

Міністерство освіти і науки України
Національний університет «Запорізька політехніка»

Методичні вказівки
для вивчення дисципліни

МЕТОДИ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

для студентів спеціальності
172 «Електронні комунікації та радіотехніка»,
які навчаються за освітньою програмою «Радіотехніка»
заочної форми навчання

Методичні вказівки для вивчення дисципліни “Методи і засоби захисту інформації” для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» заочної форми навчання /Укл.: І.М. Сметанін. – Запоріжжя: НУ «Запорізька політехніка», 2024. – 62 с.

Укладач: Сметанін І.М., старший викладач

Рецензент: Костенко В.О., доцент, канд .техн. наук.

Відповідальний за випуск: Сметанін І.М., старший викладач

Затверджено
на засіданні кафедри радіотехніки та
телекомунікацій.
Протокол № 4 від 15 лютого 2024 р.

Затверджено
на засіданні НМК факультету
ФІБЕК
Протокол №5 від 15 лютого 2024 р.

ЗМІСТ

ЗМІСТ	3
ВСТУП.....	5
1 ЗАГАЛЬНІ МЕТОДИЧНІ ВКАЗІВКИ.....	5
1.1 ОСНОВНІ ВИДИ ЗАНЯТЬ	6
1.1.1 Самостійна підготовка	6
1.1.2 Лекції.	7
1.1.3 Лабораторні роботи.....	7
1.1.4 Консультації.....	8
1.2 ОЦІНКА ЗНАНЬ	8
2 РОБОЧА ПРОГРАМА ВИВЧЕННЯ ТЕМ ДИСЦИПЛІНИ	8
Змістовий модуль 1. Основи інформаційної безпеки і захисту	
інформації.....	8
Тема 1 Вступ. Основні концептуальні положення системи захисту	
інформації	8
Тема 2 Об'єкти захисту, відомості, що охороняються, і демаскуючі	
ознаки.....	9
Тема 3 Класифікація і основні характеристики технічних каналів	
просочування інформації.	9
Тема 4 Акустичні і віброакустичні канали просочування мовної	
інформації з об'ємів виділених приміщень.	10
Тема 5 Знімання інформації з використанням закладних пристроїв.	
Загальні характеристики і побудова закладних пристроїв.	10
Змістовий модуль 2. Методи і способи захисту інформації.	11
Тема 6 Виявлення каналів просочування інформації.	11
Тема 7 Захист мовної інформації.....	11
Тема 8 Основи сучасної криптографії і питання шифрування.	
Криптографія і криптосистеми.....	11
Тема 9 Огляд сучасних криптосистем. Засоби автентифікації даних і	
управління ключами шифрування.	12
3 ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ.....	12
4. КОНТРОЛЬНІ ЗАВДАННЯ.....	13

КОНТРОЛЬНА РОБОТА № 1	16
КОНТРОЛЬНА РОБОТА № 2	36
КОНТРОЛЬНА РОБОТА № 3	55
5 РЕКОМЕНДОВАНА ЛІТЕРАТУРА	57
5.1 ОСНОВНА	57
5.2 ПЕРЕЛІК ПОСІБНИКІВ І МЕТОДИЧНИХ ВКАЗІВОК	58
5.3 РЕКОМЕНДОВАНІ ІНФОРМАЦІЙНІ ДЖЕРЕЛА:	58
ДОДАТКИ	59
Додаток 1 – ПРИКЛАД ВИКОНАННЯ ПЛАНУ ТЕРИТОРІЇ	59
Додаток 2 – ПРИКЛАД ВИКОНАННЯ ЗАГАЛЬНОГО ПЛАНУ БУДІВЛІ	60
Додаток 3 – ПРИКЛАД ВИКОНАННЯ ЗАГАЛЬНОГО ПЛАНУ ПРИМІЩЕНЬ	60
Додаток 4 – ПРИКЛАД ВИКОНАННЯ СТРУКТУРНОЇ СХЕМИ ШЛЯХІВ ФІЗИЧНОГО ПРОНИКНЕННЯ.....	61

ВСТУП

Для певної частки населення в сучасних економічних і соціальних умовах навчання в стаціонарі стає достатньо дорогим, а деколи і неможливим. Тому деякі студенти вибирають заочну форму навчання в університеті.

При тривалому міжсесійному періоді для студентів-заочників, успішність їх самостійної роботи визначається володінням технологією самоосвіти (самонавчання), розвитком культури роботи з методичними і навчальними матеріалами, а також володінням способами самоконтролю і самоаналізу своєї діяльності.

Ефективність заочної форми навчання за освітньою програмою “Радіотехніка” багато в чому залежить від правильного підходу до самостійного освоєння спеціальних дисциплін.

Ці методичні вказівки містять відомості, які необхідні для самостійного поетапного вивчення дисципліни “Методи і засоби захисту інформації” для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» заочної форми навчання.

1 ЗАГАЛЬНІ МЕТОДИЧНІ ВКАЗІВКИ

Основною метою створення цих методичних вказівок є надання допомоги студентам-заочникам в їх самостійній роботі з навчальною літературою, в оволодінні теоретичних і практичних знань, в раціональному використанні часу на вивчення дисципліни “Методи і засоби захисту інформації”.

Методичною основою вивчення дисципліни є системний підхід, який полягає в розгляданні питань фізичних основ виникнення технічних каналів витоку інформації (ТКВІ), в тісному взаємозв'язку з питаннями організаційно-технічного захисту інформації, інженерно-конструкторської побудови сучасних засобів виявлення ТКВІ, аналізу методів і способів, прийнятих і реалізованих в діючих системах інформаційної безпеки. Відповідно до системно-технічних принципів надання навчального матеріалу дисципліни він вивчається студентами з переходом від окремого до загального, від простого до складнішого, в

логічному взаємозв'язку і доцільному поєднанні питань теоретичного і практичного характеру.

Необхідний рівень науковості дисципліни забезпечується методологічною послідовністю застосування спільних принципів синтезу і аналізу при вивченні пристрою зразків апаратури, перевірки прийнятих варіантів їх реалізації на відповідність вимогам доцільності, раціональності, оптимальності, перспективам вдосконалення і розвитку інформаційної безпеки.

Практична спрямованість дисципліни забезпечується вивченням методики і отриманням практичних навиків в роботі із зразками техніки, які відносяться до сфери майбутньої професійної діяльності фахівця.

1.1 Основні види занять

Основними видами занять є самостійна робота і консультації. Додатково, в період установчої сесії, проводяться лекції і лабораторні роботи.

Відповідно до теми заняття студент-заочник самостійно або після консультації з викладачем вивчає методи і способи захисту інформації.

1.1.1 Самостійна підготовка

У години самостійної підготовки студенти закріплюють отримані на заняттях в період установчої сесії знання, вивчають рекомендовану літературу. Вона направлена, на глибоке і всебічне вивчення фізичних принципів виникнення ТКВІ, аналіз технічних характеристик пристроїв знімання інформації, методику і способи їх виявлення і усунення. При цьому студент-заочник продовжує вирішення проблемних питань, поставлених в робочій програмі і методичних вказівках.

Для якіснішого засвоєння матеріалу студентом, навчальний матеріал повинен розглядатися з позицій «чому так зроблено», «наскільки це оптимально (раціонально, доцільно)», при цьому корисно розібратися в порядку проведення заходів щодо виявлення ТКВІ.

1.1.2 Лекції.

Для надання допомоги студентам-заочникам у вивченні дисципліни в період установчої сесії їм читають лекції. При читанні лекцій подаються основні напрями вивчення дисципліни і розглядаються найбільш складні теми і питання навчального матеріалу. Матеріал лекцій дає основи наукових знань з дисципліни, яка вивчається, розкриває в діалектичному взаємозв'язку найбільш складні питання навчального матеріалу, сприяє розвитку творчого мислення студентів, відображає актуальні питання теорії і практики, сучасні досягнення науки і техніки і є основою для організації і проведення інших видів занять і самостійної роботи.

1.1.3 Лабораторні роботи

Лабораторні роботи носять пошуково-дослідницький характер і проводяться дослідницьким методом у поєднанні з методом практичних робіт з метою закріплення теоретичних знань студентів-заочників, навчання методам і прийомам експериментальних і наукових досліджень, прищеплення навиків наукового і інженерного аналізу конструкторських рішень, придбання навиків експлуатації штатних контрольно-вимірювальних приладів.

Лабораторні роботи проводяться в період установчої сесії. Для індивідуалізації і підвищення якості навчання група на лабораторному занятті розподіляється на бригади по кількості робочих місць. Лабораторна робота завершується її захистом кожним студентом і лише за цієї умови вважається за виконану. Студенти, які не встигли захиститися в ході заняття, здають звіт по роботі і захищаються під час проведення встановлених розкладом консультацій. В цей же час за узгодженням з викладачем відпрацьовують і захищають лабораторну роботу відсутні, на плановому занятті студенти. Якість занять забезпечується складом бригад не більше двох-трьох студентів в кожній, та проведенням індивідуального захисту лабораторної роботи кожним студентом.

Теми і порядок виконання відображені в методичних вказівках до проведення лабораторних робіт з дисципліни.

При проведенні занять на техніці зв'язку, в університеті керівник заняття проводить інструктаж по правилах техніки безпеки, оформлює його документально з розписом студентів в журналі.

1.1.4 Консультації

Групові і індивідуальні консультації проводяться у встановлений розкладом занять час викладачем з метою надання допомоги студентам при самостійному освоєнні ними навчального матеріалу, підготовці лабораторних занять і заліку.

1.2 Оцінка знань

Оцінка знань студентів-заочників здійснюється в ході поточного і підсумкового контролю.

Поточний контроль проводиться для перевірки повноти і якості засвоєння студентами навчального матеріалу, стимулювання їх роботи. Він здійснюється в ході лабораторних занять.

Підсумковий контроль проводиться для перевірки рівня теоретичної і практичної підготовки студентів і включає залік в 9 семестрі навчання.

2 РОБОЧА ПРОГРАМА ВИВЧЕННЯ ТЕМ ДИСЦИПЛІНИ

Змістовий модуль 1. Основи інформаційної безпеки і захисту інформації.

Тема 1 Вступ. Основні концептуальні положення системи захисту інформації.

Сучасна постановка проблеми захисту інформації. Поняття «Інформаційна безпека». Місце, цілі і завдання інформаційної безпеки.

Концептуальна модель інформаційної безпеки. Цілі переслідувані джерелами загроз. Прояв загроз інформації. Класифікація загроз.

Дії, що призводять до неправомірного оволодіння конфіденційною інформацією і їх класифікація. Розголошення. Витік. Несанкціонований доступ. Формальні та неформальні канали поширення інформації.

Забезпечення інформаційної безпеки. Основні принципи забезпечення інформаційної безпеки. Рівні (напрями) захисту інформації.

Правові основи захисту інформації. Структура законодавства України в області захисту інформації.

Організаційні заходи захисту інформації. Організаційно-правові форми захисту інформації.

Інженерно-технічний захист. Класифікація інженерно-технічний захисту.

Тема 2 Об'єкти захисту, відомості, що охороняються, і демаскуючі ознаки.

Об'єкти захисту. Основні об'єкти захисту. Перелік об'єктів, які підлягають захисту в технічних засобах передачі, зберігання і обробки інформації. Перелік об'єктів, які підлягають захисту в допоміжних технічних засобах і системах.

Відомості, що охороняються. Відомості у військовій області. Відомості в області економіки, науки і техніки. Відомості в сфері зовнішньої політики і економіки. Відомості в області розвідувальній, контррозвідувальній і оперативно-пошуковій діяльності.

Демаскуючі ознаки. Первинні демаскуючі ознаки. Вторинні демаскуючі ознаки. Формування переліку демаскуючих ознак методом експертних оцінок.

