ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до магістерської роботи на тему:

«РОЗРОБКА МОДЕЛІ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ»

Виконав: студент 6 курсу, групи
РТДМ- 61
спеціальності
172 Телекомунікації і радіотехніка
(шифр і назва спеціальності)
Герасименко Д.В.
(прізвище та ініціали)

Керівник Дакова Л.В.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Нормоконтроль_____

Київ – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Кафедра Мобільних та відеоінформаційних технологій

Ступінь вищої освіти Магістр

Спеціальність 172 Телекомунікації і радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри МВТ
_____ Н.В. Руденко
_____ _____ 2021 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Герасименко Денису Вікторовичу

1.Тема роботи: «Розробка моделі організації захисту інформації в телекомунікаційних системах», керівник роботи Дакова Лариса Валеріївна, к.т.н., затверджені наказом вищого навчального закладу від 11.10. 2021 року №170.

2. Строк подання студентом роботи 15.12.2021р.

3. Вихідні дані до роботи:
   1. Модель систем захисту телекомунікаційної системи;
   2. Процес створення системи інформаційної безпеки за рахунок правильної оцінки ефективності прийнятих рішень;
   3. Науково-технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
   1. Виявлення потенційних загроз і каналів витоку інформації;
   2. Комплексна модель системи захисту інформації;
   3. Методи ефективності системи захисту.

5. Перелік графічного матеріалу (назва слайдів презентації):

1. Технічні канали витоку інформації;
2. Модель системи захисту інформації;
3. Вимоги до моделі СЗІ;
4. Структура і завдання органів, що забезпечують безпеку ІТ;
5. Напрями захисту формуються виходячи з конкретних особливостей ІС як об'єкту захисту;
6. Етапи створення систем захисту інформації;
7. Структура моделі оцінки СЗІ;
8. Взаємозв’язок систем показників якості в інформаційній системі.

6. Дата видачі завдання
20.09.2021р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1.	Підбір науково-технічної літератури	22.09.2021	Виконано
2.	Аналіз даних та їх класифікація	20.10.2021	Виконано
3.	Дослідження інформації про потенційні загрози та канали витоку	12.11.2021	Виконано
4.	Розробка комплексної моделі зистеми захисту інформації	25.11.2021	Виконано
5.	Розгляд методів ефективності системи захисту	02.12.2021	Виконано
6.	Висновки, вступ, реферат	10.12.2021	Виконано
7	Оформлення роботи	13.12.2021	Виконано

Студент Герасименко Д.В.
(підпис) (прізвище та ініціали)

Керівник роботи Дакова Л.В.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Текстова частина магістерської роботи: 88 сторінок, 19 рис., 2 табл., 21 джерел.

Мета роботи – дослідити процес створення системи інформаційної безпеки за рахунок правильної оцінки ефективності прийнятих рішень і вибору раціонального варіанту створення комплексної реалізації системи захисту інформації.

Об'єкт дослідження – модель систем захисту інформаційної системи.

Предмет дослідження – методи та засоби захисту телекомунікаційних систем та мереж.

Методи дослідження: статистичний аналіз, метод багатокритиріального аналізу, методика та алгоритм оцінювання ефективності захисту інформаційної системи.

Короткий зміст роботи: Робота присвячена темі розробці модел організації захисту інформації в телекомунікаційних мережах. Проблема даного дослідження носить актуальний характер в сучасних умовах. Дана тема вивчається на стику відразу декількох взаємозв'язаних дисциплін. Питанням дослідження даної теми останнім часом присвячена безліч робіт. Актуальність роботи – недостатня розробленість систем інформаційної безпеки викликає потребу в пошуку шляхів підвищення захисту інформації в телекомунікаційних мережах.

Галузь використання – мережа зв'язку України.

ІНФОРМАЦІЇНА СИСТЕМА, КАНАЛИ ВИТОКУ, МОДЕЛЬ ЗАГРОЗИ, ПРИЙНЯТТЯ РІШЕНЬ, АРХІТЕКТУРА ЗАХИСТУ, СИСТЕМНИЙ ПІДХІД, МОДЕЛЬ ЗАХИСТУ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ІС – інформаційна система

ДТЗС – допоміжні технічні засоби і системи

ЕОМ – електронно-обчислювальна машина

ІзОД – інформація з обмеженим доступом

ІТС – інформаційно-телекомунікаційна система

КЗЗ – комплекс заходів захисту

КТЗІ – комплекс технічного захисту інформації

КСЗІ – комплексна система захисту інформації

КЗ – контрольована зона

ОІД – об’єкт інформаційної діяльності

ПЕМВН – побічні електромагнітні випромінювання та наводки

ПЕМВ – побічні електромагнітні випромінювання

ПЕОМ – персональна електронно-обчислювальна машина

СЗІ – служба захисту інформації

ТЗ – технічне завдання

ТКВІ – технічний канал витоку інформації

ВСТУП

Для людини уміння зберігати секрети – одна з найцінніших якостей. Для компанії в тій же мірі надбання – зберігати корпоративні секрети. У масштабах суспільства збереження інформації рівнозначне глобальній безпеці. Інформація має безмежну цінність. Тому кожен етап її використання вимагає ретельного захисту. Загроза інформаційним системам (ІС) подібна до айсберга. Його вершина – це зовнішні загрози: віруси, хакерські атаки, спами і інше, захист від яких здійснюється практично на кожному підприємстві. Проте під водою залишається невидима частина – це внутрішні погрози: саботаж, розкрадання конфіденційних даних, недбале відношення до своїх обов'язків. Близько 80% - це втрати, пов'язані з порушенням інформаційної безпеки, викликані просочуванням конфіденційної інформації, допущені усередині підприємства.

Робота присвячена темі розробці модел організації захисту інформації в телекомунікаційних мережах. Проблема даного дослідження носить актуальний характер в сучасних умовах. Дана тема вивчається на стику відразу декількох взаємозв'язаних дисциплін. Питанням дослідження даної теми останнім часом присвячена безліч робіт.

Актуальність роботи обумовлена, з одного боку, великим інтересом до теми «Захисту інформації на підприємстві від погроз» в сучасній інформаційній безпеці, з іншого боку, її недостатньою розробленістю. Розгляд питань пов'язаних з даною тематикою носить як теоретичну, так і практичну значущість.

Об’єкт дослідження – модель систем захисту інформаційної системи.

Мета роботи – дослідити процес створення системи інформаційної безпеки за рахунок правильної оцінки ефективності прийнятих рішень і вибору раціонального варіанту створення комплексної реалізації системи захисту інформації.

Предмет дослідження – методи та засоби захисту телекомунікаційних систем та мереж.

Методи дослідження – статистичний аналіз, метод багатокритиріального

аналізу, методика та алгоритм оцінювання ефективності захисту інформаційної системи.

Актуальність роботи – недостатня розробленість систем інформаційної безпеки викликає потребу в пошуку шляхів підвищення захисту інформації в телекомунікаційних мережах.

1. ВИЯВЛЕННЯ ПОТЕНЦІЙНИХ ЗАГРОЗ І КАНАЛІВ ВИТОКУ ІНФОРМАЦІЇ У ІНФОРМАЦІЙНІЙ СИСТЕМІ

1.1. Канали витоку інформації та різновиди загроз ІС

Системи, створені спеціально для передачі інформації, використовуються людьми в повсякденній практиці у відповідності зі своїм призначенням і є офіційними засобами зв'язку, робота яких контролюється з метою забезпечення надійної і достовірної передачі інформації, що виключає несанкціонований доступ до неї. Однак існують певні умови, за яких можлива передача інформації з однієї точки до іншої незалежно від бажання об'єкта і джерела інформації. У цьому випадку канал має назву - канал витоку інформації. При цьому природно думати, що такий канал у явному вигляді себе не виявляє. Очевидно, що для утворення каналу витоку інформації необхідні відповідні просторові, енергетичні й часові умови, а також визначені засоби його сприйняття і фіксації інформації на стороні зловмисника.

Фізичні процеси, що відбуваються у цих механічних засобах, створюють об'єктивні передумови для появи інформаційних сигналів, так званих паразитних, у ланцюгах і середовищах, не призначених для передачі даного сигналу, таких як навколишній простір, сторонні ланцюги (корпуси технічних засобів, ланцюги заземлення, ланцюги електроживлення та ін.).

У випадку обробки інформації з обмеженим доступом, наявність навіть слабких інформаційних сигналів у цих паразитних ланцюгах, може створити умови для одержання супротивником секретних зведень.

По фізичній природі канали витоку інформації можна розділити на наступні групи:

- візуально-оптичні (спостереження, фотографування);
- акустичні (включаючи й акустоперетворювальні);
- електричні;
- радіоканали;

- матеріально-речовий (папір, фото, магнітні носії).

Усі потенційно можливі загрози можуть бути розділені за такими різновидами:

- Зниження, нижче ніж припускається, рівня якості інформації, використовуваної для рішення задач, що мають істотне значення;
- Несанкціоноване одержання у злочинних цілях такої інформації, на доступ до якої з тих чи інших причин накладені обмеження;
- Несанкціоноване використання інформації, що є будь-чиєю власністю;
- Шкідливий вплив інформації на людей, технічні пристрої (системи) і технологічні процеси.

Загрози інформації за походженням можуть бути випадковими (такі, що викликані недостатньою надійністю інформаційних систем (ІС), стихійними лихами й іншими непередбаченими обставинами) або злочинними (такі, що викликані цілеспрямованими діями зловмисників).

Джерела та витоки загроз

Вони можуть виходити із зовнішніх і внутрішніх джерел.

До зовнішніх відносяться:

- діяльність розвідувальних і спеціальних служб;
- діяльність різних політичних, військових, фінансових або інших економічних структур, що спрямована проти інтересів держави;
- злочинні дії окремих груп, формувань та фізичних осіб.

До внутрішніх джерел відносяться:

- протизаконна діяльність різних структур, угруповань і окремих осіб в області використання інформації для приховування правопорушень, заподіяння шкоди законним інтересам інших юридичних і фізичних осіб;
- порушення встановлених правил збору, обробки й передачі інформації.

Іншими формами погроз безпеки інформації є:

- витік інформації технічними каналами;

- розкрадання, знищення, перекручування, підробка, блокування, затримка, копіювання інформації в результаті несанкціонованого доступу до носіїв або засобів її обробки, передачі й збереження;
- розкрадання або знищення (псування) носіїв інформації.

Аналіз характеристик загроз інформації

Аналіз потенційно можливих погроз інформації є одним з перших і обов'язкових етапів розробки будь-якої захищеної ІС. При цьому складається як умова повна сукупність загроз, аналізується ступінь ризику під час реалізації тієї чи іншої погрози, після чого визначаються напрямки захисту інформації в конкретній ІС.

Розмаїтність потенційних загроз інформації в ІС настільки велика, що не дозволяє передбачити кожну з них, тому аналізовані характеристики загроз варто вибирати з позицій здорового глузду, одночасно виявляючи не тільки власне загрози, імовірність їхнього здійснення, масштаб потенційного збитку, але і їхні джерела.

Загрозою може бути будь-яка особа, об'єкт чи подія, що, у випадку реалізації, може потенційно стати причиною нанесення шкоди ІС. Загрози можуть бути зловмисними (навмисна модифікація критичної інформації), випадковими (помилки в обчисленнях чи випадкове видалення файлу) або природними (повінь, ураган, блискавка і т.п.)

Уразливими є слабкі місця системи захисту інформації (СЗІ) ІС, що можуть бути використані для реалізації загрози. Зменшення уразливих місць ІС може знизити чи усунути ризик від загроз ІС.

Ідентифікація загроз передбачає розгляд дій і наслідків реалізації загроз. Проблеми, що виникли після реалізації загрози, приводять до приховування, модифікації, руйнування чи відмовлення в обслуговуванні. Більш значні довгострокові наслідки реалізації загрози приводять до втрати керування військами, порушенню таємниці, втраті адекватності даних, до людських жертв чи до інших довгострокових ефектів.

Основні види загроз безпеки суб'єктів інформаційних відносин

Основними видами загроз безпеки ІС та інформації (загроз інтересам суб'єктів інформаційних відносин) є:

- стихійні лиха й аварії (повінь, ураган, землетрус, пожежа);
- збої і відмовлення устаткування (технічних засобів) ІС;
- наслідки помилок проектування і розробки компонентів ІС (апаратних засобів, технології обробки інформації, програм, структур даних і т.п.);
- помилки під час експлуатації (користувачів, операторів і іншого персоналу);
- навмисні дії порушників і зловмисників (скривджених осіб з числа персоналу, злочинців, шпигунів, диверсантів і т.п.).

1.2. Класифікація загроз інформації

У процесі зберігання й обробки інформація може піддаватися впливу як випадкових, так і навмисних факторів. Уся множина потенційних загроз за природою їхнього виникнення розділяється на два класи: природні (об'єктивні) і штучні (суб'єктивні).

Загрози даним — потенційно існуюча небезпека випадкового чи навмисного руйнування, несанкціонованого одержання чи модифікації даних, обумовлена структурою системи обробки, а також умовами обробки і зберігання даних.

Природні загрози — це загрози, викликані впливами на ІС та її елементи об'єктивних фізичних процесів чи стихійних природних явищ, що не залежать від людини.

Штучні загрози — це загрози ІС, викликані діяльністю людини. Серед них, виходячи з мотивації дій, можна виділити:

- ненавмисні загрози, викликані помилками в проектуванні ІС та її елементів, помилками в програмному забезпеченні, помилками в діях персоналу і т.п.;
- навмисні загрози, зв'язані з корисливими інтересами людей (зловмисників).

Ненавмисні штучні загрози інформації

Основні ненавмисні штучні погрози ІС (дії вчинені випадково, через незнання, з неуважності чи з недбалості, з цікавості, але без злого наміру) такі:

- ненавмисне псування носіїв інформації;
- зараження комп'ютера вірусами;
- розголошення, передача чи втрата атрибутів розмежування доступу (паролів, ключів шифрування, ідентифікаційних карток, пропусків і т.п.);
- пересилання даних за помилковою адресою абонента (пристрою);
- введення помилкових даних;
- ненавмисне ушкодження каналів зв'язку.

Навмисні штучні загрози інформації

Основні шляхи навмисної дезорганізації роботи, виводу системи з ладу, проникнення в систему і несанкціонований доступ до інформації є такими:

- фізичне руйнування системи (зрив, підпал) або виведення з ладу найбільш важливих компонентів комп'ютерної системи (пристроїв, носіїв важливої системної інформації, осіб з числа персоналу);
- відключення чи виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, охолодження і вентиляції, ліній зв'язку);
- вербування (підкуп, шантаж і т.п.) персоналу чи окремих користувачів, що мають визначені повноваження;
- перехоплення побічних електромагнітних, акустичних і інших випромінювань пристроїв і ліній зв'язку.
- перехоплення даних по каналах зв'язку і їх аналіз.
- викрадення носіїв інформації (магнітних дисків, стрічок, мікросхем пам'яті, запам'ятовуючих пристроїв і ПК);
- несанкціоноване копіювання носіїв інформації;
- розкриття шифрів криптозахисту інформації;

Варто вказати, що найчастіше для досягнення мети зловмисник

використовує сукупність перелічених вище способів.

Спеціальні методи і технічні засоби зйому інформації

- спеціально впроваджені електронні засоби (закладки), що руйнують чи спотворюють інформацію;
- закладки, що передають оброблювану в ІС інформацію чи мовну інформацію-переговори у приміщеннях, де розгорнуті технічні засоби;
- опромінення технічних засобів інформаційної системи зондувальними сигналами (так зване - нав'язування);
- руйнування (перекручування) технічних засобів автоматизованих систем шляхом підключення їхніх елементів до сторонніх джерел напруги і ін.

1.3. Акустичні канали витоку інформації

Найбільш інформативними методами одержання конфіденційних зведень з перелічених у розділі 1 є акустичний контроль і перехоплення переговорів у лініях зв'язку, причому обидва методи передбачають використання спеціальних технічних засобів несанкціонованого зйому інформації.

Для перехоплення і реєстрації акустичної інформації існує величезний набір засобів розвідки: мікрофони, електронні стетоскопи, акустичні закладки, спрямовані і лазерні мікрофони, апаратура магнітного запису. Набір акустичних засобів розвідки, використовуваних для рішення конкретної задачі, значною мірою залежить від можливості доступу агента до контрольованого приміщення чи до осіб, що є об‘єктами зацікавленості.

У тому випадку, якщо є постійний доступ до об'єкта контролю, можуть бути використані найпростіші мініатюрні мікрофони, з’єднуючі лінії які виводять у сусідні приміщення для реєстрації і подальшого прослуховування акустичної інформації. Такі мікрофони діаметром 2.5 мм можуть вловити нормальний людський голос з відстані до 20 м.

Якщо агенти не мають постійного доступу до об'єкта, але є можливість його короткочасного відвідування під різними приводами, то для акустичної розвідки

використовуються мініатюрні диктофони і магнітофони закамуфльовані під предмети повсякденного побуту: книгу, письмовий прилад, пачку сигарет. Крім цього, диктофон може знаходитися в кого-небудь із присутніх на закритій нараді. У цьому випадку часто використовують виносний мікрофон, захований під одягом чи закамуфльований під годинник, авторучку, ґудзик.

У випадку якщо агентам не вдається проникнути на об'єкт навіть на короткий час, але є доступ у сусідні приміщення, то для ведення розвідки використовуються електронні стетоскопи. Електронні стетоскопи підсилюють акустичний сигнал, що проникає крізь стіни, підлогу, стелю у 20-30 тисяч разів і здатні уловлювати звук годинників через бетонні стіни товщиною до 1 м.

Поряд з диктофонами для перехоплення акустичної інформації використовуються акустичні закладки, які несанкціоновано і потай встановлюються в приміщеннях, автомашинах. Як канал передачі перехопленої інформації використовуються радіо і оптичний канали, силові, слабкострумові і знеструмлені комунікації.

Найбільше поширення одержали радіозакладки, які можна класифікувати за декількома критеріями:

- за використовуваним діапазоном частот;
- за потужністю випромінювання: малопотужні — до 10 мвт, середньої потужності — 10 мвт—100 мвт, великої потужності — понад 100 мвт;
- за видом використовуваних сигналів: простий (з АМ, FM і WFM), складний (ППРЧ, шумоподібні сигнали);
- за способом модуляції: з модуляцією несущої, з модуляцією проміжної частоти;
- за виконанням: у виді окремого модуля, закамуфльовані під різні предмети (авторучка, калькулятор, электроподовжувач, дерев'яний брусок).

Радіозакладки забезпечують дальність передачі від десятків метрів (авторучка — 50 м) до 1 км. При використанні ретрансляторів дальність передачі перехопленої інформації збільшується до десятків кілометрів. З метою підвищення скритності роботи радіозакладки обладнаються системами

акустозапуску, дистанційного керування, пакетної передачі, використовуються шумоподібні, скремблировані, шифровані сигнали.

Контроль і прослуховування телефонних переговорів

Прослуховування телефонних каналів зв'язку об'єкта в даний час є одним з основних способів одержання конфіденційної інформації. Знімання інформації з телефонної лінії зв'язку може здійснюватися або безпосереднім підключенням до лінії, або безконтактно за допомогою індуктивного датчика. Факт контактного підключення до лінії легко визначити, у той час як використання індуктивного підключення не порушує цілісності кабелю і не вносить зміни в параметрів телефонної лінії.

Сигнали з телефонної лінії можуть записуватися на магнітофон (використовується спеціальний адаптер) чи передаватися по радіоканалу.

Виготовляються телефонні закладки у виді окремих модулів (брусок) або камуфлюються під елементи телефонного устаткування: адаптери, розетки, телефонні і мікрофонні капсулі, конденсатори. Телефонні закладки встановлюються безпосередньо в телефонний апарат, слухавку, розетку, а також безпосередньо на телефонну лінію. Передача інформації від телефонної закладки починається в момент підняття трубки абонентом.

Поряд з телефонними і радіозакладками використовуються комбіновані закладки, які під час ведення телефонних переговорів здійснюють їхнє перехоплення, а по закінченні — автоматично переключаються на перехоплення акустичної інформації.

1.4. Перехоплення ПЕМВ

Можливість витоку інформації в процесі перехоплення побічних електромагнітних випромінювань (ПЕМВ), створюваних технічними засобами ІС.

Найбільш небезпечними джерелами ПЕМВ є дисплеї, провідні лінії зв'язку, накопичувачі на магнітних дисках і друкуючі апарати послідовного типу.

