МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

"На правах рукопису"
УДК 681.3.06

«До захисту допущено»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
“_____” __січня___2022 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТЕХНІЧНОЇ СИСТЕМИ ОХОРОНИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ**

Студент групи СЗДМ-61 Цимбалістий Вадим Іванович _____
(підпис)

Науковий керівник: к.т.н., доцент Котенко Андрій Миколайович _____
(підпис)

Нормоконтроль: Гребенніков Ассаді Болдхоягович _____
(підпис)

Київ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри
СІКЗ
_____ Г. В. Шуклін
(підпис)
“___”_____ 2022 р.

ЗАВДАННЯ

на магістерську атестаційну роботу

студенту Цимбалістому Вадиму Івановичу

1.Тема роботи: Підвищення ефективності функціонування технічної системи охорони об'єкту інформаційної діяльності

Затверджена наказом по університету “___”_____2021 р. № _____

2.Термін здачі студентом оформленої роботи “___”_____2021 р.

3.Об’єкт дослідження: Процес захисту об’єкту інформаційної діяльності.

4. Предмет дослідження: Ефективність технічної системи охорони.

5.Мета дослідження: підвищити ефективність функціонування технічної системи охорони об’єкту інформаційної діяльності.

6.Перелік питань, які мають бути розроблені:

1. Необхідність захисту інформації з обмеженим доступом на об’єкті інформаційної діяльності.
2. Складові технічної системи охорони
3. Створення ефективної технічної системи охорони об’єкту інформаційної діяльності.

7.Перелік публікацій:

8. Перелік ілюстративного матеріалу:

Презентанція на слайдах.

9. Дата видачі завдання “___”_____ 2021 р.

Науковий керівник _____ А.М. Котенко
(підпис)

Завдання прийнято до виконання _____ В.І. Цимбалістий
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	**Примітка**
1	Визначення напрямку дослідження та вибір об’єкта		Виконано
2	Отримання завдання і складання змісту (плану) дипломної роботи		Виконано
3	Складання календарного плану – графіку з підготовки дипломної роботи		Виконано
4	Написання першого розділу роботи		Виконано
5	Написання другого розділу роботи		Виконано
6	Написання третього розділу роботи		Виконано
8	Написання висновків по роботі		Виконано
9	Підготовка до захисту: доповідь, ілюстративний (роздатковий) матеріал		Виконано
10	Рецензування дипломної роботи		Виконано
11	Захист дипломної роботи магістра		Виконано

Студент групи СЗДМ-61 Цимбалістий Вадим Іванович _____
(підпис)

Науковий керівник: к.т.н. Котенко Андрій Миколайович _____
(підпис)

Нормоконтроль: _____
(підпис)

АНОТАЦІЯ

У роботі досліджені існуючі технічні канали витоку інформації, особливо матеріально-речовий канал витоку інформації, вимоги до захисту інформації з обмеженим доступом, існуючі засоби захисту інформації від витоку матеріально-речовим каналом.

Проаналізовано склад технічної системи охорони, завдання, які вирішує технічна система охорони на об’єктах інформаційної діяльності.

Проаналізовано структури технічних систем охорони, якісні переваги та недоліки цих структур, принцип функціонування виконавчого елементу охоронного сповіщувача, принцип функціонування охоронного шлейфу.

На підставі цього зроблено висновок про можливість побудови охоронного шлейфу за новим принципом функціонування з відповідними перевагами порівняно зі шлейфами існуючих технічних систем охорони.

Дипломна робота містить 70 сторінок, 22 малюнка, 2 таблиці та 18 джерел літератури.

ANNOTATION

In this work the existing technical information leakage, especially material and material information leakage requirements for data protection, existing data protection from the source material and the material channel.

Studied Composition of health. Tasks that solves the technical system of protection on objects of information activity.

The existing structures of construction of technical security systems, qualitative advantages and disadvantages of these structures, the principle of functioning of the security element actuator, and the principle of the guard loop function are investigated.

On the basis of this, it was concluded that it is possible to construct a guard loop according to the new principle of functioning with the corresponding advantages compared with the layouts of existing structures of technical security systems.

This work contains 70 pages, 22 picturesand, 2 tables, 18 sources of literature.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРМ - автоматизовані робочі місця;

ВПОС - виносний пристрій оптичної сигналізації;

ДТЗС - допоміжні технічні засоби системи;

ЕМС – електромагнітна сумісність;

ІСБ - інтегрованої системи безпеки;

ОТЗС - основні технічні засоби і системи;

ПЕМВ - побічні електромагнітні випромінювання;

ПЕВІН - побічні електромагнітні випромінювання і наведення;

ППКОП - прилад приймально-контрольний охоронно пожежний;

СЗОІ - система збору й обробки інформації;

ТЗІ – технічний захист інформації;

ТЗПІ - технічний засіб перетворення інформації;

ТЗОС – технічні засоби охоронної сигналізації;

ТСО – технічна система охорони.

ВСТУП

Увага до питань інформаційної безпеки зростає, дослідження в цій сфері свідчать про намагання збалансувати зусилля щодо зниження ризиків з підвищенням ефективності діяльності.

Варто визнати, що державні правоохоронні органи й силові структури в цей час не в змозі забезпечити в повному обсязі організацію необхідного рівня безпеки всіх об'єктів різних форм власності. Тому керівництво багатьох підприємств і організацій шукає шляхи рішення цієї проблеми власними засобами, насамперед шляхом створення своїх служб безпеки із широким використанням технічних засобів і систем.

З розвитком інформаційних технологій збільшується ризик витоку інформації, зараження вірусами, втручання в роботу системи. Важливо усвідомлювати стан захищеності ресурсів в інформаційній системі підприємства, щоб протистояти різним видам загроз її безпеці. Реальну допомогу в цьому може надати систематизація і вдосконалення управління захистом інформації на підприємстві.

Тому необхідність здійснення регулярного аналізу загроз та постійного моніторингу безпеки інформаційних систем потребує постійного удосконалення та огляд нових засобів захисту, які можна використовувати для підвищення безпеки.

На підставі цього можна зробити висновок, що тема магістерської атестаційної роботи, присвячена дослідженню існуючих структур побудови технічних систем охорони, якісних переваг та недоліків цих структур, є актуальною.

Метою магістерської атестаційної роботи є підвищення ефективності функціонування технічної системи охорони об'єкту інформаційної діяльності.

РОЗДІЛ 1
ІНФОРМАЦІЙНА БЕЗПЕКА РЕЖИМНИХ ПРИМІЩЕНЬ

1.1. Класифікація режимної інформації

Інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1].

За своїм 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.

Втім для практичного використання більш важливою є класифікація інформації за порядком доступу до неї. У відповідності до цього інформація поділяється на: відкриту та з обмеженим доступом.

Відкрита - будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом. Основними ознаками відкритої інформації є те, що доступ до неї надається будь-яким зацікавленим особам, а будь-яке обмеження права на одержання відкритої інформації забороняється.

Способи забезпечення доступу до відкритої інформації:

– систематична публікація її в офіційних друкованих виданнях (бюлетенях, збірниках);

– поширення її засобами масової комунікації;

– безпосереднє надання її зацікавленим громадянам, державним органам та юридичним особам.

ІзОД - інформація, що становить державну або іншу передбачену законом таємницю, а також конфіденційна інформація, що є власністю держави або вимога щодо захисту якої встановлена законом.

Таємна 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. Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України “Про державну таємницю”.

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.

У відповідності до Закону "Про захист інформації в інформаційно-телекомунікаційних системах" захисту в 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 (таємна інформація).

Відкрита інформація під час обробки всистеміповинна 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.

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

Усі дії, що пов’язані з обробкою інформації з обмеженим доступом виконуються на об’єктах інформаційної діяльності. Відповідно до визначення об'єкт інформаційної діяльності — будівлі, приміщення, транспортні засоби чи інші інженерно-технічні споруди функціональне призначення яких передбачає обіг інформації з обмеженим доступом[2]. Інформаційна діяльність – це сукупність дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Обробка ІзОД на об’єктах інформаційної діяльності дозволяє забезпечити безпеку інформації, яка заключається в збереженні наступних критеріїв 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.

З метою задоволення інформаційних потреб, органи державної влади, місцевого й регіонального самоврядування створюють інформаційні служби, системи, мережі, бази й банки даних. Порядок їх формування, структура, права і обов'язки визначаються Кабінетом Міністрів України або іншими органами державної влади, а також органами місцевого й регіонального самоврядування.

Основними видами інформаційної діяльності є одержання, використання, поширення й зберігання інформації.

Одержання інформації – це придбання й накопичення відповідно до чинного законодавства України документованої або публічно оголошуваної інформації громадянами, юридичними особами або державою.

Використання інформації – це задоволення інформаційних потреб громадян, юридичних осіб і держави. Поширення інформації - це розповсюдження, обнародування, реалізація у встановленому законом порядку документованої або публічно оголошуваної інформації.

Зберігання інформації – це забезпечення належного стану інформації її матеріальних носіїв.

Одержання, використання, поширення і зберігання документованої або публічно оголошуваної інформації здійснюється у порядку, передбаченому цим Законом та іншими законодавчими актами в галузі інформації. Крім того, можна виділити діяльність, пов’язану з інформаційним забезпеченням – одержання, оцінки, зберігання та переробки даних, створена з метою вироблення управлінських рішень. Це стосується різних видів діяльності, наприклад виробничої і збутової, сервісного обслуговування, включаючи підвищення технологічності виробництва, якості вироблюваної продукції, зниження її собівартості, рекламу, інформацію про асортимент продукції, ціни, форми організації сервісу тощо.

Будь який вид інформаційної діяльності (включно інформаційний бізнес) не може здійснюватись в умовах ізоляції. Його учасники (контрагенти), тобто

продавець чи покупець, роботодавець чи найманий робітник функціонують у певному середовищі, яке визначає їх позиції і називається середовищем підприємницької діяльності (підприємництва).

1.2. Безпека інформації у режимних приміщеннях

Захист інформації є одним із найважливіших у загальному комплексі заходів технічного захисту інформації (ТЗІ). Несанкціоноване ознайомлення із інформацією з метою її подальшого використання є можливим шляхом перехоплення її зловмисниками[3].

Для нелегального знімання інформації використовуються різні технічні засоби. Інформація з об'єкта надходить зловмисникові по різним фізичним каналам.

Залежно від фізичної природи виникнення інформаційних сигналів, а також середовища їх поширення і способів перехоплення повідомлення, технічні канали витоку можна розділити на:

- радіоканал;
- електричний;
- акустичний;
- оптичний;
- матеріально-речовий.

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, володіє безліччю технічних каналів витоку інформації.

Радіоканали витоку інформації утворюються за рахунок:

- мікрофонного ефекту;
- магнітного поля;
- паразитної генерації;
- по ланцюгах живлення;
- по ланцюгам заземлення;
- за рахунок взаємного впливу;
- електромагнітного випромінювання;
- ВЧ нав'язування;
- із волоконно-оптичних систем зв'язку.

Структура радіоканалу витоку інформації в загальному випадку включає (рис. 1.1) джерело сигналу або передавач, середу поширення електричного струму або електромагнітної хвилі і приймач сигналу[4].

