НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«На правах рукопису»
УДК _____

«До захисту допущено»
Завідувач кафедри
_____ Л.О. Уривський
«___»_____2018 р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Дослідження методів обробки ризиків у системах управління інформаційною безпекою»

Виконав :
студент VI курсу, групи ТС-71мп
Мокій Андрій Володимирович _____

Керівник:
Доцент кафедри
Горицький В.М. _____

Рецензент:
Посада, науковий ступінь, вчене звання,
Прізвище, ініціали _____

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ – 2018

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – другий (магістерський) за освітньо-професійною програмою

Спеціальність (спеціалізація) – 172 «Телекомунікації та радіотехніка» (172.3620.1 «Телекомунікаційні системи та мережі»)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Л.О. Уривський
«___»_____2018 р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Мокію Андрію Володимировичу

1. Тема дисертації «Дослідження методів обробки ризиків у системах управління інформаційною безпекою», науковий керівник дисертації Горицький Віктор Михайлович, доцент кафедри, затверджені наказом по університету від «___»_____ 2018 р. №_____
2. Термін подання студентом дисертації
3. Об’єкт дослідження полягає у процесі оцінки та обробки інформаційної безпеки експертними методами.
4. Предмет дослідження – дослідження експертних методів оцінки ризиків в системі управління інформаційною безпекою.
5. Перелік завдань, які потрібно розробити
6. Орієнтовний перелік графічного (ілюстративного) матеріалу
7. Орієнтовний перелік публікацій

8. Дата видачі завдання

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент Мокій А.В.

Науковий керівник дисертації Горицький В.М.

РЕФЕРАТ

Актуальність. В сучасному світі, що характеризується неосяжним розміром інформаційних ресурсів та даних, якими володіють та мають в своєму розпорядку сучасні організації та підприємства, все більше уваги приділяється проблемам забезпечення захисту даних.

Однією з головних складових сучасних систем інформаційної безпеки (ІБ) є системи управління інформаційною безпекою (СУІБ). В концентрованому вигляді важливі положення та вимоги щодо створення СУІБ, які далі можуть бути оцінені деякими спеціалізованими органами з оцінки відповідності. [5]

Головна задачею забезпечення безпеки інформації все частіше вирішується внаслідок поліпшення процесу управління інформацією на базі реалізації різних підходів і методів, дотримання нормативних вимог і застосування організаційних заходів.

Методологія визначення оцінки ризиків може бути якісною або кількісною, або деякою комбінацією. Якісна оцінка дуже часто використовується для отримання загального рівня ризику і виокремлення головних ризиків. Далі може з’явитися необхідність реалізації більш кількісного або специфічного аналізу стосовно важливих ризиків.

Сучасні інформаційні системи вразливі до цілого ряду загроз, які є результатом виконання несанкціонованого доступу, а також модифікації, викривлення або розкриття інформації. Щоб створити захист інформаційних ресурсів та послуги від можливих загроз, необхідно використати відповідні заходи обробки ризиків та управління безпекою. [12]

Дослідженню процесів обробки, реагування, аналізу та розслідування ризиків інформаційної безпеки присвячено ціла низка публікацій, тому тема роботи є актуальна.

Мета роботи – всебічний аналіз процесу управління ризиками ІБ, узагальненні існуючих методів обробки ризиками та створені адаптованої методики, що забезпечить неперервність та живучість функціонування системи безпеки даних в інформаційних системах.

Для досягнення мети роботи необхідно дослідити наступні задачі:

проаналізувати процеси прийняття рішень в управлінні інформаційній безпеці;

порівняти методи прийняття рішень для підвищення ефективності інформаційної безпеки;

дослідити експертні методи оцінки ризиків в системі управління інформаційною безпекою.

Об’єкт дослідження полягає у процесі оцінки та обробки інформаційної безпеки експертними методами.

Предмет дослідження – дослідження експертних методів оцінки ризиків в системі управління інформаційною безпекою.

Практична цінність полягає в розробці методики прийняття рішення в системі управління інформаційною безпекою. Ідентифікація критеріїв ризику визначає прийняття рішень щодо характеру можливих наслідків та способу їх вимірювання. При визначенні критеріїв необхідно визначити за якими критеріями прийматимуться рішення щодо необхідності оброблення ризику та критерії, за якими будуть прийматися рішення щодо допустимості чи прийняття ризику.

Для того, щоб побудувати систему кібербезпеки, комплексну систему захисту даних або інших систем безпеки, потрібно провести аналіз і оцінювання ризиків. Наявні на сьогодні методи оцінки ризиків в переважній

кількості засновані на статистичних підходах. У більшості країн подібна статистика не ведеться, як на державному рівні, так і на рівні підприємств. Саме це обмежує можливості засобів оцінки, наприклад відсутність інформації для використання вхідних даних для оцінки ризику.

