НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет електроніки
Кафедра акустичних та мультимедійних електронних систем

До захисту допущено:
Завідувач кафедри
_____ Сергій Найда
«_14__»____06_____2023 р.

Дипломна робота

на здобуття ступеня бакалавра
за освітньо-професійною програмою «Електронні системи мультимедіа та засоби Інтернету речей» спеціальності (спеціалізації) 171 Електроніка
на тему: **Методи та технічні засоби контролю інформаційної безпеки аудіовізуальних мереж передавання контенту**

Виконав:
студент 4 курсу, групи ДВ-91
Мошинський Дмитро Олексійович

Керівник:
Проф., д.т.н., проф., Розорінов Г.М

Рецензент: д.т.н.,доцент кафедри МЕ Татарчук Д.Д.

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент Мошинський Д.О.

Київ – 2023

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет електроніки
Кафедра акустичних та мультимедійних електронних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 171 «Електроніка»

Освітньо-професійна програма «Електронні системи мультимедіа та засоби Інтернету речей»

ЗАТВЕРДЖУЮ
Завідувач кафедри
 Сергій Найда
«_30»_____05_____2023 р.

ЗАВДАННЯ

на дипломну роботу студенту
Мошинському Дмитру Олексійовичу

1. Тема роботи «Методи та технічні засоби контролю інформаційної безпеки аудіовізуальних мереж передавання контенту», керівник роботи Розорінов Г.М, професор, доктор технічних наук, затверджена наказом по університету від « 30 » травня 2023 р. № 2063-с.

2. Термін подання студентом роботи 12 червня 2023 р.

3. Вихідні дані до роботи: Визначення мереж передавання аудіовізуального контенту загального призначення.

Основні методи аналізу ризику (повний, базовий, комбінований, експертний).

Базовий аналіз ризику BS 7799 (ISO 17799) і правила його проведення.

4. Зміст роботи: 1). Особливості побудови аудіовізуальних систем для захисту конфіденційної інформації. 2). Роль і місце аналізу ризику при

побудові систем передавання аудіовізуального контенту. 3) Покращення методів аналізу ризику.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): набір слайдів презентації з узагальнюючими матеріалами.

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання: 17 квітня 2023 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Виконання першого розділу роботи	22.04.2023	Виконано
2	Виконання другого розділу роботи	16.05.2023	Виконано
3	Виконання третього розділу роботи	05.06.2023	Виконано
4	Оформлення пояснювальної записки	10.06.2022	Виконано
5	Підготовка презентації і доповіді до захисту	12.06.2022	Виконано

Студент  Д.О. Мошинський

(підпис) (ініціали, прізвище)

Керівник роботи  Г.М. Розорінов

(підпис) (ініціали, прізвище)

УДК 004.621.3

РЕФЕРАТ

Дипломна робота: 70 с., 6 рис., 13 джерел.

Ключові слова: аналіз ризиків, інструментарій, інформаційна безпека, система передавання аудіовізуальної інформації, сертифікація.

Бакалаврська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатку і має 59 сторінок основного тексту, 6 рисунків, 11 таблиць, 2 сторінок додатку. Загальний обсяг роботи 70 сторінок.

Метою роботи є розробка рекомендацій щодо аналізу та управління ризиками інформаційно-комунікаційних систем.

У роботі проведене дослідження існуючих методів аналізу ризиків як складової частини політики безпеки аудіовізуальної мережі; дослідження методів та засобів аналізу ризику при побудові комплексних систем захисту інформації в мережі передавання аудіовізуального контенту.

У роботі розроблено методичні рекомендації щодо вибору та застосування формалізованих методів аналізу ризиків для конкретної мережі.

Запропоновані підходи можуть бути використані при розробці, впровадженні та експлуатації комплексної системи захисту інформації на підприємствах та організаціях різних форм власності.

Можливі напрямки розвитку цієї роботи пов’язані з виконанням досліджень щодо удосконалення методів аналізу та управління ризиками на основі розробки спеціальних алгоритмів та програм.

ABSTRACT

Thesis: 70 pages, 6 pictures, 13 sources.

Keywords: analysis of risks, tool, informative safety, system of transmitt ed of audiovisual information, certification.

Bachelor attestation work consists of entry, three divisions, general concl usions, list of the used sources, to addition and it is had 59 pages of basic text, 6 pictures, 11 tables, 2 pages to addition. General volume of work 70 pages.

The aim of work is development of recommendations in relation to an analysis and management the risks of the of informatively-communication systems. In-process undertaken a study of existent methods of analysis of risks as component part of politics of safety of audiovisual network; research of methods and facilities of analysis of risk is at the construction of the complex systems of priv in the network of transferrableness of audiovisual content.

Methodical recommendations are in-process worked out in relation to a choice and application of the formalized methods of analysis of risks for a concrete network.

Offered approach can be used for development, introduction and exploitation of the complex system of priv on enterprises and organizations of different patterns of ownership.

Possible directions of development of this work are related to implementation of researches in relation to the improvement of methods of analysis and management risks on the basis of development of the special algorithms and programs.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

АС – автоматизована система;

BS – британський стандарт;

Д – доступність;

ДСК - для службового користування;

ЕОМ – електронно-обчислювальна мережа;

ЕС – експертна система;

ЗЗ – засіб захисту;

ІБ – інформаційна безпека;

ІС – інформаційна система;

К – конфіденційність;

КЗЗ – комплекс засобів захисту;

КСЗІ – комплексна система захисту інформації;

ЛОМ – локальна обчислювальна мережа;

МЕ – міжмережевий екран;

НД ТЗІ – нормативний документ з технічного захисту інформації;

НД – набір даних;

НСД – несанкціонований доступ;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ТД – тнхнічна документація;

ТЗІ – технічний захист інформації;

Ц – цілісність.

ВСТУП

В даний час технології аналізу ризиків мереж передавання аудіовізуального контенту розвинуті слабо. Основна причина такого положення полягає в тому, що цей аналіз, як правило, виконується формально, з використанням власних методик невідомої якості.

У деяких розвинутих країнах це не так. Питанням аналізу ризиків приділяється особлива увага: десятиліттями збирається статистика, удосконалюються методики. Приміром, в американському словнику по безпеці можна знайти термін: Designated Approving Authority – особа, уповноважена прийняти рішення про допустимість визначеного рівня ризиків.

Серед вітчизняних фахівців служб ІБ зріє розуміння необхідності проведення такої роботи. У першу чергу це відноситься до банків, великим комерційним структурам, тобто до тих, хто в першу чергу зобов'язаний серйозно піклуватися про безпеку своїх інформаційних ресурсів. Будь-яка організація повинні мати можливість забезпечувати наступні три основні властивості інформації: **К, Ц, Д.**

Внаслідок цього приходиться адаптувати до наших умов і застосовувати методики міжнародних стандартів (ISO 9001, ISO 17799, ISO 15408, BSI і ін.), а також використовувати методи кількісного аналізу ризиків та ін.

Сьогодні сучасні методики роботи з аналізу ризиків ІБ, проектуванню і супроводу систем безпеки повинні дозволяти:

- зробити кількісну оцінку поточного рівня безпеки, задати припустимі рівні ризиків, розробити план ТЗІ з використанням сучасних методик і засобів;
- розрахувати й економічно обґрунтувати перед керівництвом розмір фінансових витрат на ІБ на основі технологій аналізу ризиків, співвіднести витрати на забезпечення безпеки з потенційним збитком і

ймовірністю його виникнення;

- виявити і провести першочергове блокування найбільш небезпечних вразливостей до здійснення атак на вразливі ресурси;
- визначити функціональні відносини і зони відповідальності при взаємодії підрозділів і осіб по забезпеченню ІБ підприємства, створити необхідний пакет організаційно-розпорядницької документації;
- розробити і погодити зі службами організації, проект впровадження необхідних комплексів ЗЗ у, що враховує сучасний рівень і тенденції розвитку ІТ;
- забезпечити підтримку впровадженого комплексу ЗЗ відповідно до умов роботи, що змінюються.

У зв'язку з цим можна зробити висновок, що тема бакалаврської роботи, присвячена розгляду різних методик оцінки ризиків в мережах передавання аудіовізуальної інформації, їх недолікам і перевагам, спробі оцінити ці методики при їх впровадженні в різних мережах,
є **актуальної задачею**.

Мета даної бакалаврської роботи – розробка рекомендацій щодо аналізу та управління ризиками мереж передавання аудіовізуального контенту.

Для досягнення поставленої мети в роботі виконуються:

- дослідження існуючих методів аналізу ризиків;
- дослідження методів та засобів аналізу ризику при побудові комплексних систем захисту інформації різних класів;
- розробка рекомендації щодо вибору та застосування формалізованих методів аналізу ризиків для конкретної системи.

Галузь застосування. Матеріали роботи можуть бути використані при планування та проведенні аудиту безпеки мереж передавання аудіовізуального контенту.

1 МЕТОДИ ТА РОЛЬ АНАЛІЗУ РИЗИКУ ПРИ ПОБУДОВІ КСЗІ МЕРЕЖ ПЕРЕДАВАННЯ АУДІОВІЗУАЛЬНОГО КОНТЕНТУ

1.1 Особливості побудови системи захисту інформації мереж другого і третього класу загального призначення

Виділяють **три ієрархічні класи систем**, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

Клас «1» — одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;
- технічні засоби (носії інформації) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження інформації.

Приклад — автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності.

Приклад — ЛОМ.

Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Приклад — глобальна мережа.

Що стосується захисту інформації необхідно пам'ятати, що найбільш захищеним вважається відокремлений комп'ютер, тобто система 1 класу. Тому у даній бакалаврській роботі більш детально буде розглянуто системи 2 и 3 класу, бо в них найважче всього забезпечити основні властивості інформації – конфіденційність, цілісність, доступність (К, Ц, Д) [1].

1.2 Особливості побудови систем для захисту конфіденційної інформації [1, 2]

З точки зору безпеки інформація характеризується трьома властивостями:

- **конфіденційність** – інформація повинна бути доступна тільки тим, хто має право доступу до неї;
- **цілісність** – інформація повинна бути не зміненою, чіткою і не застарілою;
- **доступність** – можливість одержати доступ до інформації в будь-який час.

Хоча жодна мережа не може бути захищена *цілком,* завжди треба мати можливість вчасно зреагувати на порушення безпеки системи, і відновити правильне її функціонування в оптимальний (найкоротший) період часу [1].

Розглянемо деякі особливості побудови систем другого і третього класу в залежності від того, яка інформація там циркулює. Якщо в системі циркулює конфіденційна інформація, то ціль захисту цієї інформації, а також методи і засоби її збереження одні, а якщо інформація для службового користування – то інші.

Конфіденційну інформацію визначає власник, а інформацію для службового користування – держава [1].

Для конфіденційної інформації основними цілями можуть бути визначення ймовірності збитку, кількості витрат на створення КЗЗ. Реальне оцінювання виробляється в кількісному еквіваленті, наприклад у грошовому.

Інформація з грифом ДСК визначається державою і передбачає захист від витоку і модифікації за будь-яку ціну. Не дотримання режиму ІБ припускає відповідальність кримінального характеру, наприклад штраф чи позбавлення волі на певний строк [1].

У Кримінальному кодексі України (від 2003р.) в розділі XVI наведено кілька статей стосовно комп'ютерної безпеки, а саме злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ці статті наведені у **Додатку** в кінці роботи.

1.3 Типовий алгоритм побудови КСЗІ для інформаційної мережі

Типовий алгоритм побудови КСЗІ для інформаційної мережі можна представити в наступному виді [2, 3]:

I. Дослідження інформаційної мережі.

– функціональні задачі мережі;
– архітектура побудови мережі;
– типові технології обробки інформації в мережі;
– програмно-апаратні засоби, що використовуються в мережі;
– персонал, що обслуговує мережу і його функціональні обов'язки.

Результатом є модель інформаційної мережі (математична, формалізована, описова), кількісні і/чи якісні характеристики і показники ефективності її функціонування.

II. Побудова моделі цінності інформаційної мережі.

III. Побудова моделі вразливостей інформаційної мережі.

IV. Розробка моделі порушника інформаційної мережі. При цьому використовуються такі ознаки класифікації порушника:

– бюджетні ресурси (компанії, спецслужби індустріально розвинутих держав, чи кількісна оцінка);
– Тимчасові можливості (обмежені, необмежені);
– Рівень доступу до мережі (зовнішній, локальні користувачі різних рівнів доступу, адміністратори, розроблювачі і супроводжуючі);
– кваліфікація (зв'язана з бюджетом);

V. Розробка моделі загроз.

VI. Аналіз ризику в інформаційній мережі.

VII. На підставі отриманих даних у п. I-VI – розробка політики безпеки – формулювання поняття безпечного стану системи, цілей безпеки, загальних методів їх досягнення (загальна політика), детальної політики (до технічних засобів).