Тема 3 Класифікація і основні характеристики технічних каналів просочування інформації.

Поняття і структура технічного каналу просочування інформації (ТКП). Класифікація видів ТКП.

Канали просочування інформації, що обробляється технічними засобами прийому, обробки, зберігання і передачі інформації.

Канали просочування мовної інформації. Акустичні, вібраційні, акустоелектричні, оптоелектронні (лазерні) і параметричні канали.

Канали просочування інформації при її передачі по каналах зв'язку. Електромагнітні, електричні та індукційні канали.

Технічні канали витоку відеоінформації. Спостереження за об'єктами. Зйомка об'єктів. Зняття копій документів.

Несанкціонований доступ до інформації, що обробляється засобами обчислювальної техніки. Спроби злому засобів обчислювальної техніки

Технічні канали просочування інформації, що виникає при роботі обчислювальної техніки за рахунок ПЕМВН. Класифікація каналів по середовищу поширення, за способом створення, по фізичній природі.

Тема 4 Акустичні і віброакустичні канали просочування мовної інформації з об'ємів виділених приміщень.

Основні поняття, визначення і одиниці виміру в акустиці.

Основні акустичні параметри мовних сигналів. Основні статистичні параметри: частотний діапазон, рівень мовних сигналів, динамічний діапазон, сприйняття мови, розбірливість і зрозумілість мови.

Поширення акустичних сигналів в приміщеннях і будівельних конструкціях. Основні поняття в будівельній акустиці. Коефіцієнти поглинання, відображення, звукопроникності та звукоізоляція.

Канали просочування мовної інформації. Акустичні та віброакустичні канали.

Акустичне підслуховування – пасивний спосіб добування інформації. Види об'єктів, які визначають вибір каналу прослуховування і тактику дій зловмисника.

Тема 5 Знімання інформації з використанням закладних пристроїв. Загальні характеристики і побудова закладних пристроїв.

Класифікація і загальні характеристики заставних пристроїв.

Радіозакладні пристрої.

Радіозакладні пристрої, що перевипромінюють.

Закладні облаштування типу «довге вухо».

Мережеві закладні пристрої.

Змістовий модуль 2. Методи і способи захисту інформації.

Тема 6 Виявлення каналів просочування інформації.

Заходи по виявленню і протидії роботі закладних пристроїв.

Засоби виявлення каналів просочування інформації. Засоби виявлення облаштувань знімання інформації з радіоканалом. Автоматизовані пошукові комплекси. Нелінійні локатори. Доглядова техніка. Засоби радіаційного контролю.

Тема 7 Захист мовної інформації.

Методи, які застосовуються для захисту мови від несанкціонованого прослуховування. Активні і пасивні методи. Основна ідея пасивних засобів захисту інформації. Пасивні засоби захисту виділених приміщень.

Звукоізоляція приміщень. Коефіцієнти поглинання звуку різними середовищами.

Способи активного захисту приміщень. Вібродатчики систем віброакустичного зашумлення.

Оптимальні параметри перешкод і апаратура для їх постановки.

Особливості постановки активних перешкод.

Тема 8 Основи сучасної криптографії і питання шифрування. Криптографія і криптосистеми.

Історія криптографії, основні терміни і вимоги, що пред'являються до криптосистем. Історія криптографії. Термінологія. Криптографічна система, Основні вимоги, що пред'являються до криптосистем.

Симетричні криптосистеми і системи шифрування. Перестановки.

Системи підстановок. Підстановка Цезаря. Гамування. Блокові шифри. Шифри Хілла і Плейфера. Системи шифрування Віжинера.

Датчики ПВЧ. Багатоалфавітні системи. Системи одноразового використання. Датчики М-послідовностей.

Стандарт шифрування даних ДОСТ 28147-89.

Тема 9 Огляд сучасних криптосистем. Засоби автентифікації даних і управління ключами шифрування.

Системи з відкритим ключем. Безповоротні або односторонні функції. Засоби для розподілу ключів.

Алгоритм RSA. Гарантована оцінка захищеності алгоритму RSA. Математичні результати. Практична реалізація RSA.

Криптосистема Ель-Гамала. Криптосистеми на основі еліптичних рівнянь.

Електронний підпис. Можливі порушення захисту повідомлень. Засоби автентифікації користувачів. Електронний підпис на основі алгоритму RSA.

Цифрова сигнатура. Хеш-функції. Управління ключами. Генерація ключів. Накопичення ключів. Розподіл ключів. Механізм запиту-відповіді. Механізм відмітки часу ("часовий штампель").

3 ПЕРЕЛІК ЛАБОРАТОРНИХ РОБІТ

В період проведення установчої сесії із студентами-заочниками проводяться наступні лабораторні роботи:

Лабораторна робота № 1. «Дослідження регламенту радіочастотного діапазону від 30 МГц до 1 ГГц м. Запоріжжя».

Лабораторна робота № 2. «Дослідження спрямованих мікрофонів».

Лабораторна робота № 3. «Контактне зняття мовної інформації з телефонної лінії з використанням програмно-апаратного комплексу».

Лабораторна робота № 4. «Вивчення характеристик та будови пристрою СРМ-700 («Акула»)».

Лабораторна робота № 5 «Дослідження генератору акустичного зашумлення ANG-2200».

Лабораторна робота № 6 «Дослідження маскувача мовних сигналів».

Мета, основні теоретичні дані для успішного проведення робіт, опису лабораторних стендів і вимірювальних приладів для виконання поставлених завдань, порядок дій і оформлення звітів про роботи, з переліком питань для захисту приведеній в методичних вказівках для виконання лабораторних робіт по дисципліні “Методи і засоби захисту інформації”.

4. КОНТРОЛЬНІ ЗАВДАННЯ

Кожен студент-заочник в процесі опрацювання теоретичного матеріалу по курсу "Методи і засоби захисту інформації" повинен виконати три контрольні роботи. Виконання робіт переслідує дві мети: по-перше, закріплення матеріалу, який вивчається, і, по-друге, здійснення кафедрою контролю за самостійною роботою студента, а також надання студентові допомоги в питаннях, слабо засвоєних або незрозумілих, оскільки виконання задач і складання схем захисту допомагає з'ясувати фізичний сенс і повніше розкрити істоту явищ, які вивчаються, прищеплює навички практичного застосування теоретичних знань.

Контрольні роботи містять декілька завдань, з яких кожна є завданням: вивчення і описи об'єкту захисту, докладного розрахунку вартості інформації, яка захищається, побудови моделі об'єкту захисту і порушника, моделювання погроз, безпеки інформації, розробки організаційних і технічних заходів, по захисту інформації відповідно до тем курсу.

Як початкові дані студенти вибирають абстрактний об'єкт захисту у вигляді офісу фірми, виділеного приміщення, в якому здійснюється робота з конфіденційною інформацією, кімнати для переговорів і тому подібне, які можуть бути образами аналогічних об'єктів за місцем роботи студента або знайомі йому по навчальній практиці.

Виконання чужого варіанту приводить до автоматичному незаліку роботи. Тому при виборі даних свого варіанту які-небудь помилки недопустимі.

Контрольна робота виконується на друкуючих і графічних пристроях виводу за допомогою ЕОМ (при оформленні тексту на ЕОМ необхідно витримувати вимоги СТП 15-96 п.6.1.2-6.1.4). На титульному листі мають бути розбірливо вказані адреса студента, прізвище, ім'я, по батькові (повністю), номер залікової книжки, група, дата відправки роботи на перевірку. На листах мають бути поля для зауважень викладача.

Текстовою матеріал, графічні побудови і схеми мають бути виконані в строгій відповідності з ДСТУ і ЄСКД.

План території, спільний план будівлі (поверху) і план приміщень, з розміщенням технічних засобів захисту інформації на об'єкті, що охороняється, мають бути виконані у вигляді ескізів на листах формату А3 (Додатки 1-3).

Всі розрахунки і графічні матеріали необхідно супроводжувати відповідними поясненнями. Кожній математичній операції повинне передувати письмове пояснення, потім приводиться розрахункова формула, підраховується результат. Позначення фізичних величин, які входять до розрахункової формули, мають бути єдиними.

Повністю оформлена робота, не пізніше вказаного викладачем терміну, має бути представлена йому для рецензування. Разом з роботою надається її електронна копія.

Після отримання з перевірки прорецензованої роботи студент перед пред'явленням її на заліку зобов'язаний виконати вказівки, зроблені рецензентом.

Якщо контрольна робота при рецензуванні не зарахована, студент повинен виконати її наново і представити на повторну рецензію разом з не зарахованою зі всіма зауваженнями. Поправки в не зарахованій роботі не допускаються.

Вихідні дані для виконання контрольних робіт приведені в таблицях 4.1 і 4.2.

Таблиця 4.1

Передостання цифра зал. книжки	0	1	2	3	4	5	6	7	8	9
Кількість працівників	25	26	28	22	34	22	29	21	25	30
Кількість приміщень ¹	9	9	10	8	11	8	10	8	9	10
Максимальна категорія важливості інформації	К	СК	К	ОК	ДСК	К	СК	К	ОК	ДСК

¹Включаючи службові і підсобні приміщення

Остання цифра зал. книжки	0	1	2	3	4	5	6	7	8	9
Телевізійні засоби спостереження	немає	немає	немає	є	немає	немає	немає	немає	є	немає
Пожежна сигналізація	є	є	є	є	є	є	є	є	є	є

² Всього у всій організації

Контрольна робота № 1

Для повноцінного захисту інформації потрібно вивчити структуру, розташування і роботу всього підприємства провести оцінку загроз, визначити інформаційні ресурси, які доцільно захищати насамперед, і продумати, що необхідне для забезпечення їх безпеки.

При виконанні першої роботи необхідно провести опис об'єкту (організації) захисту і моделювання об'єктів захисту.

1. У **описі об'єкту** доцільно в узагальненій формі відобразити наступні відомості:

- а) найменування об'єкту;
- б) вид його діяльності;
- в) типовий порядок роботи;
- г) які відомості можуть містити інформацію, що захищається;
- д) до чого може привести розголошування (втрата) цих відомостей;
- є) де територіально розташовується об'єкт (організація);
- ж) коли на об'єкті проводилися ремонтні або будівельні роботи;
- з) у якому вигляді представлений основний об'єм інформації, віднесеної до тієї, що захищається (електронні документи, "тверді" копії);
- і) відповідає і чи задовольняє існуючий порядок роботи з такими документами, необхідному рівню захисту;
- к) чи дотримується режим конфіденційності на об'єкті;

л) усвідомлює і чи розуміє керівництво необхідність і проблеми захисту інформації.

Як додатки до опису об'єкту необхідно скласти план території і спільний план будівлі (поверху) (Додатки 1-2).

На плані території організації вказуються місця розміщення будівлі (будівель), паркану, КПП, які граничать з територією вулиці і будівлі, місця розміщення і зони дії технічних засобів охорони, телевізійної системи спостереження і зовнішнього освітлення, місця виводу з організації кабелів, по яких можуть передаватися сигнали з інформацією.

На загальних планах поверхів будівлі указуються виділені (з інформацією, що захищається) і сусідні приміщення, схеми трубопроводів водяного опалювання, повітропроводів вентиляції, кабелів електропроводки, телефонної і обчислювальної мереж, радіотрансляції, заземлення, зони освітленості чергового освітлення, місця розміщення і зони спостереження телевізійних камер і так далі.

2. Задача моделювання об'єктів захисту полягає в об'єктивному описі і аналізі джерел конфіденційної інформації і існуючої системи її захисту.

Моделювання об'єктів захисту включає:

- ✎ структуризацію інформації, яка захищається;
- ✎ розробку просторової моделі об'єкту захисту.

