеціальних видів зв'язку.

3. У Правилах наведені нижче терміни вживаються у такому значенні:

автентифікація - процедура встановлення належності користувачеві інформації в системі (далі - користувач) пред'явленого ним ідентифікатора;

ідентифікація - процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою.

Інші терміни вживаються у значенні, наведеному в Законах України "Про інформацію", "Про державну таємницю", "Про захист інформації в інформаційно-телекомунікаційних системах", "Про телекомунікації", Положенні про технічний захист інформації в Україні, затвердженому Указом Президента України від 27 вересня 1999 р. N 1229.

4. Захисту в інформаційно-телекомунікаційній системі підлягає:

відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами (далі - відкрита інформація);

конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу (далі - конфіденційна інформація);

інформація, що становить державну або іншу передбачену законом таємницю (далі - таємна інформація).

Вимоги до забезпечення захисту інформації в ІТС:

5. **Відкрита інформація під час обробки в ІТС** повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення.

Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження.

Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

6. Під час обробки конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення.

7. Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися. У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

8. Вимоги до захисту в системі інформації, що становить державну таємницю, визначаються цими Правилами та законодавством у сфері охорони державної таємниці.

9. Забезпечення захисту в системі таємної інформації, що не становить державну таємницю, здійснюється згідно з вимогами до захисту конфіденційної інформації.

10. Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються її власником (розпорядником), якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

11. В ІТС здійснюється обов'язкова реєстрація:

результатів ідентифікації та автентифікації користувачів;

результатів виконання користувачем операцій з обробки інформації;

спроб несанкціонованих дій з інформацією;

фактів надання та позбавлення користувачів права доступу до інформації та її обробки;

результатів перевірки цілісності засобів захисту інформації.

12. Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

13. Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

14. Порядок підключення систем, в яких обробляється конфіденційна і таємна інформація, до глобальних мереж передачі даних визначається законодавством.

15. У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації.

Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

16. Відповідальність за забезпечення захисту інформації в системі, своєчасне розроблення необхідних для цього заходів та створення системи захисту покладається на керівника (заступника керівника) організації, яка є власником (розпорядником) системи, та керівників її структурних підрозділів, що забезпечують створення та експлуатацію системи.

17. Організація та проведення робіт із захисту інформації в системі здійснюється службою захисту інформації, яка забезпечує визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації. Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

Завдання Служби захисту інформації:

- організація та проведення робіт із захисту інформації в системі;
- визначення вимог до захисту інформації в системі, проектування, розроблення і модернізацію системи захисту, а також виконання робіт з її експлуатації та контролю за станом захищеності інформації.

Служба захисту інформації утворюється згідно з рішенням керівника організації, що є власником (розпорядником) системи.

У разі коли обсяг робіт, пов'язаних із захистом інформації в системі, є незначний, захист інформації може здійснюватися однією особою.

План захисту інформації в системі містить:

завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

визначення моделі загроз для інформації в системі;

основні вимоги щодо захисту інформації та правила доступу до неї в системі;

перелік документів, згідно з якими здійснюється захист інформації в системі;

перелік і строки виконання робіт службою захисту інформації.

Перед створенням системи захисту інформації в ІТС або в ОІД розробляється модель загроз інформації. Модель загроз для інформації - формалізований опис методів та засобів здійснення загроз для інформації, ймовірності реалізації таких загроз та їх наслідків.

Види захисту інформації.

Організаційний захист інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціонування засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення

технічного захисту інформації. Організаційні заходи включають в себе створення концепції інформаційної безпеки, а також:

- складання посадових інструкцій для користувачів та обслуговуючого персоналу;

- створення правил адміністрування компонент інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

- розробка планів дій у разі виявлення спроб несанкціонованого доступу до інформаційних ресурсів системи, виходу з ладу засобів захисту, виникнення надзвичайної ситуації;

- навчання правилам інформаційної безпеки користувачів.

Інженерний захист інформації — попередження руйнування носія інформації внаслідок навмисних дій або природного впливу інженерно-технічними засобами (сюди відносять обмежуючі конструкції, охоронно-пожежна сигналізація). Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" №80/94-ВР від 05.07.1994 визначає інженерний ЗІ як складову технічного захисту інформації.

Технічний захист інформації - діяльність, спрямована на запобігання порушенню цілісності, блокуванню та (чи) витоку інформації технічними каналами.

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

Несанкціонований доступ до інформації в ІТС – це доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Несанкціонований доступ може здійснюватись як з використанням штатних засобів, тобто сукупності програмно-апаратного забезпечення, включеного до складу комп'ютерної системи (КС) розробником під час розробки або системним адміністратором в процесі експлуатації, що входять у затверджену конфігурацію КС, так і з використанням програмно-апаратних засобів, включених до складу КС зловмисником.

До основних способів НСД відносяться:

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

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

- модифікація засобів захисту, що дозволяє здійснити НСД;

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

Засіб технічного захисту інформації від НСД – це програмний, апаратний або програмно-апаратний засіб, який створюється як окремий продукт

виробництва, має необхідну програмну та/або конструкторську документацію і забезпечує самостійно або в комплексі з іншими засобами захист від загроз НСД для інформації в КС, або використовується для контролю ефективності захисту інформації від НСД в таких системах.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне та системне програмне забезпечення.
- апаратна частина серверів та робочих станцій.
- комунікаційне обладнання та канали зв'язку.
- периметр інформаційної системи.

Технічний захист інформації (ТЗІ) від НСД на прикладному і програмному рівні.

Для захисту інформації на рівні *прикладного та системного ПЗ* використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації та автентифікації;
- системи аудиту та моніторингу;
- системи антивірусного захисту.

ТЗІ від НСД на апаратному рівні.

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі
- системи сигналізації
- засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.

ТЗІ від НСД на мережевому рівні.

В комунікаційних системах використовуються такі засоби мережевого захисту інформації:

- міжмережеві екрани — для блокування атак з зовнішнього середовища. Вони керують проходженням мереженого трафіку відповідно до правил захисту. Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі;

- системи виявлення втручань — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні». Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі

- засоби створення віртуальних приватних мереж — для організації захищених каналів передачі даних через незахищене середовище. Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;

- засоби аналізу захищеності — для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації. Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Для захисту периметра ОІД створюються:

- системи охоронної й пожежної сигналізації;
- системи цифрового відеоспостереження;
- системи контролю й управління доступом (СКУД).

Контрольована зона – простір (територія, будівля, частина будівлі), в якому виключено неконтрольоване знаходження співробітників та відвідуівчів організації, а також транспортних засобів. Межою контрольованої зони може бути периметр території організації, а також обмежуючі конструкції охороаняємої будівлі або охороаняємої частини будівлі, якщо воно розміщено на території яка не охороняється.

Комплекс технічного захисту інформації - сукупність заходів і засобів, призначених для реалізації технічного захисту інформації на ОІД. Для оцінки ефективності комплексу ТЗІ проводиться його атестація на відповідність вимогам нормативних документів.

З метою обґрунтування заходів з технічного захисту ІзОД, що циркулює на об'єктах, проводиться, так зване, категорирование. Категорування підлягають об'єкти, в яких обговорюється, циркулює, пересилається, приймається, перетворюється, накопичується, обробляється, відображається і зберігається інформація з обмеженим доступом (ІзОД).

3. Термінологія ТЗІ

Згідно з Положенням про технічний захист інформації в Україні Затвердженим Указом Президента України від 27 вересня 1999 р. № 1229:

Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їх керівників.

Нормативно-правові акти з технічного захисту інформації є обов'язковими для виконання всіма суб'єктами системи технічного захисту інформації.

Об'єкти технічного захисту в ІТС - інформація, що обробляється в ній, та програмне забезпечення, яке призначено для обробки цієї інформації.

Суб'єкти системи технічного захисту інформації:

- Держспецзв'язку України; *(Абзац другий пункту 8 із змінами, внесеними згідно з Указом Президента N 333/2008 від 11.04.2008)*
- органи, щодо яких здійснюється ТЗІ;
- науково-дослідні та науково-виробничі установи Держспецзв'язку України, державні підприємства, що перебувають в управлінні Держспецзв'язку України та виконують завдання з питань технічного захисту інформації;

- військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з технічного захисту інформації за відповідними дозволами або ліцензіями;

- навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з технічного захисту інформації.

Основними завданнями органів, щодо яких здійснюється ТЗІ, є:

- забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

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

- здійснення контролю за станом технічного захисту інформації.

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

Загроза — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Безпека інформації — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Комплекс засобів захисту (КЗЗ) від несанкціонованих дій з інформаціїю — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Захищена комп'ютерна система;— комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

Користувач — фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

Об'єкт-користувач — подання фізичного користувача в КС, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

Ідентифікатор об'єкта КС — унікальний атрибут об'єкта КС, що дозволяє однозначно виділити даний об'єкт серед подібних.

Санкціонований доступ до інформації — доступ до інформації, що не порушує ПРД (правила розмежування доступу).

Захист від несанкціонованого доступу; захист від НСД — запобігання або істотне утруднення несанкціонованого доступу до інформації.

Право доступу — дозвіл або заборона здійснення певного типу доступу.

Повноваження — права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів.

Авторизація — надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створившим його користувачем або процесом).

Авторизований користувач — користувач, що володіє певними повноваженнями.

Роль користувача — сукупність функцій щодо керування КС, КЗЗ і обробки інформації, доступних користувачеві.

Адміністратор безпеки — адміністратор, відповідальний за дотримання політики безпеки.

Порушник — користувач, який здійснює несанкціонований доступ до інформації.

Критична інформація — інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

Цілісність системи — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Спостереженість — властивість КС, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і/або забезпечення відповідальності за певні дії.

Атака — спроба реалізації загрози.

процесом часових характеристик системи (наприклад, часу зайнятості центрального процесора), що спостерігаються іншим процесом.

Ризик — функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Ідентифікація — процедура присвоєння ідентифікатора об’єкту КС або встановлення відповідності між об’єктом і його ідентифікатором; впізнання.

Автентифікація — процедура перевірки відповідності пред’явленого ідентифікатора об’єкта КС на предмет належності його цьому об’єкту; встановлення або підтвердження автентичності.

Цифровий підпис — дані, одержані в результаті криптографічного перетворення блоку даних і/або його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дозволяють приймальнику даних впевнитись в цілісності блоку і справжності джерела даних і забезпечити захист від підробки і підлогу.

Контрольні запитання

1. Доповісти розподіл інформації по видам за змістом.
2. Визначення конфіденційної інформації про фізичну особу
3. Доповісти вимоги до захисту відкритої інформації.

4. Доповісти вимоги до захисту конфіденційної та таємної інформації
5. Визначення інформації з обмеженим доступом.
6. Визначення таємної інформації.
7. Назвати критерії безпеки інформації.
8. Визначення доступності інформації.
9. Визначення цілісності інформації.
10. Сутність організаційного захисту інформації.
11. Визначення об’єкту інформаційної діяльності.
12. Сутність інженерного захисту інформації.
13. Визначення несанкціонованого доступу до інформації.
14. Призначення технічного захисту інформації.
15. Визначення контрольованої зони.
16. Визначення ідентифікації та автентифікації.
17. В яких складових інформаційної системи здійснюється захист від НСД.
18. Як здійснюється захист від НСД на мережевому рівні.
19. Що є об'єктом технічного захисту в ІТС.
20. Визначення політики безпеки інформації.

Лекція № 2

Тема. Інформація як об’єкт захисту

ПЛАН ЛЕКЦІЇ.

1. Загрози інформації
2. Небезпечні сигнали та їх джерела
3. Класифікація технічних каналів витоку інформації

1. Загрози інформації.

Впливи які створюються зловмисниками на інформацію є навмисними. До них відносяться як безпосередній вплив зловмисника на джерело інформації так і вплив полів та електричних сигналів технічними засобами, що створюється людиною, з метою знищення, зміни або крадіжки інформації.

Ці впливи створюють *канал несанкціонованого доступу до інформації*. Якщо впливи цілеспрямовано створюються то канал несанкціонованого доступу називається навмисний, якщо сили випадкові то канал НСД зветься випадковий.

Навмисний канал НСД створюється зловмисником.

Типові причини створення каналу несанкціонованого доступу:

- виконання операції по здобуванню інформації розвідкою іноземної держави;
- спроба несанкціоновано отримати інформацію співробітником організації для її продажу, шантажу;
- несправність програмно-апаратних засобів зберігання, обробки передачі інформації;
- помилки персоналу при обробці інформації.

Несанкціоноване розповсюдження інформації від її джерела до зловмисника називається *витоком інформації*.

Розрізняють:

- спостереження – прийом оптичних та інших сигналів для отримання зображень;
- прослуховування – прийом та аналіз акустичних сигналів.
- перехоплення – прийом та аналіз радіо та електричних сигналів.

Прослуховування розуміє використання різних технічних засобів. Цим способом здобувається різноманітна мовна інформація.

Спостереженням добувається видові ознаки об’єктів, але можливе добування семантичної інформації. Для добування інформації також застосовуються технічні засоби: відеокамери видимого діапазону, прилади чутливі до ІЧ випромінення, радіолокаційне спостереження.

Перехоплення розуміє несанкціонований прийом радіо та електричних сигналів і вилучення з них семантичної інформації, демаскуючих ознак сигналів, формування зображення об'єктів.

Різноманіття технічних засобів та їх комплексне застосування для отримання інформації іноді розмивають грані між розглянутими способами. Наприклад при перехоплення сигналів состового зв'язку здійснюється підслуховування розмови між абонентами, тобто одночасно здійснюється перехоплення і прослуховування. Враховуючи неоднозначність понять *Перехоплення та Прослуховування,* способи добування акустичної інформації відносять до прослуховування а несанкціонований прийом радіо та електричних сигналів до *Перехоплення.*

Шлях несанкціонованого розповсюдження інформації від джерела до зловмисника називається ***каналом витоку інформації***. Якщо розповсюдження інформації здійснюється за допомогою технічних засобів то канал витоку інформації називається ***технічним каналом витоку інформації***. Загрози витоку бувають *випадкові* та такі *навмисно* створювані зловмисником. Якщо характеристики джерел сигналів зловмиснику апріорі невідомі, то технічні канали витоку інформації називаються інформації називаються *випадкові*. Якщо технічний канал витоку інформації організується зловмисником наприклад за допомогою закладного пристрою (подслушка) то такий канал витоку інформації називається *організованим*.

Загроза витоку інформації оцінюється по величині шкоди, яка виникає при її реалізації. Розрізняють *потенційну* та *реальну* шкоду. Потенційна шкода існує при появі загрози. Реальна – при реалізації загрози витоку. Ймовірність або ризик виникнення загрози залежить від багатьох факторів. Основні з них:

- ціна інформації;
- рівень захищеності інформації;
- кваліфікація зловмиснику, його витрати на здобування інформації;
- криміногенна обстановка у місці знаходження організації.

2. Небезпечні сигнали

Носії інформації у вигляді електричного струму та полів називаються *сигналами*. Якщо інформація, що міститься в сигналах таємна, а сигнали можуть бути прийняті зловмисникомі і з них знята ці інформація, то такі сигнали являють собою небезпеку для інформації і називаються *небезпечними*.

Небезпечні сигнали можуть бути *функціональними та випадковими*.

Функціональні сигнали створюються радіотехнічним засобом. Для виконання ним функцій по обробці, передачі, зберігання інформації. При передачі

таємної інформації функціональними сигналами, її відправник розуміє потенційні загрози безпеці інформації.

Основні джерела функціональних сигналів:

передавачі систем зв'язку;

передавачі радіотехнічних систем;

випромінювачі акустичних сигналів;

Засоби систем зв'язку створюють найбільш багаточисленну групу джерел з семантичною інформацією. Сюди відносяться засоби радіозв'язку, проводний, радіорелейний, космічний зв'язок.

Також джерелами радіосигналів, що випромінюються навколо являються стаціонарні та мобільні радіопередавальні пристрої систем радіозв'язк, а електричних сигналів що передаються по проводам – телефонні, телеграфні прилади; ПЕОМ що обєднані мережею, модеми апаратури передачі даних.

Також в останній час для передачі інформації в якості джерел сигналів використовують лазери оптичних засобів зв'язку. Оптичні системи мають значно кращі показники по смузі пропускання та завадостійкості. Кабелі волоконно-оптичних систем зв'язку поступово витісняють кабелі пропводних систем електрозв'язку.

Радіо, електричні та світові сигнали циркулюють як внутрі організації так і можуть розповсюджуватись на великі відстані. Враховуючи широке застосування засобів зв'язку і велику дальність їх розповсюдження, перехоплення сигналів засобів зв'язку є дуже ефективним та розповсюдженим методом отримання інформації.сигнали засобів зв'язку містять не тілки семантичну інформацію, а й інформацію про ознаки сигналів та місце розташування самих засобів зв'язку.

До радіотехнічних систем та засобів відносяться засоби радіолокації, радіотелеметрії та радіопротидії (РЕБ).

Але потенційна небезпека для інформації, яка міститься в функціональних сигналах відома її власнику. Він може прийняти міри для зниження небезпеки.

Однак робота радіоелектронних засобів що використовуються для прийому, обробки та зберігання інформації супроводжується фізичними процесами та явищами які стіорюють прбічні радіо та електричні сигнали. Якщо ці сигнали містять секретну інформацію і к ним можливий доступ технічних засобів зловмисника, то небезпека до цієї інформації значно вища ніж для аналогічної інформації що міститьсяв функціональних сигналах. Такі сигнали, що виникають випадково, називаються *випадковими небезпечними сигналами.* Ці сигнали виникають в силу фізичних процесів, незалежно від користувача цього засобу. Користувач без проведення спеціальних досліджень може й не знати про їх існування і що інформація піддається небезпеці. В цьому полігає відмінність функціональних небезпечних ситналів від випадкових небезпеяних сигналів. До

технічних засобів обробки інформації які створюють небезпечні сигнали відносяться:

засоби телефонного проводного зв'язку;

засоби мобільного телефонного та радіозв'язку;

засоби електронної обчислювальної техніки;

радіоприйомні паристрої;

телевізійні засоби.

Крім того випадкові небезпечні сигнали створюються електричними приладами:

засоби охоронної та пожежної сигналізації;

засоби кондиціонування повітря;

побутові прилади, оргтехніка та інше обладнання яке має у своєму складі елементи перетворення акустичної інформації у електричні сигнали;

електропроводящі комунікації будівлі які проходять через контрольовану зону.

Характеристики випадкових небезпечних сигналів радіоелектронних засобів апріорі невідомі ні зловмиснику ні користувачеві. Для їх пошуку та визначення характеристик проводять спеціальні дослідження цих засобів.

Усі технічні засоби на об'єктах інформаційної діяльності діляться на основні технічні засоби та системи (ОТЗС) та допоміжні технічні засоби та системи (ДТЗС).

До ОТЗС відносяться засоби та їх комунікації які забезпечують обробку, зберігання та передачу інформації яку потрібно захищати.

Якщо технічний засіб на ОІД не призначено для обробки таємної інформації його називають ДТЗС. ДТЗС знаходяться у одному приміщенні з ОТЗС. З цього слідує, що ДТЗС необхідно розглядати як потенційні джерела небезпечних сигналів. До ДТЗС наприклад відносяться:

телефонні засоби та системи;

засоби охоронно-пожежної сигналізації

засоби кондиціонування повітря;

засоби електронної оргтехніки;

засоби проводної радіотрансляційної мережі.

3. Классифікація технічних каналів витоку інформації

При обробці інформації в автоматизованих системах на об'єктах інформаційної діяльності можливий її витік так званими технічними каналами витоку.

Фізичні процеси, які у пристроях обробки інформації на ОІД при її функціонуванні, створюють у навколишньому просторі побічні електромагнітні,

акустичні та інші випромінювання, які тією чи іншою мірою пов'язані з обробкою інформації.

Подібні випромінювання можуть бути виявлені на досить значних відстанях (до сотень метрів) і, отже, використовуватися зловмисниками, які намагаються отримати доступ до секретів. Тому заходи щодо ЗІ, що циркулює в технічних засобах, спрямовані насамперед на зниження рівнів таких випромінювань.

Побічні електромагнітні випромінювання виникають внаслідок непередбаченої схемою або конструкцією технічного засобу передачі інформації з паразитних зв'язків напруги, струму, заряду або магнітного поля.

Під паразитним зв'язком розуміють зв'язок електричним або магнітним ланцюгам, що з'являється незалежно від бажання конструктора. Залежно від фізичної природи елементів паразитних електричних кіл розрізняють паразитний зв'язок через загальний повний опір, ємнісний або індуктивний паразитний зв'язок.

Під технічним каналом витоку інформації розуміється сукупність фізичних полів, що несуть таємну інформацію, конструктивних елементів, що взаємодіють з ними, та технічних засобів зловмисника для реєстрації поля та зняття інформації (рис. 1.2).

Рис. 1.2 Склад технічного каналу витоку інформації

Перехоплення інформації за допомогою технічних засобів може здійснюватись лише за межами контрольованої зони – території об'єкта, на якій виключено неконтрольоване перебування осіб та транспортних засобів, які не мають постійних чи разових перепусток.

Джерелами випромінювань у технічних каналах є різноманітні технічні засоби, у яких циркулює інформація з обмеженим доступом.

Такими засобами можуть бути:

мережі електроживлення та лінії заземлення;

автоматичні мережі телефонного зв'язку;

засоби звуко- та відеозапису;

електронно-обчислювальна техніка;

електронні засоби оргтехніки.

Джерелом випромінювань у технічних каналах витоку може бути голосовий тракт людини, що викликає появу небезпечних акустичних випромінювань у приміщенні чи поза нею. Середовищем поширення акустичних випромінювань у разі є повітря, а при закритих вікнах і дверях — повітря і всілякі звукопровідні комунікації. Якщо для перехоплення інформації використовується відповідна техніка, то утворюється технічний канал витоку інформації, так званий акустичним.

В загалі, в інформаційній безпеці, прийняти наступні технічні канали витоку інформації:

радіоканали (побічні електромагнітні випромінювання технічних засобів);

акустичні (поширення звукових коливань у будь-якому звукопровідному матеріалі);

електричні (небезпечні напруги та струми в різних струмопровідних комунікаціях);

оптичні канали (електромагнітні випромінювання в інфрачервоній, видимій та ультрафіолетовій частині спектру (ВОЛЗ));

матеріально-речові канали (папір, фото, магнітні носії, відходи тощо

Утворенню технічних каналів витоку інформації сприяють певні обставини та причини технічного характеру. До них можна віднести недосконаліть елементної бази та схемних рішень, прийнятих для даної категорії технічних засобів, експлуатаційне зношування елементів виробу, а також зловмисні дії.

Основними джерелами виникнення технічних каналів витоку інформації є:

перетворювачі фізичних величин;

випромінювачі електромагнітних коливань;

паразитні зв'язки та наведення на провода та елементи електронних пристроїв.

Для кожної з цих груп, у свою чергу, можна виконати декомпозицію за принципом перетворення чи іншими параметрами. Так, за принципами перетворення акустичні перетворювачі поділяються на індуктивні, ємнісні, п'єзоелектричні.

Декомпозиція випромінювачів електромагнітних коливань виконується діапазоном частот.

Паразитні зв'язки та наведення виявляються у вигляді зворотного зв'язку (найбільш характерний позитивний зворотний зв'язок), витоку по ланцюгах живлення та заземлення.

Технічні засоби та системи можуть не тільки безпосередньо випромінювати в простір сигнали, що містять оброблювану ними інформацію, але і вловлювати за рахунок своїх мікрофонних або антенних властивостей акустичні або електромагнітні випромінювання, що існують в безпосередній близькості від них. Такі технічні засоби можуть перетворювати прийняті випромінювання на електричні сигнали і передавати їх по своїм лініям зв'язку, як правило,

безконтрольним, за територією об'єкта на значні відстані, що ще більшою мірою підвищує небезпеку витоку інформації.

Непоодинокі випадки, коли технічні пристрої мають у своєму складі, крім подібних "мікрофонів" і "антен", високочастотні або імпульсні генератори. Генеровані коливання в таких пристроях можуть бути промодульовані електричними сигналами, внаслідок чого ці технічні пристрої перетворюються на радіопередавачі і становлять серйозну небезпеку, оскільки здатні випромінювати інформацію в навколишній простір.

До основних інформаційних характеристик каналу належать:

форма інформації, що передається (дискретна, безперервна) у ланках каналу;

швидкість передачі та обсяг інформації, що передається;

пропускна спроможність каналу;

ємність каналу.

Параметри каналу визначаються фізичною структурою каналу, його типом та режимом використання.

Ширина смуги пропускання (частотний спектр) каналу $\Delta \boldsymbol{F}$ змінюється від 3100 Гц для телефонного, до 8 МГц для телебачення і сотень мегагерц для оптичних ліній зв'язку.

Перевищення сигналу над перешкодою в каналі (динамічний діапазон), що визначається співвідношення потужностів сигналу і перешкоди в каналі, - здатність каналу передавати різні рівні сигналу. Динамічний діапазон обмежує дальність передачі, і навіть впливає можливість виділення сигналу на фоні перешкод:

$$Д = 10\log(P_{\text{с}} / P_{\text{п}}),$$

де:

$P_{\text{с}}$ и $P_{\text{п}}$ — середні потужності сигнала та перешкоди у каналі на вході приймача.

Кожен канал також характеризується кількістю інформації, яка може бути передана ним.

Максимальне значення **кількості інформації**, яка може бути передана каналом зв'язку, що має смугу пропускання *F*, визначається формулою Шеннона:

$$C_{\max} = F_{\text{к}} \log(1 + P_{\text{с}} / P_{\text{ш}}) \quad [\text{дв.одиниць/с}]$$

де:

$P_{\text{с}}$ — середня потужність сигналу, $P_{\text{ш}}$ — потужність перешкод з рівномірним частотним спектром.

Як у будь-якій системі зв'язку, у каналах витоку інформації небезпечний сигнал (сигнал, що несе секретну інформацію) характеризується тривалістю T_c, динамічним діапазоном D_c та шириною спектру F_c, добуток яких представляє його об'єм $V_c = T_c \cdot F_c \cdot D$.

У тривимірному просторі обсяг сигналу можна подати у вигляді паралелепіпеда (рис. 2.2).

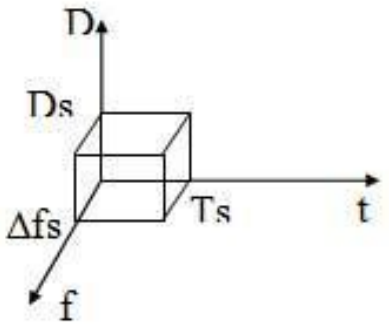


Рис. 2.2 Інтерпретація об'єму сигналу у тривимірному просторі

Якщо об'єм сигналу перевищує об'єм каналу передачі цього сигналу, то цим каналом зв'язку передача сигналу без втрати інформації неможлива. Тобто:

$$V_k . > V_c$$

Об'єм каналу визначається як:

$$V_k = D_k F_k T_k$$

де: T_k – час впродовж якого передається сигнал.

Для забезпечення неспотвореної передачі повідомлення визначеним об'ємом необхідно, щоб характеристики середовища розповсюдження та приймача відповідали ширині спектру сигналу та його динамічному діапазону.

Якщо полоса частот середовища розповсюдження або приймача вуже полоси сигналу то для забезпечення неспотворпеної передачі сигналу об'ємом V_c необхідно зменшити ширину його спектру. При цьому для забезпечення V_c = const відповідно необхідно збільшити час передачі сигналу T_c. Для неспотвореної передачі повідомлення у реальному масштабі часу смуга пропускання приймача повинна відповідати смузі спектра сигнала.

Узагальнена модель технічного каналу витоку інформації

Основою всіх сучасних технічних засобів є електронні та радіоелектронні пристрої. Фізичні процеси, що відбуваються в цих пристроях, створюють при

обробці закритої інформації об'єктивні передумови для появи небезпечних сигналів в навколишньому просторі, сторонніх інформаційних лініях, ланцюгах електроживлення, заземлення і т. д., що створює реальні умови для отримання передбачуваним противником закритих відомостей, що циркулюють технічні засоби, за допомогою засобів розвідки.

Фізичні явища, що лежать в основі появи небезпечних сигналів за межами контрольованої зони, та шляхи їх можливого витоку можуть бути різними. Тим не менш, у загальному вигляді витік інформації може розглядатися як ненавмисна передача закритої інформації деякою побічною системою зв'язку.

Перехоплення інформації за допомогою технічних засобів розвідки може здійснюватися лише за межами контрольованої зони – території об'єкта, де виключено неконтрольоване перебування осіб і транспортних засобів, які мають постійних чи разових перепусток.

В даний час перехоплення може бути організовано:

• з території посольства, місій, представництв іноземних держав та з належних їм будівель;

• із місць постійного чи тимчасового проживання іноземних громадян (житлових будинків, дач, готелів);

• із місць постійного чи тимчасового проживання розвідників;

• із дипломатичних автомобілів, обладнаних спеціальною технікою;

• з вулиць та транспортних засобів при розміщенні спец. апаратури в одязі, сумці, валізі тощо;

• із схованок, розміщених поблизу об'єкта захисту, із застосуванням закамуфльованих автономних пристроїв технічної розвідки.

Контрольні запитання.

1. Які існують групи загроз по виду реалізації
2. Причини виникнення каналів несанкціонованого доступу до інформації
3. Що називається витоком інформації і які причини її виникнення
4. Що називається технічним каналом витоку інформації
5. Чим оцінюється загроза витоку інформації
6. Що є джерелом загроз випадкових впливів
7. Які сигнали називаються небезпечними
8. Що відноситься до основних і допоміжних технічних засобів і систем при обробці інформації
9. Що розуміється під технічним каналом витоку інформації
10. Які існують технічні канали витоку інформації
11. Яка умова неспотвореної передачі сигналу по каналу зв’язку
12. Що називається об’ємом сигналу

13. Що вілноситься до основних інформаційних характеристик каналу зв’язку.

Лекція № 3

Тема: Класифікація існуючих технічних каналів витоку інформації

ПЛАН ЛЕКЦІЇ

1. Випромінювачі електромагнітних коливань
2. Класифікація радіоканалів витоку інформації
3. Класифікація акустичних каналів витоку інформації
4. Електричні канали витоку інформації
5. Оптичні канали витоку інформації
6. Матеріально-речовий канал витоку іеформації.

1. Випромінювачі електромагнітних коливань

Джерелами небезпечного сигналу (сигнал містить конфіденційну інформацію) є елементи, вузли і проводять ланцюга технічних засобів з струмами і напругами небезпечних сигналів, а також голосовий апарат людини і елементи технічних засобів, що створюють акустичні поля небезпечних сигналів.

До основних технічних засобів (ОТЗ) відносяться засоби, призначені для передачі, прийому, обробки та зберігання інформації з обмеженим доступом (ІзОД):

• електронно-обчислювальні машини (ЕОМ), в тому числі персональні (ПЕОМ);

• апаратура звукозапису, звуковідтворення і звукопідсилення;

• системи оперативно-командної і гучномовного зв'язку;

• системи внутрішнього телебачення;

• засоби виготовлення і розмноження документів.

Допоміжні технічні засоби (ДТЗ) не призначені для обробки ІзОД, але при спільному знаходженні з основними технічними системами і засобами або при установці в службових приміщеннях, де ведуться переговори або роботи, пов'язані з ІзОД, вони можуть сприяти витоку інформації або утворювати "самостійні" системи витоку .

До допоміжних технічних систем і засобів відносяться:

• системи відкритої телефонного зв'язку;

• системи радіотрансляції;

• системи електроживлення;

- кондиціонери

• системи охоронної та пожежної сигналізації.

Допоміжні технічні засоби, а також різного роду ланцюги, розташовані в безпосередній близькості від основних технічних систем і засобів, можуть

володіти антенних ефектом. Цей ефект полягає в перетворенні енергії електромагнітної хвилі що приходить від основних технічних систем і засобів в енергію електричних струмів. Вторинні технічні системи та засоби, а також їх електричні ланцюги, називаються також **випадковими приймальними антенами**.

До **зосереджених** випадкових прийомних антен відносяться телефонні апарати, електричні дзвінки, датчики охоронної та пожежної сигналізації тощо

До **розподілених** випадкових антен відносяться різного роду кабелі, проводи систем сигналізації, ретрансляційні мережі, труби, металеві конструкції і т.п. При проходженні небезпечних сигналів по елементам і ланцюгам технічних засобів, з'єднувальним лініях, в навколишньому просторі виникає електромагнітне поле. Тому такі лінії можна вважати випромінювачами. Всі джерела небезпечного сигналу що розглядають як випромінювачі, умовно підрозділяються на три типи: точкові, лінійні (розподілені) і площинні.

Крім того, електромагнітні випромінювання радіоелектронного обладнання (РЕО) можна розділити на основні і небажані. Небажані випромінювання поділяються на побічні, шумові.

Найбільш небезпечними з точки зору огляду каналів витоку інформації являються побічні випромінювання

Побічні випромінювання - це радіовипромінювання, що виникають в результаті будь-яких нелінійних процесів в радіоелектронному пристрої, крім процесів модуляції. Побічні випромінювання виникають як на основній частоті, так і на гармоніках, а також у вигляді їх взаємодії. Радіовипромінювання на гармоніці - це випромінювання на частоті (частотах), в ціле число разів більшою частоти основного випромінювання.

2. Класифікація радіоканалів витоку інформації.

Аналіз фізичної природи численних випромінювачів показує, що:

• джерелами небезпечного сигналу є елементи, вузли і провідники технічних засобів забезпечення виробничої та трудової діяльності, а також радіо- і електронна апаратура;

• кожне джерело небезпечного сигналу за певних умов може утворити технічний канал витоку інформації;

• кожна електронна система, що містить в собі сукупність елементів, вузлів і провідників, має деяким безліччю технічних каналів витоку інформації.

Радіоканали витоку інформації утворюються за рахунок:

- магнітного поля;

- паразитної генерації;

- за рахунок взаємного впливу радіоелементів;

- електромагнітного випромінювання.

За природою виникнення, діапазону випромінювання і середовищі поширення радіоканали витоку інформації класифікуються наступним чином (рис. 1.3).

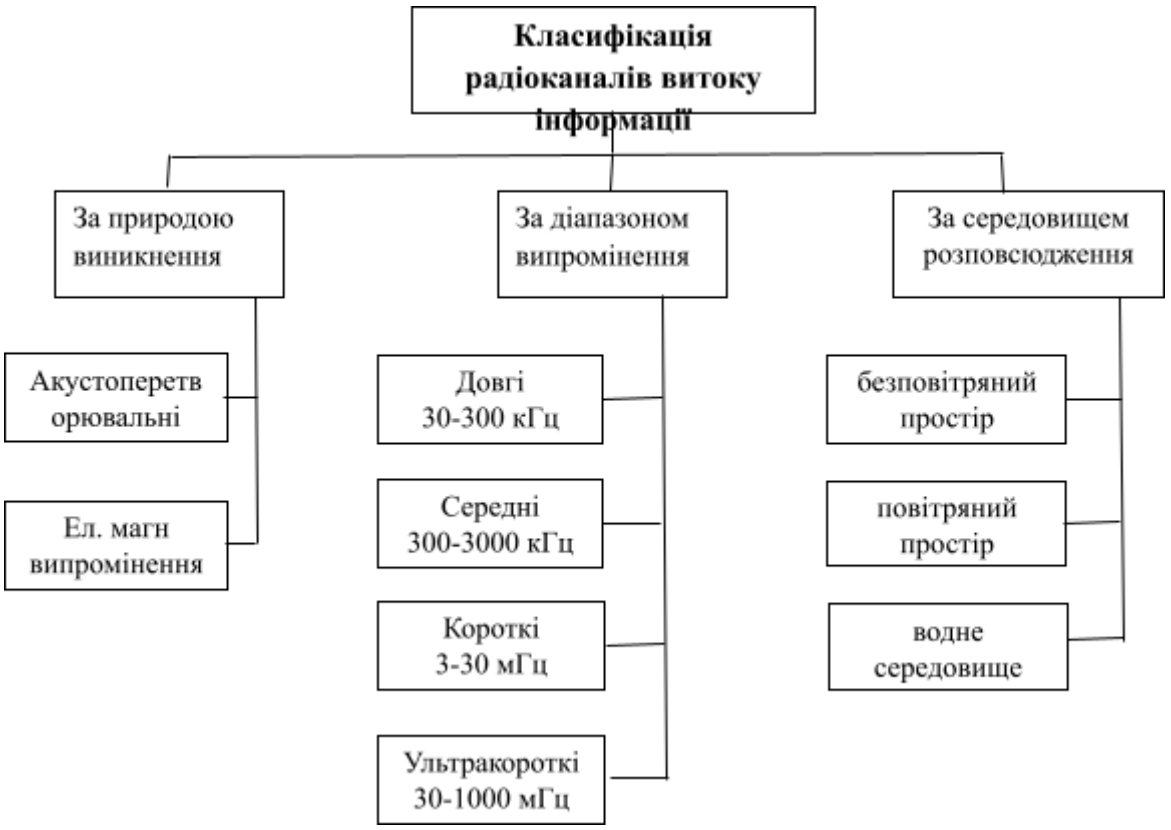


Рис. 1.3 Класифікація радіоканалів витоку інформації

3. Класифікація акустичних каналів витоку інформації

Основні визначення акустики

Перш ніж переходити до розгляду власне акустичних каналів витоку інформації, сформулюємо основні визначення акустики, на яких базуються відомості, наведені в цьому розділі.

Звуком називаються механічні коливання частинок пружного середовища (повітря, води, металу і т.д.), суб'єктивно сприймаються органом слуху. Звукові відчуття викликаються коливаннями середовища, що відбуваються в діапазоні частот від 16 до 20000 Гц.

Звуковий тиск - це змінний тиск в середовищі, обумовлене розповсюдженням в ній звукових хвиль. Величина звукового тиску оцінюється силою дії звукової хвилі на одиницю площі і виражається в ньютонах на квадратний метр (1 Н / $м^2$ = 10 бар).

Сила (інтенсивність) звука - кількість звукової енергії, що проходить за одиницю часу через одиницю площі; вимірюється в ватах на квадратний метр (Вт / $м^2$). Слід зазначити, що звуковий тиск і сила звуку пов'язані між собою квадратичною залежністю, тобто збільшення звукового тиску в 2 рази призводить до збільшення сили звуку в 4 рази.

Рівень сили звуку - відношення сили даного звуку до нульового (стандартному) рівню, за який прийнята сила звуку = 0-12 Вт / $м^2$, виражене в децибелах (дБ).

Рівні звукового тиску і сили звуку, виражені в децибелах, збігаються за величиною.

Поріг чутності - найбільш тихий звук, який ще здатний чути людина на частоті 1000 Гц, що відповідає звуковому тиску 20-5 $Н/м^2$

Гучність звуку - інтенсивність звукового відчуття, викликана цим звуком у людини з нормальним слухом. Гучність залежить від сили звуку і його частоти, вимірюється пропорційно логарифму сили звуку і виражається кількістю децибел, на яке даний звук перевищує по інтенсивності звук, прийнятий за поріг чутності. Одиниця виміру гучності - фон.

Динамічний діапазон - діапазон гучності звуку або різниця рівнів звукового тиску найгучнішого і самого тихого звуків, виражена в децибелах.

Акустичний канал витоку інформації утворюється за рахунок:

- поширення акустичних коливань у вільному повітряному просторі;
- впливу звукових коливань на елементи і конструкції будівель (віброакустичний канал);
- впливу звукових коливань на технічні засоби.

Механічні коливання стін, перекриттів, трубопроводів, що виникають в одному місці від впливу на них джерел звуку, передаються по будівельним конструкціям на значні відстані, майже не затухаючи, що не послаблюючи, і випромінюються в повітря як чутний звук. Небезпека такого акустичного каналу витоку інформації за елементами будівлі полягає в великий і неконтрольованої дальності поширення звукових хвиль, перетворених в пружні поздовжні хвилі в стінах і перекриттях, що дозволяє прослуховувати розмови на значних відстанях.

Також канал витоку акустичної інформації утворюють системи повітряної вентиляції приміщень, різні витяжні системи і системи подачі чистого повітря.

Первинними джерелами акустичних коливань є механічні системи, наприклад, органи промови людини, а вторинними - перетворювачі різного типу, в тому числі електроакустичні.

Останні являють собою пристрої, призначені для перетворення акустичних коливань в електричні і звортньо. До них відносяться п'єзоелементи, мікрофони, телефони, гучномовці та інші пристрої. Залежно від форми акустичних коливань

розрізняють прості (тональні) і складні сигнали. Мовний сигнал є складним акустичним сигналом в діапазоні частот від 200-300 Гц до 4-6 кГц.

Складний сигнал включає цілий спектр гармонійних складових.

Фізична природа, середовище поширення і спосіб перехоплення

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплення, акустичні шляхи витоку інформації бувають **повітряні, вібраційні, електроакустичні, оптико-електронні та параметричні.**

Конкретно по кожному.

Повітряні щляхи. У повітряних технічних каналах витоку інформації середовищем поширення акустичних сигналів є повітря, а для їх перехоплення використовуються мініатюрні високочутливі мікрофони і спеціальні спрямовані мікрофони.

Мікрофони об'єднуються або з'єднуються з портативними звукозаписними пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Перехоплена інформація може передаватися по радіоканалу, оптичного каналу (в інфрачервоному діапазоні довжин хвиль), по мережі електроживлення, з'єднувальним лініях ОТЗ, стороннім засобам (трубах водопостачання і каналізації, металоконструкцій і т.п.).

Вібраційні щляхи. У вібраційних (структурних) каналах витоку інформації середовищем поширення акустичних сигналів є конструкції будівель, споруд (стіни, стелі, підлоги), труби водопостачання, опалення, каналізації та інші тверді тіла. Для перехоплення акустичних коливань в цьому випадку використовуються контактні мікрофони (стетоскопи).

Електроакустичні щляхи. Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів в електричні. Перехоплення акустичних коливань здійснюється через ДТЗ, що володіють "мікрофонним ефектом" (перетворення акустичних мовних коливань повітряного середовища в електричні сигнали), а також шляхом "високочастотного нав'язування".

Оптико-електронний (оптичний) канал. Оптико-електронний (лазерний) канал витоку акустичної інформації утворюється при опроміненні лазерним променем вібруючих в акустичному полі тонких відображають поверхонь (скла, вікон, картин, дзеркал і т.д.). Відбите лазерне випромінювання (дифузне або дзеркальне) модулюється по амплітуді і фазі (згідно із законом вібрації поверхні) і приймається приймачем оптичного випромінювання, при демодуляції якого виділяється мовна інформація.