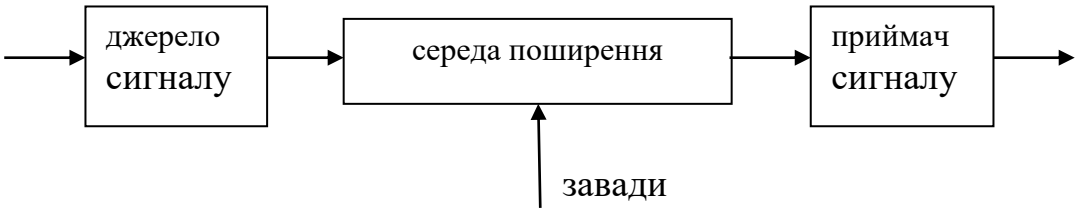

Рис. 1.1. Структура радіоканалу витоку інформації

У радіоканалах витоку інформації джерела сигналів можуть бути чотирьох видів:

- передавачі функціональних каналів зв'язку;
- джерела небезпечних сигналів;
- об'єкти, що відображають енергію радіочастоти;
- об'єкти, що випромінюють власні (теплові) радіохвилі.

Середовищем поширення радіоелектронного каналу витоку інформації є атмосфера, безповітряний простір і направляючі - електричні дроти різних типів і хвильоводи. Носій у вигляді електричного струму поширюється по дротах, а електромагнітне поле - в атмосфері, в безповітряному просторі або по

направляючим - волноводам. У приймачі проводиться виділення (селекція) носія з цікавою одержувачу інформацією по частоті, посилення виділеного слабкого сигналу і зняття з нього інформації - демодуляція.

При перехопленні сигналів функціональних каналів зв'язку передавачі цих каналів є одночасно джерелами радіоканалів витоку інформації. У загальному випадку напрям поширення електромагнітної хвилі від передавача до санкціонованого одержувача і зловмисникові відрізняються. У функціональних каналах зв'язку максимум випромінювання енергії електромагнітної хвилі орієнтують в напрямку розташування приймача санкціонованого одержувача. Тому потужність джерела сигналів радіоканалу витоку інформації, як правило, істотно менше потужності випромінювання в функціональному каналі зв'язку.

Причини виникнення електричних каналів витоку інформації:

- гальванічні зв'язки з'єднувальних ліній ТЗПІ (технічний засіб перетворення інформації) з лініями ДТЗС (допоміжні технічні засоби системи) і сторонніми провідниками;

- наведення побічних електричних випромінювань ТЗПІ на з'єднувальні ліній ДТЗС і сторонні провідники;

- наведення побічних електричних випромінювань ТЗПІ на ланцюзі електроживлення і заземлення ТЗПІ;

- «просочування» інформаційних сигналів у колі електроживлення і заземлення ТЗПІ.

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 каналах витоку інформації внаслідок наведень відносяться канали, які утворюються в мережі електроживлення технічних засобів і систем.

Крім заземлюючих провідників, які слугують для безпосереднього з'єднання ТЗПІ 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) з’єднувальних кабелів, металеві труби систем опалення та водопостачання, металева арматура залізобетонних конструкцій і т.д. Всі ці провідники разом 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.

Перехоплення інформаційних сигналів в лініях електроживлення і колах заземлення ТЗПІ можливий при гальванічному підключенні до них засоби розвідки ПЕВІН (побічні електромагнітні випромінювання і наведення).

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 відбуваються різні струми, в тому числі і небезпечні. У загальному випадку небезпечними потоками є зворотні струми для різних сигналів основних технічних засобів і систем (ОТЗС), а також струми, обумовлені наведеннями небезпечних сигналів на лінію заземлення. Причому найбільшу небезпеку представляють зворотні струми, так як вони можуть мати досить велику величину.

Витік інформації по ланцюгах заземлення може виникнути:

- при наявності рознесених точок заземлення інформативних ланцюгів в разі утворення в різних точках системи заземлення різниці потенціалів і виникнення в результаті цього струмів в ланцюгах заземлення;
- при великому значенні опору заземлення;

- внаслідок недосконалості екранів, що приводить до асиметрії ліній відносно екрана і виникнення в ланцюзі між корпусом екрана та землею інформативних струмів.

Способи перехоплення інформації яка обробляється технічними засобами представлена на рис. 1.2.

Рис. 1.2. Класифікація способів перехоплення інформації, що обробляється технічними засобами

Акустичні канали витоку інформації утворюються за рахунок:

- поширення акустичних коливань у вільному повітряному просторі;
- впливу звукових коливань на елементи і конструкції будівель;
- 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, 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.

Ще один канал витоку акустичної інформації утворюють системи повітряної вентиляції приміщень, різні витяжні системи та системи подачі чистого повітря. Можливість виникнення таких каналів визначаються конструктивними особливостями повітропроводів і акустичними характеристиками їх елементів: засувок, переходів, розподільників і ін.

Залежно від фізичної природи виникнення інформаційних сигналів, середовища поширення акустичних коливань і способів їх перехоплення, акустичні канали витоку інформації також можна розділити на повітряні, вібраційні, електроакустичні, оптико-електронні та параметричні.

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 звукозаписуючими пристроями (диктофонами) або спеціальними мініатюрними передавачами.

Перехоплена інформація може передаватися по радіоканалу, оптичного каналу (в інфрачервоному діапазоні довжин хвиль), по мережі змінного струму,

з'єднувальним лініях ДТЗС, стороннім провідникам (трубах водопостачання і каналізації, металоконструкцій і т.п.). Причому для передачі інформації по трубах і металоконструкцій можуть застосовуватися не тільки електромагнітні, а й механічні коливання.

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

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

Візуально-оптичне спостереження є найбільш відомим, досить простим, широко поширеним і добре оснащеним найсучаснішими технічними засобами розвідки. Цей вид дій володіє:

- достовірністю і точністю видобутої інформації;
- високою оперативністю отримання інформації;
- доступністю реалізації;
- документальністю отриманих відомостей (фото, кіно, TV).

Ці особливості визначають небезпеку даного виду каналів витоку інформації.

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 ПЗЗ-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.

У практиці розвідки широко використовується отримання інформації з відходів виробничої та трудової діяльності. Залежно від профілю роботи підприємства це можуть бути зіпсовані накладні, фрагменти складаються документів, чернетки листів, браковані заготовки деталей, панелей, кожухів та інших пристроїв для розроблюваних підприємством нових моделей різної техніки. Особливе місце серед такого роду джерел займають залишки бойової техніки і озброєння на випробувальних полігонах.

За своїм фізичним станом відходи виробництва можуть являти собою тверді маси, рідини і газоподібні речовини; по фізичній природі вони діляться на хімічні, біологічні, радіаційні, а по середовищу поширення на що містяться в землі, у воді і в повітрі.

Особливість матеріально-речового каналу, в порівнянні з іншими каналами, обумовлена специфікою джерел і носіїв видобувається по ньому інформації. Джерелами і носіями інформації в даному випадку є суб'єкти (люди) і матеріальні об'єкти (макро- і мікрочастинки), які мають чіткі просторові межі локалізації (за винятком випромінювань радіоактивних речовин). Витік інформації по матеріально-речовим каналах супроводжується

фізичним переміщенням людей і матеріальних тіл з інформацією за межі об'єкта, що захищається.

Основними джерелами інформації матеріально-речового каналу витоку інформації є:

- чернетки різних документів і макети матеріалів, вузлів, блоків, пристроїв, що розробляються в ході науково-дослідних і дослідно-конструкторських робіт, які ведуться в організації;
- вийшли з ладу магнітні та інші носії інформації ПЕОМ, на яких під час експлуатації містилася інформація з обмеженим доступом;
- бракована продукція та її елементи;
- секретні бібліотеки;
- інші місця зберігання матеріальних носіів ІзОД.

Перенесення інформації в матеріально-речовому каналі може здійснюватися такими суб'єктами та середовищами:

- співробітниками організації;
- повітряними атмосферними масами;
- рідкими середовищами.

Втрата носіїв цінної інформації можлива за відсутності в організації чіткої системи їх обліку. Наприклад, друкарка, зіпсувавши аркуш звіту, викидає його в кошик для сміття, з якої він переноситься прибиральницею в сміттєвий бак, що знаходиться на території організації. Потім при вантаженні або продовження транспортування сміття лист несеться вітром і потрапляє в руки випадкового перехожого. Звичайно, ймовірність забезпечення випадкового ознайомлення зловмисника з вмістом цього листа невелика. Однак якщо зловмисник активно займається добуванням інформації, область простору, в якій можливий контакт, значно звужується, що призводить до підвищення ймовірності витоку інформації по матеріально-речовим каналам.

Витік інформації через матеріально-речові канали витоку інформації можливий через:

- розкрадання носіїв інформації;

- внутрішні канали витоку (через обслуговуючий персонал);
- виробничі та технологічні відходи (папір з принтерів, виробничі відходи підприємств);
- погано прихована видова інформація про хід виробничого процесу на підприємстві.

1.4. Технічна система охорони як засіб захисту інформації

Виникнення електричних та радіоканалів витоку інформації на ОІД має місце при використанні на об’єкті інформаційно-телекомунікаційних систем[5].

Розглянемо методи протидії.

Екранування технічних засобів.

Функціонування будь-якого технічного засобу інформації пов'язано з протіканням по його струмоведучих елементів 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 ТЗПІ є причиною виникнення електромагнітних і параметричних каналів витоку інформації, а також можуть виявитися причиною виникнення наведення інформаційних сигналів в сторонніх струмопровідних лініях і конструкціях. Тому зниженню рівня побічних електромагнітних випромінювань приділяється велика увага.

Ефективним методом зниження рівня ПЕМВ є екранування їх джерел.

Розрізняють такі способи екранування:

- електростатичне;
- магнітостатичне;
- електромагнітне.

Електростатичне і магнітостатичне екранування засновані на замиканні екраном відповідно електричного і магнітного полів.

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

Основним завданням екранування електричних полів є зниження ємності зв'язку між екрануючими елементами конструкції. Отже, ефективність екранування визначається в основному ставленням ємностей зв'язку між джерелом і рецептором наведення до і після установки заземленого екрану. Тому будь-які дії, що призводять до зниження ємності зв'язку, збільшують ефективність екранування.

Магнітостатичне екранування використовується при необхідності придушити наведенняна низьких частотах від 0 до 3 ... 10 кГц.

Основні вимоги, що пред'являються до магнітостатичних екранів, можна звести до наступних:

- магнітна проникність матеріалу екрану повинна бути якомога вищою.
- збільшення товщини стінок екрану призводить до підвищення ефективності екранування, однак при цьому слід брати до уваги можливі конструктивні обмеження за масою і габаритами екрану;
- стики, розрізи і шви в екрані повинні розміщуватися паралельно лініям магнітної індукції магнітного поля. Їх кількість має бути мінімальною;
- заземлення екрана не впливає на ефективність магнітостатичного екранування.

Ефективність магнітного екранування залежить від частоти і електричних властивостей матеріалу екрану. Чим нижче частота, тим слабкіше діє екран, тим більшої товщини доводиться його робити для досягнення одного і того ж екрануючого ефекту.

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

На високих частотах застосовується виключно електромагнітне екранування. Дія електромагнітного екрану засноване на тому, що високочастотне електромагнітне поле послаблюється їм же створеним полем зворотного напрямку.

Також екрануванню підлягають монтажні дроти і сполучні лінії. Щоб зменшити рівень ПЕМВ, необхідно особливо ретельно виконувати з'єднання оболонки дрота (екрану) з корпусом апаратури. Підключення оболонки має здійснюватися шляхом безпосереднього контакту (найкраще шляхом пайки або зварювання) з корпусом.

Екрануватися можуть не тільки окремі блоки (вузли) апаратури і їх сполучні лінії, а й приміщення в цілому.

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

- струмопровідні лакофарбові покриття або струмопровідні шпалери;
- штори з металізованої тканини;
- металізоване скло, що встановлюються в металеві або металізовані рами.