VIII. Розробка стратегії безпеки чи плану захисту (деталізація політики безпеки). Розмежування області дій організаційно-правових, інженерно-технічних і технічних (включаючи криптографічні) методів захисту.

Примітка: технічні методи захисту реалізуються комплексом засобів захисту (КЗЗ).

IX. Вибір функцій, реалізованих КЗЗ (служб захисту в термінах стандарту ISO 7498-2), формування профілю захисту.

X. Вибір механізмів реалізації функцій КЗЗ.

XI. Вибір і/чи розробка і/чи настроювання конкретних засобів, що реалізують механізми захисту.

XII. Розробка адміністративно-правових (організаційних) мір і інженерно-технічних методів захисту.

XIII. Розробка ТЗ на створення КСЗІ інформаційної мережі.

XIV. Оцінка рівня захищеності КСЗІ інформаційної мережі.

– функціональний, якісний, формалізований – критерії оцінки захищеності інформаційної мережі;
– кількісний і/чи якісний аудит і аналіз ризику.

XV. Атестація КСЗІ інформаційної мережі і одержання дозволу на експлуатацію.

1.4 Роль і місце аналізу ризику при побудові КСЗІ

Етап аналізу ризиків тісно зв'язаний з етапом аналізу вразливостей. Для того, щоб зрозуміти яке важливе місце етап аналізу ризиків займає в системі звернемося до понять і визначень [2, 3]:

Загроза (Threat) - сукупність умов і факторів, що можуть стати причиною порушень цілісності, доступності, конфіденційності інформації.

Вразливість (Vulnerability) - слабкість у системі захисту, що уможливлює реалізацію загрози.

Аналіз ризиків - процес визначення загроз, вразливостей, можливого збитку, а також контрзаходів.

Аналіз ризиків може бути **базовим**, а може бути і **повним**. Все залежить від системи і вимог пред’явлених до неї.

Базовий аналіз ризиків - аналіз ризиків, проведений відповідно до вимог базового рівня захищеності. Методи даного класу застосовуються у випадках, коли до інформаційної системи не пред'являється підвищених вимог в області ІБ.

Повний (Full) аналіз ризиків - пред'являють до системи з підвищеними вимогами в області ІБ (більш високі, чим базовий рівень захищеності). Містить у собі визначення цінності інформаційних ресурсів, оцінку загроз і вразливостей, вибір адекватних контрзаходів, оцінку їхньої ефективності.

Оцінка ризиків (Risk Assessment) - ідентифікація ризиків, вибір параметрів для їхнього опису й одержання оцінок по цих параметрах.

Керування ризиками (Risk Management) - процес визначення контрзаходів відповідно до оцінки ризиків.

Відповідно до приведених визначень і за допомогою документа «Common Criteria for Information Technology Security Evolution» (Part 1) – «Загальні критерії захисту інформаційних технологій» (частина 1), можна зобразити структурну схему взаємодії загроз, вразливостей, ризиків, а також застосованих контрзаходів для їх ліквідації в наступному вигляді (рис.1). Із схеми видно, що визначення ризиків займає не останнє місце в системі ІБ [2, 3].

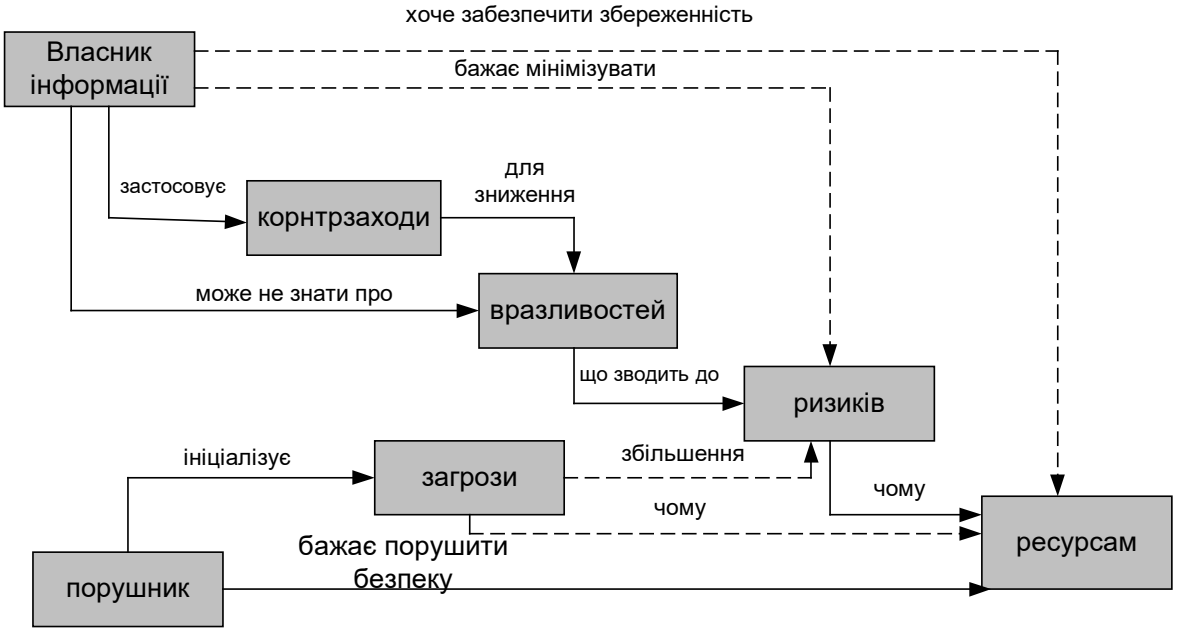

Рисунок 1– Місце ризику в інформаційній системі [2]

Задачу аналізу і керування інформаційними ризиками можна вирішити наступним чином (рис. 2).

При описі ІС значну увагу приділяють визначенню цілей і задач створення ІС у відповідність вимогам міжнародних, вітчизняних і корпоративних стандартів в області ЗІ. Визначаються границі ІС, а також

склад і структура найбільш значимих компонентів і зв'язків по керуванню і по даним. Опис можна проводити в наступному порядку [2, 3]:

- основні цілі і задачі ІБ;
- функціональні вимоги до ІС;
- критичні інформаційні ресурси, процеси і сервіси мережі;
- вхідні і вихідні потоки даних;
- топологія локальної мережі;
- склад використаємих апаратних засобів, їхня конфігурація;
- використовувані типи і формати даних;
- використовуване системне і прикладне ПЗ;
- обов'язки співробітників ІС;
- категорії користувачів системи й обслуговуючого персоналу;
- архітектура підсистеми ІБ;
- перелік програмно-технічних засобів забезпечення ІБ;
- формальні вимоги в області ІБ (законодавство, відомчі стандарти, і ін.);
- система керування в даної ІС (посадові інструкції, система планування в області забезпечення ІБ);
- існуюча система керування в області ІБ (резервне копіювання, процедури реагування на позаштатні ситуації, інструкції в області ІБ, контроль за підтримкою режиму ІБ і ін.);
- організація фізичної безпеки;
- керування безперервністю роботи ІС (контроль за зовнішнім стосовно ІС середовищем, наприклад кліматичними параметрами, електроживленням, захистом від затоплень, і ін.) [3].

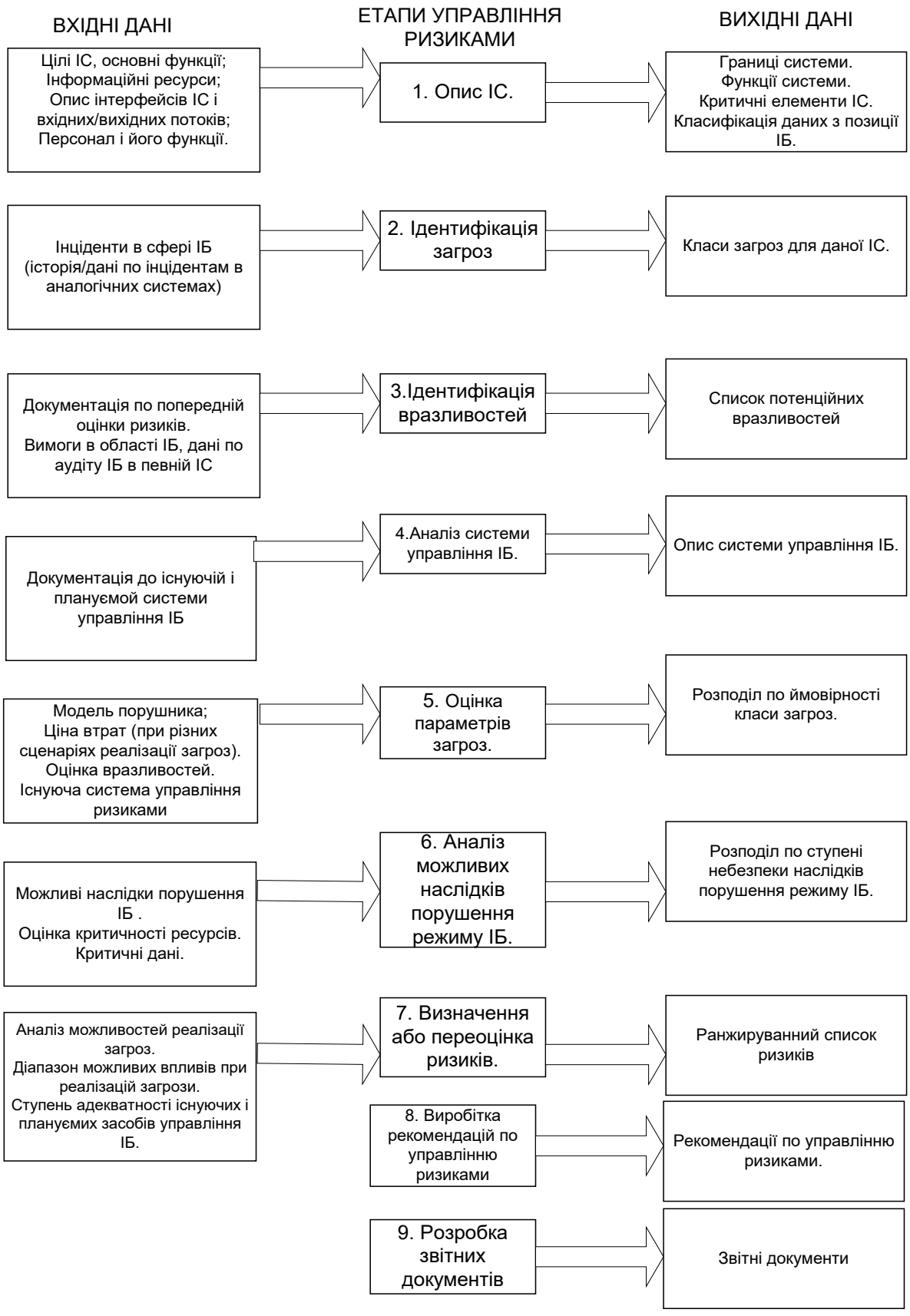

Рисунок 2 – Можлива технологія керування ризиками [3]

Таким чином, різноманітність загроз та дій порушника визначають всю множину можливих методів, механізмів та засобів захисту, а аналіз ризику визначає які саме методи треба вибрати в залежності від цінності ресурсів системи та витрат на систему захисту.

При опису мережі значну увагу приділяють визначенню цілей і задач створення мережі у відповідність вимогам міжнародних, вітчизняних і корпоративних стандартів в області ЗІ. Визначаються границі мережі, а також склад і структура найбільш значимих компонентів і зв'язків по керуванню і по даним. Опис можна проводити в наступному порядку [2, 3]:

- основні цілі і задачі ІБ для мережі;
- функціональні вимоги до ІС;
- критичні інформаційні ресурси, процеси і сервіси мережі;
- вхідні і вихідні потоки даних;
- склад використовуваних апаратних засобів, їхня конфігурація;
- топологія локальної мережі;
- використовуване системне і прикладне ПЗ;
- використовувані типи і формати даних;
- обов'язки співробітників ІС;
- категорії користувачів системи й обслуговуючого персоналу;
- формальні вимоги в області ІБ (законодавство, відомчі стандарти, і ін.);
- перелік програмно-технічних засобів забезпечення ІБ;
- архітектура підсистеми ІБ;
- система керування в даної ІС (посадові інструкції, система планування в області забезпечення ІБ);
- існуюча система керування в області ІБ (резервне копіювання, процедури реагування на позаштатні ситуації, інструкції в області ІБ, контроль за підтримкою режиму ІБ і ін.);

- організація фізичної безпеки;
- керування безперервністю роботи ІС (контроль за зовнішньою стосовно ІС середовищем, наприклад кліматичними параметрами, електроживленням, захистом від затоплень, і ін.) [2].