Параметричні канали. В результаті впливу акустичного поля змінюється тиск на всі елементи високочастотних генераторів ТЗПІ. При цьому змінюється

(незначно) взаємне розташування елементів схем, проводів в котушках індуктивності, дроселів і т.п., що може привести до змін параметрів високочастотного сигналу, наприклад, до модуляції його інформаційним сигналом. Тому цей канал витоку інформації називається параметричним. Це обумовлено тим, що незначна зміна взаємного розташування проводів в котушках індуктивності (межвиткової відстані) призводить до зміни їх індуктивності, а отже, до зміни частоти випромінювання генератора, тобто до частотної модуляції сигналу. Точно так же вплив акустичного поля на конденсатори призводить до зміни відстані між пластинами і, отже, до зміни його ємності, що, в свою чергу, також призводить до частотної модуляції високочастотного сигналу генерації. Найбільш часто спостерігається паразитна модуляція інформаційним сигналом випромінювань гетеродинов радіоприймальних і телевізійних пристроїв, що знаходяться в виділених приміщеннях і мають конденсатори змінної ємності з повітряним діелектриком в коливальних контурах гетеродинов.

Промодульовані інформаційним сигналом високочастотні коливання випромінюються в навколишній простір і можуть бути перехоплені і детектировать засобами радіорозвідки.

Параметричний канал витоку інформації може бути реалізований і шляхом ВЧ опромінення приміщення, де встановлені напівактивні заставні пристрої, що мають елементи, деякі параметри яких (наприклад, добротність і резонансна частота об'ємного резонатора) змінюються за законом зміни акустичного (мовного) сигналу.

За способом застосування технічні засоби отримання акустичної інформації можна класифікувати у такий спосіб.

Засоби, що використовуються шляхом таємного фізичного проникнення на об'єкт (заходові методи):

• радіозакладки;

• закладки з передачею акустичної інформації в інфрачервоному діапазоні;

• закладки з передачею інформації по мережі 220 В;

• закладки з передачею акустичної інформації по телефонній лінії;

• диктофони;

Засоби, що використовуються беззаходовими методами:

• апаратура, яка використовує мікрофонний ефект;

• високочастотне нав'язування;

• лазерні стетоскопи;

• спрямовані мікрофони.

Заходові методи

Перехоплення акустичної інформації за допомогою радіопередавальних засобів.

До них відноситься широка номенклатура радиозакладок (радіомікрофонів, "жучків"), призначенням яких є передача по радіоканалу акустичної інформації, одержуваної на об'єкті.

Застосування радіопередавальних засобів передбачає обов'язкову наявність приймача, за допомогою якого здійснюється прийом інформації від радіозакладки. Приймачі використовуються різні - від побутових (діапазон 88-108 МГц) до спеціальних.

Перехоплення акустичної інформації за допомогою ІЧ передавачів

Передача інформації може здійснюватися по ІЧ каналу. Акустичні закладки даного типу характеризуються крайньою складністю їх виявлення. Термін роботи цих виробів - кілька діб, але слід мати на увазі, що прослухати їх передачу можна лише на спецприймальнику і тільки в прямому візуальному контакті, тобто безпосередньо бачачи цю закладку. Тому розміщуються вони у вікон, вентиляційних отворів і т.п., що полегшує завдання їх пошуку. Основна перевага цих закладок - скритність їх роботи.

Закладки, які використовують в якості носія акустичної інформації мережу 220 В і телефонні лінії.

Подібність цих закладок в тому, що вони використовують у своїй роботі принцип низькочастотного ущільнення каналу передачі інформації. Оскільки в "чистих" лініях (220 В) і телефонних лініях присутні тільки сигнали на частотах 50 Гц і 300-3500 Гц відповідно, то передавачі таких закладок, транслюючи свою інформацію на частотах 100-250 кГц, не заважають роботі цих мереж. Підключивши до цих ліній спецприймач, можна знімати передану з закладки інформацію на дальність до 500 м.

Диктофони

Диктофони - пристрої, що записують голосову інформацію на деякий носій. Час запису різних диктофонів коливається в межах від 15 хв до 8 ч. Ця портативна апаратура звукозапису може здійснювати запис при неконтрольованому перебуванні фізичних осіб безпосередньо в виділених і захищаються. Диктофони забезпечують реєстрацію мови середньої гучності при видаленні мікрофона на відстань до 10-15 м від джерела мови.

Сучасні цифрові диктофони записують інформації у внутрішню пам'ять, що дозволяє проводити запис розмови тривалістю до декількох годин. Ці диктофони мають можливість скидання записаної інформації в пам'ять комп'ютера для її подальшої обробки (підвищення розбірливості мови, виділення корисних фонових сигналів і т.д.).

Беззаходові методи

Апаратура, яка використовує мікрофонний ефект телефонних апаратів

Прослуховування приміщень через телефон здійснюється за рахунок використання "мікрофонного ефекту". Недолік методу полягає в тому, що "мікрофонним ефектом" мають старі моделі телефонних апаратів, які зараз застосовуються рідко.

Апаратура ВЧ нав'язування.

ВЧ коливання проходять через мікрофон або деталі телефону, що володіють "мікрофонним ефектом" і модулюються в акустичний сигнал з приміщення, де встановлений телефонний апарат. Промодульований сигнал демодулюється амплітудним детектором і після підсилення подається на реєструючий пристрій.

Як мікрофон може працювати і будівля. Направлене на нього випромінювання високої частоти модулюється (змінюється) спеціальними конструктивними елементами, які здатні вловлювати звукові коливання, що виникають при розмові. Таким чином, відбите від будівлі випромінювання в зміненому вигляді несе з собою інформацію про те, що було виголошено всередині.

Електронний стетоскоп.

Стетоскопи - це пристрої, що перетворюють пружні механічні коливання твердих фізичних середовищ в акустичний сигнал. Стетоскопи дозволяють контролювати віброакустичні сигнали, що поширюються по будівельних конструкціях будівель, інженерних комунікацій. Вони можуть встановлюватися: на зовнішніх поверхнях будинків, на віконних отворах і рамах, в суміжних (службових і технічних) приміщеннях за дверними отворами, огороджувальними конструкціями, на перегородках, трубах систем опалення та водопостачання, коробах повітроводів вентиляційних і інших систем.

В сучасних стетоскопах у якості такого перетворювача служить пьезодатчик. Дана апаратура в основному застосовується для прослуховування сусідніх приміщень через стіни, стелі, підлогу або через труби центрального опалення. Професійна апаратура цього класу компактна (поміщається в кейсі середніх розмірів), автономна, має можливість підстроювання параметрів під конкретну робочу обстановку, здійснює запис отриманої інформації на диктофон. Стетоскопічніе датчики часто дообладнуються радіопередавачем, що дозволяє прослуховувати перехоплену інформацію на скануючий приймач, як від звичайної радіозакладки.

Лазерні системи акустичної розвідки (оптичні.)

На сьогоднішній день створено ціле сімейство лазерних засобів акустичної розвідки. Вони зазвичай складаються з джерела випромінювання (лазера), приймача цього випромінювання з блоком фільтрації шумів, джерела живлення, штатива і пристрої фільтрації отриманої інформації. Наведення лазерного випромінювання на шибку потрібного приміщення здійснюється за допомогою

телескопічного візира. Використовується оптична насадка, що дозволяє змінювати кут розходження променю, і система автоматичного регулювання, що забезпечує високу стабільність параметрів. Лазерна система акустичної розвідки (ЛСАР) забезпечує знімання мовної інформації з гарною якістю з віконних рам з подвійними скельцями на відстані до 250 м.

Досягнення в розвитку лазерної техніки дозволили значно поліпшити технічні характеристики і надійність роботи даних систем розвідки. Лазерні системи мають дальність ведення розвідки до 1000 м. З'явилися повідомлення про потенційну можливість роботи по об'єктах на відстані до 10 км.

Спрямовані акустичні мікрофони (САМ)

Дана техніка призначена для прослуховування акустичної інформації з певного напряму і з великих відстаней. Залежно від конструкції САМ, ширина головного променя діаграми спрямованості знаходиться в межах 5-30°, величина коефіцієнта посилення 5-20. За типом використовуваних антенних систем САМ бувають:

4. Електричні шляхи витоку інформації

Причини виникнення електричних каналів витоку інформації:

• гальванічні зв'язки з'єднувальних ліній ОТЗ (основних технічних засобів) з лініями ДТЗ (допоміжних технічних засобів) і сторонніми провідниками;

• наведення побічних електричних випромінювань ОТЗ на з'єднувальні лінії ДТЗ і сторонні провідники;

• наведення побічних електричних випромінювань ОТЗ на ланцюзі електроживлення і заземлення ОТЗ;

• «просочування» інформаційних сигналів у кола електроживлення і заземлення ОТЗ.

Одним з видів технічних каналів витоку інформації, що виникають при роботі засобів і систем інформатизації (електронно-обчислювальна, телевізійна й інша техніка), є канали, що з'являються за рахунок побічних електромагнітних випромінювань і наведень. До найбільш поширених каналів витоку інформації внаслідок наведень відносяться канали, які утворюються в мережі електроживлення технічних засобів і систем. Як правило дроти мережі електроживлення розподіляються по різним приміщенням де розташовані технічні системи та з'єднані з різними пристроями. Через це з'являється небажаний зв'язок між окремими технічними системами. Крім того провода мережі живлення є розподіленими випадковими антенами здатними випромінювати або приймати електромагнітні поля.

«Просочування» інформаційних сигналів у кола заземлення.

Крім заземлюючих провідників, призначених для безпосереднього з'єднання ОТЗ з контуром заземлення, гальванічний зв'язок з землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий провід мережі електроживлення, екрани (металеві оболонки) сполучних кабелів, металеві труби систем опалення та водопостачання, металева арматура залізобетонних конструкцій і т.д. Всі ці провідники спільно з заземлювальним пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали. Крім того, в грунті навколо заземлювального пристрою виникає електромагнітне поле, яке також є джерелом інформації.

При правильному проектуванні система заземлення виконує всі перераховані функції сприяє поліпшенню умов електромагнітної сумісності радіоелектронних засобів. У той же час помилки, допущені при проектуванні заземлений, можуть створювати умови для витоку секретної інформації за межі контрольованої зони.

Витік інформації по ланцюгах заземлення може виникнути:

- при наявності рознесених точок заземлення інформативних ланцюгів і утворення при цьому в різних точках системи заземлення різниці потенціалів і як наслідок виникнення в результаті цього струмів в ланцюгах заземлення;
- при великому значенні опору заземлення;
- внаслідок недосконалості екранів, що приводить до асиметрії ліній щодо екрану і виникнення в ланцюзі між корпусом екрану і землею інформативних струмів.

5. Класифікація оптичних каналів витоку інформації

Основою візуально-оптичного каналу є оптичне випромінювання, або світло. За діапазоном випромінювання візуально-оптичні канали витоку інформації можуть бути утворені у видимій (від 10 нм до 1 мм), інфрачервоної (від 1 мм до 770 нм) і ультрафіолетової (від 380 до 10 нм) областях спектра.

Візуально-оптичний спостереження є найбільш відомим, досить простим, широко поширеним і добре оснащеним найсучаснішими технічними засобами розвідки.

Оптичному каналу витоку інформації властиве:

- достовірність і точність видобутої інформації;
- висока оперативність отримання інформації;
- доступність реалізації;
- документальність отриманих відомостей (фото, кіно, TV).

Ці особливості визначають небезпеку даного виду каналів витоку інформації. Візуально-оптичні канали витоку інформації класифікуються наступним чином:

Оптичні методи є одними з найстаріших методів отримання інформації.

До них відносяться:

• візуальні методи спостереження;

• фотозйомка;

• відеозйомка.

Ці методи дозволяють отримувати інформацію як в звичайних умовах, так і при мінімальній освітленості, в інфрачервоному спектрі і за допомогою термографії, а також в повній темряві. В даний час для збору інформації по візуально-оптичним каналам широко застосовують волоконні світловоди і ПЗС-мікросхеми. Сучасні системи фотозйомки і відеозйомки дозволяють здійснювати дистанційне керування. Розроблено системи, здатні проводити зйомку практично в абсолютній темряві, що дозволяють фотографувати через найменші отвори.

Волоконно-оптичні лінії.

Причини виникнення випромінювання (витоку світловий інформації) в ВОЛЗ наступні:

а) радіальна неузгодженість стикуються волокон;

б) кутова неузгодженість осей світловодів;

в) наявність зазору між торцями світловода;

г) наявність взаємної непаралельности торців волокон;

д) різниця в діаметрах сердечників стикуються волокон.

Всі ці фактори призводять до випромінювання світлових сигналів в навколишній простір, що призводить до загасання, або втрати, корисного сигналу в волоконно-оптичних лініях зв'язку.

Контрольні запитання.

1. Що відноситься до допоміжних технічних систем і засобів і чому вони можуть сприяти витоку інформації?
2. Які випромінювання називаються побічними?
3. Перерахувати причини виникнення витоку світловий інформації в ВОЛЗ?
4. За рахунок чого утворюються радіоканали витоку інформації?
5. Як класифікуються радіоканали витоку інформації за діапазоном хвиль?
6. За рахунок чого утворюються акустичні канали витоку інформації?
7. Що називається випадковою антеною Які бувають?
8. Сутність заходового методу застосування технічного засобу знімання акустичної інформації.
9. Охарактеризувати спрямовані мікрофони.
10 Сутність беззаходового методу застосування технічного засобу знімання акустичної інформації
11. Назвати причини виникнення електричних каналів витоку інформації

12 В якому випадку може бути перехоплення інформаційних сигналів в лініях електроживлення і колах заземлення ОТЗ

13. Що мається на увазі під візуально-оптичним каналом витоку інформації.

Лекція № 4
Тема: Несанкціоноване отримання акустичної інформації

ПЛАН ЛЕКЦІЇ.

1. Найбільш поширені засоби несанкціонованого отримання акустичної інформації
2. Пристрої прослуховування приміщень
3. Пристрої отримання інформації з телефонних ліній

1. Найбільш поширені засоби несанкціонованого отримання акустичної інформації

Найбільш поширеними засобами несанкціонованого отримання інформації, з якими фахівцям із ЗІ часто доводиться стикатися на практиці.

1. Радіозакладки - мікропередавачі, радіус дії яких, як правило, не перевищує кількох сотень метрів. Сучасна елементна база дозволяє створювати радіозакладки в домашніх умовах.

2. Гостроспрямовані мікрофони, що мають голчасту діаграму спрямованості. За допомогою такого мікрофона можна прослухати розмову на відстані до 1 км у межах прямої видимості. За автомобілем, що рухається, аудіоконтроль вести можна тільки в тому випадку, якщо в ньому заздалегідь була встановлена закладка. На тривалих зупинках розмову можна прослуховувати спрямованим мікрофоном за умови, що автомобіль знаходиться в зоні прямої видимості і в ньому опущено одне зі стекол. У громадських місцях (кафе, ресторани тощо) прослуховування можна здійснювати спрямованим мікрофоном або закладкою. У таких випадках гучна музика, як втім і шум води, що ллється, не рятують, так як у спрямованого мікрофона дуже вузька діаграма спрямованості.

3. Засоби прослуховування телефонних розмов можуть здійснювати несанкціоноване отримання інформації за телефонною лінією кількома методами:

встановлення записуючої апаратури (ЗА) на АТС з використанням недобросовісності чи недбалості обслуговуючого персоналу;

безпосереднє підключення ЗА до телефонної лінії (наприклад, у розподільчій коробці);

вбудовування схеми несанкціонованого підключення до телефону (для цього необхідний доступ до приміщення, в якому встановлено цей апарат).

4. Якщо у приміщенні шибки не завішені, то розмову за такими вікнами можна прослухати, направивши на скло лазерний промінь. Звукові коливання в

приміщенні призводять до синхронної вібрації скла, а вони модулюють лазерний промінь, що відбивається від скла і приймається приймальним пристроєм.

5. У приміщеннях, в яких не було проведено спеціальних заходів щодо ЗІ, можна прослуховувати за допомогою пристроїв, що реєструють коливання елементів конструкції будівлі (розетки, батареї центрального опалення, вентиляція, тонкі перегородки тощо).

2. Пристрої прослуховування приміщень

До цієї групи пристроїв відносяться: приймальна апаратура, мікрофони, електронні стетоскопи, магнітофони та апаратура прослуховування телефонів.

Прослуховування - спосіб ведення розвідки, що застосовується агентами, спостерігачами, спеціальними постами прослуховування. Це один із поширених способів отримання (добування) інформації.

Прослуховування може здійснюватися безпосереднім сприйняттям акустичних коливань при прямому сприйнятті мовної інформації, або сприйнятті звукових коливань, що надходять через елементи будівель та приміщень (стіни, підлоги, стелі, вентиляційні канали, системи опалення), а також за допомогою різноманітних технічних засобів. До цього слід додати, що прослуховування ведеться в реальному масштабі часу та певною мірою може дозволити своєчасно ухвалити важливі оперативні рішення.

Прослуховування можна класифікувати так:

1. Безпосереднє

- пряме;
- через конструкції будівель та приміщень.

2. За допомогою технічних засобів

- за допомогою мікрофонів;
- за допомогою радіозакладок;
- лазерне підслуховування;
- ВЧ нав'язування.

Пристрої аудіоспостереження, за допомогою яких ведеться прослуховування, легко встановити і вкрай важко виявити, оскільки сучасна апаратура є мініатюрною, надійною і має тривалий термін дії.

Широке поширення набули прослуховувальні системи з акустоавтоматикою, що включаються автоматично під час звуку голосу.

Спрямований мікрофон

Використання явища резонансу звукових хвиль у спрямованих системах призводить до збільшення звукової енергії, що надходить мікрофон. Простий спрямований мікрофон є набір з 20 - 40 алюмінієвих трубок діаметром 10 мм

Довжина трубки визначає її резонансну частоту. Варіант розміщення спрямованих систем може бути реалізований за схемою, показаною на (рис. 1.4.)

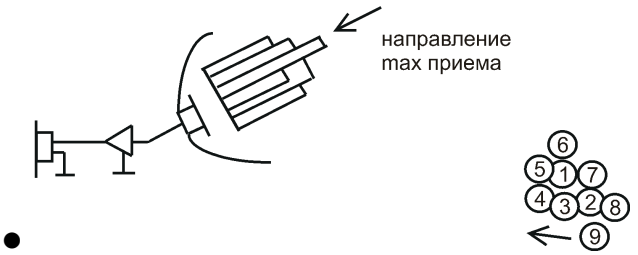


Рис. 1.4 Схема размещения спрямованих елементів спрямованого мікрофона

Довжина 20 мм відповідає частота 8200 Гц, а довжині 92 мм - частота 180 Гц. Довжину трубки можна розрахувати за формулою:

$$L(см) = 330/2F\ (Гц)$$

Мікрофон встановлюється в параболічному уловлювачі, фокусом якого є спрямовуюча система. Для подальшого посилення використовується високочутливий малошумний мікрофонний підсилювач. Для прослуховування розмови можна обмежитися набором з перших 7 трубок, оскільки основний частотний діапазон людської мови лежить у межах 180-215 Гц. Використовується в основному для прослуховування за межами приміщень.

На рис. 2.4 показано сучасний спрямований мікрофон.

Рис. 2.4 Сучасний спрямований мікрофон

Якщо немає можливості встановити пристрій стеження безпосередньо в приміщенні, інформація може бути отримана за допомогою електронних стетоскопів, які дозволяють прослуховувати розмови через вібрацію інженерних

конструкцій ОІД як то дверей, стель, вікон та бетонні стіни товщиною 50-70 см. або вікна, що прилягають до контрольованого приміщення (рис. 3.4)

Рис. 3.4 Зовнішній вигояд сучасних електронних стетоскопів

Найбільш дорогими пристроями, що перехоплюють акустичні сигнали є оптико-електронні (лазерні системи). На вікно направляється невидимий лазерний промінь, який модулюється коливаннями скла і відбивається на оптичний приймач, що перетворює його на аудіосигнали (рис. 4.4).

Рис. 4.4 Оптико-електронний (лазерний стетоскоп)

Часто для перехоплення розмов використовуються мініатюрні магнітофони. Такі пристрої вловлюють мову з відстані 8-10 м і здебільшого мають інтегрований акустоматик. Форма та розміри таких пристроїв дозволяють їх легко приховати, наприклад, у книзі середнього об'єму.

Важливим джерелом отримання інформації є лінія зв'язку, зокрема телефон. Прилади телефонного прослуховування можуть підключатися до будь-якої точки лінії, часто замасковані під різні деталі апарата. Закладки мають необмежений термін служби, оскільки живляться від телефонної лінії, причому функціонування телефону та лінії не порушується. Особливий інтерес становлять передавачі телефонного та кімнатного прослуховування, які після закінчення телефонної розмови автоматично перемикаються на спостереження за контрольованим приміщенням.

Поєднання відносно невисокої ціни і виключно високої ефективності таких пристроїв, а також відсутність суворих правових норм роблять цей канал витоку інформації одним із найнебезпечніших.

До основних типів радіопередаючих пристроїв прослуховування відносяться:

закладні пристрої (радіомікрофони);

телефонні закладки (можливі комбіновані варіанти із радіомікрофонами);

Закладки представлені широким спектром різноманітних варіантів виконання.

Встановлення радіозакладок у технічні засоби забезпечення виробничої діяльності виконується з метою одержання конфіденційної інформації акустичного характеру або інформації, що передається (опрацьовується) такими технічними засобами в електронній або електромагнітній формі.

Сигнал приймається звичайними або спеціальними радіоприймачами і фіксується на відповідній кінцевій апаратурі. Радіозакладки забезпечують реалізацію одного з найпоширеніших способів несанкціонованого доступу до джерел інформації – прослуховування. При цьому розмови, що перехоплюються, або звукові сигнали техніки та обладнання надходять до зловмисника на радіочастотах по радіо- або провідному каналам.

Мікрофонні радіозакладки - це мініатюрні радіопередавачі з вбудованим або винесеним мікрофоном. Останні застосовуються, якщо радіопередавач за будь-якими умовами не може передавати інформацію з певної зони, наприклад, через особливості поширення радіохвиль або жорсткого режиму радіоконтролю (рис. 5.4).

Рис. 5.4 Радіозакладний пристрій

Телефонні радіозакладки встановлюються в телефонні апарати або телефонну лінію в будь-якій точці між телефоном і АТС. Вони призначаються для прослуховування розмов з передачею їх зловмиснику на радіочастотах по ефіру. Телефонні радіозакладки також є мініатюрним радіопередавачем, як мікрофон якого використовується мікрофон телефонної трубки. Зручність такого рішення полягає в тому, що джерелом електроживлення закладки є телефонна лінія, що забезпечує її роботу до тих пір, поки працює АТС.

Перевагою телефонної радіозакладки є те, що прослуховується розмова обох абонентів, де б вони не розташовувалися.

Включатися телефонна радіозакладка може не тільки в телефонний апарат, а й у телефонну лінію і встановлюватися навіть поза приміщенням, де розташований телефон: у телефонній розетці, у коридорі на комутаційній коробці, у розподільчій шафі і навіть на самій АТС.

За конструктивними особливостями і принципом дії радіовипромінюючі пристрої, що прослуховують, можна *класифікувати* наступним чином.

За живленням:

з автономним живленням (від акумуляторів чи гальванічних елементів);

із зовнішнім живленням (від мережі змінного струму, від телефонної лінії тощо).

За тривалістю роботи:

необмежено (живлення від зовнішнього джерела);

від кількох годин до кількох тижнів.

По дальності дії: від одиниць до сотень метрів.

За конструктивним виконанням:

з камуфляжем під різні електро- та побутові предмети;

без елементів камуфляжу.

По частотному діапазону: від десятків кГц до сотень, а окремих випадках і тисяч МГц (найчастіше використовуються такі діапазони: 60–170, 250–290, 310–335, 360–430 і 470–1300 МГц).

За часом включення (роботи):

на запит;

безперервно.

Малі габаритні розміри, маса та використання елементів камуфляжу визначають широкий діапазон варіантів використання пристроїв, що прослуховують, і ускладнює їх виявлення. Радіозакладки підбираються індивідуально для конкретного приміщення. Це необхідно для того, щоб максимально ефективно використати можливості закладки.

3. Пристрої отримання інформації з телефонних ліній

Безпосереднє підключення до телефонної лінії — найпростіший та найнадійніший спосіб отримання інформації. У найпростішому випадку застосовується трубка ремонтника-телефоніста та навушники, підключені до лінії в розподільчій коробці, де проводиться розведення кабелів.

Для знімання інформації використовується високочастотне нав'язування (ВЧ). Під ВЧ нав'язуванням розуміється спосіб отримання інформації, при якому в телефонну лінію, що прослуховується, подають від спеціального генератора ВЧ коливання. Ці коливання за рахунок нелінійних елементів телефону взаємодіють з мовними сигналами при розмові (піднята телефонна трубка) або з електрорушійної сили мікрофонного ефекту апарату (поклдена трубка). Виходить щось на кшталт квазітелефонної радіозакладки, в якій генератор ВЧ коливань винесений, а нелінійність апарату виконує роль модулятора.

ВЧ нав'язування може використовуватися і на гучномовці та інші елементи, що володіють мікрофонним ефектом.

Принцип реалізації ВЧ нав'язування на телефон при покладеній телефонній трубці наступний (рис. 6.4).

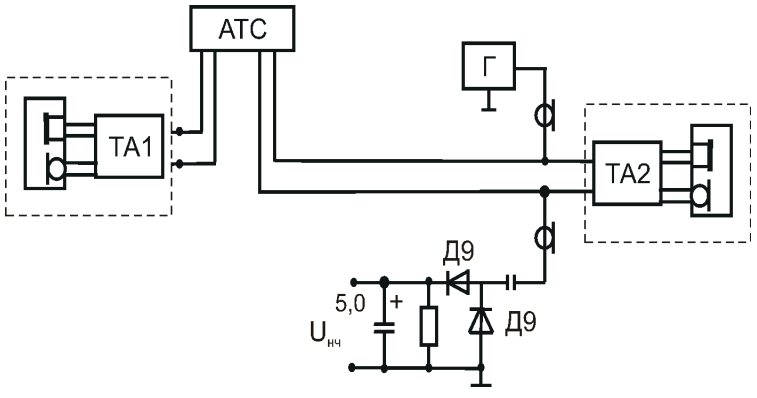


Рис. 6.4 Технічна реалізація методу ВЧ нав’язування

Відносно загального корпусу (як краще використовувати землю, труби опалення і т. д.) на один провід подаються ВЧ коливання частотою від 150 кГц і

вище. Через елементи схеми телефонного апарату (ТА), навіть якщо трубка лежить на апараті, ВЧ коливання надходять на мікрофон і далі вже промодульовані в лінію. Прийом інформації проводиться щодо загального корпусу через другий дріт лінії. Амплітудний детектор дозволяє отримати низькочастотну огинаючу для подальшого посилення та запису. Електрично не пов'язані, але розташовані елементи конструкції ТА за рахунок явища індукції є хорошими провідниками ВЧ коливань. Для якісної роботи такого пристрою бажано, щоб підключення ВЧ генератора і прийом промодульованого коливання ВЧ відбувався якомога ближче до ТА, щоб індуктивний вплив першого дроту на другий було мінімальним. Для виконання цієї умови ВЧ коливання подаються в лінію та знімаються лише екранованим дротом.

Також існує спосіб прослуховування за допомогою радіомікрофона з живленням від телефонної лінії. При цьому пристрій живиться з телефонної лінії та включається до неї послідовно з телефоном у будь-якому місці на ділянці від апарата до АТС.

Контрольні запитання

1. Назвати найпоширеніші засоби несанкціонованого отримання акустичної інформації, з якими спеціалістам часто доводиться стикатися на практиці?
2. Доповісти принцип дії електронного стетоскопу.
3. Пояснити для чого використовується лазерний стетоскоп?
4. Доповісти про мікрофонну радіозакладка?
5. Доповісти про телефонна радіозакладка?
6. Як класифікуються радіовипромінюючі пристрої, що прослуховують по: живленню, тривалості роботи, виду модуляції сигналу?
7. Доповісти сутність ВЧ нав'язування.
8. Для чого використовується спрямований мікрофон. Його принцип дії.

Лекція № 5
Тема: Захист акустичної інформації

ПЛАН ЛЕКЦІЇ.

1. Критерій захищеності акустичної інформації
2. Пасивні методи захисту акустичної інформації.
3. Активні методи захисту акустичної інформації.

1. Критерій захищеності акустичної інформації

Захист мовної інформації є важливим завданням в загальному комплексі заходів щодо забезпечення інф. безпеки об'єкта чи установи. Для її перехоплення передбачуваний «противник» може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, оптико-електронного (акустооптичні) каналам, до основною з яких відносяться:

• портативна апаратура звукозапису (малогабаритні диктофони, магніто-фони та пристрої запису на основі цифрової схемотехніки);

• спрямовані мікрофони;

• електронні стетоскопи;

• електронні пристрої перехоплення мовної інформації (закладні пристрої) з датчиками мікрофонного і контактного типів з передачею перехопленої інформації по радіо, оптичному (в інфрачервоному діапазоні довжин хвиль) і ультразвуковому каналам, мережі електроживлення, телефонних лініях зв'язку, з'єднувальним лініях допоміжних технічних засобів або спеціально прокладених лініях;

• оптико-електронні (лазерні стетоскопи) акустичні системи й т.д.

Використання тих чи інших методів і засобів визначається характеристиками об'єкта захисту і апаратурою розвідки, умовами її ведення, а також вимог, що пред'являються до ефективності захисту акустичної (мовної) інформації, як показник оцінки якої використовується **словісна розбірливість мови** на виході каналу витоку інформації. Критерії ефективності захисту акустичної (мовної) інформації багато в чому залежать від цілей, переслідуваних при організації захисту, наприклад:

• приховати смисловий зміст ведення розмови;

• приховати тематику ведення розмови і т.д.

Процес сприйняття мови в шумі супроводжується втратами складових елементів мовного повідомлення. Зрозумілість мовного повідомлення характеризується кількістю правильно прийнятих слів, що відбивають якісну

область зрозумілості, яка виражена в категоріях подробиці довідки про перехоплений розмові, яку зводять «агентом». З практичних міркувань може бути встановлена шкала оцінок якості перехопленого мовного повідомлення:

1. Перехоплене мовне повідомлення містить кількість правильно зрозумілих слів, достатнє для складання докладної довідки про практичний зміст перехопленого розмови.

2. Перехоплене мовне повідомлення містить кількість правильно зрозумілих слів, достатнє лише для складання короткої довідки-анотації, що відбиває предмет, проблему, мету і загальний сенс перехопленого розмови.

3. Перехоплене мовне повідомлення містить окремі правильно зрозумілі слова, що дозволяють встановити предмет розмови.

4. При прослуховуванні перехопленого мовного повідомлення можливо встановити факт наявності мови, але не можна встановити предмет розмови.

Відповідно до ГОСТ Р 50840-95 розуміння переданої по каналах зв'язку мови з великим напруженням уваги, перепитав і повтореннями спостерігається при складової розбірливості 25-40%, а при складової розбірливості менше 25% має місце нерозбірливість зв'язного тексту (зрив зв'язку) протягом тривалих інтервалів часу. З огляду на взаємозв'язок **словісної** і **складової** розбірливості, визначено, що зрив зв'язку буде спостерігатися при словісної чіткості менш 71%. Захист мовної інформації досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням електронних пристроїв перехоплення інформації. Використання тих чи інших методів і засобів визначається характеристиками об'єкта захисту і апаратури розвідки, умовами її ведення, а також вимог, що пред'являються до ефективності захисту акустичної (мовної) інформації, як показник оцінки якої найчастіше використовують словесну розбірливість мови *W*.

2. Пасивні методи захисту інформації.

Визначено, що для зниження розбірливості мови необхідно прагнути до зменшення відношення «рівень мовного сигналу / рівень шуму» (сигнал / шум) в місцях можливого розміщення датчиків апаратури акустичної розвідки. Зменшення відношення сигнал/шум можливо наступними способами (рис.1.5):

- Пасивні методи захисту (зменшення (ослаблення) рівня мовного сигналу);
- Активні методи захисту (збільшення рівня шуму (створення акустичних і вібраційних перешкод)).

Рис. 1.5 Методи захисту акустичної інформації

Ослаблення акустичних сигналів здійснюється шляхом звукоізоляції приміщень, яка спрямована на локалізацію джерел акустичних сигналів усередині них. Звукоізоляція оцінюється величиною ослаблення акустичного сигналу і забезпечується за допомогою архітектурних та інженерних рішень, а також застосуванням спеціальних будівельних та оздоблювальних матеріалів. У разі якщо звукоізоляція приміщення не забезпечує необхідної ефективності захисту інформації, то для її підвищення використовують спеціальні звукопоглинальні матеріали. Підвищення звукоізоляції стін і перегородок приміщення також досягається установкою на відстані в 6 ... 10 см від них одношарових і багатошарових (частіше подвійних) огороджень. У багатошарових огорожах доцільно підбирати матеріали шарів з різко відрізняються акустичними властивостями (наприклад, бетон — поролон). Для зниження величини вібраційного сигналу використовуються м'які віброізольовані опори, якими розв'язуються один від одного різні огороджувальні конструкції. В якості таких опор застосовують тверду гуму, пробку, свинець. Одним з найбільш слабких звукоізолюючих елементів огороджувальних конструкцій виділених приміщень є двері і вікна. Звукопоглинальна здатність вікон залежить, головним чином, від поверхневої густини скла і ступеня притиснення притворів. Збільшення звукоізолюючої здатності дверей досягається застосуванням ущільнюючих прокладок, оббивкою або облицюванням полотен дверей спеціальними

матеріалами. Для захисту інформації в особливо важливих приміщеннях використовуються двері зі звукоізольованим дверним прорізом, виконаному у вигляді тамбура з глибиною не менше 0,5 м При цьому внутрішній простір тамбура має бути оброблено звукопоглинальним матеріалом, полотна дверей обладнані ущільнювачами, а двері оббиті звукопоглиначем із оббивних матеріалів. В особливо важливих приміщеннях використовують спеціальні звукоізолюючі двері. Пасивні методи захисту інформації, як правило, реалізуються при будівництві або реконструкції будівель на етапі розробки проектних рішень, що дозволяє заздалегідь врахувати типи будівельних конструкцій, способи прокладки комунікацій, оптимальні місця розміщення виділених приміщень. У разі технічної неможливості використання пасивних засобів захисту приміщень або якщо вони не забезпечують необхідних норм по звукоізоляції, використовуються активні заходи захисту.

3. Активні методи захисту інформації

Якщо необхідно розробляти захист приміщення по акустичному каналу, слід впливати на середу поширення. Для цієї мети використовуються акустичні генератори шуму. Крім того, генератори шуму широко використовуються для оцінки акустичних властивостей приміщень. Під акустичним шумом розуміють шум, який характеризується нормальним розподілом амплітудного спектра і постійністю спектральної щільності потужності на всіх частотах. Для зашумлення приміщень широко застосовуються перешкоди, що представляють собою суміш випадкових і нерівномірних періодичних процесів. Найпростіші методи отримання білого шуму зводяться до використання шумливих електронних елементів (лампи, транзистори, різні діоди) з посиленням напруги шуму. Більш досконалими є цифрові генератори шуму, які генерують коливання, що представляють собою тимчасової випадковий процес, близький за своїми властивостями до процесу фізичних шумів. Цифрова послідовність двійкових символів в цифрових генераторах шуму являє собою послідовність прямокутних імпульсів з псевдовипадковими інтервалами між ними. Період повторень всієї послідовності значно перевищує найбільший інтервал між імпульсами. Найбільш часто для отримання сигналу зворотного зв'язку застосовуються послідовності максимальної довжини, які формуються за допомогою регістрів зсуву і підсумовуються по модулю За принципом дії всі технічні засоби просторового зашумлення можна розділити на три великі групи:

1. Засоби створення акустичних маскуючих перешкод (рис. 1.5):

- генератори шуму в акустичному діапазоні;
- пристрої віброакустичного захисту;
- технічні засоби ультразвукового захисту приміщень.

Генератори шуму в мовному діапазоні отримали досить широке поширення в практиці ЗІ. Вони використовуються для захисту від несанкціонованого зйому акустичної інформації шляхом маскування безпосередньо корисного звукового сигналу. Маскування проводиться білим шумом з коригувати спектральної характеристикою. Білий шум -стаціонарний шум (шум характеризується постійністю середніх параметрів: інтенсивності (потужності), розподілу інтенсивності по спектру (спектральна щільність), автокореляційної функції), спектральні складові якого рівномірно розподілені по всьому діапазону задіяних частот. Найбільш ефективним засобом захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалення, двері і т.д. є пристрої віброакустичного захисту. Дана апаратура дозволяє запобігти прослуховування за допомогою дротових мікрофонів, звукозаписної апаратури, радіомікрофонів і електронних стетоскопів, систем лазерного знімання акустичної інформації з вікон і т.д. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи конструкції будівлі.

Генератор формує білий шум в діапазоні звукових частот. Передача акустичних коливань на огороджувальні конструкції проводиться за допомогою п'єзоелектричних і електромагнітних вібраторів з елементами кріплення. Конструкція і частотний діапазон випромінювачів повинні забезпечувати ефективну передачу вібрації. Віброперетворювачі збуджують шумові віброколивання в огороджувальних приміщеннях, забезпечуючи при цьому мінімальний рівень перешкоджуваного акустичного сигналу в приміщенні, який практично не впливає на комфортність проведення переговорів. Передбачена в більшості виробів можливість підключення акустичних випромінювачів дозволяє зашумлять вентиляційні канали та дверні тамбури.

Як правило, є можливість плавного регулювання рівня шумового акустичного сигналу. Відмінною особливістю цих засобів є вплив на мікрофонний пристрій і його підсилювач достатньо могутнім ультразвуковим сигналом, що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що призводять, в кінцевому рахунку, до порушення працездатності мікрофонного пристрою. Оскільки вплив здійснюється по каналу сприйняття акустичного сигналу, то абсолютно не важливі його подальші трансформації і способи передачі. Акустичний сигнал пригнічується саме на етапі сприйняття чутливим елементом. Все це робить комплекс достатньо універсальним в порівнянні з іншими засобами активного захисту.

Захист від вбудованих і вузькоспрямованих мікрофонів.

Мікрофони, як відомо, перетворюють енергію звукового сигналу в електричні сигнали. У сукупності зі спеціальними підсилювачами і фільтрами вони використовуються в якості пристроїв аудіоконтролю приміщень. Для цього

створюється прихована провідна лінія зв'язку (або використовуються деякі з наявних в приміщенні провідних ланцюгів), виявити яку можна лише фізичним пошуком або за допомогою контрольних вимірів сигналів у всіх проводах, наявних в приміщенні. Природно, що методи радіоконтролю, ефективні для пошуку радіозакладок, в даному випадку не мають сенсу. Для захисту від вбудованих і вузько спрямованих мікрофонів рекомендуються такі заходи:

- При проведенні нарад слід обов'язково закривати вікна і двері (найкраще, щоб кімната для наради представляла собою ізольоване приміщення);

- Для проведення переговорів потрібно вибирати приміщення, стіни яких не є зовнішніми стінами будівлі;

- Необхідно забезпечити контроль приміщень, що знаходяться на одному поверсі з кімнатою для нарад, а також приміщень, що знаходяться на суміжних поверхах.

З застосовуваних зараз технічних засобів захисту (ТЗЗ) акустичної інформації можна виділити наступні основні групи:

- генератори акустичного шуму;

- нелінійні локатори;

- скремблери (системи захисту телефонних переговорів);

- детектори мережі 220 В 50 Гц;

- детектори підключень до телефонної лінії;

- комплекси, що забезпечують виконання декількох функцій по "очищенню приміщень";

Завдання технічної контррозвідки ускладнюється тим, що, як правило, невідомо, яке конкретно технічний пристрій контролю інформації застосовано. Тому робота з пошуку і знешкодження технічних засобів спостереження дає обнадійливий результат тільки в тому випадку, якщо вона проводиться комплексно, коли обстежать одночасно всі можливі шляхи витоку інформації. Класифікація пристроїв пошуку технічних засобів підслуховування може бути наступною:

1. Пристрої пошуку активного типу:

1). нелінійні локатори (досліджують відгук на вплив електромагнітним полем);

2). ретгенметри (просвічують за допомогою рентгенівської апаратури);

2. Пристрої пошуку пасивного типу:

1). металошукачі;

2). тепловізори;

3) пристрої та системи пошуку по електромагнітному випромінюванню (скануючий приймач, детектор електромагнітного поля);

4). пристрою пошуку по зміні параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);

5). пристрою пошуку по зміні магнітного поля (детектори записуючої апаратури).

Спеціальні приймачі для пошуку працюють передавачів в широкому діапазоні частот називають сканерами. З активних засобів пошуку апаратури прослуховування в основному використовують нелінійні локатори. Принцип їх дії заснований на тому, що при опроміненні радіоелектронних пристроїв, що містять нелінійні елементи, такі, як діоди, транзистори і т.п., відбувається відображення сигналу на вищих гармоніках. Відбиті сигнали реєструються локатором незалежно від режиму роботи радіоелектронного пристрою, тобто незалежно від того, включено воно або вимкнено. Для захисту приміщень широко використовуються пристрої постановки перешкод. Сигнали перешкоди радіодіапазоні прийнято ділити на загороджувальні і прицільні. Загороджувальна перешкода ставиться на весь широкий діапазон частот, в якому передбачається робота радіопередавача, а прицільна - точно на частоті цього пристрою радіосигналу. Принцип роботи постановника прицільної перешкоди полягає в наступному. Постановник перешкоди працює в автоматичному режимі. Приймач-сканер сканує весь радіодіапазон, а частотомір вимірює частоти виявлених радіопередавачів. Потім пристрій аналізує дані, що надходять і порівнює їх із записаними в пам'ять. При появі сигналів, про які в пам'яті відсутня інформація, видається команда радіопередавачу на постановку прицільної перешкоди. Недоліком таких комплексів є їх висока вартість.

Постановники перешкод інфрачервоного і надвисокочастотного діапазону є складними і дорогими системами. Це пов'язано з тим, що передавачі та приймачі цих діапазонів мають гостру діаграму спрямованості, і, щоб придушити сигнал передавача цих діапазонів, постановник перешкоди повинен точно встановити розташування приймального пристрою, інакше перешкода буде малоефективна. Отже, чим більше спрямованими антенами забезпечені радіомікрофони та їх приймальні пристрої, тим важче поставити проти них перешкоду. Крім того, при тому ж рівні сигналу такі радіолінії мають більшу дальність, що, в свою чергу, ускладнює постановку перешкод.

Найбільш поширеними є постановники перешкод акустичного діапазону з використанням функції створення віброзавад. Це відносно прості й недорогі пристрої, які створюють просторове зашумлення в основному спектрі звукових частот, що забезпечує маскування розмов і знижує ефективність систем прослуховування. Найбільшу ефективність дають пристрої, вібратори які встановлюються по периметру всього приміщення, в тому числі на підлогу, стелю, стіни, вентиляційні отвори та ін. (рис. 2.5).

Рис. 2.5 Генератор акустичного та віброакустичного шуму

Призначений для захисту об'єктів від витоку конфіденційної інформації акустичними та віброакустичними каналами (рис. 2.5) шляхом створення шумового сигналу в діапазоні частот від 180 Гц до 5,6 кГц.