Фільтрація інформаційних сигналів.

Одним з методів локалізації небезпечних сигналів, що циркулюють в технічних засобах і системах обробки інформації, є фільтрація. У джерелах електромагнітних полів і наведень фільтрація здійснюється з метою запобігання поширенню небажаних електромагнітних коливань за межі пристрою - джерела небезпечного сигналу. Фільтрація в пристроях - рецепторах електромагнітних полів і наведень повинна виключити їх вплив на рецептор.

Для фільтрації сигналів в ланцюгах живлення ТСПІ використовуються розділові трансформатори і шумоподавляючі фільтри.

Розділові трансформатори повинні забезпечувати розв'язку первинної та вторинної ланцюгів за сигналами наводки [6]. 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 і ємнісних ланцюгів зв'язку між обмотками.

Для зменшення зв'язку обмоток за сигналами наведень часто застосовується внутрішній екран, який виконан у вигляді заземленої прокладки або фольги, що укладається між первинною і вторинною обмотками. За допомогою цього екрана наводка, діюча в первинній обмотці, замикається на землю. Однак електростатичне поле навколо екрану також може служити причиною проникнення наведень у вторинний ланцюг.

Розділові трансформатори використовуються з метою вирішення ряду завдань, в тому числі для:

- поділу по ланцюгах живлення джерел і рецепторів наведення, якщо вони підключаються до одних і тих же шин змінного струму;
- усунення асиметричних наведень;
- ослаблення симетричних наведень в ланцюзі вторинної обмотки, обумовлених наявністю асиметричних наведень в ланцюзі первинної обмотки.

В даний час існує велика кількість різних типів фільтрів, що забезпечують ослаблення небажаних сигналів в різних ділянках частотного діапазону. Це фільтри нижніх і верхніх частот, смугові та загороджуючі фільтри. Основне призначення фільтрів - пропускати без значного ослаблення сигнали з частотами, що лежать в робочій смузі частот, і пригнічувати (послаблювати) сигнали з частотами, що лежать за межами цієї смуги. Для виключення просочування інформаційних сигналів у колі електроживлення використовуються фільтри нижніх частот.

Основні вимоги, що пред'являються до захисних фільтрів, полягають в наступному:

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

- величина послаблення небажаних сигналів в діапазоні робочих частот повинна бути не менше необхідної;

- послаблення корисного сигналу в смузі прозорості фільтра має бути незначним;

- габарити і маса фільтрів повинні бути мінімальними;

- фільтри повинні забезпечувати функціонування за певних умов експлуатації (температура, вологість, тиск) і механічних навантаженнях (удари, вібрація і т.д.);

- конструкції фільтрів повинні відповідати вимогам техніки безпеки.

Просторове і лінійне зашумлення.

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

Для виключення перехоплення побічних електромагнітних випромінювань по електромагнітному каналу використовується просторове зашумлення, а для виключення знімання наведень інформаційних сигналів з сторонніх провідників і сполучних ліній допоміжних технічних засобів - лінійне зашумлення.

До системи просторового зашумлення, яка застосовується для створення маскувальних електромагнітних перешкод, висуваються такі вимоги:

- система повинна створювати електромагнітні перешкоди в діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;

- створювані перешкоди не повинні мати регулярну структури;

- рівень створюваних перешкод (як по електричній, так і по магнітної складової поля) повинен забезпечити ставлення с / ш на кордоні контрольованої зони менше допустимого значення у всьому діапазоні частот можливих побічних електромагнітних випромінювань ТЗПІ;

- система повинна створювати перешкоди як з горизонтальною, так і з вертикальною поляризацією;

- на кордоні контрольованої зони рівень перешкод, створюваних системою просторового зашумлення, не повинен перевищувати встановлених норм по електромагнітній сумісності(ЕМС).

Мета просторового зашумлення вважається досягнутої, якщо відношення небезпечний сигнал / шум на кордоні контрольованої зони не перевищує деякого допустимого значення, що розраховується за спеціальними методиками для кожної частоти інформаційного (небезпечного) побічного електромагнітного випромінювання ТЗПІ.

У системах просторового зашумлення в основному використовуються слабонаправлені рамкові жорсткі і гнучкі антени. Рамкові гнучкі антени виконуються зі звичайного дроту і розгортаються в двох-трьох площинах, що забезпечує формування завадового сигналу як з вертикальною, так і з горизонтальною поляризацією в усіх площинах.

Системи лінійного зашумлення застосовуються для маскування наведених небезпечних сигналів в сторонніх провідниках і з'єднувальних лініях ДТЗС, що виходять за межі контрольованої зони.

У найпростішому випадку система лінійного зашумлення представляє собою генератор шумового сигналу, який формує шумову маскуючу напруга із заданими спектральними, тимчасовими і енергетичними характеристиками, який гальванічно підключається в зашумлюючу лінію (сторонній провідник). На практиці найбільш часто подібні системи використовуються для зашумлення ліній електроживлення.

Розглянемо методи протидії від витоку інформації по акустичному каналу.

Захист мовної інформації є важливим завданням в загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта чи установи.

Для її перехоплення «противник» може використовувати широкий арсенал портативних засобів акустичної мовної розвідки, які дозволяють перехоплювати мовну інформацію по прямому акустичному, віброакустичному, електроакустичному і оптико-електронного (акустооптичні) каналам до основних з яких відносяться:

- портативна апаратура звукозапису (малогабаритні диктофони, магнітофони 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'єднувальних лініях допоміжних технічних засобів або спеціально прокладених лініях;
- оптико-електронні (лазерні) акустичні системи й т.п.

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 використовується словесна розбірливість мови на виході каналу витоку інформації.

Пасивні методи захисту інформації.

Визначено, що для зниження розбірливості мови необхідно прагнути до зменшення відношення «рівень мовного сигнала / рівень шуму» (сигнал / шум) в місцях можливого розміщення датчиків апаратури акустичної розвідки.

Зменшення відношення сигнал / шум можливо наступними способами:

- пасивні методи захисту (зменшення) рівня мовного сигналу);
- активні методи захисту (збільшення рівня шуму).

Ослаблення акустичних (мовних) сигналів здійснюється шляхом звукоізоляції приміщень, яка спрямована на локалізацію джерел акустичних сигналів всередині 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 звукопоглинаючі матеріали. Підвищення звукоізоляції стін і перегородок приміщення також досягається установкою на відстані в 6 ... 10 см від них одношарових і багатошарових (частіше подвійних) огороджень.

Одним з найбільш слабких звукоізолюючих елементів огороджувальних конструкцій виділених приміщень є двері і вікна.

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.

Активні методи захисту інформації.

Якщо необхідно проводити 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.

За принципом дії всі технічні засоби просторового і лінійного зашумлення можна розділити на три великі групи:

Засоби створення акустичних маскуючих перешкод:

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

Засоби створення електромагнітних маскуючих перешкод:

- технічні засоби просторового зашумлення;
- технічні засоби лінійного зашумлення, які діляться на засоби створення маскуючих перешкод в комунікаційних мережах і засоби створення маскуючих перешкод в мережах електроживлення.

Багатофункціональні засоби захисту.

Найбільш ефективним засобом захисту приміщень, призначених для проведення конфіденційних заходів, від знімання інформації через шибки, стіни, системи вентиляції, труби опалення, двері і т.п. є пристрої віброакустичного захисту [7]. Дана апаратура дозволяє запобігти прослуховування за допомогою дротових мікрофонів, звукозаписуючої апаратури, радіомікрофонів і електронних стетоскопів, систем лазерного знімання акустичної інформації з вікон і т.п. Протидія прослуховуванню забезпечується внесенням віброакустичних шумових коливань в елементи сигналу.

Відмінною особливістю технічних засобів ультрозвукового захисту приміщень є вплив на мікрофонний пристрій і його підсилювач достатньо сильним ультразвуковим сигналом, що викликає блокування підсилювача або виникнення значних нелінійних спотворень, що призводять, в кінцевому випадку, 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 вузьконаправлених мікрофонів.

Мікрофони, як відомо, перетворюють енергію звукового сигналу в електричні сигнали. У сукупності зі спеціальними підсилювачами і фільтруючими елементами 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. Звичайно, що методи радіоконтролю, ефективні для пошуку радіозакладок, в даному випадку не мають сенсу.

Для захисту від вузькоспрямованих мікрофонів рекомендуються такі заходи:

- при проведенні нарад слід обов'язково закривати вікна і двері (найкраще, щоб кімната для нарад 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.

Класифікація пристроїв пошуку технічних засобів розвідки може бути наступною:

Пристрої пошуку активного типу:

- нелінійні локатори (досліджують відгук на вплив електромагнітним полем);
- рентгенметри (просвічують за допомогою рентгенівської апаратури);

Пристрої пошуку пасивного типу:

- металошукачі;
- пристрої та системи пошуку по електромагнітному випромінюванню;

- пристрої пошуку по зміні параметрів телефонної лінії (напруги, індуктивності, ємності, добротності);

- пристрої пошуку по зміні магнітного поля (детектори записуючої апаратури).

Спеціальні приймачі для пошуку працюючих передавачів в широкому діапазоні частот називають скануючими пристроями[8]. 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.

Вирішення задач пов’язаних із запобіганням витоків інформації матеріально-речовим каналом з об’єктів інформаційної діяльності полягає у використанні фізичної та технічної складової служби безпеки організації.

Одним з елементів технічної складової є технічні засоби охорони об’єктів які і являються предметом досліджень дипломної роботи.

Технічні засоби охорони поєднуються у технічну система охорони (ТСО) яка призначена для:

- постановки і зняття з охорони приміщень;

- формування та видачі сигналів тривоги при несанкціонованому появі або спробі проникнення людини в закриті і здані під охорону приміщення; перегляду стану охоронюваних приміщень на планах в графічній формі на автоматизованих робочих місцях (АРМ) інтегрованої системи безпеки (ІСБ) і відображення на них сигналів тривоги або несправності в графічному, текстовому та голосовому вигляді з прив'язкою до плану об'єкта;

- ведення протоколу подій системи ТСО в пам'яті комп'ютера з можливістю перегляду на моніторі і його роздруківки; ведення електронного журналу, фіксуючого дії операторів в стандартних і позаштатних ситуаціях.

У загальному вигляді технічна система охорони включає в себе наступні засоби (рис. 1.3):

- засіб виявлення (сповіщувач) - це пристрій, призначений для автоматичного формування сигналівіз 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 прийомо-контрольним охоронно-пожежним (ППКОП);

- 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.).

Рисунок 1.3. Технічна система охорони об’єкту

Висновок по розділу. Встановлено, що існують види інформації, які згідно законів України потребують захисту. Загрозу інформації на об’єктах інформаційної діяльності являють: радіоканал, електричний, акустичний канал, оптичний канал та матеріально-речовий канал. Технічна система охорони призначена для захисту інформації від витоку матеріально-речовим каналом. Існує необхідність підвищення ефективності функціонування таких систем.

РОЗДІЛ 2
СКЛАД ТЕХНІЧНОЇ СИСТЕМИ ОХОРОНИ

2.1. Термінологія технічних систем охорони

Технічний засіб охорони – це базове поняття, що позначає апаратуру (вид техніки), яка використовується у складі комплексів (систем) технічних засобів призначених для охорони об'єктів (територій, будівель, приміщень) від несанкціонованого проникнення[9].