Перехоплення ПЕМВ може здійснюватися за допомогою портативної апаратури. Така апаратура може являти собою широкополосний автоматизований

супергетеродинний приймач. У якості пристроїв реєстрації прийнятих сигналів (повідомлень) можна використовувати магнітний носій або дисплей.

Витік оброблюваної в ІС інформації під час прийому інформаційних сигналів, наведених у ланцюгах електроживлення і заземлення апаратних засобів ІС, що виходять за межі охоронюваної (контрольованої) зони — зони безпеки.

Можливість витоку оброблюваної в ІС інформації під час прийому сигналів, наведених у проводах і кабелях допоміжних технічних засобів ІС, що знаходяться в зоні впливу ПЕМВ працюючих технічних засобів ІС.

Джерела витоку інформації по каналах ПЕМВН

До технічних засобів, що можуть бути джерелом витоку інформації каналами ПЕМВН відносяться:

- засоби і системи телефонної, телеграфної (телетайпної), директорського, гучномовного, диспетчерського, внутрішнього, службового і технологічного зв'язку;
- засоби і системи звукопідсилення, звукозапису і звуковідтворення;
- засоби і системи спеціальної охоронної сигналізація (на розкриття дверей, вікон і проникнення у приміщення сторонніх осіб), пожежної сигналізації (з датчиками, що реагують на дим, світло, тепло, звук);
- засоби і системи кондиціонування (датчики температури, вологості, кондиціонери);
- засоби і системи електроосвітлення і побутового електроустаткування (світильники, люстри, настільні і стаціонарні вентилятори, електронагрівальні прилади, холодильники, бумагорізальні машини, провідна мережа електроосвітлення);
- електронна й електрична оргтехніка.

У процесі функціонування засобів обчислювальної техніки в конструктивних елементах і кабельних з'єднаннях циркулюють електричні струми інформативних сигналів, у результаті чого формуються електромагнітні поля, рівні яких можуть бути достатніми для прийому сигналів і витягу інформації за допомогою спеціальної апаратури.

Канали витоку інформації можуть виникати унаслідок випромінювання інформативних сигналів при роботі ТЗ і наведення цих сигналів у лініях зв'язку, ланцюгах електроживлення і заземлення, інших комунікаціях, що мають вихід за межі контрольованої території (КТ). Інформативні сигнали можуть поширюватися на великі відстані і реєструватися засобами технічних розвідок за межами КТ.

Частоти, на яких можуть випромінюватися (наводитися) інформативні сигнали, залежать від типів і видів апаратурних засобів і можуть поширюватися в діапазоні від сотень герців до декількох десятків гигагерц.

Витік інформації по ланцюгах заземлення

Витік інформації по ланцюгах заземлення може виникнути при наявності рознесених точок заземлення інформативних ланцюгів у випадку утворення в різних точках системи заземлення різниці потенціалів і виникнення в результаті цього струмів у ланцюгах заземлення, при великому значенні опору ланцюга заземлення, а також унаслідок недосконалості екранів, що приводить до асиметрії ліній відносно екрана й до виникнення в ланцюзі між корпусом екрана і землею інформативних струмів.

Крім того, можливі канали витоку інформації утворюються:

- низькочастотними електромагнітними полями, що виникають при роботі ТЗ;
- при впливі на ТЗ електричних, магнітних і акустичних полів;
- при виникненні паразитної високочастотної (ВЧ) генерації;
- при проходженні інформативних (небезпечних) сигналів у ланцюзі електроживлення;
- при взаємному впливі ланцюгів;
- при проходженні інформативних (небезпечних) сигналів у ланцюзі заземлення;
- внаслідок помилкових комутацій і несанкціонованих дій.

При передачі інформації в елементах схем, конструкцій, у проводах що підводять сигнали або струм та з'єднують технічні засоби протікають струми інформативних сигналів. Виникаючі при цьому електромагнітні поля можуть

впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть привести до утворення каналів витоку інформації.

Інформативні (небезпечні) сигнали можуть виникати на елементах технічних засобів, чуттєвих до впливу:

- електричного поля (неекрановані проводи й елементи технічних засобів);
- магнітного поля (мікрофони, гучномовці, головні телефони, трансформатори, катушки індуктивності, дроселі, електромагнітні реле);
- акустичного поля (мікрофони, гучномовці, головні телефони, трансформатори, котушки індуктивності, дроселі, електромагнітні реле).

При наявності в технічних засобах елементів, здатних перетворювати ці поля в електричні сигнали, можливий витік інформації по незахищених ланцюгах абонентських ліній зв'язку, електроживлення, заземлення, керування і сигналізації.

Витік інформації через джерела електроживлення

Під час роботи ТЗ можливий витік інформації через джерела електроживлення:

- у результаті проходження інформативного сигналу через технічні засоби на вхідному опорі його джерела живлення може виникнути напруга, що несе сигнал, який містить інформативну складову. Через випрямний пристрій і силовий трансформатор цей сигнал поширюється по мережних лініях за межі контрольованої території;
- при проходженні мовного сигналу через кінцевий підсилювальний пристрій може спостерігатися нерівномірне споживання струму від джерела живлення. Струм споживаний підсилювачем від мережі, може бути модульований інформативним сигналом, що проходить через підсилювач.

Траси кабельних ланцюгів, що несуть інформацію, можуть прокладатися в одній кабельній каналізації з незахищеними ланцюгами ТЗ і проходити через загальні коробки і шафи.

Джерелами утворення інформативних сигналів є ділянки, охоплені випадковими ємнісними і магнітними зв'язками. Такими ділянками можуть бути

відрізки рівнобіжного пробігу ліній, що несуть інформацію, з незахищеними лініями, що ідуть за межі контрольованої території; монтажні колодки, роз‘єми блоків, контакти перемикачів і реле, використовувані для комутації вихідних ліній, і блоки, піддані впливу електромагнітного поля.

Джерелом утворення інформативних сигналів є елементи ланцюгів і схем, якщо ці елементи знаходяться під потенціалом таких сигналів і виходять з екранів.

При надходженні високочастотних сигналів у нелінійні (чи параметричні) ланцги, що несуть інформативні сигнали, відбувається модуляція високочастотного сигналу. Таким чином, високочастотні коливання стають носіями інформативних сигналів і створюють канал витоку інформації.

Лініями, на які подається чи з яких знімається високочастотний сигнал, можуть бути незахищені лінії зв'язку, ланцюги електроживлення, заземлення, управління і сигналізації; ланцюги, утворені паразитними зв'язками, конструктивними елементами будинків, споруджень, устаткування і т.п.

При виникненні несправностей у апаратурі чи при несанкціонованих діях обслуговуючого персоналу в схемах управління може виникнути небажана комутація інформативного сигналу, що призводить до виходу інформації в незахищений канал зв'язку.

Джерелами інформативного сигналу цього каналу є пульти керування, щити розподілу і комутації, блоки контролю, реле, трансформатори, роз‘єми, перемикачі або запам'ятовуючі пристрої, у яких може виникнути помилкова комутація в результаті несправностей чи несанкціонованих дій.

1.5. Параметри оцінки загроз інформації

Основними параметрами можливого витоку інформації по каналах ПЕМВН є:

- напруженість електричних і магнітних полів інформативного сигналу;
- величина звукового тиску;

- величина напруги інформативного сигналу;
- величина напруги наведеного інформативного сигналу;
- величина напруги шумів (перешкод);
- величина струму інформативного сигналу;

Зазначені параметри визначаються і розраховуються за результатами вимірів у заданих точках. Гранично припустимі значення основних параметрів є нормованими величинами і визначаються за відповідними методиками. Співвідношення розрахункових (вимірених) значень основних параметрів до гранично припустимих (нормованих) значень визначають необхідні умови захисту інформації.

Найкраще аналізувати небезпеку ще на стадії проектування локальної мережі чи робочого місця системи, щоб відразу визначити потенційні втрати й установити вимоги до мір забезпечення безпеки. Вибір захисних і контрольних заходів на ранній стадії вимагає набагато менших витрат, ніж виконання подібної роботи з комп'ютерною системою яка вже експлуатується. Але й в останньому випадку аналіз небезпек може виявити уразливі місця, які можна підсилити розумними засобами.

У більшості випадків навіть проведення аналізу можливих небезпек дозволяє персоналу краще усвідомити проблеми, що можуть проявитися під час роботи, що дозволяє підсилити програму управління ризиком. Що стосується останньої, то раніше за розробку таких заходів за звичай відповідав менеджер системи інформації і управління або автоматизованої обробки даних. Тепер застосовується інший підхід, при якому в кожній організації відповідальність за виконання аналізу небезпек і розробку методики їхнього виключення покладається на кілька груп службовців.

2. КОМПЛЕКСНА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1.Завдання моделі захисту інформації

Практичне завдання забезпечення інформаційної безпеки полягає в розробці моделі представлення системи (процесів) ІБ, яка на основі науково-методичного апарату, дозволяла б вирішувати завдання створення, використання і оцінки ефективності СЗІ для проектованих і існуючих унікальних ІС. У спрощеному вигляді модель СЗІ представлена на рис. 2.1.

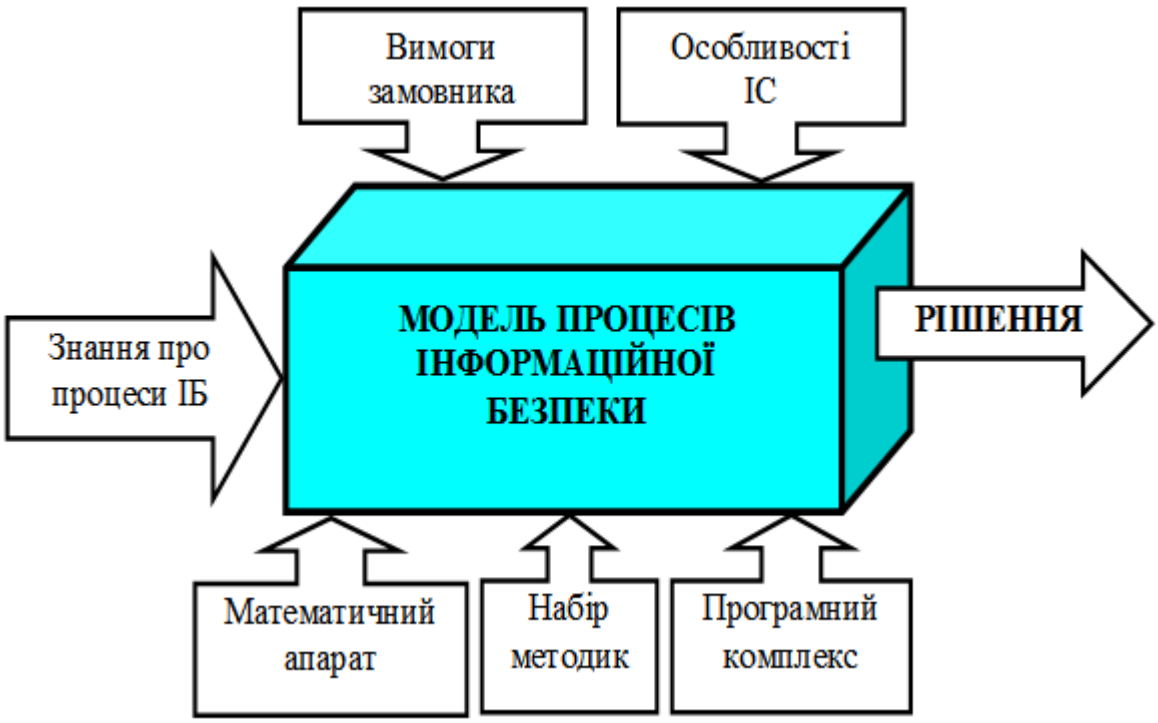

Рис. 2.1 Модель системи захисту інформації

Основним завданням моделі є наукове забезпечення процесу створення системи інформаційної безпеки за рахунок правильної оцінки ефективності ухвалюваних рішень і вибору раціонального варіанту технічної реалізації системи захисту інформації.

Специфічними особливостями рішення задачі створення систем захисту є:

- неповнота і невизначеність початкової інформації про склад ІС і характерних загроз; багатокритеріальність завдання, пов'язана з необхідністю обліку великого числа приватних показників (вимог) СЗІ;
- наявність кількістних та якісних показників, які необхідно приймати при рішенні задач розробки СЗІ;
- неможливість використання класичних методів оптимизації.

Вимоги до моделі

Така модель повинна задовольняти наступним вимогам (рис. 2.2.):

- Використовуватися в якості:
  - керівництва по створенню СЗІ;
  - методики формування показників і вимог до СЗІ;
  - інструменту (методики) оцінки СЗІ;
  - моделі СЗІ для проведення досліджень (матриця стану).
- Володіти властивостями:
  - універсальність;
  - комплексність;
  - простота використання;
  - наочність;
  - практична спрямованість;
  - бути самонавчальною (можливість нарощування знань);
  - функціонувати в умовах високої невизначеності початкової інформації.
- Дозволяти:
  - встановити взаємозв'язок між показниками (вимогами);
  - задавати різні рівні захисту;
  - отримувати кількісні оцінки;
  - контролювати стан СЗІ;
  - застосовувати різні методики оцінок;
  - оперативно реагувати на зміни умов функціонування;
  - об'єднати зусилля різних фахівців єдиним задумом.

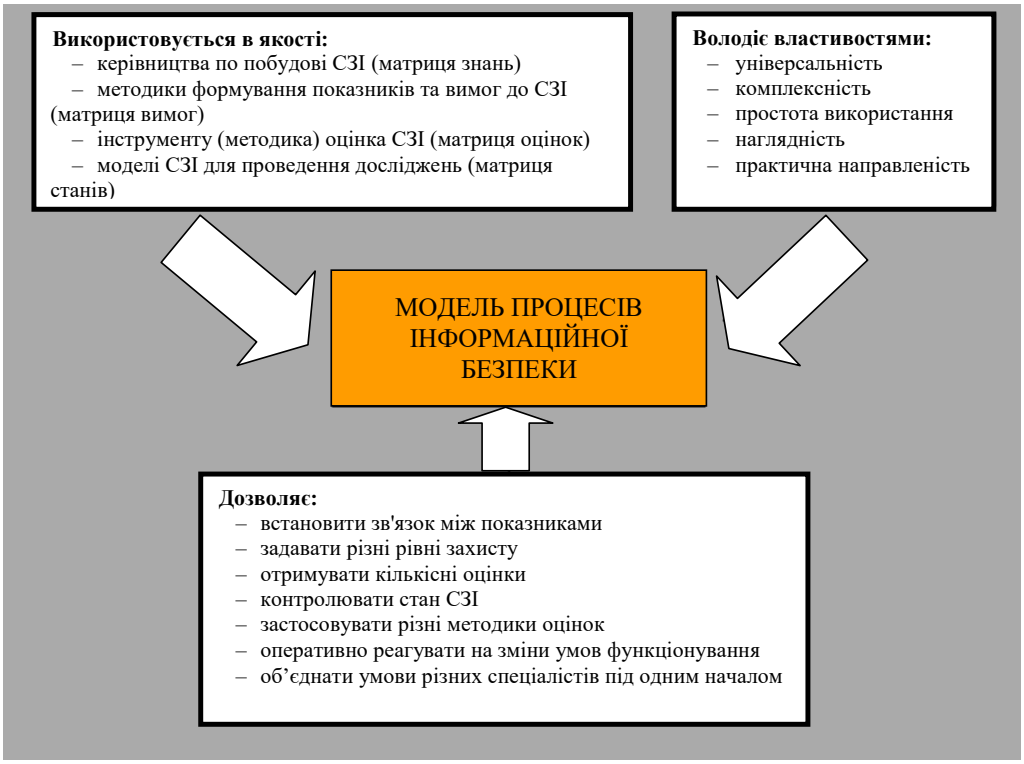

Рис. 2.2 Вимоги до моделі СЗІ

Опис підходу до формування моделі ІБ.

Людина отримує як найповніше уявлення про явище, що цікавить його, коли їй вдається розглянути це щось невідоме з усіх боків, в тривимірному вимірюванні. Скористаємося цим принципом. Розглянемо три "координати вимірювань" - три групи складових моделі СЗІ.

- (ОСНОВИ) З чого складається.
- (НАПРЯМИ) Для чого призначена.
- (ЕТАПИ) Як працює.

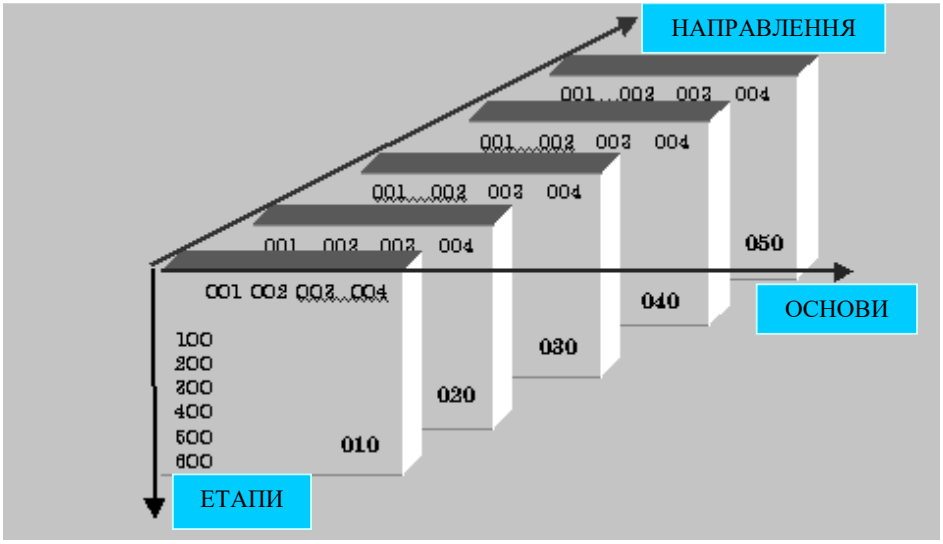

Рис. 2.3 Три "координати вимірювань"

ОСНОВАМИ або складовими частинами практично будь-якої складної СИСТЕМИ (у тому числі і системи захисту інформації) є: законодавча, нормативно-правова і наукова база.

Структура і завдання органів (підрозділів), що забезпечують безпеку ІТ приведені на рис. 2.4.

Рис. 2.4 Координати ОСНОВИ

НАПРЯМИ формуються виходячи з конкретних особливостей ІС як об'єкту захисту.

У загальному випадку, враховуючи типову структуру ІС і види робіт, що історично склалися, по захисту інформації, пропонується розглянути наступні напрями:

- Захист об'єктів інформаційних систем;
- Захист процесів, процедур і програм обробки інформації;
- Захист каналів зв'язку;
- Придушення побічних електромагнітних випромінювань;
- Управління системою захисту.

Перелічені напрями можна представити у вигляді схеми рис. 2.5

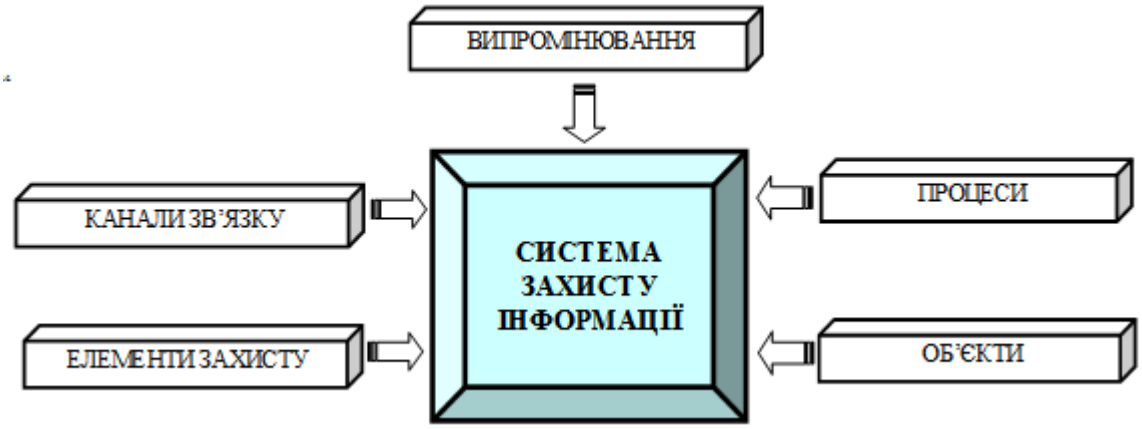

Рис. 2.5 Координата НАПРЯМУ

Але, оскільки кожен з цих НАПРЯМІВ базується на перерахованих вище ОСНОВАХ, то елементи ОСНОВ і НАПРЯМІВ, розглядаються нерозривно один з одним. Наприклад, одну з ОСНОВ під назвою "Законодавча база." необхідно розглядати по всіх НАПРЯМАХ, а саме:

- Законодавча база захисту об'єктів.
- Законодавча база захисту процесів, процедур і програм.
- Законодавча база захисту каналів зв'язку.
- Законодавча база придушення побічних електромагнітних випромінювань.