Комплекс віброакустичного захисту " **РІАС-2ГС** " має чотири канали формування перешкод, до кожного з яких можуть підключатися віброперетворювачі п'єзоелектричного або електромагнітного типу, а також акустичні системи, що забезпечують перетворення електричного сигналу, який формується приладом, в механічні коливання в огороджувальних конструкціях приміщення, вікон, а також в акустичні коливання повітря.

Максимальна вихідна потужність акустичного та електромеханічного каналу – не менше 10 Вт. Вихідна середньоквадратична напруга акустичного та електромагнітного каналів при мінімальному опорі навантаження 4 Ом – не менше 5 В. Максимальна вихідна потужність п'єзоелектричного каналу – не менше 10 Вт. Вихідна середньоквадратична напруга п'єзоелектричного каналу при максимальній ємності навантаження 0,5 мкФ - не менше 20 В. Прилад забезпечує глибину регулювання окремо низько- та високочастотної складових шумового сигналу в робочому діапазоні частот не менше 20дБ.

На рис. 3.5 – 5.5 наведені приклади вібровипромінювачі.

Рис. 3.5 Вібровипромінювач "Копійка" - монтується на скло

Рис. 4.5 Вібровипромінювач"Молот" – випромінювач монтується на стіну

Рис. 5.5 Вібровипромінювач "Серп" – монтується на раму вікна

Контрольні запитання

1. Назвати основні засоби перехоплення мовної інформації.
2. Що використовується в якості критерію ефективності захисту акустичної інформації?
3. За рахунок чого добиваються зниження розбірливості мови?
4. Чим забезпечується реалізація пасивного методу захисту акустичної інформації?
5. Доповісти сутність активного методу захисту інформації по акустичні каналу.
6. Доповісти сутність пасивного методу захисту інформації по акустичні каналу.
7. Доповісти сутність віброакустичного захисту приміщень по акустичному каналу.

9. Визначення загороджувальної і прицільної перешкоди по частоті радіосигналу.

Лекція № 6

Тема: Засоби перехоплення побічних радіосигналів (ПЕМВ)

ПЛАН ЛЕКЦІЇ

1. Склад засобу перехоплення радіосигналів
2. Антени
3. Радіоприймачі
4. Технічні засоби аналізу сигналів

1. Склад засобу перехоплення радіосигналів

Перехоплення ел. магнітного, магнітного та електричних полів, а також електричних сигналів з інформацією здійснюють органи радіо- та радіотехнічної розвідки. При перехопленні вирішуються наступні основні задачі:

- пошук у просторі та по частоті сигналів з потрібною інформацією;
- виявлення сигналів які цікавлять органи розвідки;
- підсилення сигналів та отримання з них інформації;
- аналіз технічних характеристик сигналів які приймаються;
- виявлення місцезнаходження (координати) джерел сигналів;
- обробка отриманих даних з метою формування первинних ознак джерел випромінення або тексту перехопленого повідомлення.

Спрощена структура типового комплексу засобу перехоплення показано на (рис. 1.6):

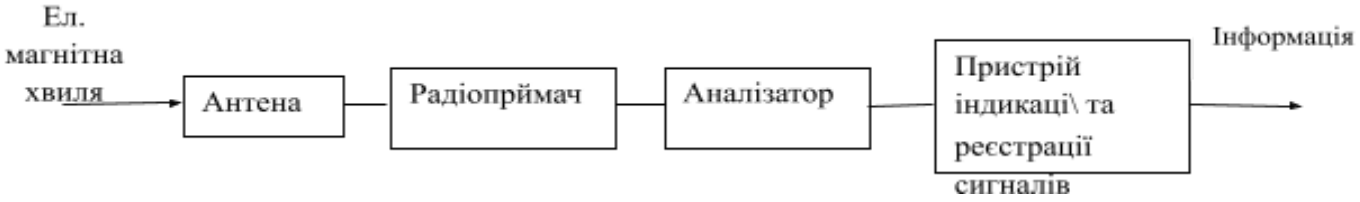


Рис. 1.6 Склад комплексу засобу перехоплення радіосигналів

Типовий комплекс складається з:

- приймальна антенна;
- радіоприймач;
- аналізатор технічних характеристик сигналів;
- реєструючий пристрій.

Антена призначена для просторової селекції та перетворення електромагнітної хвилі у електричні сигнали, амплітуда, частота і фаза яких відповідають аналогічним характеристикам електромагнітної хвилі.

Радіоприймач здійснює пошук та селекцію радіосигналів по частоті, підсилення та демодуляція отриманих сигналів, підсилення та обробка де модульованих сигналів: мовневих, цифрових даних, відеосигналів тощо.

Для аналізу радіосигналів після частотної селекції та підсилення, їх подають на входи вимірювальної апаратури аналізатора, яка визначає параметри сигналів: частотні ,часові, енергетичні, види модуляції, структуру кодів тощо.

Радіопеленгатор призначений для визначення направлення на джерело випромінення (пеленг) або його координат.

Реєструючий пристрій забезпечує запис сигналів для документування та подальшої обробки.

2. Антени

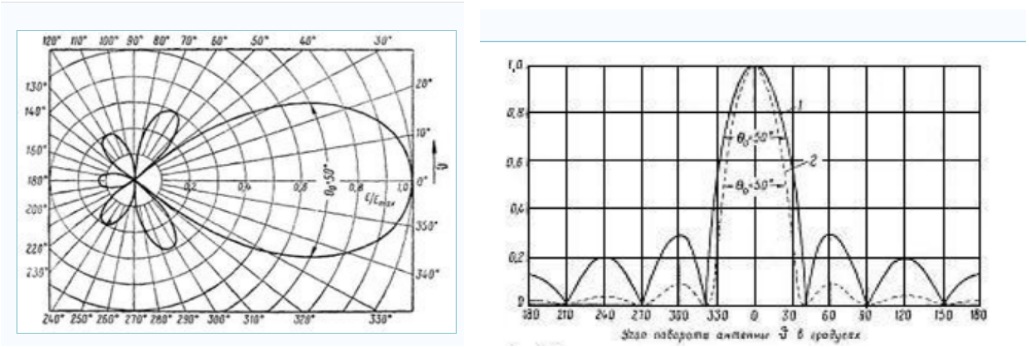
Антени являють собою електромеханічні конструкції з токопровідних елементів, розмір і конфігурація яких визначають ефективність перетворення електричних сигналів в радіосигнали (для передавальних антен) і радіосигналів в електричні (для приймальних антен).

Спроможності антен як приймальних так і передавальних визначаються наступними електричними характеристиками:

- діаграмою спрямованості та її шириною;
- коефіцієнтом корисної дії;
- коефіцієнтом підсилення;
- смугою робочих частот.

Діаграма спрямованості представляє собою графічне зображення рівня випромінюємого або приймаємого сигналу у горизонтальній та вертикальній плоскостях. Диаграми спрямованості (ДС) відображаються у прямокутній або полярнійсистемах координат (рис. 2.6).

ДС – это зависимость напруги на вхідних зажимах антени від напряму прихода электромагнітної хвилі εА = εА(θ, φ).



Полярна система координат Прямокутна система координат

Рис. 2.6 Діаграма спрямованості антени

Коефіцієнт підсилення приймальної антени - це число, яке показує, у скільки разів активна потужність на вході приймача при даній антені буде більше активної потужності на його вході в разі застосування неспрямована антени.

Коефіцієнтом корисної дії (передавальної антени) - відношення потужності радіовипромінювання, створюваного антеною, до потужності радіочастотного сигналу, що підводиться до антени.

Смуга робочих частот антени – діапазон частот у межах яких основні параметри антени майже не змінюються.

Загальна класифікація антен:

1. По функциональному призначенню:

− приймальні;

− передавальні;

− прийомо-передавальні.

2. По конструкції та принципу дії:

− лінійні;

− апертурні;

3. По полярізації (просторова орієнтація вектора електричної напруженості ел. магнітної хвилі):

− антени лінійної поляризації (вертикальна та горізонтальна);

− антени кругової полярізації.

4. По смузі пропускання:

− вузькополосні;

− широкополосні;

− широкодіапазонні.

5. По направленним властивостям:

− ненаправлені;

− вузьконаправлені.

6. За місцем встановлення:

− наземні (стаціонарні);

− бортові (мобільні).

Призначення передавальних та приймальних антен ясно з їх найменування. За своїми електричними параметрами вони не відрізняються. Багато з них в залежності від схеми підключення (до передавача або приймача) можуть використовуватися як передавальні або приймальні ,наприклад антени радіолокаційних станцій. Але якщо до передавальної антени підводиться велика

потужність, то в неї приймаються спеціальні заходи по запобіганню пробою між елементами антени які знаходяться під великою напругою.

Ефективність антени залежить від узгодження розмірів елементів антени з довжиною випромінюваних або отримуваних хвиль. Мінімальна довжина узгодженої з довжиною хвилі електромагнітного коливання штирової антени складає від λ\2 до λ\4, де:

λ (м) = 300/f [МГц] – довжина ел. магнітної хвилі.

Розмір та конструкція антен розрізняються як для різних діапазонів частот так і внутрі діапазонів.

Якщо для стаціонарних антен вимога до геометричних розмірів достатньо просто виконується для коротких та ультракоротких хвиль, то для антен які встановлюються на мобільні засоби вимоги до розмірів виконати складно. Наприклад раціональна довжина антени (λ\4) для забезпечення зв'язку на частоті 30 мГц складе 2,5 м, що незовсім зручно. Тому використовують укорочені антени, але при цьому зменшується їх ефективність. Скорочення довжини антени у 2 рази зменшує ефективність до 60%, у 5 разів – до 10%, а ефективність антени укороченої у 10 раз складає усього 3 % від раціонального варіанту.

По типу випромінюючих елементів антени бувають **лінійні, апертурні.**

У лінійних антен поперечні розміри малі у порівнянні з прокольними і з довжиною хвилі. Лінійні антени роблять з протяжних токопроводящих елементів (металеві стержні та дріт) ,увздовж яких розповсюджуються токи високої частоти. В залежності від величини навантаження лінії у ній виникають стоячі хвилі (лінія розімкнута) або хвилі що бігуть (опір навантаження дорівнює волновому опору лінії). По конструкції розрізняють симетричні і несиметричні електричні вібратори, біжучої хвилі, ромбічні і рамочні антени. У симетричному вібраторі провода лінії - вібратори розведені на 180^0 (рис. 3.6 а)

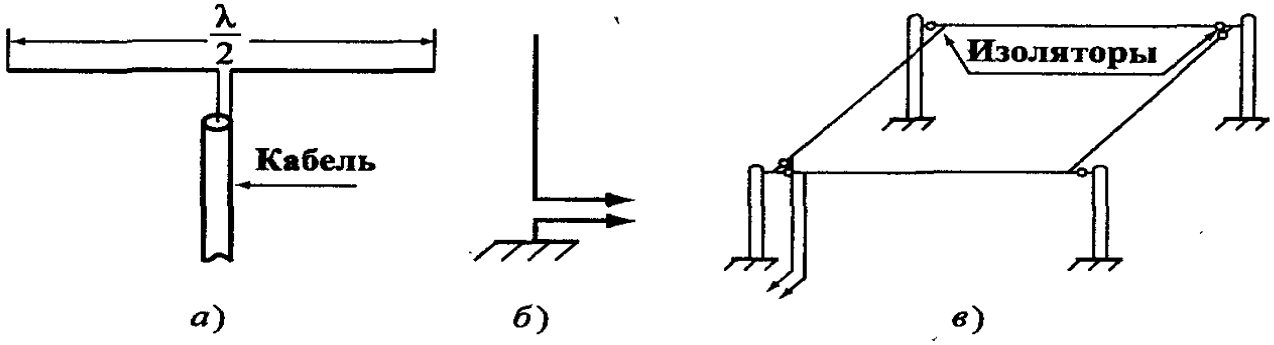


Рис. 3.6 Типи лінійних антен

Несиметричним вібратором називається одинокій лінійний провідник, розташований вертикально над токо провідною поверхнею (корпус земля) (рис. 3.6 б).

Ромбічна антена (рис. 3.6 в) має високу спрямованість випромінювання та представляє собою довгу двопроводну лінію, провода якої розходяться у входа ,а потім утворюючи ромб, зходяться замикаясь на активне навантаження, опір якого якого дорівнює хвильовому опору лінії.

Рамочну антену утворює один або декілька послідовно з'єднаних витков проводу квадратної, круглої або трьокутної форми розташованих зазвичай у вертикальній площині.. Лінійні антени використовуються у ДВ СВ КВ УКВ діапазонах хвиль.

Випромінюючим елементом *апертурних* антен є їх раскрив. По виду апертури розрізняють рупорні, лінзові, дзеркальні та щілинні антени. (рис. 4.6).

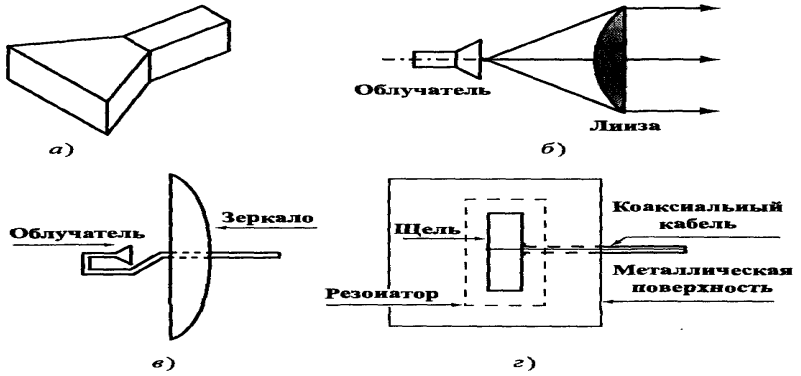


Рис. 4.6 Типи апертурних антен

Так для ефективного випромінювання, розміри апертури антени повинні бути спів розмірні з довжиною хвилі, то ці антени ефективні у діапазоні надвисоких частот.

Рупорна антена (рис. 4.6 а) являє собою закінчення хвилеводу з рупором прямокутної або круглої форми. По хвилєводу передається ел. магнітна енергія від генератора передавача, а рупор забезпечує плавний перехід від хвилеводу до вільного простору, що зменшує відбиття ел. магнітної хвилі від закінчення хвилеводу.

Основним елементом лінзових антен (рис. 4.6 б) є лінза, принцип роботи якої аналогічний оптичній лінзи.

У передавальній антені перетворює ел. магнітну хвилю яка розходиться від опромінювача (рупор, кінець хвилеводу, вібратор) електромагнітну хвилю у плоску хвилю. Прийомна антена фокусує на опромінювач ел. магнітну хвилю яка падає на раскрив лінзи. Лінзи поділяються на уповільнюючі, у яких фазова

швидкість розповсюдження ел. магнітної хвилі нижча за швидкість світла, пришвидчуючі. Уповільнюючі лінзи роблять з діелектрика, у який вкраплені струмопровідні елементи. Пришвидчуючі лінзи виготовляються з паралельних металевих пластин або секцій прямокутних хвилеводів. Найбільш широко використовуються багатопроменеві лінзи, що забезпечують широкий спектр частот випромінювання та прийому.

Лінзи, у яких електромагнітне поле формується у результаті відбиття електромагнітної хвилі, що випромінюється опромінювачем, від металевої поверхні рефлектора (дзеркала) називаються дзеркальними (рис. 4.6 в).

Форма лінзи у вигляді параболоїда, усіченого параболоїду, параболічного циліндру або циліндру спеціальної форми створює потрібну діаграму спрямованості антени. У діапазоні дециметрових і більш довгих хвиль у якості опромінювача застосовується вібратор, у діапазоні більш коротких хвиль – хвилєводно – рупорні опромінювані.

У лінзових антенах шляхом збільшення розмірів дзеркала можна забезпечити великий кутовий дозвіл. Вони широко застосовуються у сантиметровому та дециметровому діапазонах хвиль, найчастіше для забезпечення космічного звязку.

Щілинна антена (рис. 4.6 г) – металевий лист з щіллю, яка опромінюється ел. магнітним полем. В основному застосовується вузька прямокутна щілина шириною (0,03 – 0,05) λ і довжиною 0,5λ, але щіль може бути іншої форми, у вигляді кута ,хреста та ін. У щілині, що розташована перпендикулярно токам які наводяться у листі, збуджується електромагнітне поле. Для забезпечення односторонньої спрямованості поля що випромінюється, щілина з тильної сторони закривається резонатором у вигляді металевої коробки. Збуджуючий сигнал підводиться до країв щілини коаксіальним кабелем безпосередньо, або за допомогою зонду, що знаходиться усередині резонатору.

Для лінійних антен (наприклад вібраторів) коефіцієнт підсилення антени характеризується діючою висотою або довжиною $h = E_a/E$, де E_a – максимальне значення електродвіжуої сили що наводиться у антені, E – напруженість електромагнітного поля у точці прийому. Смуга частот, у межах якої зберігаються задані технічні характеристики антени називаються смугою її пропускання.

Для параболічної антени коефіцієнт підсилення антени розраховується за формулою:

$$K_n = 4\pi S/\lambda^2 ,$$

де:

S – ефектина площа дзеркала антени;

λ – довжина електромагнітної хвилі.

Створення антен з високим коефіцієнтом підсилення і широкою смугою пропускання є основною проблемою при конструювання антен. Чим вищий коефіцієнт підсилення, тим важче забезпечити широкосмуговість антени.

У залежності від **смуги пропускання**, антени діляться на вузькосмугові, широкосмугові, діапазонні та широкодіапазонні.

Вузькосмугові антени забезпечують прийом сигналів у діапазоні 10% від основної частоти. У широкосмугових антен ця величина дорівнює 10 – 50% ,у діапазонних антен коефіцієнт перекриття(відношення верхнього значення частои пропускання до антени до нижнього значення) складає 1,5 – 4, а у широкодіапазонних антен це відношення дорівнює 4 – 20 і більше.

Сукупність однотипних антен, розташованих за визначеним порядком у просторі, створює антенну решітку. Сигнал антенної решітки дорівнює сумі сигналів від окремих антен. Розрізняють лінійні (одномірні) та плоскі (двомірні) антенні решітки. Антенні решітки, у яких можна регулювати фази сигналів від окремих антен називають фазованим антенними решітками. Шляхом зміни фаз сигналів, що підсумовуються можна змінювати діаграму спрямованості у горизонтальній та вертикальній площинах і робити швидкій пошук сигналів у просторі та орієнтувати приймальну антену на джерело випромінення.

Діапазоном робочих частот (пропускною здатністю) антени називається інтервал частот від f min до f max, в межах якого всі параметри антени не виходять із заданих меж: $\Delta f = f max - f min$.

Діапазон робочих частот антени найчастіше виражають у відсотках до середньої частоті діапазону $\Delta f / fcp$. Якщо $\Delta f / fcp < 10\%$, то антена - вузбкосмугова; якщо $10\% < \Delta f / fcp < 50\%$, то антена - широкосмугова; якщо $\Delta f / fcp > 100\%$, то антена - широкодіапазонна.

Антена "*волновий канал*" *(*рис. 5.6).

Антена складається з розташованих на траверсі (на малюнку — Т) активного (А) і ряду пасивних вібраторів розташованих відносно напряму прийому — рефлектору (R), а також директорів (D), розташованих перед активним вібратором. Частіше за усе застосовується один рефлектор (є конструкції з безліччю рефлекторів), число директорів змінюється від одного до десятків. Довжина активного вібратора становить близько половини довжини хвилі, що приймається (0,5 λ), рефлектор чує більше 0,5 λ, а директорів чує менше 0,5 λ і з невеликим скороченням по напряму від активного вібратора. У трьохелементній антенні відстань від активного вібратора до рефлектора і до директора становлять близько 0,25 λ.

R - рефлектор;

A – активний вібратор;

D – директор.

Використовуються у діапазоні метрових та дециметрових хвиль.

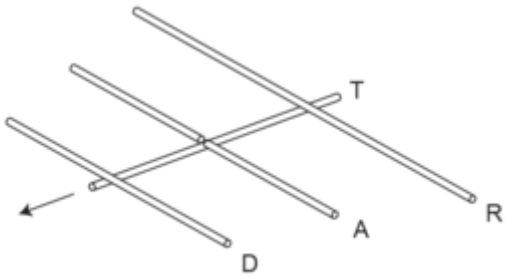


Рис. 5.6 Антена “волновий канал”

2. Радиоприймачі

Радіоприймач – основний технічний засіб перехоплення який здійснює пошук, селекцію, прийом та обробку радіосигналів. До його складу входять пристрої, що виконують:

- задають частоту приймача і селекцію (виділення) потрібного радіосигналу;
- підсилення виділеного сигналу;
- детектування (збір інформації);
- підсилення відео- або низькочастотного первинного сигналу.

Розрізняють два види радіоприймачів: **прямого підсилення** та **супергетеродинні**. Першими були приймачі прямого підсилення але вони поступилися супергетеродинним майже в усіх радіодіапазонах, за винятком дуже високих частот. Така тенденція пояснюється більшою селективністю та чутливістю супергетеродинного радіоприймача в порівнянні з приймачем прямого підсилення.

У **приймачах прямого підсилення (**рис. 6.6) сигнал на вході приймача (виході антени) селектується та підсилюється без зміни його частоти. Якість інформації, отриманої з цього сигналу, тим більше, чим менше рівень перешкод (сигналів різної природи з частотами, близькими до настройки приймача). В ідеалі ланцюжки селекції повинні забезпечувати П-подібну форму з полосою пропускання, рівною ширині спектра радіо тестеру сигналу.

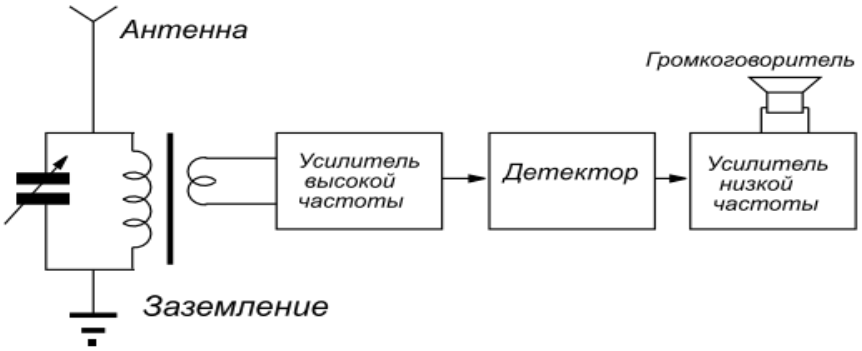


Рис. 6.6 Структурна схема приймача прямого підсилення

У **супергетеродинного приймача (**рис. 7.6) проблема одночасного забезпечення високих значень чутливості та селективності вирішується шляхом перетворення високоточного сигналу що приймається після його попередньої селекції та підсилення в підсилювачі високої частоти у сигнал постійної частоти, який називається проміжною частотою.

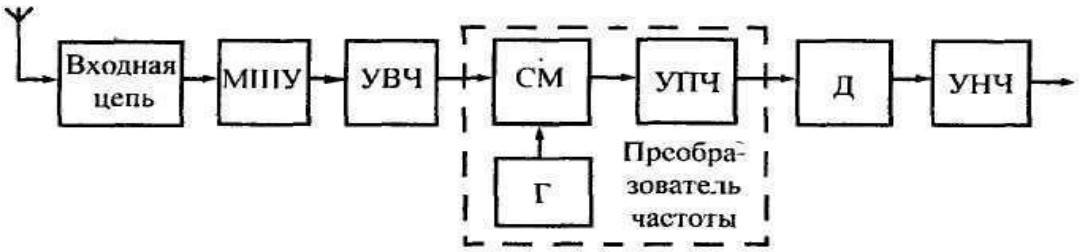


Рис. 7.6 Структурна схема супергетеродинного приймача

Після перетворення сигналу, його підсилення та селекція виконуються на проміжній частоті. Для постійної проміжної частоти завдання забезпечення високої вибірковості та чутливості вирішуються простіше й краще.

Властивості радіоприймача визначаються наступними технічними характеристиками:

- діапазоном приймаємих частот;
- чутливістю;
- вибірковістю;
- динамічним діапазоном;
- якістю відтворення прийнятого сигналу (рівнями нелінійних та фазових спотворень);

Діапазон приймаємих частот забезпечується шириною смуги пропускання селективних елементів вхідних фільтрів та інтервалів частот гетеродина. Налаштування приймача на потрібний діапазон або під діапазон частот виконується шляхом перемикання елементів вхідних контурів та контуру гетеродина, а налаштування на частоту всередині діапазону (адіотестеру) – шляхом зміни частоти гетеродина.

Чутливість радіоприймача оцінюється мінімальною потужністю або напругою сигналу на його вході, при якому рівень сигналу та відношення сигнал/шум на виході приймача забезпечують нормальну роботу кінцевих пристроїв (індикації та реєстрації). Така чутливість називається реальною.

У діапазоні дециметрових та коротших хвиль чутливість вимірюється у ватах або децибелах відносно рівня у 1 мВт, у спектральній щільності в Вт/Гц або децибелах (відносно Вт/Гц), на метрових та довших хвилях – у мікровольтах (мкВ). Реальна чутливість сучасних професійних супергетеродинних приймачів діапазонів дециметрових та сантиметрових хвиль становить 10^{-12} – 10^{-15}Вт або -180…-200 дБ відносно Вт/Гц, а приймачів метрових та довших хвиль – 0,1-10 мкВ.

Вибірковість приймача оцінюється параметрами амплітудно-частотної характеристики (АЧХ) його селективних ланцюгів, що визначає залежність коефіцієнта підсилення приймального тракту від частоти. Вибірковість приймача максимальна, коли його амплітудно-частотна характеристика повторює форму спектру прийнятого сигналу. У такому випадку будуть прийняті всі його спектральні складові, але не будуть пропущені спектральні складові інших сигналів (перешкод). Практично здійснити цю вимогу дуже складно, оскільки спектр сигналів з різною інформацією має нерівномірну й постійно змінюючуся форму, і існують великі технічні проблеми при формуванні амплітудно-частотної характеристики складної заданої форми.

Динамічний діапазон. Оскільки активні елементи підсилювальних каскадів радіоприймача (транзистори, діоди та ад.) мають достатньо вузький інтервал значень вхідних сигналів, при яких забезпечується їх лінійне перетворення, то при обробці сигналів з амплітудою поза цими інтервалами виникають їхні лінійні 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 співвідношенням у децибелах максимального рівня до мінімального рівня прийнятого сигналу.

Для підвищення динамічного діапазону в сучасних радіоприймачах застосовується пристрій автоматичного регулювання підсилення (АРП)

приймального тракту, який змінює його коефіцієнт підсилення відповідно до рівня адіо тестер сигналу. Неспіввідношення амплітудно-частотної і фазової характеристик, динамічного діапазону радіоприймача поточним характеристикам сигналу призводять до його **частотних, фазових та нелінійних спотворень** та втрати інформації.

Окрім перерахованих електричних характеристик можливості радіоприймачів оцінюються також по їх надійності, оперативності управління, типам електроживлення та споживаній потужності, масо габаритним показникам.

Традиційні аналогові радіоприймачі поступово витісняються цифровими, у яких сигнал перетворюється у цифровий вид з наступною його обробкою засобами обчислювальної техніки.

Великі можливості по перехопленню радіосигналів у широкому діапазоні частот надають скануючи приймачі.

Особливості цих радіоприймачів:

- швидка (перестройка частоти) настройки приймача у широкому діапазоні частот;
- наявність пристроїв пам’яті, які запам’ятовують частоти які вводить користувач, а також знайдені у процесі пошуку, частоти які становлять або не становлять інтерес для користувача;
- інформаційно-технічне спряження приймача з ПЕОМ для передачі сигналів у комп’ютер для обробки та управління приймачем.

Пам’ять адіо тесте приймача дозволяє запам’ятовувати частоти виявлених радіосигналів і не витрачати час на їх аналіз при наступному скануванні діапазону частот. В результаті цього сильно скорочується час для простоту широкого діапазону частот.

На основі скануючи приймачів та ПЕОМ створено автоматизовані комплекси радіоконтролю (радіомоніторингу) приміщень. Комплекс управляється ПЕОМ у реальному масштабі часу та забезпечує відображення на екрані монітору амплітудно-частотних характеристик сигналів, їх реєстрацію з можливістю наступної обробки. Пришвидшений огляд діапазону частот забезпечується за допомогою програмно-апаратних засобів швидкого панорамного огляду (на основі швидкого перетворення Фур’є.

Для перехоплення радіосигналів які мають складну структуру. Наприклад у мобільному зв’язку, створюються спеціальні прийомні комплекси.

4. Технічні засоби аналізу сигналів

Технічні засоби вимірювання ознак сигналу мають великий набор різних програмно-апаратних засобів та приладів як то: пристрої аналізу спектрів

сигналів, селективні вольтметри, вимірювачі часових параметрів дискретних сигналів, прилади визначення модуляції сигналів.

Портативні аналізатори спектра сигналів дозволяють приймати сигнали широкого діапазону частот (30 Гц – 40 гГц) і аналізувати їх структуру.

Селективний вольтметр - високочутливий вимірювальний супергетеродинний приймач, що працює в частотному діапазоні від одиниць МГц до 1000 МГц. Прилад призначений для аналізу високочастотних синусоїдних напруг і для квазіпікового вимірювання імпульсної напруги перешкод (рис. 8.6).

Рис. 8.6 Селективний вольтметр.

Радіочастотоміри призначені для вимірювання частоти джерела радіосигналу.

Програмно-апаратний комплекс DigiScan (рис. 9.6).

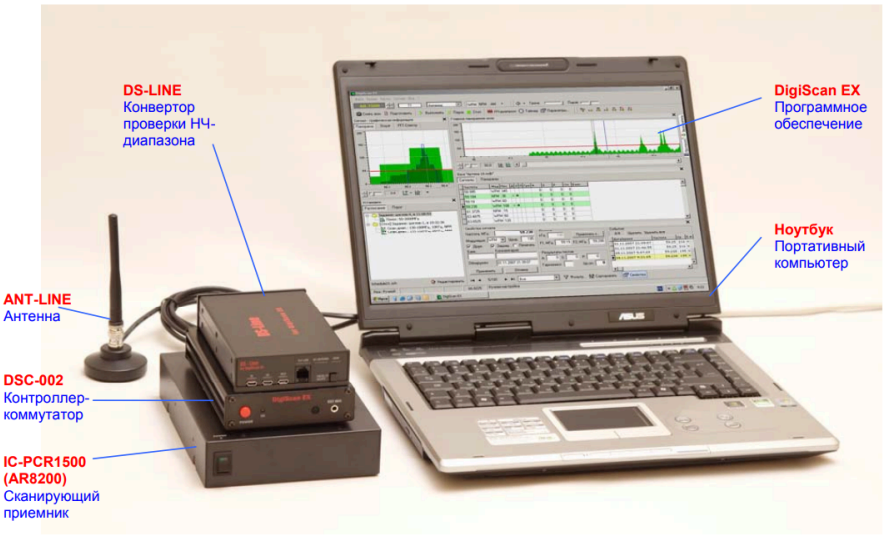


Рис. 9.6 Прилад DjScan

Він призначений для проведення оперативних заходів щодо виявлення та локалізації технічних засобів негласного отримання інформації, а також для виявлення та контролю природних та штучно створених каналів витоку інформації.

Прилад складається з основного блоку управління та індикації, комплекту перетворювачів та дозволяє працювати в наступних режимах:

- високочастотний детектор-частомір;
- скануючий аналізатор провідних ліній;
- детектор ІЧ-випромінювань;
- детектор низькочастотних магнітних полів;
- диференціальний низькочастотний підсилювач;
- віброакустичний приймач;
- акустичний приймач.

Контрольні запитання

1. Склад комплексу перехоплення радіосигналів.
2. Доповісти основні характеристики антенн
3. Доповісти загальну класисифікацію антен
4. Що називається діаграмою спрямованості антени
5. Доповісти про антену типу фазована антенна решітка.
6. Доповісти классификацію антен по типу випромінюючих елементів.
7. Охарактеризувати лінійні антени
8. Охарактеризувати апертурні антени
9. Яка різниця між широкодіапазонною антеною та вузькосмуговою
10. Що називається смугою пропускання антени

11. Доповісти основні технічні характеристики радіоприймача.
12. Доповісти типи існуючих радіоприймачів. Охарактеризувати їх
13. Охарактеризувати приймач прямого підсилення
14. Охарактеризувати супергетеродинний приймач

Лекція № 7

Тема: Загрози інформації в автоматизованих системах

ПЛАН ЛЕКЦІЇ

1. Класифікація загроз інформації в автоматизованих системах
2. Види і природа каналів витоку інформації при експлуатації автоматизованих систем
3. Методи забезпечення захисту інформації від витоку через побічні електромагнітні випромінювання (ПЕМВ)
4. Оцінка рівня ПЕМВ

1. Класифікація загроз інформації в автоматизованих системах

Модель загроз інформації - це опис методів і засобів здійснення загроз для інформації в конкретних умовах функціонування автоматизованої інформаційної системи і можливого збитку від реалізації погрози.

Формування моделі загроз інформації є одним з головних чинників забезпечення її безпеки, оскільки безпосередньо пов'язане з вибором необхідного переліку послуг безпеки, заходів і засобів захисту, що реалізуються в автоматизованій системі (АС). Довершеність і повнота аналізу загроз дає необхідну впевненість, що враховані всі суттєві загрози безпеки інформації.

Конструктивним шляхом створення моделі загроз є формування окремих моделей загроз для кожної компоненти системи зокрема, для АС - центральний вузол АС (наприклад, центральний сервер при клієнт-серверній архітектурі тощо; окремі досить незалежні підсистеми АС; канали зв'язку і комутаційний центр окремих підсистем; вузол зв'язку з Internet і ін.) і типових об'єктів захисту (робочих станцій, серверів, мережевого обладнання ЛВС тощо). Формування окремих моделей загроз повинно здійснюватися на підставі загальної класифікації загроз інформації.

Протягом життєвого циклу кожної АС модель загроз необхідно переглядати в зв'язку з модернізацією і розвитком АС, а також періодично, в зв'язку з удосконаленням технічних і програмних засобів подолання механізмів захисту.

Згідно з нормативними документами ТЗІ (НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99) за результатами впливу на інформацію і систему її обробки загрози поділяються на чотири класи:

- порушення конфіденційності інформації (отримання інформації користувачами або процесами всупереч встановленим правилам доступу);

• порушення цілісності інформації (повне або часткове знищення, викривлення, модифікація, нав'язування неправдивої інформації);

• порушення доступності інформації (втрата часткова або повна працездатності системи, блокування доступу до інформації);

• втрата спостереженості або керованості системи обробки (порушення процедур ідентифікації та аутентифікації користувачів і процесів, надання їм повноважень, здійснення контролю за їх діяльністю, відмова від отримання або пересилання повідомлень).

Для забезпечення конфіденційності, цілісності та доступності інформації, а також керованості системою (спостереженість) необхідно захищати інформацію не тільки від витоку технічними каналами та несанкціонованого доступу, а й виключати можливість негативного впливу на інформацію, втручання в процес її обробки, порушення працездатності системи. Таким чином, захищати необхідно всі компоненти АС: апаратуру та обладнання, програми, дані, персонал.

Процес прояви можливих загроз інформації (далі - загроз) і впливу їх на інформацію грунтується на системній класифікації (рис. 1.7):

Рис. 1.7 Загальна класифікація загроз інформації в АС

Об'єктивні загрози є стихійними природними явищами та об'єктивними фізичними процесами.

Суб'єктивні загрози є наслідком діяльності людини, технічних засобів і систем;

• за можливістю виникнення загрози поділяються на випадкові і навмисні. Випадкові загрози викликаються помилками проектування автоматизованої системи та системи захисту інформації, помилками в програмному забезпеченні, збоями та відмовами апаратури і систем забезпечення, помилками персоналу тощо. Навмисні загрози зумовлені цілеспрямованими діями людей (порушників);

• за місцем розміщення джерела загроз щодо автоматизованої системи навмисні загрози поділяються дистанційні та контактні. До дистанційним відносяться загрози, джерело яких знаходиться за межами контрольованої території. Контактні загрози здійснюються в межах контрольованої зони, як правило, при проникненні в приміщення, де розташовані засоби обробки і зберігання інформації.

Перелік можливих загроз інформації, яка обробляється в автоматизованій системі та циркулює в зв'язку з цим у відповідних приміщеннях, наводиться в

таблиці 1. У графі "Наслідки" наведені основні властивості інформації і відповідної автоматизованої системи, порушення яких можливо при реалізації загроз.

2. Види і природа шляхів витоку інформації при експлуатації АС

З точки зору захисту інформації ці технічні пристрої є прекрасним прикладом для вивчення практично всіх каналів витоку інформації - починаючи від радіоканалу і закінчуючи матеріально-речовим. Розглянемо детальніше принципи утворення каналів витоку інформації при експлуатації персональної електронно-обчислювальної машини (ПЕОМ).

Як відомо, сучасні ПЕОМ можуть працювати як незалежно один від одного, так і взаємодіючи з іншими ЕОМ по комп'ютерних мережах, причому останні можуть бути не тільки локальними, а й глобальними.

З урахуванням цього фактора, повний перелік тих ділянок, в яких можуть знаходитися підлягають захисту дані, може мати наступний вигляд:

• безпосередньо в оперативній або постійної пам'яті ПЕОМ;

• на знімних магнітних, магнітооптичних, лазерних та інших носіях;

• на зовнішніх пристроях зберігання інформації колективного доступу (RAID-масиви, файлові сервери і т.п.);

• на екранах пристроїв відображення (дисплеї, монітори, консолі);

• в пам'яті пристроїв введення / виведення (принтери, графічні, сканери);

• в пам'яті керуючих пристроїв і лініях зв'язку, що утворюють канали сполучення комп'ютерних мереж.

Природні канали витоку інформації утворюються як при роботі ЕОМ, так і в режимі очікування.

Джерелами таких каналів є:

електромагнітні поля (*радіоканал витоку інформації*) – ПЕМВ (побічні ел. магнітні випромінення ПЕОМ);

наведення струмів і напруг у проводних системах (живлення, заземлення та з'єднувальних) *(електричний канал витоку*).

Крім того, класифікацію можливих каналів витоку інформації у першому наближенні можна провести на підставі принципів, відповідно до яких обробляється інформація, що отримується з можливого каналу витоку. Передбачаються три типи обробки: людиною, апаратурою, програмою. Відповідно до кожного типу обробки всілякі канали витоку також розбиваються на три групи. Стосовно до ПЕОМ групу каналів, в яких основним видом обробки є **обробка людиною**, складають наступні можливі канали витоку:

- розкрадання матеріальних носіїв інформації (магнітних дисків, стрічок, карт);

- читання інформації з екрану сторонньою особою;
- читання інформації з залишених без нагляду паперових роздруківок.

У групі каналів, в яких основним видом обробки є обробка апаратурою, можна виділити наступні можливі канали витоку:

- підключення до ПЕОМ спеціально розроблених апаратних засобів, що забезпечують доступ до інформації;
- використання спеціальних технічних засобів для перехоплення електромагнітних випромінювань технічних засобів ПЕОМ.

У групі каналів, в яких основним видом обробки є програмна обробка, можна виділити наступні можливі канали витоку:

• несанкціонований доступ програми до інформації;
• розшифровка програмою зашифрованої інформації;
• копіювання програмою інформації з носіїв;
• блокування або відключення програмних засобів захисту.

При перехопленні інформації з ПЕОМ через ПЕМВ використовується схема, представлена на рис.2.7.

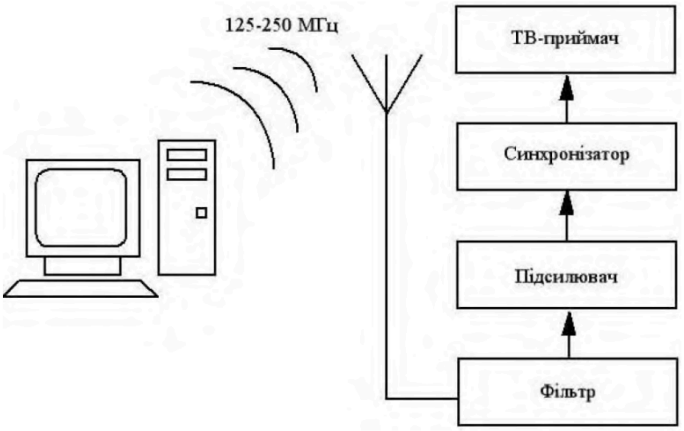


Рис. 2.7 Схема перехоплення інформації з ПЕОМ через ПЕМВ

При цьому технічному контролю повинні піддаватися наступні потенційні канали витоку інформації:

побічні електромагнітні випромінювання в діапазоні частот від 1 МГц до 1000 МГц;

наведення сигналів в ланцюгах електроживлення, заземлення і в лініях зв'язку;

щляхи витоку інформації, що утворюються в результаті впливу високочастотних електромагнітних полів на різні дроти, які знаходяться в приміщенні і можуть, таким чином, стати прийомною антеною. В цьому випадку перевірка проводиться в діапазоні частот від 1 МГц до 1000 МГц

Найбільш небезпечним каналом витоку є дисплей, так як з точки зору захисту інформації він є найслабшою ланкою в системі. Це обумовлено принципами роботи відеоадаптера, що складається зі спеціалізованих схем для генерування електричних сигналів управління обладнанням, яке забезпечує генерацію зображення.

Розглянемо докладніше можливості витоку інформації, що обробляється на ПЕОМ, через побічні електромагнітні випромінювання (ПЕМВ).

При проведенні аналізу можливості витоку інформації необхідно враховувати такі особливості радіоканалу витоку з вузлів цифрової електронної техніки.

Не всі ПЕМВ є небезпечними з точки зору реальної витоку інформації. Як правило, найбільший рівень відповідає неінформативним випромінюванням (в ПЕОМ найбільший рівень мають випромінювання, породжувані системою синхронізації).

Наявність великої кількості паралельно працюючих електричних ланцюгів призводить до того, що інформативні та неінформативні випромінювання можуть перекриватися за діапазоном (взаємна перешкода).

3. Методи забезпечення захисту інформації від витоку через ПЕМВ

Основними напрямками захисту інформації від витоку технічними каналами є:

- запобігання витоку оброблюваної інформації за рахунок побічних електромагнітних випромінювань і наведень, створюваних функціонуючими технічними засобами, а також за рахунок електроакустичних перетворень;
- виявлення впроваджених на об'єкти і в технічні засоби електронних пристроїв перехоплення інформації (закладних пристроїв).

Захист інформації, що обробляється технічними засобами, здійснюється із застосуванням пасивних і активних методів і засобів.

Пасивні методи захисту інформації спрямовані на:

- ослаблення побічних електромагнітних випромінювань (інформаційних сигналів) основних технічних засобів і систем (ОТЗС) на межі контрольованої зони до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів;
- ослаблення наведень побічних електромагнітних випромінювань (інформаційних сигналів) ОТЗС в сторонніх провідниках і сполучних лініях допоміжних технічних засобів і систем (ДТЗС), що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів;

- виключення (ослаблення) просочування інформаційних сигналів ОТЗС у кола електроживлення, що виходять за межі контрольованої зони, до величин, що забезпечують неможливість їхнього виділення засобом розвідки на фоні природних шумів.