Історично склалося декілька підходів до вирішення проблем класифікації ТЗО. Нами буде розглянутий підхід, який можна характеризувати як узагальнений, не провокуючий полеміки на предмет більшої або меншої коректності тих або інших підходів, бо їх відмінності виникають з відмінностей цілком певної мети класифікації. Деякі незручності для розуміння можуть створювати відмінності в термінології, коли близькі поняття позначаються різними словами, як то: засіб виявлення, датчик, сповіщувач. Іноді стосовно конкретних фізичних принципів дії застосовується слово “детектор„ як різновид сповіщувача. По суті до всіх цих термінів слід відноситися як до синонімів, що позначають близькі поняття - елементи апаратури технічних засобів охоронної сигналізації (ТЗОС), виконуючих функцію реагування на зовнішню дію. Наприклад, сейсмічний ЗВ реагує на коливання ґрунту, викликане рухом якого-небудь (людини, тварини) або чого-небудь (автомобіля, трактора і ін..). Кожний ЗВ будується на певному фізичному принципі, на основі якого діє його чутливий елемент (ЧЕ) (наприклад, електромагнітний, вібраційний, радіотехнічний, ємкісний, оптичний і ін.). Таким чином:

– засіб виявлення - це пристрій, призначений для автоматичного формування сигналу із заданими параметрами (сигналу тривоги, сигналу спрацьовування або сповіщення) унаслідок вторгнення або подолання об'єктом виявлення чутливої зони (говорять також – зони виявлення) даного пристрою.

– чутливий елемент - це первинний перетворювач, що реагує на дію на нього (пряме або непряме) об’єкта виявлення і сприймає зміну стану навколишнього середовища;

При виборі і впровадженні ТЗОС на об'єктах приділяється особлива увага досягненню високої захищеності апаратури від її подолання (обходу). Виробники ТЗОС пропонують різні способи реалізації цього завдання: контроль відкриття блоків, автоматична перевірка справності засобів виявлення і каналів передачі інформації, захист доступу до управління апаратурою за допомогою кодів (паролів), архівація всіх виникаючих подій, захист інформаційних потоків між складовими частинами ТЗОС методами маскування і шифрування і ін. Як правило, сучасні ТЗОС мають одночасно декілька ступенів захисту.

Таким чином, одним з головних завдань при проектуванні ТЗОС є створення засобів захисту від обходу їх зловмисником (порушником) і це є складним багатоплановим завданням.

Під комплексом ТЗОС розуміється сукупність функціонально зв'язаних засобів виявлення, системи збору і обробки інформації і допоміжних засобів і систем (системи тривожного сповіщення, системи охорони периметра і ін..), об'єднаних завданням по виявленню порушника.

2.2. Принципи побудови комплексів систем охорони

Структура типових варіантів побудови комплексів ТЗОС визначається розподілом логічної обробки інформації від ЗВ між станційною апаратурою і периферійними блоками (ПБ), а також способом зв'язку між ними і ЗВ[10]. На вибір варіанту структури побудови комплексу головним чином роблять вплив наступні чинники:

– якісний і кількісний склад обслуговуваних ЗВ і ПБ (концентратори, виносні пульти сигналізації і ін);

– ступінь централізації управління СЗОІ;

– 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):

– радіальний (променевий) безконцентраторний;

– радіальний (променевий) з концентраторами;

– шлейфовий (магістральний) без концентраторів і з концентраторами;

– змішана (радіально-шлейфова).

Радіальний (променевий) безконцентраторний (рис. 2.1).

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;

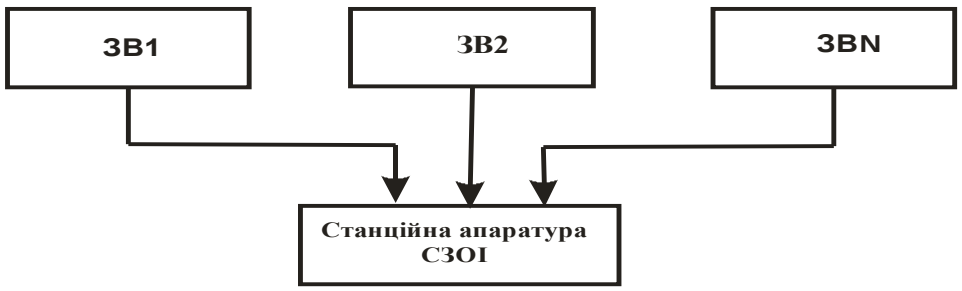

Рис. 2.1. Радіальне (променеве) безконцентраторне з'єднання станційної апаратури із ЗВ

– 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;

Шлейфовий (магістральний) без концентраторів (рис. 2.1) і з концентраторами (рис. 2.3) .

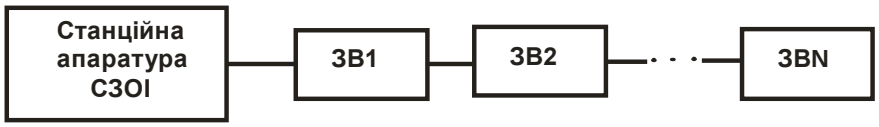

Рис. 2.2. Шлейфове (магістральне) без концентраторів з'єднання станційної апаратури із ЗВ

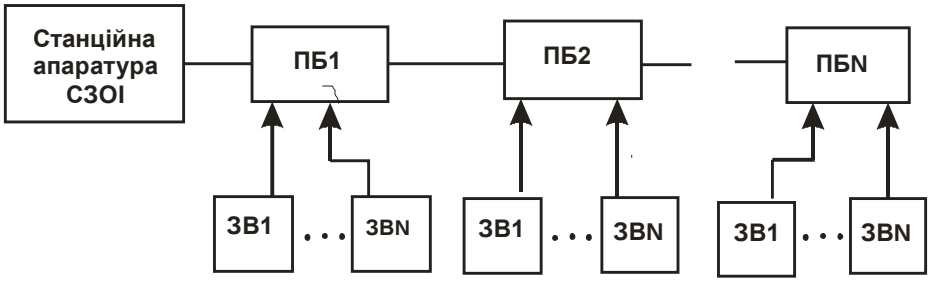

Рис. 2.3. Шлейфове (магістральне) з концентраторами з'єднання станційної апаратури з ПБ і ЗВ

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 [11]. 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).

Змішана (радіально-шлейфова) або деревовидна структура (рис. 2.3).

Дана структура СЗОІ є комбінацією технічних засобів, сполучених по радіальній і шлейфовій схемам.

Необхідно відзначити, що вказані способи зв'язку периферійних блоків і ЗВ із станційною частиною СЗОІ можуть бути використані і дляорганізації зв'язку ЗВ з ПБ. Зв'язок ПБ із ЗВ також може бути організований за допомогою локальної мережі, що має шлейфову або деревовидну структуру. Для включення ЗВ на загальну магістраль локальної мережі необхідна розробка спеціальних блоків сполучення, що встановлюються поряд з кожним ЗВ і служать буфером між мережею і стандартизованими вихідними/вхідними ланцюгами ЗВ у вигляді контактів реле. Проте, часто вартість такого пристрою може бути сумірна з вартістю деяких ЗВ і перевищуватиме виграш у вартості, що отримується за рахунок скорочення довжини кабелів зв'язку.

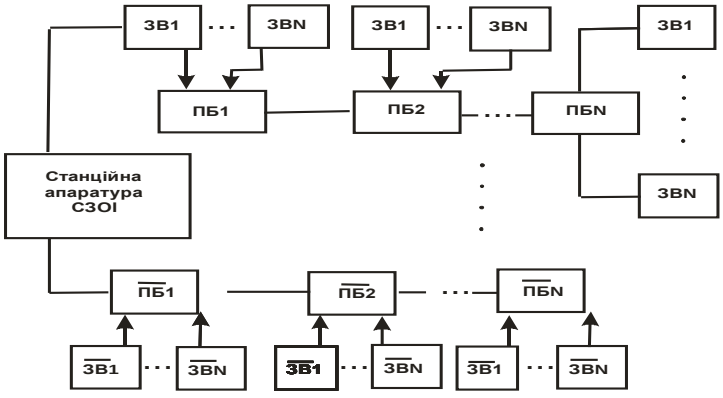

Рис. 2.4. Змішане (радіально-шлейфове) з'єднання станційної апаратура з ПБ і ЗВ

2.3. Засоби охорони зовнішніх меж об’єктів інформаційної діяльності

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 [12]. Такі рубежі (або зони безпеки) повинні розташовуватися послідовно - від огорожі навколо території об'єкту до головного, особливо важливого приміщення і інші (рис.2.4).

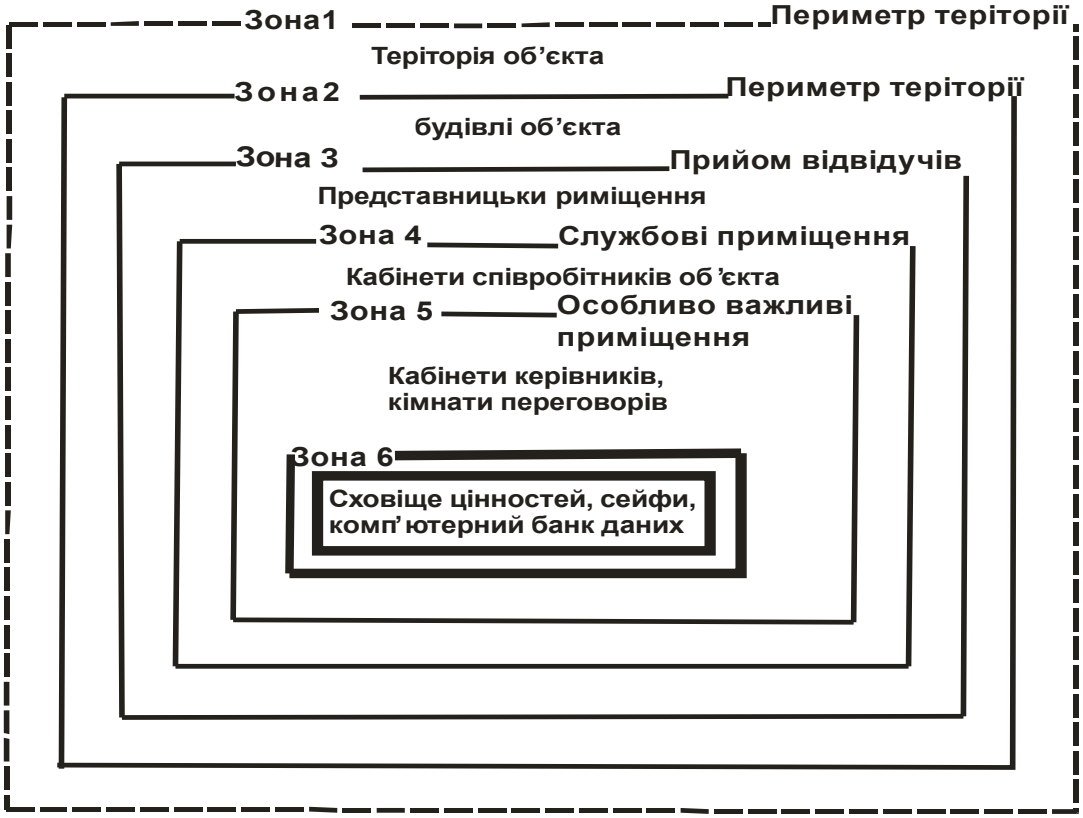

Рис.2.5. Розташування зон безпеки

Для захисту зовнішніх рубежів використовують такі засоби виявлення [13]:

– активні інфрачервоні засоби виявлення;
– сейсмічні засоби виявлення;
– ємнісні сповіщувачі;
– системи відеоспостереження.