При моделюванні об'єктів захисту проводиться:

- визначення джерел інформації, яка захищається;
- опис просторового розташування основних місць розміщення джерел інформації, що захищається;

Структуризація інформації, яка захищається

Для структуризації інформації як початкові дані використовуються:

- перелік відомостей, які складають державну, відомчу або комерційну таємницю;
- перелік джерел інформації в організації.

Структуризація інформації проводиться шляхом класифікації інформації відповідно до структури, функцій і завдань організації з прив'язкою елементів інформації до її джерел. Деталізацію інформації доцільно проводити до рівня, на якому елементу інформації відповідає одне джерело.

Схема класифікації розробляється у вигляді графа-структури, нульовий (верхній) рівень ієрархії якої відповідає поняттю «Конфіденційна інформація», а *i*-ий (ніжній) - елементам інформації одного джерела з переліку джерел організації. Основна вимога до схеми класифікації - спільна ознака і повнота класифікації, відсутність перетинів між елементами класифікації одного рівня, тобто одна і та ж інформація не повинна указуватися в різних елементах класифікації.

Результати структуризації оформляються у вигляді:

- схеми класифікації інформації, приклад якої наведений на рис.4.1;
- таблиці, варіант форми якої приведений в таблиці. 4.3.

Конфіденційна інформація

Про організацію:	Про внутрішню діяльність організації:	Про зовнішню діяльність організації:
– структура; – методи управління; – фінанси; – плани і програми; – проблеми і шляхи їх рішення; – безпека.	– якість продукції; – собівартість продукції; – характеристики продукції, що розробляється; – можливості виробництва; – технології; – дослідницькі роботи.	– принципи, концепція і стратегія маркетингу; – канали придбання і збуту; – партнери; – конкуренти; – переговори і угоди.

Рисунок 4.1 – Варіант структури конфіденційної інформації

Таблиця 4.3

№ елемента інформації	Найменування елемента інформації	Гриф конфіденційності інформації	Ціна інформації	Найменування джерела інформації	Місцезнаходження джерела інформації
1	2	3	4	5	6

Таблиця розробляється на основі схеми класифікації інформації. У першому стовпці указується номер елемента інформації в схемі класифікації.

Порядковий номер елемента інформації відповідає номеру тематичного питання в структурі інформації. Значність номера дорівнює кількості рівнів структури, а кожна цифра - порядковому номеру

тематичного питання на даному рівні серед питань, які відносяться до одного тематичного питання на попередньому рівні.

Наприклад, номер 2635 відповідає інформації 5-го тематичного питання на 4-му рівні, вхідного в 3-є укрупнене питання 3-го рівня, який, у свою чергу, є часткою 6-го тематичного питання 2-го рівня, що є питанням 2-ої теми 1-го рівня.

У стовпці «найменування елементу інформації» указується тематичне питання, відповідне порядковому номеру цього елементу. Гриф і ціна елементу можуть бути призначені виходячи з прийнятої шкали класифікації конфіденційної інформації, показано в табл.4.4. $\bar{Z}_B$ – відносна вартість біта інформації яка виражена в умовній вартості одиниці інформації.

Таблиця 4.4 – Класифікація конфіденційної інформації

Категорія (гриф) важливості		Віднос на вартість біта інформації $\bar{Z}_B$	Потрібна надійність захисту QT (%)	Категорія захисту	Опис грифу таємності
скорочене	повне				
ОВ (ОК)	Особливий важливості (особливо конфіденційно)	10^4	99,99	Гранично високий рівень	Призначається інформації тієї, що містить найвищу таємність, при розголошенні якої можливі найтяжчі наслідки
СТ (СК)	Суворо таємно (строго конфіденційно)	10^3	99,9	Високий рівень	Призначається інформації такою, що містить високий ступінь таємності
Т(К)	Таємно (конфіденційно)	10^2	99,0	Достатній рівень	Призначається інформації тієї, що містить таємні відомості
ДСК	Для службового користування	10	90,0	Допустимий рівень	Має найменшу таємність, призначається в основному внутрішнім документам
В	Відкрита	1	37,0	Низький рівень	Для інформації тієї, що не містить таємні відомості

Кожному грифові конфіденційності інформації можна поставити у відповідність свій K_z – коефіцієнт цінності інформації (чим вище цей коефіцієнт, тим цінніше інформація):

Наприклад:

- ☆ Для Службового Користування (ДСК) – (0.1);
- ☆ Конфіденційно (К) – (0.4);
- ☆ Строго конфіденційно (СК) – (0.7).

Розрахунок ціни інформації, яка захищається

Для визначення вартості інформації, що захищається, використовуються два підходи.

1) Перший полягає в обчисленні вартості інформації виходячи з її **об'єму і вартості одиниці інформації** (1 кілобайт, 1 сторінка і ін.).

2) Другий підхід полягає в оцінці вартості інформації за вартістю збитку, який буде причинний при втраті або розголошенні інформації, що захищається, в цьому випадку ціна інформації призначається **методом експертної оцінки**.

Очевидно, що не всі елементи інформації мають однакову вартість. Тому обчислювати ціну інформації можна тільки для інформації, яка має гриф секретності і знаходиться на носіях в електронному або “твердому” вигляді. Для такої інформації обчислення методом експертних оцінок буде неефективним, і обчислення за допомогою застосування об'єму інформації матиме незначну погрішність. У решті всіх випадків ціна інформації визначається методом експертних оцінок.

Тому при виконанні розрахунків вартості інформації, що захищається, в електронному або “твердому” вигляді необхідно використовувати перший підхід, а для тієї, що всієї залишилася – другий. При цьому у виконуваний контрольній роботі мають бути присутніми обидва підходи.

Розгледимо більш докладніше ці підходи.

Як вже наголошувалося **перший підхід** полягає в обчисленні вартості інформації виходячи з її об'єму і вартості одиниці інформації, який визначається таким чином.

Середній об'єм інформації в сторінці розміром А4 для шрифту кеглем 14 складає приблизно 4 тисячі знаків, що складає 4 Кб.

Враховуючи, що листи практично не бувають заповненими повністю, можна прийняти середній об'єм інформації в 2,5 Кб на сторінку.

Необхідно враховувати, що інформація в паперовому і цифровому вигляді не повинна дублювати один одного, тобто враховується тільки об'єм унікальної інформації і при розрахунках береться об'єм що міститься в одному з джерел. Також необхідно застосовувати для обчислення об'єм корисної інформації, тобто інформації в чистому вигляді, оскільки інколи невелика кількість інформації може займати значний об'єм. Особливо це характерно для електронної інформації.

Для обліку корисної інформації вводиться «**Коефіцієнт корисності цифрової інформації**» або «**коефіцієнт інформативності**» (K_{III}). Коефіцієнт інформативності означає частку корисної інформації в спільному об'ємі інформації.

Наприклад:

Для документів широко поширеною програми MS Word при створенні документа без графічних картинок $K_{III}=15-20\%$, саме стільки займає сам текст, що залишилися 80% - службова інформація програми. А в базі даних об'ємом 2 Мб може міститися всього 100 Кб корисної інформації – решту всього об'єму займають службові дані, що не мають практичної цінності. В цьому випадку «КП цифрової інформації»

$$\text{складатиме } K_{III} = \frac{100 \text{ Кб}}{2 \text{ Мб}} = 5\% .$$

Емпіричним шляхом визначені коефіцієнти інформативності для найбільш поширених об'єктів, які містять інформацію і приведені в таблиці 4.5:

Таблиця 4.5 – Коефіцієнти інформативності для найбільш поширених об'єктів

Об'єкт, який містить інформацію	K_{III}	Примітка
Текст договору, угоди або іншого офіційного документа	25%	на 75% доводиться інформація, що повторюється, спільні фрази і формулювання
Схема, таблиця, креслення, технічний малюнок	90%	що підтверджує "краще один раз побачити чим сто разів почути"
електронний документ, підготовлений в текстовому процесорі	20%	наприклад MS Word, Open Office і ін.
електронна база даних різного ПЗ	85%	формати спеціально розроблені для зберігання значних об'ємів даних, наприклад DBF, MDB і ін.
початковий код ПЗ у вигляді лістингу (роздруки)	90%	10% - коментарі
мова людини	30%	без врахування емоційної складової

В рамках першого підходу вартість інформації обчислюється за спільним обсягом інформації V_I , за вартістю одиниці інформації Ze і коефіцієнту інформативності K_{III} .

$$Z = Ze \cdot V_I \cdot K_{\text{III}}$$

де Z – ціна елемента інформації, яка захищається в у.о.;

V_I – об'єм інформації, яка захищається, в Кбайт;

Ze – ціна за одиницю об'єму інформації (привласнюється кожному елементу окремо і вноситься до таблиці 4.6).

K_{III} – коефіцієнт корисності цифрової інформації або коефіцієнт інформативності.

Об'єм інформації, що захищається, визначається по формулі:

$$V_I = V_{\text{циф}} + V_{\text{бум}} \cdot V_{\text{стр}}$$

де $V_{\text{циф}}$ – об'єм інформації, яка захищається, на цифровому носії в Кбайт;

$V_{\text{бум}}$ – об'єм інформації, яка захищається, на паперовому носії в сторінках;

$V_{\text{стр}}$ – середній об'єм інформації на 1 стор. в Кбайт.

Відповідно до першого підходу ці елементи інформації мають бути оцінені і результати занесені в таблицю 4.6 і в стовпець 4 (табл.4.3).

Таблиця 4.6

№	Найменування елементу інформації	Розрахунок ціни інформації			
		Z_e , ye/ Кб.	V_I (Кб)	K_{III} %	$Z = Z_e \cdot V_I \cdot K_{III}$
1	2	3	4	5	6

Приклад заповнення таблиці 4.6

№	Найменування елементу інформації	Розрахунок ціни інформації			
		Z_e , ye/ Кб.	V_I (Кб)	K_{III} %	$Z = Z_e \cdot V_I \cdot K_{III}$
1.1.1	Стратегічний план розвитку фірми	10 000	20	20%	40 000
1.1.2	Внутрішня кадрова інформація	15	500	85%	6 375
1.1.3	Внутрішня фінансова документація	18	1000	85%	15 300
1.1.4	Відомості про досягнуті угоди і домовленості	100	300	25%	7 500
1.1.5	Плани зустрічей і поїздок керівництва	300	100	30%	9 000
1.1.6	Зведення по внутрішній безпеці фірми	400	500	25%	50 000
1.4.4	Архів проведених аудиторських операцій	15	10000	85%	127 500

Далі визначається ціна інформації, об'єм якої піддається експертній оцінці.

Згідно **другому підходу**, для елементів інформації проводиться експертна оцінка. При цьому розглядаються по черзі всі невраховані в першому підході категорії інформації, яка захищається, і кожному елементу залежно від можливого заподіяного збитку заявляється певна вартість.

Для визначення «ваги» і збитків від розкриття інформації доцільно вдаватися до допомоги експертів, відомостей, що добре розуміють цінність, і їх взаємозв'язок з вказаними чинниками. Можливість прояву різних чинників в динаміці життєвого циклу інформації оцінюється суб'єктивною вірогідністю.

Наприклад: Із структури конфіденційної інформації проведемо експертну оцінку інформації отриманою від клієнтів.