- Законодавча база по управлінню і контролю самої системи захисту.

Аналогічно слід розглядати решту граней ОСНОВ (структуру, заходи, засоби) по всіх НАПРЯМАХ.

Проведений аналіз існуючих методик (послідовностей) робіт із створення СЗІ дозволяє виділити наступні ЕТАПИ:

- Визначення інформаційних і технічних ресурсів, а також об'єктів ІС, що підлягають захисту;
- Виявлення повного множина потенційна можливих погроз і каналів просочування інформації;
- Проведення оцінки уразливості і рисок інформації (ресурсів ІС) при наявній безлічі погроз і каналів витоку;
- Визначення вимог до системи захисту інформації;
- Здійснення вибирання засобів захисту інформації і їх характеристик;
- Впровадження і організація використання вибраних мір, способів і засобів захисту.
- Здійснення контролю цілісності і управління системою захисту.

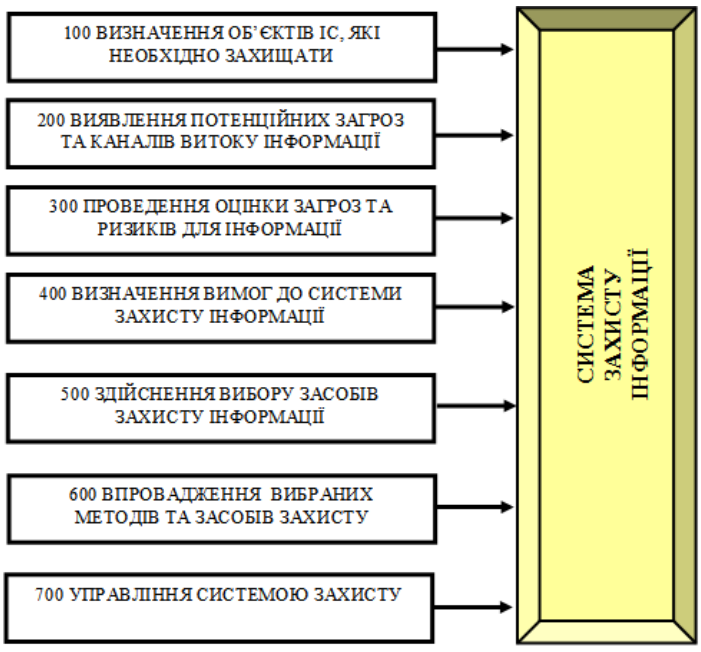

Рис. 2.6 Етапи створення систем захисту інформації

Оскільки ЕТАПІВ сім, і по кожному треба освітити 20 вже відомих вам питань то в цілому для формування уявлення про конкретну систему захисту необхідно відповісти на 140 простих питань. Абсолютно очевидно що з кожного питання (елементу) виникне декілька десятків уточнень. У загальному випадку кількість елементів матриці може бути визначене із співвідношення: $K = O_i \times H_j \times M_k$.

Де: К - кількість елементів матриці, O_i - кількість складових блоку "ОСНОВИ", H_j - кількість складових блоку "НАПРЯМУ", M_k - кількість складових блоку "ЕТАПИ".

У нашому випадку загальна кількість елементів "матриці" рівна 140 $K=4\times5\times7=140$, оскільки $O_i=4$, $H_j=5$, $M_k=7$

Нагадаємо, що матриця у вигляді двомірної таблиці з'являється не сама по собі, а формується у кожному конкретному випадку, виходячи з конкретних завдань по створенню конкретної СЗІ для конкретної ІС.

2.2. Основи побудови систем захисту інформації

Оцінки параметрів СЗІ в умовах високого ступеня невизначеності умов її функціонування повинні обчислюватися з використанням не однієї математичної моделі, а погодженого сімейства моделей, що адаптивно конструюються одна до одної і, таким чином, безупинно удосконалюється на основі оптимального вибору вихідних даних.

При синтезі оптимальних систем захисту вихідними повинні стати наступні два положення:

- вибір математично продуктивного критерію оптимальності відповідно до архітектури системи захисту і технології обробки інформації в ІС;
- чітке математичне формулювання задачі, що враховує всі апріорні зведення і дозволяє вирішити її відповідно до прийнятого критерію.

Підсумком рішення задачі синтезу оптимальної системи захисту і його кінцевою метою повинні бути чотири змістовних результати:

- архітектура системи захисту;
- кількісна оцінка якості її функціонування;
- оцінка практичної чутливості розроблених моделей до відхилень від апріорних даних;
- фізичне впроваджування синтезованих систем захисту в сучасних системах обміну даними (відповідність технології обробки інформації рівню її захисту).

Під ефективністю систем захисту інформації будемо розуміти ефективність її використання, як активний засіб в операції забезпечення конфіденційності обробки, збереження і передачі інформації.

При цьому, оцінка ефективності операції полягає у виробленні оцінного судження щодо придатності заданого способу дій фахівців із захисту інформації чи пристосованості засобів захисту до рішення задач.

Введення показника ефективності вимагає також визначення критерію ефективності як правила, що дозволяє співставляти стратегії, що характеризується різним ступенем досягнення мети, і здійснювати вибір стратегій із множини припустимих.

Теоретичні основи побудови оптимальних систем захисту винятково складні і, незважаючи на інтенсивність досліджень у цій предметній області, ще далекі від досконалості.

Під методологією оптимізації систем захисту інформації будемо розуміти розробку теорії, що зв'язує їхню структуру, логічну організацію, методи і засоби діяльності з метою формування функції вибору і виділення підмножини найкращих стратегій.

Оптимальним буде вважатися рішення, котре у передбачуваних умовах щонайкраще задовольнить умовам розглянутої задачі. Оптимальність рішення досягається за рахунок найбільш раціонального розподілу ресурсів, затрачуваних на рішення проблеми захисту.

У процесі створення оптимальної СЗІ неминуче виникає задача корекції вимог до системи захисту. Труднощі її рішення полягає у тому, що виникають невизначеності не стохастичного характеру, обумовлені:

- наявністю цілеспрямованої протидії сторони протиборчої системи, способи дій якої невідомі досліднику;
- недостатньою вивченістю деяких явищ, що супроводжували процес функціонування систем захисту;
- нечітким представленням мети операції, що приводить до неоднозначного трактування відповідності реального результату операції до необхідного.

Проблеми коректності постановки задач

Труднощі дослідження питань забезпечення безпеки інформаційних технологій збільшується великою невизначеністю умов функціонування ІС.

Тому постановка задачі забезпечення захисту інформації, як правило, виявляється некоректною, оскільки найчастіше формулюється в умовах непередбачуваності поводження системи в нестандартних і, особливо, екстремальних ситуаціях. Вплив невизначеності особливо сильно виявляється у трансформованих, нестабільних, слабко організованих ІС через неповноту, несвоєчасність, не нормованість і низьку вірогідность інформації.

Задачі забезпечення безпеки інформаційних технологій, як правило, не мають властивістю одиничності рішення, ефективність і оптимальність якого визначаються ступенем урахування обмежень, характерних для конкретної ситуації. Для підвищення ступеня коректності постановки задач забезпечення БІТ необхідно підвищувати знання про ІС у безупинно змінюючихся умовах її функціонування.

Одержання і використання знань має здійснюватися безпосередньо в процесі функціонування системи шляхом поступового накопичення необхідної інформації, аналізу і використання її для ефективного виконання системою заданої цільової функції у змінюваних умовах внутрішнього і зовнішнього середовища.

Відомі математичні моделі, використовувані для опису структури, поводження і керування СЗІ, в умовах некоректної постановки задач не дають бажаного

результату. Тому необхідна розробка нових, орієнтованих на специфіку процесів захисту інформації методів і засобів моделювання.

Для одержання інформації про поводження СЗІ потрібно виділити групи параметрів і визначити час перевірки їхніх значень. При цьому розглядаються особливо значущі і важливі з позиції реалізації мети функціонування системи параметри.

Перевірка й аналіз значень зазначених параметрів, необхідні для підвищення знань про систему, мають здійснюватися таким чином, щоб забезпечити можливість прийняття своєчасних і достовірних рішень, а також коректування поводження системи в процесі функціонування. Таким чином, у СЗІ обов'язково має бути передбачено виконання процедур контролю її працездатності і діагностування станів.

Прийняття рішень у більшості випадків базується на експертних оцінках. Однак в умовах невизначеності вихідних даних і некоректності постановки задач управління ці оцінки можуть внести додаткову некоректність у прийняте рішення, збільшивши тим самим вихідну невизначеність.

Дослідження предметної області з метою створення математичної моделі СЗІ. Рішення проблем моделювання СЗІ вимагає поетапного виконання наступних досліджень:

- Розробка принципів, методів і засобів скорочення розмірності опису СЗІ, що включає:
  - аналіз інформаційної структури системи і взаємозв'язків між розв'язуваними в ній задачами;
  - аналіз динамічних характеристик рішення задач;
  - аналіз кореляційних залежностей між параметрами системи, що є результатами рішення окремих задач;
  - виділення на основі аналізу сукупностей задач, результат рішення кожної з який дозволяє визначити один з контрольованих параметрів системи.

У результаті розробки повинні бути сформульовані вимоги і рекомендації з раціональної організації структури СЗІ, декомпозируваної по рівнях контролю і управління. Це дозволить проводити подальші дослідження в умовах мінімізованої розмірності опису системи.

- Розробка методології, методів і засобів рішення задач забезпечення БІТ в умовах невизначеності, що включає:
  - дослідження питань коректності постановки задач при недостатнім розумінні кінцевих результатів і цілей рішення в різко мінливих умовах;
  - дослідження питань використання невизначеності (неповноти, низької вірогідності й ін.) вихідних даних при рішенні задач ЗІ.

Результатом досліджень повинна стати розробка методологічних основ, методів і засобів рішення некоректно поставлених задач в умовах невизначеності.

- Розробка принципів, методів і засобів самоорганізації СЗІ, включає наступні задачі:
  - конструювання адаптивних моделей для опису структури і поводження системи, прогнозування значень її параметрів;
  - конструювання адаптивних моделей для формування підмножин контрольованих параметрів і діапазонів значень зон їхнього контролю на основі заданих вимог до стійкості функціонування системи;
  - конструювання адаптивних моделей контролю працездатності і діагностування порушень працездатності системи;
  - самоорганізацію і саморозвиток сімейств моделей для опису структури, поводження, прогнозування, контролю і діагностування з урахуванням забезпечення необхідної стійкості системи в умовах впливу факторів внутрішнього і зовнішнього середовища.

Вирішенням досліджень повинні бути створені на основі відомих і спеціально розроблених методів і засобів адаптивні моделі для опису структури і поводження СЗІ, а також контролю, діагностування і прогнозування її станів.

- Розробка методів і засобів підтримки прийняття рішень, включає наступні задачі:

- розробку методів і засобів вибору рішень із усієї множини альтернативних варіантів на підставі аналізу стану і поводження системи і з урахуванням вимог управління, реального ресурсу, що задовольняє цим вимогам.
- розробку методів і засобів декомпозиції прийнятих рішень по рівнях управління системи;
- розробку методів і засобів підтримки прийняття рішень по самоорганізації системи у процесі її функціонування для удосконалювання усіх видів перерахованих вище моделей і їхніх сімейств.

Дослідження базуються на використанні всіх отриманих раніше результатів і орієнтовані на створення банку знань про систему ЗІ.

Для рішення перерахованих і інших теоретичних і прикладних проблем необхідна цілеспрямована, виконувана в рамках державних програм і на єдиній концептуальній і методологічній основі робота. Кінцевим результатом досліджень має бути модель СЗІ.

Короткий аналіз загальних моделей СЗІ

Основне призначення загальних моделей складається зі створення передумов для об'єктивної оцінки загального стану ІС з точки зору міри або рівня уразливості захищеності інформації в ній. Необхідність у таких оцінках зазвичай виникає під час аналізу загальної ситуації з метою вироблення стратегічних рішень при організації захисту інформації.

Загальними моделями систем і процесів захисту інформації названі такі, котрі дозволяють визначати (оцінювати) загальні характеристики зазначених систем і процесів на відміну від моделей локальних і часток, що забезпечують визначення (оцінки) деяких локальних чи часток характеристик систем або процесів.

Системну класифікацію загальних моделей у даний час виконати практично неможливо, тому що через мале число таких моделей для цього немає достатніх даних. Тому класифікацію розглянутих моделей представимо простим переліком і короткою характеристикою лише деяких з них.

Загальна модель процесу захисту інформації.

Дана модель у самому загальному виді і для самого загального об'єкта захисту повинна відображати процес захисту інформації як процес взаємодії дестабілізуючих факторів, що впливають на інформацію, і засобів захисту інформації, що перешкоджають дії цих факторів. Підсумком взаємодії буде той чи інший рівень захищеності інформації;

Узагальнена модель системи захисту інформації.

Будучи подальшим розвитком загальної моделі процесу захисту, узагальнена модель системи захисту повинна відображати основні процеси, здійснювані в ній з метою раціоналізації процесів захисту. Зазначені процеси в самому загальному вигляді можуть бути представлені як процеси розподілу і використання ресурсів, що виділяються для захисту інформації;

Модель загальної оцінки загроз інформації.

Основною спрямованістю цієї моделі є оцінка не просто загроз інформації як таких, а ще й оцінка тих втрат, що можуть мати місце при прояві різних загроз. Моделі даного напрямку важливі ще й тим, що саме на них найбільшою мірою були виявлені ті умови, за яких такі оцінки можуть бути адекватні реальним процесам захисту інформації. Загальна характеристика математичних методів оцінки й обґрунтування вимог до СЗІ.

Системи захисту інформації, з одного боку, є складовою частиною інформаційної системи, з іншого - самі по собі представляють складну технічну систему. Рішення задач аналізу і синтезу СЗІ ускладнюється з огляду на їхні особливості, основними з який є:

- складний опосередкованого взаємозв'язку показників якості СЗІ з показниками якості інформаційної системи;
- необхідність обліку великої кількості показників (вимог) СЗІ при оцінці й виборі їхнього раціонального варіанта;
- переважно якісний характер показників (вимог), що враховуються при аналізі й синтезі СЗІ;

- істотний взаємозв'язок і взаємозалежність цих показників (вимог), що мають суперечливий характер;
- труднощі одержання вихідних даних, необхідних для рішення задач аналізу і синтезу СЗІ, особливо на ранніх етапах їхнього проектування.

Зазначені особливості роблять практично неможливим застосування традиційних математичних методів, у тому числі методів математичної статистики і теорії ймовірностей, а також класичних методів оптимізації для рішення прикладних задач аналізу і синтезу СЗІ.

Складність процесу прийняття рішень, відсутність математичного апарату призводять до того, що при оцінці й при виборі альтернатив можливо, (а найчастіше просто необхідно) використовувати й обробляти якісну експертну інформацію.

2.3. Модель загроз безпеки інформаційних систем

Одним зі складних і трудомістких процесів розробки концепції системи інформаційної безпеки (СІБ) для інформаційних систем (ІС) є дослідження можливих загроз і виділення потенційно небезпечних.

Розглядаючи цілі, переслідувані порушником безпеки ІС, варто акцентувати увагу на наступних: порушення конфіденційності, цілісності і доступності інформації, що захищається. У більшості випадків досягнення зазначених цілей прямо пов'язано з порушенням відповідного законодавства, договірних відносин між ІС і користувачами, етичних норм й приводить до відчутних утрат.

На розробку і реалізацію загроз впливає величезна кількість факторів (економічних, технічних, технологічних і т.д.). Варто виділити наступні:

- очікуваний порушником “ефект” від реалізації загроз;
- складність розробки і реалізації;
- необхідні витрати;
- можливе покарання у випадку ідентифікації погрози, порушника й ін.

Усі загрози безпеки і зловживання доцільно розділити на три основні групи:

- безпечні загрози, яких легко запобігають чи виявлявити, нейтралізувати або усунути;
- небезпечні, для яких процеси запобігання, виявлення і нейтралізації, з погляду технології, не відпрацьовані;
- дуже небезпечні, котрі мають максимальні оцінки по всіх параметрах і реалізація процесів протистояння пов‘язані з величезними витратами.

Дане виділення є несуворим і може варіювати і змінюватися при зміні методу розрахунків комплексної оцінки. У той же час даний підхід буде корисним при оцінці ризику.

На основі проведеного аналізу представляється можливість опису привабливості загроз для порушника, яка будується з використанням наступних змінних:

B_0 - виграш порушника від реалізації загрози;

C_0 - витрати порушника для підготовки і реалізації загрози.

Отже можна стверджувати, що чим більше значення відносини B_0/C_0, тим більше економічних основ для реалізації погрози.

Тоді показник привабливості загрози для порушника (γ) дорівнює:

$$\gamma = \frac{P^U B_0}{C_0}, \qquad (2.1)$$

де P^U – визначає середнє значення успіху реалізації загрози.

Порушник прагне розробити/інтегрувати загрозу з максимальним значенням показника привабливості (g > max). Основною задачею СІБ є запобігання проникнення і розвитку загроз, тобто мінімізація даного показника (g> min).

Розглянемо модель можливих результатів взаємодії комплексу погроз і СІБ. Проміжними в моделі можуть бути стани p_1, p_2, p_3, p_4, p_5, p_6, характеристики яких відображують наступне:

- стан p_1 - загроза відвернена, імовірність такого результату дорівнює $P^{П}$;

- стан p_2 - загроза не відвернена, імовірність такого результату дорівнює $1 - P^{П}$;
- стан p_3 - загроза виявлена, імовірність такого результату дорівнює P^{O};
- стан p_4 - загроза не виявлена, імовірність такого результату дорівнює $1 - P^{O}$;
- стан p_5 - загроза нейтралізована, імовірність такого результату дорівнює P^{H};
- стан p_6 - загроза не нейтралізована, імовірність такого результату дорівнює $1 - P^{H}$.

Результуючими станами взаємодії можуть бути події A,B,C і D (рис. 2.1). Розглянемо докладніше їхній зміст.

Результуюча подія A - загроза відвернена. Тоді імовірність такого результату (P^{A}) дорівнює:

$$P^{A} = P^{П} \tag{2.2}$$

Результуюча подія B - загроза не відвернена, але виявлена і нейтралізована. Імовірність результату (P^{B}) дорівнює:

$$P^{B} = (1 - P^{П})P^{O}P^{H} \tag{2.3}$$

Результуюча подія C - загроза не відвернена, виявлена, але не нейтралізована. Імовірність результату (P^{C}) дорівнює:

$$P^{C} = (1 - P^{П})P^{O}(1 - P^{H}) \tag{2.4}$$

Результуюча подія D - загроза не відвернена і не виявлена. Імовірність результату (P^{D}) дорівнює:

$$P^{D} = (1 - P^{П})(1 - P^{O}) \tag{2.3}$$

Таким чином, події A і B є сприятливими для СІБ, а події C і D - несприятливі для СИБ, але сприятливі для порушника. Визначимо імовірність результату подій (A+B) і (C+D).

Імовірність події A+B (P^{AB}) дорівнює:

$$P^{AB} = P^{П} + (1 - P^{П})P^{O}P^{H} \quad (2.4)$$

Імовірність події C+D (P^{CD}) дорівнює:

$$P^{CD} = (1 - P^{П})((1 - P^{П}) + P^{O}(1 - P^{H})) = (1 - P^{П})(1 - P^{O}P^{H}) \quad (2.5)$$

Таким чином, можна зробити висновок, що показник P^{CD} і є значенням успіху реалізації загрози в загальному випадку і справедливе наступне дорівнювання:

$$P^{U} = P^{CD} = (1 - P^{П})(1 - P^{O}P^{H}) \quad (2.6)$$

З урахуванням (2.8), вираз (2.1) приймає вигляд:

$$\gamma = \frac{(1 - P^{П})(1 - P^{O}P^{H})B_0}{C_0}, \quad (2.7)$$

Розглянемо далі процес комбінування порушником комплексу зловживань для досягнення поставленої мети. Основними критеріями є вибір на основі даних таблиці оцінок загроз з погляду їхньої небезпеки. При цьому, загрозами з кращими параметрами можна вважати ті, для яких показники приймають наступні значення:

Неможливо запобігти ($P^{П} = 0$);

Неможливо знайти ($P^{O} = 0$);

У даному випадку привабливість загрози очевидна і досить велика.