Таким чином, можна сказати, що різноманітність загроз та дій порушника визначають всю множину можливих методів, механізмів та засобів захисту, а аналіз ризику визначає які саме методи треба вибрати в залежності від цінності ресурсів системи та витрат на систему захисту.

1.5. Висновки за 1 розділом.

1. Розглянуті особливості побудови системи захисту інформації мереж другого і третього класу загального призначення.

2. Вказане місце ризику в інформаційній системі.

3. Проаналізовані можливі технології керування ризиками.

2 ІСНУЮЧІ МЕТОДИ АНАЛІЗУ РИЗИКУ

2.1 Основні методи аналізу ризику (повний, базовий, комбінований, експертний)

Жодна організація не може бути повністю захищена від загроз. Вона повинна своєчасно зреагувати на загрозу системі безпеки і у мінімальний проміжок часу повернути її до нормального функціонування. У цьому їй може допомогти правильно сформульована **політика безпеки** [2, 3, 6, 7]**.**

Під ***політикою безпеки інформації*** варто розуміти набір законів, правил, обмежень, рекомендацій та інш., які регламентують порядок обробки інформації і спрямовані на ЗІ від загроз. Створення політики безпеки для ІС зможе допомогти одночасно зменшити ризики і разом з тим

адекватно визначити витрати, необхідні для підтримки режиму ІБ, і вірно ці засоби розподілити.

Інша перевага політики ІБ полягає в тому, що вона надає каркас, що визначає розподіл ролей і відповідальності, дозволяє формулювати і підтверджувати необхідні правила і директиви й однозначно визначає позицію організації щодо будь-яких дій, що загрожують безпеці інформаційної системи.

Виконання політики безпеки на практиці вимагає розробку деталізованого плану безпеки, елементами якого є [6, 7]:

- визначення цінності контенту мережі;
- визначення загроз цьому контенту;
- визначення з попередніх кроків необхідних заходів безпеки, що відповідають цінності контенту;
- підготовка ресурсів, необхідних для прийняття цих заходів безпеки;
- навчання персоналу, необхідне для підтримки політики безпеки;
- періодичні перегляди плану безпеки для відповідності його з вимогами, що змінюються, а також змінами в персоналі і навколишньому оточенні.

Виконанню політики безпеки сприяє правильно обрані методи аналізу й оцінки вихідних даних з метою чіткого визначення необхідних засобів інформаційної безпеки. Такі методи називаються **методами аналізу ризику** [6, 7]**.**

Мета процесу оцінювання ризиків є у визначенні характеристик ризиків ІС і її ресурсів. На основі таких даних можуть бути обрані необхідні засоби захисту.

При проведенні аналізу ризиків необхідно визначити:

- вразливі місця в даній інформаційній системі;

- існуючі загрози, їх рівень;

- припустимий рівень загроз;

- комплекс мір, що дозволяє знизити ризики до припустимого рівня.

По кожному з цих пунктів потрібно проведення спеціальних досліджень.

При забезпеченні ІБ важливо не упустити яких-небудь істотних деталей. Це буде гарантувати деякий **мінімальний (базовий) рівень** ІБ, обов'язковий для будь-якої мережі. У випадку підвищених вимог в області ІБ використовується **повний варіант** аналізу ризиків. На відміну від базового варіанта, виробляється оцінка цінності ресурсів, характеристик ризиків і вразливостей.

Існують різні підходи до оцінки ризиків, вибір яких залежить від рівня вимог, пропонованих в організації до режиму ІБ.

При оцінюванні ризиків враховуються багато факторів [8, 9]:

- цінність ресурсів;
- значимість загроз;
- ефективність існуючих і планованих засобів захисту;
- інші фактори.

Аналіз ризиків – необхідний етап при розробці політики інформаційної безпеки.

Застосування яких-небудь апаратних засобів не є обов'язковим, однак, їх використання дозволяє зменшити трудомісткість проведення аналізу ризиків і вибору контрзаходів. В даний час існує біля двох десятків програмних продуктів для аналізу ризиків: від найпростіших, орієнтованих на базовий рівень безпеки, до складних і дорогих продуктів, що дозволяють провести повний аналіз ризиків і вибрати комплекс контрзаходів необхідної ефективності.

Використання **методу аналізу ризику** – основа для правильного визначення вимог по безпеці і зменшення ризику в ІС. Крім того, необхідно

мати повну організаційну стратегію для аналізу ризику в системі. Стратегія повинна гарантувати, що обраний підхід задовольняє необхідним вимогам і зосереджує зусилля по забезпеченню безпеки там, де вони дійсно необхідні.

В даний час використовуються кілька підходів до аналізу ризиків [11].

Їх вибір залежить від оцінки власниками цінності своїх інформаційних ресурсів і можливих наслідків порушення режиму ІБ.

У найпростішому випадку власники інформаційних ресурсів можуть не оцінювати ці параметри.

Найчастіше передбачається, що цінність ресурсів, що захищаються, не є надмірно високою. У цьому випадку аналіз ризиків виконується за спрощеною схемою: розглядається стандартний набір найбільш розповсюджених загроз безпеки без оцінки їх ймовірності і забезпечується **мінімальний (базовий)** рівень ІБ. Існує ряд стандартів і специфікацій, у яких розглядається мінімальний (типовий) набір найбільш ймовірних загроз, таких як віруси, помилки обладнання, НСД і ін. Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи поза залежністю від ймовірності їх здійснення й вразливості ресурсів. Таким чином, характеристики загроз на базовому рівні розглядати не обов'язково.

Повний варіант аналізу ризиків застосовується у випадку підвищених вимог до ІБ. На відміну від базового варіанта в тому чи іншому виді виконується оцінка цінності ресурсів, характеристик ризиків і вразливостей ресурсів. Як правило, проводиться аналіз вартість/ефективність декількох варіантів захисту.

Таким чином, при проведенні **повного аналізу ризиків** необхідно [11]:

- визначити цінність ресурсів;

- до стандартного набору додати список загроз, актуальних для досліджуваної мережі;

- оцінити ймовірність загроз;

- визначити вразливість ресурсів;

- запропонувати рішення, що забезпечує необхідний рівень ІБ.

При проведенні аналізу ризику можлива **комбінація підходів**, що полягає в тому, що спочатку проводиться початковий аналіз ризику, а потім детальний. Детальний аналіз ризику повинний проводитися в порядку пріоритету. Комбінація підходів повинна забезпечувати баланс між зменшенням часу і зусиллями, витраченими на визначення ЗЗ, і гарантуванням того, що системи з високим рівнем ризику будуть відповідно захищені.

В даний час відомо безліч методів оцінювання загроз, більшість з який побудовані на використанні таблиць [6, 7, 11].

Такі методи порівняно прості у використанні і досить ефективні. Однак не варто говорити про «кращий» метод, тому що в різних випадках вони будуть різними. Важливо з наявного різноманіття методів вибрати саме той, котрий забезпечував би відтворені результати для даної організації.

У матриці чи таблиці можна наочно побачити зв'язок факторів негативного впливу (показників ресурсів) і ймовірностей реалізації загрози з урахуванням показників вразливостей (табл. 1) [3, 11].

Таблиця 1

Дескриптор загрози (а)	**Показник негативного впливу (б)**	**Ймовірність реалізації загрози (с)**	**Показник ризику (д)**	**Ранг загрози (е)**
Загроза A	5	2	10	2
Загроза B	2	4	8	3
Загроза C	3	5	15	1
Загроза D	1	3	3	5
Загроза E	4	1	4	4

Загроза F	2	4	8	3

На першому кроці оцінюється негативний вплив (показник ресурсу) по заздалегідь визначеній шкалі, наприклад від 1 до 5, для кожного ресурсу, якому загрожує небезпека (стовпчик *б* у таблиці).

На другому – по заздалегідь заданій шкалі, наприклад від 1 до 5, оцінюється ймовірність реалізації кожної загрози (стовпчик *с)*.

На третьому кроці обчислюється показник ризику (стовпчик *д у таблиці*). У найпростішому варіанті методики це робиться шляхом множення (*б* × *с*). Однак необхідно пам'ятати, що операція множення визначена для **кількісних шкал**. Для рангових (якісних) шкал виміру, якими є показник негативного впливу і ймовірність реалізації загрози, наприклад, зовсім не обов'язково показник ризику, що відповідає ситуації b=1, c=3, буде еквівалентний b=3, c=1. Відповідно, повинна бути розроблена методика оцінювання показників ризиків стосовно до конкретної організації.

На четвертому кроці (стовпчик *е)* загрози ранжирують за значеннями їхнього фактору ризику.

У розглянутому прикладі для позначення найменшого негативного впливу і найменшої ймовірності реалізації обраний показник дорівнює 1.

Дана процедура дозволяє порівнювати і розділяти по пріоритету загрози з різними негативними впливами й імовірностями реалізації.

Розглянемо приклад оцінки **негативного впливу від небажаних подій (частота повторюваності).**

Кожному ресурсу привласнюється визначене значення, що відповідає потенційному збитку від впливу загрози. Такі показники привласнюються ресурсу стосовно всіх можливих загроз.

Далі оцінюється показник частоти повторності. Частота залежить від ймовірності виникнення загрози і простоти використання вразливості.

Показник частоти є суб'єктивною мірою можливості реалізації загрози й оцінюється, як правило, у якісних шкалах. Прикладом є табл. 2, де задані суб'єктивні частоти реалізації події в шкалі 0 (дуже рідко) – 4 (дуже часто) для різних рівнів загроз і вразливостей (Н, З, У – низький, середній, високий рівень вразливості). Далі визначається суб'єктивна шкала ризиків у залежності від показника цінності ресурсу і частоти, приклад приведений у табл. 3 (0 – мінімальний ризик, 8 – максимальний ризик). Ці значення повинні відбивати позицію організації стосовно розглянутих ризиків [11].

Таблиця 2

Рівень загрози								
Низький			Середній			Високий		
Рівні вразливості			Рівні вразливості			Рівні вразливості		
Н	С	В	Н	С	В	У	С	В
0	1	2	1	2	3	2	3	4

де Н, С, В – означає низький, середній, високий рівень.

Розглянемо приклад методу, побудованого на використанні таблиць і враховуючий тільки вартісні характеристики ресурсів.

Цінність фізичних ресурсів оцінюється з погляду вартості їх заміни чи відновлення працездатності (тобто ***кількісних показників***). Ці вартісні величини потім перетворяться в якісну шкалу, що використовується також для інформаційних ресурсів. Програмні ресурси оцінюються тим же способом, що і фізичні, виходячи з витрат на їхнє придбання чи відновлення.

Якщо для інформаційного ресурсу існують особливі вимоги до конфіденційності чи цілісності (наприклад, якщо вихідний текст має високу комерційну цінність), то оцінка цього ресурсу виробляється по тій же схемі, тобто у вартісному вираженні.

Кількісні показники ризику інформаційних ресурсів оцінюються на підставі опитувань співробітників компанії (власників інформації) – тих, хто може оцінити цінність інформації, визначити її характеристики і ступінь критичності. На основі результатів опитування виробляється оцінювання показників і ступеня критичності інформаційних ресурсів для найгіршого варіанта розвитку подій. Розглядається потенційний вплив на бізнес-процес при можливому несанкціонованому ознайомленні з інформацією, зміні інформації, відмовленні від виконання обробки інформації.

Далі розробляється система показників у бальних шкалах (приклад – чотирьохбальна шкала (від 0 до 4), приведена в табл. 3) [3, 11].

Таблиця 3

Показник ресурсу	**Показник частоти**				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Таким чином, кількісні показники використовуються там, де це припустимо і виправдано, а якісні – там, де кількісні оцінки неможливі, наприклад, при загрозі людському життю.

По кожній групі ресурсів, зв'язаної з даною загрозою, оцінюється рівень останньої (ймовірність реалізації) і ступінь вразливості (легкість, з яким реалізована загроза здатна привести до негативного впливу). **Оцінювання проводиться в якісних шкалах** [11].

Наприклад, рівень загроз і рівень вразливостей можна оцінити по шкалі ***«високий – середній - низький».*** Інформацію збирають, опитуючи

співробітників, що займаються технічними питаннями, і аналізуючи документацію.

Розглянемо приклад - рівні ризику визначаються трьома параметрами: цінністю ресурсу, рівнями загрози й вразливостями.

Кожному значенню рівня ризику повинен відповідати опис, що дозволяє однозначно його трактувати різним людям і розуміти, де проходить межа між значеннями.