Тут виділяємо елементи інформації, що підлягають експертній оцінці:

Для фірми що займається проведенням аудиторських перевірок і дослідженнями фінансових установ:

- зведення про кредитово-інвестиційну діяльність клієнтів;
- інша інформація отримана з джерел, що не афішуються, і так далі

Ці відомості є дуже важливими, мають гриф “конфіденційно” або «строго конфіденційно”. Оскільки для конкурентів найбільше значення має саме інформація про кредитово-інвестиційну діяльність клієнтів, то, на підставі експертної оцінки, збиток при витоку даних буде в 10 разів вище за збиток при витоку інших відомостей про нього. У зв'язку з цим, встановимо наступне співвідношення цін двох вищезгаданих елементів інформації – 10 до 1. Вартість інформації про різних клієнтів різна, тому виводиться середня ціна відомостей про кредитово-інвестиційну діяльність одного клієнта (рівній втраті одного укладеного контракту) і множається на кількість контрактів, що діють (актуальних). А відомості отримані з джерел, що не афішуються, в 10 разів дешевше, тобто складе 10% від важливішої інформації.

Результати проведеної експертної оцінки заноситься в таблицю 4.7

Таблиця 4.7–Результати експертної оцінки

№	Найменування елементу інформації	Ціна елементу інформації, у.о.	Пояснення
1	2	3	4

Наприклад: Для нашого випадку з ТОВ «Акварель» відповідно до другого підходу, наступні елементи інформації після проведення експертної оцінки отримали заявлену вартість:

Приклад заповнення таблиці 4.7

№	Найменування елементу інформації	Ціна елементу інформації, у.о.	Примітка
1.2.1	<i>Зведення про кредитово-інвестиційну діяльність клієнтів</i>	50 000	<i>дорівнює збитку від втрати укладеного контракту на проведення аудиту</i>
1.2.2	<i>Фінансова документація клієнтів</i>	50 000	<i>дорівнює збитку від втрати укладеного контракту на проведення аудиту</i>
1.2.3	<i>Зведення про організаційну структуру клієнтів</i>	50 000	<i>дорівнює збитку від втрати укладеного контракту на проведення аудиту</i>
1.2.4	<i>Інша інформація, надана клієнтами в рамках аудиту</i>	50 000	<i>дорівнює збитку від втрати укладеного контракту на проведення аудиту</i>
1.2.5	<i>Інша інформація про клієнтів, отримана з джерел, що не афішуються</i>	5 000	<i>дорівнює вартісної частки (до 10%) інформації, що отримується з цих джерел</i>
1.4.1	<i>Проміжні і попередні результати аудиторських перевірок клієнта</i>	50 000	<i>дорівнює збитку від втрати укладеного контракту на проведення аудиту</i>

№	Найменування елементу інформації	Ціна елементу інформації, у.о.	Примітка
1.4.2	<i>Підсумкові результати аудиторської перевірки клієнтів, підготовлені для них</i>	50 000	<i>дорівнює збитку від втрати укладеного контракту на проведення аудиту</i>
1.4.3	<i>Результати аудиторської перевірки клієнта, для внутрішнього користування</i>	20 000	<i>дорівнює собівартості робіт по проведенню аудиторської перевірки</i>
1.1.7	<i>Відомості про джерела інформації, що не афішуються, задіяні в рамках ведення аудиторської діяльності</i>	5000	<i>дорівнює втрати інформації від цих джерел, до 10% від спільного об'єму інформації</i>
1.3.2	<i>Розроблені методичні вказівки по методах проведення аудиту</i>	20 000	<i>дорівнює собівартості робіт по проведенню аудиторської перевірки</i>
1.3.3	<i>Початкові коди і працюючі версії ПЗ, розробленого для проведення аудиту</i>	20 000	<i>дорівнює собівартості робіт по проведенню аудиторської перевірки</i>

Результати експертного визначення ціни інформації, яка захищається, також заносяться в стовпець 4 (табл.4.3).

У стовпці 5 (табл.4.3) указується найменування джерела (посада, назва і тип документа або його номер по книзі обліку, найменування і номер виробу і т.д.), а в графі 6 - місця розміщення або зберігання (можливі робочі місця людей-джерел інформації, місця розташування, розміщення або зберігання інших носіїв).

Ці місця в спільному випадку є:

- приміщення (службові, лабораторії, офіси, цехи, склади, квартири і ін.);

- письмові столи робочих місць співробітників, сховища і сейфи, шафи дерев'яні і металеві в приміщеннях.

У приміщеннях розміщуються більшість джерел інформації: люди, документи, продукція, яка розробляється, і її елементи, засоби обробки і зберігання інформації і ін., а також джерела функціональних і небезпечних сигналів.

Таким чином закінчується складання підсумкової таблиці, яка вміщує перелік елементів інформації, що підлягають захисту, оцінку їх цінності, а також джерела, з яких ці елементи інформації можуть бути отримані (джерелами можуть бути люди, документи на різних носіях, фізичні поля і матеріальні об'єкти). Ця таблиця і буде структурною моделлю об'єкту захисту. У випадку, якщо в таблиці не вказано, на яких носіях зберігаються документи, то маються на увазі паперові носії. Якщо в колонці “Місцезнаходження джерела інформації” для документів вказане тільки приміщення, це означає, що дані документи часто використовуються (тобто міняється їх точне місце розташування в приміщенні), як правило, такі документи знаходяться на робочих місцях співробітників, в столах, або в шафах.

Наприклад: Структурна деталізована модель інформації, що захищається, представлена у вигляді таблиці матиме вигляд:

Приклад заповнення таблиці 4.3

№	Найменування елемента інформації	Гриф конф ід.	Ціна інформації	Найменування джерела інформації	Місцезнаходження джерела інформації
1.1.1	Стратегічний план розвитку фірми	К	40 000	Керівництво фірми паперові і електронні документи	кабінет керівництва сейф і ПЕВМ в кабінеті керівництва
1.1.2	Внутрішня кадрова інформація	ДСК	6 375	Паперові і електронні документи, БД кадрового ПЗ	сейф і ПЕВМ в приймальні, сейф і ПЕВМ в кабінеті керівництва

№	Найменування елемента інформації	Гриф конф ід.	Ціна інформації	Найменування джерела інформації	Місцезнаходження джерела інформації
1.1.3	Внутрішня фінансова документація	ДСК	15 300	Гол. бухгалтер, паперові і електронні документи, БД бухгалтерського ПЗ	Робочий стіл, шафа, сейф і ПЕВМ гол. бухгалтера
1.1.4	Відомості про досягнуті угоди і домовленості	К	7 500	Керівництво фірми, паперові документи.	Робочий стіл, сейф і ПЕВМ в кабінеті керівництва
1.1.5	Плани зустрічей і поїздок керівництва	ДСК	9 000	Керівництво фірми, секретар, паперові і електронні документи	Кабінет керівництва, приймальня, робочі столи і ПЕВМ керівництва і секретаря
1.1.6	Відомості про внутрішню безпеку фірми	ДСК	50 000	Керівництво фірми, паперові і електронні документи	Робочий стіл, сейф і ПЕВМ в кабінеті керівництва
1.1.7	Відомості про джерела інформації, що не афішуються, використовувані в рамках ведення аудиторської діяльності	К	50 000	Керівництво, співробітники груп інформаційного забезпечення, паперові і електронні документи	Сейф і ПЕВМ в кабінеті керівництва і групи інформаційного забезпечення

№	Найменування елемента інформації	Гриф конф ід.	Ціна інформації	Найменування джерела інформації	Місцезнаходження джерела інформації
1.2.1	Відомості про кредитово-інвестиційну діяльність клієнтів, надані ними для проведення аудиту	К	500 000	Співробітники групи кредитово-інвестиційного аудиту, паперові і електронні документи	Сейфи в сховищі документів; сейфи, робочі столи і ПЕВМ в кабінеті групи кредитово-інвестиційного аудиту
1.2.2	Фінансова документація клієнтів, надана ними в рамках аудиту	К	500 000	Співробітники групи фінансового аудиту, паперові і електронні документи	Сейфи в сховищі документів; сейфи, робочі столи і ПЕВМ в кабінеті групи фінансового аудиту
1.2.3	Відомості про організаційну структуру клієнтів, надані ними для проведення аудиторської перевірки	К	500 000	Співробітники групи організаційного аудиту, паперові і електронні документи	Сейфи в сховищі документів; сейфи, робочі столи і ПЕВМ в кабінеті групи організаційного аудиту
1.2.4	Інша інформація, надана клієнтами для проведення аудиторської перевірки	К	500 000	Керівництво, співробітники груп аудиту, паперові і електронні документи	Сейфи в сховищі документів; сейфи, робочі столи і ПЕВМ в кабінетах груп аудиту і керівництва

№	Найменування елемента інформації	Гриф конф ід.	Ціна інформації	Найменування джерела інформації	Місцезнаходження джерела інформації
1.2.5	Інша інформація про клієнтів, отримана з не афішуємих джерел при проведенні аудиторської перевірки	К	500 000	Керівництво, начальники груп аудиту	Сейфи в сховищі документів; сейфи, робочі столи і ПЕВМ в кабінетах керівництва і груп аудиту
1.3.2	Розроблені методичні вказівки по проведенню аудиту	ДСК	200 000	Паперові і електронні документи в групах аудиту	Шафи, сейфи і ПЕВМ в кабінетах груп аудиту
1.3.3	Початкові коди і працюючі версії ПЗ, розробленого для проведення аудиту	ДСК	200 000	ПЕВМ	ПЕВМ групи інформаційного і технічного забезпечення, ПЕВМ робочих груп
1.4.1	Проміжні і попередні результати аудиторських перевірок клієнта	СК	500 000	Керівництво, начальники груп аудиту, паперові і електронні документи	Кабінети керівництва і груп аудиту, сейфи, робочі столи і ПЕВМ в кабінетах груп аудиту
1.4.2	Підсумкові результати аудиторської перевірки клієнтів, для клієнта	СК	500 000	Керівництво, паперові і електронні документи	Кабінет керівництва, сейф і ПЕВМ в кабінеті керівництва

№	Найменування елемента інформації	Гриф конф ід.	Ціна інформації	Найменування джерела інформації	Місцезнаходження джерела інформації
1.4.3	Результати аудиторської перевірки клієнта, для внутрішнього користування	СК	200 000	паперові і електронні документи	Сейф і ПЕВМ в кабінеті керівництва, сейфи в сховищі документів
1.4.4	Архів проведених аудиторських операцій	СК	127 500	паперові і електронні документи	сейфи і шафи в приміщенні архіву

Таким чином, були проведені класифікація і структуризація інформації відповідно до функцій, завдань і структури організації, інформація, яка внаслідок цього захищається, була представлена у вигляді окремих елементів інформації.

Розробка просторової моделі об'єкту захисту

Модельовання проводиться на основі просторових моделей контрольованих зон з вказівкою місць розташування джерел інформації, які захищаються, - планів приміщень, поверхів будівель, території в цілому. На планах (Додаток 3) приміщень указуються в масштабі місця розміщення огороджувальних, екранів, повітропроводів, батареї і труби опалювання, елементів інтер'єру і інших конструктивних елементів, сприяючих або ускладнюючих розповсюдження сигналів з інформацією, яка захищається, а також місця розміщення і зони дії технічних засобів охорони і телевізійного спостереження. Їх параметри доцільно об'єднати в таблиці, варіант якої приведений у вигляді табл.4.8.

Таблиця 4.8.