Активні методи захисту інформації спрямовані на:

- створення маскувальних просторових електромагнітних завад з метою зменшення відносини сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗС;

- створення маскувальних електромагнітних перешкод в проводах і сполучних лініях ДТЗС з метою зменшення відносини сигнал/шум на межі контрольованої зони до величин, що забезпечують неможливість виділення засобом розвідки інформаційного сигналу ОТЗС.

Класифікація способів і методів захисту інформації, що обробляється засобами цифрової електронної техніки, від витоку через ПЕМВ приведена на (рис. 3.7).

Електромагнітне екранування приміщень в широкому діапазоні частот є складним технічним завданням, вимагає значних капітальних витрат, постійного контролю і не завжди можливо по естетичним і ергономічним міркуванням. Доопрацювання засобів електронної техніки з метою зменшення рівня ПЕМВ здійснюється організаціями, що мають відповідні ліцензії. Використовуючи різні радіопоглинаючі матеріали і схемо технічні рішення, за рахунок доопрацювання вдається істотно знизити рівень випромінювань. Вартість такого доопрацювання залежить від радіуса необхідної зони безпеки і становить від 20% до 70% від вартості ПЕОМ.

Шифрування здійснюється або програмно, або апаратно за допомогою вбудованих засобів. Такий спосіб захисту виправдовується при передачі інформації на великі відстані по лініях зв'язку.

Активне радіотехнічне маскування передбачає формування і випромінювання маскуючого сигналу у безпосередній близькості від об’єкту, що захищається. Розрізняють декілька методів активного радіотехнічного маскування: енергетичні методи; метод "синфазної перешкоди"; статистичний метод.

Рис. 3.7 Засоби та методи захисту інформації, що обробля’ється засобами електронної техніки від витоку через ПЕМВ

При **енергетичному маскуванні методом "білого шуму"** випромінюється широкосмуговий шумовий сигнал з постійним енергетичним спектром, рівень якого істотно перевищує максимальний рівень випромінювання електронної техніки. На даний час дуже поширений. До його недоліків слід віднести створення неприпустимих перешкод радіотехнічним і електронним засобам, що знаходяться поблизу від захищаємої апаратури.

Спектрально-енергетичний метод полягає в генеруванні перешкоди, що має енергетичний спектр, який визначається модулем спектральної щільності інформативних випромінювань техніки. Даний метод дозволяє визначити оптимальну перешкоду з обмеженою потужністю для досягнення необхідного співвідношення сигнал/перешкода на кордоні контрольованої зони.

Перераховані методи можуть бути використані для захисту інформації як в аналоговій, так і в цифровій апаратурі. Як показник захищеності в цих методах використовується співвідношення сигнал/перешкода. Наступні два методи призначені для захисту інформації у техніці, що працює з цифровими сигналами.

У методі "синфазної перешкоди" в якості маскуючого сигналу використовуються імпульси випадкової амплітуди, що збігаються за формою і часу існування з корисним сигналом. В цьому випадку перешкода майже повністю маскує сигнал, прийом сигналу втрачає сенс, тому що апостеріорні ймовірності наявності і відсутності сигналу залишаються рівними їх апріорним значенням. Показником захищеності в даному методі є гранична повна ймовірність помилки (ГПВП) на кордоні мінімально допустимої зони безпеки. Однак через відсутність апаратури для безпосереднього вимірювання цієї величини пропонується перерахувати ГПВП в необхідне співвідношення сигнал / перешкода.

Статистичний метод захисту інформації полягає в зміні ймовірнісної структури сигналу, що приймається розвідприймачем шляхом випромінювання спеціальним чином сформованого маскуючого сигналу.

До переваг даного методу варто віднести те, що рівень маскуючого сигналу не перевищує рівня інформативних ПЕМВ техніки.

Механізм виникнення ПЕМВ засобів цифрового електронного техніки.

Побічні електромагнітні випромінювання, які генеруються електромагнітними пристроями, обумовлені протіканням диференціальних і синфазних струмів.

У напівпровідникових пристроях електромагнітне поле утворюється при синхронному протікання диференційних струмів в контурах двох типів. Один тип контуру формується провідниками плати або шинами, по яких напівпровідникові прилади підключені до джерела живлення. Інший тип контура утворюється при передачі логічних сигналів від одного пристрою до іншого з використанням у якості зворотнього проводу шини живлення. Провідники передачі даних спільно з шинами живлення формують динамічно працюючі контури, що з'єднують передавальні та прийомні пристрої.

Випромінювання, викликане синфазними струмами, обумовлено виникненням падінь напруги в пристрої, що створює синфазну напругу відносно землі. Як правило, в цифровому електронному обладнанні здійснюється синхронна робота логічних пристроїв. В результаті при перемиканні кожного логічного пристрою відбувається концентрація енергії в імпульсні складові, що збігаються за часом. При їх накладенні між собою, сумарні рівні випромінювання можуть виявитися вище, ніж може створити будь-який з окремих пристроїв.

У багатьох випадках основними джерелами випромінювань виявляються кабелі, по яких передається інформація в цифровому вигляді. Такі кабелі можуть розміщуватися всередині пристрою або з'єднувати їх між собою.

Застосування у якості заземлення обплетення кабелю або проводу, які характеризуються великими індуктивністю і активним опором для ВЧ перешкод, призводить до того, що кабель починає діяти як передавальна антена.

Технічна реалізація пристроїв активного радіотехнічного маскування

Для здійснення активного радіотехнічного маскування ПЕМВ використовуються пристрої, що створюють шумове електромагнітне поле у діапазоні частот від декількох кГц до 1000 МГц із спектральним рівнем, що істотно перевищує рівні природних шумів та інформаційних випромінювань ОТЗС. Для цих цілей використовуються малогабаритні надширокосмугові передавачі шумових маскуютчих коливань типу наприклад ГШ-1000 і ГШ-К-1000, які є модернізацією виробу "Шатер-4" (рис. 4.7).

Рис. 4.7 Генератор електромагнітного шуму

Сформований генератором шумовий сигнал за допомогою антени випромінюється в простір.

Спектральна щільність випромінюваного електромагнітного поля рівномірно розподілена по частотному діапазону і забезпечує необхідну перевищення маскуючого сигналу над інформативним в задану кількість разів (як вимагають нормативні документи) на кордонах контрольованої зони об'єктів.

4. Оцінка рівня ПЕМВ

Оцінка рівня ПЕМВ засобів цифрової електронної техніки може проводитися з точки зору відповідності цих рівнів наступним нормам і вимогам:

- санітарно-гігієнічні норми (ГОСТ 12.1.006-84);
- норми електромагнітної сумісності (ЕМС);
- норми і вимоги по захисту інформації від витоку через ПЕМВ.

Залежно від того, відповідність яким нормам потрібно встановити, використовуються ті чи інші прилади, методи та методики проведення вимірювань.

Слід зауважити, що норми на рівні ЕМВ з точки зору ЕМС істотно (на кілька порядків) суворіше санітарно-гігієнічних норм. Очевидно, що норми, методики та прилади, які використовуються в системі забезпечення безпеки життєдіяльності, не можуть бути використані при вирішенні задач захисту інформації.

Рівні ПЕМВ цифрового електронного техніки з точки зору ЕМС регламентовані цілим рядом міжнародних та вітчизняних стандартів (публікації CISPR - спеціального міжнародного комітету щодо радіоперешкод, ГОСТ 29216-91) встановлює такі норми напруженості поля радіозавад від устаткування інформаційної техніки (табл. 1.7).

Таблиця 1.7 Норми напруженості поля радіозавад

Смуга частот, МГц	Квазіпикові норми, ДБ (мВ/м)
30–230	30 (31,6)
230–1000	37 (70,8)

Рівні напруженості поля випромінюваних перешкод нормуються на відстані 10 або 30 м від джерела перешкод в залежності від того, де буде експлуатуватися обладнання (в житлових приміщеннях або в умовах промислових підприємств).

Наведені допустимі рівні випромінювання достатні для перехоплення ЕМВ на значній відстані. Крім того, в діапазоні частот 0,15 -30 МГц нормуються тільки рівні напруги перешкод на мережевому устаткуванні і не нормується напруженість поля радіозавад. Дані норми при серійному випуску виконуються з якоюсь ймовірністю. Таким чином, відповідність ПЕМВ засобів цифрової електронної техніки нормам на ЕМС не може бути гарантією збереження конфіденційності інформації, що обробляється за допомогою цих засобів.

Характеристика використовуваної вимірювальної апаратури:

діапазон робочих частот - 9 МГц - 1000 МГц;

можливість зміни смуги пропускання;

наявність детекторів квазіпікового, пікового, середнього і середньоквадратичного значень;

можливість слухового контролю сигналу, що має амплітудну і частотну модуляцію;

наявність виходу проміжної частоти і виходу на осцилограф;

наявність комплекту стандартних калібрувальних антен.

Сучасні вимірювальні приймачі (ЕЛМАС, ESH-3, ESVP, SMV-41) автоматизовані і оснащені відповідними інтерфейсами, що представляє можливість управляти режимами роботи приймача за допомогою зовнішньої ЕОМ, а передавати виміряні значення на зовнішню ЕОМ для їх обробки.

Крім того для вимірювання побічних ЕМІ засобів цифрового електронного техніки можуть бути використані аналізатори спектра в комплекті з вимірювальними антенами.

В процесі обробки можуть виконуватися такі функції: пошук екстремальних значень сигналу; відбір сигналів, рівень яких перевищує заданий зсув по осі частот для оптимальної реєстрації сигналу. Вбудований мікропроцесор забезпечує обробку амплітудно-частотних спектрів, а також оптимізацію часу вимірювання і роздільної здатності для розглянутого інтервалу частот.

На відміну від завдань ЕМС, де потрібно визначити максимальний рівень випромінювання в заданому діапазоні частот, при вирішенні задач захисту інформації потрібно визначити рівень випромінювання в широкому діапазоні частот, відповідному інформативному сигналу. Тому оцінка рівня випромінювань при вирішенні задач захисту інформації повинна починатися з аналізу технічної документації та відбору електричних ланцюгів, за якими можна передавати інформацію з обмеженим доступом. Необхідно провести аналіз і визначити характеристики небезпечних сигналів:

використовуваний код: послідовний, паралельний;

періодичне повторення сигналу: є, немає;

часові характеристики сигналу.

спектральні характеристики сигналу.

Після цього можна приступати безпосередньо до визначення рівнів інформативних ПЕМВ. Тут використовуються такі методи: метод оціночних розрахунків, метод примусової (штучної) активізації; метод еквівалентного приймача.

Метод оціночних розрахунків

Визначаються елементи конструкції обладнання, в яких циркулюють небезпечні сигнали, складаються моделі, проводиться оцінний розрахунок рівня випромінювань. Цей метод добре реалізується при наявності програмного забезпечення для ПЕОМ у вигляді експертної системи, що містить банк моделей випромінювачів.

Метод примусової активізації (використовується на практиці).

Активізується (програмно або апаратно) канал (один небезпечний ланцюг) еталонним сигналом, який дозволяє ідентифікувати випромінювання, і вимірюються рівні виникаючих ПЕМВ. Для вимірювань за даним методом можуть бути використані вимірювальні приймачі та аналізатори спектра.

Метод еквівалентного приймача

Синтезується приймач для відновлення інформації, що міститься в ПЕМВ. Після калібрування такий приймач може бути використаний для вимірювання рівнів інформаційних випромінювань.

Кожен з методів має свої достоїнства і недоліками. В даний час найбільш прийнятним для практики методом оцінки рівнів інформативних ПЕМВ являється метод примусової активізації.

Контрольні запитання

1. На які типи, за результатами впливу на інформацію і систему її обробки, підрозділяються загрози.

2. Доповісти загальну класифікацію загроз інформації.

3. Що є джерелами утворення природних каналів витоку інформації які утворюються при роботі ПЕОМ.

4. Доповісти сутність пасивних методи захисту інформації

5. Доповісти сутність активних методи захисту інформації

6. Доповісти сутність активного радіотехнічного маскування і його різновиди

7. Доповісти сутність енергетичного маскування методом "білого шуму"

8. Які методи використовуються для визначення рівнів інформативних побічних електромагнітних випромінювань

9. Доповісти сутність методу примусової активізації при визначенні рівнів інформативних побічних електромагнітних випромінювань

Лекція № 8

Тема лекції: Електричний канал витоку інформації

ПЛАН ЛЕКЦІЇ

1. Причини виникнення електричних каналів витоку інформації.
2. Паразитні зв’зки та наведення.
3. Просторове та лінійне зашумлення.
4. Фільтрація інформаційних сигналів у електричних колах об’єкту інформаційної діяльності.

1. Причини виникнення електричних каналів витоку інформації

Причини виникнення електричного каналу витоку інформації на ОІД наступні:

- гальванічні зв'язку з'єднувальних ліній ОТЗ з лініями ДТЗ (допоміжні технічні засоби) і сторонніми провідниками;
- наведення побічних електричних випромінювань ОТЗ на з'єднувальні лінії ДТЗ і сторонні провідники;

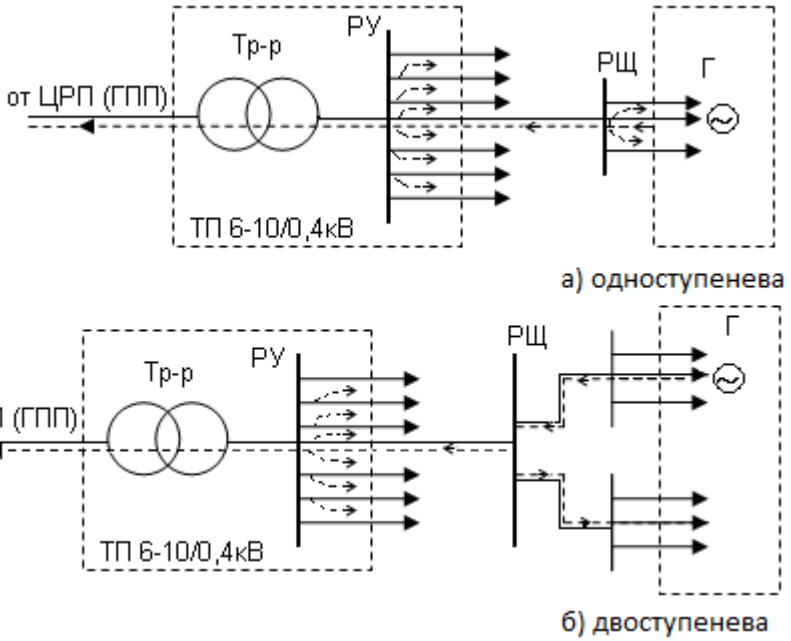
- наведення побічних електричних випромінювань ОТЗ на ланцюзі електроживлення і заземлення ОТЗ;
- «Просочування» інформаційних сигналів у кола електроживлення і заземлення ОТЗ.

Одним з видів технічних каналів витоку інформації, що виникають при роботі засобів і систем інформатизації (електронно-обчислювальна, телевізійна й інша техніка), є канали, що з'являються за рахунок побічних електромагнітних випромінювань і наведень. До найбільш поширених шляхів витоку інформації внаслідок наведень відносяться щляхи, які утворюються в мережі електроживлення технічних засобів і систем.

Аналіз схем електропостачання технічних засобів і систем (ТЗС) інформатизації, встановлених на різних об'єктах підприємств і організацій, показує, що електроживлення цих ТЗС здійснюється від трансформаторних підстанцій ТП 6-10 / 0,4 кВ, як правило, по радіальної схемою (радіальна схема - такий спосіб розподілу енергії, при якому кожен окремий споживач або зосереджена група споживачів харчується по окремої лінії від того чи іншого комутаційного вузла).

Радіальна схема є одноступеневою в разі, якщо споживачі отримують електроенергію від ТП 6-10 / 0,4 кВ безпосередньо через силовий розподільчий щит РЩ (складання); двоступеневої, якщо вони забезпечуються електроенергією

від одного проміжного розподільного пункту (ПРП 1); триступеневої, якщо їх електропостачання здійснюється через два проміжних розподільних пункту (ПРП 1 і ПРП2). На підстанцію ТП 6-10 / 0,4 кВ електроенергія подається від центрального розподільного пункту (ЦРП) або головної знижувальної підстанції (ДПП). Одноступінчата і двоступенева схеми електропостачання технічних засобів обробки інформації на ОІД наведені на (рис. 1.8.)



ї діяльності;
ку електроживлення)

Рис. 1.8 Схема утворення електричного каналу витоку інформації на ОІД

Контрольована зона різних підприємств і організацій, на об'єктах яких розміщуються ТЗС (технічні засоби системи) інформатизації, може охоплювати більшу або меншу частину їх ланцюгів електропостачання.

Зустрічаються варіанти електропостачання ТЗС інформатизації, коли і підстанції ТП 6-10 / 0,4 кВ розміщуються за межами контрольованої території. При використанні всіх розглянутих схем електропостачання від підстанцій ТП 6-10 / 0,4 кВ або від наступних за ними розподільних пристроїв часто може здійснюватися живлення будь-яких сторонніх по відношенню до ТЗС інформатизації споживачів електроенергії, розташованих за кордоном контрольованої зони.

Інформативні сигнали потрапляючи в кабелі живлення і потім, поширюючись по ним і далі по різним елементам мереж електропостачання, включеним після (по ходу руху сигналів) цих кабелів, можуть бути в зручному для зловмисника місці за межами контрольованої зони перехоплені за допомогою

спеціальних технічних засобів і систем, а за прийнятими таким чином сигналам може бути відновлена інформація. Структуру будь-якого технічного каналу витоку інформації, в тому числі і каналу витоку за рахунок наведень в мережу електроживлення ТЗС інформатизації, можна представити у вигляді системи передачі інформації. Одним з елементів цієї структурної схеми є тракт розповсюдження інформативних сигналів, що представляє собою середовище, в якій вони переміщаються. У нашому випадку зазначені ділянки мереж електропостачання ТЗС інформатизації, що виходять за межі контрольованої зони, і є такими трактами.

Можливі тракти поширення інформативних сигналів у мережах електропостачання ТЗС інформатизації показані на рис. 1 пунктирними лініями (ТЗС, які є їхніми джерелами, позначені у вигляді еквівалентних генераторів).

Очевидно, що всі тракти, крім тих, які включають в себе трифазний силовий трансформатор підстанції ТП 6-10 / 0,4 кВ, можна ліквідувати за рахунок усунення споживачів електроенергії, які постачаються від даної підстанції та знаходяться за межами контрольованої зони.

Нижчк приведено рекомендації щодо захисту інформації, що обробляється технічними засобами і системами інформатизації, від витоку за рахунок наведень в мережу їх електроживлення.

Основними принципами, на яких будується використання найбільш поширених заходів захисту інформації від витоку за рахунок наведень в мережу електроживлення ТЗС інформатизації, є:

- фізичне усунення окремих трактів поширення інформативних сигналів.
- маскування інформативного сигналу спеціально створюваним шумовим сигналом.

Заходи захисту, засновані на першому принципі, вже були згадані на початку статті (мова йде про ліквідацію споживачів електроенергії знаходяться за кордоном контрольованої зони, які постачають від тієї ж трансформаторної підстанції ТП 6-10 / 0,4 кВ, від якої отримують енергію захищаються ТЗС інформатизації , і т.п.).

Рекомендації, для реалізації заходів захисту, в основу яких покладено третій принцип.

1. При проведенні робіт із захисту інформації від витоку за рахунок наведень в мережі електроживлення ТЗС інформатизації необхідно мати на увазі наступне.

З розширенням діапазону частот інформативних сигналів, наведених в мережі електроживлення ТЗС інформатизації, в сторону високих частот можливості з перехоплення цих сигналів в цілому знижуються через збільшення

загасання трактів їх поширення. Виняток становлять смуги частот, в яких мають місце значні провали частотних характеристик загасання таких трактів, що мають в загальному випадку хвилеподібний характер. Зазначені закономірності частково коректуються зменшенням рівнів шумових сигналів, на тлі яких здійснюється перехоплення, зі збільшенням частоти.

Збільшення ослаблення інформативних сигналів, джерелом яких є ТЗС інформатизації, наведених в мережі їх електроживлення, може досягатися збільшенням власних згасань окремих елементів таких трактів і неузгодженістю хвильових опорів цих елементів в діапазонах частот наведених інформативних сигналів (при збереженні їх узгодження на частоті 50 Гц).

2. З метою збільшення ослаблення рівнів інформативних сигналів в мережах електроживлення ТЗС інформатизації застосовувати розділові трансформатори, завадоподавляющі фільтри, джерела безперебійного живлення. При цьому в обов'язковому порядку враховувати, що практично кожне із зазначених технічних засобів ефективно з точки зору придушення наведених інформативних сигналів лише в певних смугах частот, часто не збігаються з діапазонами частот таких сигналів.

3. Для електропостачання ТЗС інформатизації краще використовувати ланцюги електропостачання, елементами яких є силові трифазні трансформатори якомога меншої потужності. Застосовувати розділові трансформатори також мінімально можливої потужності.

4. Вибирати (в разі наявності альтернативних варіантів) в якості ланцюгів електроживлення ТЗС інформатизації ланцюга, що мають на ділянці «ТЗС інформатизації - межа контрольованої зони» максимально можливе число елементів (силових кабелів, трансформаторних підстанцій і т. П.). Використовувати в складі цих ланцюгів силові кабелі, що мають максимально можливу довжину в межах контрольованої зони.

2. Паразитні зв'язки та наведення

Елементи, ланцюги, тракти, з'єднувальні дроти і лінії зв'язку будь-яких електронних систем і схем постійно знаходяться під впливом власних (внутрішніх) і сторонніх (зовнішніх) електромагнітних полів різного походження, які індукують чи навідних в них значні напруги. Такий вплив називають електромагнітним впливом або просто впливом на елементи ланцюга. Оскільки такий вплив утворюється непередбачуваними зв'язками, в подібних випадках говорять про паразитні (шкідливі) зв'язки і наведення, які призводять до утворення електричних каналів витоку інформації.

Основними видами паразитних зв'язків у схемах радіоелектронного обладнання (РЕО) є ємнісні та індуктивні зв'язки через джерело живлення і заземлення РЕО.

Наведення (струми і напруги) в струмопровідних елементах обумовлені електромагнітним випромінюванням технічних засобів обробки інформації (ТЗОІ) (в тому числі, і їх сполучними лініями), а також ємнісними і індуктивними зв'язками між ними. Сполучні лінії ДТЗС (допоміжні технічні засоби системи) або сторонні провідники є як би випадковими антенами, при гальванічному підключенні до яких засобів розвідки, наведення інформаційних сигналів може бути перехопленно. Випадкові антени можуть бути зосередженими і розподіленими. Зосереджена випадкова антена являє собою компактне технічне засіб (наприклад, телефонний апарат, гучномовець радіотрансляційної мережі, датчик пожежної сигналізації і т.д.), підключений до лінії, що виходить за межі контрольованої зони. До розподіленим випадковх антен відносяться випадкові антени з розподіленими параметрами: кабелі, дроти, металеві труби та інші струмопровідні комунікації, що виходять за межі контрольованої зони. Рівень сигналів що наводяться в них в значній мірі залежить не тільки від потужності випромінюваних сигналів, але і відстані від ліній ТЗОІ до ліній ДТЗС або сторонніх провідників, а також довжини їх спільного пробігу.

«Просочування» інформаційних сигналів у колі електроживлення можливо при наявності внутрішніх паразитних ємнісних і (або) індуктивних зв'язків випрямного пристрою блоку живлення ТЗОІ. Наприклад, в підсилювачі низької частоти струми підсилюються сигналів замикаються через джерело електроживлення, створюючи на його внутрішньому опорі падіння напруги, яке при недостатньому загасання в фільтрі випрямного пристрою може бути виявлено в лінії електроживлення при наявності магнітного зв'язку між вихідним трансформатором підсилювача і трансформатором випрямного пристрою.

«Просочування» інформаційних сигналів у колі заземлення.

Крім заземлюючих провідників, службовців для безпосереднього з'єднання ТЗОІ з контуром заземлення, гальванічний зв'язок з землею можуть мати різні провідники, що виходять за межі контрольованої зони. До них відносяться нульовий провід мережі електроживлення, екрани (металеві оболонки) сполучних кабелів, металеві труби систем опалення та водопостачання, металева арматура залізобетонних конструкцій і т.д. Всі ці провідники спільно з заземлювальним пристроєм утворюють розгалужену систему заземлення, на яку можуть наводитися інформаційні сигнали.

Перехоплення інформаційних сигналів в лініях електроживлення і колах заземлення ТЗОІ можливий при гальванічному підключенні до них засобу розвідки через ПЕМВН.

Таким чином, перехоплення інформації, що обробляється технічними засобами, може здійснюватися шляхом:

- перехоплення побічних електромагнітних випромінювань, що виникають при роботі технічних засобів;
- перехоплення наведень інформаційних сигналів зі сполучних ліній ДТЗС і сторонніх провідників;

Паразитні ємнісні зв'язки.

Паразитні ємнісні зв'язку обумовлені електричної ємністю, що утворюється між елементами, деталями і провідниками схем, які несуть потенціал сигналу. Так як опір ємності, що створює паразитне ємнісний зв'язок, падає з ростом частоти, що проходить через неї енергія з підвищенням частоти збільшується. Чим більше посилення сигналу між ланцюгами і каскадами, що мають ємнісний зв'язок, тим менше ємності потрібно для його самозбудження.

Паразитні індуктивні зв'язки

Паразитні індуктивні зв'язку обумовлені наявністю взаємоіндукції між провідниками і деталями РЕО, головним чином між її трансформаторами та катушками індуктивності. При зменшенні розмірів трансформаторів паразитний індуктивний зв'язок послаблюється.

Витік інформації по ланцюгах заземлення

Термін «земля» позначає систему провідних поверхонь і електричних з'єднань призначених для виконання наступних функцій. По-перше, заземлення корпусів захищають від ураження обслуговуючого персоналу електричним струмом. По-друге, система заземлення - це провідні поверхні, потенціал яких вважається нульовим і приймається за початок відліку напруг різних сигналів. По-третє, зазначені поверхні і провідники призначені для протікання зворотних струмів в ланцюгах сигналів і електроживлення. Нарешті, заземлення екранують елементів сприяє ослабленню небажаних зв'язків і таким чином включає функції складової частини системи екранування.

При правильному проектуванні система заземлення виконує всі перераховані функції сприяє поліпшенню умов електромагнітної сумісності радіоелектронних засобів. У той же час помилки, допущені при проектуванні заземлений, можуть створювати умови для витоку секретної інформації за межі контрольованої зони.

Одна з основних причин утворення каналів витоку інформації лініями заземлення пов'язана з тим, що перераховані типи заземлення рідко вдається виконати відокремленими. Поєднання декількох функцій однієї системою провідників і провідних поверхонь призводить до того, що по ним протікають різні струми, в тому числі і небезпечні.

Витік інформації по ланцюгах електроживлення

У мережі електроживлення технічних засобів і систем, в яких циркулює секретна інформація, можлива поява небезпечних сигналів як у випадках, коли частота оброблюваних сигналів вище частоти струму по мережі електроживлення, так і тоді коли небезпечні сигнали мають низькочастотні спектральні складові.

Низькочастотний канал утворюється за рахунок нерівномірності споживання струму мережі електроживлення і призводить до зміни амплітуди і тривалості імпульсів струму заряду ємності фільтра випрямного блоку джерела живлення. Цими імпульсами може передаватися тільки інформація, частота зміни якої нижче частоти електроживлення. Це можуть бути, наприклад, сигнали низькочастотних друкуючих пристроїв, що огинає мовного сигналу і т.д.

Високочастотні небезпечні сигнали можуть проникати в мережу електроживлення через паразитні ємнісні зв'язку, наявні між первинною і вторинною обмотками мережевого трансформатора, або наводиться на дроти мережі елементами і вузлами ОТЗС, що мають недостатній ступінь екранування ПЕМВ (рис. 2.8).

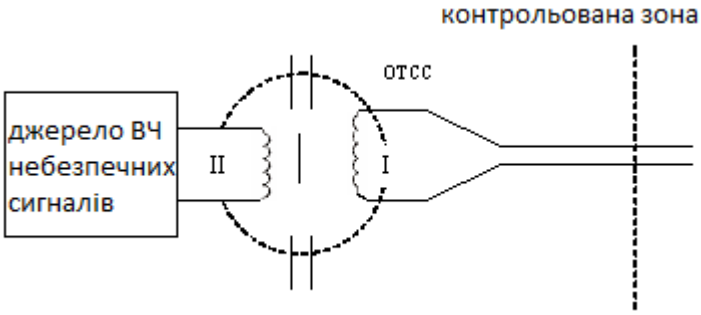


Рис. 2.8 Високочастотні небезпечні сигнали

3. Просторове та лінійне зашумлення

Реалізація пасивних методів захисту, заснованих на застосуванні екранування та фільтрації, призводить до ослаблення рівнів побічних електромагнітних випромінювань та наведень (небезпечних сигналів) ТЗОІ та тим самим до зменшення відносини небезпечний сигнал/шум (с/ш). Однак у ряді випадків, незважаючи на застосування пасивних методів захисту, на межі контрольованої зони відношення с/ш перевищує допустиме значення. У цьому випадку застосовуються активні заходи захисту, що ґрунтуються на створенні перешкод засобам розвідки, що також призводить до зменшення відношення с/ш.

Для виключення перехоплення побічних електромагнітних випромінювань використовується **просторове зашумлення**, а для виключення знімання наведень

інформаційних сигналів з сторонніх провідників і з'єднувальних ліній допоміжних технічних засобів - **лінійне зашумлення.**

До системи просторового зашумлення, що застосовується для створення електромагнітних перешкод, що маскують, пред'являються такі вимоги:

- система має створювати електромагнітні перешкоди у діапазоні частот можливих побічних електромагнітних випромінювань ТЗОІ;

- перешкоди, що створюються, не повинні мати регулярної структури;

- рівень створюваних перешкод (як електричної, так і магнітної складової поля) повинен забезпечити відношення с/ш на межі контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТЗОІ;

- система повинна створювати перешкоди як із горизонтальною, так і з вертикальною поляризацією (тому вибору антен для генераторів перешкод приділяється особлива увага);

- на межі контрольованої зони рівень перешкод, створюваних системою просторового зашумлення, не повинен перевищувати необхідних норм ЕМС.

Мета просторового зашумлення вважається досягнутою, якщо відношення небезпечний сигнал/шум на межі контрольованої зони не перевищує деякого допустимого значення, що вказаного у нормативних докумкетах.

У системах просторового зашумлення переважно використовуються перешкоди типу "білого шуму" або "синфазні перешкоди".

В даний час в основному застосовуються системи просторового шуму, що використовують перешкоди типу "білий шум", тобто випромінюють широкосмуговий шумовий сигнал (як правило, з рівномірно розподіленим енергетичним спектром у всьому робочому діапазоні частот), що істотно перевищує рівні побічних електромагнітних випромінювань. Такі системи використовуються для захисту широкого класу технічних засобів: електронно-обчислювальної техніки, систем звукопідсилення та звукового супроводу, систем внутрішнього телебачення тощо.

Генератори шуму виконуються або у вигляді окремого блоку з живленням від мережі 220 В ("Гном", "Хвиля", "ГШ-1000" та ін.), або у вигляді окремої плати, що вставляється (вбудовується) у вільний слот системного блоку ПЕОМ та живленням від загальної шини комп'ютера ("ГШ-К-1000", "Смог" та ін). Діапазон робочих частот генераторів шуму від 0,01...0,1 до 1000 МГц. При потужності випромінювання близько 20 Вт забезпечується спектральна густина перешкоди 40...80 дБ (рис. 3.8).

У системах просторового зашумлення в основному використовуються слабонаправлені рамкові жорсткі та гнучкі антени. Рамкові гнучкі антени виконуються із звичайного дроту і розгортаються у двох-трьох площинах, що

забезпечує формування перешкодового сигналу як з вертикальною, так і горизонтальною поляризацією у всіх площинах.

При використанні систем просторового зашумлення необхідно пам'ятати, що поряд з перешкодами засобам розвідки створюються перешкоди та іншим радіоелектронним засобам (наприклад, телебачення, радіосвізі і т.д.). Тому при введенні в експлуатацію системи просторового зашумлення необхідно проводити спеціальні дослідження щодо вимог забезпечення електромагнітної сумісності (ЕМС). Крім того, рівні перешкод, які створює система зашумлення, повинні відповідати санітарно-гігієнічним нормам. Однак норми на рівні електромагнітних випромінювань за вимогами ЕМС істотно суворіші за санітарно-гігієнічні норми. Отже, основну увагу необхідно приділяти виконання норм ЕМС. Просторове зашумлення ефективне як закриття електромагнітного, а й електричного каналів витоку інформації, оскільки перешкодовий сигнал при випромінюванні наводиться у сполучних лініях ДТЗ і сторонніх провідниках, які виходять межі контрольованої зони.

Системи лінійного зашумлення застосовуються для маскування наведених небезпечних сигналів у сторонніх провідниках та сполучних лініях ДТЗ, що виходять за межі контрольованої зони.

У найпростішому випадку система лінійного зашумлення являє собою генератор шумового сигналу, що формує шумову напругу, що маскує, з заданими спектральними, тимчасовими і енергетичними характеристиками, який гальванічно підключається в зашумлювану лінію (сторонній провідник). На практиці найчастіше подібні системи використовуються для зашумлення ліній електроживлення (наприклад, ліній електроживлення освітлювальної та розеткової мереж).

Рис. 3.8 Генератор електромагнітного шуму ГШ 1000

4. Фільтрація інформаційних сигналів у електричних колах об’єкту інформаційної діяльності

Фільтрація інформаційних сигналів – відноситься до пасивних засобів захисту інформації від витоку електричним каналом.

Одним із методів локалізації небезпечних сигналів, що циркулюють у технічних засобах та системах обробки інформації, є фільтрація інформаційних сигналів.

У джерелах електромагнітних полів та наведень фільтрація здійснюється з метою запобігання розповсюдженню небажаних електромагнітних коливань за межі пристрою – джерела небезпечного сигналу.

Для фільтрації сигналів в ланцюгах живлення ТЗОІ використовуються розділові трансформатори і електричні фільтри.

Розділові трансформатори. Такі трансформатори повинні забезпечувати розв'язку первинного та вторинного ланцюгів за сигналами наведення. Це означає, що у вторинний ланцюг трансформатора не повинні проникати наведення, що з'являються в ланцюзі первинної обмотки. Проникнення наведень у вторинну обмотку пояснюється наявністю небажаних резистивних та ємнісних ланцюгів зв'язку між обмотками.

Для зменшення зв'язку обмоток по сигналах наведень часто застосовується внутрішній екран, який виконується у вигляді заземленої прокладки або фольги, що укладається між первинною та вторинною обмотками. За допомогою цього екрана наведення, що діє у первинній обмотці, замикається на землю. Однак електростатичне поле навколо екрана також може спричинити проникнення наведень у вторинний ланцюг.

Розділові трансформатори використовуються для вирішення ряду завдань, у тому числі для:

- поділу по ланцюгах живлення джерел та рецепторів наведення, якщо вони підключаються до тих самих шин змінного струму;
- усунення асиметричних наведень;
- ослаблення симетричних наведень у ланцюзі вторинної обмотки, зумовлених наявністю асиметричних наведень у ланцюзі первинної обмотки.

Засоби розв'язки та екранування, що застосовуються в розділових трансформаторах, забезпечують максимальне значення опору між обмотками та створюють для наведення шлях з малим опором з первинної обмотки на землю.

Зазначені особливості трансформаторів для ланцюгів живлення забезпечують більш високий рівень придушення наведень, ніж звичайні трансформатори.

Електричні фільтри. В даний час існує велика кількість різних типів фільтрів, що забезпечують ослаблення небажаних сигналів у різних ділянках частотного діапазону. Це фільтри нижніх і верхніх частот, смугові та фільтри, що загороджують. Основне призначення фільтрів - пропускати без значного

ослаблення сигнали з частотами, що у робочої смузі частот, і придушувати (послаблювати) сигнали з частотами, що лежать поза цієї смуги. Для виключення просочування інформаційних сигналів у ланцюзі електроживлення використовуються фільтри нижніх частот. Фільтр нижніх частот (ФНЧ) пропускає сигнали з частотами нижче граничної частоти (f < fгр) і пригнічує з частотами вище граничної частоти. Послідовна гілка ФНЧ повинна мати малий опір постійного струму і нижніх частот. Разом з тим, щоб вищі частоти затримувалися фільтром, послідовний опір має зростати з частотою. Цим вимогам задовольняє індуктивність L

Паралельна гілка ФНЧ, навпаки, повинна мати малу провідність для низьких частот для того, щоб струми цих частот не шунтувалися паралельним плечем. Для високих частот паралельна гілка повинна мати велику провідність, тоді коливання цих частот нею шунтуватимуться, і їх струм на виході фільтра послаблюватиметься. Таким вимогам відповідає ємність.

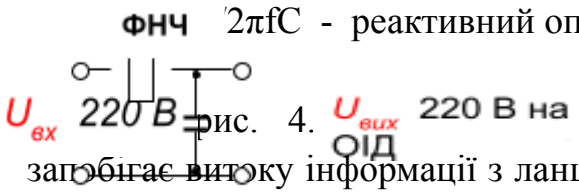


Рис. 4. р мережевий перешкододавляючий ФП-6 запобігає витоку інформації з ланцюгів електроживлення, а також захищає засоби оргтехніки від зовнішніх перешкод. ФП 6 послаблює будь-які сигнали в діапазоні 0,1 - 1,8 ГГц з ефективністю 60 дБ і відповідно не пропускають інформативні сигнали, що виникають при роботі засобів оргтехніки.

Рис. 4.8 Зовнішній вигляд фільтру низьких частот для живлення ОІД

На рис. 4.9 приведено амплітудно-частотну характеристику ФНЧ яка пояснює сутність його функціонування.

ис. 4.9 Амплітудно-частотна та фазо-частотна характеристики ФНЧ

Більш складні багатоланкові ФНЧ (Чебишева, Баттерворта, Бесселя тощо) конструюють з урахуванням поєднань різних одиничних ланок. Основні вимоги до захисних фільтрів полягають у наступному:

- величини робочої напруги та струму фільтра повинні відповідати напрузі та струму фільтрованого ланцюга;

- величина ослаблення небажаних сигналів у діапазоні робочих частот має бути не меншою за необхідну;

- ослаблення корисного сигналу у смузі прозорості фільтра має бути незначним;

- габарити та маса фільтрів повинні бути мінімальними;

- фільтри повинні забезпечувати функціонування за певних умов експлуатації (температура, вологість, тиск) та механічних навантажень (удари, вібрація тощо);

- конструкції фільтрів повинні відповідати вимогам техніки безпеки.

До фільтрів ланцюгів живлення поряд із загальними висуваються такі додаткові вимоги:

- загасання, що вноситься такими фільтрами в ланцюги постійного струму або змінного струму основної частоти, має бути мінімальним (наприклад, 0,2 дБ і менше) і мати велике значення (більше 60 дБ) у смузі придушення, яка в залежності від конкретних умов може бути досить широкій (до 10 ГГц);

- мережеві фільтри повинні ефективно працювати при сильних струмах, що виходять, високих напругах і високих рівнях потужності проходять і затримуваних електромагнітних коливань;

Наприклад, фільтри серії ФСПК-100 (200), що використовуються на практиці, призначені для встановлення в чотирипровідних лініях електроживлення частотою 50 Гц і напругою 220/380 В. Максимальний робочий струм становить 100 (200) А. В - діапазоні частот від 0,02 до 1000 МГц фільтри забезпечують загасання сигналу щонайменше 60 дБ.

Контрольні запитання

1. Назввати причини виникнення електричних каналів витоку інформації.

2. За рахунок чого утворюються канали витоку інформації обумовлені наведеннями в мережу електроживлення ОТЗ інформатизації?

3. Перерахувати основні принципи на яких будується використання найбільш поширених заходів захисту інформації від витоку за рахунок наведень в мережу електроживлення

4. Які заходи захисту рекомендуються використовувати для ослаблення інформативного сигналу в тракті розповсюдження даного вірусу.

6. Чим обумовлені наведення (струми і напруги) в струмопровідних елементах?

7. Визначення зосередженої і розподіленої випадкової антени.

8. Назвати способи перехоплення інформації, що обробляється технічними засобами

9. Пояснити пристрій, принцип дії розподільчого тр-ра. Для вирішення яких завдань використовується?

10. Для чого застосовуються завадодавні фільтри? Основні вимоги до них

Лекція № 9

Тема лекції: Екранування технічних засобів для захисту інформації в автоматизованих системах від витоку побічними електромагнітними випромінюваннями (ПЕМВ)

ПЛАН ЛЕКЦІЇ

1. Типи екранувань
2. Заземлення технічних засобів.

1. Типи екранувань

Функціонування будь-якого технічного засобу інформації пов'язане з протіканням по його струмопровідним елементам електричних струмів різних частот і утворенням різниці потенціалів між різними точками його електричної схеми, які породжують магнітні та електричні поля, звані побічними електромагнітними випромінюваннями.

Побічні електромагнітні випромінювання ТЗОІ (технічний засіб перетворення інформації) є причиною виникнення електромагнітних та параметричних каналів витоку інформації, а також можуть стати причиною виникнення наведення інформаційних сигналів у сторонніх струмопровідних лініях та конструкціях. Тому зниженню рівня побічних електромагнітних випромінювань приділяється велика увага.

Ефективним методом зниження рівня ПЕМВ є екранування їх джерел.

Розрізняють такі способи екранування:

- електростатичний;
- магнітостатичне;
- електромагнітне.

Електростатичне та магнітостатичне екранування засновані на замиканні екраном (що володіє в першому випадку високою електропровідністю, а в другому - магнітопровідністю) відповідно електричного та магнітного полів.

Електростатичне екранування по суті зводиться до замикання електростатичного поля на поверхню металевого екрану та відведення електричних зарядів на землю (на корпус приладу). Заземлення електростатичного екрану є необхідним елементом для реалізації електростатичного екранування. Застосування металевих екранів дозволяє повністю усунути вплив електростатичного поля.

Основним завданням екранування електричних полів є зниження ємності зв'язку між елементами конструкції, що екрануються. Отже, ефективність екранування визначається переважно відношенням ємностей зв'язку між

джерелом і рецептором наведення до і після установки заземленого екрана. Тому будь-які дії, що призводять до зниження ємності зв'язку, збільшують ефективність екранування.

Екрануюча дія металевого листа істотно залежить від якості з'єднання екрана з корпусом приладу та частин екрану один з одним. Особливо важливо не мати з'єднувальних дротів між частинами екрану та корпусом.

У діапазонах метрових і більш коротких довжин хвиль з'єднувальні провідники завдовжки кілька сантиметрів можуть різко погіршити ефективність екранування. На ще більш коротких хвилях дециметрового та сантиметрового діапазонів сполучні провідники та шини між екранами неприпустимі.