Наприклад, показник ризику виміряється в шкалі від 0 до 8 з наступними визначеннями рівнів ризику:

1 – ризик практично відсутній. Теоретично можливі ситуації, при яких подія настає, але на практиці це случається рідко, а потенційний збиток порівняно невеликий.

2 – ризик дуже малий. Події подібного роду трапляються досить рідко, крім того, негативні наслідки порівняно невеликі.

…....

8 – ризик дуже великий. Подія швидше за все наступить, і наслідки будуть надзвичайно важкими.

Приклад матриці приводиться в табл. 4 [6, 11].

Таблиця 4

Цінність ресурсу	**Рівень загрози**								
	Низький			Середній			Високий		
	Рівень вразливості			Рівень вразливості			Рівень вразливості		
	Н	С	В	Н	С	В	Y	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Для кожного ресурсу розглядаються стосовні для нього вразливі місця і відповідні їм загрози. Якщо вразливість існує, але немає зв'язаної з нею загрози чи існує загроза, не зв'язана з якими-небудь вразливими місцями, то в такій ситуації ризиків немає. Однак треба мати на увазі, що надалі ситуація може змінитися.

Кожен рядок у матриці визначається показником ресурсу, а кожен стовпець – ступенем небезпеки загрози й вразливості. Наприклад, ресурс має цінність 3, загроза має ступінь «висока», а вразливість – «низька». Показник ризику в даному випадку буде дорівнювати 5. У випадку, коли ресурс має цінність 2, наприклад, для модифікації, рівень загрози – низький, а вразливості, навпроти, високі, показник ризику дорівнює 4.

Розмір матриці, що враховує кількість ступенів загроз і вразливостей, категорій ресурсів, може бути іншим і визначається конкретною організацією.

Після того як оцінювання ризиків було виконано перший раз, його результати звичайно зберігають у базі даних. Надалі проводити повторне оцінювання буде значно легше.

Інший спосіб оцінювання ризиків складається в поділі їх тільки на прийнятні і не прийнятні. Підхід ґрунтується на тім, що кількісні показники ризиків використовуються тільки для їх упорядкування і визначення першочергових дій. Але цього можна досягти і з меншими витратами.

Матриця, використовувана в даному підході, містить не числа, а тільки символи **Д** (ризик допустимо) і **Н** (ризик не допустимо). Наприклад, може бути використана матриця (табл. 5) [11].

Таблиця 5

Показник ресурсу	**Показник частоти**				
	0	**1**	**2**	**3**	**4**
0	Д	Д	Д	Д	Н

1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Питання про те, як провести границю між прийнятними і не прийнятними ризиками, залишається на розсуд користувача [3, 11].

Для правильного прийняття рішень у тому чи іншому випадку (наприклад, при аналізі ризику) часто використовуються експертні системи (ЕС). Створенню ЕС сприяє комп'ютеризація різних обчислювальних процесів. Вони являють собою пакети ПЗ, що імітують діяльність людини-експерта. ЕС поєднують можливості комп'ютера зі знаннями експерта для того, щоб надати споживачу - суб’єкту, що приймає рішення, розумну раду по будь-якому питанню, на основі прозорої процедури пошуку рішення, що розширює можливості змістовного аналізу на якісному рівні, що підвищує стійкість результатів розрахунків з поясненням кожного з його етапів.

Важливий напрямок по створенню ЕС – розробка програм, що при рішенні важких задач забезпечують одержання результатів, що не уступають по якості й ефективності рішенням, одержуваним експертами.

Необхідність у розвитку такого напрямку в розробці ЕС полягає в тім, що потрібна надійна система-порадник, що переборює, зокрема, труднощі інтерпретації результатів розрахунків, проведених на основі строгих методів.

Точні методи складні, непрозорі, громіздкі і викликають у ряді випадків неадекватне їх розуміння; вимагають трудомісткого програмування і найчастіше розроблені без врахування унікальної здатності людини приймати компромісні рішення.

Через невірогідність вихідної інформації, нечіткість критерію на вибір рішення, спрощеність формалізованого представлення економічної

реальності в моделях, а також мала розробленість математичного апарату в результаті розрахунків виходить все-таки умовно оптимальне рішення, що у ряді випадків не реалізується безпосередньо на практиці, оскільки остаточний варіант практично приймається на якісному рівні в ході змістовного аналізу.

Надійність рішення задач на основі строгих методів знижується також внаслідок можливих збоїв у комп'ютерній технології. Некритичне застосування програмних засобів вселяє іноді своєрідну ілюзію об'єктивності і точності, хоча нерідко методи, закладені в програму машинного розрахунку менш коректні, чим евристичний метод, реалізований у ЕС [10].

Евристика дозволяє за рахунок організації рівнобіжних розрахунків внести простоту, ясність і прозорість у рішення питань надійності і доцільності використання самих програмних пакетів, тому що задача тестування цих пакетів у даний час перетворюється в самостійну проблему.

Евристичні методи не протиставляються строгим методам, а доповнюють їх, забезпечуючи поглиблення якісного аналізу результатів розрахунків і підвищення надійності отриманого рішення.

Евристичні міркування й аналіз зв'язані з логічним і досить прозорим пошуком рішень. Цей пошук заснований на використанні минулого досвіду і знань. Пошук рішення виробляється практично найбільш простим способом.

В даний час процедури евристичних рішень застосовуються в основному для **неформалізованих** чи **слабо формалізованих задач** [10]**.**

До неформалізованих відносяться задачі, що не мають алгоритмічного рішення чи не можуть бути задані в числовій формі. У більшості випадків ці задачі характеризуються помилковістю чи неповнотою вихідних даних, недостатньою розробленістю способу рішення.

Рішення **формалізованих задач** обумовлено цілим рядом причин (невірогідністю вихідних даних, недоліками самих строгих методів чи неправильним їхнім використанням, збоями в комп'ютерній технології, чи помилками, навмисним перекручуванням результатів розрахунків при їх інтерпретації). До числа формалізованих відносяться також складні задачі, у яких ефективність операцій визначається на основі не одного, а декількох критеріїв.

Сучасні експертні системи при необхідності поєднуються з традиційними програмними засобами, а результати розрахунків іноді перевершують ті, котрих досягає людина-експерт. Власне кажучи, створюються автоматизовані інформаційні системи **інтелектуального типу.** Важлива відмінність цих систем полягає в наступному [10]:

- крім бази даних функціонує база знань;
- мається пристрій (розв’язувач) з логікою розумового процесу експерта, що дозволяє використовувати комп'ютер для підготовки результатів аналізу, варіантів висновків і побудови гіпотез.

Однак, остаточний вибір найбільш правильного рішення, як відзначалося вище, залишається за суб’єктом, що приймає рішення (керівником робіт).

Експертні системи складаються з ряду блоків [10]:

- бази знань, що містить необхідну інформацію про дану предметну область з урахуванням логічних зв'язків між інформаційними блоками;
- розв’язувача інтелектуальної ІС, де зосереджені логічні операції, що дозволяють установлювати зв'язок між професійними знаннями експертів і реальними ситуаціями;
- механізму висновку, здатного використовувати логічні зв'язки для формування висновків (порад), орієнтованих на

користувача;

- системи пояснень, що повідомляє користувачу аргументи підготовлених комп'ютером висновків;
- системи адаптації механізму пояснень до знань користувача, що працює з системою.

База даних являє собою робочу область, в якій зберігаються вихідні і проміжні данні тих задач, що зважуються в той чи інший момент часу. Процес наповнення експертної системи знаннями здійснюється в основному користувачем [10].

Експертні системи часто використовуються як засіб одержання знань.

Відомі кілька *інтелектуальних методів виявлення й аналізу знань.* Найбільш розповсюджена операція інтелектуального аналізу знань - *класифікація,* що дозволяє виявляти ознаки, що характеризують групу, до якої, належить той чи інший об'єкт, та чи інша перемінна. Якщо прийняті категорії взаємно виключають один одного, то об'єкт може потрапити тільки в одну з них. Якщо ж категорії не є взаємовиключними, то об'єкт може бути поміщений у кілька категорій, для яких він перевищив граничне значення визначеного критерію [10].

Можлива *стратегія пошуку рішення, заснована на наявності мети чи наявності деякої інформації.* Зокрема, експертні системи оцінюють, яку користь можна витягти з отриманої інформації і потім перевіряє наступні значення перемінних.

Використовуються також *"дерева рішень", що* розбивають дані на визначені групи на основі значень тих чи інших перемінних. Однак набір операторів "якщо → те" іноді буває неясним, особливо, якщо список умов довгий і складний.

У ході аналізу і витягу знань в експертних системах застосовуються також *методи візуалізації* (візуальне представлення відразу декількох

перемінних достатньо виразне і може охоплювати великі обсяги даних), *методи нечіткої логіки* (представлення і використання ненадійних даних). Для підтримки процесів класифікації і кластеризації використовується набір *статистичних методів* [10].

Розроблювальні в даний час експертні системи призначені для пошуку рішень практичних задач, що не задані в числовій формі, не забезпечені достовірною інформацією, не мають алгоритмічного рішення чи вимагають великих витрат часу і машинної пам'яті.

Інструментарій експертних систем не може замінити рішення задач строгими методами. Однак, при наявності евристичної методики, придатної для рішення формалізованих задач, експертні системи можна використовувати для рівнобіжних розрахунків задач на додаток до строгих методів. За рахунок ясності і прозорості евристичного алгоритму в ході рівнобіжних розрахунків забезпечується висока надійність рішення задач і розширюється можливості остаточного вибору найкращого варіанта в наступному якісному аналізі.

Рівнобіжні розрахунки в системі підтримки прийняття рішень повинні забезпечити не тільки зростання надійності вибору правильного рішення задач, з огляду на визначені недоліки самих строгих методів, але і надати необхідну допомогу користувачу.

Для виконання рівнобіжних розрахунків потрібно особлива універсальна евристична методика. Таким новим напрямком у створенні інтелектуальних інструментальних засобів є розглянута в даній роботі універсальна евристична методика (евристична методика структурного діагностичного аналізу, діаграма "ефект/витрати"), придатна для рішення широкого кола задач статистики, традиційного програмування і деяких слабо формалізованих задач [10].

2.2 Базовий аналіз ризику BS 7799 (ISO 17799) і правила його проведення [4]

За кордоном почали починатися спроби знайти загальні відповіді на питання забезпечення ІБ. Першою вдалою спробою в цій області став британський стандарт BS 7799 «Практичні правила керування інформаційною безпекою» (1995), у якому узагальнений досвід забезпечення режиму ІБ в ІС різного профілю. Цей стандарт послужив основою для розробки нового стандарту ISO 17799, що був прийнятий наприкінці 2000 року [4].

Існують аналогічні стандарти різних організацій і відомств, у тому числі німецький стандарт BSI.

Зміст цих документів в основному відноситься до етапу базового аналізу ризиків, на якому визначаються загрози безпеки й вразливості інформаційних ресурсів, уточнюються вимоги до режиму ІБ.

Для того щоб забезпечити базовий рівень безпеки, досить перевірити виконання вимог відповідного стандарту (специфікації), наприклад ISO 17799. Програмні продукти, призначені для цієї мети, дозволяють сформувати список питань, що стосується виконання цих вимог. На основі відповідей генерується звіт з рекомендаціями з усунення виявлених недоліків.

Прикладом програмного продукту цього класу є COBRA, виробник C &A Systems Security Ltd. COBRA дозволяє істотно полегшити процес перевірки на відповідність вимогам Британського стандарту BS 7799 (ISO 17799) інформаційної системи [4].

Мається кілька баз знань: загальні вимоги BS 7799 (ISO 17799) і спеціалізовані бази, орієнтовані на різні області застосування.

Ідеї, що містяться в цих документах, полягають у наступному: практичні правила забезпечення ІБ на всіх етапах життєвого циклу інформаційної технології повинні носити комплексний характер і

ґрунтуватися на перевірених практикою прийомах і методах. Наприклад, в ІТ повинні обов'язково використовуватися деякі засоби ідентифікації й автентифікації користувачів (сервісів), засоби резервного копіювання, антивірусний контроль та інші.

Режим ІБ у подібних системах забезпечується:

- на процедурному рівні – шляхом розробки і виконання розділів інструкцій для персоналу, присвячених ІБ, а також мірами фізичного захисту;
- на програмно-технічному рівні – застосуванням апробованих і сертифікованих рішень, стандартного набору контрзаходів: резервне копіювання, антивірусний захист, парольний захист, МЕ, шифрування даних і ін.

Документ BS 7799 (ISO 17799) складається з двох частин [4].