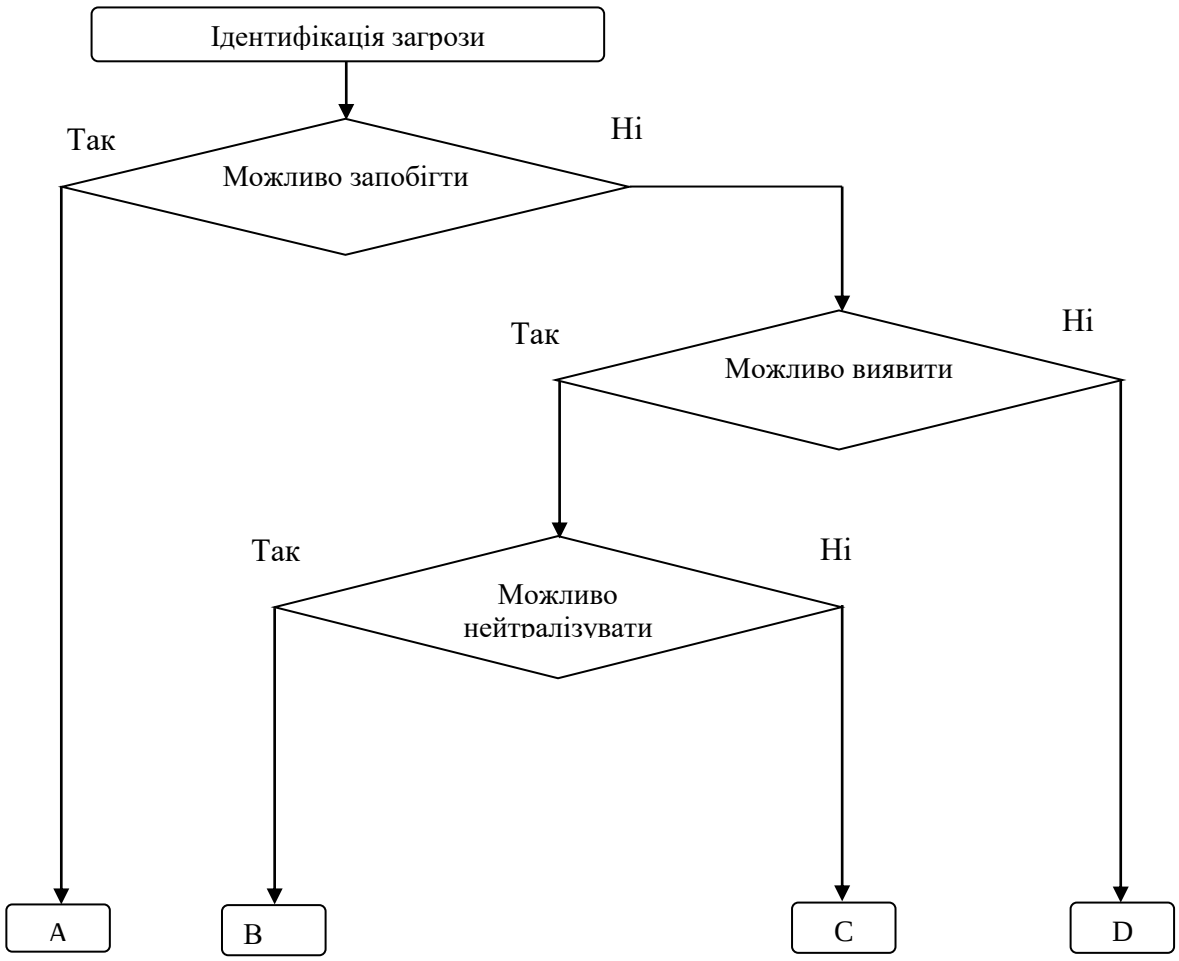

Рис. 2.7 Алгоритм аналізу реалізації загроз і протистояння СІБ

Достатньою умовою реалізації загрози в цьому випадку, є відношення $З_0 > В_0$, тому що значення успіху реалізації погрози P^U дорівнює 1:

$$P^U = (1 - P^П)(1 - P^O P^H) = (1 - 0)(1 - 0 \cdot P^H) = 1 \qquad (2.8)$$

де $P^П = 0$ – імовірність запобігання загрози СІБ;

$P^O = 0$ – імовірність виявлення загрози СІБ;

P^H - імовірність нейтралізації загрози СІБ. Тому що рівень нейтралізації загрози (P^H) залежить від інформації про неї, тобто можна стверджувати, що чим менше обсяг інформації про загрозу існує, тим менше імовірність, що будуть розроблені в СІБ механізми для її виявлення. У такому випадку, відповідно, не будуть розроблені і механізми для її нейтралізації. Іншими словами, коли $P^O \to 0$

і $P^H \to 0$. У такому випадку завжди буде справедливим твердження, що $P^H \le P^O$.

Тоді вираз (2.9) буде виглядати:

$$\gamma = \frac{B_0}{C_0} \tag{2.9}$$

що цілком відповідає виразу (2.1).

2.4. Модель порушника

Розглянемо модель потенційного порушника й імовірність його проходження системи захисту, припускаючи найбільш небезпечну ситуацію:

- Порушник може з'явитися у будь-який час, у будь-якому місці;
- Кваліфікація і поінформованість порушника може бути на рівні розроблювача системи;
- Постійно збережувана інформація про принципи роботи системи, включаючи секретну, порушнику відома;
- Для досягнення своєї мети порушник вибере наслабшу ланку в системі захисту інформації;
- Порушником може бути не тільки стороння особа, але й співробітник організації;
- Порушник може впровадити злочинні дії;
- Порушник може мати найбільш удосконаленими технічними засобами.

Позначимо через:

P_1 – імовірність появи порушника;

P_2 – імовірність того, що кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи;

P_3 – імовірність того, що порушнику відома інформація про принципи роботи системи, включаючи секретну;

P_4 – імовірність вибору порушником найбільш слабкої ланки в системі захисту інформації;

P_5 – імовірність того, що порушник - співробітник організації;

P_6 – імовірність того, що порушник впроваджує злочинні дії;

P_7 -імовірність того, що порушник має найбільш досконалі технічні засоби.

Розглянемо такі випадки:

- Порушник є співробітником організації.
  - ➢ впроваджує злочинні дії.

Тоді імовірність того, що порушник має найбільш досклоналі технічні засоби P_7=1. І імовірність того, що кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи P_2=1. Імовірність проходження системи захисту залежить від вибору слабкої ланки в системі захисту інформації P_4 і від імовірності того, що порушнику відома інформація про принципи роботи системи, включаючи секретну P_3.

$$P_1 \cdot P_2 \cdot P_3 \cdot P_4 \cdot P_5 \cdot P_6 \cdot P_7 = P_1 \cdot P_3 \cdot P_5 \cdot P_6 \qquad (2.12)$$

де: P_1 – імовірність появи порушника;

P_2 – імовірність того, що кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи;

P_3 – імовірність того, що порушнику відома інформація про принципи роботи системи, включаючи секретну;

P_4 – імовірність вибору порушником найбільш слабкої ланки в системі захисту інформації;

P_5 – імовірність того, що порушник - співробітник організації;

P_6 – імовірність того, що порушник впароваджує злочинні дії;

P_7 -імовірність того, що порушник має найбільш досконалі технічні засоби.

- ➢ впроваджує незлочинні дії.

Тоді імовірність того, що порушник має найбільш досоналі технічні засоби P_7=1. Імовірність проходження системи захисту інформації не залежить від рівня поінформованості P_2, і від імовірності того, що йому відома інформація про принципи роботи системи, включаючи секретну P_3 але залежить від вибору слабкої ланки в системі захисту інформації P_4:

$$P_1 \cdot P_5 \cdot (1 - P_6) \cdot P_7 \cdot P_4 = P_1 \cdot P_5 \cdot (1 - P_6) \cdot P_4 \quad (2.13)$$

де: P_1 – імовірність появи порушника;

P_4 – імовірність вибору порушником найбільш слабкої ланки в системі захисту інформації;

P_5 – імовірність того, що порушник - співробітник організації;

P_6 – імовірність того, що порушник впроваджує злочинні дії;

P_7 -імовірність того, що порушник має найбільш досконалі технічні засоби.

- Порушник є сторонньою особою.
  - розпочинає злочинні дії.

Тоді розглядаємо тільки ту ситуацію, коли імовірність того, що кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи P_2 =1, і імовірність того, що порушник має найбільш досконалі технічні засоби P_7=1. Кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи. Порушник має найбільш досконалі технічні засоби.

Припустимо, що порушнику відома інформація про принципи роботи системи, включаючи секретну, тоді імовірність проходження системи захисту інформації не залежить від вибору найбільш слабкої ланки системи захисту інформації P_4:

$$P_1 \cdot (1 - P_5) \cdot P_6 \cdot P_3 \cdot P_2 \cdot P_7 = P_1 \cdot (1 - P_5) \cdot P_6 \cdot P_3 \quad (2.14)$$

де: P_1 – імовірність появи порушника;

P_2 – імовірність того, що кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи;

P_3 – імовірність того, що порушнику відома інформація про принципи роботи системи, включаючи секретну;

P_5 – імовірність того, що порушник - співробітник організації;

P_6 – імовірність того, що порушник впровадджує злочинні дії;

P_7 -імовірність того, що порушник має найбільш досконалі технічні засоби.

Припустимо, що порушнику невідома інформація про принципи роботи системи, тоді імовірність проходження системи захисту інформації залежить від вибору найбільш слабкої ланки в системі захисту інформації P_4:

$$P_1 \cdot (1-P_5) \cdot P_6 \cdot (1-P_3) \cdot P_4 \cdot P_2 \cdot P_7 = P_1 \cdot (1-P_5) \cdot P_6 \cdot (1-P_3) \cdot P_4 \quad (2.15)$$

де: P_1 – імовірність появи порушника;

P_2 – імовірність того, що кваліфікація і поінформованість порушника знаходиться на рівні розроблювача системи;

P_3 – імовірність того, що порушнику відома інформація про принципи роботи системи, включаючи секретну;

P_4 – імовірність вибору порушником найбільш слабкої ланки в системі захисту інформації;

P_5 – імовірність того, що порушник - співробітник організації;

P_6 – імовірність того, що порушник впроваджує злочинні дії;

P_7 -імовірність того, що порушник має найбільш досконалі технічні засоби.

- впроваджує незлочинні дії.

Тоді імовірність проходження системи захисту інформації не залежить від імовірності того, що кваліфікація і поінформованість порушника знаходяться на рівні розроблювача системи P_2 і від імовірності того, що порушник має найбільш досоналі технічні засоби P_7, але залежить від імовірності вибору порушником найбільш слабкої ланки в системі захисту інформації P_4, і не залежить від імовірність того, що порушнику відома інформація про принципи роботи системи, включаючи секретну P_3:

$$P_1 \cdot (1-P_5) \cdot (1-P_6) \cdot P_4 \quad (2.16)$$

де: P_1 – імовірність появи порушника;

P_4 – імовірність вибору порушником найбільш слабкої ланки в системі захисту інформації;

P_5 – імовірність того, що порушник - співробітник організації;

P_6 – імовірність того, що порушник впроваджує злочинні дії.

Тоді загальна імовірність проходження порушником системи захисту інформації буде об'єднання всіх імовірностей, отриманих у вищерозглянутих випадках, тому що ці випадки взаємовиключні:

$$\begin{aligned} \mathrm{P} = P_1 \cdot P_3 \cdot P_5 \cdot P_6 \cup P_1 \cdot P_5 \cdot (1-P_6) \cdot P_4 \cup P_1 \cdot (1-P_5) \cdot P_6 \cdot P_3 \cup \\ \cup P_1 \cdot (1-P_5) \cdot P_6 \cdot (1-P_3) \cdot P_4 \cup P_1 \cdot (1-P_5) \cdot (1-P_6) \cdot P_4 \end{aligned} \qquad (2.17)$$

2.5. Модель системи захисту інформації

Оцінка рівня чи захищеності ефективності системи ЗІ можлива на підставі аналізу узагальненої моделі взаємодії системи захисту інформації (СЗІ) і навколишнього середовища. Причому, узагальнена модель повинна відображати процес ЗІ як процес взаємодії дестабілізуючих факторів і засобів захисту. В даний час широко використовується ймовірнісна модель (мал. 3.3), у відповідності, з якою обробка інформації на об'єкті O_i, здійснюється в умовах впливу на інформацію різних загроз $\{Y_j\}$. Для забезпечення інформаційної безпеки об'єкта використовується СЗІ $\{C_\eta\}$, що нейтралізуюче впливає на дестабілізуючі фактори і загрози.

У загальному випадку P_y - імовірність негативного впливу j-го фактора на і-й об'єкт у к- м стані, а $P_{зі}$ - імовірність нейтралізації, впливу j -ї погрози на і-й об'єкт у k-м стані з застосуванням η -го засобу захисту. При цьому характер і рівень впливу одних факторів не залежить від характеру і рівня впливу інших. Однак можуть бути і взаємозалежні фактори. Точно так і засоби захисту можуть бути як незалежні, з погляду ефективності застосовуваного захисту, так і взаємозалежними.

У попередньому підрозділі ми змоделювали поводження потенційного порушника, що багато в чому визначає і принципи побудови СЗІ.

Визначимо, що таке порушення. Порушенням вважається спроба несанкціонованого доступу (НСД) до будь-якої частини підлягаючіої захисту інформації, що зберігається, обробляється або передається.

Оскільки час і місце прояву навмисного НСД спрогнозувати неможливо, доцільно розробити деяку модель поводження потенційного порушника, припускаючи найбільш небезпечну ситуацію:

- Порушник може з'явитися в будь-який час і в будь-якім місці;
- Кваліфікація і поінформованість порушника може бути на рівні розроблювача системи;
- Постійно збережена інформація, про принципи роботи системи, включаючи секретну, порушнику відома;
- Для досягнення своєї мети порушник вибере найбільше слабку ланку в СЗІ;
- Порушником може бути не тільки стороння особа, але й співробітник організації.

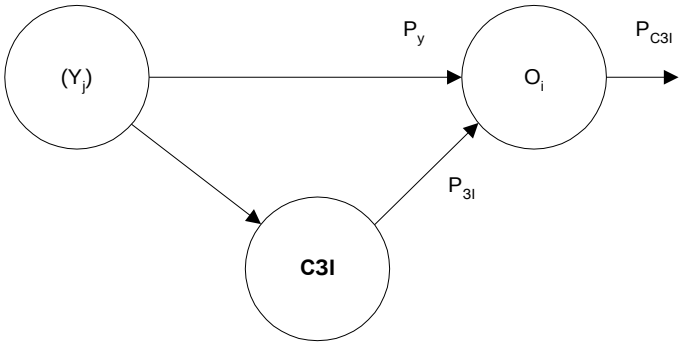

Рис. 2.8 Узагальнена модель процесу захисту інформації

Дана модель дозволяє визначитися з вихідними даними для побудови СЗІ і намітити основні принципи її побудови.

Згідно п.1 необхідно будувати систему, що постійно діє і має замкнутий контур.

Згідно п.2 СЗІ повинна, по можливості, відповідати очікуваній поінформованості і кваліфікації порушника.

Згідно п.3 и 4 для подолання системи захисту необхідна перемінна секретна інформація, відома тільки користувачеві і підсумкова надійность СЗІ визначається його найслабшою ланкою. І останнє, на підставі п.5, розрахунок надійності

захисту має вироблятися для двох можливих варіантів: порушник перебуває за межами контрольованої зони і - усередині неї.

У загальному випадку найпростіша модель захисту може бути представлена у виді (рис. 2.10), де O_i-об'єкт захисту, $\{C_\eta\}$- СЗІ, $P_{зі}$- імовірність нейтралізації НСД.

З рис. 2.10 видно, що об'єкт захисту поміщений у замкнуте й однорідне середовище, що і являє собою СЗІ. Ефективність захисту залежить від особливостей і характеристик СЗІ.

Для одержання більш об'єктивної оцінки СЗІ при розробці моделі необхідно враховувати витрати часу на подолання системи захисту порушником.

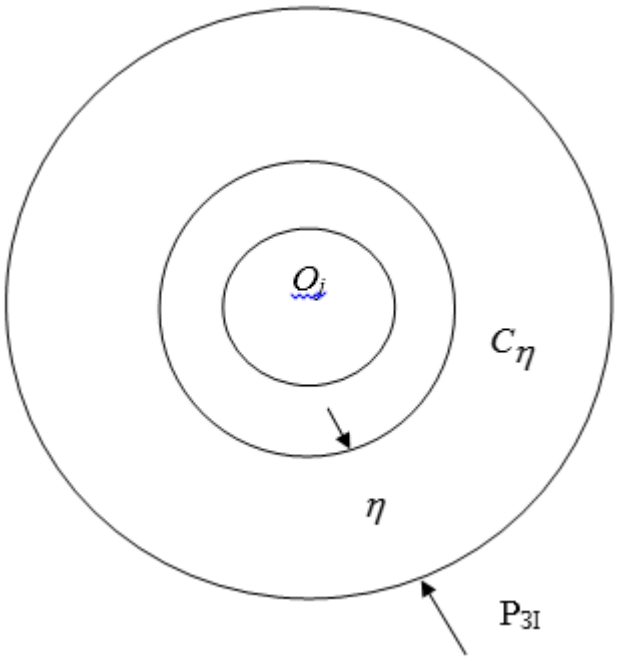

Рис. 2.9 Модель захисту

Загальновідомо, що інформація згодом може утратити свою цінність. Тоді умовою ефективності СЗІ при відсутності її обходу можна вважати перевищення витрат часу порушником на її подолання над часом життя інформації. Це співвідношення можна записати у виді:

$$P_{зі} = (1 - P_{пр})(1 - P_{об}) \qquad (2.18)$$

за умови $t_ж > t_{пр}$ і $P_{об} > 0$, де P_{ijk_η} - імовірність не подолання системи чи порушником нейтралізації НСД; $P_{пр}$ – імовірність подолання СЗІ за час, менший часу життя інформації $t_{пр} < t_ж$; $P_{об}$- імовірність обходу СЗІ.

При реалізації виразу (2.18) можливі наступні випадки, коли:

$P_{зі}=1$, якщо $t_{ж} < t_{пр}$ и $P_{об}=0$;

$P_{зі}=(1-P_{пр})$, якщо $t_{ж} > t_{пр}$ и $P_{об}=0$;

$P_{пр}=0$, якщо $t_{ж} < t_{пр}$;

$P_{пр}>0$, якщо $t_{ж} > t_{пр}$.

Це вираз справедливийе для випадку присутності двох порушників, причому один переборює перешкоду, а другий її обходить. Якщо ж НСД здійснює один порушник, то він обов'язково вибере один зі шляхів - найбільше простій. Тоді вираз (2.18) для даного випадку запишеться у вигляді:

$$P_{зі} = (1 - P_{пр}) \cup (1 - P_{об}), \tag{2.19}$$

де $\cup$-знак “АБО”.

Отже, ефективність СЗІ після визначення і порівняння величин $(1-P_{пр})$ і (1-роб) буде дорівнювати найменшому значенню однієї з них.

Необхідно також враховувати, що обхід СЗІ може мати кілька шляхів. Тоді в цьому випадку вираз (2.19) прийме вигляд:

$$P_{зі} = (1 - P_{пр}) \cup (1 - P_{об1}) \cup (1 - P_{об2}) \cup .... \cup (1 - P_{обп}), \tag{2.20}$$

де n- число можливих шляхів обходу СЗІ.

У тому випадку, коли інформація має свою цінність і забезпечити $t_{ж} < t_{пр}$ за якимись причинами неможливо, застосовується СЗІ, що володіє властивостями контролю і виявлення НСД. Вона може в себе включати додаткову систему контролю, що здійснюється періодично. Тоді імовірність подолання СЗІ порушником у цьому випадку можна описати виразом

$$P_{пр_k} = 1 - \frac{t_{пр}}{t_k}, \tag{2.21}$$

де t_k - періодичність контролю.