1	Назва приміщення			
2	Поверх		Площа, м ²	
3	Кількість вікон, тип сигналізації, наявність штор на вікнах		Куди виходять вікна	
4	Двері, к-ть, одинарні, подвійні		Куди виходять двері	
5	Сусідні приміщення, назва, товщина стін			
6	Приміщення над стелею, назва,			

	товщина перекриттів		
7	Приміщення під підлогою, назва, товщина перекриттів		
8	Вентиляційні отвори, місця розміщення, розміри отворів		
9	Батареї опалювання, типи, куди виходять труби		
10	Ланцюги електроживлення	Напруга, (В), кількість розеток електроживлення, вхідних кабелів, що виходять	
11	Телефон	Типи, місця установки телефонних апаратів, тип кабелю	
12	Радіотрансляція	Типи гучномовців місця установки	
13	Електричний годинник	Тип, куди виходить кабель електричного годин	
14	Побутові радіозасоби	Радіоприймачі, телевізори, аудіо і відеомагнітофони, їх к-ть і типи	
15	Побутові електроприлади	Вентилятори і ін., місця їх розміщення	
16	ПЕВМ	К-ть, типи, склад, місця розміщення	
17	Технічні засоби охорони	Типи і місця розташування сповіщувачів, зони дій випромінювань	
18	Телевізійні засоби спостереження	Місця установки, типи і зони спостереження телевізійних трубок	
19	Пожежна сигналізація	Типи сповіщувачів, схеми з'єднання і виведення шлейфу	
20	Інші засоби		

Примітка: у таблицю можна вносити позиційні позначення елементів ТЗП і ВТСС з вказівкою їх координат на плані приміщення (наприклад, Пк1:А4 може позначати персональний комп'ютер, розташований в квадраті А4 плану). Ланцюги електроживлення, слабкострумові ланцюги, газо- і водопроводи і тому

подібне в таблиці позначаються колірними умовними позначеннями, які вони мають на плані.

Приклад складання просторових моделей контрольованих зон

1. Найменування приміщення	Серверна	Адміністра торська	Приймаль ня	Кабінет директора
2. Поверх; майдан, м ²	4 поверх, 40 м ²	4 поверх; 22 м ²	4 поверх; 18 м ²	4 поверх; 28 м ²
3. Кількість вікон, тип, сигналізація, наявність штор, жалюзі	3 вікна, ПВХ-профіль 2х-камерний, тоновані із зовнішнього боку, вертикальні жалюзі, сигналізація Velleman HAM103	1 вікна тоновані із зовнішнього боку, ПВХ-профіль 2-камерний, сигналізація Velleman HAM103, горизонтальні жалюзі	1 вікно тоноване із зовнішнього боку, ПВХ-профіль 2-камерний, сигналізація Velleman HAM103, горизонтальні жалюзі	1 вікно тоноване із зовнішнього боку, ПВХ-профіль 2-камерний, сигналізація Velleman HAM103
4. К-ть дверей, тип, одинарні або подвійні	2 двері, ПВХ-профіль, одинарні	1 двері, одинарні, алюміній, замкнув на магнітній карті з відеокамерою NTC PM640E	1 двері вхідні, одинарні дерев'яні, перехід у відділ по роботі з клієнтами	Вхідні двері з приймальні, одинарні, дерев'яні
5. Сусідні приміщення	Малий коридор, адміністраторська	Малий коридор, відділ по роботі з клієнтами	Кабінет директора, відділ по роботі з клієнтами	Приймальня, відділ по роботі з клієнтами
6. Приміщення над стелею	Немає (дах)	Немає (дах)	Немає (дах)	Немає (дах)

7. Приміщення під підлогою	<i>Торгівельна точка (магазин одягу)</i>	<i>Торгівельна точка (магазин одягу)</i>	<i>Торгівельна точка (магазин одягу)</i>	<i>Торгівельна точка (магазин одягу)</i>
8. Вентиляція, місця розміщення, розміри отворів	<i>Місцева, в межах робочих місць, 40х40см</i>	<i>Місцева, в межах робочих місць, 40х40см</i>	<i>Місцева, під стелею, 40х40см</i>	<i>Місцева, в межах робочих місць, 40х40см</i>
9. Батареї опалювання, типи, куди виходять труби	-	-	-	-
10. Ланцюги електроживлення, напруга (В), к-ть розеток, входи і виходи кабелів	<i>Напруга 220В, введення основного і резервного живлення, 2 вимикачі, 2 розетки</i>	<i>Напруга 220В, введення основного і резервного живлення, 1 вимикач 1 розетка</i>	<i>Напруга 220В, введення основного і резервного живлення, 1 вимикач, 1 розетка</i>	<i>Основне+резервне живлення. Напруга 220В</i>
11. Телефон, типи, місця установки, тип кабелю	-	<i>Телефон внутрішньої АТС, на столі адміністрації</i>	<i>Телефон внутрішньої АТС, телефон/факс міської АТС, на столі</i>	<i>Телефон внутрішньої АТС</i>
12. Електронний годинник, тип, куди виходять кабелю	-	-	-	-
13. Побутові радіозасоби, типи, місця	-	-	-	-

розташування				
14. Побутові електроприлади, місця розташування	2 кондиціонера		Настільна лампа денного світла	Кондиціонер <i>p</i> Ariston ASC-1212E, на стіні зліва від входу
15. ПЕВМ, типи, склад, місця розташування	Веб-сервер-сервер: Dual-Core Intel XEON 5100, 4GB DDR, SATA-Raid 400GB, екранований Сервер каталогів і баз даних: Intel Core 2 Duo, 2GB DDR, 350GB HDD, екранований Обидва розташовано в центрі кімнати на відстані 4 метри один від одного 2 апаратних firewall Cisco підключені до кожного сервера	1 ПЕВМ Intel Core 2 Duo, 1024Mb DDR, DVD-RW-Drive, 4xUSB+2, Monitor TFT 19" – на робочих місцях Сервер, обслуговуючи й мережу Компанії: Intel Core 2 Duo 2.0GHz, 4GB DDR	1 ПЕВМ Intel Core 2 Duo, 1024Mb DDR, DVD-RW-Drive, 4xUSB+2, HDD 80Gb, Monitor TFT 19", принтер лазерний Smasung ML-1520P – на робочому столі	1 ПЕВМ Intel Core 2 Duo, 1024Mb DDR, DVD-RW-Drive, 4xUSB+2, HDD 80Gb, Monitor TFT 19"
16. ТСО, типи і місця установки сповіщувачів, зони дії	Visonic DISCOVERY-LT з розширеним температурним діапазоном, кут 78 градусів	-	-	-

17. ТС спостереження, типи і місця установки, зони дії	-	-	-	-
18. Пожежна сигналізація, типи сповіщувачів, схеми з'єднання і виводи шлейфу	<i>Ю9001. Сповіщувач In103-3-a2-1м тепловий максимальний 62С</i>	<i>Ю9001. Сповіщувач In103-3-a2-1м тепловий максимальний 62С</i>	<i>Ю9001. Сповіщувач In103-3-a2-1м тепловий максимальний 62С</i>	<i>Ю9001. Сповіщувач In103-3-a2-1м тепловий максимальний 62С</i>

Контрольна робота № 2

При виконанні другої роботи необхідно провести моделювання погроз безпеці інформації для об'єкту який розглянуто в контрольній роботі №1.

Моделювання погроз безпеці інформації передбачає аналіз способів її розкрадання, зміни і знищення з метою оцінки що наноситься цими способами збитку.

Моделювання погроз включає:

- моделювання способів фізичного проникнення зловмисника до джерел інформації;
- моделювання технічних каналів витоку інформації.

Завданнями моделювання погроз є:

- прогнозування і виявлення шляхів розповсюдження носіїв з інформації, що захищається, за межі контрольованих зон (приміщень, будівель, території організації);
- опис з вказівкою характеристик існуючих перешкод на шляхах розповсюдження носіїв з інформацією за межі контрольованих зон.

Розробка моделі загрози фізичного проникнення.

Для створення моделі загрози фізичного проникнення, достатньо близької до реальної, необхідно «перевтілитися» в зловмисника, тобто спробувати в думках програти з позиції зловмисника варіанти проникнення до джерела інформації. Чим більше при цьому буде

враховано чинників, які впливають на ефективність проникнення, тим вище адекватність моделі. В умовах відсутності інформації про зловмисника, його кваліфікацію, технічній оснащеності щоб уникнути грубих помилок краще переоцінити загрозу, чим її недооцінити, хоча такий підхід і може привести до збільшення витрат на захист.

На основі такого підходу зловмисник повинен виглядати таким чином:

- ✓ представляє серйозного супротивника, який ретельно готує операцію проникнення, вивчає: обстановку навколо території організації, спостережувані механічні перешкоди, засоби охорони, телевізійного спостереження і чергового (нічного) освітлення, а також співробітників з метою добування від них інформації про способи і засоби захисту;
- ✓ має в розпорядженні сучасні технічні засоби проникнення і подолання механічних перешкод;
- ✓ всіма доступними способами здобуває і аналізує інформацію про розташування будівель і приміщень організації, про кордони охорони, про місця зберігання джерел інформації, види і типів засобів охорони, телевізійного спостереження, освітлення і місцях їх установки;
- ✓ проводить аналіз можливих шляхів проникнення до джерел інформації і відходу після виконання завдання.

При моделюванні дій кваліфікованого зловмисника необхідно також виходити з припущення, що він добре представляє сучасний стан технічних засобів захисту інформації, типові варіанти їх застосування, слабкі місця і «мертві» зони діаграм спрямованості активних засобів охорони.

На даному етапі розглядаються всілякі шляхи безпосереднього доступу до інформації шляхом фізичного проникнення до її джерел. На підставі планів і схем з Додатка створимо структурну схему (граф), що наочно показує всі можливі шляхи проникнення в організацію і переміщення по ній (Додаток 4). У цій структурній схемі вказуються приміщення, двері і вікна організації і взаємозв'язок між ними. Приміщення, в яких знаходяться джерела інформації, що захищається, що представляють інтерес для зловмисника при фізичному проникненні, виділені. Для кожного з таких приміщень вказані номери елементів інформації, джерела яких знаходяться в ній. Також на схемі приведені

відносні складнощі проникнення в приміщення різними способами, відповідно до наступної таблиці.

Шлях складається по планах приміщення з позначеними кімнатами (R) і дверима (D). Він складається з послідовності вікон (W) і дверей, які потрібно подолати зловмисникові для досягнення мети.

Оцінка реальності шляху:

Реальність шляху є вірогідністю вибору зловмисником цього шляху. Вона визначається методом експертних оцінок. Вірогідність залежить від простоти реалізації саме цього шляху проникнення. Очевидно, що через деякі вікна і двері легко проникнути, тому повинне враховуватися декілька міркувань:

1. Проникнути легко через вікно, яке виходить на вулицю, чим через вікно, що виходить у внутрішній двір організації, банку;
2. Проникнути легше через двері, ніж через вікно;
3. Складність механічних перешкод (складність замків і т.і.).
4. Легко проникнути у вікно, яке не містить додаткових засобів захисту, чим у вікно з ґратами;
5. Проникнути легко через звичайні двері, чим через залізну;
6. У вікно першого поверху легко забратися, чим у вікно другого *(оскільки може бути, що впритул до будівлі не прилягають які-небудь будівлі, або пожежних сходів немає – дах знаходиться під повним контролем; також ґрати на вікнах першого поверху вертикальні, тобто забратися по ним на другий поверх важче)*;
7. Чим більше потрібно минути перешкод, тим шлях менш вірогідний;
8. Проглядність вікна (двері) з головного входу і з КП на в'їзді на територію двору, де може чергувати охорона;
9. Наявність на дверях (вікні) сигналізації і так далі

Можливі шляхи проникнення зловмисників наголошуються лініями на планах (схемах) території, поверхів і приміщень будівель, а результати аналізу шляху заносяться в таблиці. 4.10.

При оцінці складності проникнення через двері, ведучу в основну будівлю, має бути врахований той факт, що таке проникнення задоволене складно, оскільки як правило вхідні двері обладналися додатковими захисними засобами.