2.3.1. Активні інфрачервоні системи

Розробка вітчизняних активних ІЧЗВ ведеться з початку 60-х рр. У перших розробках як джерела випромінювання використовувалися лампи розжарювання. Модуляція випромінювання в цих виробах здійснювалася за допомогою механічних модуляторів. Такі ІЧЗВ мали низьку ефективність, великі габаритні розміри і значні струми споживання.

Оптична система джерела випромінювання (скорочено передавача - ПРД) створює вузьконаправлений промінь ІЧ-випромінювання. Як джерело ІЧ-випромінювання використовують напівпровідникові випромінюючі діоди з робочою довжиною хвилі 0,94 мкм, які розташовують у фокусі оптичної системи.

ІЧ-випромінювання фокусується оптичною системою ПРМ на чутливий майданчик фотоприймачів (фотодіодів). Отримувані з них імпульси фотоструму посилюються і поступають на пристрої обробки для формування сигналів тривоги.

Залежно від кількості променів і їх розташування (горизонтальне або вертикальне) ІЧЗВ можуть виконувати різні тактичні завдання. Горизонтальне розташування двох променів дозволяє за рахунок тимчасової обробки сигналів визначати напрям руху порушника. Вертикальне розташування променів в активних ІЧЗВ підвищує надійність блокування рубежів і периметрів в порівнянні з однопроменевими ЗВ.

Конвективні завади обумовлені дією потоків повітря, що переміщаються, наприклад протягів при відкритій кватирці, щілин у вікні, а також побутових опалювальних приладів – радіаторів і кондиціонерів. Потоки повітря викликають хаотичну флуктуаційну зміну температури фону, амплітуда і частотний діапазон якого залежать від швидкості потоку повітря і характеристик фонової поверхні.

Електричні завади виникають при включенні будь-яких джерел електро- і радіовипромінювання, вимірювальної і побутової апаратури, освітлення, електродвигунів, радіопередавальних пристроїв, а також при коливаннях

струму в кабельній мережі і лініях електропередач. Значний рівень перешкод створюють також розряди блискавок.

Чутливість піроприймача дуже висока – при зміні температури на 1°С вихідний сигнал безпосередньо з кристала складає долі мікровольта, тому наведення від джерел завад в декілька вольт на метр можуть викликати завадовий імпульс, в тисячі разів більший за корисний сигнал. Проте велика частина електричних завад має малу тривалість або крутий фронт, що дозволяє відрізнити їх від корисного сигналу.

Власні шуми піроприймача визначають найвищу межу чутливості ІЧЗВ і мають вигляд білого шуму. У зв'язку з цим методи фільтрації тут не можуть бути використані. Інтенсивність завади збільшується при підвищенні температури кристала приблизно в два рази на кожні десять градусів. Сучасні піроприймачі мають рівень власних шумів, що відповідають зміні температури на 0,05...0,15°С

Рис.2.6. Активні інфрачервоні засоби виявлення

2.3.2. Сейсмічні системи

В даний час при організації охорони території, разом з іншими типами засобів виявлення, достатньо широко застосуються сейсмічні засоби виявлення (СЗВ), в яких реєструються і потім обробляються сигнали, що виникають в ґрунті (або іншій підстилаючій поверхні) при перетині людиною зони, що

охороняється. До основних переваг СЗВ відносяться відсутність власного випромінювання, можливість повного усунення демаскуючих ознак на ділянці, що охороняється, за рахунок установки лінійної частини (чутливих елементів і сполучних кабелів) в грунт. Сейсмічні засоби виявлення, будучи пасивними засобами охорони, не виявляються електронними засобами розвідки. Візуально приховані СЗВ різко знижує вірогідність їх подолання навіть при обізнаності порушника про принципи роботи і ТТХ засобу. Сейсмічні засоби зручні для блокування ділянок на нерівній місцевості і широко застосовуються в цілях охорони протяжних рубежів держкордону і периметрів об'єктів.

Як чутливі елементи, що перетворюють сейсмічні коливання ґрунту в електричні сигнали, найчастіше використовуються сейсмоприймачі (СП). Невеликі масогабарітні показники СП у поєднанні з простими методами обробки сигналів дозволили створити портативні автономні засоби блокування малих ділянок місцевості радіусом до 5 м. Такі засоби застосовуються для блокування підходів до місць тимчасового базування спецгруп, для виявлення груп людей і техніки на шляхах їх вірогідного пересування.

До недоліків СЗВ в цілому, а особливості тих, які не використовують складних алгоритмів обробки, відносяться низька перешкодостійкість при заданій вірогідності виявлення ($Р_{виявл}$ > 0,9. . .0.95) в умовах дії різноманітних сейсмічних перешкод (наприклад, від літаків, автотранспорту, промислових підприємств, дощу, вітру і тому подібне).

2.3.3. Ємнісні засоби

Сповіщувач охоронний ємнісний поверхневий для периметрів СО-03 призначений для роботи в системах охорони периметрів об'єктів, складських приміщень, кімнат, сейфів і ін., в яких як чутливий елемент використовують:

а) сигналізаційні загородження, відповідно до ОС-058.00.000 ИЭ, виконані у вигляді наступних конструкцій:

- металева сітка або ґрати, закріплені на опорах (типу «С»); - система проводів, закріплених на опорах (типу «К»);

- козиркові системи («КФ-1», «КИ», «КС-1», «КС-2»);

- системи типу «Кольцо» і «Цилиндр»;

- двостулкові залізничні й автомобільні ворота, хвіртки;

б) до 8 різних пристроїв, що мають вихідний сигнал типу «сухий контакт» (замкнено-розімкнено):

- датчики на ІЧ-променях, датчики присутності;

- кінцеві перемикачі воріт, хвірток.

Сповіщувач за допомогою комплекту перехідників та кронштейнів може бути підключений замість приладів Радиан-М, Радиан-А, СО-02. У порівнянні із зазначеними приладами, сповіщувач має розширені діапазони вибору чутливості і порогів спрацювання, розвинену багаторівневу систему автопідстроювання на постійні збуджуючі фактори та інтелектуальну режимі ретрансляції й повного дуплексу (4-х проводний режим). Сповіщувач також має релейний вихід, який використовують в системах охоронної сигналізації при заміні приладів типу РАДИАН.

Сповіщувач виконаний на основі сучасної інтегральної однокристальної мікро-ЕОМ, котра за рахунок автоматичного вибору режимів забезпечує надійну роботу при несприятливих погодних умовах (туман, дощ, снігопад, грозові розряди), у безпосередній близькості від залізниць та автомобільних магістралей, перехресних ЛЕП, при прольоті й посадці на огорожу птахів.

Сповіщувач автоматично настроюється на постійні вхідні параметри об'єкта та автоматично здійснює тестування основних функціональних вузлів з передачею діагностичної інформації обробку сигналів, що дозволяє понизити ступінь помилкових спрацьовувань і локалізувати ділянки системи захисту (далі – СЗ) - ліве плече СЗ - праве плече СЗ , що полегшує обслуговування контрольованого рубежу.

Більше розвинена система індикації (2 семисегментних світлодіодних індикатори), у порівнянні із сигналізатором СО-02, дозволяє оперативно контролювати ситуацію у випадку автономного застосування сповіщувача (рис. 2.7).

Сповіщувач підключається до системи охоронної сигналізації, в складі якої є персональна ЕОМ, через фізичний інтерфейс типу RS-485 через канал зв'язку. Програмно-апаратні засоби сповіщувача дозволяють при роботі (як автономно, так і в складі системи охоронної сигналізації) дистанційно контролювати його роботоздатність, керувати основними режимами: чутливістю, величинами напруги на СЗ і порогів спрацювання, робочою частотою (5,4 кГц чи 10,8 кГц) і т.д.

Рис.2.7. Ємнісні сповіщувачі

2.4. Засоби охорони внутрішніх меж об’єктів інформаційної діяльності

Розглянемо такі засоби охорони приміщень:

– пасивні інфрачервоні засоби виявлення;
– магнітоконтактний сповіщувач;
– радіопроменевій сповіщувач;
– сповіщувачі розбиття скла;
– комбінований інфрачервоний сповіщувач руху та розбиття скла.

2.4.1. Отико-електронні засоби

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.

Сучасні ПІЧ-сповіщувачі використовують цифрову обробку сигналів, здійснюють постійний самоконтроль, розрізняють сигнали від домашніх тварин і реальних порушників, мають підвищену стійкість до впливу різних дестабілізуючих факторів (радіозавад, сонячного світла і т.п.). З огляду на те, що при таких можливостях ці пристрої мають цілком прийнятні ціни, вони можуть використовуватися для охорони найрізноманітніших по тактиці охорони і необхідному рівню безпеки об'єктів (рис. 2.8).

Рис.2.8. Пасивні інфрачервоні засоби виявлення

2.4.2. Магнітоконтактні пристрої

Магнітоконтактний сповіщувач містить у собі два основних елементи. Перший елемент – це геркон, що складається з герметичної колби, у якій знаходяться пластини з контактами, які мають малий опір. До пластин під'єднані провідники, 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 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.

Контакти звичайно покриваються спеціальним сплавом, наприклад, родієвим, що забезпечує малий опір і тривалий термін служби.

На цей час фірми-виробники випускають різноманітні типи МКС, які розрізняються за: способом встановлення, місцем використання, конструктивним виконанням, основними параметрам і іншими ознаками.

Стійкість до вібрацій і ударних навантажень.

Це досить важливий параметр, що впливає на імовірність помилкового спрацьовування. Стійкість до вібрацій і ударних навантажень пояснюється тим, що при деяких впливах можливі короткочасні розмикання контактів.

Типові параметри, що характеризують стійкість МКС: при вібрації в діапазоні 10...2000 Гц і прискоренні до 30 g тривалість замикання чи розмикання контактів не перевищує 20 мс; те ж саме буде і при ударних навантаженнях 100 g тривалістю 11 мс

Робочий зазор.

Робочий зазор визначає мінімальну відстань, на якій відбувається замикання контактів геркона (рис.2.9 *а*). Величина робочого зазору змінюється в залежності від взаємного розташування геркона і магніта.

При зсуві магніта в бік величина зазору зменшується (рис 2.9 *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. 2.10).

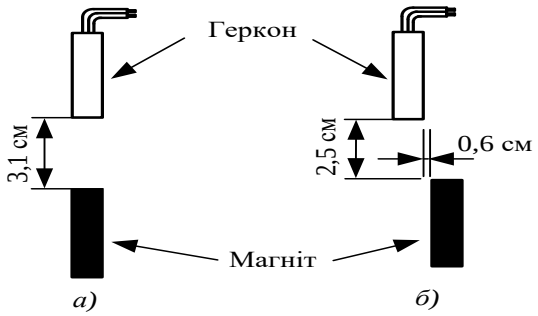

Рисунок 2.9. Робочий зазор МКС

Зазор відпускання

Визначає величину зазору, при якому відбувається розмикання контактів геркона. Бувають випадки коли зазори замикання і розмикання співпадають (МКС типу MPS-45WG).