Загальне оцінювання ризику дає змогу впроваджувати необхідні міри на рівні підрозділів, проектів, конкретних ризиків або на рівні організації в цілому. Після завершення загального оцінювання ризику провадять обробляння ризику, що передбачає прийняття одного чи декількох підходящих варіантів, які дають можливість зменшити ймовірність виникнення ризиків та їх вплив на систему.

Таким чином, у випускній роботі, що має практичне і наукове значення, досліджуються вже існуючі методи обробки ризику інформаційної безпеки та їх адаптація і впровадження на підприємствах.

ABSTRACT

Topicality. In today's world, characterized by the immense amount of information resources and data that modern organizations and enterprises possess and have at their disposal, more and more attention is paid to the problems of data protection.

One of the main components of modern information security systems (IS) is the Information Security Management System (ISMS). In a concentrated form, important provisions and requirements for the creation of the ISIS, which can then be assessed by some specialized conformity assessment bodies. [5]

The main task of ensuring the security of information is increasingly solved as a result of improving the information management process based on the implementation of different approaches and methods, compliance with regulatory requirements and the application of organizational measures.

The methodology for determining risk assessment can be qualitative or quantitative, or some combination. A qualitative assessment is often used to obtain a general level of risk and distinguish the main risks. Further, there may be a need for more quantitative or specific analysis of important risks.

Modern information systems are vulnerable to a variety of threats that result from unauthorized access, modification, distortion or disclosure. In order to protect information resources and services from potential threats, appropriate risk management and security management measures should be used. [12]

A wide range of publications is devoted to the study of processes of processing, reacting, analyzing and investigating information security risks, so the topic of work is relevant.

The purpose of the work. Is a comprehensive analysis of the risk management process of IBs, generalization of existing methods of risk management, and the

creation of an adapted methodology that will ensure the continuity and survivability of the operation of the data security system in information systems.

In order to achieve the goal of the work, the following tasks should be investigated:

- analyze decision-making processes in the management of information security;
- compare decision-making methods to increase the effectiveness of information security;
- to investigate expert methods of risk assessment in the information security management system.

The object of the study - is the process of evaluation and processing of information security by expert methods.

Subject of research - research of expert methods of risk assessment in the system of information security management.

The practical value is to develop a decision-making technique in the information security management system. Identification of risk criteria determines decision-making on the nature of possible consequences and how to measure them. In determining the criteria, it is necessary to determine what criteria will be used to decide on the need for risk management and the criteria by which decisions on admissibility or acceptance of risk will be made.

In order to build a cybersecurity system, an integrated system for data protection or other security systems, it is necessary to analyze and evaluate the risks. Available today methods of risk assessment in the vast majority are based on statistical approaches. In most countries, such statistics are not conducted, both at the state level and at the enterprise level. That is precisely what restricts the capabilities of the assessment tool, such as the lack of information to use input for risk assessment.

A general risk assessment allows you to implement the necessary measures at the level of subdivisions, projects, specific risks or at the organization level as a

whole. Upon completion of the overall risk assessment, the risk is treated, which involves the adoption of one or several suitable options that reduce the risk of occurrence and their impact on the system.

Thus, in the final work of practical and scientific significance, existing methods of information security risk management and their adaptation and implementation at enterprises are investigated.

ЗМІСТ

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АЗ – апаратне забезпечення

БД – база даних

БЗ – база знань

ЕР – елементи ризику

ЗОТ – засоби обчислювальної техніки

ІБ – інформаційна безпека

ІС – інформаційна система

ІТ – інформаційна технологія

ОІБ – організація інформаційної безпеки

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

ПР – правила для ризиків

СВ – структури впливу

СУІБ – система управління інформаційною безпекою

ФВ – фактори впливу на загрози

ВСТУП

Актуальність. В сучасному світі, що характеризується неосяжним розміром інформаційних ресурсів та даних, якими володіють та мають в своєму розпорядку сучасні організації та підприємства, все більше уваги приділяється проблемам забезпечення захисту даних.

Однією з головних складових сучасних систем інформаційної безпеки (ІБ) є системи управління інформаційною безпекою (СУІБ). В концентрованому вигляді важливі положення та вимоги щодо створення СУІБ, які далі можуть бути оцінені деякими спеціалізованими органами з оцінки відповідності. [5]

Головна задачею забезпечення безпеки інформації все частіше вирішується внаслідок поліпшення процесу управління інформацією на базі реалізації різних підходів і методів, дотримання нормативних вимог і застосування організаційних заходів.

Методологія визначення оцінки ризиків може бути якісною або кількісною, або деякою комбінацією. Якісна оцінка дуже часто використовується для отримання загального рівня ризику і виокремлення головних ризиків. Далі може з’явитися необхідність реалізації більш кількісного або специфічного аналізу стосовно важливих ризиків.