Вузькі щілини та отвори в металевому екрані, розміри яких малі в порівнянні з довжиною хвилі, практично не погіршують екранування електричного поля. Зі збільшенням частоти ефективність екранування знижується. Основні вимоги до електричних екранів можна сформулювати таким чином:

- конструкція екрана повинна вибиратися такою, щоб силові лінії електричного поля замикалися на стінки екрана, не виходячи за межі;

- в області низьких частот (при глибині проникнення (σ) більше товщини (d), тобто при σ>d) ефективність електростатичного екранування практично визначається якістю електричного контакту металевого екрана з корпусом пристрою і мало залежить від матеріалу екрану та його товщини;

- в області високих частот (при d<σ) ефективність екрану, що працює в електромагнітному режимі, визначається його товщиною, провідністю та магнітною проникністю.

Магнітостатичне екранування використовується за необхідності придушити наведення на низьких частотах від 0 до 3...10 кГц.

Основні вимоги до магнітостатичних екранів можна звести до наступних:

- магнітна проникність μ матеріалу екрана має бути можливо вищою. Для виготовлення екранів бажано застосовувати магнітом'які матеріали з високою магнітною проникністю (наприклад, пермалою);

- збільшення товщини стінок екрану призводить до підвищення ефективності екранування, проте при цьому слід брати до уваги можливі конструктивні обмеження за масою та габаритами екрану;

- стики, розрізи та шви в екрані повинні розміщуватись паралельно лініям магнітної індукції магнітного поля. Їх кількість має бути мінімальною;

- Заземлення екрану не впливає на ефективність магнітостатичного екранування.

Ефективність магнітостатичного екранування підвищується під час застосування багатошарових екранів.

Екранування високочастотного магнітного поля засноване на використанні магнітної індукції, що створює в екрані змінні вихрові індукційні струми (струми Фуко). Магнітне поле цих струмів усередині екрану буде спрямоване назустріч збуджувальному полю, а за його межами - в той же бік, що й збуджуюче поле. Результуюче поле виявляється ослабленим усередині екрану та посиленим поза ним. Вихрові струми в екрані розподіляються нерівномірно за його перерізом (товщиною). Це викликається явищем поверхневого ефекту, сутність якого полягає в тому, що змінне магнітне поле слабшає принаймні проникнення в глиб металу, так як внутрішні шари екрануються вихровими струмами, що циркулюють у поверхневих шарах.

Завдяки поверхневому ефекту щільність вихрових струмів та напруженість змінного магнітного поля у міру заглиблення в метал падає по експонентному закону.

Ефективність магнітного екранування залежить від частоти та електричних властивостей матеріалу екрану. Чим нижче частота, тим слабше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту. Для високих частот, починаючи з діапазону середніх хвиль, екран з будь-якого металу завтовшки 0,5...1,5 мм діє дуже ефективно. При виборі товщини та матеріалу екрану слід враховувати механічну міцність, жорсткість, стійкість проти корозії, зручність стикування окремих деталей та здійснення між ними перехідних контактів з малим опором, зручність паяння, зварювання та ін.

Для частот вище 10 МГц мідна і тим більше срібна плівка завтовшки більше 0,1 мм дає значний ефект, що екранує. Тому на частотах вище 10 МГц цілком допустимо застосування екранів із фольгованого гетинаксу або іншого ізоляційного матеріалу з нанесеним на нього мідним або срібним покриттям.

При екрануванні магнітного поля заземлення екрана не змінює величини струмів, що збуджуються в екрані, і, отже, на ефективність магнітного екранування не впливає.

На високих частотах використовується виключно **електромагнітне** екранування. Дія електромагнітного екрана заснована на тому, що високочастотне електромагнітне поле послаблюється ним же створеним (завдяки вихровим струмам, що утворюється в товщі екрана) полем зворотного напрямку.

Теорія та практика показують, що з точки зору вартості матеріалу та простоти виготовлення переваги на стороні екранованого приміщення з листової сталі. Однак при застосуванні сітківки можуть значно спроститися питання вентиляції та освітлення приміщення. У зв'язку з цим сітчасті екрани знаходять широке застосування.

Металеві листи або полотнища сітки повинні бути електрично з'єднані по всьому периметру. Для суцільних екранів це може бути здійснено

електрозварюванням або паянням. Шов електрозварювання або паяння повинен бути безперервним для того, щоб отримати цільнозварну конструкцію екрана.

Для сітчастих екранів придатна будь-яка конструкція шва, що забезпечує хороший електричний контакт між сусідніми полотнищами сітки не рідше ніж через 10...15 мм Для цієї мети може застосовуватися паяння або точкове зварювання.

Також екрануванню підлягають і монтажні дроти та сполучні лінії. Щоб зменшити рівень ПЕМВ, необхідно ретельно виконувати з'єднання оболонки дроту (екрана) з корпусом апаратури. Підключення оболонки повинно здійснюватися шляхом безпосереднього контакту (найкраще шляхом паяння чи зварювання) із корпусом.

На низьких частотах доводиться використовувати складніші схеми екранування - коаксіальні кабелі з подвійним оплеткою (тріаксіальні кабелі).

На вищих частотах, коли товщина екрана значно перевищує глибину проникнення поля, потреба у подвійному екрануванні відпадає. У цьому випадку зовнішня поверхня відіграє роль електричного екрану, а по внутрішній поверхні протікають зворотні струми. Довжина екранованого монтажного дроту повинна бути менше чверті довжини найкоротшої хвилі спектра сигналу, що передається по дроту. При використанні більш довгих ділянок екранованих проводів необхідно мати на увазі, що в цьому випадку екранований провід слід розглядати як довгу лінію, яка, щоб уникнути спотворень форми сигналу, що передається повинна бути навантажена на опір, рівне хвильовому

Екрануватися можуть не лише окремі блоки (вузли) апаратури та їх з'єднувальні лінії, а й приміщення загалом.

У звичайних (неекранованих) приміщеннях основний екрануючий ефект забезпечують залізобетонні стіни будинків. Екрануючі властивості дверей та вікон гірші. Для підвищення екрануючих властивостей стін застосовуються додаткові засоби, у тому числі:

- струмопровідні лакофарбові покриття або струмопровідні шпалери;
- штори із металізованої тканини;
- металізоване скло (наприклад, з двоокису олова), що встановлюється в металеві або металізовані рами.

У приміщенні екрануються стіни, двері та вікна. При зачиненні дверей повинен забезпечуватись надійний електричний контакт зі стінками приміщення (з дверною рамою) по всьому периметру не рідше ніж через 10...15 мм. Для цього може бути використана пружинна гребінка з фосфористої бронзи, яку зміцнюють по всьому внутрішньому периметру дверної рами. Вікна повинні бути затягнуті одним або двома шарами мідної сітки з коміркою не більше 2х2 мм, причому відстань між шарами сітки має бути не менше ніж 50 мм. Обидва шари сітки

повинні мати хороший електричний контакт зі стінками приміщення (з рамою) по всьому периметру. Сітки зручніше робити знімними та металеве обрамлення знімної частини також повинно мати пружні контакти у вигляді гребінки з фосфористої бронзи. Розміри екранованого приміщення вибирають виходячи з його призначення та вартості. Зазвичай екрановані приміщення будують площею 6...8 м2 при висоті 2,5...3 м

2. Заземлення технічних засобів

Необхідно пам'ятати, що екранування ТЗОІ та з'єднувальних ліній ефективне лише при правильному їх заземленні. Тому однією з найважливіших умов захисту ТЗОІ є правильне заземлення цих пристроїв.

Нині існують різні типи заземлень. Найчастіше використовуються одноточкові, багатоточкові та комбіновані (гібридні) схеми.

Одноточкова послідовна схема заземлення найпростіша (рис. 1.9). Однак їй притаманний недолік, пов'язаний з протіканням зворотних струмів різних ланцюгів по спільній ділянці ланцюга, що заземлює. Внаслідок цього можлива поява небезпечного сигналу в сторонніх ланцюгах.

В одноточковій паралельній (радіальній) схемі заземлення (рис. 2.9) цього недоліку немає. Однак така схема вимагає великої кількості протяжних заземлюючих провідників, через що може виникнути проблема із забезпеченням малого опору заземлення ділянок ланцюга. Крім того, між заземлюючими провідниками можуть виникати небажані зв'язки, які створюють декілька шляхів заземлення для кожного пристрою. В результаті в системі заземлення можуть виникнути зрівняльні струми та з'явитися різниця потенціалів між різними пристроями.

Багатоточкова схема заземлення (рис. 3.9) вільна від недоліків, властивих одноточковій схемі. У цьому випадку окремі пристрої та ділянки корпусу індивідуально заземлені.

Як правило, одноточкове заземлення застосовується на низьких частотах при невеликих розмірах пристроїв, що заземлюються, і відстанях між ними менше $0,5\ \lambda$

На високих частотах при великих розмірах пристроїв, що заземлюються, і значних відстанях між ними використовується багатоточкова система заземлення.

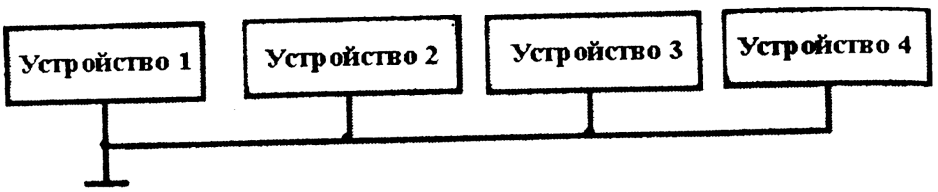


Рис. 1.9 Одноточкова послідовна схема заземлення

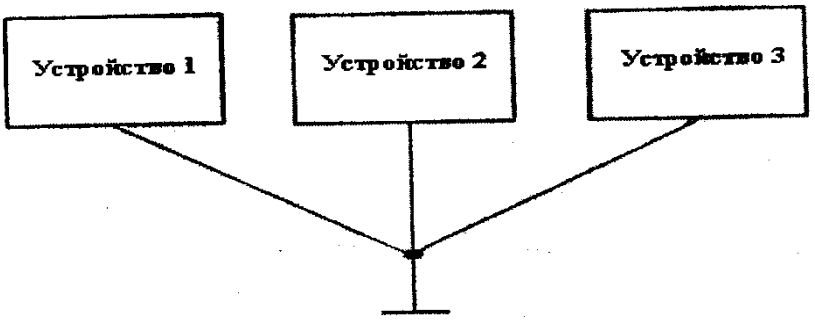


Рис. 2.9 Одноточкова паралельна (радіальна) схема заземлення

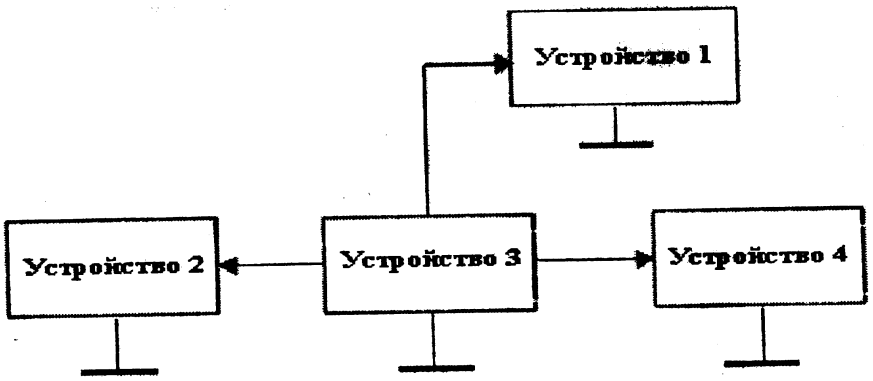


Рис. 3.9 Багатоточкова схема заземлення

Основні вимоги до системи заземлення полягають у наступному:

- система заземлення повинна включати загальний заземлювач, заземлюючий кабель, шини та дроти, що з'єднують заземлювач з об'єктом;
- опори заземлюючих провідників, а також земляних шин мають бути мінімальними;
- кожен елемент, що заземляється, повинен бути приєднаний до заземлювача або до заземлюючої магістралі за допомогою окремого відгалуження.
- послідовне включення до заземлюючого провідника кількох заземлюваних елементів забороняється;

- у системі заземлення повинні бути замкнуті контури, утворені з'єднаннями або небажаними зв'язками між сигнальними ланцюгами і корпусами пристроїв, між корпусами пристроїв і землею;

- слід уникати використання загальних провідників у системах екрануючих заземлень, захисних заземлень та сигнальних ланцюгів;

- якість електричних з'єднань у системі заземлення має забезпечувати мінімальний опір контакту, надійність та механічну міцність контакту в умовах кліматичних впливів та вібрації;

- контактні сполуки повинні виключати можливість утворення оксидних плівок на поверхнях, що контактують, і пов'язаних з цими плівками нелінійних явищ;

- контактні з'єднання повинні унеможливлювати утворення гальванічних пар для запобігання корозії в ланцюгах заземлення;

- забороняється використовувати як заземлюючий пристрій нульові фази електромереж, металоконструкції будівель, що мають з'єднання із землею, металеві оболонки підземних кабелів, металеві труби систем опалення, водопостачання, каналізації тощо.

Опір заземлення визначається головним чином опором розтікання струму землі. Величину цього опору можна значно знизити за рахунок зменшення перехідного опору між заземлювачем та ґрунтом шляхом ретельного очищення перед укладанням поверхні заземлювача та утрамбовуванням навколо нього ґрунту, а також підсипкою кухонної солі. Таким чином, величина опору заземлення в основному визначатиметься опором ґрунту. з'єднання в одній точці.

При підвищених вимогах до величини опору заземлення (опір заземлення ТЗПІ не повинен перевищувати 4 Ом) застосовують багаторазове заземлення, що складається з ряду одиночних симетрично розташованих заземлювачів, з'єднаних між собою. На практиці найчастіше як заземлювач застосовують:

- стрижні з металу, що мають високу електропровідність, занурені в землю та з'єднані з наземними металоконструкціями засобів ТЗПІ;

- сіткові заземлювачі, виготовлені з елементів з високою електропровідністю та занурені в землю (служать як доповнення до заземлюючих стрижнів).

При необхідності влаштування високочастотного заземлення потрібно враховувати не тільки геометричні розміри заземлювачів, їх конструкцію та властивості ґрунту, а й довжину хвилі високочастотного випромінювання. Сумарний високочастотний опір заземлення складається з високочастотного опору магістралі заземлення (проводу, що йде від заземлюваного пристрою до поверхні землі) і високочастотного опору самого заземлювача (проводу, металевого стрижня або листа, що знаходиться в землі). Величина заземлення переважно

визначається не опором заземлення, а опором заземлюючої магістралі. Для зменшення останнього слід прагнути насамперед зменшення індуктивності заземлюючої магістралі, що досягається за рахунок зменшення її довжини і виготовлення магістралі у вигляді стрічки, що володіє в порівнянні з проводом круглого перерізу меншою індуктивністю.

Найбільш придатними для заземлювачів є труби, що дозволяють досягти глибоких і найбільш вологих шарів землі, що мають найбільшу провідність і не підсихають або промерзають. Однак тут необхідно враховувати, що із зменшенням опору ґрунту зростає корозія металу.

Заземлювачі слід з'єднувати між собою шинами з допомогою зварювання. Перетин шин та магістралей заземлення за умов механічної міцності та отримання достатньої провідності рекомендується брати не менше (24 х 4) мм^2

Провідник, що з'єднує заземлювач із контуром заземлення, повинен бути лудженим для зменшення гальванічної корозії, а з'єднання повинні бути захищені від впливу вологи. Магістралі заземлення поза будівлею необхідно прокладати на глибині близько 1,5 м, а всередині будівлі - стіною або спеціальними каналами таким чином, щоб їх можна було зовні оглядати. З'єднують магістралі із заземлювачем лише за допомогою зварювання. До заземлюваного пристрою ТСПІ магістраль підключають за допомогою болтового зєднання.

Контрольні запитання

1. Для чого застосовується гранування технічних засобів обробки інформації?
2. Які способи екранування використовуються на практиці?
3. Доповісти сутність електростатичного екранування
4. Доповісти сутність магнітостатичного екранування
5. Доповісти сутність електромагнітного екранування
6. Навіщо використовується заземлення технічних засобів. Що використовується як заземлювач?
7. Доповісти про схему одноточкової послідовної схеми заземлення та її характеристики
8. Доповісти про схему одноточкової паралельної схеми заземлення та її характеристики
9. Доповісти про схему багатоточкової схеми заземлення та її характеристики
10. Доповісти основні вимоги до системи заземлення

Лекція № 10

Тема лекції: Програмний засіб захисту інформації в автоматизованих системах класу 1 від несанкціонованого доступу Рубіж РСО

ПЛАН ЛЕКЦІЇ

1. Інсталяція програмного забезпечення КЗЗ Рубіж-РСО
2. Деінсталяція програмного забезпечення КЗЗ Рубіж-РСО

1. Інсталяція програмного забезпечення КЗЗ Рубіж-РСО

Інсталяційний пакет ПЗ КЗЗ “Рубіж-РСО” постачається розробником на CD для проведення робіт з інсталяції програмних засобів та відновлення програмного забезпечення у випадку його знищення. Структура та склад пакета наведені у таблиці 1.10.

Таблиця 1.10 Склад дистрибутивного носія

Розташування	Модуль	Опис
<диск CD>		
	ReadMe.txt	інформаційний файл
<диск CD>\Docs		місце розташування документації
	Instr_user.doc	Інструкція користувача
	ZO.doc	Загальний опис
	Instr_inst.doc	Інструкція з інсталяції
	exp_visn.jpg	Експертний висновок
<диск CD>\Install		місце розташування інсталяційного ПЗ
	Setup.exe	програма запуску інсталяції
	nof8ntldr	
	mash.dat	
	DATA.TAG	
	data1.cab	
	data1.hdr	
	lang.dat	
	layout.bin	
	os.dat	
	Setup.bmp	
	SETUP.INI	
	setup.ins	
	setup.lid	
	INST32I.EX	
	_ISDel.exe	
	Setup.dll	
	_sys1.cab	
	_sys1.hdr	
	_user1.cab	
	user1.hdr	
	fsetup.dll	

Програмний засіб захисту інформації в автоматизованих системах класу 1 Рубіж РСО призначений для запобігання несанкціонованого доступу до інформації щляхом розмежування доступу до між користувачами АС 1.

Загальні вимоги. ПЗ КЗЗ “Рубіж-РСО” призначений для встановлення лише на операційні системи Microsoft Windows 2000 Professional з пакетом оновлень SP4 або Microsoft Windows XP Professional з пакетом оновлень SP2.

Для нормального функціонування ПЗ КЗЗ “Рубіж-РСО” необхідне виконання наступних мінімальних системних вимог:

- процесор Pentium на 233 МГц або більш потужний (або сумісний з ним);
- об’єм оперативної пам’яті 128 мегабайт (МБ);
- 20 МБ вільного місця на жорсткому диску;
- монітор VGA;
- клавіатура;
- миша;
- дисковід компакт-дисків.

Процес інсталяції неможливий у разі відсутності локальних адміністративних повноважень облікового запису користувача – виконавця інсталяції, а також у разі встановлення ПЗ КЗЗ “Рубіж-РСО” на диск, файлова система якого не NTFS. До процесу інсталяції повинно бути сформоване довірче середовище (“Інструкція користувача” [21502504.184154.705.И3] – далі Інструкція користувача, п.1.2.2, п.2.10) та проініційовані засоби політики безпеки ОС (**Адміністрування – Локальна політика безпеки**).

Процес інсталяції включає:

- запуск на виконання модулю Setup.exe;
- послідовну відповідь на питання під час процесу інсталяції;
- додаткове налагодження операційної системи;
- перезавантаження операційної системи.

У накопичувач CD-ROM вставляється інсталяційний диск ПЗ КЗЗ “Рубіж-РСО” та виконується з нього файл **setup.exe**. З’являється екранна форма (Рис. 1), яка відображає інформацію про початок інсталяції ПЗ.

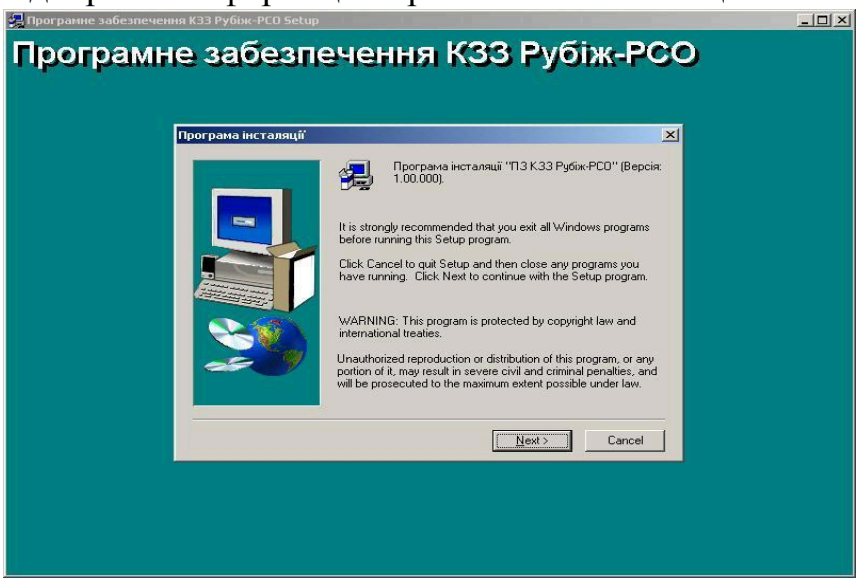


Рис. 1.10 Початок інсталяції ПЗ КЗЗ “Рубіж-РСО”

Для продовження процесу інсталяції лівою кнопкою миші натиснути кнопку Next >, а для відмови від подальшої інсталяції – кнопку Cancel.

На наступному етапі інсталяції заповнюємо форму “Реєстраційні дані” (Рис. 2.10). У полі **Serial** заносимо серійний номер продукту (CD Key), наданий разом з інсталяційним диском.

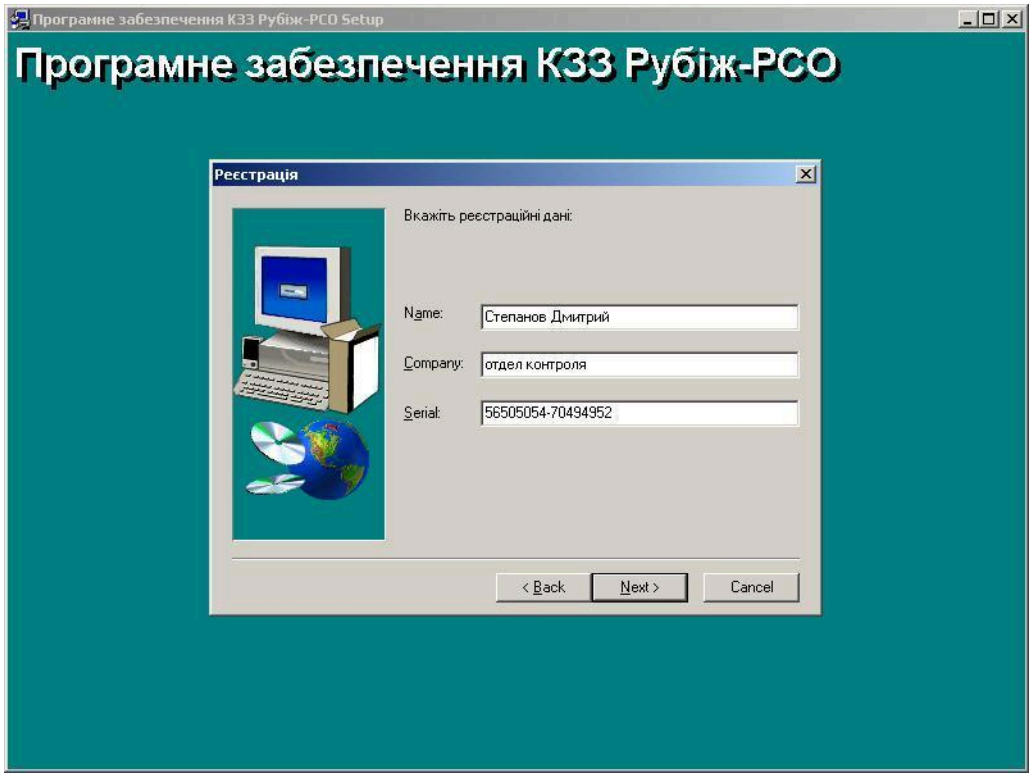


Рис. 2.10 Вікно внесення реєстраційних даних

На наступному етапі обираємо технологію оброблення інформації (рис. 3.10):

- **без збереження на жорсткому диску** – інформація АС зберігається у вигляді текстових, графічних файлів або у вигляді електронних таблиць тільки на з’ємних магнітних (гнучкі магнітні диски, Flash диски) та оптичних носіях (CD-R/RW), які зареєстровані адміністратором в базі даних КЗЗ “Рубіж-РСО”. На одному носії зберігаються дані одного ступеню конфіденційності, який відповідає встановленому для носія грифу конфіденційності;
- **зі збереженням на жорсткому диску** – дані зберігаються на машинних носіях великої ємності (жорсткі магнітні диски, вбудовані в ПЕОМ; з’ємні магнітні та оптичні диски; магнітні стрічки тощо). На машинних носіях великої ємності зберігаються дані одного ступеня конфіденційності, який відповідає встановленому для носія грифу конфіденційності.

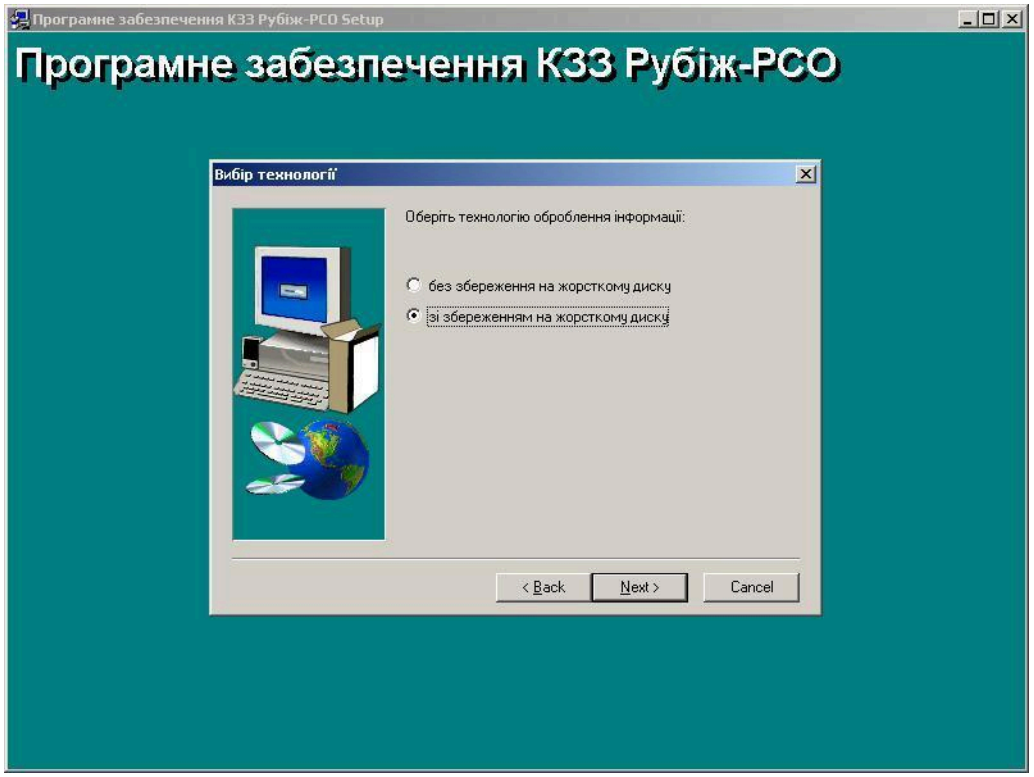


Рис. 3.10 Вибір технології оброблення інформації

Далі обираємо рівень обмеження доступу (рис. 4.10). Відповідно до розподілу повноважень доступу до інформації КЗЗ “Рубіж-РСО” (Інструкція користувача п.2.4.1) для організації розмежування доступу до інформації різних рівнів в КЗЗ введені наступні локальні групи:

RSO_ADMINS - для доступу до інформації з адміністративним рівнем доступу;

RSO_GROUP_2– для доступу до інформації з високим рівнем доступу;

RSO_GROUP_3– для доступу до інформації із середнім рівнем доступу;

RSO_GROUP_4 – для доступу до інформації з базовим рівнем доступу.

При інсталяції в системі по замовчуванню створюється група RSO_ADMINS, в яку автоматично вноситься обліковий запис користувача – ініціатора інсталяції.

У разі вибору рівня **Високий** – створюються усі 3 групи: RSO_GROUP_2, RSO_GROUP_3, RSO_GROUP_4.

У разі вибору рівня **Середній** – створюються тільки 2 групи: RSO_GROUP_3, RSO_GROUP_4.

У разі вибору рівня **Базовий** – створюються тільки група RSO_GROUP_4.

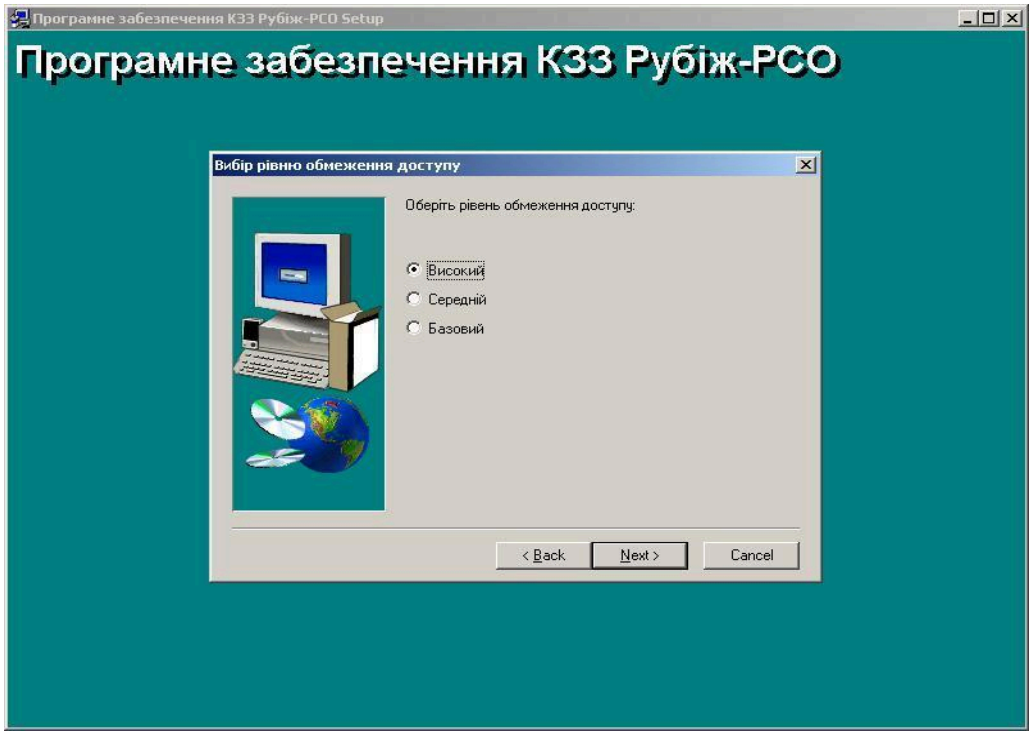


Рис. 4.10 Вибір рівня обмеження доступу

Далі обираємо шлях встановлення ПЗ КЗЗ “Рубіж-РСО” (рис. 5.10).

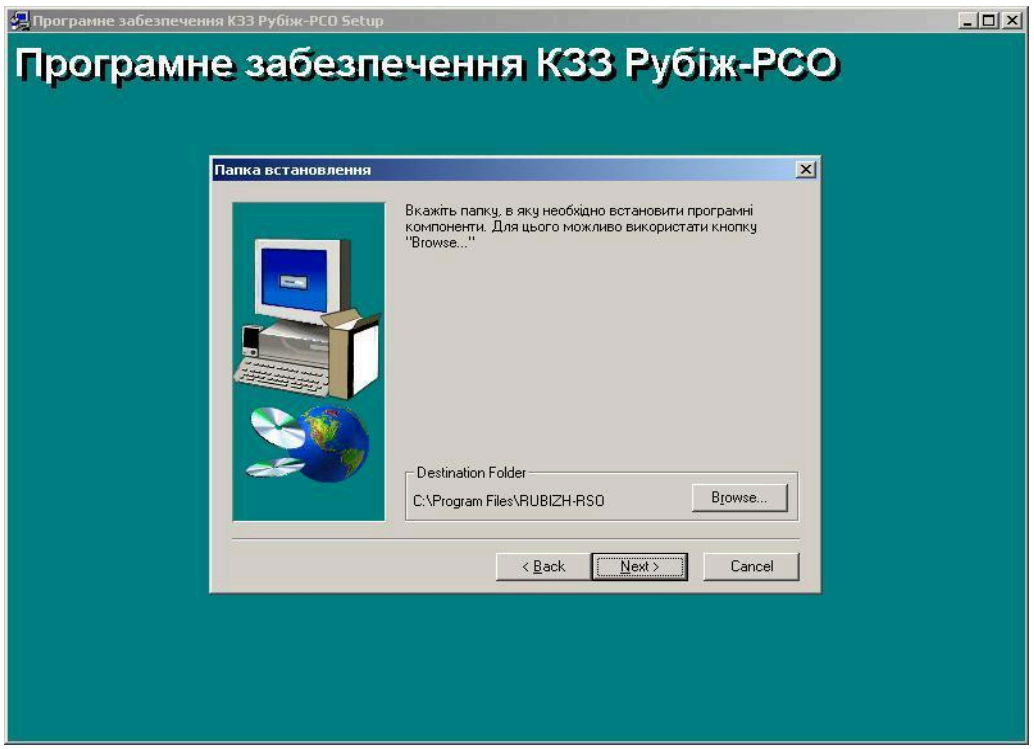


Рис. 5.10 Вибір шляху встановлення ПЗ

Після натискання лівою кнопкою миші на кнопку  починається саме встановлення ПЗ КЗЗ “Рубіж-РСО” на робочу станцію (рис. 6.10). Перервати

процес інсталяції можливо, якщо натиснути лівою кнопкою миші на кнопку Cancel.

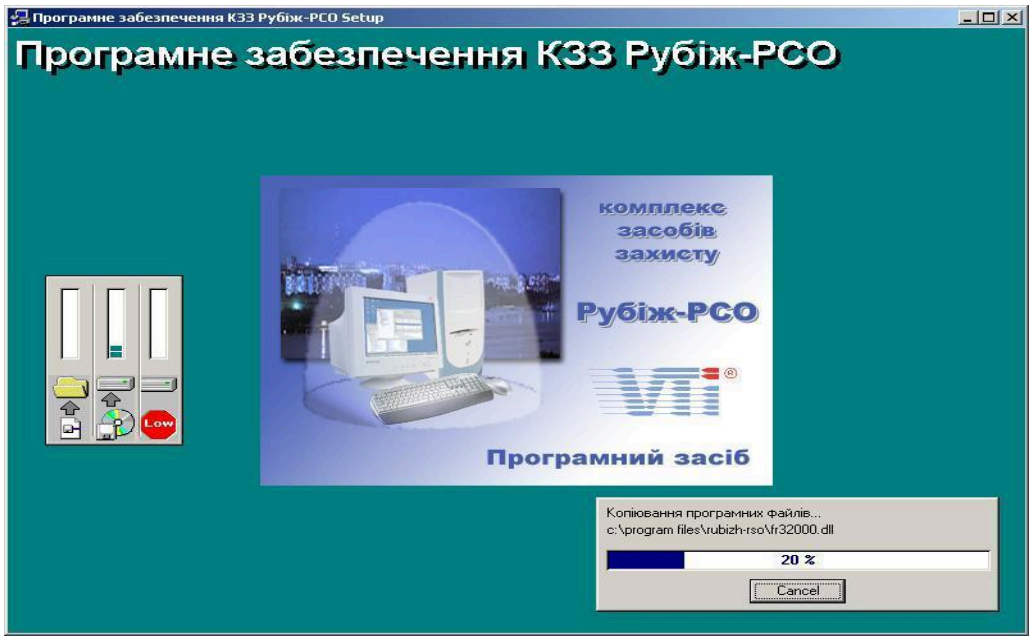


Рис. 6.10 Процес інсталяції ПЗ

Після закінчення інсталяції з'являється вікно (рис. 7.10) з пропозицією перезавантажити робочу станцію, на якому треба вибрати пункт "No, I will restart my computer later". Далі необхідно виконати додаткове налагодження операційної системи в залежності від її версії.

Носій, з якого проводилася інсталяція буде автоматично зареєстрований і в подальшому може бути використаний для посиленої автентифікації.

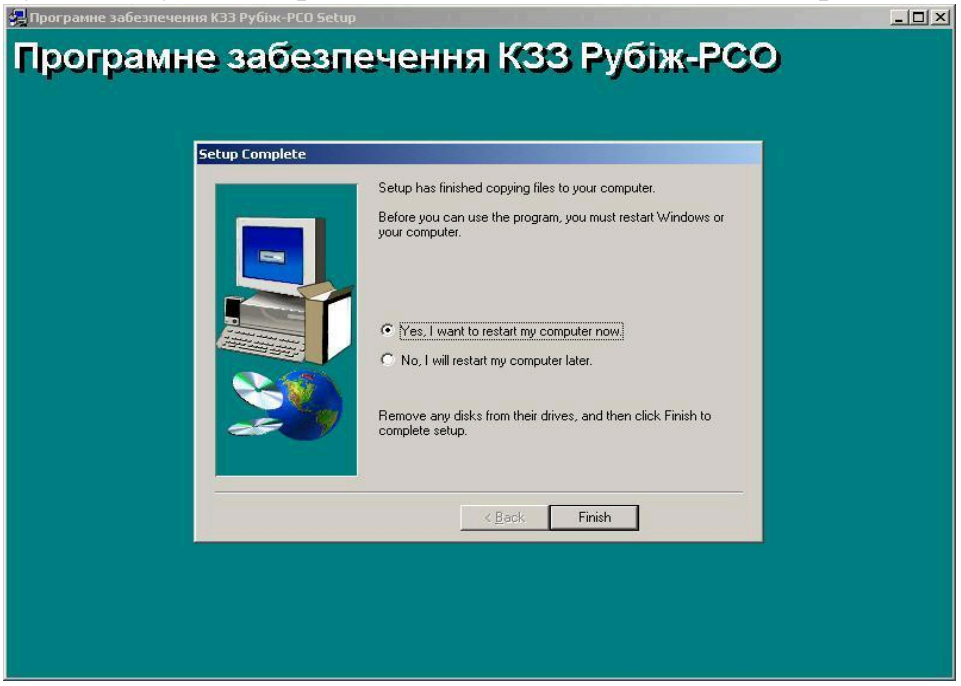


Рис. 7.10 Завершення інсталяції ПЗ "Рубіж-РСО"

Додаткове налагодження для ОС Windows 2000

В разі встановлення ПЗ КЗЗ “Рубіж-РСО” на платформу Windows 2000 перед встановленням Microsoft Office можливі ситуації відмови у роботі серверної частини у зв’язку з необхідністю ініціалізації системою першого виклику Microsoft.Jet.OLEDB. Виявити таку помилку можна з аналізу системного журналу **Журнал приложений**. Для того, щоб привести ПЗ до робочого стану необхідно засобами ОС встановити повний доступ до папки (в яку була проведена інсталяція ПЗ) і усіх її елементів обліковому запису **Все**. (**Проводник** – *<папка з ПЗ>* – **Свойства** – **Безопасность** – **Все** – **Полный доступ** (рис. 8.10) – **Дополнительно** – **Сбросить разрешения для всех дочерних объектов**... (Рис. 9)– **Применить**). Після цього запустити службу (**Администрирование** – **Службы** – **RSOClassService** – **Запуск службы**). В разі успіху ПЗ “Рубіж-РСО” відкриває інтерфейс користувача.

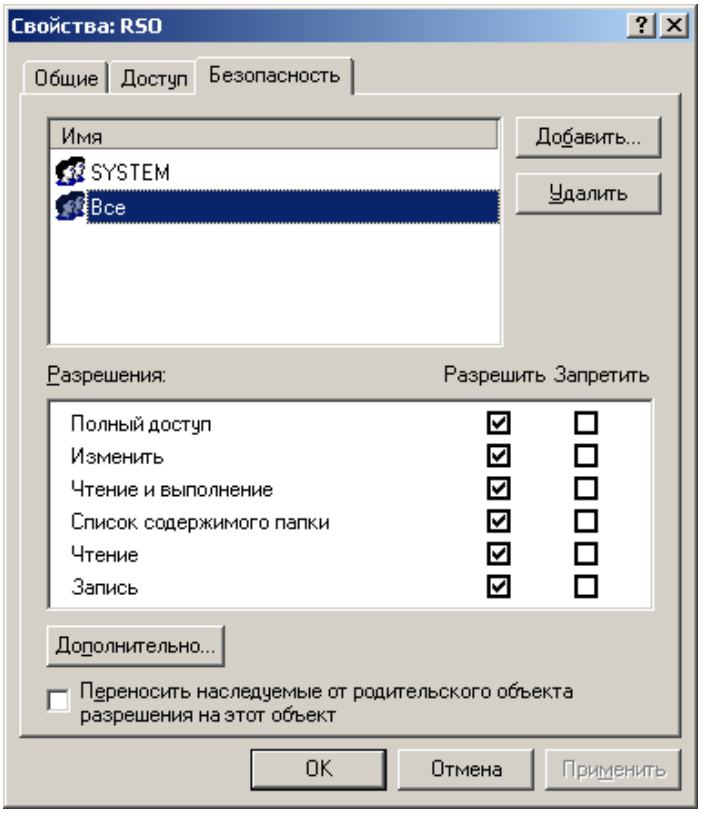


Рис. 8.10 Властивості папки

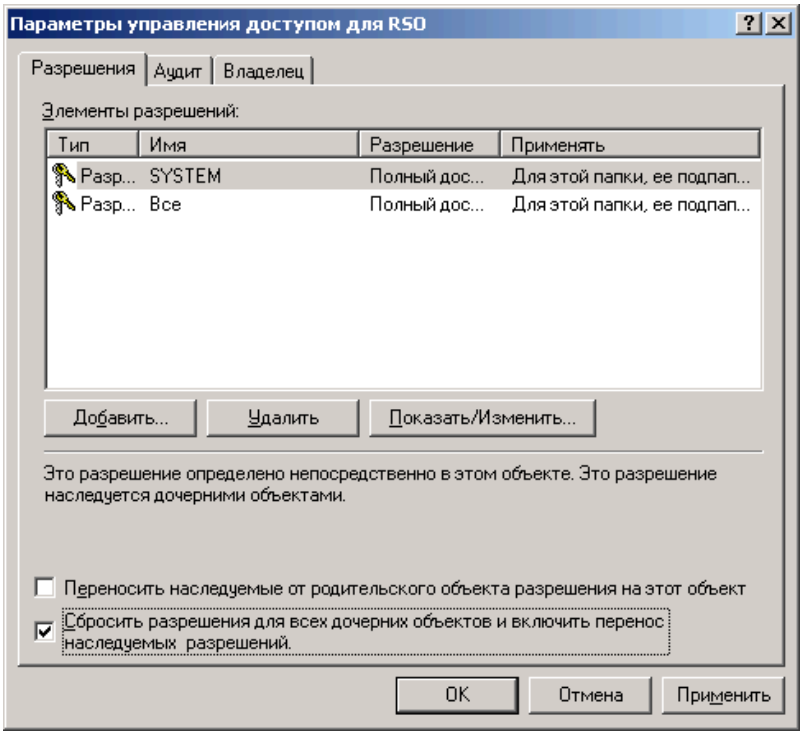


Рис. 9.10 Параметри керування доступом обраної папки

В разі виявлення при вході в систему проблеми з використанням операційної пам’яті (за допомогою диспетчера задач (Рис. 10.10)) між процесами *winlogon.exe* та *servicrs.exe* необхідно здійснити запуск ОС у безпечному режимі для того, щоб дати проініціалізуватися взаємодії між цими процесами. Запуск ОС у безпечному режимі здійснюється за допомогою завантажувальної дискети після зміни у BIOS порядку завантаження ОС. У безпечному режимі повинен бути доступний функціонуючий інтерфейс користувача ПЗ “Рубіж-РСО”.