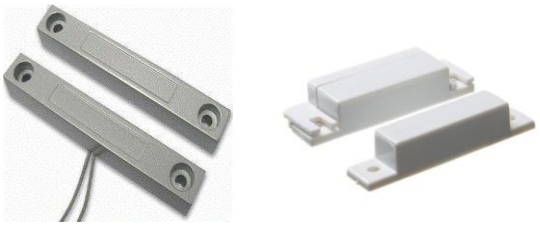

Рис.2.10. Зовнішній вигляд магнітоконтактного сповіщувача

2.4.3. Радіопроменеві сповіщувачі

Пристрій і спосіб забезпечують сигнальне блокування об'єктів, що охороняються, при вторгненні сторонніх осіб на протяжних ділянках периметра до 500 м відкритій місцевості і в умовах міської забудови, протяжністю до 100 м. Пристрій реєструє створюються тілом людини обурення мікрохвильового електромагнітного поля, що посилається спрямованими антенами від передавача до приймача. На протяжних ділянках відкритій місцевості, довжиною понад 100 м, в антенах встановлюється знімне дзеркало з вертикальним розміром апертури до 0,75-1,5 м, що дозволяє сформувати практично плоску зону виявлення забірного типу і багаторазово послабити помеховое вплив підстилаючої поверхні, дрібних птахів і тварин. Спосіб установки дзеркала на місцевості і взаємного розміщення опромінювача дзеркала дозволяє використовувати в конструкції укорочену лінійну фазированную ґрати випромінювача завдовжки не більше 0,2-0,3 м, конструктивно об'єднану з корпусами передавача і приймача в портативні антенні відповідно приймальний і передавальний модулі.

На ділянках міської забудови (огорожі, будівлі, вхідні портали, об'єм приміщень) великогабаритні дзеркала видаляються, а антена має підвищену надійність електричних контактів і простоту установки. У блок-схему пристрою введені генератор пачок імпульсів, видеоусилитель і видеодетектор, що дозволяє знизити споживану і випромінювану енергію. Укорочена лінійна решітка дозволяє використовувати пристрій в діапазоні частот до 50-70 ГГц. Винахід відноситься до галузі охоронної сигналізації і хвилеводної техніки НВЧ, зокрема, до пристроїв і способів для формування радіопроменевій зони між рознесеними в просторі передавачем і приймачем НВЧ поля виявлення людини, вторгающегося в цю зону.

Радіопроменеві сповіщувачі (системи, сенсори, датчики) широко відомі в техніці охорони. Зону виявлення формують з допомогою антен, встановлених на протилежних сторонах охороняється кордону і спрямовуються зустрічно максимумами діаграм спрямованості.

Спосіб формування антени на рубежі визначає просторові розміри зони. Якщо розміри випромінюючої апертури антени менше 0,2-0,3 м, то при використанні пристрою на протяжних рубежах охорони антени встановлюють на висоті 1,0-1,5 м над грунтом. Від місця установки антени до місця торкання радиолучом ґрунту існує "мертва зона" по виявленню. Відомий недолік усувають шляхом збільшення до 1,0-1,5 м вертикального розміру апертури антени і установкою нижнього краю апертури над рівнем грунту. При цьому багаторазово зростає відношення корисний сигнал/завада, зникають "мертві зони".

Рис. 2.11. Радіопроменеві сповіщувачі

2.4.4. Пристрої реєстрації розбиття скла

Акустичні сповіщувачі розбиття скла є найбільш розповсюдженими на цей час. Це викликано рядом їхніх переваг, таких як відсутність якихось елементів на контрольованих поверхнях скла, можливість контролювати кілька вікон одним сповіщувачем та ін. Тому зупинимося докладніше на особливостях акустичних коливань, що виникають при розбитті скла.

Як відомо, при руйнуванні скла виникають акустичні коливання різних частот. У перший момент при ударі по склу воно деформується. Ця деформація, тобто вигин скла, викликає появу акустичних коливань низьких частот (рис. 1*а*). Коли величина деформації досягає граничного значення, відбувається механічне руйнування скла. Останнє супроводжується акустичними коливаннями високих частот. Причому для виявлення факту розбиття скла

потрібно враховувати і те, що ці звукові коливання з’являються у визначеному часовому інтервалі.

Після удару виникають коливання, спектр яких поширюється до частот близько 25 кГц. При цьому низькочастотні складові зосереджені головним чином в області частот десятків і сотень герц і пов'язані з деформацією скла в момент удару. Ці складові мають максимальну амплітуду в перші 200-300 мс і потім поступово загасають у часі.

Практично відразу після удару виникає широкополосне коливання, що обумовлене механічним руйнуванням скла. Ці високочастотні складові досить швидко загасають у часі.

Через декілька сот мілісекунд знову виникають високочастотні коливання зі спектральними складовими в області 3-20 кГц. Ці складові викликані акустичними коливаннями, що виникають при падінні осколків скла на підлогу і їхньому подальшому руйнуванні.

На сьогодні широко використовуються акустичні сповіщувачі, які реєструють звукові коливання, що виникають при руйнуванні скла. Такий принцип використовується в сучасних акустичних сповіщувачах. Це забезпечує такі важливі переваги, як відсутність будь-яких елементів на контрольованих поверхнях скла, можливість контролювати декілька вікон одним сповіщувачем та інші.

Як згадувалося вище, при руйнуванні скла виникають акустичні коливання різних частот. У перший момент при ударі по склу воно деформується. Ця деформація, тобто вигин скла, викликає появу акустичних коливань низьких частот. Коли величина деформації досягає визначеного розміру, відбувається механічне руйнування скла. Воно супроводжується акустичними коливаннями високих частот. У такий спосіб для виявлення факту розбиття скла потрібно реєструвати звукові коливання визначеного спектрального складу і звукові коливання, які з’являються один за одним в деякому часовому інтервалі.

У найпростішому випадку акустичний сповіщувач складається з мікрофона М, фільтра Ф, що виділяє найбільш типові спектральні складові сигналу, схеми обробки СО і виконавчого елемента – реле Р (рис. 2.11).

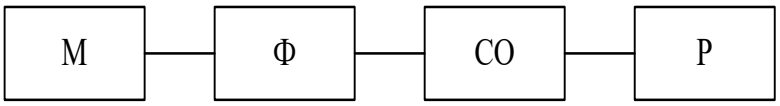

Рис. 2.12. Склад сповіщувача розбиття скла

У сучасних акустичних сповіщувачах використовуються наступні алгоритми обробки акустичного сигналу.

Одноканальні граничні алгоритми.

Структурна схема найпростішого акустичного сповіщувача, що використовує одноканальний пороговий алгоритм, зображена на рис. 2.11.

Схема обробки такого пристрою містить у собі підсилювач, детектор і пороговий пристрій. У розглянутому сповіщувачі смуга пропускання фільтра повинна бути досить широкою, щоб пропускати всі основні спектральні складові сигналу розбиття скла.

З мікрофона можуть надходити сигнали, обумовлені акустичними коливаннями, викликаними різними причинами. Спектральний склад цих коливань буде істотно відрізнятися. Тому можуть мати місце помилкові тривоги. Однак, реєстрація тривоги (помилкової) може мати місце й в інших випадках, коли присутні тільки сигнали достатньої інтенсивності, у спектрі яких є або тільки низькочастотні, або тільки високочастотні складові. У такий спосіб при деякій привабливості, викликаній простотою і, отже, більш низькою ціною, такі сповіщувачі значно поступаються у функціональних характеристиках. Зокрема, вони в значно більшому ступені піддаються впливу джерел помилкових тривог.

Звуження смуги пропускання фільтра дозволить знизити імовірність помилкових тривог. Але при цьому падає й імовірність правильного виявлення.

Двоканальні граничні алгоритми

Реєстрація послідовності акустичних коливань, що відповідають деформації скла (низькочастотні коливання) і його руйнуванню (високочастотні), покладена в основу принципу дії більшості сучасних акустичних сповіщувачів розбиття скла. Прийняті роздільно у визначеній часовій послідовності ці сигнали порівнюються по інтенсивності з фіксованими значеннями порогових рівнів для кожного виду коливань. При їхньому перевищенні сповіщувач фіксує тривогу.

Принцип двоканальної обробки дозволяє істотно зменшити число помилкових спрацьовувань у порівнянні з одноканальним, котрий може бути викликаний звуковими коливаннями іншого походження. Наприклад, падіння зв'язки ключів викликає тільки високочастотні звукові коливання, що не приводять до спрацьовування сповіщувача.

Багатопараметричні алгоритми

Подальше підвищення надійності виявлення при одночасному зниженні імовірності помилкових тривог можливе при використанні багатопараметричних алгоритмів. При цьому використовується більш тонкий, детальний аналіз декількох параметрів сигналів. Реально реалізація подібних алгоритмів стала можливою при використанні цифрової обробки сигналів. Зрозуміло, що використання багатопараметричних алгоритмів повинне виконуватися в сполученні з багатоканальною (по частоті) обробкою. Звичайно це двоканальна обробка.

Основна особливість і проблема використання багатопараметричних алгоритмів – це вибір аналізованих параметрів сигналів, які будуть аналізуватися. Ці параметри повинні, з одного боку, бути типовими для контрольованого класу скла і, з іншого боку, відрізнятися від відповідних параметрів сигналів джерел помилкових тривог.

Мікропроцесор містить чотири аналогово-цифрових перетворювачі аналогових сигналів, прийнятих мікрофоном, у цифрову форму. Програма обробки акустичних сигналів складається з 1019 команд і виконується в

центральному блоці мікропроцесора. Програма записується в пам'ять мікропроцесора. Інші види сповіщувачів використовують ПЗУ, які перепрограмовуються, що не виключає імовірності втрати інформації. Цифровий сигнал, прийнятий мікрофоном, порівнюється по восьми параметрам із пороговими значеннями. Тільки при виконанні даних восьми умов сповіщувач зафіксує тривогу.

2.4.5. Комбіновані охоронні пристрої

Датчик руху та розбиття скла призначений для відстеження руху людини в приміщенні, що охороняється і детектування ударів по склу та розбиття скла. Принцип дії сенсора руху заснований на визначенні інфрачервоного (ІЧ) випромінювання. Кожна жива істота - джерело ІЧ випромінювання. Як тільки сповіщувач починає ІЧ-випромінювання в межах охоронної зони, він відсилає сигнал тривоги на центральний блок охоронної сигналізації. У датчику реалізований імунітет від тварин вагою до 25 кг і висотою до 1 м, спрацювання генерується тільки при русі людини. Якщо в приміщенні впаде який-небудь предмет, пробіжить кішка сповіщувач не спрацює.

Вбудований електретний мікрофон дозволяє виявити удари по склу та розбиття скла. При цьому використовується захист від помилкових спрацьовувань. Вхідний звук аналізується поетапно. Для включення тривоги спочатку повинні бути зроблені низькочастотні звуки (удар по склу), а потім - високочастотні (звук скла, що розбивається), тільки після цього відправиться сигнал тривоги.

Комбінований сповіщувач руху та розбиття скла використовується для охорони практично всіх об'єктів: заміських будинків, дач, офісів, торгових залів, квартир. Сповіщувач руху - один з найпоширеніших елементів охоронних сигналізацій.

Рис.2.13. Комбіновані інфрачервоні сповіщувачі руху та розбиття скла

2.5. Прилади реєстрації тривожних сигналів

Прилади приймально-контрольні й контрольні панелі відносяться до технічних засобів контролю і реєстрації інформації. Вони призначені для безперервного збору інформації від сповіщувачів, включених в шлейф сигналізації, аналізу тривожної ситуації на об'єкті, формування та передачі сповіщень про стан об'єкта на пульт централізованого спостереження, а також управління місцевими світловими і звуковими сповіщувачами і індикаторами. Крім того, прилади забезпечують здачу і зняття об'єкта з охорони за прийнятою тактикою, а в ряді випадків - електроживлення сповіщувачів. Прилади є основними елементами, що формують на об'єкті інформаційно-аналітичну систему охоронної або охоронно-пожежної сигналізації. Така система може бути автономною або централізованою. При автономній охороні прилади встановлюються в приміщенні (пункті) охорони, який розміщується на об'єкті або в безпосередній близькості від нього. При централізованій охороні об'єктовий комплекс технічних засобів, що формується одним або декількома приладами, утворює об'єктову підсистему охоронно-пожежної сигналізації, яка за допомогою системи передачі сповіщень передає в заданому вигляді інформацію про стан об'єкта на пульт централізованого спостереження, що розміщується в центрі прийому сповіщень про тривогу (пункті централізованої

охорони). Інформація, яка формується приладом, як при автономної, так і централізованої охорони передається співробітникам спеціальних служб забезпечення охорони об'єкта, на яких покладено функції реагування на тривожні повідомлення, що надходять з об'єкта.