З виразу (2.20) видно, що при збільшенні $t_{пр}$ імовірність подолання СЗІ зменшується, і при $t_{пр}>t_k$ НСД через систему не має сенсу. У цьому випадку порушник обов'язково буде шукати шлях для обходу системи захисту.

Але тому що дана СЗІ має здатність виявляти НСД, то можна записати $P_{обн}=1-P_{прк}$.

При $t_{пр}>t_k$ порушник буде виявлений, тобто $P_{обн} = 1$. В іншому випадку $t_k<t_{пр}<t_{обн}$ імовірність виявлення порушника буде визначатися як і при визначенні виразу (2.21) і запишеться у такий спосіб:

$$P_{обн} = 1 - \frac{t_{пр}}{t_{об}} \tag{2.22}$$

Крім уже перелічених складових моделі необхідно враховувати імовірність можливості відмовлення системи захисту, що може відбутися через стихійне лихо або у результаті цілеспрямованих дій порушника:

$$P_{СЗИ} = C_к P_{отн}(1-P_{отн})(1-P_{обх1}) \cup (1-P_{обх2}) \cup .... \cup (1-P_{обхn}) \tag{2.23}$$

де C_η є частка η-го режиму роботи СЗІ в аналізований конкретний період часу. Найбільш об'єктивним є представлення C_η у виді інтервалу часу перебування системи захисту в η-м стані (Δt_η) в загальній тривалості оцінюваного інтервалу часу ΔT, тобто

$$C_\eta = \frac{\Delta t_\eta}{\Delta T}. \tag{2.24}$$

На практиці в більшості випадків СЗІ складається з декількох ланок і рубежів. Відомо, що при спробі перебороти захист, порушник спробує використовувати найбільше слабкий напрямок у цій системі. З цієї причини підсумкова міцність СЗІ буде визначатися міцністю найслабкішим напрямком у цій системі. З цієї причини підсумкова міцність СЗІ буде визначатися міцністю найбільш слабкого напрямку в системі.

Якщо міцність слабкого напрямку СЗІ не задовольняє заданим вимогам, то цей напрямок зміцнюється або заміняється на більш міцний.

Отже, імовірність ефективного захисту інформації при багатоланковій і багаторубіжній системі визначається залежністю

$$P_{\Sigma} = P_{СЗІ1} P_{СЗІ2} \cdots P_{СЗІN} \qquad (2.25)$$

де $P_{СЗІ}$ – імовірність ефективного захисту N -ої ланки чи рубежу СЗІ.

Необхідно при цьому врахувати фактор часу. Дійсно, показники захищеності, виражені приведеними вище залежностями, будуть справедливі лише для відрізка часу δ t. Якщо ж цей інтервал часу ΔT, на якому оцінюється захищеність інформації істотно більше δ t, тоді

$$P_{\Sigma}(\Delta t) = \prod_{z=1}^{\bar{z}} P_{СЗІ}(\delta t) \qquad (2.26)$$

де $\bar{z} = \left[\frac{\Delta T}{\delta t} \right]$ ціле, а $P_{СЗІ}(\delta t)$ -показник захищеності інформації на окремій ланці чи рубежі на z-му інтервалі довжиною δ t.

Розглянута модель приваблива своєю простотою, тому що для визначення показників захищеності інформації досить знати ймовірністні характеристики дестабілізуючих впливів на інформацію й ефективність функціонування системи захисту. Недоліком моделі є відсутність обліку можливого збитку від впливу різних факторів на функціонування СЗІ й ефективність самої СЗІ. Але варто враховувати, що користувач не знає, коли і якими засобами зловмисник спробує здійснити НСД. Тому моделями даного типу варто корисуватися лише для оперативної оцінки можливостей проектованих СЗІ та СЗІ що експлуатуються.

Але доцільніше використовувати модель, у якій відображається взаємодія самої СЗІ з джерелом інформації (ДІ) і користувачем інформації (КІ). Причому в цій моделі враховується вплив зовнішнього середовища на всі складові (СЗІ, ДІ, КІ), що по своїй природі буває як природне, так і штучне (дії зловмисників). Аналіз концептуальних підходів до ЗІ та еволюції організаційно-технічних засобів, призначених для цих цілей, показав доцільність використання для опису і наступного аналізу ієрархічної структури взаємозв'язку окремо узятих систем - СЗІ, КІ, ДІ Неважко помітити, що представлена на мал.3 модель взаємозв'язку

здійснюється як по вертикалі, по основних рубежах захисту, так і по горизонталі - межсистемний зв'язок на одному з рубежів ЗІ.

Процес функціонування комплексу систем СЗІ, КІ і ДІ складається з їхньої взаємодії між собою і з зовнішнім середовищем. Це здійснюється через вхідні (i, m, p) і вихідні (j, n, q) вузли моделі. При цьому реалізуються загальносистемні, міжсистемні (W_{mj}, W_{in},…)і самостійні функції систем СЗІ, КІ, і ДІ. Загальна кількість вузлів кожної із систем визначається кількістю системних властивостей, що виявляються на кожнім рубежі ЗІ.

Для рішення комплексу задач ЗІ, ефективного керування безпекою надійністю інформації, що циркулює між КІ і ДІ необхідним є аналітичний опис цієї взаємодії, що можливо для будь-якого рівня причинно-наслідкової невизначеності цих зв'язків на різних рубежах ЗІ.

Для опису внутрісистемних (СЗІ, КІ, ДІ) зв'язків скористаємося наступною системою матричних рівнянь

$$\begin{cases} A_j = A_j W_{ji} \\ A_n = A_m W_{mn} \\ A_q = A_p W_{qp} \end{cases} \tag{2.27}$$

припускаючи, що для змінних

$$\begin{cases} a_j = \sum a_i w_{ji} \\ a_n = \sum a_m w_{nm} \\ a_q = \sum a_p w_{qp} \end{cases} \tag{2.28}$$

Аналогічний аналітичний опис справедливий і для опису зв'язку розглянутих систем із зовнішнім середовищем, через змінні {a} по входах

$$\begin{cases} A_i = A_{i0} W_{i0} \\ A_m = A_{m0} W_{m0} \\ A_p = A_{p0} W_{p0} \end{cases} \tag{2.29}$$

з обліком змінних

$$\begin{cases} a_{0i} = \sum a_{i0} w_{i0} \\ a_{0m} = \sum a_{m0} w_{m0} \\ a_{0p} = \sum a_{p0} w_{p0} \end{cases} \quad (2.30)$$

а по входах цих систем

$$\begin{cases} a_{j0} = \sum a_{j0} w_{j0} \\ a_{n0} = \sum a_{n0} w_{n0} \\ a_{q0} = \sum a_{q0} w_{q0} \end{cases} \quad (2.31)$$

або у матричному виді

$$\begin{cases} A_q = A_{q0} W_{q0} \\ A_j = A_{j0} W_{j0} \\ A_n = A_{n0} W_{n0} \end{cases} \quad (2.32)$$

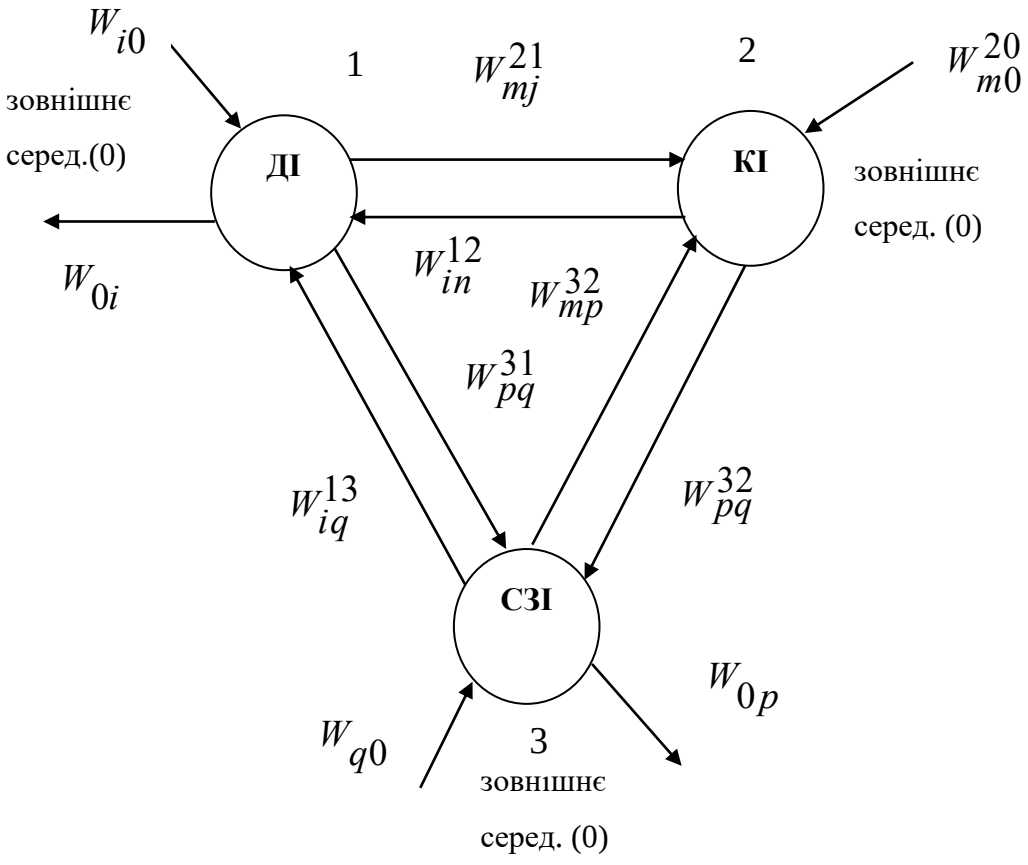

Рис. 2.10 Модель взаємозв'язку СЗІ з ДІ і КІ

Такий опис справедливий і для міжсистемних зв'язків СЗІ, КІ і ДІ. У матричному вигляді без обліку зовнішніх впливів його можна представити в наступному виді:

$$\begin{cases} A_i = A_n W_{in} + A_q W_{iq} \\ A_m = A_j W_{mj} + A_q W_{mq} \\ A_p = A_j W_{pj} + A_n W_{pn} \end{cases}, \qquad (2.33)$$

Розглядаючи й аналізуючи вплив зовнішнього середовища на функціонування СЗІ і систем рівнянь (2.27)–(2.33), можна прийти до наступної системи матричних рівнянь

$$\begin{cases} A_{0j} = A_i W_{ji} W_{0i} = (A_n W_{in} + A_q W_{iq} + A_{i0} W_{i0}) W_{ji} W_{0j} \\ A_{0q} = A_p W_{qp} W_{0q} = (A_j W_{jp} + A_n W_{pn} + A_{p0} W_{p0}) W_{qp} W_{0q} \\ A_{0n} = A_m W_{nm} W_{0n} = (A_j W_{mj} + A_q W_{mq} + A_{m0} W_{m0}) W_{nm} W_{0n} \end{cases} \qquad (2.34)$$

Аналізуючи систему (2.34) щодо керованих змінних {а}, можна вирішити задачу управління безпекою інформації, оцінити рівні ефективності рубежів захисту, проаналізувати можливості СЗІ в різних умовах експлуатації і на різних об'єктах КІ. У найпростішому випадку це можливо у виді аналізу системних властивостей, шляхом їхнього перебору по вертикалі і горизонталі й обліку їхній відповідній взаємодії для різних систем - КІ і ДІ, КІ і СЗІ, СЗІ і ДІ. У загальному ж випадку кращим є аналітичний підхід, що враховує як можливості досконального аналізу роботи СЗІ, так і об'єктивної оцінки ефективності її функціонування при різних умовах і зовнішніх впливах.

В узагальненому вигляді рівняння (2.27) – (2.33) можна записати у наступному виді

$$a_I^K = \sum_{\substack{k \in K \\ \varphi \in \Psi}} a_N^{\Psi} W_{IN}^{k\varphi} + \sum a_{IN}^k W_{I0}^{K0} + \sum_{\substack{I \neq J \\ k \in K}} a_j W_{JI}^{KK} \qquad (2.35)$$

де I, J - точки входу і виходу системи ДО $(I \neq J)$; N - точки виходу системи φ.

У приведеному виразі (2.35) складові правої частини в порядку проходження являють собою добуток узагальнених множин змінних довільної

досліджуваної К - системи на оператори {W}, що характеризують можливість (способи) реалізації цих властивостей, трансльовані відповідно N-точками виходу φ-системи, зовнішнього середовища (0) і Ψ-точками внутрішніх перемінних К-системи. Модель, реалізована на базі цього виразу, дозволяє позбутися недоліків, що притаманні ймовірнісним моделям.

2.6. Модель комплексної оцінки СЗІ

Пропонується розглянути наступну модель створення і комплексної оцінки системи захисту інформації. Модель СЗІ представлена у виді наступних основних блоків показників:

- Блок показників “ОСНОВИ”;
- Блок показників “НАПРЯМКИ”;
- Блок показників “ЕТАПИ”.

Розглянемо зміст цих блоків.

Блок показників ОСНОВИ (O_i)

Проведений аналіз основних підходів до створення СЗІ дозволяє виділити наступну групу показників:

- $ПРО_1$. Нормативно-правова і наукова база;
- $ПРО_2$. Структура і задачі органів;
- $ПРО_3$. Організаційні заходи і методи (політика безпеки);
- $ПРО_4$. Програмно-технічні способи і засоби.

Значення кожного з перерахованих показників блоку “ОСНОВИ” має бути деталізованим для конкретної ІС.

Блок показників НАПРЯМКИ (H_j)

Проведений аналіз існуючих способів і методів захисту інформації дозволяє виділити наступні основні показників створення й оцінки СЗІ:

- H_1. Захист об'єктів корпоративних систем;
- H_2. Захист процесів, процедур і програм обробки інформації;
- H_3. Захист каналів зв'язку;

- H_4. Придушення побічних електромагнітних випромінювань;
- H_5. Управління системою захисту.

Очевидно, що кожний з показників блоку “напрямків” має бути структурований у залежності від заданої глибини деталізації СЗІ.

Блок показників ЕТАПИ (M_k)

В даний час розглядають різні етапи побудови СЗІ усі вони досить ефективні і дозволяють вирішувати поставлені задачі. На основі проведеного аналізу пропонується розгляд наступних показників створення СЗІ, котрі підлягають оцінці:

- M_1. Визначення інформації, що підлягає захисту;
- M_2. Виявлення повної множини потенційно можливих загроз і каналів витоку інформації;
- M_3. Проведення оцінки уразливості і ризиків інформації при наявній множині загроз і каналів витоку;
- M_4. Визначення вимог до системи захисту;
- M_5. Здійснення вибору засобів захисту інформації і їхнії характеристик;
- M_6. Впровадження й організація використання обраних заходів, способів і засобів захисту;
- M_8. Здійснення контролю цілісності і управління системою захисту.

Етапи можуть бути розбиті на більш детальні пункти (кроки).

Структура моделі оцінки СЗІ наочно показана на рис. 2.11.

Вона полягає в логічному об'єднанні показників блоків “ОСНОВИ”, “НАПРЯМКИ” і “ЕТАПИ” у МАТРИЦЮ ОЦІНОК, що складає з К елементів.

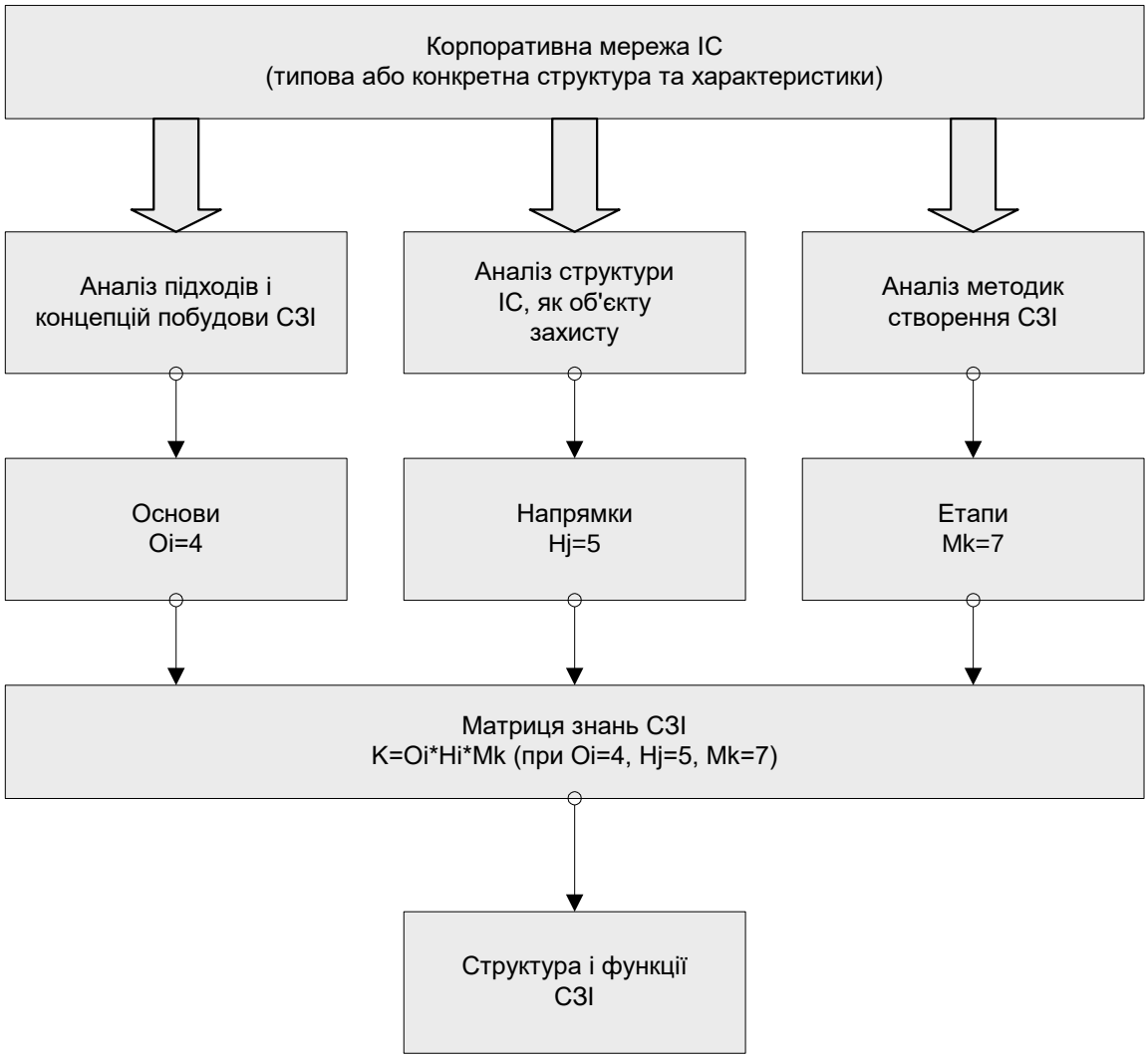

Рис. 2.11 Структура моделі оцінки СЗІ

У загальному випадку кількість елементів “матриці” може бути визначене зі співвідношення :

$$K = O_i \cdot H_j \cdot M_k \tag{2.36}$$

На основі проведеного вище аналізу в даному варіанті (за умови, що $O_i = 4, H_j = 5, M_k = 7$) загальна кількість елементів “матриці” складає $K = 4 \cdot 5 \cdot 7 = 140$

Зміст кожного з елементів матриці, що формується із сукупності трьох приватних показників:

Перше знакмісце позначає номер показника “ЕТАПИ”, друге знакомісце — номер показника “НАПРЯМКИ”, а третє знакомісце — номер показника “ОСНОВИ”.

У загальному випадку для “Матриці експертних оцінок” формується 140 питань (за числом її елементів). Відповіді на ці питання дозволяють скласти повне уявлення про СЗІ й оцінити досягнутий рівень захисту.

Розглянута модель створення і комплексної оцінки системи захисту інформації. Основним завданням моделі є наукове забезпечення процесу створення системи інформаційної безпеки за рахунок правильної оцінки ефективності ухвалюваних рішень і вибору раціонального варіанту технічної реалізації системи захисту інформації.

Модель СЗІ представлена у виді наступних основних блоків показників: основи, напрямки, етапи. Елементи основ і напрямів, розглядаються нерозривно один з одним. Оскільки етапів сім, і по кожному треба освітити 20 питань то в цілому для формування уявлення про конкретну систему захисту необхідно відповісти на 140 простих питань. Відповіді на ці питання дозволяють скласти повне уявлення про СЗІ й оцінити досягнутий рівень захисту.