У частині 1: «Практичні рекомендації» 1995р., визначаються і розглядаються наступні аспекти ІБ [4]:

- Політика безпеки.
- Організація захисту.
- Класифікація і керування інформаційними ресурсами.
- Керування персоналом.
- Фізична безпека.
- Адміністрування комп'ютерних систем і мереж.
- Керування доступом до систем.
- Розробка і супровід систем.
- Планування безперебійної роботи організації.
- Перевірка системи на відповідність вимогам ІБ.

У частині 2: «Специфікація системи», 1998 р., розглядаються ці ж аспекти з погляду сертифікації ІС на відповідність вимогам стандарту [7, 8].

.

2.3 Методи детального аналізу ризику [12]

При виконанні повного аналізу ризиків в інформаційних системах з підвищеними вимогами до безпеки приходиться вирішувати ряд складних проблем:

Як визначити цінність ресурсів?

Як скласти повний список загроз ІБ і оцінити їх параметри?

Як правильно вибрати контрзаходи й оцінити їх ефективність?

Процес оцінювання ризиків містить кілька етапів [12]:

- ідентифікація ресурсу й оцінювання його кількісних показників чи визначення потенційного негативного впливу на об’єкт;

- оцінювання загроз;

- оцінювання вразливостей;

- оцінювання існуючих і передбачуваних засобів забезпечення ІБ;

- оцінювання ризиків.

На основі оцінювання ризиків вибираються засоби, що забезпечують режим ІБ. Ресурси, значимі для власника і маючі визначений ступінь вразливості, піддаються ризику, якщо стосовно них існує яка-небудь загроза. При оцінюванні ризиків враховуються потенційний негативний вплив від небажаних подій і показники значимості розглянутих вразливостей і загроз для них. Ступінь ризику залежить від:

- показників цінності ресурсів;

- ймовірності реалізації загроз;

- простоти використання вразливості при виникненні загроз;

- існуючих чи планованих до впровадження засобів забезпечення ІБ, що зменшують вразливості, скорочують ймовірність виникнення загроз і негативних впливів.

Визначення цінності ресурсів.

Ресурси звичайно підрозділяються на кілька класів, наприклад, фізичні, програмні і дані. Для кожного класу повинна існувати своя методика оцінки цінності елементів.

Для оцінки цінності ресурсів вибирається придатна система критеріїв. Критерії повинні дозволяти описати потенційний збиток, зв'язаний з порушенням К, Ц, Д.

Цінність фізичних ресурсів оцінюється з погляду вартості їх заміни чи відновлення працездатності. Ці вартісні величини потім перетворяться в якісну шкалу, що використовується також для інформаційних ресурсів. Програмні ресурси оцінюються тим же способом, що і фізичні, на основі визначення витрат на їх придбання чи відновлення.

Якщо для інформаційного ресурсу існують особливі вимоги до конфіденційності чи цілісності (наприклад, якщо вихідний текст має високу комерційну цінність), то оцінка цього ресурсу виробляється по тій же схемі, тобто у вартісному вираженні.

Крім критеріїв, що враховують фінансові втрати, можуть бути присутніми критерії, що відображують [12]:

- збиток репутації організації;
- неприємності, зв'язані з порушенням діючого законодавства;
- збиток для здоров'я персоналу;
- збиток, зв'язаний з розголошенням персональних даних окремих осіб;
- фінансові втрати від розголошення інформації;
- фінансові втрати, зв'язані з відновленням ресурсів;
- втрати, зв'язані з неможливістю виконання зобов'язань;
- збиток від дезорганізації діяльності.

Можуть використовуватися й інші критерії в залежності від профілю організації.

Повний аналіз ризиків [6–9]**.**

Програмні засоби, що дозволяють провести повний аналіз ризиків, будуються з використанням структурних методів системного аналізу і проектування (SSADM – Structured Systems Analysis and Design) і являють собою інструментарій для:

- побудови моделі ІС з погляду ІБ;
- оцінки цінності ресурсів;
- складання списку загроз і вразливостей, оцінки їх характеристик;
- вибору контрзаходів і аналізу їх ефективності;
- аналізу варіантів побудови захисту;
- документування (генерація звітів).

Прикладами програмних продуктів цього класу є:

- CRAMM – розроблювач Logica (Великобританія);
- MARION – розроблювач CLUSIF (Франція);
- RiskWatch (США).

Обов'язковим елементом цих продуктів є база даних, що містить інформацію з інцидентів в області ІБ, що дозволяє оцінити ризики й вразливості, ефективність різних варіантів контрзаходів у визначеній ситуації. Один з можливих підходів до розробки подібних методик – нагромадження статистичних даних про реальні події, що відбулися, аналіз і класифікація причин, виявлення факторів ризику. На основі цієї інформації можна оцінити загрози й вразливості в інших ІС.

Метод CRAMM

У 1985 році Центральне агентство по комп'ютерам і телекомунікаціям (ССТА) Великобританії почало дослідження існуючих методів аналізу ІБ для того, щоб рекомендувати методи, придатні для використання в урядових закладах, зайнятих обробкою несекретної, але критичної інформації. Жоден з розглянутих методів не підійшов. Тому був розроблений новий метод, що відповідає вимогам ССТА.

Він одержав назву **CRAMM** – метод ССТА аналізу і контролю ризиків. Потім з'явилося кілька версій методу, орієнтованих на вимоги міністерства оборони, цивільних державних установ, фінансових структур, приватних організацій. Одна з версій, «комерційний профіль», є комерційним продуктом. В даний час продається версія CRAMM 4.0. Метою розробки методу було створення формалізованої процедури, що дозволяє:

- переконатися, що вимоги, зв'язані з безпекою, цілком проаналізовані і документовані;
- уникнути витрат на зайві міри безпеки, можливі при суб'єктивній оцінці ризиків;
- допомагати в плануванні і здійсненні захисту на всіх стадіях життєвого циклу ІС;
- забезпечити проведення робіт у стислий термін;
- автоматизувати процес аналізу вимог безпеки;
- представити обґрунтування для мір протидії;
- оцінювати ефективність контрмір, порівнювати різні варіанти контрзаходів;
- генерувати звіти.

В даний час CRAMM, судячи з числа посилань в Інтернету, є найбільш розповсюдженим методом аналізу і контролю ризиків.

Аналіз ризиків містить у собі ідентифікацію й обчислення рівнів ризиків на основі оцінок, привласнених ресурсам, загрозам і вразливостям ресурсів. Контроль ризиків складається з ідентифікації і виборі контрзаходів, що дозволяють знизити ризики до допустимого рівня. Формальний метод, заснований на цій концепції, дозволяє переконатися, що захист охоплює всю систему й існує впевненість у тім, що:

- усі можливі ризики ідентифіковані;
- вразливості ресурсів ідентифіковані і їх рівні оцінені;

- загрози ідентифіковані і їх рівні оцінені;

- контрзаходи ефективні;

- витрати, зв'язані з ІБ, виправдані.

Дослідження ІБ системи за допомогою CRAMM проводиться в три етапи:

Етап 1: аналізується усе, що стосується ідентифікації і визначення цінності ресурсів системи. Наприкінці цього етапу замовник дослідження буде знати, чи досить йому існуючої традиційної практики, чи він має потребу в проведенні повного аналізу безпеки.

Етап 2: розглядається усе, що відноситься до ідентифікації й оцінки рівнів загроз для груп ресурсів і їх вразливостей. Наприкінці другого етапу замовник одержує ідентифіковані й оцінені рівні ризиків для своєї системи.

Етап 3: пошук адекватних контрзаходів. Власне кажучи, це пошук варіанта системи безпеки, що максимально відповідає вимогам замовника. Наприкінці етапу він буде знати, як варто модифікувати систему в термінах мір відхилення від ризику, а також вибору спеціальних мір протидії, що ведуть до зниження ризиків, які залишилися, до припустимого рівня.

Кожна стадія з'являється закінченої після детального обговорення й узгодження результатів із замовником.

2.4 Недоліки існуючих методів аналізу ризику. Покращення методів аналізу ризику.

Для керування ризиками можна використовувати різні широко відомі методики. Однак є ряд недоліків:

- що відкриті документи найчастіше не містять ряду важливих деталей, що обов'язково треба конкретизувати при розробці застосовних на практиці методик.
- Конкретизація цих деталей залежить від рівня зрілості організації, специфіки її діяльності і деяких інших факторів.

Сучасні технології аналізу ризиків дозволяють оцінити існуючий рівень залишкових інформаційних ризиків у вітчизняних компаніях. Це особливо важливо в тих випадках, коли до ІС підприємства пред'являються підвищені вимоги в області ІБ. Сьогодні існує ряд методик аналізу ризиків, у тому числі з використанням CASE-засобів, адаптованих до використання у вітчизняних умовах.

До переваг методів аналізу ризику можна віднести наступне:

- якісно виконаний аналіз ризиків дозволяє провести порівняльний аналіз «ефективність - вартість» різних варіантів захисту;
- вибрати адекватні контрзаходи;
- оцінити рівень залишкових ризиків.

До недоліків існуючих статистичних методів можна віднести наступні:

- по-перше, повинний бути зібраний дуже великий матеріал про події в цій області;
- по-друге, застосування цього підходу виправдано далеко не завжди.

Альтернативою статистичному підходу є підхід, заснований на аналізі особливостей технології. Прикладом є згаданий німецький стандарт BSI з великим каталогом загроз і контрзаходів.

Застосування стандарту BSI при аналізі ризиків має ряд недоліків:

- цей підхід також не універсальний тому, що темпи технологічного прогресу в області IT такі, що наявні оцінки відносяться до уже застарілих чи застаріваючих технологій;
- для новітніх технологій таких оцінок поки не існує.

Метод аналізу і контролю ризиків CRAMM має ряд недоліків**:**

- не погоджений з вітчизняними стандартами;
- можливість використання методів у наших умовах не є очевидним;

- продукт не надає потрібної гнучкості, що необхідна для ефективного використання його для аналізу вітчизняних систем.

Методи, засновані на побудові дерев відмовлень мають ряд недоліків і переваг:

- будуть випробувати експонентний ріст складності своєї структури при збільшенні розмірів системи – їхнього використання для аналізу складних систем недоцільне, але воно може бути досить ефективною при аналізі окремих компонентів системи унаслідок використання специфічних алгоритмів обробки дерев.

Імовірнісний і статистичний кількісний аналіз:

- вимагає величезної бази подій, що мали місце в умовах швидких темпів інформаційно-технологічного прогресу;
- цей метод недоцільно використовувати для детального аналізу ризиків у складних і високотехнологічних системах — бази знань будуть застарівати, не встигнувши створитися;
- неможливо створити базу знань, що буде давати достатню кількість інформації про можливі порушення режиму ІБ, за такий короткий час.

Методи якісного аналізу - засновані на побудові таблиць показників ресурсів і загроз мають ряд недоліків:

- не мають досить гнучких механізмів оцінювання допустимості рівнів ризику;
- таблиці, що використовуються для ранжирування загроз і оцінювання рівнів ризику мають у наявних продуктах фіксований вид;
- при корекції засобів захисту (якщо, наприклад, змінилася важливість для функціонування системи її визначеного компонента) у складній системі з великою кількістю ресурсів,

загроз і вразливостей значно легше змінити рівень припустимих ризиків, чим заново збирати інформацію про рівень загроз. Ці методи варто програмувати за допомогою апарата кінцевих автоматів.

Позитивні сторони оцінки ризику по якісній моделі полягають у наступному**:**

- обчислення прискорюються і спрощуються;
- немає необхідності привласнювати грошову вартість активу;
- немає необхідності обчислювати частоту прояву загрози і точний розмір збитку;
- не потрібно обчислювати відповідності ефективності передбачуваних мір загрозам.

Негативні сторони більшості методів оцінки ризиків полягають в основному в суб'єктивності підходу до оцінки і відсутності можливості установити точну відповідність витрат загрозам.

Тому можуть бути запропоновані деякі рекомендації [6, 7]:

1) Необхідний рівень ІБ у системі можна забезпечити використовуючи базовий і повний (детальний) підхід до аналізу ризиків, чи комбінацію цих підходів. Тобто, так чи інакше, прийдеться застосовувати якісь методи детального аналізу ризику;

2) Детальний варіант аналізу ризику передбачає декомпозицію складної системи на велику кількість порівняно маленьких елементів, що, безсумнівно, ускладнює процесу аналізу. З більшою деталізацією зв'язане значне збільшення кількості можливих загроз і ризиків, а отже, можливих контрзаходів по їх ліквідації;

3) Для декомпозиції складних систем доцільно використовувати метод побудови „дерев відмовлень”, особливо для графічного відображення взаємозв'язків між компонентами системи. Цей метод допоможе в точному визначенні границь системи, без якого неможливе створення повного переліку ресурсів системи;

4) При створенні нового продукту буде доцільно використовувати табличний метод ранжирування загроз і оцінки рівнів ризику, але необхідно зробити його по можливості гнучким, аби зробити можливість його використання для систем більш широкого спектру складності. Необхідне створення нових якісних профілів і типових методик з метою диверсифікованості переліку можливих варіантів використання продукту.