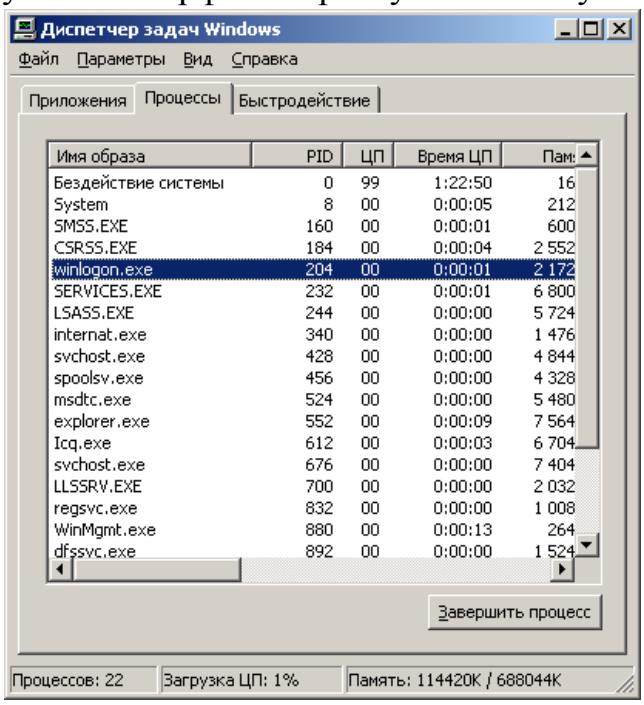


Рис. 10.10 Диспетчер задач

В разі, коли ПЗ “Рубіж-РСО” припиняє свою роботу з характерними повідомленнями ОС про COM об’єкти необхідно: зупинити службу серверної частини (**Администрирование – Службы – RSOClassService** (рис. 11.10) – **Остановка службы**). Потім вводимо в командному рядку *dcomcnfg*. Обираємо **RSOClassCom Object – Свойства** (Рис. 12.10). Далі переходимо на сторінку **Безопасность**. Проводимо налагодження шляхом переключення на **Использовать пользовательские разрешения доступа** та **Использовать пользовательские разрешения запуска** і **OK**.

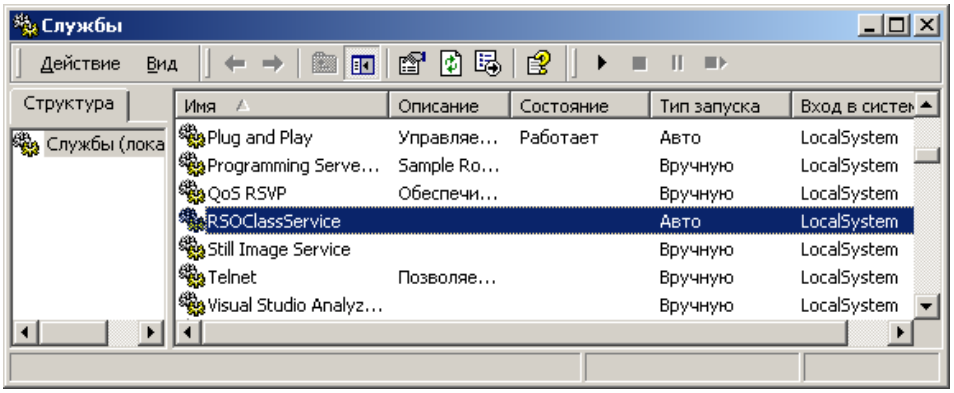


Рис. 11.10 Служби

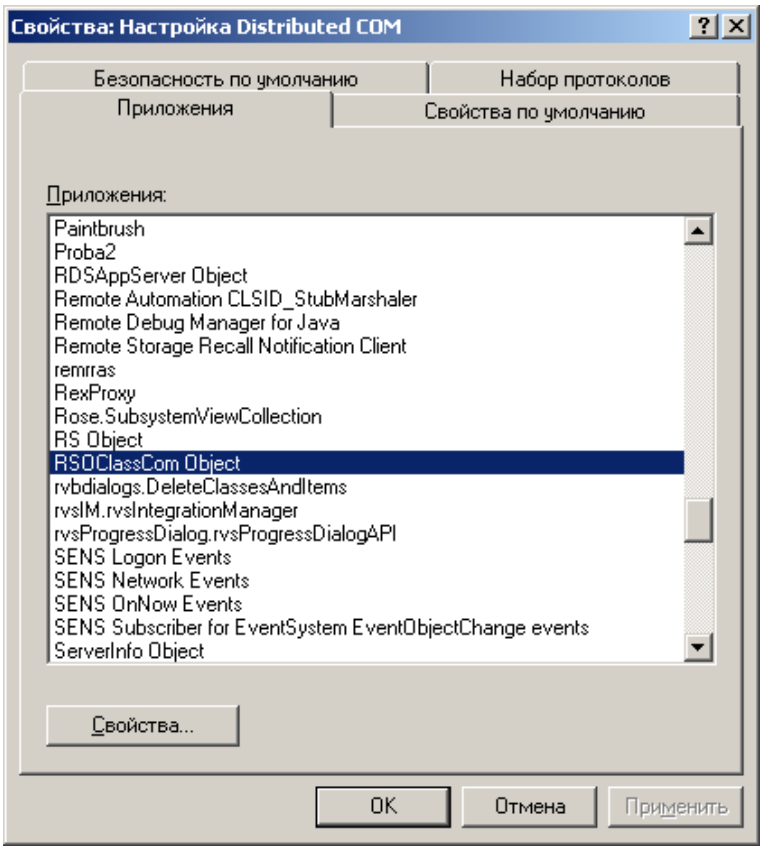


Рис. 12.10 Налагодження COM

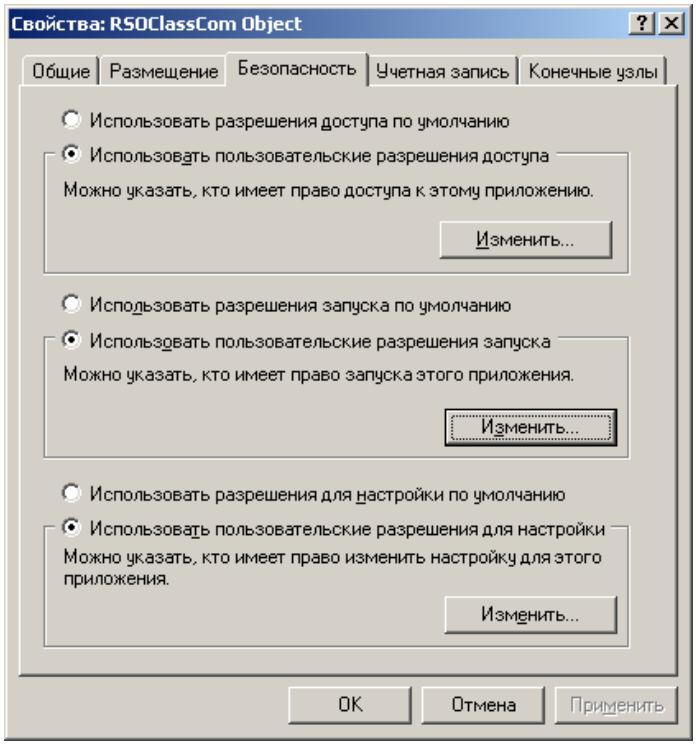


Рис. 13.10 Безпека властивостей обраного COM-об'єкта

Додаткове налагодження для ОС Windows XP

В разі встановлення ПЗ КЗЗ "Рубіж-РСО" на платформу Windows XP з другим пакетом оновлення (SP 2), або інколи і без нього, необхідно провести перед перезавантаженням системи наступні дії:

Брендмауер. Доступ до нього можна отримати, наприклад, з властивостей локальної мережі, обравши пункт **Изменить параметры брэндмауэра Windows**. Необхідно відключити його на першій закладці (рис. 14.10).

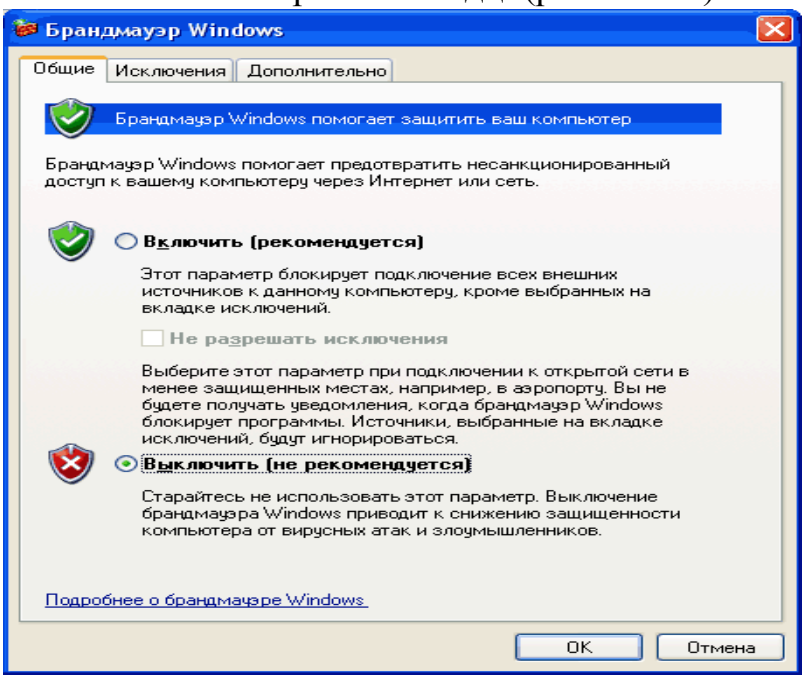


Рис. 14.10 Брендмауер Windows

DCOM. Вводимо в командному рядку *dcomcnfg*. Обираємо в **Службы компонентов - Компьютеры - Мой компьютер - Настройка DCOM** *{D02C5AC7-B837-4C43-9FFD-D60666C695B6}* (Рис. 15.10).

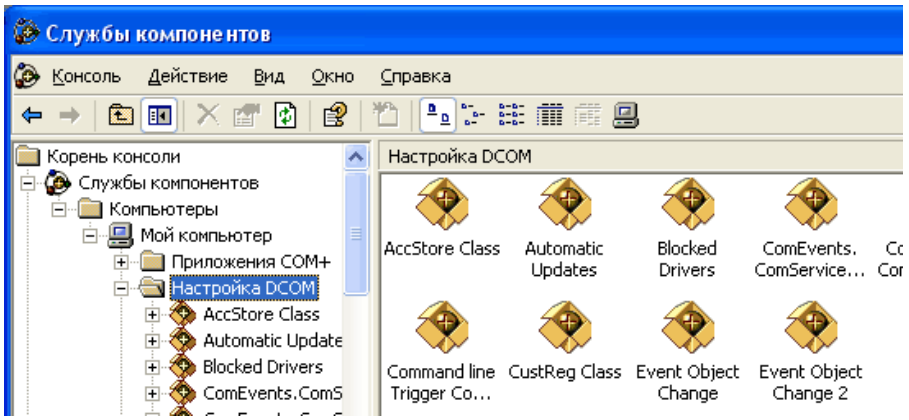


Рис. 15.10 Служби компонентів Windows

Права кнопка миші - **Свойства**. Закладка **Безопасность** (Рис. 16.10).

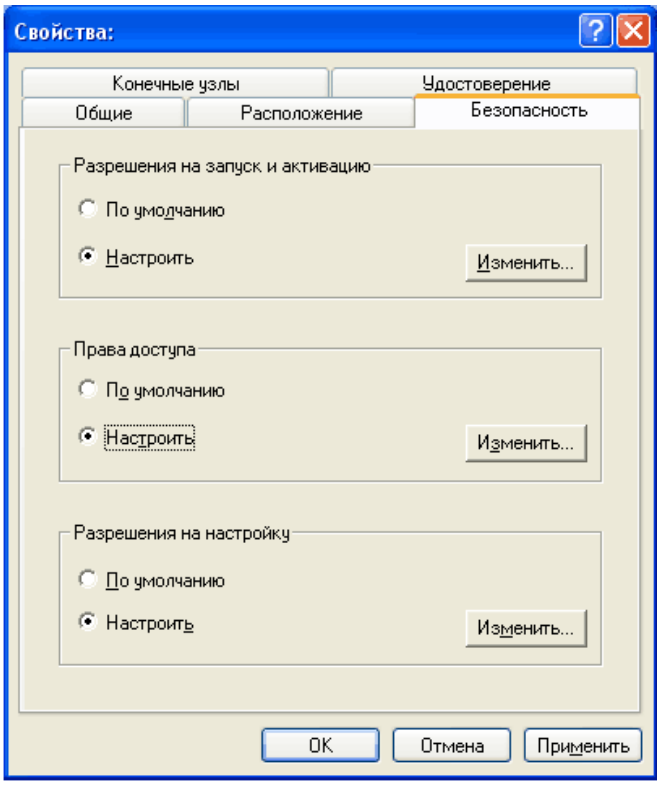


Рис. 16.10 Властивості

Проводимо налагодження **Разрешения на запуск и активацию** і **Права доступа** шляхом переключення на **Настроить - Изменить** та додавання користувача *АНОНИМНЫЙ ВХОД,* для якого встановлюємо дозвіл тільки на **Локальный запуск** та **Локальная активация** (рис. 10, рис. 18.10).

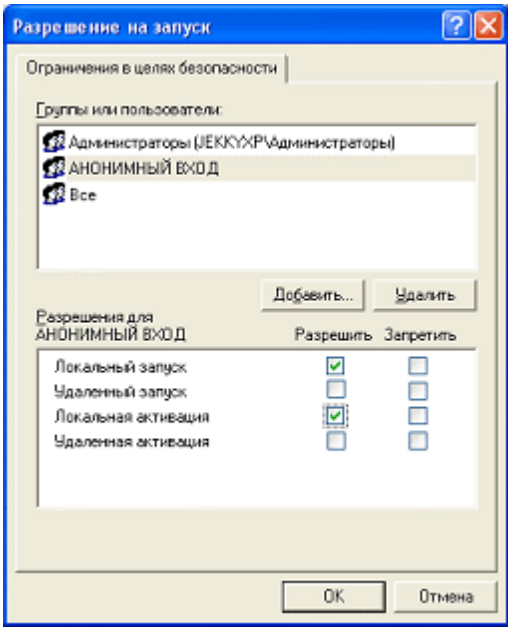


Рис. 17.10 Дозвіл на запуск

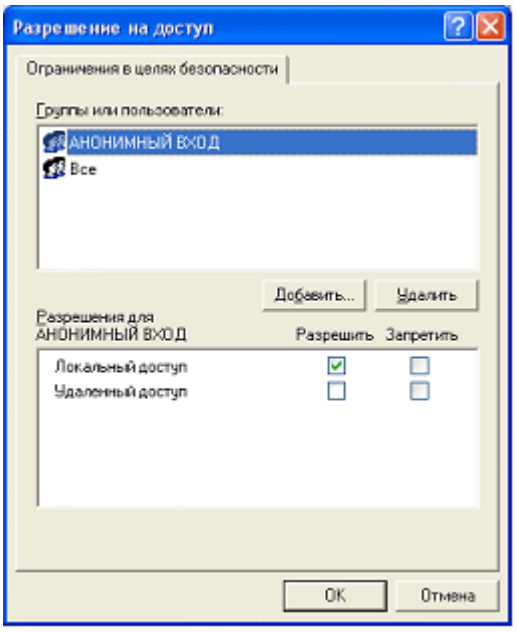


Рис. 18 .10Дозвіл на доступ

Створення облікового запису адміністратора безпеки

Після завершення інсталяції ПЗ КЗЗ “Рубіж-РСО” та перезавантаження операційної системи, користувач з правами локального адміністратора (виконавець інсталяції) входить в неї використовуючи в якості PIN-диску інсталяційний диск. Далі, згідно з Інструкцією користувача п.2.1, створює обліковий запис адміністратора безпеки, присвоює первинний пароль та заносить

запис у групу RSO_ADMINS. Згідно з Інструкцією користувача п.4.2.1, призначає адміністратору безпеки PIN-код, використовуючи PIN-диск, що входить в комплект поставки, який в подальшому буде використовуватись в якості PIN-диску адміністратора безпеки. Адміністратор безпеки змінює свій пароль при першому вході у систему, який здійснюється при обов'язковій наявності призначеного йому PIN-диску у приводі CD-ROM. Усі подальші включення робочої станції з встановленим ПЗ КЗЗ "Рубіж-РСО" також обов'язково відбуваються за умови присутності зареєстрованого PIN-диску у приводі CD-ROM.

2. Деінсталяція програмного забезпечення КЗЗ Рубіж-РСО

Для деінсталяції програмного забезпечення КЗЗ "Рубіж-РСО" необхідно виконати наступні дії:

- увійти в операційну систему під обліковим записом адміністратора безпеки; зупинити служби **RSO_Auth** та **RSOClassService** (**Администрирование** – **Службы** – **RSOClassService** (рис. 19.10) – **Остановка службы**);

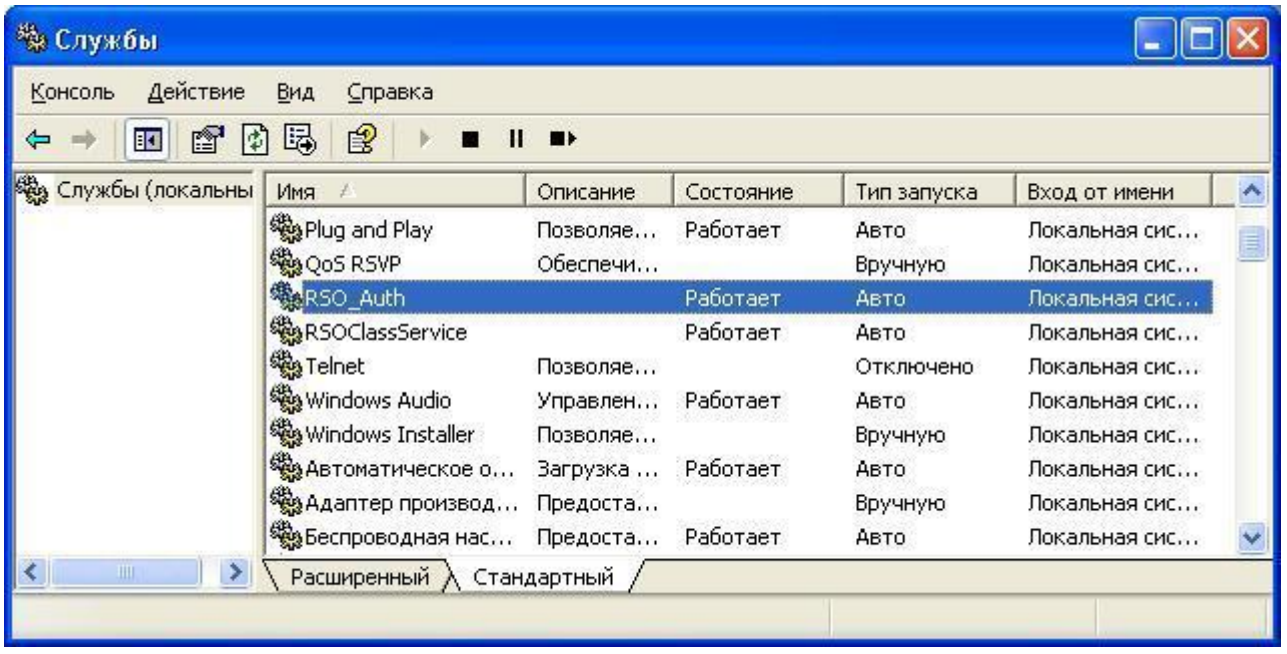


Рис. 19.10 Служби

- провести деінсталяцію програмного забезпечення КЗЗ "Рубіж-РСО" (**Панель управления** – **Установка и удаление программ** – **Програмне забезпечення КЗЗ Рубіж-РСО** (рис. 20.10) – **Заменить/Удалить**);
- перезавантажити операційну систему та увійти в неї під обліковим записом адміністратора безпеки (в даному випадку PIN-диск вже не потрібен);
- встановити повний доступ до папки (в яку була проведена інсталяція ПЗ) і усіх її елементів обліковому запису **Все**. (**Проводник** – *<папка з ПЗ>* –

Свойства – Безопасность – Все – Полный доступ (Рис. 21) – **Дополнительно – Сбросить разрешения для всех дочерних объектов**... (Рис. 22)– **Применить**).

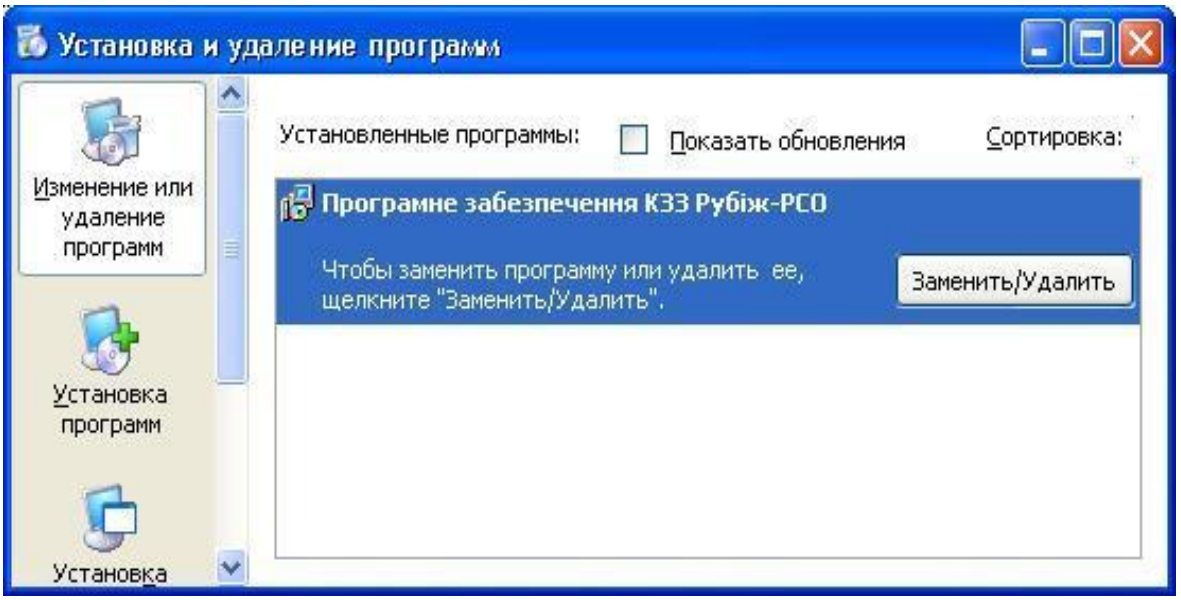


Рис. 20.10 Встановлення та видалення програм

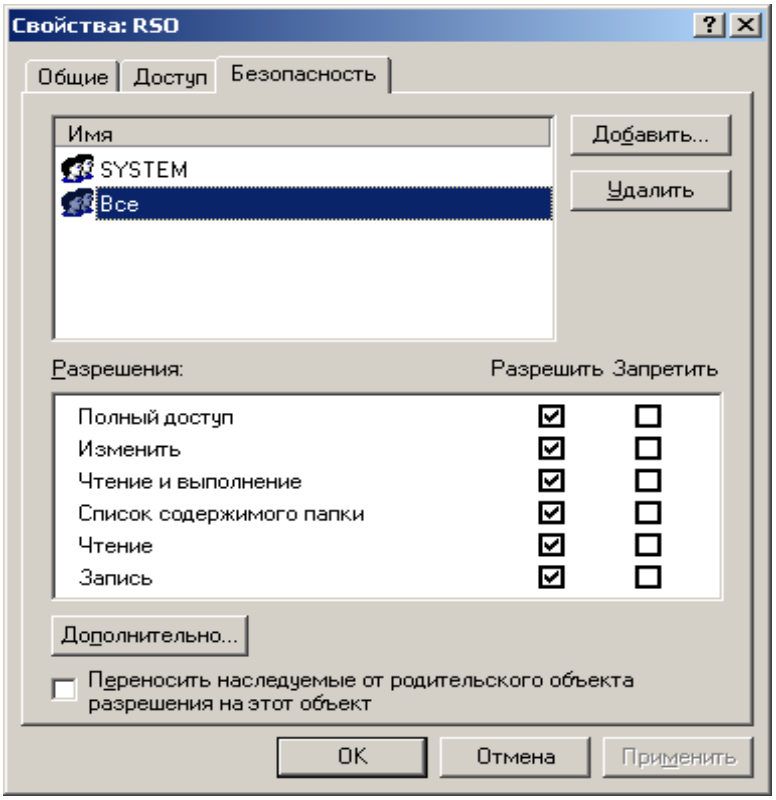


Рис. 21.10 Властивості папки

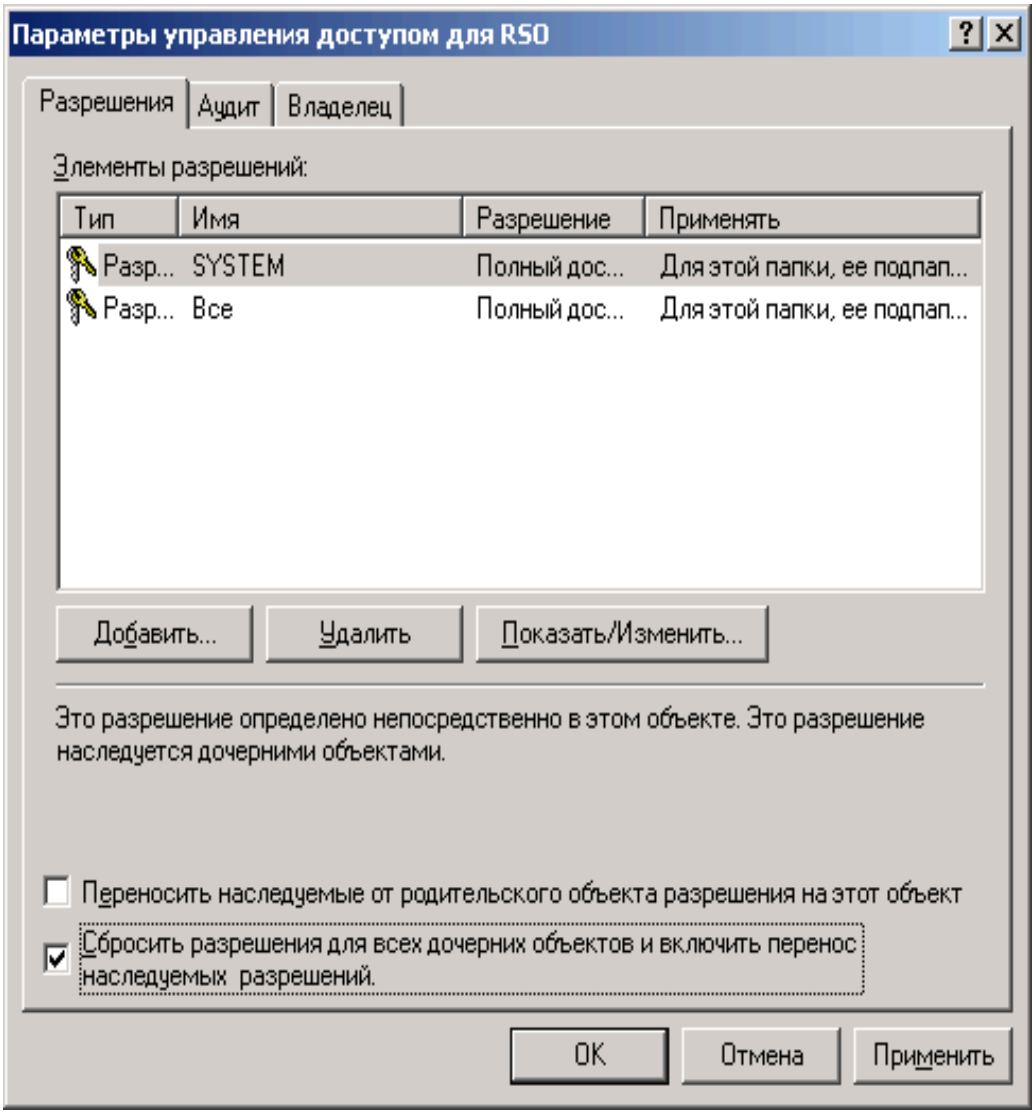


Рис. 22.10 Параметри керування доступом обраної папки

- видалити засобами операційної системи папку в яку була проведена інсталяція ПЗ.

ЕКСПЕРТНИЙ ВИСНОВОК

Комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу „1”, „Рубіж-РСО”, версія 1.0, виробництва ВАТ „КП ОТІ”

Зареєстровано в Департаменті спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України
“01” червня 2006 р. за № 82
Дійсний до “01” червня 2009 р.
Начальник ДСТСЗІ СБ України
К.Бойко
М.П.

За результатами експертизи встановлено, що **комплекс засобів захисту інформації від несанкціонованого доступу**
назва засобу технічного захисту інформації
в автоматизованій системі класу „1” „Рубіж-РСО”, версія 1.0,

наданий на експертизу **ВАТ „КП ОТІ”,**
назва та адреса організації
03115, м. Київ, вул. Ф.Пушіної, 30/32,

відповідає
відповідає, не відповідає
вимогам нормативних документів системи технічного захисту інформації в Україні в обсязі функцій, зазначених у документі „Комплекс засобів захисту інформації від несанкціонованого доступу в автоматизованій системі класу „1” „Рубіж-РСО”. Технічне завдання” [21502504.184154.705.ТЗ], сукупність яких визначається функціональним профілем **КА-2, КО-1, ЦА-1, ДВ-1, НР-2, НИ-3, НК-1, НО-2, НЦ-1, НТ-2** із рівнем гарантій **Г-3** оцінки коректності їх реалізації згідно з НД ТЗІ 2.5-004-99.

Вимоги до умов експлуатації та сфери використання об’єкта експертизи визначені у розділі 8 цього експертного висновку.

Директор НДЦ „ТЕЗІС”
НТУУ „КПІ”
керівник організатора експертизи — підпис — **М.І. Прокофьєв** (ініціали, прізвище)
М.П.

Рис. 23.10 Експертний висновок на КЗЗ від НСД РУБІЖ-РСО

Контрольні запитання

1. Доповісти призначення програмного засобу захисту інформації в автоматизованих системах класу 1 Рубіж РСО.
2. Доповісти системні вимоги ПЕОМ для встановлення Рубіж РСО.
3. Доповісти що включає в себе процес інсталяції Рубіж РСО.
4. Які існують варіанти обробки інформації у ПЗ Рубіж РСО.
5. Які існують варіанти рівнів обмеження доступу у ПЗ Рубіж РСО.
6. Доповісти профіль захищеності який забезпечує у ПЗ Рубіж РСО.
7. Доповісти порядок деінсталяції ПЗ Рубіж РСО.

Лекція № 11

Тема лекції: Склад та призначення технічної системи охорони об’єктів

ПЛАН ЛЕКЦІЇ

1. Матеріально-речовий канал витоку інформації.
2. Склад технічної системи охорони.
3. Структури технічних систем охорони.
4. Класифікація чутливих елементів засобів виявлення
5. Інтегрована система забезпечення безпеки об'єктів інформаційної діяльності**.**

1. Матеріально-речовий канал витоку інформації

Особливість цього каналу викликана специфікою джерел і носіїв інформації в порівнянні з іншими каналами. Джерелами і носіями інформації в ньому є суб'єкти (люди) і матеріальні об'єкти (макро і мікрочастинки), які мають чіткі просторові межі локалізації, за винятком випромінювань радіоактивних речовин. Витік інформації в цих каналах супроводжується фізичним переміщенням людей і матеріальних тіл з інформацією за межами контрольованої зони. Для більш чіткого опису розглянутого каналу доцільно уточнити склад джерел і носіїв інформації.

Основними джерелами витоку інформації з матеріально-речового каналу є наступні:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, що ведуться в організації;
- відходи діловодства та видавничої діяльності в організації, у тому числі використана копіювальний папір, забраковані листи при оформленні документів та їх розмноженні;
- містять захищається інформацію дискети ПЕОМ, нечитані через їх фізичних дефектів і спотворень завантажувальних або інших секторів;
- бракована продукція та її елементи;
- відходи виробництва з демаскуючими речовинами в газоподібному, рідкому і твердому вигляді.

Перенесення інформації в цьому каналі за межі контрольованої зони можливий наступними суб'єктами та об'єктами:

- співробітниками організації;
- повітряними масами атмосфери;
- рідким середовищем;

Ці носії можуть переносити всі види інформації: семантичну і ознаковими, а також демаскуючі речовини.

Для добування інформації зловмисник, як правило, використовує кілька шляхів її витоку. Комплексне використання шляхів витоку інформації грунтується на наступних принципах:

- комплексируємі канали доповнюють один одного за своїми можливостями;

- ефективність комлексування підвищується при зменшенні залежності між джерелами інформації та демаскуючими ознаками в різних каналах.

Комплексування каналів витоку інформації забезпечує:

- збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їх поточних ознакових структур;

- підвищення достовірності семантичної інформації і точності вимірювання ознак, особливо у разі добування інформації з недостатньо надійних джерел.

Коли виникають сумніви в достовірності інформації, то з метою виключення дезінформації, отримані відомості і дані перепровіряють по іншому каналу.

Для запобіганню витоку інформації матеріально-речовим каналом використовують технічні, фізичні засоби.

До технічних відносять: технічні системи охорони, системи відеоспостереження, системи контролю та управління доступом на ОІД.

2 Склад технічної системи охорони.

У загальному вигляді технічна система охорони включає в себе наступні засоби (рис. 1.11):

- засіб виявлення (ЗВ) (сповіщувач) - це пристрій, призначений для автоматичного формування сигналів із заданими параметрами (сигналу тривоги) внаслідок вторгнення або подолання зловмисником зони виявлення даного пристрою.

- прилад приймально-контрольний охоронно пожежний (ППКОП) - пристрій, який отримує сигнал тривоги від сповіщувачів та здійснює управління за заданим алгоритмом виконавчими пристроями (у простому випадку контроль за роботою охоронно-пожежної сигналізації складається з включення і виключення сповіщувачів, фіксації сигналів тривоги, в складних, розгалужених системах сигналізації контроль і управління здійснюються за допомогою комп'ютерів);

- шлейф сигналізації — електричний ланцюг, який поєднує сповіщувач з приладом приймально-контрольним охоронно-пожежним;

- виконавчі пристрої - агрегати, які забезпечують виконання заданого алгоритму дій системи у відповідь на ту чи іншу тривожну подію (подача сигналу оповіщення, включення механізмів пожежогасіння, автодозвон за заданими номерами телефонів і т п.).

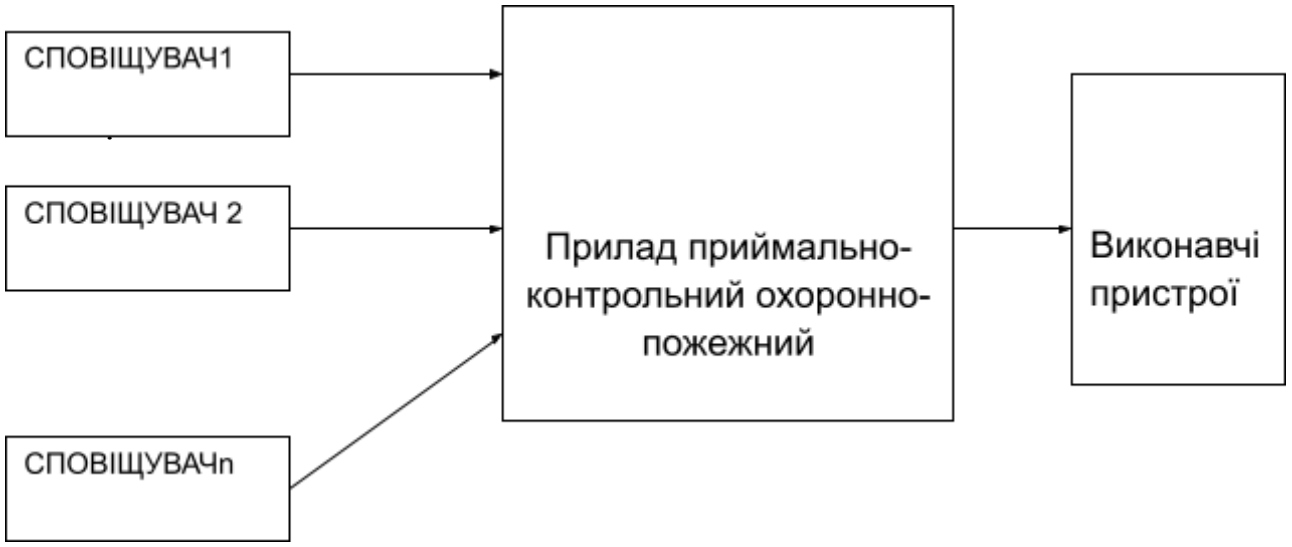


Рис. 1.11 Склад технічної системи охорони об’єкту

3. Структура типових варіантів побудови комплексів ТЗОС визначається розподілом логічної обробки інформації від ЗВ і станційною апаратурою (ППКОП) (периферійними блоками), а також способом зв'язку між ними і ЗВ. На вибір варіанту структури побудови комплексу головним чином роблять вплив наступні чинники;

– якісний і кількісний склад обслуговуваних ЗВ і ПБ (концентратори, ППКОП і ін);

– ступінь централізації управління ППКОП;

– структурні особливості об'єктів, що охороняються;

–чинники вартості і надійності.

Відомі наступні основні способи з'єднання станційної апаратури з периферійними блоками і ЗВ (варіанти побудови структурних схем ТЗО):

1. **Радіальний** (променевий) безконцентраторний (рис. 2.11).

Як правило, комплекси ТЗОС з радіальною безконцентраторною структурою мають наступні основні особливості;

– простота виконання і технічного обслуговування апаратної частини (підключення, налаштування, ремонту і ін.);

– підключення кожного ЗВ здійснюється по окремих ланцюгах електроживлення, дистанційної перевірки і контролю стану;

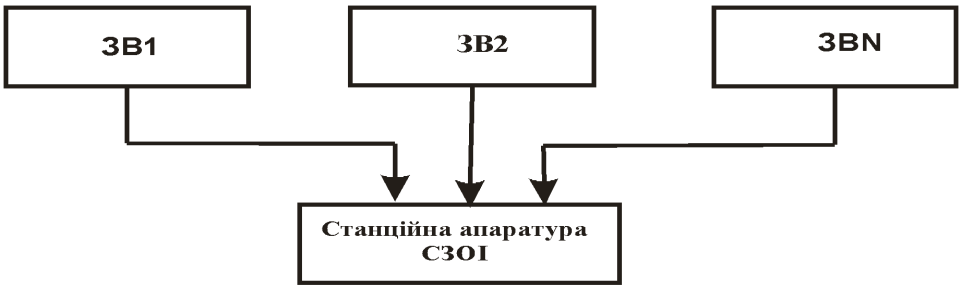


Рис. 2.11 Радіальне (променеве) безконцентраторне з'єднання станційної апаратури із ЗВ

– несправності, що виникають в лініях зв'язку ЗВ і вхідних ланцюгах станційної апаратури, впливають на працездатність тільки окремого каналу сигналізації, що при відповідній організації охорони не впливає на функціонування всього комплексу ТЗОС;

– значний об'єм і розгалуженість кабельних ліній (для дротяних систем).

2. **Радіальний (променевий) з концентраторами** (рис. 3.11).

Призначення концентраторів в СЗОІ (ППКОП) різного типу може відрізнятися по різних ознаках.

ПБ – периферійний блок

Рис. 3.11 Радіальне (променеве) з концентраторами з'єднання станційної апаратури з ПБ і ЗВ

Окрім функцій збільшення ємності апаратури (під ємністю розуміють кількість каналів сигналізації СЗОІ (ППКОП), тобто кількість одиничних апаратно-програмних засобів СЗОІ (ППКОП), кожне з яких призначене для контролю над станом одного ЗВ і ущільнення інформації що передається, концентратори можуть служити для об'єднання ЗВ по ділянках блокування, автоматичної перевірки їх працездатності і забезпечення контролю лінії зв'язку.

У окремих системах окрім названих функцій в концентратори закладаються функції попередньої обробки сигналів від ЗВ. Через них же здійснюється і електроживлення ЗВ.

До особливостей комплексів ТЗОС з радіальною структурою з концентраторами можна віднести наступні:

– при постановці на охорону/зняття охорони якого-небудь каналу сигналізації подача/зняття електроживлення здійснюється на всю групу каналів, підключених до одного концентратора, тобто по одній лінії зв'язку здійснюється електроживлення концентратора і всіх ЗВ, підключених до даного концентратора. Цю обставину можна не враховувати при малому енергоспоживанні ЗВ і малих відстанях від ЗВ до станційної апаратури. Проте воно накладає жорсткі обмеження на опір відповідних сполучних проводів при значному енергоспоживанні, або при великій довжині лінії зв'язку;

– вища вартість апаратури в порівнянні з апаратурою комплексів, побудованих по радіальній безконцентраторній схемі;

– при порушенні зв'язку з концентратором втрачається інформація про стан цілої групи ЗВ, підключеною до нього.

Основна перевага комплексів з такою структурою – відносно низька вартість кабельних комунікацій і відносно короткий час їх монтажу.

3. **Шлейфовий (магістральний) без концентраторів** (рис. 4.11) **і з концентраторами** (рис. 5.11) .