3. МЕТОДИ ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Оцінювання рівня інтегрованої загрози на ІС

При формалізації задачі оцінювання ефективності системи захисту інформаційної системи будемо вважати, то система будується у вигляді багаторівневої ієрархії I_p, де p-кількість рівнів ієрархії (у нашому випадку p=3). Для підсистем на кожному p-му рівні ієрархії вибрана множина об'єктів захисту M_{kp}, де k-максимальний номер об'єкта на p-му рівні ієрархії. За допомогою експертного оцінювання для кожного M_{kp} об'єкта сформовано вектор загроз V_{skp}, де s-номер загрози для k-го об'єкта на p-му рівні ієрархії.

Зниження ефективності функціонування інформаційно-аналітичної системи на кожному p-му рівні ΔE_P визначається складним впливом реально діючих загроз на об'єкти p-го рівня, тобто

$$\Delta E_p(t) = F\{M_{kp}, V_{skp}, t\}, \tag{3.1}$$

де F{*} - функціонал, що описує вплив реально діючих загроз V_{skp} на множину об'єктів M_{kp} в підсистемі p-го рівня; t - часова характеристика.

Будемо вважати, що відновлення ефективності підсистеми p-го рівня ІАС можливо лише за рахунок проведення адекватного рівню інтегрованої загрози комплексу заходів безпеки Z_{jkp}, де j-максимальний номер заходу безпеки Z стосовно k-го об'єкта підсистеми p-го рівня. Для ідеального випадку цей постулат можна записати у вигляді

$$\forall Z_{jkp} : \Delta E_p(t) = 0, \quad j = 1, J; k = 1, K; t > 0, \tag{3.2}$$

де символ V - читається так: "комплекс J заходів безпеки стосовно К об'єктів підсистеми p-го рівня нейтралізує дію інтегрованої загрози, яка знизила ефективність ІАС на величину ΔE_P на момент часу t".

Звідси можна записати функцію управління безпекою підсистеми р-го рівня ІАС підрозділу

$$\forall Z_{jkp}(t) : \Delta E_p(t+\Delta t) \le \Delta E_p(t), \quad j = 1, J; k = 1, K; \Delta t > 0, \tag{3.3}$$

де Δt - час реакції системи на виявлену загрозу.

Практика показує, що для розв'язування задач такого класу відомі методики й алгоритми формально не можуть бути подані суворими математичними виразами та співвідношеннями типу (3.1) та (3.2). Оскільки вхідними даними у подібних задач класу являються повільно мінливі у часі процеси з нечіткими кількісно-якісними параметрами, з різним ступенем достовірності, а в багатьох випадках і дезінформаційного змісту, а вихідними даними повинні бути кількісні, якісні і кількісно-якісні результати, то необхідно вибрати відповідний науково-методичний аппарат для їх отримання.

Основними вимогами, що пред'являються до науково-методичного апарату , який використовується для розв'язання подібних задач, є виявлення, аналіз і оцінка можливих загроз ІАС, їх характеру і рівнів, аналіз причин їх виникнення і оцінка дестабілізуючих чинників, попередні оцінки їхнього спрямування та наслідків проявлення, прогнозування тенденцій змін криміногенної обстановки та активності порушників, появи нових можливих загроз (наприклад, терористична атака на США 11 вересня 2001 року) та оцінка їх рівнів, а також можливість обгрунтування порогів реагування на виявлений рівень інтегрованої загрози ІАС підрозділу .

Широко відомий науково-методичний аппарат (НМА), що використовується для рішення таких задач, базується, як правило, на методах експертного оцінювання, проб і помилок, що вносить елементи суб'єктивізму в розрахунки і супроводжується досить великими похибками.

Оскільки задача оцінювання рівня інтегрованої загрози АІС у формальному виді представляється у вигляді I_p- рівневої ієрархічної задачі (рис. 3.1), то для її вирішення доцільно вибрати НМА , який базується на використанні методів дослідження операцій, аналізу ієрархій, векторної алгебри, експертного оцінювання і математичного моделювання.

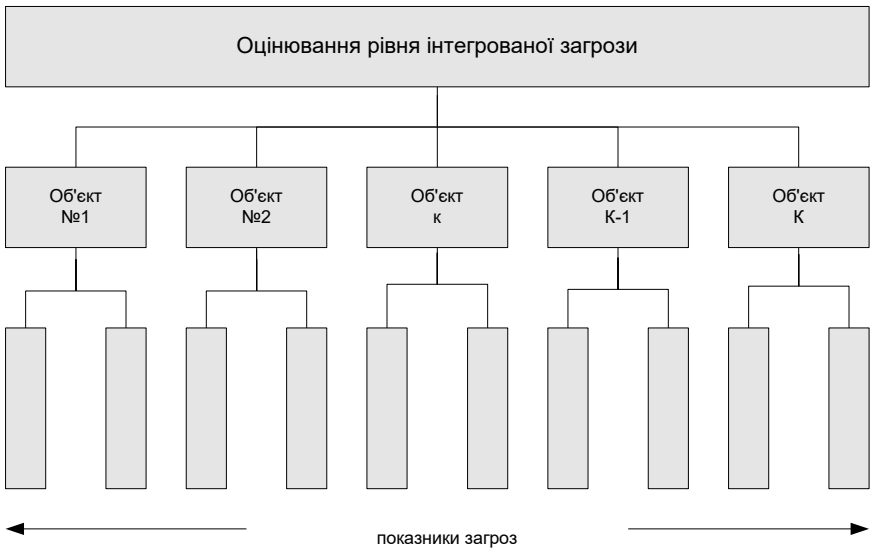

Рис. 3.1 Ієрархія побудови задачі оцінювання рівня інтегрованої загрози АІС

Вибраний НМА дозволяє на основі всебічного аналізу проявів загроз об'єктам захисту отримувати кількісні оцінки рівня інтегрованої загрози U, то еквівалентно оцінці зниження ефективності АІС в цих умовах (U ~ ΔE).

Пропонується при рішенні данної задачі вибрати p=3 рівні ієрархії (рис. 3.1):

1-й рівень - формулюється мета оцінювання;

2-й рівень - визначається множина $\{M_k\}$ об'єктів захисту відповідної підсистеми, яким можуть проявлятися загрози.

3-й рівень - визначаються показники прояву загроз функціонуванню об'єктів у складі розглядаємої підсистеми.

Вибраний НМА дозволяє отримувати на вибраний момент оцінювання t кількісне значення підсумкового рівня інтегрованої загрози U в системі координат: рівень загрози - час.

На рис. 3.2 наведено гіпотетичний приклад оцінки зростання рівня інтегрованої загрози U на інтервалі $[T_4, T_1]$.

Для якісного та всебічного оцінювання рівня інтегрованої загрози U необхідно вибрати достатньо повну систему (вектор) показників прояву загроз об'єктам захисту. Слід зауважити, що для кожної підсистеми такий вектор мас

бути свій. Для полегшення побудови ієрархії пропонується типова (базова) система показників, яку в кожному конкретному випадку доповнюють або скорочують відповідно до обстановки та регіону (області), по відношенню до якої організовується згадане оцінювання.

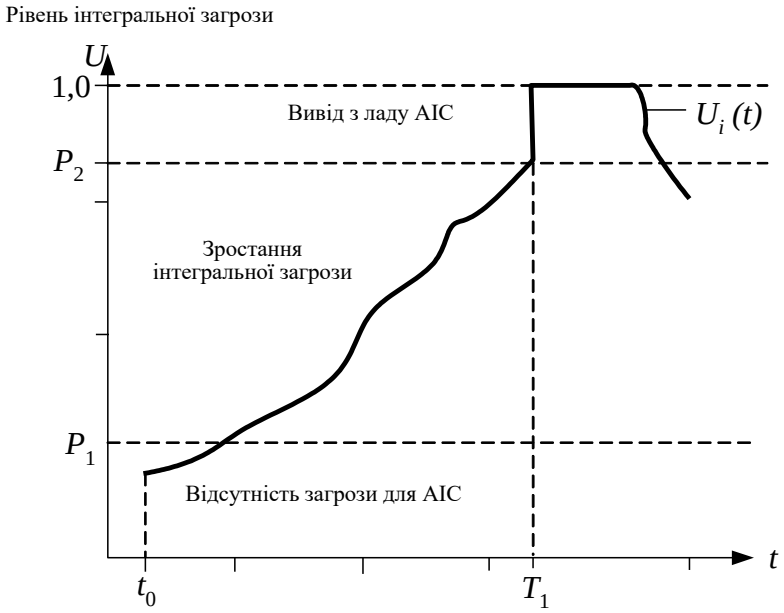

Рис. 3.2 Гіпотетичний приклад з оцінки зростання рівня інтегрованої загрози U на інтервалі [T_4, T_1]

Оцінювання рівня загрози k-му об'єкту (k=1, К) здійснюється по сукупності окремих показників U_{kn} для відповідного об'єкта. Кожний n-й показник відображає події, що зв'язані із зростанням (дійсним чи імітованим) загрози функціонуванню розглядаємої підсистеми АІС р-го рівня.

Дійсні події спостерігаються в ході повсякденної діяльності підсистеми, а імітовані - нав'язуються та суспільству для приховування істинних намірів щодо вибору сил та засобів для порушення роботи АІС.

На основі аналізу подій, що характеризували прояви небажаного впливу на аналогічні за призначенням АІС деяких провідних країн світу в останнє десятиліття, була сформована базова множина (вектор $U_K = U_1,.... U_n,..., U_N$. де N - розмірність вектора для k-го об'єкта) показників для оцінювання рівня інтегрованої загрози АІС підрозділу.

Для об'єктів підсистеми центрального (першого) рівня ІАС підрозділу:

• Вектор показників оцінювання загроз автоматизованим інформаційним системам U_{AIC}:

➢ несанкціонований доступ до конфіденційної інформації сторонніх осіб та користувачів АІС;

➢ несанкціоноване копіювання, спотворення або знищення інформації;

➢ викрадення носіїв інформації;

➢ хакерські атаки через локальну мережу, корпоративну мережу та мережу Інтернет;

➢ перехват інформації по каналах побічних електромагнітних випромінювань, наведень та по відвідним колам.

• Вектор показників оцінювання загроз Центральному Сховищу Даних $U_{цсд}$:

➢ несанкціонований доступ до конфіденційної інформації сторонніх осіб та користувачів АІС;

➢ зараження інформаційної системи програмними кодами, направленими на завдання шкоди (віруси, "троянські коні" тощо);

➢ несанкціоноване копіювання, спотворення або знищення інформації;

➢ викрадення носіїв інформації;

➢ перехват інформації по каналах побічних електромагнітних випромінювань, наведень та по відвідним колам.

• Вектор показників оцінювання загроз структурним підрозділам, обслуговуючому персоналу і працівникам $U_{сп}$:

➢ відсутність підготовленого персоналу;

➢ невміння працювати з програмними і технічними засобами;

➢ відсутність політики безпеки, плану захисту інформації, однозначних інструкції і правил, їх недостатня повнота та взаємна неузгодженість;

➢ неправильна організація роботи декількох користувачів на одному робочому місці;

➢ втрата засобів розмежування доступу;

- втрата матеріальних носіїв, що містять інформацію про систему захисту в АІС, користувачів, технічне, програмне, інформаційне забезпечення та т. ін.;
- використання підслуховуючих пристроїв тощо.

• Вектор показників оцінювання загроз обчислювальній та оргтехніці, носіям інформації і архівам $U_{от}$:

- несанкціоноване підключення до АІС технічних засобів (в т. ч. приватних) (модемів, жорстких магнітних дисків, сканерів та т. ін.);
- порушення режимів функціонування АІС;
- несанкціоноване копіювання вихідних документів;
- втрата інформації у разі переривання енергоживлення;
- відключення систем фіксації відправлених даних;

• Вектор показників оцінювання загроз зовнішнім каналам нформаційного зв'язку (комунікацій) $U_{зкз}$:

- несанкціонований доступ до баз даних та інформації, що циркулює та обробляється в АІС;
- копіювання або руйнування інформації в системі або в Центральному Сховищі Даних;
- зараження інформаційної системи програмними кодами, направленими на завдання шкоди (віруси, „троянські коні" тощо);
- дистанційне внесення програмних закладок в програмне забезпечення системи;
- хакерські атаки через локальну мережу, корпоративну мережу та мережу Інтернет;

• Вектор показників оцінювання загроз внутрішнім каналам зв'язку комунікацій) $U_{вкз}$:

- несанкціонований доступ до баз даних та інформації, що циркулює та обробляється на різних рівнях А1С;
- копіювання, руйнування або знищення інформації в підсистемах або в Центральному Сховищі Даних;

- хакерські атаки через локальну мережу, корпоративну мережу та мережу Інтернет;
- несанкціоноване підключення до алгоритмів обробки з метою інформаційного впливу на процес обробки інформації.

• Вектор показників оцінювання загроз приміщенням, офісам $U_{оф}$:

- несанкціоноване ознайомлення з конфіденційною інформацією сторонніми особами;
- несанкціоноване копіювання, руйнування або знищення інформації;
- застосування пристроїв для дистанційного підслуховування та спостереження.

• Вектор показників оцінювання загроз системам електроживлення, зв'язку, теле- та радіомовлення $U_{еж}$:

- руйнування баз даних, інформації;
- знищення файлів, що розроблялися в момент виключення системи живлення;
- руйнування жорстких дисків, системних блоків.

Для об'єктів підсистем и регіонального (другого) рівня IAC підрозділу об'єкти захисту та типові загрози для них залишаються такими ж. за винятком Центрального Сховища Даних. Змінюватися будуть скоріше за все масштаби загроз та їх кількість, що буде враховуватися експертами при проведенні конкретного оцінювання.

Природно, що в кожному конкретному випадку базова система показників може доповнюватися або скорочуватися експертами, що залучаються для оцінювання рівня загрози АІС підрозділу .

Враховуючи викладене, у формалізованому виді рівень інтегрованої загрози АІС на момент оцінювання t можна оцінити функціоналом

$$U(t) = F\{M_{kp}, V_{skp}, t\}. \quad \text{(3.4)}$$

Звісно, що встановити сувору математичну залежність функціоналу (3.4) не представляється можливим, тому доцільно йти шляхом часткових розрахунків U(t) у фіксовані моменти часу t на основі використання технології методу аналіза ієрархій (MAI), а потім по окремим точкам встановити функціональну залежність, яку можна використовувати у подальшому для прогнозування зміни рівня інтегрованої загрози з плином часу.

Вибираємо межі існування функціоналу

$$4 \le U(t) \le 1 \qquad (3.5)$$

де U(t) = 4 - означає повну відсутність загрози для АІС; U(t) = 1 - означає вивід з ладу АІС (ефективність АІС нейтралізована на 144%), що не суперечить фізичному змісту введеного функціоналу (3.5) і забезпечує адекватність математичного опису вивчаємого процесу.

Таким чином, процес відстеження рівня інтегрованої загрози АІС з боку вибраної моделі порушника, вплив якого характеризується вектором показників U, у формалізованому виді запропоновано описувати функціоналом (3.5), числове значення змін якого знаходиться у межах від нуля до одиниці.

Оскільки рівень інтегрованої загрози оцінюється за допомогою вектора обраних показників, то необхідно здійснення постійного моніторингу для добору фактів, що характеризують ці показники. Практика показує, що накопичення інформації по фактам доцільно робити стосовно до обраних об'єктів АІС, а усередині кожного об'єкту "сортування" інформації проводити відносно вибраних показників.

3.2. Методика та алгоритм оцінювання ефективності захисту інформаійної системи

ІС відноситься до систем, що забезпечують функціонування , працює в тісній взаємодії з іншими інформаційними системами держави, її ефективність залежить від обсягів, повноти, достовірності та своєчасності отримання

інформації, своєчасності та точності її обробки, що ускладнюється суттєвими труднощами її формалізації та відсутністю відповідного науково-методичного апарату, а також деструктивним впливом порушників на різного роду об'єкти АІС, що в реальні оцінки і прогнози вносить досить істотні похибки або взагалі руйнує чи спотворює інформацію, що циркулює в АІС.

Відомі прийоми дослідження подібних складних систем базуються здебільшого на методах опитування й експертного оцінювання і характеризуються великими похибками, а результати залежать від особистостей експертів.

У найбільшій мірі вільним від зазначених недоліків для оцінювання рівня інтегрованої загрози для АІС можна вважати метод аналізу ієрархій .

Ключовим моментом використання МАІ є побудова ієрархії із ρ рівнів. Отже, якщо представити процес впливу (приведення в дію загрози) порушника на р-му рівні проти $К_р$-го об'єкта у виді р-рівневої ієрархії (для задачі оцінювання рівня інтегрованої загрози АІС р=3), то для оцінювання рівня цієї активності можна застосувати процедуру МАІ з удосконаленнями.

Враховуючи сказане, методика визначення поточного рівня інтегрованої загрози АІС повинна включати наступні етапи (рис. 3.3).

Етап № 1: формулюється мета оцінювання та визначаються об'єкти, стосовно яких спостерігаються прояви впливу порушників.

Етап № 2: будується ієрархія об'єктів та показників оцінювання. На першому рівні находиться мета оцінювання, з метою зв'язуються вибрані об'єкти (другий рівень), у яких спостерігаються або, на думку експертів, будуть проявлятися ознаки впливу порушників на ефективність функціонування АІС. На третьому рівні розташовують вибрані показники оцінювання рівня загроз об'єктам системи і показують зв'язки вибраних показників з об'єктами. При побудові третього рівня ієрархії слід ввести обмеження на кількість показників, яких не повинно бути більше дев'яти .

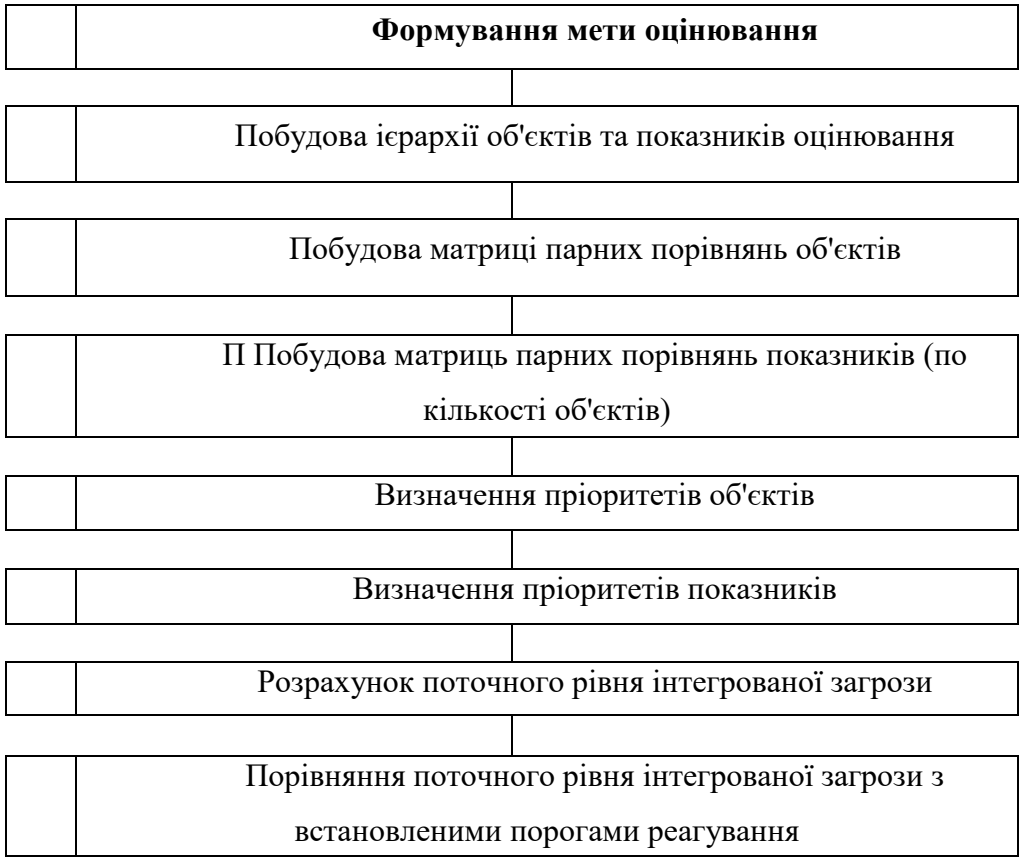

Рис. 3.3 Методика визначення поточного рівня інтегрованої загрози АІС

Етапи № 3 - № 4: після побудови та перевірки ієрархії розробляються бланки матриць парних порівнянь для кожного з I_p рівнів ієрархії. На рис. 3.4 показано бланк такої матриці для порівняння об'єктів.