Сучасні інформаційні системи вразливі до цілого ряду загроз, які є результатом виконання несанкціонованого доступу, а також модифікації, викривлення або розкриття інформації. Щоб створити захист інформаційних ресурсів та послуги від можливих загроз, необхідно використати відповідні заходи обробки ризиків та управління безпекою. [12]

Дослідженню процесів обробки, реагування, аналізу та розслідування ризиків інформаційної безпеки присвячено ціла низка публікацій, тому тема роботи є актуальна.

Мета роботи – всебічний аналіз процесу управління ризиками ІБ, узагальненні існуючих методів обробки ризиками та створені адаптованої методики, що забезпечить неперервність та живучість функціонування системи безпеки даних в інформаційних системах.

Для досягнення мети роботи необхідно дослідити наступні задачі:

проаналізувати процеси прийняття рішень в управлінні інформаційній безпеці;

порівняти методи прийняття рішень для підвищення ефективності інформаційної безпеки;

дослідити експертні методи оцінки ризиків в системі управління інформаційною безпекою.

Об’єкт дослідження полягає у процесі оцінки та обробки інформаційної безпеки експертними методами.

Предмет дослідження – дослідження експертних методів оцінки ризиків в системі управління інформаційною безпекою.

Практична цінність полягає в розробці методики прийняття рішення в системі управління інформаційною безпекою. Ідентифікація критеріїв ризику визначає прийняття рішень щодо характеру можливих наслідків та способу їх вимірювання. При визначенні критеріїв необхідно визначити за якими критеріями прийматимуться рішення щодо необхідності оброблення ризику та критерії, за якими будуть прийматися рішення щодо допустимості чи прийняття ризику.

Для того, щоб побудувати систему кібербезпеки, комплексну систему захисту даних або інших систем безпеки, потрібно провести аналіз і оцінювання ризиків. Наявні на сьогодні методи оцінки ризиків в переважній кількості засновані на статистичних підходах. У більшості країн подібна статистика не ведеться, як на державному рівні, так і на рівні підприємств.

Саме це обмежує можливості засобів оцінки, наприклад відсутність інформації для використання вхідних даних для оцінки ризику.

Загальне оцінювання ризику дає змогу впроваджувати необхідні міри на рівні підрозділів, проектів, конкретних ризиків або на рівні організації в цілому. Після завершення загального оцінювання ризику провадять обробляння ризику, що передбачає прийняття одного чи декількох підходящих варіантів, які дають можливість зменшити ймовірність виникнення ризиків та їх вплив на систему.

Таким чином, у випускній роботі, що має практичне і наукове значення, досліджуються вже існуючі методи обробки ризику інформаційної безпеки та їх адаптація і впровадження на підприємствах.

РОЗДІЛ 1. ТЕХНОЛОГІЯ ПРИЙНЯТТЯ РІШЕНЬ У СИСТЕМАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Основні функції теорії прийняття рішень

Теорія – філософська категорія для позначення розвитку системи знань, що вірогідно та адекватно відбивають сутність і закономірності явищ певної області об'єктивної дійсності й виступають як керівництво для практичної діяльності. За аналогією з цим визначенням під теорією прийняття рішень (ТПР) треба, імовірно, розуміти систему знань, що відбивають сутність понять «рішення» і «закономірність», з урахуванням яких вони (рішення) розробляються, приймаються і реалізуються на практиці, а також принципах, організаційних формах, методах і технологіях функціонування системи прийняття рішень в організації. Основними рисами ТПР повинні бути «об'єктивна істина, логічна цілісність, формальна несуперечність, здатність розвитку, відносна самостійність, активний вплив на практику». [15]

Теорія прийняття рішень досліджує свій предмет з різних сторін, що становлять окремі, але взаємозалежні аспекти. До основних з них можна віднести методологічні, організаційні, економічні, технологічні, соціально-психологічні та правові.

Як і будь-яка інша наукова теорія, теорія прийняття рішень виконує пізнавальну і прогнозуючу функції. Пізнавальна функція проявляється в розкритті сутності процесів прийняття рішень, закономірностей і принципів, яким вона підкоряється, виникненні та розвитку ТПР на різних історичних етапах, поясненні основних властивостей і взаємозв'язків предмета дослідження, обґрунтуванні технології та системи прийняття рішення. Прогнозуюча функція ТПР полягає у визначенні тенденцій

подальшого розвитку процесів і системи прийняття рішення, організаційних форм і методів діяльності в процесі прийняття рішення.