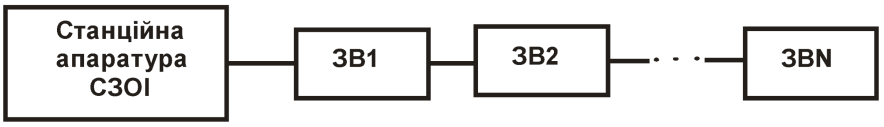


Рис. 4.11. Шлейфове (магістральне) без концентраторів з'єднання станційної апаратури із ЗВ

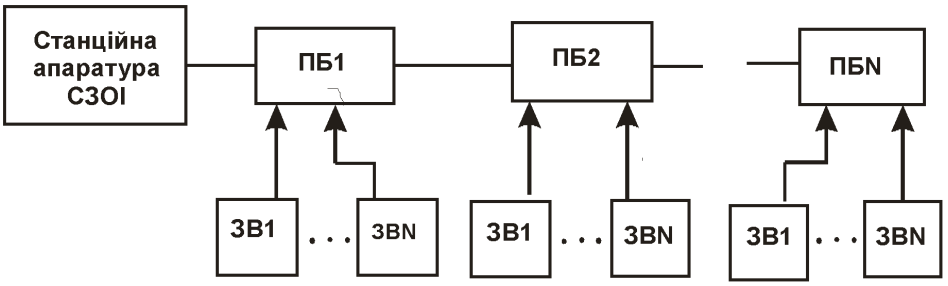


Рис. 5.11. Шлейфове (магістральне) з концентраторами з'єднання станційної апаратури з ПБ і ЗВ

Працездатність комплексів ТЗОС з шлейфовою структурою у великій мірі визначається справним станом ліній зв'язку (у таких системах структура кабельних комунікацій менш розвинена, чим в радіальних ТЗОС), оскільки виникнення короткого замикання в лінії повністю порушує роботу комплексу, а у разі обриву в робочому стані залишається тільки та частина комплексу, з якою підтримується зв'язок. Враховуючи дану обставину, останнім часом використовується резервування сполучних ліній і вузлів. При цьому подача електроживлення і зв'язок з пристроями комплексу здійснюється по двох незалежних шлейфах. Тому при виході з ладу одного з них працездатність комплексу підтримується за рахунок іншого. Проте у цьому випадку вартість кабельних ліній і електромонтажних робіт збільшується практично в два рази. Також на працездатність комплексу ТЗОС з шлейфовою структурою великий вплив робить організація електроживлення ЗВ, оскільки живлення повинне подаватися по обмеженій кількості проводів і повинен враховуватися сумарний струм споживання всіх ЗВ і концентраторів (при їх наявності).

Вибір структури побудови комплексу ТЗОС і СЗОІ

При виборі структури побудови комплексу ТЗОС і відповідної апаратури СЗОІ враховуються:

– категорія об’єкта, що оснащується комплексом;

– витрати на устаткування об'єкта;

– рівень підготовленості персоналу, якому належить працювати зі встановлюваним комплексом;

- час пошуку і усунення несправностей і надійність лінії зв'язку для комплексів відносно невеликої ємності (до 100... 150 каналів), як правило, використовується радіальна схема з'єднання периферійних пристроїв і Із із станційною апаратурою, а для комплексів більшої ємкості – шлейфовая з концентраторами інформації сигналізації. При цьому обробка інформації повинна здійснюватися переважно в концентраторах, об'єднаних із станційною частиною по шинній структурі (локальній обчислювальній мережі).

Як правило, найбільш переважною є змішана структура побудови комплексів ТЗОС:

– для найбільш важливих ділянок блокування - радіальна структура;

– для менш важливих приміщень – шлейфова/магістральна структура.

Відмітною особливістю побудови комплексів ТЗОС, що містять багато типів ЗВ, є способи адаптації СЗОІ до конкретних типів контрольованих нею ЗВ. При сполученні ЗВ і СЗОІ необхідно погоджувати наступні стикувальні параметри:

– напруга електроживлення ЗВ (якщо воно потрібне);

– час нестійкого стану вихідних контактів ЗВ після подачі на нього напруги електроживлення (час перехідних процесів ЗВ);

– тип дистанційної перевірки працездатності ЗВ.

З метою здійснення контролю за діями оператора по управлінню комплексом ТЗОС і для зручності оперативної роботи до складу комплексу вводиться апаратура зберігання (архівації) і документування інформації. Найбільше розповсюдження отримали накопичення інформації в спеціальному оперативному запам’ятовуючому пристрої (ОЗП) або на жорсткому диску ПЕОМ з можливістю виведення інформації на букво-цифровий індикатор (екран монітора ПЕОМ) і\ або її розпечатування.

Проте введення до складу комплексу пристроїв документування вимагає передбачати блоки автоматики, призначені для логічної обробки і підготовки сигналів управління блоками цифро-друкуючого пристрою. Останнім часом для документування і систематизації інформації сигналізації до складу СЗОІ вводиться блок стикування з ПЕОМ. Сигналізаційна інформація з ОЗП СЗОІ через цей блок передається в ПЕОМ, де її можна систематизувати:

– по вибраних каналах;

– по вибраному інтервалу часу;

– по видах повідомлень.

Класифікація чутливих елементів засобів виявлення.

В попередніх розділах ми розглянули можливі шляхи і способи проникнення порушника на об'єкт охорони. Очевидно, при своєму русі людина-порушник залишає безліч різноманітних слідів свого руху і/або перебування, які можуть бути зафіксовані (а при необхідності зміряні) різними приладами. Насправді, людина володіє цілком певними (кажучи в термінах математики, розташованими в цілком певних областях існування) параметрами, як то: геометричними розмірами, масою, температурою тіла, запахом, електричними, біомеханічними і біодинамічними характеристиками, швидкостями руху, частотою кроку і ін..

При своєму русі він порушує звукові і ультразвукові коливання в атмосфері і навколишніх предметах, а також сейсмічні коливання в ґрунті і будівельних конструкцій. В процесі виконання тих або інших дій чоловік надає безпосередню силову дію на предмети, що цікавлять його, а також динамічну дію на поля електромагнітної і акустичної енергії, викликаючи порушення їх структури в просторі.

Рух людини супроводжується генерацією наднизькочастотних електричних полів, що виникають як наслідок перенесення індукованого в результаті тертя взуття об поверхню підлоги і взаємного тертя елементів тіла і одягу електростатичного заряду.

Крім того відомо, що в процесі фізичної діяльності чоловік випромінює електромагнітні сигнали в дуже широкому спектрі частот, а органи дихання і кровообігу генерують акустичні коливання. Потові залози людини виділяють в навколишню атмосферу продукти, у складі яких налічуються десятки хімічних речовин, деякі з яких є характерними тільки для людини.

В процесі проникнення в приміщення порушник відкриває двері, вікна, кватирки; іноді вимушений вирізувати і/або вибивати стекла, або пробляти отвори і проломи в стелях, підлозі або стінах. Усередині приміщення він пересуває предмети, обстановку, намагається розкрити металеві шафи або сейфи, фотографувати документи або вироби. Для виконання цих дій він може мати з собою фотоапаратуру, різний інструмент, а також зброю або вибухові речовини. Вказані чинники володіють самостійними інформативними характеристиками, що виявляють присутність (або сліди перебування) людини в приміщенні, що охороняється, одночасно збільшуючи об'єм інформації про нього.

Так, зброя, що є у порушника, або інструмент володіють певними фізичними параметрами і їх наявність може привести до зміни напруженості магнітного поля, частоти опромінюючого сигналу НВЧ. Застосування механічного інструменту для відкриття дверей і металевих шаф, створення проломів і отворів в стінах і підлогах приміщень супроводиться збудженням характерних коливань (вібрацій) в твердих тілах і акустичних хвиль в повітряному середовищі приміщення.

При використанні газового пальника має місце теплове випромінювання полум'я, змінюється температура об'єкту на який діє порушник, з'являється специфічний запах горючої суміші, який, як і у разі застосування вибухових речовин, приводить до зміни хімічного складу повітря.

Таким чином, поява порушника в приміщенні, що охороняється, в загальному випадку може бути виявлене по великому числу фізикохімічних явищ. Це виявлення здійснюється за допомогою технічних засобів, в основу побудови яких покладені самі різні принципи реєстрації змін стану середовища.

Типові підходи до класифікації засобів виявлення і технічних засобів охорони. Як було сказано раніше, основу комплексу технічних засобів охорони складають: засоби виявлення (ЗВ); система збору, обробки, відображення і документування інформації (ППКОП); допоміжні засоби і пристрої (блоки резервного електроживлення, і ін..).

Взагалі засоби виявлення класифікують за наступними ознаками:

1. За способом приведення в дію (постановка на охорону, зняття з охорони з центрального пульта) ЗВ підрозділяють на автоматичні і автоматизовані

2. За призначенням автоматичні ЗВ підрозділяють:

– для закритих приміщень;

– для відкритих майданчиків і периметрів об'єктів.

3. По виду зони, контрольованої ЗВ, виділяються:

– лінійні;

– поверхневі;

– об'ємні (просторові).

4. За фізичним принципом дії розглядаються ЗВ наступних типів:

– механічні (на практиці виділяють електроконтактні, магнітоконтактні, ударноконтактні);

– ємнісні;

– акустичні;

– сейсмічні;

– оптико-електронні;

– радіохвильові;

– радіопроменеві (мікрохвильові);

– комбіновані.

5. По дальності дії ультразвукові, оптико-електронні і радіохвильові ЗВ для закритих приміщень розглядають:

– малої дальності дії – до 12 м;

- середньої дальності дії – понад 12 до 30 м;

- великої дальності дії – більше 30 м (окрім ультразвукових ЗВ).

6. По дальності дії оптико-електронні і радіохвильові ЗВ для відкритих майданчиків і периметрів об'єктів підрозділяють:

– малу дальність дії – до 50 м;

– середню дальність дії – понад 50 до 200 м;

– велику дальність дії – понад 200 м.

7. По конструктивному виконанню ультразвукові, оптико-електронні і радіохвильові ЗВ прийнято підрозділяти на:

– однопозиційні – один або більше передавачів (випромінювачів) і приймачів суміщені в одному блоці;

– двохпозиційні – передавач (випромінювач) і приймач виконані у вигляді окремих блоків;

– багатопозиційні – більше двох блоків (один передавач, два або більше приймачів; один приймач, два або більше передавачів; два або більше приймачів.

8. По принципу дії – активні (випромінюють радіо або інфрачервоне випромінення), пасивні (працюють тільки на прийом випромінювань).

Кожен з названих класів ЗВ представлений на ринку безліччю різних датчиків, розрахованих для застосування в конкретних умовах.

Апріорі ясно, що вибір на ринку конкретного ЗВ виникає з відповідності його тактико-технічних характеристик (ТТХ) умовам застосування. Це означає, що

ЗВ з даними (ТТХ) застосовують лише за певних умов, тобто ЗВ повинен бути встановлений в такому середовищі, характеристики якого (рельєф місцевості, електромагнітні поля, вібраційний фон, наявність або відсутність рослинності, параметри вологості, температури і так далі) в максимально можливій мірі задовольняють можливостям вибраного ЗВ, визначуваним його ТТХ.

ТТХ повинні задовольняти умовам експлуатації, тобто безлічі таких чинників, як:

– кліматичні (вітер, пил, пісок, осадки, туман, тиск, сонячна радіація, температура, грозові та сезонні явища і ін..);

– біологічні (рослини, тварини, комахи, птахи);

– геологічні (рельєф місцевості, тип і хімічний склад ґрунту, водний простір, сейсмообстановка);

– механічні (вібрації, удари, прискорення);

– електромагнітні поля і випромінювання;

– акустичні коливання;

– рівень радіоактивності;

– рівень освітленості і ін..;

– режими роботи апаратури (інтенсивність, тимчасові параметри);

- умови електроживлення;

– рівень кваліфікації обслуговуючого персоналу і ін..;

– вартісні (розробки, виготовлення, монтажу і наладки, експлуатації) і багато що інше.

Виходячи з тих або інших чинників, обумовлюючих застосування ЗВ розглядають (закладають при розробці) наступні основні ТТХ:

– характеристики зони виявлення;

– вірогідність виявлення з вказана моделлю порушника;

– напрацювання на помилкове спрацьовування;

– чутливість ЗВ;

– параметри вхідних і вихідних сигналів;

– верхню і нижню межі швидкості переміщення порушника (об'єкту виявлення);

– час готовності ЗВ після включення напруги живлення;

– час відновлення чергового режиму після закінчення сигналу спрацьовування;

– показники надійності і ряд інших.

Створення рубежів охорони

У основі системи захисту об'єкту лежить принцип створення послідовних рубежів, в яких погрози мають бути своєчасно виявлені, а їх розповсюдженню повинні перешкоджати надійні перешкоди. Такі рубежі (або зони безпеки) повинні

розташовуватися послідовно - від огорожі навколо території об'єкту до головного, особливо важливого приміщення, такого як сховище цінностей і інформації, вибухонебезпечних матеріалів, зброї і інші. (рис. 6.11).

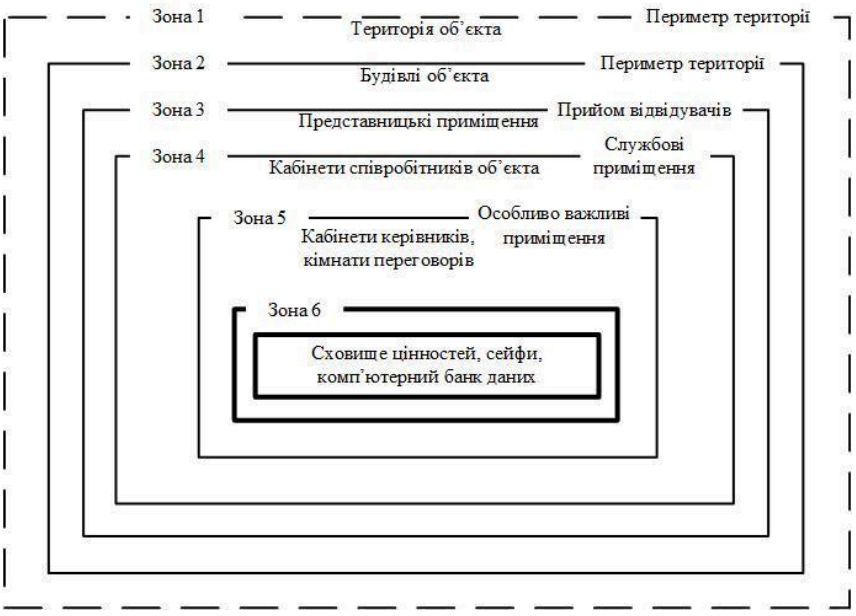


Рис. 6.11 Принцип рубіжності

Чим складніше і надійніше захист кожної зони безпеки, тим більше часу буде потрібно зловмисникові на її подолання і тим більше вірогідність того, що розташовані в зонах засоби виявлення погроз подадуть сигнал тривоги, а отже, у співробітників охорони залишиться більше часу для визначення причин тривоги і організації ефективного захисту і ліквідації загрози.

Основу системи захисту складають технічні засоби виявлення, відбиття і ліквідації наслідків. Охоронна сигналізація і охоронне телебачення, наприклад, відносяться до засобів виявлення погроз. Огорожі навколо території об'єкту – це засоби відбиття несанкціонованого проникнення на територію; посилені двері, стіни і стелі сейфової кімнати захищають від стихійних лих і аварій, а крім того, до певної міри служать захистом і від підслуховування і вторгнення.

Обов'язковою на ОІД є пожежна сигналізація, яка є більш розгалуженою, ніж інші види і зазвичай охоплює майже всі приміщення будівлі.

Пожежна і охоронна сигналізації по своїй побудові і вживаній апаратурі мають багато загального - канали зв'язку, прийом і обробка інформації, подача тривожних сигналів і ін. З цієї причини в сучасних системах захисту ці типи засобів сигналізації іноді об'єднуються в єдину систему охоронно-пожежної (ОП) сигналізації.

Контроль і управління ОП сигналізацією здійснюються з центрального поста охорони, на якому встановлюється відповідна стаціонарна апаратура. Склад і характеристики цієї апаратури залежать від важливості об'єкту, складності і розгалуженості системи сигналізації.

Критерієм ефективності і досконалості апаратури ОП сигналізації є зведення до мінімуму числа помилок і помилкових спрацьовувань. Наприклад, для особливо важливих об'єктів бажано, щоб вірогідність виявлення ЗВ була близька до 0.98; **напрацювання на помилкове спрацьовування** – до 2500 годин (для пасивних) і до 3500 годин (для активних).

Каналами зв'язку в системі ОП сигналізації можуть бути спеціально прокладені дротяні лінії, телефонні лінії об'єкту, телеграфні лінії і радіоканали. Енергопостачання системи охоронної сигналізації обов'язково резервується.

Для вирішення завдань оснащення периметра якого-небудь об'єкту технічними засобами охоронної сигналізації заздалегідь слід знати відповіді на питання:

1. Яка протяжність периметра.
2. Вид наявної загорожі (її параметри, матеріал).
3. Кількість наявних воріт, хвірток, їх розміри, матеріал.
4. Найближча відстань від рубежу, що охороняється, до приміщення охорони, до найближчої до периметра будівлі.
5. Наявність застав (труби, кабелі).
6. Розмір зони відчуження усередині периметра, наявність кущів і/або дерев в зоні відчуження.
7. Необхідність скритності засобів виявлення (або відсутність такої необхідності).
8. Необхідна точність виявлення порушника на контурі периметра (3 м, 10 м).
9. Необхідна кількість рубежів охорони (периметр, підходи до будівель), режими охорони: цілодобовий, в міру необхідності, N-часової.
10. Необхідність блокування: перелазу через огорожу, руйнування огорожі, підкопу під огорожу.
11. Наявність в даний час (тобто на момент попереднього аналізу об'єкту охорони) яких-небудь засобів виявлення, станційної апаратури в приміщенні служби охорони – системи збору і обробки інформації.
12. Які витрати може дозволити собі Замовник на вирішення завдань оснащення об'єкту (зокрема периметра) технічними засобами охоронної сигналізації і системою збору і обробки інформації.
13. У які терміни потрібне проведення такої роботи.
14. Необхідний план об'єкту (ескіз), параметри по висоті будівель.

Приведений перелік питань – мінімально необхідний з позицій попереднього аналізу, але далеко не повний з позицій системного підходу.

5. Об'єктивна необхідність побудови високоефективних систем безпеки об'єктів в умовах різкого загострення криміногенної обстановки привела до розробки наукоємних інтегрованих систем безпеки (ІСБ). ІСБ по суті націлена на реалізацію ідей системної концепції забезпечення комплексної безпеки об'єкту з паралельним (інтегрованим із завданнями забезпечення безпеки) вирішенням завдань автоматизації управління широкою гаммою систем життєзабезпечення об'єкту, як то: енергопостачанням, вентиляцією, опалюванням, водопостачанням, ліфтовим устаткуванням, кондиціонуванням і ін..

Серед функцій, обов'язкових для виконання в контурі ІСБ, слід вважати:

– контроль за великою кількістю приміщень із створенням декількох рубежів захисту (ІСБ розробляється тільки для великих об'єктів і будівель);

– ієрархічний доступ співробітників і відвідувачів в приміщення з чітким розмежуванням повноважень по праву доступу в приміщення за часом доби і по днях тижня;

– ідентифікацію і аутентифікацію особи людини, що перетинає рубіж контролю;

– попередження просочування (витоку) інформації;

– попередження попадання на об'єкт заборонених матеріалів і устаткування;

– накопичення документальних матеріалів для використання їх при розгляді і аналізі подій;

– оперативний (автоматизований) інструктаж працівників охорони про порядок дій в різних штатних і нештатних ситуаціях шляхом автоматичного виводу на екран монітора інструкцій в потрібний момент;

– забезпечення повної інтеграції систем відеоспостереження, сигналізації, моніторингу доступу, сповіщення, зв'язку між персоналом СБ (О), персоналом служби пожежної безпеки, персоналом служб життєзабезпечення об'єкту і ін..;

– забезпечення взаємодії постів охорони і органів правопорядку при несенні охорони і у разі відповідних подій;

– стеження за точним виконанням персоналом охорони своїх службових обов'язків.

Виходячи з викладеного раніше ясно, що **складовими частинами ІСБ** (укрупнено) мають бути:

– мережі ЗВ, що забезпечують отримання максимально повної інформації зі всього простору, що знаходиться у полі зору служби безпеки і що дозволяє відтворювати на центральному пульті спостереження і управління всесторонню

об'єктивну картину стану приміщень, всієї території об'єкту і працездатності всієї апаратури і устаткування, включеного в контур ІСБ;

– виконавчі пристрої, здатні при необхідності діяти автоматично або по команді оператора;

- пункти контроля і управління системою відображення інформації, через яких операторів можно стежити за роботою всієї системи в межах своїх повноважень;

– комунікації, по яких здійснюється обмін інформацією між елементами системи і операторами.

При цьому важлива наявність можливості оперативного програмування (перепрограмування) функцій ІСБ. Це дозволяє ефективно протидіяти таким хитруванням зловмисника як:

– переривання каналів передачі тривоги;

– нейтралізація частини системи людьми, що мають доступ до її елементів;

– проникнення з сигналом тривоги і знищення потім інформації про подію (змова);

– використання відхилень від наказаного порядку несення служби персоналом охорони;

– створення нештатних ситуацій в роботі системи і ряду інших.

Контрольні запитання

1. Що складає основу комплексу технічних засобів охорони
2. Які існують засоби виявлення (ЗВ) за призначенням
3. Які існують засоби виявлення (ЗВ) по виду контрольованої зони
4. Які основні ТТХ розглядають при розробці нових ЗВ
5. Які основні компоненти: виділяються в структурі технічних засобів охорони
6. Що являється критерієм ефективності і досконалості апаратури охоронно-пожежної сигналізації

Лекція № 12

Тема лекції: Сповіщувачі технічних систем охорони

ПЛАН ЛЕКЦІЇ

1. Магнітоконтактний сповіщувач
2. Пасивний інфрачервоний сповіщувач
3. Радіохвильовий та радіо променевий засіб виявлення

1. Магнітоконтактний сповіщувач

Магнітоконтактні сповіщувачі – це найбільш простий, дешевий і, в той же час, досить надійний вид сповіщувачів, що використовуються в системах охоронної сигналізації. Згадані переваги разом з малими габаритами і простотою встановлення призвели до широкого використання МКС. Основою МКС є контакти, керовані магнітним полем. Основне призначення таких сповіщувачів – фіксація моменту відкривання дверей, вікон або аналогічних конструктивних елементів, а також зсуву предметів.

Магнітоконтактний сповіщувач містить у собі два основних елементи. Перший елемент – це геркон (рис. 1.12), що складається з герметичної колби 1, у якій знаходяться пластини 2 з контактами, які мають малий опір. До пластин під'єднані провідники 3, що забезпечують підключення МКС. Для виготовлення пластин використовуються метали або сплави (наприклад, сталь), які забезпечують ефективне керування пластинами магнітним полем. Один з варіантів побудови геркона – використання протилежно намагнічених пластин. Під впливом магнітного поля від розташованого поруч магніту 4 відбувається замикання чи розмикання контактів. У більшості випадків під впливом магнітного поля контакти нормально замкнуті. При знятті магнітного поля під дією пружних сил відбувається розмикання контактів.

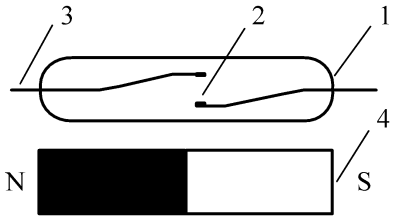


Рис. 1.12. Основні елементи магнітоконтактного сповіщувача

Контакти звичайно покриваються спеціальним сплавом, наприклад, родієвим, що забезпечує малий опір і тривалий термін служби.

Основні параметри магнітоконтактних сповіщувачів

*Робочий зазор*Робочий зазор визначає мінімальну відстань, на якій відбувається замикання контактів геркона (рис. 3, *а*). Наприклад, на рис. 4 показані криві, що визначають робочий зазор МКС типу MPS-45WG і MPS-20WG компанії С&К. Видно, що величина робочого зазору змінюється в залежності від взаємного розташування геркона і магніта.

При зсуві магніта в бік величина зазору зменшується (рис 2.12, *б*).

Деякі МКС мають збільшений робочий зазор, що дає можливість встановлювати їх на конструкції, які мають люфти та збільшені зазори між елементами конструкції, що блокуються.

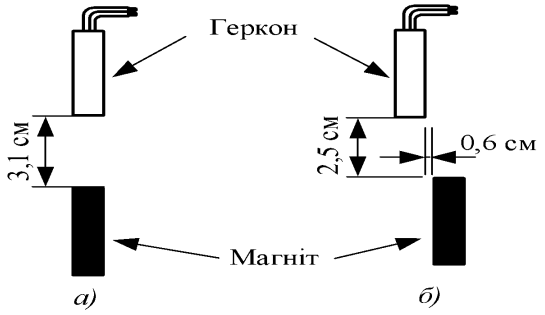


Рис. 2.12. Робочий зазор МКС

Зазор відпускання

Визначає величину зазору, при якому відбувається розмикання контактів геркона.

За способом монтажу можна виділити дві основні групи МКС: призначені для встановлення на поверхні конструкції (дверях, рамі і т.п.) (рис. 3.12 *а*) і для прихованого встановлення (всередині елементу, що блокується) (рис. 3.12 *б*).

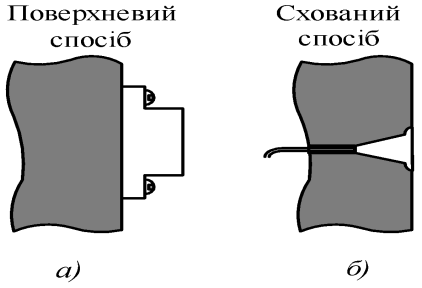


Рис. 3.12. Способи встановлення МКС

Захист від блокування

Один з основних принципів побудови систем безпеки полягає в тому, що система повинна бути стійкою до можливих спроб втручання в неї з метою блокування, виводу її з ладу. Варіант такого способу блокування МКС – впливати сильним магнітним полем: наприклад, піднести сильний магніт до зовнішньої частини дверей, за якою розташований МКС. Найпростіший і в той же час

надійний спосіб протидіяти цьому – заглиблений, схований монтаж. При цьому зловмиснику невідоме місце положення МКС.

З конструктивних засобів можна відзначити екранування датчика від блокування. Це досягається використанням спеціального екрана, що захищає МКС від можливого впливу.

Для контролю цілісності шлейфа, у який включений МКС, використовують додаткове нормально замкнуте коло контролю обриву шлейфа. Так, сповіщувачі серії EMPS компанії C&K мають додаткову пару виводів такого нормально замкнутого кола.

2. Пасивний інфрачервоний сповіщувач

Рис. 4.12 Пасивний ІЧ сповіщувач

Пасивні інфрачервоні сповіщувачі руху чи сповіщувачі, відомі також за назвою оптико-електронні, є пристроями, які найчастіше використовуються для виявлення руху в контрольованій зоні. Це обумовлено досить високою ефективністю виявлення руху та низькою вартістю цих пристроїв. Ефективність виявлення проникнення в зону, що охороняється, визначається насамперед тим, що пасивні інфрачервоні сповіщувачі дозволяють контролювати весь об’єм приміщення. Тим самим вирішується задача реєстрації вторгнення не тільки через найбільш уразливі місця, але практично при будь-якому шляху проникнення: через вікна, двері, проломи підлоги, стелі, стіни. Очевидно, що це значно ефективніше, ніж блокування тільки периметра об'єкта (вікон, дверей і тому подібних конструктивних елементів об'єкта). Це не виключає блокування першого рубежу охорони, що дозволяє в більшості випадків отримати ранній сигнал тривоги і мати більше часу на відповідну реакцію.

Контроль об’єму всього приміщення – це не єдина задача, яку розв'язують ПІЧ-сповіщувачі. Використовуючи змінні лінзи (оптичні системи), можна ефективно контролювати вузьку смугу (наприклад, коридор) чи створити

горизонтальну фіранку (наприклад, для контролю приміщень, у яких знаходяться домашні тварини) чи формувати вертикальну зону виявлення уздовж стін з вікнами чи дверима.

Основні елементи, які повинні входити до складу ПІЧ-сповіщувача для того, щоб він реєстрував зміну ІЧ-випромінювання, показані на (рис. 5.12).

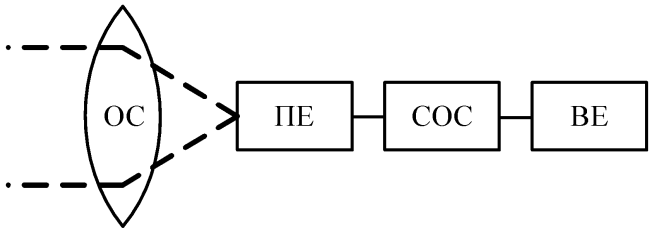


Рис. 5.12 Основні елементи ПІЧ-випромінювання

По-перше, це чутливий елемент - піроелемент (ПЕ), що перетворює ІЧ-випромінювання в електричний сигнал. По-друге, оптична система (ОС), яка фокусує на піроелементі ІЧ-випромінювання з визначеної частини об'єкта. По-третє, це схема обробки сигналу (СОС) від чутливого елементу. І, нарешті, виконавчий елемент (ВЕ), що забезпечує підключення сповіщувача до шлейфу сигналізації, тобто сполучення сповіщувача з іншими елементами системи сигналізації.

Основні типи діаграм спрямованості ПІЧ сповіщувачів.

Приклад типової реальної діаграми спрямованості приведений на (рис. 6.12), на (рис. 6.12 а) зображений вид зверху, а на (рис. 6.12 б) – вид збоку. Діаграма спрямованості такого типу називається “широкий кут” чи “об’ємна”.

Це одна з найбільш розповсюджених діаграм спрямованості, що дозволяє контролювати весь об’єм приміщення. Діаграми такого типу можуть відрізнятися декількома основними особливостями. По-перше, наявністю чи відсутністю зони контролю безпосередньо знизу під сповіщувачем (див. рис. 5.13 а) По-друге, співвідношенням чутливості при русі в центрі діаграми і по її краях (рис. 5.13 б).

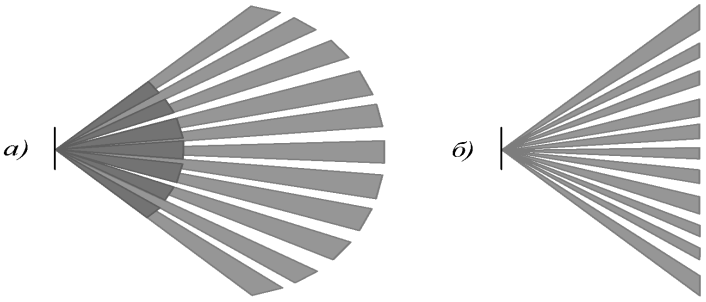


Рис. 6.12 Об'ємна діаграма спрямованості

Зауважимо, що рівномірна чутливість по всій діаграмі спрямованості дуже важливий фактор, яким володіють деякі пристрої. Тільки при рівномірній чутливості по всій зоні виявлення можна досягти високої імовірності виявлення при низькому рівні помилкових тривог. Нерівномірність чутливості приводить до того, що той самий порушник, рухаючись в різних ділянках зони, буде викликати появу сигналів, що значно відрізняються по амплітуді. При такому самому рівні шумів це означає різне співвідношення сигнал/шум для різних ділянок зони. Пов'язано це насамперед з тим, що коефіцієнт підсилення тракту обробки сигналу повинен вибиратися виходячи з вимоги забезпечення необхідної імовірності правильного виявлення в гірших умовах, у частині діаграми з найменшою чутливістю. Однак при цьому в ділянках з більшою чутливістю зростає не тільки імовірність правильного виявлення, але й імовірність помилкових тривог.

Інший досить розповсюджений тип діаграм забезпечує контроль вузької смуги, наприклад, коридору. Така діаграма має на виді зверху два-три промені. Кількість променів на виді збоку (у вертикальній площині) може трохи відрізнятися. Справа в тому, що існують дві схожі діаграми – «коридорна» чи «лінійна» (рис. 7.12) і «вертикальна» чи «бар'єр вертикальна фіранка» (рис. 8.12).

Якщо перша орієнтована в більшій мірі на однакову надійність виявлення при русі як уздовж, так і поперек діаграми, то друга насамперед забезпечує реєстрацію руху поперек, мінімізуючи "вікна" у діаграмі. Помітимо одну важливу особливість. При використанні таких діаграм повинна установлюватися висока чутливість сповіщувача.

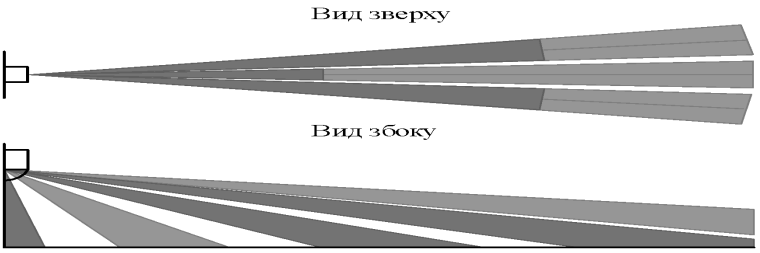


Рис. 7.12 Коридорна діаграма спрямованості

Третій тип діаграми спрямованості використовується в сповіщувачах, що контролюють приміщення з домашніми тваринами (наприклад, собаками). Такі діаграми, типу “горизонтальна штора”, мають один горизонтальний сектор променів.

Спровіщувач встановлюється на висоті близько 1,2 м Рух тварини під діаграмою не викликає спрацьовування, у той час як рух людини, що перетинає її, реєструється. Ясно, що в цьому випадку надійність виявлення сповіщувачем

порушника буде в цілому гірше. Більш того, по висоті установки сповіщувача легко зрозуміти, яка діаграма спрямованості. Тому порушник може використовувати для проникнення незахищену нижню зону.

Ще одна особливість пов'язана з необхідністю виключити зону контролю під сповіщувачем.

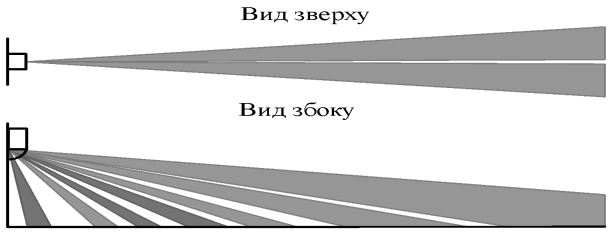


Рис. 8.12 Діаграма спрямованості “вертикальна штора”

3. Р**адіопроменеві системи**

Двопозиційні радіопроменеві системи (охорона периметра) (рис. 9.12).

Принцип дії.

Інженерні засоби охорони периметра різноманітні та відрізняються один від одного не лише технічно-експлуатаційними характеристиками, а й призначенням. Ефективними технічними елементами вважатимуться радіопроменеві засоби виявлення.

Принцип дії таких систем є простим. Радіопроменева система складається з передавача та приймача, які утворюють невидиму зону виявлення, «позначаючи» межі. Розміри зони виявлення можуть бути різними: перш за все, вона залежить від того, наскільки далеко один від одного знаходяться приймач і передавач. Важливо відзначити, що така система демонструє свою високу ефективність лише на певних територіях: ландшафт має бути рівним, без чагарників, дерев тощо.

Особливості радіопроменевих засобів виявлення.

Радіопроменеві засоби виявлення мають недолік, який виявляється у виникненні «мертвих зон». У безпосередній близькості від передавача та приймача чутливість системи дещо знижена, що може позначитися на ефективності охорони. Тим не менш, цей недолік легко нівелювати - достатньо зробити установку з перекриттям кілька метрів. Важливо враховувати і той факт, що радіопроменеве засіб виявлення призначене для запобігання проникненню порушників, які пересуваються стоячи або зігнувшись. Тому проектуючи комплексну охоронну систему, цю особливість необхідно усунути шляхом встановлення інших елементів охорони.

Радіопроменевий засіб має досить широку зону чутливості. Це, своєю чергою, обмежує спектр застосування. Наприклад, не рекомендується встановлювати таку систему на об'єктах, де до зони охорони можуть випадково потрапити інші суб'єкти: транспорт, люди. Якщо об'єкт потребує встановлення

саме радіопроменевої системи, підвищення її ефективності рекомендується облаштувати зону відчуження (розмістити додаткове огородження).

Установка блоків радіопроменевих систем повинна здійснюватися на стінах споруд, на огорожі або на ґрунті. Безпосередньо перед встановленням системи необхідно підготувати територію – прибрати ландшафтні елементи та видалити рослинність.

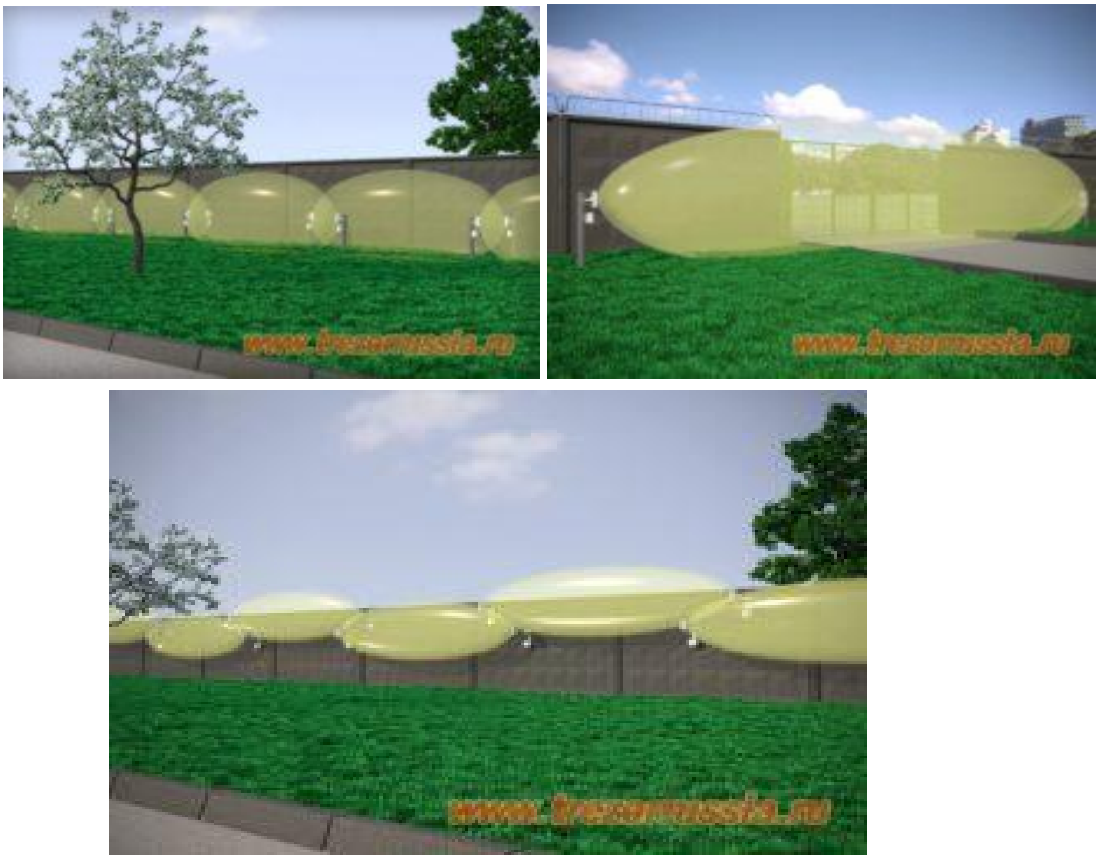


Рис. 9.12 Двопозиціна радіопроменева система

Однопозиційні радіопроменеві системи (охорона внутрі приміщень та для периметру) (рис. 10.12)

Однопозиційний об'ємно-чутливий НВЧ датчик. Працюють на доплерівському принципі (допплерівський зсув частот). Ця система розроблена для виявлення предметів, що рухаються, і призначений для роботи на зовнішньому периметрі або всередині приміщень.

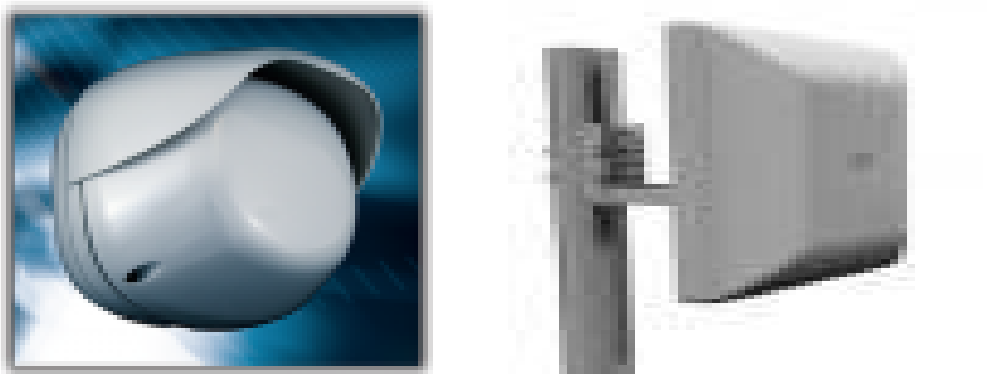


Рис. 10.12 Однопозиційна раліопроменева система

Радіохвильові системи на ефекті хвилі, що витікає (рис. 11.12, 12.12).

Система відноситься до радіохвильових сповіщувачів. Термін "лінія витікаючої хвилі" (ЛВХ) пов'язаний з особливостями конструкції чутливого елемента (ЧЕ).

Він являє собою перфорований кабель, в якому зовнішній провідник не забезпечує повного екранування центрального провідника, певна частина енергії високочастотного сигналу, що передається, випромінюється через отвори у зовнішнє середовище, частина енергії проникає в приймальний кабель такої ж конструкції. У передавальному кабелі встановлюється режим, близький до режиму хвилі, що біжить, а в приймальному кабелі наводиться опорний сигнал.

Принцип дії ЛВХ ґрунтується на реєстрації обурення електромагнітного поля при перетині порушником об'ємної зони виявлення. Відбита від порушника електромагнітна хвиля приймається приймальним кабелем, унаслідок чого відбувається низькочастотна модуляція амплітуди та фази опорного сигналу.

Кабелі (ЧЕ) можуть встановлюватися на огорожу та закопуватись у ґрунт.

Ширина зони виявлення залежить від чутливості кабелю (виду його конструкції), частоти сигналу, відстані між кабелями, параметрів поверхні, що підстилає, способу обробки сигналу. Висота зони виявлення може досягати 1,5 м

Перевагами цих сповіщувачів є:

- при розміщенні кабелів на огорожі – можливість контролю проникнення через «жорсткі» огорожі без додаткового обладнання їх металевими козирками та контроль руйнування «жорстких» конструкцій (залізобетон, цегла, камінь, дерево);
- при встановленні кабелів у ґрунт – можливість створення невидимих надійних рубежів охорони;
- стійкість до впливу рослинності та нечутливість до дрібних тварин та птахів. У сповіщувачі використовується діапазон робочих частот у межах від 40 до 80 МГц, який дозволяє виявити людину та пропустити дрібних та середніх тварин;
- завадостійкість до електромагнітних перешкод;
- стійкість до акустичних та сейсмічних перешкод.