2.5. Висновки за 2 розділом.

1. Зроблено порівняльний аналіз методів детальної оцінки ризиків.
1. Виявлено недоліки існуючих методів аналізу ризику.
2. Запропоновано можливі шляхи покращення методів аналізу ризику.

3 ОБГРУНТУВАННЯ ТА ВИБІР МЕТОДУ ОЦІНКИ РИЗИКУ ДЛЯ МЕРЕЖІ ПЕРЕДАВАННЯ АУДІОВІЗУАЛЬНОГО КОНТЕНТУ

3.1 Методи аналізу ризику, як спеціалізовані системи підтримки і прийняття рішень

Система управління ризиками це свого роду спеціалізована система підтримки і прийняття рішень [10].

Головною особливістю IT підтримки прийняття рішень є якісно новий метод взаємодії людини та комп'ютера. Вироблення рішення, що є основною метою цієї технології, здійснюється в результаті ітераційного процесу (рис. 3), в якому беруть участь:

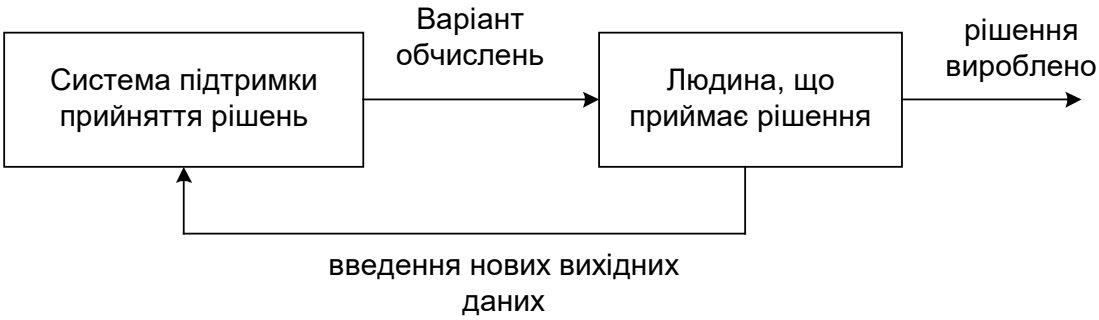

Рисунок 3 – Інформаційна технологія підтримки прийняття рішень як ітераційний процес [10]

• системи підтримки прийняття рішень у ролі обчислювальної ланки та об'єкта управління;

• людини як управляючої ланки, що задає вхідні дані та оцінює одержаний результат обчислень на комп'ютері.

Закінчення ітераційного процесу відбувається вибором людини. У цьому випадку можна говорити про здатність ІС разом із користувачем створювати нову інформацію для прийняття рішень.

ІТ підтримки прийняття рішень може використовуватися на будь-якому рівні управління. Крім того, рішення, що приймаються на різних рівнях управління, часто повинні координуватися. Тому важливою функцією і систем, і технологій є координація осіб, що приймають рішення як на різних рівнях управління, так і на одному рівні.

До складу системи підтримки прийняття рішень входять три головних компоненти:

- база даних;
- база моделей;
- програмна підсистема, яка складається із системи керування базою даних (СКБД), системи керування базою моделей (СКБМ) і системи керування інтерфейсом між користувачем і комп'ютером [9].

3.2. Отримання кількісних експертних оцінок показників ризику

Оцінка ризиків веде за собою перехід від якісних понять до кількісних.

Керування ризиками — це процес визначення, аналізу й оцінки, зниження, усунення чи переносу (переспрямування) ризику, який (процес) полягає у відповіді на наступні питання [12].

1. Що може відбутися?

2. Якщо це "щось" відбудеться, то який буде результат чи збиток?

3. Як часто може відбуватися ця подія?

4. Наскільки ми впевнені у відповідях на вищевказані питання (оцінка ймовірності)?

5. Що може бути зроблене для зниження чи усунення ймовірності події?

6. Скільки буде коштувати те, що може бути зроблено?

7. Наскільки ефективно те, що може бути зроблено?

Сам ризик, як такий і складається з поняття ймовірності (четверте питання), тобто чим більше ймовірність перших трьох питань (подія відбувається часто і з великим збитком), тим більше ризик, чим менше ймовірність, тим менше ризик.

Для кількісної оцінки використовується конкретна кількісна методика. Далі розглянемо три методики оцінки ризиків:

- модель якісної оцінки;
- традиційна методика під умовною назвою "Кількісна модель ризиків" (англ. Quantative Risk Model — QRM);
- "Модель узагальненого вартісного результату" Міори (англ. Miora Generalized Cost Consequence Model).

Модель якісної оцінки.

Якісна оцінка звичайно зводиться до побудови таблиці наступного виду (рис. 4).

Рисунок – 4. Таблиця якісної оцінки [12]

Таблиця заповнюється екземплярами інформаційних активів чи окремими системами на основі інтуїтивного представлення про ту чи іншу інформацію, на основі заповнення підготовлених опитувальних листів, анкет для компетентних співробітників організації. Рішення приймається в залежності від конкретної організації для об'єктів, що лежать у чорній зоні або в чорній і сірій зонах.

Можливий ще більш спрощений підхід під назвою ***основна лінія*** (Baseline). Він полягає в тім, що організація аналізує обстановку з побудовою систем безпеки, що склалася в мережі. Потім порівнює зі схемою безпеки, побудованої в самій компанії. Якщо виявляються відставання, ресурси направляються на приведення ситуації до рівня, близькому до середнього в галузі.

Кількісна модель ризиків (загальна методика).

Кількісна модель ризиків оперує такими поняттями, як:

- **річна частота події** (англ. Annualized Rate of Occurence — ARO), інакше кажучи, ймовірність появи збитку;
- **очікуваний одиничний збиток** (англ. Single Loss Expectancy — SLE), тобто вартість збитку від однієї успішної атаки;

- **очікуваний річний збиток** (англ. Annualized Loss Expectancy — ALE), величина, рівна добутку ARO на SLE.

$$ALE = ARO \text{ x } SLE$$

ARO — це частота появи події, що приносить збиток на річній основі, тобто, якщо подія відбувається раз у 5 років, то величина *ARO* дорівнює 1/5 чи 0,2, а якщо подія відбувається 3 рази на рік, то *ARO* дорівнює 3. Як бачимо, ця величина відмінна від математичної ймовірності, що не може бути більше 1. Величина *ARO* не обмежена зверху. Якщо в організації з 100 чоловік 50 щодня експлуатують ІС, при цьому 5 з них, володіючи високими правами, але низкою кваліфікацією, можуть щомісяця допускати серйозні помилки, що приводять до порушень у роботі системи, то *ARO* для цієї системи по даній події буде дорівнювати: 5 x 12 = 60.

SLE розраховується як добуток кількісного (вартісного) значення активу (англ. Asset Value — AV) на фактор впливу (англ. Exposure Factor — EF).

Фактор впливу — це розмір збитку чи впливу на значення активу (від 0 до 100%), тобто частина значення, що актив втратить у результаті події:

$$SLE = AV \times EF$$

Визначення ймовірності події.

Незважаючи на граничну простоту формул, числення ризиків за методикою QRM таїть у собі іншу складність: розрахунок складових.

Першим компонентом формули є *ARO.* Як обчислити ймовірність того чи іншого інциденту? Якщо розбити загрози по категоріях, то багато питань проясняться. Так, з питань загроз, що залежать від кліматичних умов (затоплення, урагани, зледеніння), треба звернутися в локальне чи державне метеорологічне бюро й одержати там необхідні статистичні дані. По пожежах — у керування пожежної охорони, по землетрусах — у сейсмічний

центр. Комп'ютерні злочини можуть бути закритою інформацією, або враховуватися органами внутрішніх справ по інших статтях, тоді необхідно звернутися до доступної світової статистики, роблячи виправлення на те, що визначений відсоток таких злочинів ховається постраждалими компаніями. Статистику відмовлень устаткування і ПЗ можна запросити в постачальників і, зважаючи на те, що виробники схильні прикрашати свій товар, звернутися до наявних незалежних експертних оцінок.

Визначення вартості активів.

Розділимо їх на відчутні і невловимі активи. До **відчутного** віднесемо засоби обслуговування ІТ — апаратне забезпечення, мережне забезпечення (середовище передачі даних), запасні частини, документація і зарплата персоналу для підтримки функціонування систем. Вартісні характеристики цих активів звичайно відомі або легко вираховуючи.

Вартість **невловимих** активів повинна враховувати два види витрат: витрати на заміну/відновлення програмного забезпечення і даних, витрати на порушення К, Ц, Д.

Визначення вартості невловимих активів — задача не завжди проста. Існують окремі методики такої роботи, наприклад, *Guideline for Information Valuation (GIV) — Інструкція з оцінки вартості інформації*, що доступна зареєстрованим членам Information Systems Security Association на сайті http://www.issa.org/.

Для оцінки вартості за **конфіденційністю** необхідне дослідження ряду додаткових умов.

- Якщо розголошення інформації про деталі дослідження ніяк не вплине на діяльність групи, то НД не має вартості в цьому змісті.
- Якщо розголошення інформації про НД, наприклад, конкурентам, означає крах усього дослідження, то витрати в цьому випадку

дорівнюються організації нових досліджень, тобто витратам у позиції 2.

- Якщо роботи групи були сегментовані таким чином, що НД пред'являє собою окремі об'єкти, не зв'язані один з одним, то, можливо, порушення конфіденційності одного з них не вплине на стан конфіденційності інших, витрати складуть меншу частину.

Для оцінки вартості порушення **цілісності** необхідно знати, наскільки таке порушення істотне для проекту чи для робіт. При цьому варто розрізняти значні помилки самого дослідження, помилки персоналу при роботі з даними, помилки устаткування, зміни, внесені зловмисниками, і ін. Також варто розрізняти дані по чутливості до порушень Ц.

Порушення **доступності** доцільно розрізняти за часом. Два основних види недоступно протягом періоду часу, що враховується, і недоступні назавжди. Остання ситуація аналогічна випадкам 1 і 2, а часткову неприступність варто класифікувати по проміжках часу — який збиток піде, якщо НД не буде доступний (частково доступний) протягом хвилини, години, дня і ін.

Для того щоб не упустити з розгляду всі можливі варіанти одержання збитку, необхідно зробити зв'язок між вразливістю, загрозою і впливом на актив. Приклад такого зв'язку приведений на рис. 5.

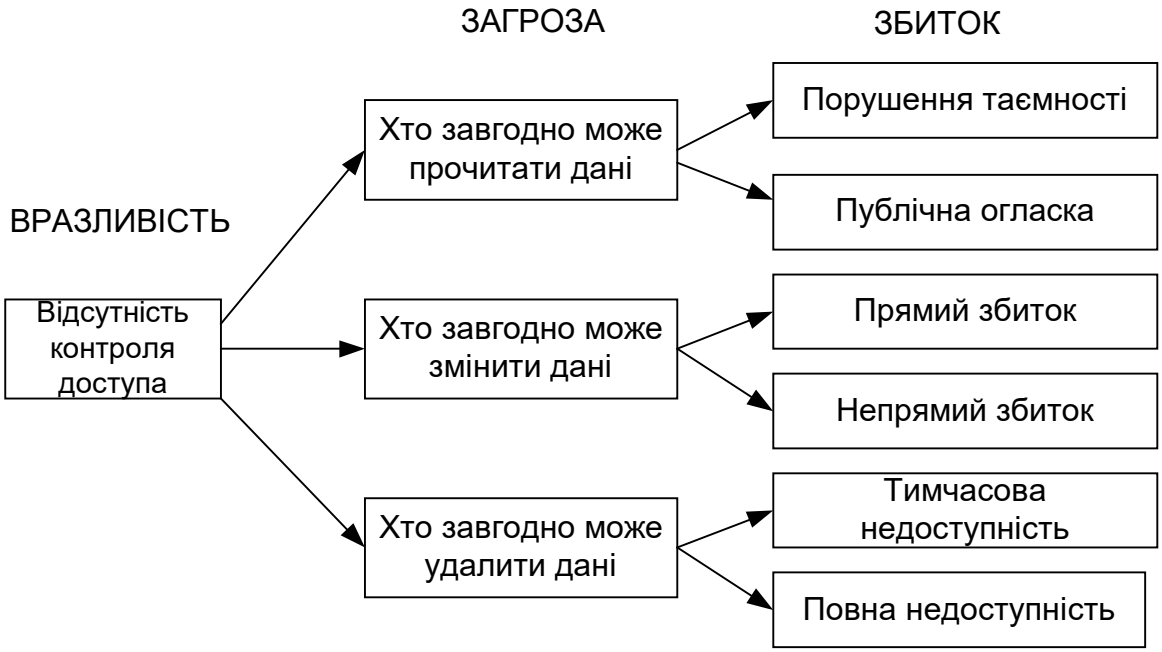

Рисунок 5 – Зв'язок "вразливість — загроза — збиток" [8]

Модель узагальненого вартісного результату Міори (GCC).