Таблиця 4.9 – Приклад визначення відносної складності проникнення в приміщення лабораторії різними способами

Спосіб проникнення	Відносна складність
<i>Вікна в лабораторних боксах</i>	3
<i>Вікна в кабінеті начальника і приміщенні обслуговування лабораторного устаткування</i>	5
<i>Внутрішні двері лабораторії</i>	2
<i>Основний вхід в лабораторію</i>	6
<i>Запасний вхід в лабораторію</i>	4
<i>Двері з основної будівлі інституту</i>	7

Таблиця 4.10 – Модель способів фізичного проникнення.

№	Найменування елемента інформації	Ціна інформації	Шлях проникнення зловмисника	Оцінка реальності шляху	Величина загрози	Ранг загрози
1	2	3	4	5	6	7

Оцінка реальності шляху проникнення проводиться по наступній формулі:

$$Op = \frac{1}{\sum Bi},$$

де Op – оцінка реальності шляху;

$\sum Bi$ – сумарна складність шляху проникнення.

Величина загрози якому-небудь з елементів інформації, що захищається, при даному шляху проникнення розраховується так:

$$Sy = Op \cdot Z$$

де Sy – величина загрози, у.е.;

Z – ціна елементу інформації що захищається в у.о., (береться з Таблиці 4.6).

Для угруповання погроз по ступеню значності, проводиться їх ранжирування – величини погроз розбиваються на інтервали, і кожному

інтервалу відповідає свій ранг загрози (чим менше значення рангу, тим вище загроза).

Таблиця 4.11– Ранжирування погроз фізичного проникнення

Величина загрози	Ранг загрози
Більше 100	1
30 . 100	2
10 . 30	3
Менше 10	4

Підсумкова таблиця з моделлю способів фізичного проникнення зловмисника до джерел інформації представлена нижчим. У дужках вказані альтернативні продовження шляхів проникнення, що мають однакову складність (а відповідно, і оцінку реальності шляху).

При обчисленні величин погроз безпеці інформації, для кожного елементу інформації, що захищається, використовується найбільше з наявних значень оцінки реальності шляху (таблиця 4.10 колонка 5). Це робиться з метою визначення величини загрози на найбільш вірогідному шляху проникнення зловмисника.

Як вже було сказано, завдання побудови системи захисту інформації відноситься до класу слабоформалізованих завдань, всі величини тут, на відміну від строго математичних завдань, у будь-якому випадку мають

Приклад заповнення таблиці 4.10.

№	Найменування елементу інформації	Ціна інформації	Шлях проникнення зловмисника	Оцінка реальності шляху	Величина загрози	Ранг загрози
1	Відомості про хімічний склад зразків	1000	1) D7.1-D1.1 (D1.2, D1.3, D2, D4); 2) D7.2-D1.1 (D1.2, D1.3, D2, D4); 3) D7.3-D1.1 (D1.2, D1.3, D2, D4); 4) W1.11 (W1.12, W1.21, W1.22, W1.31, W1.32); 5) W2	0,125 0,167 0,111 0,333 0,2	330	1

№	Найменування елементу інформації	Ціна інформації	Шлях проникнення злоумисника	Оцінка реальної шкоди	Величина загрози	Ранг загрози
2	<i>Дані про назви і параметри зразків</i>	100	1) D7.1-D1.1 (D1.2, D1.3, D3, D4); 2) D7.2-D1.1 (D1.2, D1.3, D3, D4); 3) D7.3-D1.1 (D1.2, D1.3, D3, D4); 4) W1.11 (W1.12, W1.21, W1.22, W1.31, W1.32); 5) W3	0,125 0,167 0,111 0,333 0,2	33	2
3	<i>Перелік зразків, які зберігаються в приміщенні R4 в даний момент</i>	55	1) D7.1-D3 (D4); 2) D7.2-D3 (D4); 3) D7.3-D3 (D4); 4) W3	0,125 0,167 0,111 0,2	11	3
4	<i>Дані про майбутнє надходження зразків</i>	110	1) D7.1-D3; 2) D7.2-D3; 3) D7.3-D3; 4) W3	0,125 0,167 0,111 0,2	22	3
5	<i>Порядок повернення (знищення) невикористаних зразків</i>	88	1) D7.1-D3; 2) D7.2-D3; 3) D7.3-D3; 4) W3	0,125 0,167 0,111 0,2	18	3

приблизний характер. Точність їх залежить від якості експертних оцінок і ступеня інформованості про об'єкт захисту.

Моделювання технічних каналів витоку інформації

Моделювання технічних каналів витоку інформації по суті є єдиним методом достатньо повного дослідження їх можливостей з метою подальшої розробки способів і засобів захисту інформації. В основному застосовуються вербальні і математичні моделі.

Виявлення і розпізнавання каналів витоку інформації, так само як будь-яких об'єктів, проводиться по їх демаскуючих ознаках. Як достатній спільних ознак або індикаторів каналів витоку інформації можуть служити ознаки, вказані в таблиці. 2.10. Приведені індикатори є лише орієнтирами при пошуку потенційних каналів витоку. У конкретних умовах їх склад істотно більший.

Потенційні канали витоку визначаються для кожного джерела інформації, причому їх кількість може не обмежуватися одним або двома. Наприклад, від джерела інформації - керівника фірми витоку інформації можливе по наступних каналах:

- ✓ через двері в приймальню або коридор;
- ✓ через вікно на вулицю або в двір;
- ✓ через вентиляційний отвір в сусідні приміщення;
- ✓ з небезпечними сигналами по радіоканалу;
- ✓ з небезпечними сигналами по кабелях, що виходять з приміщення;
- ✓ по трубах опалювання в інші приміщення будівлі;
- ✓ через стіни, стелю і підлогу в сусідні приміщення;
- ✓ за допомогою закладних пристроїв за територію фірми.

Стосовно моделей каналів витоку інформації доцільно мати моделі, які описують канали в статичі і динаміці.

Статичний стан каналу характеризують структурна і просторова моделі. Структурна модель описує структуру (склад і зв'язки елементів) каналу витоку. Просторова модель містить опис положення каналу витоку в просторі: місця розташування джерела і приймача сигналів, віддаленість їх від кордонів території організації, орієнтація вектору розповсюдження носія інформації в каналі витоку інформації і його протяжність. Структурну модель каналу доцільно представляти в табличній формі, просторову - у вигляді графа на плані приміщення, будівлі, території організації, прилеглих зовнішніх ділянок середі. Структурна і просторова моделі не є автономними, а взаємно доповнюють один одного.

Таблиця 4.12

Вид каналу	Індикатори
Оптичний	Вікна, які виходять на вулицю, близькість до них протилежних будинків і дерев. Відсутність на вікнах завісок, штор, жалюзі. Проглядність змісту документів на столах з боку вікон, дверей, шаф в приміщенні. Проглядність змісту плакатів на стінах приміщення для наради з вікон і дверей. Мала відстань між столами співробітників в приміщенні. Проглядність екранів моніторів ПЕВМ на столах співробітників з боку вікон, дверей або інших співробітників. Складування продукції у дворі без навісів. Мала висота забору і дірки в нім. Перенесення і перевезення зразків продукції у відкритому вигляді. Поява біля території організації (підприємства) сторонніх людей (у тому числі в автомобілях) з біноклями, фотоапаратами, кіно і відеокамерами.
Радіоелектронний	Наявність в приміщенні радіоелектронних засобів, ПЕВМ, ТА міської і внутрішньої АТС, гучномовців мережі трансляції і інших предметів. Вихід вікон приміщення на вулицю, близькість до них вулиці і протилежних будинків. Застосування засобів радіозв'язку. Паралельне розміщення кабелів в одному джгуті при розводці їх усередині будівлі і на території організації. Відсутність заземлення радіо і електричних приладів. Тривале і часте паркування біля організації чужих автомобілів, особливо з людьми, які сидять в машині.
Акустичний	Мала товщина дверей і стін приміщення. Наявність в приміщенні відкритих вентиляційних отворів. Відсутність екранів на опалювальних батареях. Близькість вікон до вулиці і її будинків. Поява біля організації людей з достатньо великими сумками, довгими і товстими парасольками. Тривале і часте паркування біля організації чужих автомобілів.

<i>Вид каналу</i>	<i>Індикатори</i>
Матеріально-речовий	Відсутність закритих і опечатаних ящиків для паперу і твердих відходів з демаскуючими речовинами. Застосування радіоактивних речовин. Неконтрольований викид газів з демаскуючими речовинами, злив у водоймища і вивіз на звалище твердих відходів. Запис співробітниками конфіденційної інформації на неврахованих листах паперу.

Динаміку каналу витоку інформації описують функціональна і інформаційна моделі. Функціональна модель характеризує режими функціонування каналу, інтервали часу, протягом яких можливе витік інформації, а інформаційна містить характеристики інформації, витік якої можливий по даному каналу: кількість і цінність інформації, пропускна спроможність каналу, прогнозована якість інформації, яка приймається злоумисником.

Вказані моделі об'єднуються і ув'язуються між собою в рамках комплексної моделі каналу витоку. У ній указуються інтегральні параметри каналу витоку інформації: джерело інформації і її вигляд, джерело сигналу, середа розповсюдження і її протяжність, місце розміщення приймача сигналу, інформативність каналу і величина загрози безпеки інформації.

Кожен вид каналу містить свій набір показників джерела і приймача сигналів в каналі, що дозволяють оцінити максимальну дальність каналу і показники можливостей органів державної і комерційної розвідки.

Оскільки приймач сигналу є приналежністю злоумисника і точні місце його розташування і характеристики не відомі, то моделювання каналу проводиться стосовно гіпотетичного приймача. Як приймач доцільно розглядувати приймач, параметри якого відповідають сучасному рівню, а місце розміщення вибране раціонально. Поважне відношення до інтелекту і технічних можливостей противника гарантує від крупних помилок в значно більшому ступені, ніж зневажне.

Якщо можливе місце розміщення приймача сигналів обране, то під час моделювання каналу розраховується енергетика носія на вході приймача з урахуванням потужності носія на виході джерела, загасання

його в середі розповсюдження, рівня перешкод, характеристик сигналу і його приймача.

Наприклад, **дозволяючу спроможність при фотографуванні** людей і предметів, які знаходяться в службовому приміщенні, з відстані L легко оцінити по відомій формулі:

$$H = hL/f$$

де h - дозволяюча спроможність в долях мм системи «об'єктив-фотоплівка»

f - фокусна відстань телеоб'єктиву фотоапарата

L - відстань від об'єкту спостереження до фотоапарата.

Якщо фотографування проводиться фотоапаратом «Фотоснайпер ФС-122» з $f = 300$ мм і $h = 0,03$ мм (дозвіл 33 лин/мм), то для $L = 50$ м H дорівнює 5 мм. Враховуючи, що для виявлення і розпізнавання об'єкту його зображення повинне полягати не менше чим з 9 крапок, то мінімальні розміри об'єкту будуть складати 15х15 мм. Очевидно, що на фотографії можна буде роздивитись людину, продукцію, але не можна прочитати машинописний текст на папері або екрані монітора.

Загасання акустичної хвилі на кордоні контрольованої зони залежить від безлічі чинників, таких як конструкція приміщення, матеріал стін, тип і кількість дверей і вікон, наявність звукопоглинальних елементів і тому подібне Для орієнтовної оцінки можна використовувати дані, приведені в нижченаведених таблицях.

Значення послаблення звуку обгороджуваннями, виконаними з деяких будівельних матеріалів, які часто використовуються, вказані в табл.4.13.

Рівень акустичного сигналу за обгороджуванням можна приблизно оцінити по формулі:

$$R_{ог} \approx R_{рс} + 6 + 10 \lg S_{ог} - K_{ог} \quad (\text{дБ}),$$

де $R_{рс}$ - рівень мовного сигналу в приміщенні (перед обгороджуванням), дБ;

$S_{ог}$ - площа обгороджування, м²;

$K_{ог}$ - звукоізолююча здатність обгороджування, дБ.