У порівнянні з об’єктом №

	Об'єкт № 1	**Об'єкт № 2**	**…**	**Об'єкт № K_p**
Об'єкт № 1				
Об'єкт № 2		'		
…				
Об'єкт № K_p				

На скільки важливий об’єкт

Рис. 3.4 Матриця парних порівнянь об'єктів

Для порівняння показників загальний вид матриці зберігається, збільшується тільки її розмірність, кожний прилягаючий зверху елемент матриці залежить від кількості рівнів і типу зв'язків між показниками.

Наприклад, для другого рівня ієрархії матриця парних порівнянь має вигляд:

$$A_{nn} = \begin{matrix} a_{11} & a_{12} & \dots & a_{1Kp} \\ a_{21} & a_{22} & \dots & a_{2Kp} \\ . & . & . & \\ a_{Kp1} & a_{Kp2} & \dots & a_{KpKp} \end{matrix}, \quad (3.6)$$

де a_{11}... $a_{Кр\ Кр}$ - елементи матриці парних порівнянь; s - кількість рядків і стовпчиків матриці.

Пояснимо властивості матриці парних порівнянь і їх зв'язок з оцінюванням рівня інтегрованої загрози на простому прикладі (рис. 3.5).

Нехай F_1, F_2, F_3,..., $F_{Кр}$ - множина із $К_р$ об'єктів, стосовно яких спостерігаються ознаки впливу порушників, w_1, w_2, w_3, $w_{Кр}$ - відповідно їх важливість (якщо розглядати матрицю 2-го рівня ієрархії).

Якщо порівнювати важливості кожного елементу множини F_1, F_2, F_3,..., $F_{Кр}$ з важливістю будь-якого іншого елементу цієї множини по відношенню до спільної для них мети, то тоді матрицю парних порівнянь можна записати у вигляді:

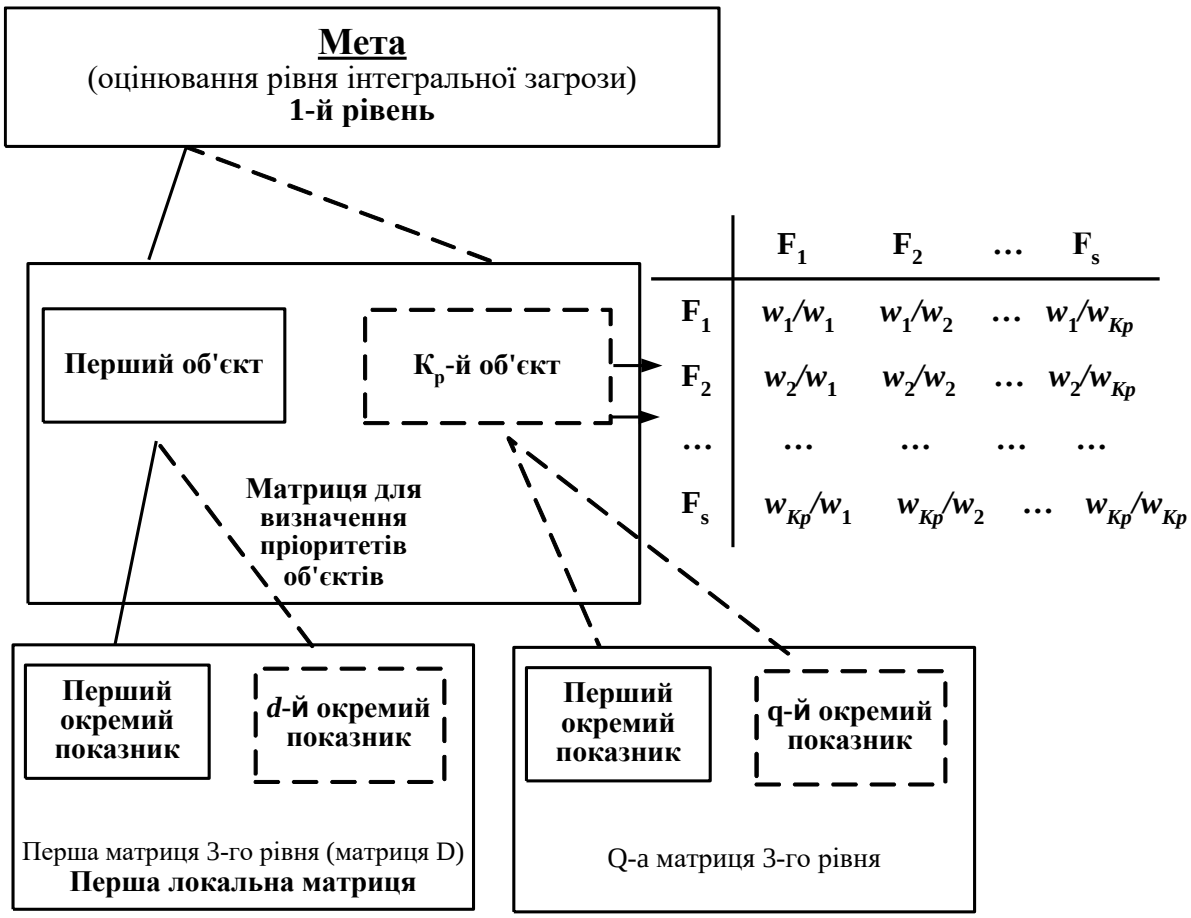

Рис. 3.5 Приклад побудови трирівневої ієрархії для оцінювання рівня інтегрованої загрози

$$W = \begin{matrix} w_1/w_1 & w_1/w_2 & \dots & w_1/w_{Kp} \\ w_2/w_1 & w_2/w_2 & \dots & w_2/w_{Kp} \\ . & . & . & \\ w_{Kp}/w_1 & w_{Kp}/w_2 & \dots & w_{Kp}/w_{Kp} \end{matrix}, \qquad (3.7)$$

Якщо вхідна інформація носить кількісний характер, то проблем у побудові матриць типу (3.7) немає. Але, як було сказано вище, для оцінювання рівня інтегрованої загрози АІС з боку порушників, інформація про дії яких носить переважно якісний характер, необхідно з нею здійснити ряд процедур, спрямованих на її приведення до кількісного виду.

Кількісні значення матриць парних порівнянь можна також отримати з допомогою методів експертного оцінювання . Попарні порівняння елементів матриці проводяться з використанням суб'єктивних міркувань експертів, що чисельно оцінюються за шкалою відносної важливості, табл. 4.1.

При цьому заповнення матриці парних порівнянь 2-го рівня потребує $К_р(К_р-1)/2$ міркувань. Заповнення матриць 3-го рівня потребує відповідно d(d-1)/2 +... + q (q-1)/2 міркувань, де d, q відповідно розмірності часткових матриць 3-го рівня.

Таблиця 3.1

Шкала відносної важливості

ІНТЕНСИВНОСТІ ВАЖЛИВОСТІ	**ВИЗНАЧЕННЯ**	**ПОЯСНЕННЯ**
1	Рівна важливість	Рівний внесок двох елементів
3	Незначна перевага одного елемента над іншим	Досвід і міркування дають легку перевагу одного елемента над іншим
5	Істотна, або сильна перевага	Досвід і міркування дають сильну перевагу одного елемента над іншим
7	Значна перевага	Одному елементу надається настільки сильна перевага, що він стає практично значимим
9	Дуже сильна перевага	Очевидність переваги одного елемента над іншим підтверджується найбільш сильно
2, 4, 6, 8	Проміжні рішення	Застосовуються у компромісному випадку
1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9	Отримуються при зворотному порівнянні	Застосовуються у випадках зворотного переважання

Етапи № 5 - № 6: визначаються пріоритети відповідно об'єктів і показників. Для визначення пріоритетів об'єктів і показників (деякі дослідники показники називають загрозами) використовуються матриці парних порівнянь відповідно об'єктів і показників, які були побудовані на попередніх етапах. При цьому основна увага концентрується на об'єктах і показниках, що мають саму велику важливість (вагу).

Із групи побудованих матриць парних порівнянь формують набір локальних пріоритетів, які виражають відносний вплив множини елементів прилеглого зверху рівня ієрархії. Для квадратної зворотньосиметричної матриці такими локальними

пріоритетами буде власний вектор матриці , нормалізований до одиниці. При проведенні оцінювання рівня інтегрованої загрози з боку порушників, що розглядаються, глобальними пріоритетами будуть пріоритети вибраних (глобальних) об'єктів. Обчислення глобальних пріоритетів L_{Kp}, k_p =1, K_p (для об'єктів р-го рівня) стосовно матриці 2-го рівня ієрархії здійснюється за відомими формулами теорії матричного обчислювання

$$
\begin{aligned}
&r_1 = w_1/w_1 \cdot w_1/w_2 \cdot \ldots \cdot w_1/w_{Kp}; \quad L_1 = r_1 \Big/ \sum_{j=1}^{Kp} r_j \\
&r_2 = w_2/w_1 \cdot w_2/w_2 \cdot \ldots \cdot w_2/w_{Kp}; \quad L_2 = r_2 \Big/ \sum_{j=1}^{Kp} r_j \\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
&r_2 = w_{Kp}/w_1 \cdot w_{Kp}/w_2 \cdot \ldots \cdot w_{Kp}/w_{Kp}; \quad L_{Kp} = r_{Kp} \Big/ \sum_{j=1}^{Kp} r_j
\end{aligned}
\qquad (3.8)
$$

де S - кількість пріоритетів (кількість рядків і стовпчиків матриці об'єктів (згідно з рис. 4.6): r_1, r_2,..... r_s - значення розрахунків пріоритетів матриці 2-го рівня ієрархії; L_1 L_2..... L_{Kp}- нормовані до одиниці значення пріоритетів.

Важливим моментом у проведенні обчислень з використанням МАІ є визначення узгодженості міркувань експертів перед отриманням пріоритетів в матриці парних порівнянь. Індекс узгодженості матриці парних порівнянь (матриці об'єктів) має вигляд

$$I = (\lambda_{max} F - S)/(S-1). \qquad (3.9)$$

де λ_{max}F - найбільше власне значення матриці парних порівнянь (матриці 2-го рівня ієрархії); S - число порівнюваних елементів.

Далі порівнюється індекс узгодженості 1 з середніми узгодженостями для випадкових матриць різного порядку. Середні узгодженості для випадкових матриць різного порядку наведені в табл. 3.2.

Таблиця 3.2

Середні узгодженості для випадкових матриць різного порядку

Розмір матриці S	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Середня узгодженість S_n	4	4	4,58	4,9	1,12	1,24	1,32	1,41	1,45

У підсумку обчислюється відношення узгодженості V

$$V = (I/S_n) * 100\%, \tag{3.10}$$

де S_n - випадкова узгодженість n-го порядку.

Якщо величина V<14 %, можна продовжувати порівняння в матрицях третього рівня і проводити обчислення, якщо ж V>14 %, то експертам слід перевірити свої міркування в матриці другого рівня, або переглянути ієрархію з метою перевірки її відповідності обраній меті дослідження (не всі показники можуть бути враховані) . Цим пояснюється і те, що кількість порівнюваних елементів не може бути більше 9, так як у цьому випадку матиме місце неприйнятна величина S_n. Всі проведені обчислення (визначення пріоритетів та визначення узгодженості міркувань) стосуються також матриць наступних рівнів ієрархії і проводяться аналогічним чином.

Найбільш просто матриця парних порівнянь складається для 2-го рівня ієрархії, тобто для об'єктів впливу порушників.

Для упорядкування матриць парних порівнянь 3-го рівня ієрархії слід враховувати ряд особливостей.

По-перше, для наочності отримання результатів попарних порівнянь показників доцільно для кожного об'єкта побудувати окрему ієрархію показників (загроз).

По-друге, парні порівняння необхідно проводити з врахуванням відносного впливу порівнюваних показників (загроз) на зростання рівня інтегрованої загрози тільки щодо розглядаємого показника. Кількість матриць парних порівнянь на 3-му рівні дорівнює кількості розглянутих об'єктів.

Процес парних порівнянь за технологією MAI проводиться в наступній послідовності .

Починають із лівого елемента матриці і ставлять запитання: наскільки об'єкт № 1 важливіший об'єкта № 2, потім об'єкта № 3 і так далі до об'єкта $К_р$. Потім зліва беруть об'єкт № 3 і проводять аналогічне порівняння з об'єктом № 4 і так далі до об'єкта $К_р$**.**

Аналогічно проводять парні порівняння для 3-го рівня ієрархії.

Для автоматизації процесу парних порівнянь можна використовувати комп'ютерну технологію, яка дозволяє ці етапи алгоритму представити наступними кроками.

- На екран комп'ютера виводиться незаповнена матриця парних порівнянь об'єктів і лінійна шкала для оцінювання важливостей об'єктів (рис. 3.6).

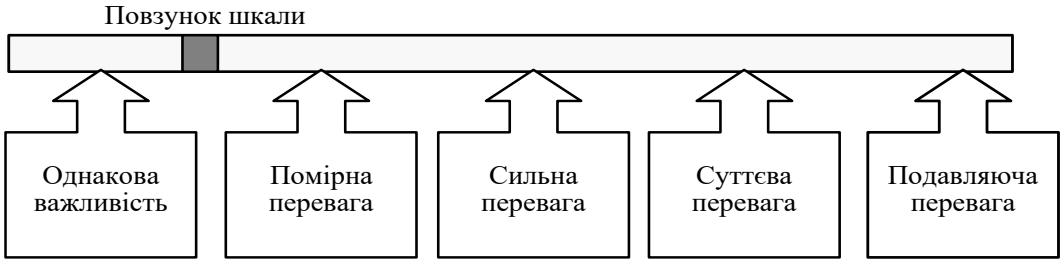

Рис. 3.6 Шкала для оцінювання важливостей об'єктів

- Експерти визначають об'єкт, що найменше впливає на рівень інтегрованої загрози, і ставлять її відмітку в початок шкали (рис. 3.6).
- Потім експерти визначають об'єкт, що найбільш впливає на рівень інтегрованої загрози, і виставляють її відмітку в масштабі на шкалі з урахуванням важливості вже обраного об'єкта.
- Надалі експерти по ступеню впливу інших об'єктів щодо об'єкту, поставленого в початок шкали, розставляють відмітки важливостей решти об'єктів.
- Після відліку числових значень важливостей об'єктів експертами заповнюється матриця парних порівнянь і по відомому алгоритму розраховуються пріоритети об'єктів L_1... L_{Kp}, де K_p-кількість оцінюваних об'єктів (ці операції виконуються комп'ютером автоматично).

Процедура визначення пріоритетів показників P_1,..., P_i,... $P_к$, де к -сума розмірностей часткових матриць парних порівнянь показників, що були побудовані для 3-го рівня ієрархії, аналогічна розглянутій для об'єктів.

Звісно, що така процедура оцінювання висуває підвищені вимоги до компетентності експертів, проте дозволяє в найбільшій мірі автоматизувати

процеси парних порівнянь і обчислень відповідних пріоритетів. Це забезпечує прийнятну узгодженість думок експертів.

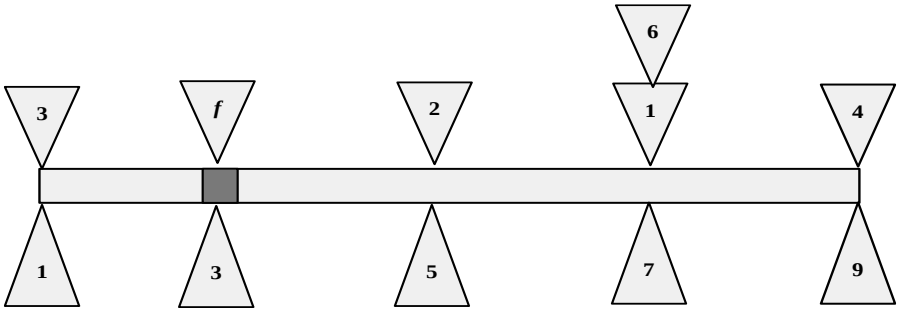

Рис. 3.7 Приклад вводу важливостей факторів за допомогою лінійної шкали

f = 3 - мінімально впливає на ступінь відхилення;

f = 4 - максимально впливає на ступінь відхилення.

Етап №7: розраховується підсумкове нормоване значення рівня інтегрованої загрози на момент оцінювання t_4 за процедурою:

$$U(t_0) = \sum_i^k (L_i P_i) \Big/ \sum_i^k max(L_i P_i). \quad (3.11)$$

Етап № 8: отриманий підсумковий рівень активності $U(t_4)$ порівнюється з встановленими порогами реагування.

У залежності від того, який фіксований рівень інтегрованої загрози перевищує отриманий рівень $U(t_4)$, пропонується відповідний комплекс заходів для реагування.

3.3. Метод багатокритеріального аналізу ефективності функціонування та забезпечення інформаційної безпеки інформаційних систем

Проблема багатьох інформаційних систем (ІС) зв’язку зводиться до того, що кількість параметрів, необхідних для опису поводження системи (розмірність системи), виявляється дуже великою і прийняти правильне рішення в таких мережах досить складно, враховуючи, що інформація про стан мережі може бути досить суперечливою. Збільшення розмірності сучасної технології представляється об’єктивною тенденцією, яку можна спостерігати в історичному зрізі протягом усього розвитку цифрових ІКС.

Поява концепції інформаційних мереж нового покоління (NGN та FN – мереж майбутнього) дозволить операторам значно розширити горизонти своєї діяльності, спектр послуг. Проте шлях переходу до мереж, на базі яких можливе надання мультисервісних послуг, складний і тернистий. Тому ставиться питання, чи не простіше продовжувати експлуатувати існуючі мережі, поки є попит на перелік послуг, що вже склався і піклуватися про їх якість.

Безумовно в стрімкому розвитку мереж нового покоління можна назвати і "болючі точки" експлуатації інформаційних мереж нового покоління з погляду оператора**.** Ключові моменти в експлуатації мережі – її надійність і досконалість системи управління. До "болючих точок" експлуатації мереж нового покоління можна віднести не стільки проблеми з технологіями, які застосовуються, скільки завдання забезпечення стійкої роботи мережевого устаткування, стиковка протоколів, інтерфейсів різних постачальників та забезпечення інформаційної безпеки.

Гарантування безпеки інформації в мережах нового покоління взагалі та їх системах управління є складним комплексним завданням. У міжнародних стандартах проблеми захисту інформації вирішуються одночасно зі стратегічними та конкретними питаннями розвитку архітектури мережі.

Такий підхід відповідає комплексному характеру забезпечення безпеки систем телекомунікацій на всіх етапах їх життєвого циклу – від концептуальних схем та проектування до технічної експлуатації та використання. Окремими заходами досягти мети, як правило, не вдається й тому в кожному випадку потрібно розглядати всю систему в комплексі, причому захищеність усієї інфокомунікаційної системи (мережі) визначається рівнем захищеності її найбільш слабкої частини.

Бурхливий розвиток інформаційних систем у напрямку збільшення їх розміру та ускладнення, розширення спектру послуг, які надаються абонентам, росту кількості компаній, які займаються проектуванням, експлуатацією пов'язаних між собою мереж, що належать різним власникам, необхідність підвищення надійності роботи мережі, якості обслуговування, економічної ефективності та інших вимог, провідні фірми та корпорації світу прийшли до

однозначного висновку – необхідності створення гнучкої та надійної системи управління й ними, що і дасть можливість повисити якість ефективності функціонування системи в цілому.

Інфокомунікаційна система (ІКС) – це безліч взаємозалежних матеріальних об’єктів (засобів і комплексів зв’язку, а також персоналу, що їх обслуговують), що безпосередньо беруть участь у проведенні операції (функціонуванні системи зв’язку) і об’єднаних загальною метою (надання послуг зв’язку). Дана система відносяться до класу цілеспрямованих складних систем, у яких як взаємозалежні елементи виступають матеріальні об’єкти (технічні засоби зв’язку й управління, а також обслуговуючий їх персонал). Система є модульною та дозволяє пристосування до мереж різноманітної структури та призначення. Для того щоб оцінити ефективність функціонування такої системи і пропонується даний ймовірнісний метод багатокритеріального аналізу.