Розроблена як альтернатива кількісної моделі ризиків (QRM) для поліпшення і полегшення розрахунків і обчислень. Одним з основних недоліків QRM є те, що визначається її імовірнісна складова. Дійсно, що рідко відбуваються події з великим збитком і часто відбуваються події з маленьким збитком і часто вимагають різних підходів у визначенні захисних мір, однак, як можна бачити з формул, виглядати при розрахунках вони будуть однаково.

Модель GCC не враховує ймовірностей катастрофічних подій, вона оперує поняттям збитку від простою, як функцією від часу після настання подій. Для кожного інформаційного активу чи групи подібних по ряду ознак активів, називаних категорією, визначається розмір можливого збитку, термін початку його впливу на організацію і розподіл за часом.

Іноді зручніше представити розвиток картини збитку у виді графіка, де категорії — це функції по двох осях "час у днях" — "збиток у грошах". Звичайно в результуючому графіку показані дві криві:

- сумарний збиток організації при відсутності захисних заходів — аварійного плану (англ. disaster recovery plan — DRP);
- сумарний збиток при наявності DRP.

На такому графіку наочно видна необхідність і ефективність застосовуваних мір для забезпечення ЗІ.

Модель розрізняє три види збитків [8, 9]:

- прямий відчутний збиток;

- непрямий відчутний збиток;

- невловимий збиток.

Прикладами першого виду є категорії, що безпосередньо беруть участь у виробництві прибутку організації, тобто виробничі активи.

Другий вид — це в основному функції підтримки, активи, зв'язані з зовнішніми джерелами, і ін.

В третьому виді включений збиток репутації, невиконані обіцянки, негативна суспільна думка.

Як один з можливих підходів до розробки методик аналізу ризику в ІС можна запропонувати адаптацію існуючих аналітичних методів з інших областей. Одним з таких методів може бути так називаний SWOT-аналіз.

SWOT-аналіз - один з методів стратегічного менеджменту. Особливість його в тім, що інформаційне поле цього методу формується не високооплачуваними фахівцями й експертами, що можуть і не мати потрібного ступеня компетентності в даній конкретній задачі, а самим керівництвом організації і найбільш компетентними співробітниками. Це інформаційне поле складається у виді **матриці якісного аналізу,** що має назву SWOT (Strengths — сильні сторони; Weaknesses — слабості; Opportunities — можливості; Threats — загрози). Ця матриця являє собою ефективний інструмент структурного опису стратегічних характеристик системи і навколишнього середовища. При її створенні використовується так званий „дихотомичний” принцип — із самого початку усе поділяється

на дві частини — внутрішню і зовнішню, а потім усі можливі події в цих двох частинах у свою чергу розподіляються на сприятливі і несприятливі.

Для використання цього методу в безпеці ІС потрібно його адаптувати під цю систему, але не змінювати суті його ідеології, що може бути представлене у виді наступних складових [12, 13]:

- Місія;
- Цілі;
- Аналіз;
- Вибір стратегії;
- Реалізація стратегії;
- Корекція стратегії.

Місія в нашому випадку – це не досягнення визначених фінансових цілей (хоча можна виходити і з цього). Вона визначається призначенням самої ІС.

Як сильні сторони системи можна взяти наявні системи захисту інформації. Слабкі сторони — вразливості. Загрози свого змісту не втрачають. Даний метод дозволяє визначити напрямки розвитку системи ІБ, вибрати оптимальні засоби захисту для забезпечення необхідного рівня ІБ. Аналіз можна проводити як для системи в цілому, так і для її компонентів. При цьому необхідно чітко визначити границі кожної підсистеми, що розглядається.

Для оцінки загроз і вразливостей часто використовуються методи основані на непрямих факторах, наприклад у вигляді анкет і опитувальних листів [12].

Методи збирання інформації для систем формального аналізу.

На практиці, для збору й обробки первинної інформації про що захищається ІС можна використовувати:

- заздалегідь розроблені анкети, запитальники і контрольні аркуші для управлінського й обслуговуючого персоналу ІС;
- форми інтерв'ю експертів для проведення співбесід зі співробітниками компанії.
- існуючу техніко-економічну інформацію про ІС.
- спеціалізовані інструментальні програмні засоби для автоматизації процесу опису (наприклад, за допомогою сканерів, що дозволяють скласти карту ІС, а також знайти деякі вразливості для відповідних
- служб і сервісів мережі).

Ідентифікація загроз

Основними поняттями тут є:

- джерело загрози – подія або ситуація і спосіб, що може привести до реалізації
- загрози (у результаті використання потенційної вразливості);
- загроза – потенціал (чи міра) можливості реалізації джерела загрози;
- вразливість – слабість у захисті ІС.

Одним зі способів ідентифікації загроз є побудова моделі порушника, наприклад у виді таблиці (табл. 6) [7–9].

Таблиця 6

Джерело загрози	**Мотивація**	**Результат реалізації загрози (сценарій)**
Хакер	Хуліганство, самоствердження	Неавторизований доступ в ІС с використанням відомих вразливостей ОС (опис сценарію)
Криміналіст	Отримання фінансової інформації	Проникнення в ІС з метою отримання конфіденційних даних (опис сценарію)

Ідентифікація вразливостей.

У результаті виконання даного кроку складається список потенційних вразливостей даної ІС і можливі результати їх реалізації. Одним з можливих способів є складання таблиці, наприклад, що випливає типу (табл. 7).

Таблиця 7

Вразливість	Джерело загрози	Результат реалізації загрози (сценарій)
МЕ допускає доступ з публічної мережі к серверу А по протоколу Telnet, в тому числі в гостевому режимі	Неавторизований користувач зовні	Використовуючи вразливість протоколу, можливий доступ до файлової системі сервера А (опис сценарію)
Облікові записи співробітників, що залишили компанію, видаляються з мережі з запізненням на 1-2 дні	Внутрішні порушники, можливо в зговорі із співробітниками, що звільнилися	Незаконні фінансові операції (опис сценарію)

При оцінюванні рівня вразливості приймаються до увагі існуючі процедури і методи забезпечення режиму ІБ, дані внутрішнього аудиту і результати аналізу інцидентів, що мали місце.

Формування списку керуючих впливів організації.

Складається список керуючих впливів, структурований по рівням чи областям відповідальності у відповідність з використовуваною моделлю комплексного забезпечення режиму ІБ (табл. 8).

Таблиця 8

Рівень	Клас керуючих дій і критеріїв безпеки
Організаційний рівень	Розподіл відповідальності
	Періодичний перегляд системи управління в області ІБ
	Протоколювання і розбір інцидентів в області ІБ
	Оцінка ризиків
	Навчання в області ІБ

	Процедура авторизації в ІС і видалення облікових записів
	Підтримка в актуальному стані плану забезпечення ІБ
Процедурний рівень	Забезпечення правил підтримки режиму ІБ
	Доступ к носіям інформації
	Контроль роботи співробітників в ІБ
	Забезпечення потрібної якості роботи силової мережі, кліматичних установок
	Контроль за даними, що поступають в ІС
Програмно-технічний рівень	Комплекс мір захисту програмно-технічного рівня
	Активний аудит і система реагування
	Ідентифікація і автентифікація
	Криптографічний захист
	Реалізація ролевої моделі доступу
	Контроль режиму роботи мережного обладнання

Аналіз системи керування ІБ.

Параметри загроз, обумовлених на наступному кроці, істотно залежать від організації системи керування ІБ. На даному кроці виробляється аналіз системи керування з позиції можливого впливу на виявлені загрози й вразливості.

Звичайно розглядаються дві категорії: методи керування технічного і нетехнічного рівня.

Методи технічного рівня [2, 3]:

- забезпечення вимог базового рівня (ідентифікація, керування системою розподілу ключів, адміністрування, методи захисту елементів системи і ПЗ);
- методи, що випереджають, (автентифікація, авторизація, забезпечення безвідмовності, контроль доступу, забезпечення конфіденційності транзакцій);

- виявлення порушень в області ІБ і процедури відновлення (аудит, виявлення вторгнень, антивірусний захист, перевірка цілісності ПЗ і даних).

Методи нетехнічного рівня – безліч методів керування організаційного і процедурного рівня забезпечення ІБ.

Вибір шкали для оцінки параметрів ризиків.

Під оцінкою параметрів ризиків розуміється оцінка можливості реалізації потенційної вразливості, що приведе до інциденту. Типовою (найбільш розповсюдженою) шкалою є якісна (бальна) шкала з декількома градаціями, наприклад: низький, середній і високий рівень. Оцінка виробляється експертом з урахуванням ряду об'єктивних факторів. Рівні загроз визначаються, наприклад, у такий спосіб (табл. 9) [12, 13].

Таблиця 9

Рівень ризику	Визначення
Високий	Джерело загрози (порушник) має високий рівень мотивації, існуючі методи зменшення вразливості мало ефективні
Середній	Джерело загрози (порушник) має дуже високий рівень мотивації, однак використовуються ефективні методи зменшення вразливості
Низький	Джерело загрози (порушник) має низький рівень мотивації або існують надзвичайно ефективні методи зменшення вразливості

Аналіз можливих наслідків порушення режиму ІБ.

Визначається ціна порушення режиму ІБ. Вибирається система критеріїв для оцінки наслідків порушення режиму ІБ і визначається інтегрована шкала для оцінки ваги наслідків. Приклад шкали приводиться в табл. 10 [12, 13].

Таблиця 10

Рівень важкості наслідків порушення режиму ІБ	Визначення
Високий	Випадок оказує сильний (катастрофічний) вплив на діяльність організації, що виражається у виконання одного або декількох умов
	• Висока вартість прямих фінансових втрат (сума повинна бути конкретизована)
	• Значний ущерб здоров'ю персонала (загибель, інвалідність або необхідність довгочасного лікування співробітника)
	• Втрата репутації, яка приводить к значному зниженню ділової активності організації
	• Дезорганізація діяльності на значний (конкретизується) період часу
Середній	Випадок приводить до негативних результатів, виражаючихся в одному або декількох умовах
	• Помітна вартість прямих фінансових втрат (сума повинна бути конкретизована)
	• Втрата репутації, яка може привести к зменшенню потоку заказів і негативної реакції ділових партнерів
	• Неприємність з боку державних органів, маючих результатом зниження ділової активності компанії
Низький	Випадок приводить до невеликих негативних наслідків, виражаючихся в одному або кількох умовах
	• Невелика вартість прямих фінансових втрат (сума повинна бути конкретизована)
	• Затримки в роботі декотрих служб або дезорганізації діяльності на невеликий період часу
	• Необхідність відновлення інформаційних ресурсів

Оцінка ризиків.

На цьому кроці виміряється рівень ризиків порушення К, Ц, Д інформаційних ресурсів. Рівень ризику залежить від рівнів загроз, вразливостей і ціни можливих наслідків.

Існують різні методики виміру ризиків, наприклад, табличні методи. Якщо використовуються якісні методи, можливі ризики порушення ІБ повинні бути розподілені по ступені їх небезпеки з урахуванням факторів: ціна можливих втрат, рівень загрози й вразливості. Ризики можуть бути

оцінені в кількісних шкалах. Це дає можливість спростити аналіз вартість/ефективність пропонованих контрзаходів. Однак у цьому випадку пред'являються більш високі вимоги до шкал виміру вихідних даних і перевірці адекватності використовуваної моделі.

У найпростішому випадку можна оцінювати ризики по двом факторам**:** ймовірності події і ваги можливих наслідків. Звичайно вважається, що ризик тим вище, чим більше ймовірність події і вага наслідків. У цьому випадку:

$$РИЗИК = P \text{ події} \times \text{Ціна втрати.}$$

Якщо перемінні є кількісними величинами, ризик – це оцінка математичного очікування втрат. Якщо перемінні є якісними величинами, то метрична операція множення не визначена. Таким чином, у явному виді ця формула використовуватися не повинна.

Розглянемо варіант використання якісних величин.

Спочатку повинні бути визначені шкали. Визначатися суб'єктивна шкала імовірностей подій може, наприклад, так:

A – подія практично ніколи не відбувається;

B – подія стається рідко;

C – ймовірність події в розглянутий проміжок часу близько 50 %;

D – швидше за все, подія відбудеться;

E – подія майже напевно відбудеться.