При розрахунках слід мати на увазі, що рівень звуку при помірній мові складає 50...60 дБ, а гучна мова відповідає 70...80 дБ.

Ступінь послаблення електромагнітного випромінювання залежить від розмірів контрольованою зони і від наявності перешкод на шляху

розповсюдження електромагнітної хвилі. Екрануючі властивості деяких елементів будівлі приведені в табл.4.17.

Таблиця 4.13 – Звукопоглинальні властивості деяких будівельних конструкцій

Матеріал	Товщина	Звукоізоляція на частотах (Гц), дБ					
		125	250	500	1000	2000	4000
Цегельна стінка, стінка, яка виштукатурена з двох сторін	0,5 цеглини	39	40	42	48	54	60
	1 цеглина	36	41	44	51	58	64
	1,5 цеглини	41	44	48	55	61	65
	2 цеглини	45	45	52	59	65	70
	2,5 цеглини	47	55	60	67	70	70
Стіна із залізобетонних блоків	40 мм	32	36	35	38	47	53
	100мм	40	40	44	50	55	60
	200мм	42	44	51	59	65	65
	300мм	45	50	58	65	69	69
	400мм	48	55	61	68	70	70
	800мм	55	61	68	70	70	70
Стіна з шлакоблоків	220мм	42	42	48	54	60	63
Перегородка з деревинно-стружкової плити	20см	23	26	26	26	26	26

Таблиця 4.14 – Звукоізоляція вікон

Схема скління	Звукоізоляція (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Одинарне скління:						
товщина 3 мм	17	17	22	28	31	32
товщина 4 мм	18	23	26	31	32	32
товщина 6 мм	22	22	26	30.	27	25
Подвійне скління з повітряним проміжком:						
57 мм (товщина 3 мм)	15	20	32	41	49	46
90 мм (товщина 3 мм)	21	29	38	44	50	48
57 мм (товщина 4 мм)	21	31	38	46	49	35
90 мм (товщина 4 мм)	25	33	41	47	48	36

Таблиця 4.15 – Звукоізоляція звичайних дверей

Конструкція дверей	Умови застосування	Звукоізоляція (дБ) на частотах, Гц					
		125	250	500	1000	2000	4000
Двері щитова, фанера з двох сторін	без прокладки	21	23	24	24	24	23
	з прокладкою з пористої гуми	27	27	32	35	34	35
Типові двері ГТ-327	без прокладки	13	23	31	33	34	36
	з прокладкою з пористої гуми	29	30	31	33	34	41

Таблиця 4.16 – Звукоізоляція спеціальних дверей

Конструкція дверей	Звукоізоляція (дБ) на частотах, Гц					
	125	250	500	1000	2000	4000
Двері звукоізолююча полегшена	18	30	39	42	45	43
Двері звукоізолююча полегшена, подвійна із зазором більше 200 мм	25	42	55	58	60	60
Двері звукоізолююча важка	24	36	45	51	50	49
Двері звукоізолюючі важкі, подвійні із зазором більше 300 мм	34	46	60	60	65	65
Двері звукоізолюючі важкі, подвійні з облицюванням тамбура	45	58	65	70	70	70

Таблиця 4.17

Тип будівлі	Послаблення, дБ на частоті		
	100 МГц	500 МГц	1 ГГц
Дерев'яна будівля з товщиною стін 20 см	5-7	7-9	9-11
Цегельна будівля з товщиною стін 1,5 цеглини	13-15	5-17	16-19
Залізобетонна будівля з вічком арматури 15x15 см і завтовшки 160 мм	20-25	18-19	15-17

Примітка: вказані в таблиці дані отримані для стін, 30% майданів яких займають віконні отвори із звичайним склом. Якщо віконні отвори закриті металевими ґратами з коміркою 5 см, то екранування збільшується на 30-40 %. Екрануючі властивості цегельних і залізобетонних стін будівель в 2-3 рази вищі, ніж дерев'яних.

Напруженість електричного поля електромагнітної хвилі зменшується пропорційно відстані від джерела випромінювання і визначається формулою

$$E_H = \frac{\sqrt{30P_I}}{r}$$

де P_I — потужність випромінювання;

r — відстань від джерела випромінювання.

Наприклад, напруженість поля, що створюється випромінюванням радіозакладки з потужністю випромінювання 10 мВт, на відстані 500 метрів від закладки складатиме 0,001 В/м, що цілком достатньо для прийому цього сигналу будь-яким приймачем з невисокою чутливістю.

Всі виявлені потенційні канали витоку інформації і їх характеристики записуються в таблицю (наприклад, такої форми, як таблиці. 4.18).

Найменування джерела інформації запозичуються з таблиці. 4.18. У графі 4 указуються основні елементи середі розповсюдження і можливі місця розміщення приймача сигналів. По фізичній природі носія визначається вид каналу витоку інформації.

Таблиця 4.18.

№ елемента інформації	Ціна інформації	Джерело сигналу	Шлях витоку інформації	Вид каналу	Оцінки реальності каналу	Величини загрози	Ранг загрози
1	2	3	4	5	6	7	8

Оцінка показників погроз безпеці (графи 6-8) представляє достатньо складне завдання через наступні обставини:

- ✓ добування інформації нелегальними шляхами не афішується і фактично відсутні або дуже бідно представлені в літературі реальні статистичні дані по видах погроз безпеці інформації. Крім того, слід пам'ятати, що характер і частість реалізації погроз залежать від криміногенної обстановки в районі знаходження організації і дані про погрози, наприклад, в країнах з розвинутою ринковою економікою, не можуть бути однозначно використані для українських умов;

- ✓ різноманіття способів, варіантів і умов доступу до інформації, яка захищається, істотно утрудняють можливість виявлення і оцінки погроз безпеці інформації.
- ✓ канали витоку інформації можуть розповсюджуватися на достатньо великі відстані і включати як елементи середі розповсюдження труднодоступні місця;
- ✓ апіорі не відомий склад, місця розміщення і характеристики технічних засобів добування інформації зловмисника.

Оцінки погроз інформації в результаті проникнення зловмисника до джерела або її витоку по технічному каналу проводяться з урахуванням вірогідності того, що реалізовується розглянутий шлях або канал, а також ціни відповідного елементу інформації. Тому можуть бути створені два типи моделей погроз інформації: статистична і економічна.

Для розуміння статистичної моделі інформаційних погроз розглянемо деяку умовну зону інформаційного захисту. Припустимо, що мова йде про захисті конфіденційних розмов в деякому службовому приміщенні. Для конкретного приміщення завжди можна скласти достатньо повний перелік погроз і їх сценаріїв. Всі погрози будуть пронумеровані і матимуть описову частку. Як найповнішою статистичною характеристикою кожною з погроз є вірогідність $P(T)$ її реалізації за деякий заданий час T або пов'язана з нею величина p щільності вірогідності загрози в одиницю часу¹. Статистична модель передбачає складання таблиць, де для кожної з погроз разом з описовою її часткою указується її вірогідність (графа 6 таблиць. 4.18).

Наведемо приклад.

Якісний опис: загроза S_p - віброакустичний контроль приміщення із сторони сусідніх приміщень (застосування стетоскопів).

Статистичний опис: вірогідність загрози $P(T) = 0,1\%$ за час $T = 5$ років або щільність вірогідності

$$p = P(T) / T = 0,02\% \text{ в рік.}$$

На жаль, практично цей шлях нереальний. Річ у тому, що величини P_K як правило, не відомі навіть для класів підприємств, не говорячи вже

¹ При пуассоновских процессах вірогідність $P(T)$ реалізації загрози за час T пов'язана з щільністю вірогідності загрози в часі співвідношенням вигляду: $P(T) = 1 - \exp(-pT)$.

про конкретну комерційну установу. Ці величини залежать від регіону, криміногенності обстановки, виду бізнесу і багатьох інших причин.

Відсутність точних величин вірогідності P_K інформаційних погроз принципово обмежує можливість використання методів статистичних рішень, теорія яких добре розвинена для різних прикладних завдань.

Проте рекомендовані теорією правила вибирання засобів і методів інформаційного захисту не завжди вимагають знань абсолютних величин $\{P\}$. Ці правила передбачають порівняння між собою так званих рангових коефіцієнтів, пропорційних вірогідності P_K . Формально це означає, що замість величин P_K можна використовувати будь-які інші характеристики, пропорційні P_K .

Конструктивно в цьому відношенні є економічна модель інформаційних погроз. У основу моделі закладена ідея про те, що всі погрози мають бути зрештою економічно виправдані. Дійсно, реалізація будь-якої інформаційної загрози зв'язана з певними витратами: витрачаються засоби на вивчення обстановки, розробку плану і технології загрози, придбання устаткування і необхідних спеціальних технічних засобів, є витрати і на етапі реалізації загрози. Джерело загрози сподівається на те, що всі ці витрати окупляться тими конфіденційними відомостями, які воно отримає. Мірою такого зіставлення є величина відношення

$$Z/b(s)$$

де Z – еквівалентна вартість отриманих відомостей

а $b(s)$ – сукупні витрати по організації і на реалізацію загрози (враховуємо для простоти тільки вартість спеціальних технічних засобів).

Чим більше величина $Z/b(s)$, тим більше вірогідність загрози². У першому наближенні щільність вірогідності загрози пропорційна величині

$$\alpha = Z/b(s),$$

званою в подальшому *коефіцієнтом небезпеки загрози*.

² Строго кажучи, своє рішення джерело погроз формує на підставі величини $(1 - Q) Z/b(s)$

де Q – ефективність захисту, що здається йому (або відома), від даного виду загрози (напрями).

Таким чином, загроза завжди діє із слабозахищеного (Q мало) або незахищеним зовсім ($Q = 0$) напрямом.

Використовуючи економічну модель погроз, можна зробити наступні спільні висновки:

- ✓ чим більше інформаційна значущість зони Z_3 , тим більше вірогідність загрози за інших рівних умов;
- ✓ чим менше витрати на реалізацію загрози (маловитратні погрози), тим більше за вірогідність загрозу;
- ✓ високопрофесійні (витратні) погрози реальні (вірогідні) тільки для зон захисту з великою значущістю.

Проілюструємо пропоновану методику кількісного оцінювання інформаційних погроз на конкретному прикладі. Розглянемо акустичні погрози відносно деякого умовного приміщення.

Складемо повний перелік можливих каналів витоку мовної інформації (характеристики каналу зв'язку не враховуємо). Допустимо, що перелік включає 15 видів інформаційних погроз, зведених в табл.4.19.

Для кожної з погроз експертно визначаємо основні характеристики каналу витоку інформації, у тому числі:

- тривалість T роботи (за рік);
- q середньоспектральне відношення потужності сигналу до потужності перешкоди (відношення сигнал/перешкода);
- смугу частот ΔF ;
- витрати в $b(s)$ на реалізацію загрози (враховуємо для спрощення тільки вартість спеціальних технічних засобів).

Ці дані представлені в табл.4.19.

Для кожної з погроз розраховуємо коефіцієнт небезпеки погроз α :

$$\alpha = \frac{\bar{Z}V_{\Pi}}{b(s)} = \bar{Z} \frac{\Delta F \log_2(1+q)}{b(s)}$$

де $\bar{Z}$ – вартість біта інформації (приймається рівною 1, оскільки всі погрози порівнюються між собою);

V_{Π} – об'єм «викраденої» інформації (при реалізації загрози);

ΔF – смуга пропускання каналу;

q – середньоспектральне відношення потужності сигналу до потужності перешкоди (відношення сигнал/перешкода).

Результати розрахунків відображуються в тій же таблиці.