З метою підвищення достовірності одержуваної інформації при організації контролю стану об'єкта за допомогою технічних засобів застосовують багаторубежеві комплекси охоронної сигналізації. Кожен з рубежів сигналізації являє собою сукупність послідовно об'єднаних електричним колом (шлейфом сигналізації) спільно діючих технічних засобів охоронної сигналізації, що дозволяє видати повідомлення про проникнення (спробі проникнення) в зону, що охороняється (зони) незалежно від інших технічних засобів, який не входять в даний ланцюг. При цьому в кожен рубіж сигналізації включають сповіщувачі, засновані на різних принципах дії.

Крім здачі під охорону і зняття об'єкта (приміщення) з охорони за прийнятою тактикою, зазвичай забезпечують електроживлення сповіщувачів.

Прилади приймально-контрольні класифікуються за:

– інформаційної ємності (кількість контрольованих шлейфом сигналізації) на прилади малої (до 5 ШС), середньої (від 6 до 50 ШС) і великий (понад 50 ШС) інформаційної ємності;

– інформативності - можуть бути малої (до 2 видів повідомлень), середньої (3 ... 5 видів) і великий (понад 5 видів) інформативності.

За кількістю напрямків передачі інформації вони поділяються на системи з одно- і двобічної передачею інформації (з наявністю зворотного каналу).

За способом відображення надходить на пульт централізованого спостереження інформації системи передачі сповіщень підрозділяються на системи з індивідуальним або груповим відображенням інформації у вигляді світлових і звукових сигналів, з відображенням інформації на дисплеї з застосуванням пристроїв обробки та накопичення бази даних.

Шлейф сигналізації - це електричний ланцюг, що з'єднує вихідні ланцюги сповіщувачів, що включає в себе допоміжні елементи (діоди, резистори і т.п.),

з'єднувальні дроти і коробки та призначена для видачі сповіщень про проникнення, спробу проникнення, пожежі, несправності, а в деяких випадках і для подачі електроживлення на сповіщувачі. Таким чином, шлейф сигналізації призначений для контролю стану деякої зони, що охороняється.

Зона охорони - це частина об'єкту, що охороняється, контрольована одним або декількома шлейфами сигналізації.

Сучасні багатофункціональні КП мають широкі можливості по організації систем охоронної, пожежної та охоронно-пожежної сигналізації. Знання цих можливостей дозволить зробити правильний вибір КП, характеристики і параметри якої найбільш повно задовольняють вирішення поставлених завдань з охорони конкретного об'єкта.

Робота КП може здійснюватися в різних режимах, а саме: охорона, спостереження (зняття з охорони), програмування.

Режим "охорона".

У цьому режимі КП контролює свої параметри і стан шлейфів. Порушення шлейфів призводить до формування сигналів тривоги. При цьому можливі наступні різновиди режиму:

- повна охорона - КП контролює стан всіх шлейфів і самого себе.
- часткова охорона з контролем частини шлейфів і самій КП.

Процедура взяття об'єкта під охорону і зняття з охорони відноситься до тактичних параметрах і може розділятися на такі різновиди:

- автоматична постановка під охорону.
- постановка на охорону з затримкою на вихід.
- постановка на охорону без затримки на вихід.

Режим "спостереження (знято з охорони)"

У режимі «спостереження» КП знятий з охорони, але продовжує контролювати всі шлейфи і самого себе (рис. 2.13).

Шлейф сигналізації є однією з необхідних складових частин технічної системи охорони. Практика показує, що однією з основних причин нестійкої роботи приладів ТСО на об'єкті є порушення шлейфу сигналізації, які

представляють собою відмову у вигляді обриву або короткого замикання в шлейфі. Не повинна виключатися також можливість умисного втручання в електричний ланцюг шлейфу з метою порушення його правильного функціонування (саботаж).

Рис. 2.14. Зовнішній вигляд ППКОП

Існують три методи контролю шлейфу сигналізації:

- з живленням шлейфу сигналізації постійним струмом і використанням у якості виносного елементу резистора;
- з живленням шлейфу сигналізації знакозмінною імпульсною напругою і використанням у якості навантаження послідовно з'єднаних резистора та напівпровідникового діода;
- з живленням шлейфу сигналізації імпульсною напругою і використанням у якості виносного елементу конденсатора.

Прилади й пульти приймально-контрольні пожежні призначені для живлення пожежних сповіщувачів по шлейфах пожежної сигналізації, прийому тривожних сповіщень від пожежних сповіщувачів, контролю пожежних шлейфів на обрив і коротке замикання, формування повідомлень «Пожежа» і

«Несправність», формування сигналів включення систем пожежогасіння та димовидалення , а також для передачі цих повідомлень на пульт централізованого спостереження або інші ППК.

Основними характеристиками пожежних ППК, також як і охоронних, є інформаційна ємність і інформативність.

Сигнально-пускові пристрої - це, по суті, ті ж прилади приймально-контрольні, які доповнені можливістю формування сповіщення «Увага» при спрацьовуванні одного пожежного сповіщувача, сповіщення «Пожежа» при спрацьовуванні не менше двох пожежних сповіщувачів, регульованою затримкою сигналу пуску систем пожежогасіння, можливістю управління системами оповіщення про пожежу. Відмінною особливістю ППК даного покоління приладів є променева структура побудови систем пожежної сигналізації та використання неадресних, порогових пожежних сповіщувачів, які самі приймають рішення про пожежу, як тільки контрольований ними параметр виходить за рамки допустимого значення.

Виносний пристрій оптичної сигналізації (ВПОС) призначений для дублювання оптичного сигналу спрацьовування пожежних сповіщувачів, візуальний оперативний доступ до яких утруднений. ВПОС рекомендується використовувати для визначення сповіщувача, який подав повідомлення «Пожежа», і встановлювати в доступному для огляду місці, наприклад в коридорі над дверима приміщення, що охороняється.

Системи пожежної сигналізації діляться на три класи: неадресні системи, адресні і адресно-аналогові пожежні системи.

Головна їхня відмінність це метод, за яким система приймає рішення про тривожну ситуацію, тобто про пожежу. У неадресних і адресних системах це рішення приймається безпосередньо самими встановленими пожежними сповіщувачами і потім тривожний сигнал передається на приймально-контрольоване обладнання і на підставі цього сигналу з сповіщувача включається система пожежогасіння.

Спроби виявити загоряння на ранній стадії шляхом зниження порогів чутливості точкових димових сповіщувачів зазвичай призводять до помилкових спрацьовувань пожежної сигналізації і хибним пусків систем пожежогасіння. Постійний пошук компромісу між раннім виявленням і хибним пуском.

В адресно-аналогових системах принцип прийняття рішення про виникнення пожежі зовсім інший. На приймально-контрольне обладнання передається значення контрольованого сповіщувачем параметра (температура, задимленість в приміщенні). Головне обладнання постійно відстежує стан навколишнього середовища в усіх приміщеннях будівлі і відстежує динаміку зміни зазначених параметрів. На підставі цих даних приймає рішення не тільки про формування сигналу «Пожежа», а й сигналу «Попередження». Тобто адресно-аналогова система пожежної сигналізації побудована на ухваленні рішення про тривогу не окремими пожежними датчиками, а приймально-контрольним обладнанням на основі динаміки зміни даних, що надходять з сповіщувачів. Адресно-аналогові системи, постійно контролюючи стан середовища в приміщенні, негайно виявляють зміну температури або задимленість і видають черговому попереджуючий сигнал.

Раннє виявлення спалаху дозволяє своєчасно евакуювати людей ще на початковій стадії пожежі і провести запуск автоматичної установки пожежогасіння. Попутно вирішується так само ряд важливих завдань, наприклад, контроль працездатності сповіщувачів. Так, в адресно-аналогової системі в принципі не може бути несправного сповіщувача, що не виявленого приймально-контрольним приладом, так як весь час сповіщувач повинен передавати певний сигнал. Якщо до цього додати потужну самодіагностику самих сповіщувачів, автоматичну компенсацію запиленості та виявлення запилених димових сповіщувачів, то стає очевидним, що ці чинники тільки підвищують ефективність адресно-аналогових систем.

Висновок по розділу. Встановлено: існують дві основні схеми побудови технічної системи охорони – радіальна, шлейфова та їх різновиди.

Для охорони внутрішніх рубежів ОІД використовуються: магнітоконтактний сповіщувач, пасивний інфрачервоний, акустичний розбиття скла, комбінований сповіщувач. Для охорони зовнішніх меж ОІД застосовуються: активний інфрачервоний бар’єр, сейсмічні засоби, ємнісні засоби. Для реєстрації сигналів сповіщувачів застосовується прилад прийомо-контрольний охоронно-пожежний.

РОЗДІЛ 3
СТВОРЕННЯ ЕФЕКТИВНОЇ ТЕХНІЧНОЇ СИСТЕМИ ОХОРОНИ РЕЖИМНОГО ОБ'ЄКТУ

3.1. Якісний аналіз структур технічних систем охорони

У багатьох джерелах наведені приклади структур побудови ТСО, серед яких найбільшу практичну цінність мають радіальна та магістральна (шлейфова) структури. Структура ТСО є визначальною в питанні ідентифікації відповідного сповіщувача (об'єкта що охороняється) при прийнятті рішення про реагування на тривожне спрацювання сповіщувача. Проте ці дві структури побудови мають, як буде показано далі, свої характерні недоліки та переваги. запропонування нового методу ідентифікації сповіщувачів ТСО в охоронному шлейфі, який буде компромісним ефективним рішенням між радіальною та магістральною структурами. Перед висвітленням нового методу ідентифікації сповіщувачів в охоронному шлейфі, доцільно розглянути як здійснюється ідентифікація сповіщувачів в існуючих охоронних шлейфах.

На вибір варіанту структури побудови ТСО, в основному, роблять вплив наступні чинники;

– якісний і кількісний склад обслуговуваних ЗВ і периферійного обладнання (концентратори, виносні пульти сигналізації і ін);

– ступінь централізації управління ТСО;

– структурні особливості об'єктів, що охороняються;

– чинники вартості і надійності.

Радіальна (променева) структура побудови (рис. 3.1).

Комплекси ТСО з радіальною структурою мають наступні основні переваги:

– 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;

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

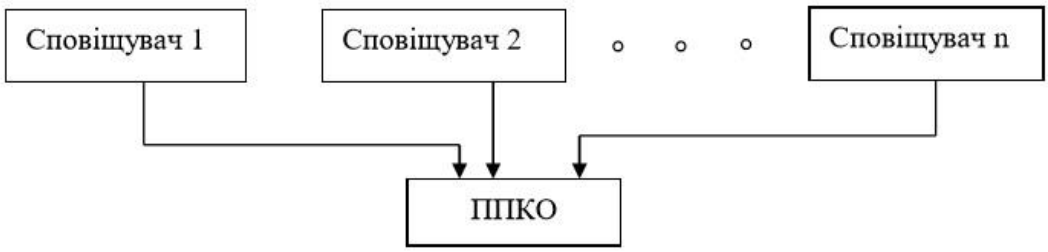

Рис. 3.1 Радіальне (променеве) з'єднання ППКО і сповіщувачів

Також властивий недолік:

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

Основна перевага комплексів з такою структурою – низька вартість сповіщувачів та ППКО.