Крім того, визначається суб'єктивна шкала серйозності подій, наприклад:

N (Negligible) – впливом можна зневажити;

Mi (Minor) – незначна подія: наслідки легко переборні, витрати на ліквідацію наслідків не великі, вплив на інформаційну технологію незначний;

Mo (Moderate) – подія з помірними наслідками: їх ліквідація не зв'язана з великими витратами, вплив на IT не великий і не торкає критично важливих задач;

S (Serious) – подія із серйозними наслідками: їх ліквідація зв'язана із значними витратами, вплив на IT відчутний і позначається на виконанні критично важливих задач;

C (Critical) – подія спричиняє неможливість рішення критично важливих задач.

Для оцінки ризиків визначається шкала з трьох значень:

- низький ступінь ризику;
- середній ступінь ризику;
- високий ступінь ризику.

Ризик, зв'язаний з визначеною подією, залежить від двох факторів і може бути визначений як в таблиці 11.

Шкали факторів ризику і сама таблиця можуть бути визначені інакше, мати інше число градацій [12].

Таблиця 11

	Negligible	Minor	Moderate	Serious	Critical
A	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
B	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
C	Низький ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
D	Середній ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
E	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

При розробці (використанні) методик оцінювання ризиків необхідно враховувати ряд особливостей.

- Значення шкал повинні бути чітко визначені і розумітися однаково всіма учасниками процедури експертної оцінки.
- Вимагаються обґрунтування обраної таблиці. Необхідно переконатися, що різні інциденти, що характеризуються однаковими сполученнями факторів ризику, мають з погляду експертів однаковий рівень ризиків.

Для цього існують спеціальні процедури перевірки. Подібні методики широко застосовуються при проведенні аналізу ризиків **базового рівня**.

У методиках, розрахованих на більш високі вимоги, чим базовий рівень, використовується модель оцінки ризику по трьох факторах: загроза, вразливість, ціна втрати.

При цьому ймовірність події, що у даному підході може бути об'єктивною або суб'єктивною величиною, залежить від рівнів (імовірностей) загроз і вразливостей:

$$P \text{ події} = P \text{ загрози} \times P \text{ вразливості}.$$

Відповідно, ризик визначається таким чином**:**

$$РИЗИК = P \text{ загрози} \times P \text{ вразливості} \times Ціна \text{ втрати}.$$

Даний вираз можна розглядати як математичну формулу, якщо використовуються кількісні шкали, або як формулювання загальної ідеї, якщо хоча б одна зі шкал – якісна. В останньому випадку використовуються різного роду табличні методи для визначення ризику в залежності від трьох факторів:

- привабливістю ресурсу (цей показник враховується при розгляді загрози навмисного впливу з боку людини);
- можливістю використання ресурсу для одержання доходу (показник враховується при розгляді загрози навмисного впливу з боку людини);
- простотою використання вразливості при проведенні атаки [5, 11].

3.3 Поліпшена методика аналізу ризику

Головною метою будь-якої системи ІБ є забезпечення стійкого функціонування об'єкта, запобігання загроз його безпеки, захист законних інтересів Замовника від протиправних зазіхань, недопущення розкрадання фінансових засобів, розголошення, утрати, витоку, перекручування і знищення службової інформації. Іншою метою системи ІБ є підвищення якості наданих послуг і гарантій безпеки майнових прав і інтересів клієнтів. Досягнення заданих цілей можливо в ході рішення наступних основних задач:

• віднесення інформації до категорії обмеженого доступу;

• прогнозування і своєчасне виявлення загроз безпеки інформаційним ресурсам, причин і умов, що сприяють нанесенню фінансового, матеріального і морального збитку, порушенню його нормального функціонування і розвитку;

• створення умов функціонування з найменшою імовірністю реалізації загроз безпеки інформаційним ресурсам і нанесення різних видів збитку;

• створення механізму й умов оперативного реагування на загрози ІБ і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних мір і засобів забезпечення безпеки;

• створення умов для максимально можливого відшкодування і локалізації збитку, ослаблення негативного впливу наслідків порушення ІБ на досягнення стратегічних цілей.

Для побудови збалансованої системи ІБ передбачається спочатку провести аналіз ризиків в області ІБ. Потім визначити оптимальний рівень ризику для мережі на основі заданого критерію. Систему ІБ (контрзаходу) має бути побудувати таким чином, щоб досягти заданого рівня ризику.

У ході робіт повинні бути встановлені границі дослідження. Для

цього необхідно виділити ресурси інформаційної системи, для яких надалі будуть отримані оцінки ризиків. При цьому має бути розділити розглянуті ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути засоби обчислювальної техніки, програмне забезпечення, контент. Прикладами зовнішніх елементів є локальні мережі зв'язку, зовнішні сервіси і ін.

При побудові моделі інформаційної системи будуть враховуватися взаємозв'язки між ресурсами. Наприклад, вихід з ладу якого-небудь устаткування може привести до втрати контенту, чи іншого критично важливого елемента системи.

Ця модель, у відповідність із пропонованою методикою, будується в такий спосіб: для виділених ресурсів визначається їхня цінність, як з погляду асоційованих з ними можливих фінансових втрат, так і з погляду збитку репутації організації, дезорганізації її діяльності, нематеріального збитку від розголошення конфіденційної інформації і ін. Потім описуються взаємозв'язки ресурсів, визначаються загрози безпеки й оцінюються ймовірності їхньої реалізації.

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, що знижують ризики до припустимих рівнів і найбільш ефективні. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту.

Забезпечення підвищених вимог до ІБ припускає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів виробляється по завершенні етапу аналізу ризиків і вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму ІБ політиці безпеки, сертифікація інформаційної системи на відповідність вимогам визначеного стандарту безпеки.

У завершення робіт, можна буде визначити міру гарантії безпеки

інформаційного середовища Замовника, засновану на оцінці, з яким можна довіряти інформаційному середовищу об'єкта.

Даний підхід припускає, що велика гарантія випливає з застосування великих зусиль при проведенні оцінки безпеки. Адекватність оцінки заснована на:

• залученні в процес оцінки більшого числа елементів інформаційного середовища об'єкта;

• глибині, що досягається за рахунок використання при проектуванні системи забезпечення безпеки більшого числа описів деталей виконання;

• строгості, що полягає в застосуванні більшого числа інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей чи на зменшення ймовірності їхньої наявності.

Отже визначаються характеристики ризиків в інформаційній системі і її ресурсах. На основі таких даних вибираються необхідні засоби керування ІБ.

Процес оцінювання ризиків містить кілька етапів [8, 12]:

• опис об'єкта і мір захисту;

• ідентифікація ресурсу й оцінювання його кількісних показників;

• аналіз загроз ІБ;

• оцінювання вразливостей;

• оцінювання існуючих і передбачуваних засобів забезпечення ІБ;

• оцінювання ризиків.

Ризик характеризує небезпека, який може піддаватися система і її організація, що використовує, і залежить від:

• показників цінності ресурсів;

• ймовірностей нанесення збитку ресурсам (загроз, що виражаються через ймовірності реалізації, для ресурсів);

• ступеня легкості, з яким вразливості можуть бути використані при виникненні загроз (вразливості системи захисту);


порушник
загроза
Модель порушника розробляється при участі Служби безпеки
Повний перелік загроз: використовуються типові і специфічні для організації загрози ІБ
$P_{ЗАГРОЗИ}$
Оцінка ймовірності виникнення загрози: розробляється на основі переліку загроз і моделі перушника
Вразливості СЗІ
Система захисту інформації (СЗІ)
Повний перелік вразливостей СЗІ: розробляється аналітично з використанням інструментальних досліджень
Фактичний стан СЗІ
$P_{реалізації}$
Ймовірність реалізації загрози
Інформаційні ресурси (ІР)
Цінність ІР
Електронні або бумажні ІР
Оцінка потенційно можливої втрати у випадку реалізації загрози
$P_{втрати}$
Ймовірність матеріальних втрат дорівнюємо ймовірності реалізації загрози, як найгірший випадок
Ризик
Оцінка ризику в ІС для категорій інформації (використовується в подальшому в якості основного критерію)
Висновок
Ітогова оцінка ризику в ІС

Рисунок 6 – Можливий алгоритм оцінювання інформаційних ризиків [12]

• існуючих чи планованих засобів забезпечення ІБ.

Розрахунок цих показників виконується на основі математичних методів, що мають такі характеристики, як обґрунтування і параметри точності методу (рис 6).

У цілому розглянута вище методика дозволяє оцінити чи переоцінити рівень поточного стану ІБ мережі, виробити рекомендації з забезпечення (підвищенню) ІБ, знизити потенційні втрати шляхом підвищення стійкості функціонування мережі, розробити концепцію і політику безпеки, а також запропонувати плани захисту конфіденційної інформації, переданої по відкритих каналах зв'язку, захисту інформації від навмисного перекручування (руйнування), несанкціонованого доступу до неї, чи її копіювання [12].

ВИСНОВКИ

1. Розглянуті особливості побудови системи захисту інформації мереж другого і третього класу загального призначення.

2. Вказане місце ризику в інформаційній системі.

3. Проаналізовані можливі технології керування ризиками.

4. **А**наліз ризиків передбачає визначати: вразливі місця в даній мережі; рівень існуючих загроз; перелік мір, для зниження ризиків до необхідного рівня.

5. Повний варіант аналізу ризиків використовується тільки у випадку високих вимог.

Повний аналіз ризиків, проводиться з використанням програмних засобів і структурних методів системного аналізу і проектування.

6. Застосування інструментальних засобів не є обов'язковим, однак це дозволяє спростити аналіз ризиків і вибір контрзаходів.

7. Відомо безліч методів оцінювання загроз, але не має «кращого» методу, тому що в різних випадках вони будуть різними.

ПЕРЕЛІК ПОСИЛАНЬ

1. НД ТЗІ 2.5-005-99 „Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу”.
2. Богуш В.М., Кудін А.М. Моніторинг систем інформаційної безпеки. Київ: ДУІКТ, 2006. 414 с.
3. Домарев В.В. Безопасность информационных технологий. Системный подход. Київ: ТНД "ДС", 2004. 992 с.
4. «Common Criteria for Information Technology Security Evolution» (Part 1).
5. Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. URL: www.president.gov.ua/documents/962016-19836 (дата звернення 29.11.2022).
6. Низенко Е.І., Каленяк В.П. Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К. : МАУП, 2006. – 134 с.
7. Сірченко Г.А. Оцінка методів підвищення цілісності та доступності інформації в спеціальних системах зв’язку. Захист інформації. Збірник праць НАУ. Вип.17, 2010. С. 321-325.
8. Захист інформації в комп’ютерних системах та мережах : навч. посіб. / С.Г. Семенов, А.О. Подорожняк, О.І. Баленко, С.Ю. Гавриленко – Х.: НТУ «ХПІ», 2014.– 251 с.
9. В.М. Богуш, О.К. Юдін. Основи інформаційної культури. – Київ, 2003.
10. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень: Навчальний посібник. — Запоріжжя: ЗНТУ, 2008. — 341 с.
11. Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 27 січня 2016 року. URL: www.president.gov.ua/documents/962016-19836 (дата звернення 29.11.2022).
12. Анализ рисков в информационных системах, практические аспекты. С.В. Симонов (Защита информации). – Конфидент/март-апрель 2’2001. С. 48-53.
13. Реорганизация корпоративных сетей безопасности. С.А. Петренко. – Конфидент/ март-апрель 1/2002. С. 30-36.
14. Кримінальний кодекс України від 5 квітня 2001 року № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 10.01.2023).

Додаток

Розділ XVI: злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

(Розділ із змінами, внесеними згідно із Законом України від 05.06.2003 р. N 908-IV)

Стаття 361. Незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

1. Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, а так само незаконне втручання в роботу мереж електрозв'язку, що призвело до знищення, перекручення, блокування інформації або до порушення встановленого порядку її маршрутизації, - **караються** штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

2. Ті самі дії, якщо вони заподіяли істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб, - **караються** штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років, або позбавленням волі на строк від трьох до п'яти років.

Примітка. Під істотною шкодою, якщо вона полягає в завданні матеріальних збитків, слід розуміти таку шкоду, яка в триста і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Стаття 362. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем

1. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем - **караються** штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - **караються** штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк.

3. Дії, передбачені частинами першою або другою цієї статті, якщо вони заподіяли істотну шкоду, - **караються** позбавленням волі на строк від двох до п'яти років.

Стаття 363. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем

1. Порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж, - **карається** штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до п'яти років, або виправними роботами на строк до двох років.

2. Те саме діяння, якщо воно заподіяло істотну шкоду, - **карається** штрафом до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.