Внаслідок критичних ситуацій, які виникають в мережах, та неспроможності відвернути їх, почались пошуки нових принципів, методів та засобів управління ефективністю системи. Одним з варіантів вирішення цієї проблеми є застосування штучного інтелекту.

Аналіз шляхів підвищення ефективності функціонування інформаційних систем провідних фірм та корпорацій світу, шляхів створення та тенденції розвитку управління ними, дозволяє зробити висновки:

- у всіх розвинутих країнах світу розроблені, або розробляються та впроваджуються автоматизовані системи управління мережами зв’язку, які забезпечують ефективність та надійність роботи устаткування, що постійно ускладнюється;
- система управління ІКС вирішує питання збору та обробки інформації про стан мережі та обладнання, виявлення та локалізації несправності апаратури та ділянок мережі, керує навантаженням мережі, при необхідності змінює конфігурацію мережі, сприяє плануванню розвитку мережі, контролює правильність проведення розрахунків за послуги, тощо;

- у зв’язку з тенденцією інтеграції різних видів інформації та послуг зв’язку у єдину мережу і з появою цифрових мереж інтегрального обслуговування (ЦМІО), виникла необхідність у створенні єдиної системи управління. Управління такими мережами, що несуть змішану інформацію (мова, дані, зображення, інформацію для телеуправління і контролю), оснащеними різними видами апаратури систем передачі та різними терміналами, можливе тільки із застосуванням нових способів та систем управління мережами;
- розробка та створення таких систем здійснюється за стандартами та Рекомендаціями МСЕ (Міжнародна спілка електрозв’язку), які містять вимоги до надійності мереж, до реакції на відновлення, до управління структурою мережі, до тарифікації, до управління якістю обслуговування та забезпеченням безвідмовності, безпеки та захисту інформації в мережах.

Поряд із системою інформаційного обміну, що включає станції, вузли та лінії зв’язку, функціонує взаємозалежна з нею автоматизована система управління (АСУ), що включає центри та станції контролю й управління, а також канали управління між ними. АСУ створюється з метою управління елементами системи інформаційного обміну (СІО).

Зміна стану складної інформаційної системи під впливом навколишнього середовища обумовлюється цілеспрямованими процесами функціонування елементів і всієї системи в цілому. По цілому ряді ознак, таких як наявність великої кількості взаємозалежних елементів, можливість розбивки на підсистеми, складність процесу функціонування, активна взаємодія із зовнішнім середовищем, наявність системи управління й т. ін., ІКС можна віднести до складних систем.

Завдання оцінки ефективності інфокомунікаційної системи можна розглядати як одне із приватних завдань сучасної теорії дослідження операцій. У загальному виді завдання оцінки ефективності такої системи можна сформулювати так: при заданих вихідних умовах необхідно визначити систему, що у порівнянні з еталонною є кращою в змісті обраного або заданого критерію.

Від вибору критерію й системи показників якості (СПЯ) багато в чому залежить результат оцінки і його практична цінність. Загальноприйнятим

підходом до розробки системи показників якості складних систем є формулювання безлічі локальних СПЯ, що відповідає сукупності властивостей ІКС, які впливають на виконання поставлених перед нею завдань. Глобальна СПЯ, що характеризує загальну, єдину задачу, яка стоїть перед інфокомунікаційною системою, реалізується шляхом з'єднання вихідних локальних систем показників якості.

Пропонується метод формування системи показників якості, відмінний від традиційного, тобто пропонується, ґрунтуючись на математичних методах теорії декомпозиції (факторизації, функціональної й параметричної декомпозиції), замість визначення локальних СПЯ (ЛСПЯ) низького рівня ієрархії й наступного їхнього об'єднання в глобальну СПЯ (ГСПК) розглядати завдання функціонування ІКС у цілому. При такому підході до оцінки ефективності інфокомунікаційної системи зростає розмірність завдання, яке розв'язується, оскільки формулюється не одна ГСПЯ, а сукупність ієрархічно зв'язаних ЛСПЯ, але зате забезпечується конструктивність рішення завдання й ураховуються реальні поточні ймовірнісні характеристики приватних показників ефективності (ППЕ). Повнота такої СПЯ ґрунтується на тім, що вихідними даними для її формулювання є вимоги, які запропоновані користувачем до ІКС, математично коректно декомпозовані в інтересах їхнього подальшого використання.

Локальні системи показників якості більш низького рівня ієрархії деталізують внутрішні властивості системи, а глобальна СПЯ описує зовнішні властивості системи. Розмірність локальної СПЯ значно знижується за допомогою методу редукції, заснованого на оцінці ступеня лінійної незалежності показників якості їхньої чутливості до змінного стану ІКС.

Основними зовнішніми властивостями інфокомунікаційної системи є види й рівень інформаційних послуг, які надаються споживачам. Поряд із процесом інформаційного обміну в системі існує процес управління якістю обміну інформацією, структурою, алгоритмами роботи й параметрами даної мережі, що, як і процес зв'язку, характеризується набором властивостей (якостей). Елементи інфокомунікаційної системи – система інформаційного обміну (СІО) і система

управління (СУ) – володіють характерним для них набором основних внутрішніх властивостей (якостей). Взаємозв’язок властивостей системи і відповідних їм показників якості функціонування представлена на рис. 3.8.

До складу глобальної системи показників якості

$$\vec{Y}_{\text{ф}}(k)=\left[t_{\text{дп}}(k);t_{\text{дф}}(k);\vec{B}_{\text{ф}}(k)\right]^{T} \tag{3.12}$$

входять час доставки повідомлення на k-му кроці функціонування мережі, час доступності до процесу функціонування на k-му кроці й вектор витрат ресурсів на процес функціонування ІКС на k-му кроці.

Серед локальних СПЯ основною виступає система показників якості процесу інформаційного обміну (зв’язку), що містить у собі час доставки повідомлення на k-му кроці функціонування мережі, час доступності до повідомлення на k-му кроці, а також вектор витрат ресурсів на доставку повідомлення на k-му кроці:

$$\vec{Y}_{\text{зв}}(k)=\left[t_{\text{дп}}(k);t_{\text{чДП}}(k);\vec{B}_{\text{д}}(k)\right]^{T} \tag{3.13}$$

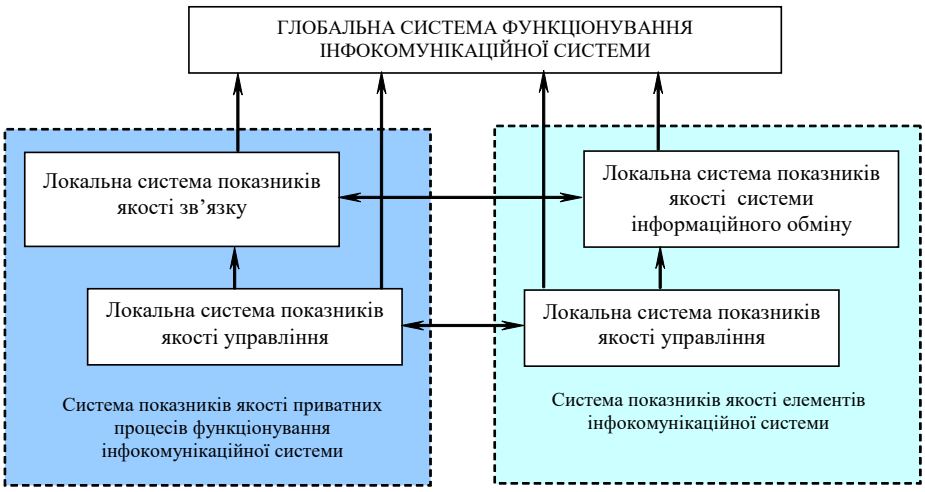

Рис. 3.8 Взаємозв’язок систем показників якості в інформаційній системі

Показники якості зв'язку для складних маршрутів проходження повідомлень по системі інформаційного обміну інфокомунікаційної системи, обумовлені в інтересах поточного оцінювання ефективності функціонування, які знаходяться за виразом

$$\vec{Y}_{\text{зв}}(k) = \Pi\left(t_1(k); t_2(k)\right) t_r\left[M_m(k); M_{Y_{\text{зв}}}(k)\right]^T, \quad (3.14)$$

де $\Pi\left(t_1(k); t_2(k)\right)$ – показник часового інтервалу, що приймає значення 1 в інтервалі передачі повідомлення $\left(t_1(k); t_2(k)\right)$ й 0 за його межами;

$M_m(k) = \left\{\varepsilon_{jj'}^m\right\};\ j, j' = \overline{1, J_S};$ m = 1, M – матриця маршруту проходження повідомлення на k-му кроці функціонування мережі з одиничними елементами $\varepsilon_{jj'} = 1$ на шляху його передачі й нульовими $\varepsilon_{jj'} = 0$ в противному випадку;

$M_{Y_{\text{зв}}}(k)$ – матриця значень і-х показників якості, обумовлена для jj'-х напрямків зв'язку на k-му кроці функціонування мережі.

Локальна система показників якості управління має більше низький рівень ієрархії в порівнянні із ЛСПЯ зв'язку, оскільки функції управління зв'язком забезпечують процес інформаційного обміну. Вона включає:

$$\vec{Y}_{\text{у}}(k) = \left[T_{\text{цу}}(k); \vec{Y}_{\text{зв}}^{y}(k); t_{\text{ду}}(k); \vec{B}_{\text{у}}(k)\right]^T, \quad (3.15)$$

тривалість циклу управління параметрами напрямку інфокомунікаційної системи при порушенні нормальних умов функціонування на k-му кроці функціонування системи; вектор збільшень значень показників якості зв'язку на k-му кроці функціонування мережі, обумовлених помилками в контурі управління; час доступності до сигналів управління на k-му кроці й вектор витрат ресурсів управління на k-му кроці функціонування.

Два основних елементи інфокомунікаційної системи – система інформаційного обміну та система управління – є технічною базою (матеріальною основою) процесів інформаційного обміну й управління. Проблема управління інфокомунікаційними мережами є однією з найважливіших у практиці експлуатації мереж.

Показані принципи побудови системи управління сучасними мережами. Визначено основні показники якості системи управління, які обумовлюють характеристику інфокомунікаційної мережі в цілому та на базі яких доцільно реалізувати метод багатокритеріальної оптимізації ІКС.

Під показником ефективності процесу функціонування будь-якої складної системи розуміється міра відповідності реального результату процесу функціонування системи необхідному. Виходячи з вимог, які ставляться до показників ефективності, з огляду на специфіку процесу функціонування інфокомунікаційної системи, у якості показників ефективності використається ймовірність відповідності системи зв'язку своєму функціональному призначенню $P_{вик.ф.}$ (імовірність досягнення мети $P_{дм}$) як найбільш інформаційний і комплексний показник:

$$P_{\text{вик.ф}} = P\left\{y_i \le y_i^{\text{доп}}\right\} \qquad (3.16)$$

Багатокритеріальний характер вимог до якості зв'язку й управління, облік процесів, що протікають у інфокомунікаційній системі, приводять до постановки векторного завдання аналізу ефективності функціонування системи в цілому.

Аналіз різних методів формування узагальненого показника ефективності інформаційних систем показав, що найбільш повний облік особливостей рішення завдання оцінки ефективності функціонування інфокомунікаційної системи, а також природне рішення проблем нормалізації й згортки систем показників якості досягається при застосуванні методу ймовірнісної скаляризації.

Суть методу полягає у використанні в якості узагальненого показника ефективності спільної ймовірності виконання вимог, пропонованих користувачем до системи по своєчасній, достовірній, безпечній і економічній передачі повідомлень.

Проектування інформаційних мереж, організація й застосування СЗІ (систем захисту інформації) фактично пов'язане з невідомими подіями в майбутньому й тому завжди містять елементи невизначеності. Крім того, присутні й інші причини неоднозначності, такі як недостатньо повна інформація для ухвалення рішень управління або соціально-психологічні чинники. Тому, наприклад, етап проектування мережі та СЗІ природним чином супроводить значна невизначеність. У міру реалізації проекту її рівень знижується, але ніколи ефективність СЗІ не може бути адекватно виражена й описана детермінованими

показниками. Процедури випробувань, сертифікації або ліцензування не усувають повністю невизначеність властивостей СЗІ або її окремих елементів і не враховують випадковий характер атак.

Тому об’єктивною характеристикою якості СЗІ будь-якої мережі, ступенем її пристосованості до досягнення рівня безпеки, який вимагається, в умовах реальної дії випадкових чинників, може служити ймовірність, яка характеризує ступінь можливостей конкретної СЗІ при заданому комплексі умов. Іншими словами – вірогідність досягнення мети операції або вірогідність виконання задачі системою. Ця вірогідність повинна бути встановлена в основу комплексу показників і критеріїв оцінки ефективності СЗІ. При цьому критеріями оцінки служать поняття придатності та оптимальності. Придатність означає виконання всіх встановлених до СЗІ вимог, а оптимальність – досягнення однієї із характеристик екстремального значення при дотриманні обмежень і умов на інші властивості системи. При виборі конкретного критерію необхідно його узгодження з метою, що покладається на СЗІ.

Під час синтезу системи виникає проблема рішення задачі з багатокритеріальним показником. При цьому розглядаються показники ефективності, які призначені при рішенні задачі порівняння різних структур СЗІ.

Оцінка оптимального рівня гарантій безпеки в певній мірі залежить від збитку, пов’язаного з помилкою у виборі конкретного значення показника ефективності. Для отримання чисельних оцінок ризику необхідно знати розподіли ряду випадкових величин. Це певною мірою обмежує кількісне дослідження рівнів гарантій безпеки, які надаються СЗІ, але в багатьох практичних випадках такі оцінки можна отримати за допомогою імітаційного моделювання або за наслідками активного аудиту СЗІ. Багаторівневій структурі системи показників ефективності СЗІ відповідає багаторівнева структура форм представлення відповідних показників, які змінюються від кількісної шкали для оцінки показників нижнього рівня до якісної - на верхніх.

Існує адекватна система показників ефективності СЗІ – система математичних моделей для їх оцінки. Відповідно до даної вимоги кожному рівню

пірамідальної мережі показників ефективності СЗІ ставиться у відповідність певний тип математичних моделей, які забезпечують оцінку показників цього рівня. Існує уніфікований формальний опис процесів функціонування СЗІ, виходячи з якого, можна отримати будь-який тип математичної моделі, яка відповідає переліку властивостей. Властивості СЗІ виявляються при рішенні відповідних задач захисту інформації. Таким чином, можна зробити висновок про необхідність оцінки ефективності систем безпеки не тільки по якісних характеристиках, але й по кількісних показниках.

Таким чином, поняття ефективність нерозривно пов’язане з результатами процесу функціонування інфокомунікаційної системи, опирається на систему показників якості процесу функціонування й вимоги до них. Узагальнений показник ефективності системи із урахуванням наявності взаємообумовлених випадкових факторів, що визначають її роботу, доцільно визначати на основі апарата умовних імовірностей у вигляді спільної ймовірності виконання всіх завдань, які розв’язуються у ході функціонування інфокомунікаційної системи та забезпечення її безпеки.

Розглянутий імовірнісний метод аналізу ефективності функціонування ІКС дозволяє на основі результатів аналізу проводити оптимізацію рішень на етапах планування й оперативного управління зв’язком у системі із урахуванням всіх видів випадкових впливів на неї з боку протиборчих систем.

Вибір методу оцінки ефективності функціонування систем спеціального призначення і ліній зв’язку в кожному конкретному випадку визначається особливостями процесу ведення зв’язку в інфокомунікаційній системі, зовнішніми умовами, наявним обчислювальним ресурсом і необхідним часом. Застосування методів оцінки ефективності функціонування системи дозволяє оцінити внесок окремих підсистем у виконання завдань, поставлених перед системою в цілому, оптимізувати підхід до рішення завдань обґрунтування технічних вимог, розробки структури системи управління інфокомунікаційної системи, розподілу ресурсів між її підсистемами та забезпечення інформаційної безпеки.

ВИСНОВКИ

В дипломній роботі було розглянуто потенційні загрози і канали витоку інформації. Аналізувати небезпеку найкраще ще на стадії проектування інформаційної системи, щоб відразу визначити потенційні втрати й установити вимоги до мір забезпечення безпеки.

Досліджено модель створення і комплексної оцінки системи захисту інформації. Основним завданням моделі є наукове забезпечення процесу створення системи інформаційної безпеки за рахунок правильної оцінки ефективності схвалюваних рішень і вибору раціонального варіанту технічної реалізації системи захисту інформації. Під ефективністю систем захисту інформації треба розуміти ефективність її використання в якості активного засобу в розробці забезпечення конфіденційності обробки, зберігання і передачі інформації.

Розглянуто методи ефективності захисту інформаційної системи. Вибір методу оцінки ефективності функціонування систем визначається особливостями процесу ведення зв’язку в інфокомунікаційній системі, зовнішніми умовами, наявним обчислювальним ресурсом і необхідним часом. Застосування методів оцінки ефективності функціонування системи дозволяє оцінити внесок окремих підсистем у виконання завдань, поставлених перед системою в цілому на забезпечення інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. – М.: Издательский центр «Академия». – 2446. – 256 с.
2. Домарев В.В. Безопасность информационных технологий. Системный подход. – Изд-во: ТИД «ДС». – 2444. – 992с.
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком. - 2444. - 284с.
4. Хорошко В.А. Модель системы защиты иформации. ”Захист інформації”,№1, 1999.
5. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. – К.: Юниор, 2443. - 541 с.
6. Борисов А.Н., Алексеев А.В., Меркурьев Г.В. и др. Обработка нечетной информации в системах принятия решений. - М: Радио и связь, 1989.-344с.
7. Герасименко В.А. Комплексная защита информации в современных системах обработки данных. ”Зарубежная радиоэлектроника”, №2, 1993.
8. Закон України “Про захист інформації в інформаційних системах”
9. Алексеев А.В. Интерпретация и определение функций принадлежности нечетких множеств / А.В. Алексеев // Методы и системы принятия решений. - Рига: Риж. политехн. ин-т, 1979. - С. 42 - 50.
10. Бочарников В.П. Fuzzy - технология: Математические основы. Практика моделирования в экономике / В.П. Бочарников. - СПб.: “Наука” РАН, 2001. - 328с.
11. Заде Л. Понятие лингвистической переменной и ее применение к принятию приближенных решений / Л. Заде. - М.: Мир, 1976. - 165 с.
12. Модели принятия решений на основе лингвистической переменной / [А.Н. Борисов, А.В. Алексеев, О.А. Крумберг и др.] – Рига: Зинатне, 1982. – 256 с.
13. Толюпа С.В. Метод багатокритеріального аналізу ефективності функціонування та забезпечення інформаційної безпеки / С.В. Толюпа // Науково-технічний журнал „Захист інформації”. - 2012. - №3 (54). с. 80-86.

14. Бусленко Н. П. Моделирование сложных систем / Н.П. Бусленко. - М. : Главная ред. физ-мат лит-ры изд-ва “Наука”, 1968. - 356 с.

15. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22 “Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу”, НД ТЗІ 2.5-004-99 – 58 с.

16. Власов О.М. Комплексний підхід оцінки ефективності систем захисту інформації в інформаційних мережах нового покоління / О.М. Власов, С.В. Толюпа // Наукові записки Наукові записки УНДІЗ. Науково-вироб. зб. – 2011 - №3(19). – С. 38-45.

17. Толюпа С.В. Структура інформаційної мережі та показники її ефективності. / С.В. Толюпа, А.В. Сухін. // Зб. наук. праць КВІУЗ – 2001. – № 3.– С. 68 – 73.

18. Макаров И.М. Интеллектуальные системы автоматического управления. – М.: Физматпит, 2005. – 573 с.

19. Ливенцев С.П. Оценка эффективности комплексных систем защиты информации в информационно-телекоммуникационных системах / С.П. Ливенцев // Зв’язок. – 2003. – № 1. – С. 28 – 31.

20. Толюпа С.В. Векторний синтез систем управління телекомунікаційними мережами / С.В. Толюпа // Зб. наук. праць ВІТІ НТУ “КПІ”. - 2002. - № 2. – С. 74 – 79.

Кувшинов О.В., Лівенцев С.П. Вибір параметрів багатопозиційних сигналів для підвищення ефективності системи передачі інформації / О.В. Кувшинов, С.П. Лівенцев // Зб. наук. праць ВІТІ НТУУ “КПІ”. – 2004. – Вип. 5. – С. 87 – 93.

ДЕМОНСТРАТИВНІ МАТЕРІАЛИ