Таблиця 4.19

Код загрози	Вид загрози	ΔF (кГц)	T (год ин)	q (ДБ)	V_I (Мб)	$b(s)$ (y.e.)	α $\frac{Mб}{y.e.}$
1	2	3	4	5	6	7	8
Sp1	Автономне радіозакладання, що вноситься або заздалегідь встановлена, у тому числі з дистанційним управлінням ДУ	3,5	200	40	$4,35 \times 10^3$	1000	4,35
Sp2	Довготривале радіозакладання з мережевим живленням, у тому числі з ДУ	3,5	3000	40	$6,3 \times 10^4$	500	126
Sp3	Використання природних звуководів	3,5	3000	30	$4,7 \times 10^4$	300	157
Sp4	Контроль стін (стетоскопи)	3,5	3000	10	$1,57 \times 10^4$	1000	15,7
Sp5	Контроль труб (стетоскопи)	2,0	1500	10	$4,5 \times 10^3$	1000	4,5
Sp6	Використання диктофонів, які вносяться	3,5	50	40	$1,05 \times 10^3$	1500	0,7
Sp7	Направлені мікрофони	2,0	200	10	6×10^2	2000	0,3
Sp8	Мімічний канал	3,5	1500	30	$2,36 \times 10^4$	6000	3,94
Sp9	Лазерний контроль шибок	2,5	1500	20	$1,1 \times 10^4$	100 000	0,11
Sp10	Пасивні оптичні закладки-відбивачі	3,5	1500	30	$2,35 \times 10^4$	50 000	0,47
Sp11	Дротяні (телефонні) закладання	3,5	3000	20	$3,14 \times 10^4$	200	157
Sp12	Дротяні (пасивні) закладання, пристрої складних модифікацій	3,5	2000	20	$2,1 \times 10^4$	400	52,3

Код загрози	Вид загрози	ΔF (кГц)	T (год ин)	q (ДБ)	V_I (Мб)	$b(s)$ (y.e.)	α $\frac{Mб}{y.e.}$
1	2	3	4	5	6	7	8
Sp13	Мережеві дротяні закладання	3,5	3000	40	$6,3 \times 10^4$	400	157
Sp14	Спеціальні дротяні системи	3,5	3000	40	$6,3 \times 10^4$	5000	12,6
Sp15	Активні системи підвищеної енергетичної скритності	3,5	3000	40	$6,3 \times 10^4$	30 000	2,1

Таблиця 4.20.

Код погроз	Найменування загрози	T (год ина)	m (шт)	V_{FDD} (Мб)	$l \times m$	F_k (Гц)	q (ДБ)	V_{II} (Мб)	$b(s)$ (y.e.)	α $\frac{Mб}{y.e.}$
S1	Перехоплення побічних випромінювань від ЕОМ	3000						10^6	40000	0,02
S2	Застосування закладних пристроїв в ЕОМ	3000						10^6	20000	0,05
S3	Програмні розкрадання з банку даних ЕОМ	3000						10^6	10000	0,10
S4	Копіювання інформації з магнітних носіїв	3000	50	1,44				72	1000	0.07
S5	Зовнішній (через вікна) відеоконтроль з документування	200			250×250	25	10	$4,7 \times 10^6$	10000	47

Код погро- оз	Найменування загрози	T (год ина)	m (шт)	V_{FDD} (Мб)	$l \times m$	F_k (Гц)	q (ДБ)	V_{II} (Мб)	$b(s)$ (y.e.)	α $\frac{Mб}{y.e.}$
	<i>m</i>									
S6	<i>Спеціальний відеоконтроль через малі отвори в конструкціях, які захищають</i>	1000			250×250	25	40	$7,0 \times 10^6$	40000	175
S7	<i>Використання тих, що вносяться, короткочасної дії відеоконтрольних пристроїв або мікрофотокамер</i>	100			250×250	25	40	$2,6 \times 10^6$	1000	0,26

Аналогічним чином формується (для даного приміщення) спектр сигнальних погроз. Початкові дані для нього відбиті в таблиці 4.20.

Коефіцієнти небезпеки погроз сигнальній інформації оцінюються по формулі:

$$\alpha = \frac{\bar{Z}V_{II}}{b(s)},$$

де V_{II} - спільний об'єм викраденої інформації по каналу її витоку за час аналізу T (прийнято, що $T=1$ рік);

$b(s)$ - вартість реалізації загрози;

$\bar{Z}$ - середня вартість інформації (прийнята при розрахунках рівної 1).

Введена у формулу величина V_{II} об'єму інформації може прийматися рівною:

$V_{II}=V_{HDD}=106 \text{ Мб}$ - для варіантів розкрадання інформації з жорсткого диска EOM, або

$V_{\Pi} = m V_{FDD}$, - для варіантів копіювання дискет (документів)

де m - число дискет

а $V_{FDD} = 1,44$ Мб - ємкість дискети;

$V_{\Pi} = (l \times m) F_K \log_2(1 + q) T$ - для варіантів відеоконтролю

де $l \times m$ - число елементів (число pixel) дозволу в полі зображення;

F_K - частота кадрів;

q - середньоспектральне відношення потужності сигналу до потужності перешкоди (відношення сигнал/перешкода).;

$T_{ш}$ - час штатної роботи (хороша видимість і ін.).

Слід підкреслити, що всі початкові дані є умовними, хоча і відображають в першому наближенні реальні можливості погроз і їх економічну основу. Основна мета прикладів - проілюструвати методику формування спектрів погроз.

На підставі отриманих даних можна заповнити графи 7 і 8 таблиць. 4.18.

Контрольна робота № 3

При виконанні третьої роботи необхідно провести розробку організаційних і технічних мерів по захисту інформації для об'єкту який розглядався в контрольних роботах №1 і 2.

Заходи по захисту інформації доцільно розподілити на 2 групи: організаційні і технічні. При такій класифікації до технічних відносяться заходи, що реалізуються шляхом установки нових або модернізації використовуваних інженерних і технічних засобів захисту інформації. Основу організаційних заходів інженерно-технічного захисту інформації складають заходи, які визначають порядок використання цих засобів.

Організаційні заходи інженерно-технічного захисту інформації включають, перш за все, заходи щодо ефективного використання технічних засобів, регламентації і управління доступом до інформації, що захищається, а також по порядку і режимам роботи технічних засобів захисту інформації. Організаційні заходи інженерно-технічного захисту інформації є частиною її організаційного захисту, основу якої складають регламентація і управління доступом.

Регламентація - це встановлення часових, територіальних і режимних обмежень в діяльності співробітників організації і роботі технічних засобів, направлені на забезпечення безпеки інформації.

Регламентация передбачає:

- ✓ встановлення кордонів контрольованих зон, які охороняються;
- ✓ визначення рівнів захисту інформації в зонах;
- ✓ регламентация діяльності співробітників і відвідувачів (розробка розпорядку дня, правил поведінки співробітників в організації і поза нею і т. д.);
- ✓ визначення режимів роботи технічних засобів, у тому числі збору, обробки і зберігання інформації, що захищається, на ПЕВМ, передачі документів, порядку складування продукції і так далі

Управління доступом до інформації включає наступні заходи:

- ідентифікацію осіб і звернень;
- перевірку повноважень осіб і звернень;
- реєстрацію звернень до інформації, що захищається;
- реагування на звернення до інформації.

Ідентифікація користувачів, співробітників, відвідувачів, звернень по каналах телекомунікацій проводиться з метою їх надійного впізнання.

Перевірка повноважень полягає у визначенні прав осіб і звернень по каналах зв'язку на доступ до інформації, що захищається. Для доступу до інформації рівень повноважень звернення не може бути нижче дозволеного. З метою забезпечення контролю над проходженням носіїв із закритою інформацією проводиться реєстрація (протоколювання) звернень до них шляхом запису в картках, журналах, на магнітних носіях.

Реагування на будь-яке звернення до інформації полягає або в дозволі доступу до інформації, або у відмові. Відмова може супроводитися включенням сигналізації, сповіщенням служби безпеки або правоохоронних органів, затриманням зловмисника при його спробі несанкціонованого доступу до інформації, яка захищається.

Технічні заходи передбачають застосування способів і засобів, що перешкоджають просочуванню інформації за межі контрольованої зони. Очевидно, що вибирання інженерно-технічних засобів захисту представляє непросте завдання, оскільки від нього залежить, з одного боку, надійність захисту, а з іншої - ціна, яку необхідно заплатити, щоб цей захист забезпечити.

Таким чином, вибиранням інженерно-технічних засобів локального захисту інформації завжди є процес зіставлення вимог і можливостей.

Можливості інженерно-технічних засобів захисту інформації визначаються їх тактико-технічними характеристиками (рівнями послаблення сигналів, рівнями створених перешкод, рівнями екранування і т.і.). Вимоги повинні зважати на специфіку зон захисту, ступінь важливості інформації, допустимий ризик (допустимі втрати) і ін.

5 РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Для повного і якісного вивчення дисципліни і виконання контрольних робіт рекомендується наступна література:

5.1 Основна

1. Бурячок В.Л. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. [Текст] / В.Л. Бурячок, С.В. Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. – К.:ДУТ, 2015. – 345 с.
2. Іванченко С.О. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник [Текст]/ С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗІ НТУУ «КПІ», 2016. – 104 с.
3. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект. Підручник. [Текст] / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. За заг. ред. докт. техн. наук, проф. В.Б. Толубко. – К.: ДУТ, 2015. – 288 с.
4. Вишня В.Б. Основи інформаційної безпеки: навч. посібник [Текст] / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.
5. Остапов С.Е. Технології захисту інформації: навчальний посібник [Текст] / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
6. Жилін А.В. Технології захисту інформації в інформаційно-телекомунікаційних системах: навч. посіб. [Текст] / А.В. Жилін, О.М. Шаповал, О.А. Успенський; ІСЗІ КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.

7. Остапов С.Е. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. [Текст] / С.Е. Остапов, С.П. Євсєєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

5.2 Перелік посібників і методичних вказівок

1. Методичні вказівки до виконання лабораторних робіт з дисципліни "Методи і засоби захисту інформації" для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» всіх форм навчання. Частина 1 / Укл. І.М. Сметанін – Запоріжжя: НУ «Запорізька політехніка», 2024. – 79 с.
2. Методичні вказівки до виконання лабораторних робіт з дисципліни "Методи і засоби захисту інформації" для студентів спеціальності 172 «Електронні комунікації та радіотехніка», які навчаються за освітньою програмою «Радіотехніка» всіх форм навчання. Частина 2 / Укл. І.М. Сметанін – Запоріжжя: НУ «Запорізька політехніка», 2024. – 66 с.

5.3 Рекомендовані інформаційні джерела:

- Система дистанційного навчання НУ «Запорізька політехніка» (Система Moodle) <https://moodle.zp.edu.ua/>;
- Електронний Інституційний репозиторій НУ «Запорізька політехніка» <http://eir.zp.edu.ua/>;
- Інформаційні електронні ресурси наукової бібліотеки НУ «Запорізька політехніка» <http://library.zp.edu.ua/>.

[illegible]



Додаток 3 – Приклад виконання загального плану приміщень

Додаток 3 (Варіант)

План офісу ТОВ "Акдарель"

№	Назва	Площа	Вартість
1	Офіс	100	100
2	Ліфт	10	10
3	Ліфт	10	10
4	Ліфт	10	10
5	Ліфт	10	10
6	Ліфт	10	10
7	Ліфт	10	10
8	Ліфт	10	10
9	Ліфт	10	10
10	Ліфт	10	10
11	Ліфт	10	10
12	Ліфт	10	10
13	Ліфт	10	10
14	Ліфт	10	10
15	Ліфт	10	10

Додаток 4 – Приклад виконання структурної схеми шляхів фізичного проникнення