Ідентифікація сповіщувачів у такий ТСО здійснюється за номером сполученої лінії між сповіщувачем та ППКО.

Шлейфова (магістральна) структура побудови (рис. 3.2).

Рис. 3.2. Шлейфове (магістральне) без концентраторів з'єднання ППКО із сповіщувачами

Працездатність комплексів ТСО з шлейфовою структурою у великій мірі визначається справним станом ліній зв'язку 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, що є недоліком системи. 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 недоліком є більша вартість апаратної частини, оскільки сигнали від сповіщувачів у системі передаються по однієї сполученої лінії і для ідентифікації сповіщувачів необхідно застосовувати спеціальні кодові пристрої, що й здорожує усю ТСО.

Проте у таких системах структура кабельних комунікацій менш розвинена, ніж у радіальних систем, що є перевагою при монтажі системи.

Результати якісного порівняння двох структур наведено у таблиці 3.1.

Таблиця 3.1.

Якісне порівняння структур систем

Тип структури	**Вартість системи**	**Час розгортання системи**	**Надійність системи**
Радіальна	Мала	Великий	Велика
Шлейфова	Велика	Малий	Мала

3.2. Спосіб підвищення ефективності технічної системи охорони режимного об'єкту

В основі нового методу, що пропонується, покладено використання шлейфової структури (рис. 3.2), але ідентифікація сповіщувачів здійснюється

не за рахунок використання кодових пристроїв, а шляхом виміру опору шлейфу ТСО який буде залежати від опору та кількості підключених до нього резисторів сповіщувачів. Структурна схема ТСО побудованої за таким методом приведена на рис. 3.3 Для детального розгляду методу доцільно структурну схему (рис. 3.3) відобразити принциповою електричною схемою (рис. 3.4).

Принцип роботи охоронних сповіщувачів визначає, що у стані спостереження, а саме у такому стані працює основний час сповіщувач, контакти виконавчого елементу сповіщувача замкнуті і відповідний резистор, що є невід'ємним елементом шлейфу підключений до шлейфу. У такому випадку опір усього шлейфу можна розрахувати за відомому виразом для випадку паралельного з'єднання резисторів:

$$\frac{1}{R_\Sigma} = \frac{1}{R_1} + \frac{1}{R_2} + \cdots + \frac{1}{R_n}$$

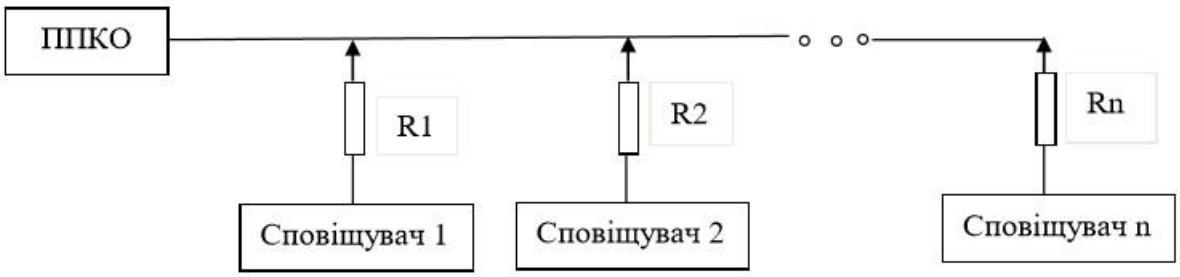

Рис. 3.3 Шлейфова структура з резисторами.

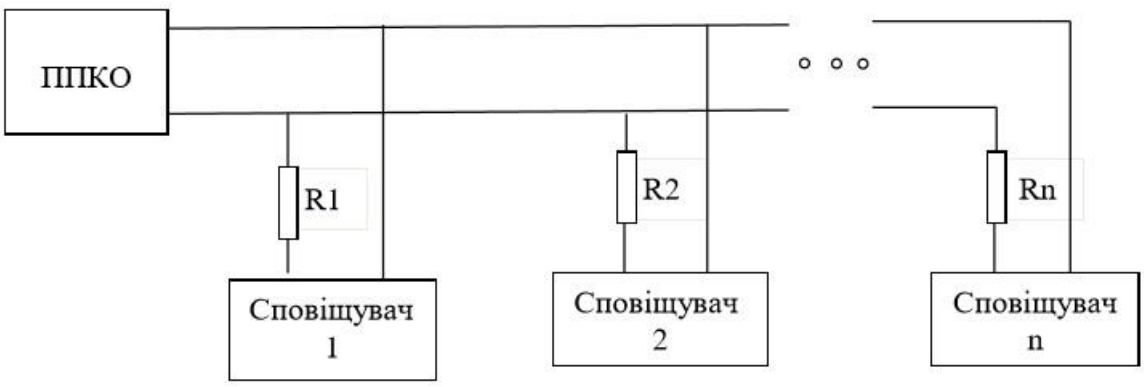

Рис. 3.4. Принципова електрична схема шлейфової структури з резисторами

У випадку спрацювання одного, або декількох сповіщувачів, контакти виконавчого елементу сповіщувача короткочасно (порядку 2 – 3 секунд) розмикаються і відповідний, або відповідні резистори відключаються від схеми на цей час. Це означає, що сумарний опір шлейфу буде змінюватися. Проте виникає питання, а як же ідентифікувати сповіщувач і відповідно об’єкт на якому він спрацював? Для виконання цього завдання необхідно використовувати у шлейфі резистори з різними неповторюваними опорами з прив’язкою до конкретного сповіщувача (об’єкта).

Припустимо що ТСО складається з чотирьох сповіщувачів. У такому випадку її еквівалентна електрична схема шлейфової структури з резисторами буде наступною (рис. 3.5).

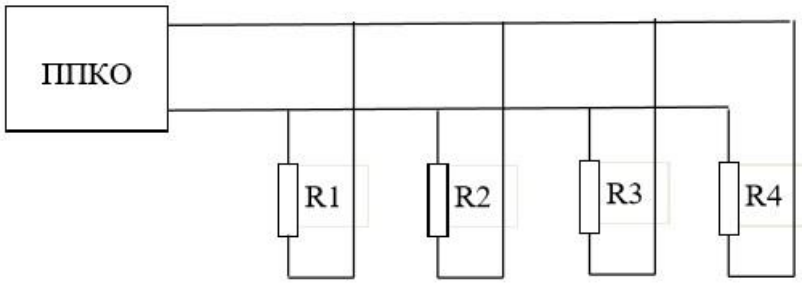

Рис. 3.5. Еквівалентна електрична схема шлейфової структури з резисторами

Припустимо, R1 = 1кОм; R2 = 2кОм; R3 = 3кОм; R4 = 4кОм. У такому випадку опір шлейфу у залежності від номеру (номерів) сповіщувачів, що спрацювали одночасно становитиме відповідні величини (табл.3.2).

Таким чином, як видно з таблиці, даний метод дозволить по опору шлейфу ідентифікувати сповіщувач який спрацював, а відповідно й об’єкт де виникла тривожна ситуація.

Використання даного методу дозволить зберегти таку позитивну якість шлейфової структури ТСО як малий час розгортання (табл. 3.1) та позбутися негативної якості – високої вартості системи.

Таблиця 3.2
Опір шлейфів залежно від схеми включення

N з/п	**№ R, що спрацювали**	**RΣ (кОм)**
1	1	1,1
2	1, 2	2,4
3	1, 3	1,5
4	1, 4	1,33
5	1, 2, 3	6
6	1, 2, 3, 4	∞
7	2	0,352
8	2, 3	0,857
9	2, 4	0,8
10	2, 3, 4	1
11	3	0,6
12	3, 4	0,666
13	4	0,571
14	-	0,522

При цьому слід зазначити, що дуже малоймовірний випадок, щоб у період часу тривалістю 2 – 3 секунди одночасно спрацювали усі n, або більшість сповіщувачів. З практичної точки зору ймовірніше спрацювання одного сповіщувача у такий малий проміжок часу і стосовно наведеного прикладу практичну значимість будуть мати випадки № 1, 7, 11, 13, 14. Проте не відкидаються й ймовірність одночасного спрацювання декількох сповіщувачів, але це напрям подальших досліджень.

Висновок по розділу. Запропоновано спосіб підвищення, на якісному рівні, ефективності технічної системи охорони об’єкту інформаційної діяльності. Використання даного методу дозволить зберегти таку позитивну якість шлейфової структури ТСО як малий час розгортання (табл. 1) та позбутися негативної якості як висока вартість системи.

ВИСНОВКИ

В даній магістерській атестаційній роботі зроблено огляд існуючих принципів та засобів охорони об’єктів інформаційної діяльності з використанням технічних засобів охорони.

Досліджено склад технічної системи охорони та завдання, які вирішує технічна система охорони на об’єктах інформаційної діяльності.

Досліджено існуючі структури побудови технічних систем охорони, якісні переваги та недоліки цих структур, принцип функціонування виконавчого елементу охоронного сповіщувача, принцип функціонування охоронного шлейфу.

На підставі цього зроблено висновок про можливість побудови охоронного шлейфу за новим принципом функціонування з відповідними перевагами порівняно зі шлейфами існуючих структур технічних систем охорони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України Про інформацію № 2657-XII від 2 жовтня 1992 року

2. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення

3. Гольдштейн Б. С., Пінчук А. В., Суховицкий А. Л. IP-телефония: Радио и связь, 2008.

4. Стів Мак-Квері, Келлі Мак-Грю, Стівен Фой. Передача голосових даних по мережах Cisco Frame Relay, ATM та IP; Київ, 2007.

5. Безпека інформаційно-комунікаційних систем М.В. Грайворонський, О.М. Новіков – К. : Вид.група BHV, 2009. – 608 с.

6. Б.С. Гольштейн, А. А. Зарубин, В. В. Саморезов. Справочник по телекоммуникационным протоколам: «Протокол SIP».2005.-456с.

7. Загрози, атаки і способи їх відображення. – Доступний з http://alls.in.ua/5414-ip-telefoniya-zagrozi-ataki-i-sposobi-h-vidobrazhennya.html

8.Сучасний стан захисту інформації. – Доступний з http://www.immsp.kiev.ua/publications/articles/2009/2009_2/Litvinov_02_2009.pdf

9. Сигналізація. – Доступний з http://www.znanius.com/3798.html?&L

10. Баричев С.Г. и др. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. 2001. – 144 с.

11. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. 2009. – 608 с.

12. http://bastion.lviv.ua/ua/shop/category/security/izveshchateli-ohrannye

13. http://www.bezpeka-shop.com/catalog/datchiki_20467/

14. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методы и средства защиты информации / Под ред. В.А. Хорошко. – К.: , 2010. –465 с.

15. Торокін А.О., Інженерно-технічний захист інформації: навч. Посібник для студентів які навчаються по спеціальностям у галузі інформаційної безпеки. – М.: Геліос АРВ, 2005. – 906 с.

16. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації / За ред. проф. В.О.Хорошка – К.: Видавництво НАУ, 2002. – 208с.

17. Синилов Вячеслав Григорьевич. Системы охранной, пожарной и охранно-пожарной сигнализации: Учебник – М.: Издательство: «Академия» 2006 г. – 512 с.

18. [Електронний ресурс] // Режим доступу: www.savitec.com.ua/ohrana/datchik-dvizheniya-ik-passivnyj-srp100.html