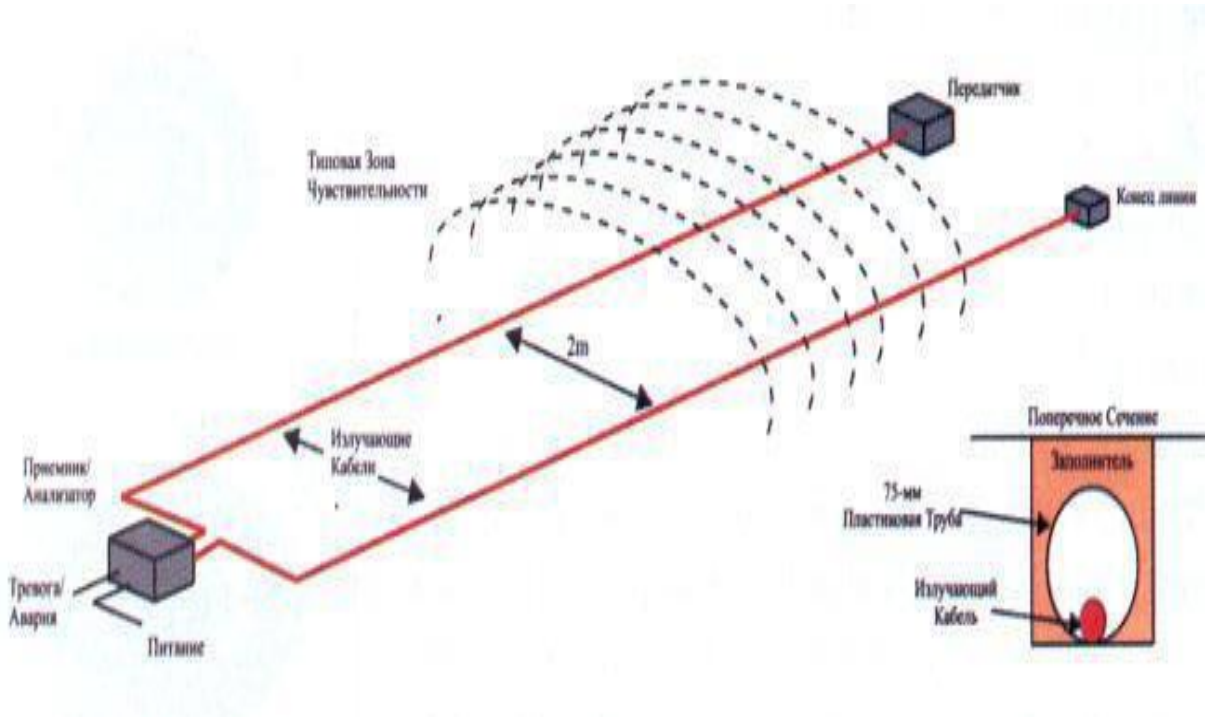
Недоліки:

1 Великі масогабаритні характеристики

2 Необхідність захисту оболонки.

Будь-яке пошкодження діелектричної оболонки може призвести до виходу з ладу дорогого кабелю. Тому найкращим способом є укладання і закладання кабелю в канали, виконані в стіні, що різко збільшує вартість монтажних робіт.

3 Нерівномірність чутливості за довжиною кабелю.



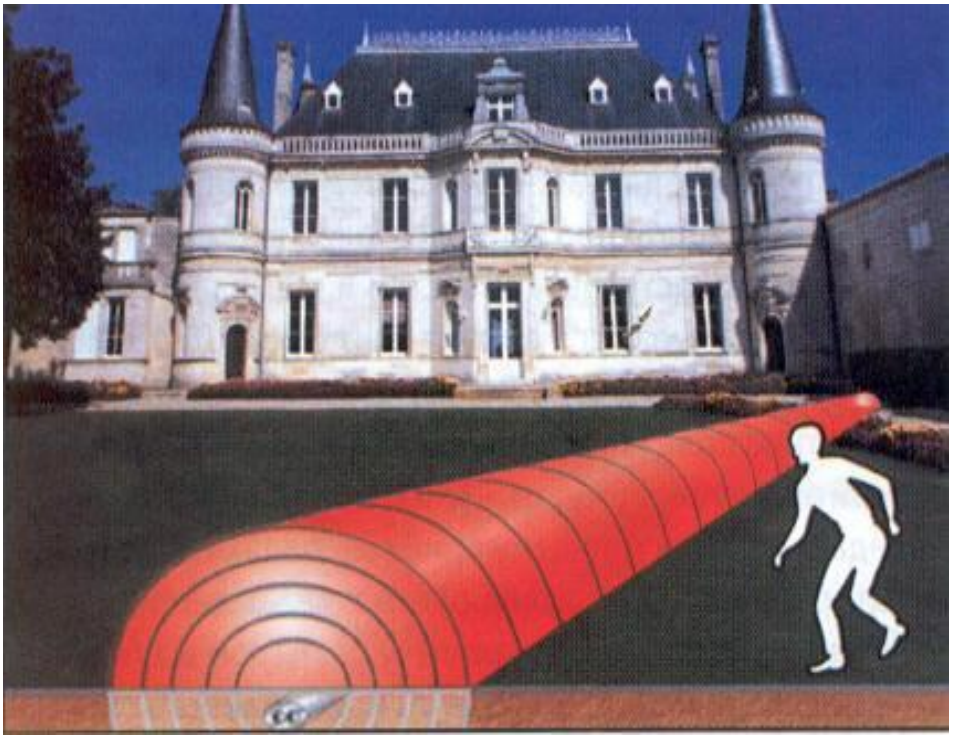
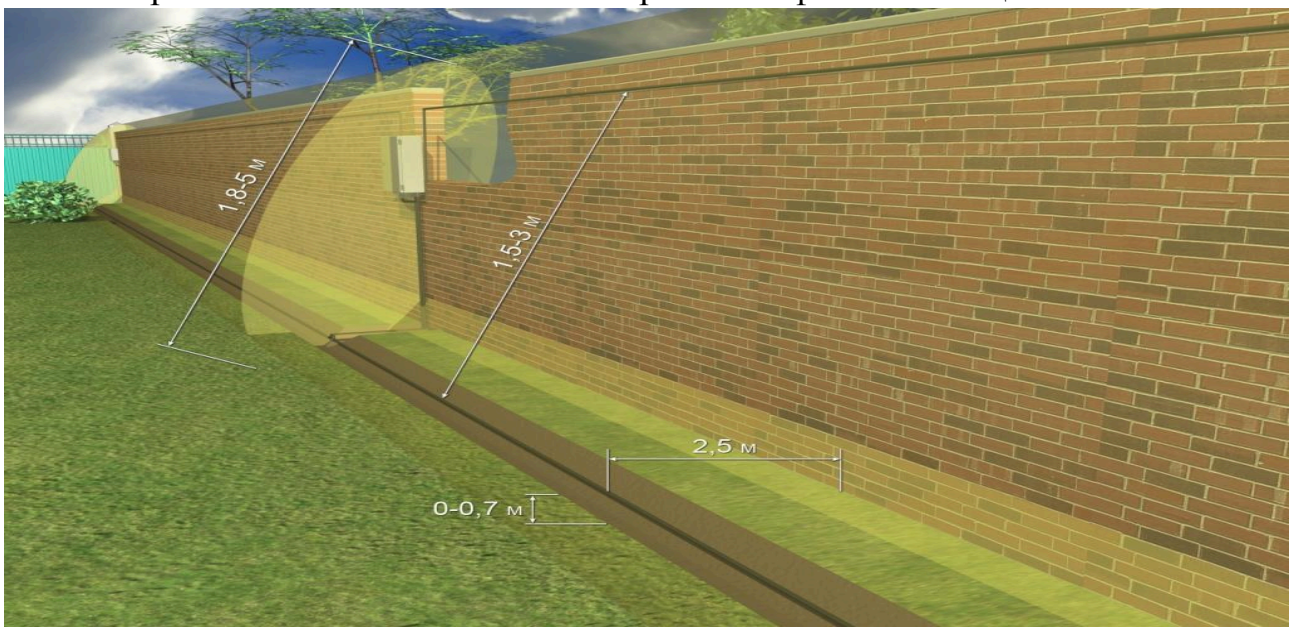


Рис. 11.12 Прихована технічна система охорони на ефекті хвилі що витікає



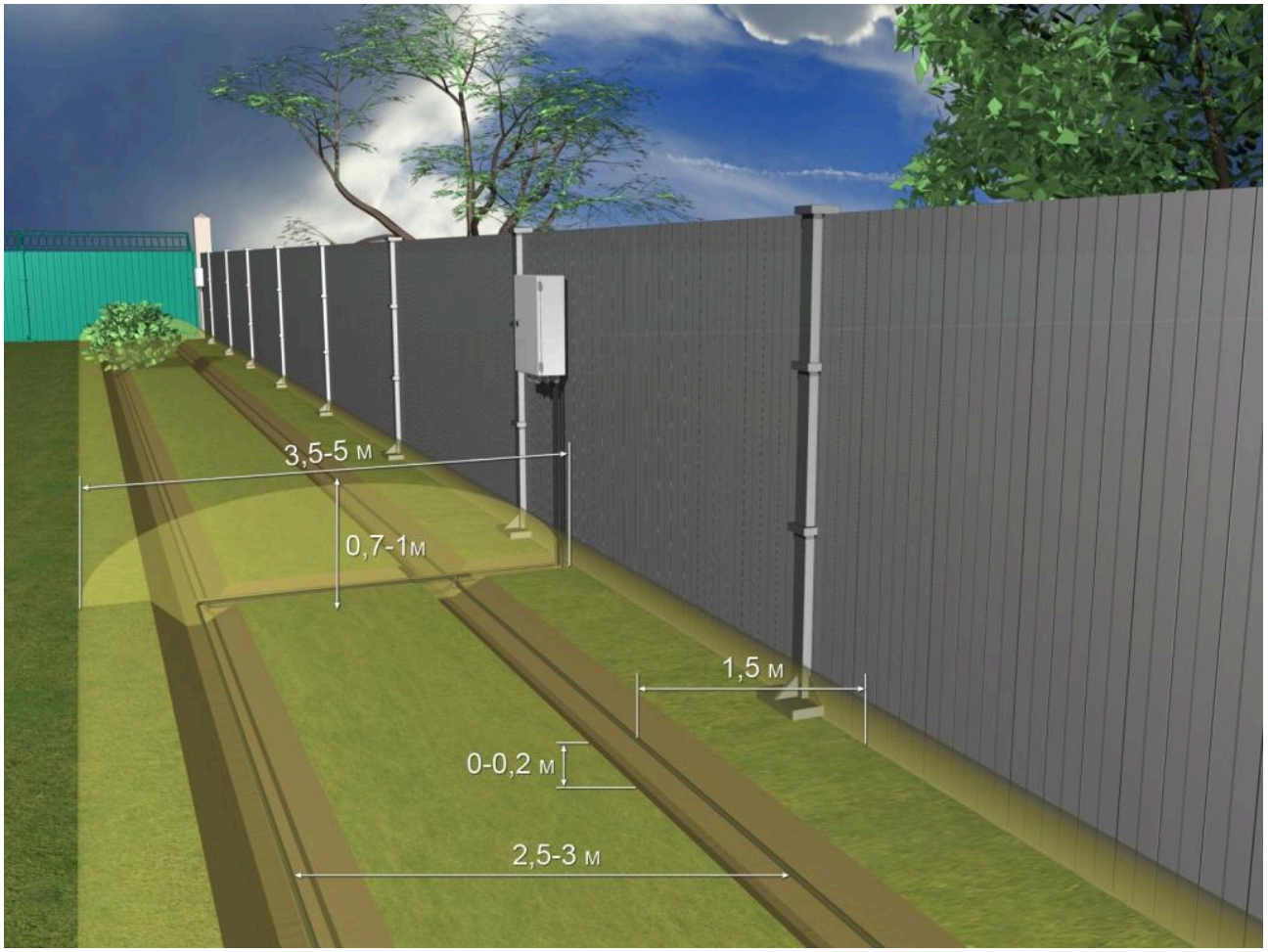


Рис. 12.12 Охорона периметру ОІД системою на ефекті хвилі що витікає

Контрольні запитання.

1. Доповісти призначення та принцип дії радіопроменевої охоронної системи.
2. Доповісти призначення та принцип дії радіохвильової охоронної системи.
3. Яке призначення магнітоконтактних сповіщувачів?
4. Як конструктивно влаштований МКС?
5. Які основні параметри МКС Ви знаєте?
6. Від чого залежать робочий зазор та зазор відпускання МКС?
7. Визначення пасивного ІЧ сповіщувача та для чого він призначений?
8. Принцип дії пасивного ІЧ сповіщувача та його склад
9. Визначення зони виявлення пасивного ІЧ сповіщувача, чим вона визначається, на що впливає?
10. Охарактеризувати коридорну та вертикальна штора діаграми спрямованості пасивного ІЧ сповіщувача

Лекція № 13

Тема лекції: Системи контролю та управління доступом на ОІД

ПЛАН ЛЕКЦІЇ

1.

1. Призначення СКУД. Класифікація СКУД.
2. Ідентифікатор користувача
3. Контролери СКУД
4. Виконавчі пристрої СКУД

1. Призначення СКУД. Класифікація СКУД

Захист будь-якого об'єкта включає кілька рубежів, число яких залежить від рівня режимності об'єкта. При цьому у всіх випадках важливим рубежем буде система управління контролю доступом (СКУД) на об'єкт.

Під СКУД розуміється сукупність програмно-технічних і організаційно-методичних засобів, за допомогою яких вирішується завдання контролю і управління доступом до приміщення підприємства і окремих приміщень, а також оперативний контроль за пересуванням персоналу і часу його знаходження на території підприємства.

Такі системи можуть здійснювати контроль переміщення людей і транспорту по території охоронюваного об’єкта, забезпечувати безпеку персоналу і відвідувачів, а також збереженість матеріальних і інформаційних ресурсів підприємства. Системи контролю й керування доступом використовуються на промислових підприємствах, в офісах, магазинах, на автостоянках і автосервісах, в житлових приміщеннях.

Інтерес до систем контролю і управління доступом зростає ще й тому, що наявність такої системи важливо для ефективної роботи підприємства. Контроль не тільки істотно підвищує рівень безпеки, але й дозволяє оперативно реагувати на поведінку персоналу і відвідувачів. Також важливим завданням для багатьох підприємств є необхідність контролювати графік і вести облік робочого часу. Особлива увага приділяється системам, що дозволяє вибудовувати необхідні конфігурації з стан дротяних блоків, враховуючи всі особливості підприємства.

Існуючі керівні документи у цілому поділяють СКУД за наступними ознаками:

- за способом управління;
- число контрольованих точок доступу;
- функціональні характеристики;
- виду об'єктів контролю;
- рівню захищеності системи від несанкціонованого доступу.

Також відповідно до керівних документів всі СКУД діляться на чотири класи.

СКУД 1-го класу - малофункціональні системи малої ємності, що працюють в автономному режимі і здійснюють допуск всіх осіб, які мають відповідний ідентифікатор. У такій системі використовується ручне або автоматичне керування виконавчими пристроями, а також світлова або/і звукова сигналізація.

СКУД 2-го класу - монофункціональні системи. Вони можуть бути однорівневими і багаторівневими і забезпечують роботу як в автономному, так і в мережевому режимах. Допуск осіб (груп осіб) може здійснюватися за датою, тимчасових інтервалах. Система здатна забезпечити автоматичну реєстрацію подій і автоматичне управління виконавчими пристроями.

СКУД 3-го і 4-го класів, як правило, є мережевими. У них використовуються більш складні ідентифікатори та різні рівні мережевої взаємодії (клієнт-сервер, інтерфейси зчитувачів карт Віганда або магнітних карт, спеціалізовані інтерфейси та ін.)

Основні можливості системи контролю й керування доступом.

Основні можливості, які надає установка СКУД на об'єкті, що охороняється:

Контроль і керування доступом -це основна функція системи. Як уже було замічено раніше, за допомогою даної функції виробляється поділ прав доступу співробітників у певні приміщення, а також відмова в доступі небажаним особам. Крім того, можливо дистанційне керування пристроями, що блокують (замки, турнікети та ін.). СКУД дозволяє заборонити прохід для співробітників у святкові й вихідні дні, а також після закінчення робочого дня.

Збір і надання статистики. СКУД збирає інформацію про осіб, які пройшли через певні крапки контролю доступу. По кожному співробітнику можливе одержання наступної інформації: час входу й виходу, спроби доступу в заборонені для нього приміщення й зони, а також спроби проходу в недозволений час. Також можливо відстежити переміщення співробітника по території із вказівкою місця й часу. Таким чином, всі виявлені порушення трудової дисципліни можуть бути занесені в особисту справу співробітника, а керівництво порушника сповіщене в робочому порядку. Крім того, випливаючи інформації про останню крапку проходу, СКУД дозволяє визначитимісцезнаходження співробітника в будь-який момент часу.

Доступ співробітника тільки по особистому ідентифікаторі. При проході за допомогою ідентифікаційної карти на екрані монітора в пункті охорони може відображатися вся інформація зі співробітника і його фотографія, що виключає можливість проходу по чужому ідентифікаторі. Також на рівні правил реакції СКУД можна забезпечити захист від передачі ідентифікатора іншій особі й блокувати повторний вхід на територію об'єкта по тій же самій карті доступу.

Автономність роботи системи. СКУД оснащується системою безперебійного живлення, що дозволяє не переривати роботу у випадку відключення електрики в будинку. Також система контролю доступом завдяки функціоналові контролера має можливість продовжувати роботу, наприклад, при виході керуючого комп'ютера з ладу.

Охорона об'єкта в реальному часі. СКУД дає можливість ставити певні приміщення на охорону й знімати їх з охорони. Крім того, у реальному часі можна одержувати відомості про всілякі позаштатні й тривожні ситуації через спеціальні оповіщення відповідальних осіб. Крім цього в базі дані системи реєструються всі тривожні події й події, що дає можливість доступу до цієї інформації надалі при необхідності. Завдяки наявним у СКУД засобам, співробітник охорони зі свого робочого місця за допомогою комп'ютера має можливість не тільки управляти дверима й турнікетами, але й подавати сигнали тривоги. У комп'ютер СКУД у співробітника охорони можуть бути занесені поповерхові плани будинку зі схемою розташування контролерів обмеження доступу.

Віддалене керування системою через інтернет або з мобільного телефону. Якщо при установці підключити СКУД до мережі Інтернет, то в адміністрації з'являється можливість вести віддалене керування й контроль за роботою системи. Аналогічне можна сказати й про можливість керування СКУД зі свого мобільного телефону.

Інтеграція СКУД з іншими системами безпеки й охорони. Системиконтролю й керування доступом прекрасно сполучаються й вбудовуються з іншими системами безпеки: системою відеоспостереження, охоронною й пожежною сигналізацією. Так, наприклад, контроль доступом разом з відеоспостереженням забезпечують абсолютний контроль над охоронюваними приміщеннями. При виникненні позаштатної ситуації така система в найкоротший термін дозволить виявити й заблокувати порушника. При інтеграції СКУД і охоронною сигналізацією є можливість настроїти спільну реакцію системи на несанкціоноване проникнення в те або інше приміщення. Наприклад, можна включити сирену на пункті охорони, тривожну лампу або ж і зовсім заблокувати всі двері в необхідній частині будинку.

Інтеграція СКУД із системою пожежної сигналізації дозволяє автоматично розблокувати двері, турнікети й прохідні у випадку пожежі. Всі ці міри значно спрощують евакуацію персоналу в настільки важкий період.

2. Ідентифікатор користувача

Ідентифікатор користувача - це пристрій або ознака, за якою визначається користувач. Для ідентифікації застосовуються атрибутні і біометричні ідентифікатори. Як атрибутні ідентифікатори використовують автономні носії ознак допуску: магнітні картки, безконтактні проксіміті-карти, брелоки «тач-мемори», різні радіобрелки. Біометричні - зображення райдужної оболонки ока, відбиток пальця, відбиток долоні, риси обличчя і багато інших фізичні ознаки. Кожен ідентифікатор характеризується певним унікальним двійковим кодом. У СКУД кожному коду ставиться у відповідність інформація про права і привілеї власника ідентифікатора. У даний час застосовуються:

- безконтактні радіочастотні проксіміті-карти (proxmity) - найбільш перспективний в даний час тип карт. Безконтактні картки спрацьовують на

відстані і не вимагають чіткого позиціонування, що забезпечує їх стійку роботу і зручність використання, високу пропускну здатність;

- магнітні картки - найбільш широко поширений варіант.

Існують карти з низькокоерцитивною і висококоерцитивною магнітною смугою і з записом на різні доріжки;

- карти Виганда (Wiegand) - названі по імені вченого, який відкрив магнітний сплав, у якого прямокутної петлею гистерезиса;

- штрих-кодові карти - на карту наноситься штриховий код. Є окремі норми-яття більш складний варіант - штрих-код закривається матеріалом,

- прозорим тільки в інфрачервоному світлі, зчитування відбувається в ІЧ-області;

- ключ-брелок «тач-меморі» (touch-memory) - металева таблетка, всередині якої розташований чіп ПЗУ.

Ідентифікатори користувачів СКУД можуть мати різний статус. Для забезпечення більшості необхідних в реальному житті вимог, як мінімум, треба, щоб контролери підтримували такі типи карт:

- постійна: для співробітників підприємства;
- тимчасова: з обмеженням терміну дії;
- «разова»: автоматично анулюється після вичерпання числа проходів;

3. Контролери СКУД

Контролери - пристрої, призначені для обробки інформації від зчитувачів ідентифікаторів, ухвалення рішення і управління виконавчими пристроями. Саме контролери дозволяють прохід через пропускні пункти. Контролери різняться ємністю бази даних і буфера подій, що обслуговуються пристроїв ідентифікації.

Контролер СКУД складається з чотирьох основних частин (рис. 2.1): зчитувача, схем обробки сигналу, прийняття рішення і схеми буфера подій

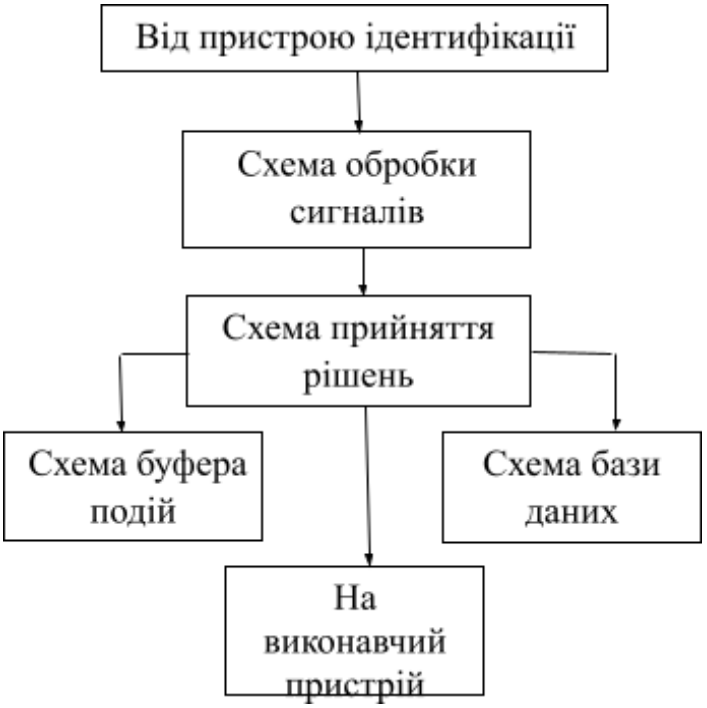


Рис. 1.13 Схема контролера СКУД

Зчитувач карт (пристрій ідентифікації) передає інформацію на схему обробки сигналів контролера. Далі інформація в цифровому вигляді видається на схему прийняття рішення, яка заносить факт спроби проходу в схему буфера подій, запитує схему бази даних на предмет правомірності проходу і в разі позитивної відповіді пускає в хід виконавчий пристрій. Обмеження вже знято, але система контролю доступу ще не завершила обробку інформації: сам факт проходу саме цю людину заноситься в схему буфера подій.

Незалежно від типу застосовуваних зчитувачів контролери повинні підтримувати такі режими доступу:

- по одній карті і / або ПІН-коду;
- доступ з підтвердженням оператором;
- контроль кількості людей в приміщенні (мінімум і максимум).

Останнє важливо в ситуаціях коли, наприклад, за умовами служби в приміщенні не повинно залишатися менш одного (двох, трьох) осіб.

Основу сучасних СКУД складають автоматичні і автоматизовані СКУД. У них процедура перевірки може включати також сопоставління особи, що перевіряється з відеопортретом на моніторі контролера. Сучасні автоматичні і автоматизовані СКУД в залежності від способу управління поділяються на **автономні, мережеві (централізовані) і розподілені (комбіновані)**

Автономні контролери - повністю закінчені пристрої, призначені для обслуговування, як правило, однієї точки проходу. Можливість об'єднання з іншими аналогічними контролерами не передбачена. Існує багато видів таких пристроїв: контролери, суміщені зі зчитувачем, контролери, вбудовані в електромагнітний замок і т. д. В автономних контролерах застосовуються зчитувачі самих різних типів. Як правило, автономні контролери розраховані на обслуговування невеликого числа користувачів, зазвичай не більше 500 осіб. Вони працюють з одним виконавчим пристроєм без передачі інформації на центральний пункт охорони і без контролю з боку оператора. Прикладом подібної системи контролю доступу може служити досить проста комбінація: «електромагнітний замок + зчитувач карт ідентифікації». Якщо необхідно контролювати тільки одні двері і в майбутньому розширення системи контролю доступу не планується, це оптимальне і досить недороге рішення.

Мережеві контролери можуть працювати в мережі під управлінням компьютера. У цьому випадку рішення приймає персональний комп'ютер з встановленим спеціалізованим програмним забезпеченням. Мережеві контролери застосовуються для створення СКУД будь-якого ступеня складності. Число мережевих контролерів в системі може бути від двох до кількох сотень з обміном інформацією з центральним пунктом охорони і контролю. У цьому випадку

розміри системи контролю доступу визначаються по числу пристроїв ідентифікації, а не за кількістю контрольованих дверей, оскільки на кожні двері може бути встановлено один-два пристрої ідентифікації в залежності від застосовуваної технології проходу.

Використовуючи мережеві контролери, адміністрація отримує ряд додаткових можливостей:

- отримання звіту про присутність або відсутність співробітників на роботі;
- уточнення місцезнаходження конкретного співробітника;
- ведення табеля обліку робочого часу;
- складання звіту про переміщення співробітників практично за будь-який період часу;
- формування часових графіків проходу співробітників;
- ведення бази даних співробітників (електронної картотеки).

Мережеві СКУД використовуються на великих підприємствах і в тих випадках, якщо потрібні її специфічні можливості, такі, як облік робочого часу співробітників. Мережеві контролери об'єднуються в мережу.

До базових характеристик мережевих контролерів відносять такі кількісні характеристики:

- число підтримуваних точок проходу;
- обсяг бази даних користувачів,
- обсяг буфера подій.

Число підтримуваних точок проходу. Оптимальне рішення в цьому випадку наступне: один мережевий контролер на дві точки проходу, так як загальні ресурси (корпус, джерело живлення з акумулятором) потрібні в меншій кількості. Контролери з великим числом обслуговуваних дверей існують, але їх небагато з наступних причин:

- висока вартість джерела живлення на 4-5 Ампер з резервуванням;
- збільшується вартість комунікацій між контролером і дверима. Крім того, якщо двері розташовані далеко один від одного, то стає проблемою і прокладка дроти живлення замка, так як при токах споживання близько 1 А виникають великі втрати.

Обсяг бази даних користувачів визначається виключно кількістю людей, які будуть ходити через максимально напружену точку проходу (прохідну).

Обсяг буфера подій визначає, скільки часу мережева система зможе працювати при вимкненому (завислому, згорілому) комп'ютері, не втрачаючи інформації про події. Наприклад, для офісу з числом співробітників близько 20 осіб обсягу буфера подій, що дорівнює 1000, може вистачити на тиждень. А для заводської прохідної, через яку проходить 3 тис. чоловік, і буфера на 10 тис. подій з працею вистачить на добу.

Практично всі контролери підтримують інтерфейс Віганда, і практично всі типи зчитувачів, в тому числі і біометричні, підтримують цей формат.

Сучасний контролер доступу повинен підтримувати гнучку систему тимчасових розкладів, на основі яких приймається рішення про доступ тієї чи іншої людини. При цьому стандартні тижневі цикли з вихідними днями - це найпростіше рішення. Реально ще потрібно задавати свята, робочі дні в свята, а найголовніше різні «плаваючі» графіки по типу «доба через три» і т. П У професійному контролері тимчасові розкладу можуть управляти не тільки доступом користувачів, а й автоматично відкривати і закривати двері в заданий час, ставити на охорону і знімати приміщення з охорони (при наявності охоронних функцій), перемикати додаткові реле.

Комбіновані контролери поєднують функції мережевих і авто-автономних контролерів. При наявності зв'язку з керуючим комп'ютером (онлайн) контролери працюють як мережеві пристрої при відсутності зв'язку - як автономні.

Суміжні функції контролерів. В першу чергу це функції підтримки охоронно-пожежної сигналізації, інтеграції з підсистемами телеспостереження і керування деякими функціями оповіщення і пожежегасіння. можлива також підтримка локальних комп'ютерних мереж з різними робочими станціями і правами доступу, передачі інформації через Інтернет.

4 . Виконавчі пристрої СКУД

У СКУД передбачаються заходи щодо забезпечення стійкості до розтину зловмисниками замків і запірних механізмів, за запобігання-обертанню спостереження за введенням ідентифікаційних ознак та копіювання еталонних ознак ідентифікаторів.

Так як перегороджуючі пристрої можуть піддаватися руйнуючим і неруйнуючим впливам зловмисників, то їх по механічній стійкості стандарт класифікує наступним чином:

- підвищена стійкість до злому шляхом нанесення ударів і застосуванні інструментів;
- висока стійкість, яка характеризується кулє- та вибухостійкістю суцільного перекриття прохідного отвору.

Електричні замки і засувки

Електричні замки рекомендується використовувати в якості основного замикаючого пристрою в денний час. Ці замки на відміну від механічних відкриваються дистанційно по електричному сигналу і використовуються спільно з домофонами, кодовими панелями, зчитувачами карток різних типів. Електрозамки діляться на два класи: електромагнітні та електромеханічні.

Електромагнітні замки представляють собою корпус з електромагнітом і відповідну металеву пластину. Пластина кріпиться на дверному полотні, а сам замок - на одвірку. Електромагнітний замок утримує двері в закритому стані за рахунок зусилля потужного електромагніту. При знеструмленні замку двері

залишаються відкритими, тому для забезпечення роботи в умовах відключення напруги живлення необхідно застосовувати блоки гарантованого живлення.

Електромеханічний замокмає механічний ригель (засув), утримуючий двері в закритому стані, а управління цим ригелем здійснюється відносно малопотужним соленоїдом. При закритті дверей підводящий ригель замку зводить наявну в замку пружину, при цьому робочий ригель входить у відповідну частину замку і утримує двері в закритому стані. При подачі напруги соленоїд відпускає фіксатор пружини, і робочий ригель під дією пружини втягується в замок - двері можуть бути відкриті. Після того як двері буде відкрита, а потім закрита, вона знову опиниться в замкненому стані. Передбачається режим, виключаючий автоматичне замикання замків і випадкове закривання дверей.

У соленоїдних електрозамках ригель приводиться в рух зусиллям електромагніта. Обладнана таким замком двері можуть бути відкриті тільки в період дії керуючого сигналу. Після зняття цього сигналу зачинені двері залишиться замкненою незалежно від того, відкривалася чи вона. Існують також інші різновиди електромеханічних замків: електромоторні (ригель приводиться в рух електромотором з редуктором), з ручним приводом ригеля (ригель приводиться в рух поворотом ручки, а електромагніт розблокує механізм приводу). Електромеханічні замки можуть бути накладного і врізного типу.

Електрозащілки представляють собою відповідну частину замку і використовуються спільно зі звичайним механічним замком. При подачі напруги розблокується фіксатор електрозащілки, і двері можуть бути відкриті при висунутому положенні ригеля механічного замка. При цьому використовується механічний замок не повинен відкриватися зовні поворотом ручки. При наявності ручки з внутрішньої сторони дверей вона може бути відкрита зсередини поворотом ручки без подачі напруги, що управляє на засувку. Спеціальні моделі соленоїдних замків і електрозащілок призначені для обладнання аварійних виходів. Такі замки відкриваються при відключення напруги живлення.

Турнікети.

Усі турнікети відносяться до розділу «Пристрої перегороджують керовані (УПУ)» і класифікуються за такими двома ознаками:

- вид перекриття отвору;
- спосіб управління УПУ.

По виду перекриття отвору розрізняють наступні види турнікетів:

- з частковим перекриттям отвору;
- з повним перекриттям отвору;
- з блокуванням об'єкта в отворі (шлюзи, кабіни прохідні).

За способом управління УПУ ділять на пристрої:

- з ручним керуванням;
- з напівавтоматичним керуванням;
- з автоматичним управлінням.

Принцип роботи турнікета СКУД простий: якщо запит на доступ правомірний, то механічна система, повертаючись, відкриває прохід на територію, що охороняється.

До основних видів турнікетів відносяться:

- хвіртки;
- триподи;
- роторні поясні турнікети;
- турнікети з висувними стулками;
- турнікети з відкидними стулками на електроприводи;
- роторні повнопрофільні або повнозростові турнікети.

Нормально відкриті турнікети мають більш високу пропускну здатність, але не виключають можливість проходу декількох притиснувшихся один до одного людина.

Вони поділяють потік людей по одному, забезпечуючи при цьому високу пропускну здатність. У режимі однократного проходу через турнікет в дозволеному напрямку може пройти одна людина, після чого турнікет автоматично повертається в закрите положення. При необхідності пропуску групи осіб встановлюється режим багаторазового проходу в потрібному напрямку, можливий режим вільного проходу. Напрямок прохода висвічується на табло. У разі екстрених ситуацій можливе механічне розблокування планок за допомогою ключа або їх демонтаж. При відключенні від джерела турнікет переходить на роботу від акумулятора.

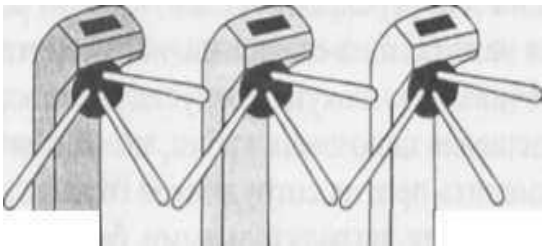


Рис. 2.13 Турнікети-триподи стрьома перегороджуючими планками

Турнікети й хвіртки - найбільш популярний вид турнікета. Це обумовлено їх невисокою вартістю і компактністю. Триподи мають сучасний елегантний зовнішній вигляд, легко монтуються.

Роторні турнікети можуть працювати в автономному режимі з управлінням від пульта охоронця, а також у складі СКУД. У режимі однократного проходу через турнікет в дозволеному напрямку людина штовхає планки у дозволеному напрямку, після чого відбувається автоматичний доворот «вертушки» у вихідне закрите положення. При не-обходимо пропуску групи осіб встановлюється режим багаторазового проходу в потрібному напрямку, можливий режим вільного проходу. У разі екстрених ситуацій можлива механічне розблокування лопатей за допомогою ключа. При відключений від джерела турнікет переходить на роботу від акумулятора.

Турнікети-хвіртки широко використовуються в магазинах, аеропортах, во-кзалах для організації вільного проходу в одну сторону і заборони проходу в іншу сторону, а також в банках, установах, на підприємствах для організації вільного виходу.

Хвіртки можна використовувати в системах контролю доступу, але для більш повного захисту необхідно підключати до хвіртки датчики проходу і організувати додатковий контроль. Ці турнікети не поділяють потік людей по одному і після відкриття хвіртки через неї можуть пройти кілька людей.

Автоматична електромеханічна хвіртка з приводом автоматично відчиняється по команді з пульта охорони або при спрацьовуванні ІЧ датчика. Створку при необхідності можна притримати або штовхнути швидше. Електромеханічна хвіртка без приводу управляється від пульта, але при проході створка відводиться рукою. При відключенні від джерела хвіртка працює від акумулятора.

Механічна хвіртка не має дистанційного керування і просто механічно забезпечує вільний прохід в одну сторону і заборона проходу в іншу сторону.

Після проходу людини створка хвіртки будь-якої моделі автоматично повертається у вихідне положення і блокується. В екстрених випадках хвірткуможна відкрити звичайним ключем, а створку повернути рукою, звільнивши прохід.

Огородження призначені для формування потоків людей, обмеження зон проходу.

При обладнанні прохідних турнікетами різного типу часто оказується, що зона проходу перекрита в повному обсязі і є необхідність в огородженні. Огородження можна виконати в єдиному дизайні з турнікетами. Як заповнень можна використовувати тоновані або дзеркальні скла з нанесенням логотипу замовника. Огородження легко монтуються і можуть бути будь-якій висоти і форми.

Турнікети поясні залишають можливість для перепригування, оскільки, як випливає з їх назви, загороджувальний бар'єр доходить тільки до пояса людини. При їх використанні практично неможливо забезпечити захист від перекидання предметів, тому такі турнікети обов'язково повинні бути встановлені в зоні видимості охорони.

Електричні замки і засувки

Електричні замки рекомендується використовувати в якості основного замикаючого пристрою в денний час. Ці замки на відміну від механічних відкриваються дистанційно по електричному сигналу і використовуються спільно з домофонами, кодовими панелями, зчитувачами карток різних типів. Електрозамки діляться на два класи: електромагнітні та електромеханічні.

Електромагнітні замки представляють собою корпус з електромагнітом і відповідну металеву пластину. Пластина кріпиться на дверному полотні, а сам замок - на одвірку. Електромагнітний замок утримує двері в закритому стані за рахунок зусилля потужного електромагніту. При знеструмленні замку двері залишаються відкритими, тому для забезпечення роботи в умовах відключення напруги живлення необхідно застосовувати блоки гарантованого живлення.

Електромеханічний замокмає механічний ригель (засув), утримуючий двері в закритому стані, а управління цим ригелем здійснюється відносно малопотужним соленоїдом. При закритті дверей підводящий ригель замку зводить наявну в замку пружину, при цьому робочий ригель входить у відповідну частину

замку і утримує двері в закритому стані. При подачі напруги соленоїд відпускає фіксатор пружини, і робочий ригель під дією пружини втягується в замок - двері можуть бути відкриті. Після того як двері буде відкрита, а потім закрита, вона знову опиниться в замкненому стані. Передбачається режим, виключаючий автоматичне замикання замків і випадкове закривання дверей.

У соленоїдних електрозамках ригель приводиться в рух зусиллям електромагніта. Обладнана таким замком двері можуть бути відкриті тільки в період дії керуючого сигналу. Після зняття цього сигналу зачинені двері залишиться замкненою незалежно від того, відкривалася чи вона. Існують також інші різновиди електромеханічних замків: електромоторні (ригель приводиться в рух електромотором з редуктором), з ручним приводом ригеля (ригель приводиться в рух поворотом ручки, а електромагніт розблокує механізм приводу). Електромеханічні замки можуть бути накладного і врізного типу.

Електрозащілки представляють собою відповідну частину замку і використовуються спільно зі звичайним механічним замком. При подачі напруги розблокується фіксатор електрозащілки, і двері можуть бути відкриті при висунутому положенні ригеля механічного замка. При цьому використовується механічний замок не повинен відкриватися зовні поворотом ручки. При наявності ручки з внутрішньої сторони дверей вона може бути відкрита зсередини поворотом ручки без подачі напруги, що управляє на засувку. Спеціальні моделі соленоїдних замків і електрозащілок призначені для обладнання аварійних виходів. Такі замки відкриваються при відключення напруги живлення.

Контрольні запитання.

1. Визначення СКУД
2. За якими ознаками у відповідності з керівними документами поділяють СКУД
3. На які класи у відповідності з керівними документами поділяють СКУД
4. Назвати основні можливості які надає оснащення СКУДом підприємства
5. Назвати основні СКЛАДОВІ СКУД
6. Що таке ідентифікатор користувача. які існують
7. Призначення контролера в СКУД. склад контролера
8. Охарактеризувати автономний контролер СКУД
9. Охарактеризувати мережевий контролер СКУД
10. Призначення виконавчого пристрою СКУД.
11. Які типии електричних замків існують.
12. Доповісти принцип дії електромеханічного замку

3. СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України. Про захист інформації в автоматизованих системах (Відомості Верховної Ради (ВВР), 1994, № 31, ст.286) (Вводиться в дію Постановою ВР № 81/94-ВР від 05.07.94, ВВР, 1994, № 31, ст.287.
2. Закон України "Про Державну службу спеціального зв'язку та захисту інформації України".
3. Закон України "Про захист інформації в інформаційно-телекому-нікаційних системах" (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286) {Вводиться в дію Постановою ВР N 81/94-ВР від 05.07.94, ВВР, 1994, N 31, ст.287}
4. Закон України. Про державну таємницю. №1079-XIV 21 вересня 1999 року.
5. Указ Президента України "Про Положення про технічний захист інформації в Україні" від 27 вересня 1999 р. № 1229
6. Постанова КМУ. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних інформаційно-телекомунікаційних системах від29 березня 2006 р № 373
7. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации Под ред. В.А. Хорошко. – К.: 2010. – Том I - II. Несанкционированное получение информации.
8. Тихонов Ю.О., Савченко В.А., Котенко А.М., Зідан А.М. Лабораторний практикум з теорії кіл і сигналів в інформаційному та кіберпросторах. Практикум. - К.: ДУТ, 2019.- 221с.
9. Котенко А.М. Курс лекцій для студентів зі спеціальності 125 «Кібербезпека та захист інформації» з дисципліни «Системи контролю та управління доступом на об'єкти інформаційної діяльності». –К, ДУІКТ, 2024. – 79 с.
10. Закон України. Про інформацію № 2657-XII від 2 жовтня 1992 року.

Навчально-методичне видання

ПРОГРАМНО-АПАРАТНІ ЗАСОБИ ЗАХИСТУ

Конспект лекцій

Для студентів з галузі знань 12 «Інформаційні технології»
за спеціальністю 125 «Кібербезпека та захист інформації»

Укладачі:
А.М. Котенко, канд. техн. наук, доцент
Ю.І. Хлапонін, д.т.н, професор
В. М. Трофимчук

Ум. друк. арк. 3,02. Обл.-вид. арк. 3,25 Електронний документ. Вид № 45/V-24.

Виконавець і виготовлювач
Київський національний університет будівництва і архітектури

Проспект Повітряних Сил, 31, Київ, Україна, 03680
Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи ДК № 808 від 13.02.2002 р