При цьому основними завданнями теорії прийняття рішення є:

-вивчення і узагальнення досвіду прийняття рішень в умовах визначеності, невизначеності та ризику;

-виявлення і дослідження об’єктивних закономірностей, що властиві процесам прийняття рішень, а також формування на їхній основі принципів організації діяльності, організаційних форм і методів, технологій розробки, прийняття і реалізації рішень;

-формування практичних рекомендацій з роботи системи при прийнятті рішень у реальних умовах складної обстановки шляхом застосування програмно-технічних засобів систем автоматизації;

-розроблення методів дослідження проблем розвитку системи прийняття рішень, принципів і методів оцінювання їх ефективності, а також заходів щодо вдосконалювання процесу діяльності. [6]

Рішення – це вибір альтернативи. Прийняття рішень – сполучний процес, необхідний для виконання будь-якої функції в умовах:

повної визначеності апріорної вихідної інформації, коли точно відомо результат, який має бути отриманий на виході;

ризику (імовірної визначеності апріорної вихідної інформації), коли приймаються рішення, як правило, з певною вірогідністю;

невизначеності апріорної вихідної інформації, коли встановлюється ймовірність можливих наслідків здебільшого на основі власного досвіду.

В науковій літературі процес прийняття рішень розглядається, як правило, у двох аспектах – широкому та вузькому. У широкому розумінні прийняття рішень ототожнюється з усім процесом інформаційної безпеки – ходом його виконання і контролю результатів. У вузькому воно трактується, як вибір

найкращого рішення з багатьох можливих альтернатив. Враховуючи таке, поняття «прийняття рішень» може бути визначено як процес, який починається з виникнення проблемної ситуації і закінчується вибором рішення, тобто вибором дій з її усунення. Місце такої діяльності у загальному процесі можна представити блок-схемою, поданою на рис. 1.1.

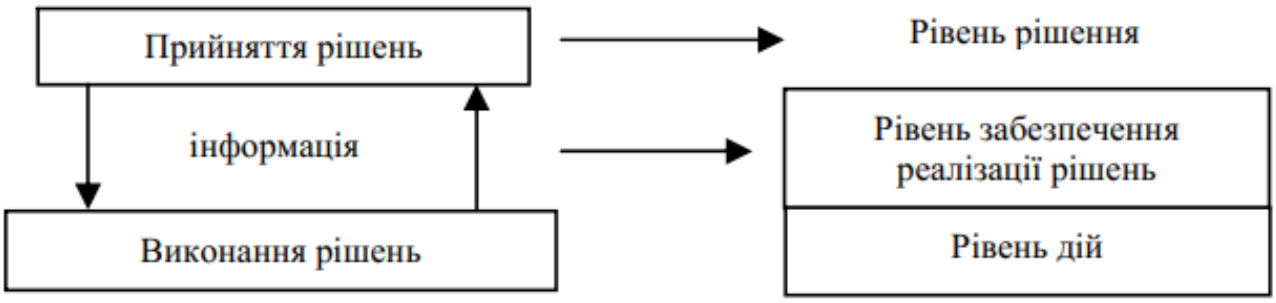

Рисунок 1.1 Місце прийняття рішень в процесі інформаційної безпеки

Кінцевим результатом прийняття рішення є саме рішення, яке постає як первісний, базовий елемент, що забезпечує функціонування будь-якої системи інформаційної безпеки за рахунок взаємозв'язку формальних і неформальних, інтелектуальних та організаційно-практичних аспектів. Фактично воно є важливою ланкою формування і реалізації відношень в системах безпеки, а також інструментом впливу на певний об'єкт та його окремі підсистеми. [20]

При цьому, як інструмент впливу, будь-яке рішення:

- формується на основі аналізу стану об'єкта за критеріями цілей, ресурсів та ефективності;
- прописується у межах встановлених норм та регламентів, які існують в системі;
- є виразом впливу суб'єкта на об'єкт системи безпеки.

При формуванні та обґрунтуванні рішення, що має бути прийняте, доволі часто постає питання – як зробити цей процес більш комфортним, технологічним, а саме головне, ефективним. [14]

У цей час існує безліч технологій, що дають можливість суттєво полегшити життя та допомогти у рішенні проблем, пов'язаних з процесами прийняття рішень у різних предметних (прикладних) галузях.

Найбільш простою серед них є *інтуїтивна технологія* прийняття рішень. Вона передбачає, що рішення визначається досвідом, накопиченим інформаційною системою у подібних ситуаціях. Основним критерієм при цьому є забезпечення найменших збитків для досягнення певної мети. Тобто, якщо раніше аналогічні рішення не приймалися – вірогідність прийняття помилкового рішення суттєво зростає. [19]

Головними етапами інтуїтивної технології є: реєстрація змін; селекція рішень, що знаходяться у пам'яті системи та прийняття рішення. Її перевага полягає у швидкості прийняття рішень, недолік – у великій вірогідності помилки.

Більш складною порівняно з інтуїтивною є *раціональна технологія* прийняття рішень (рис. 1.2), фактична кількість етапів (кроків), операцій і процедур якої визначається складністю і типом розв'язуваної проблеми.

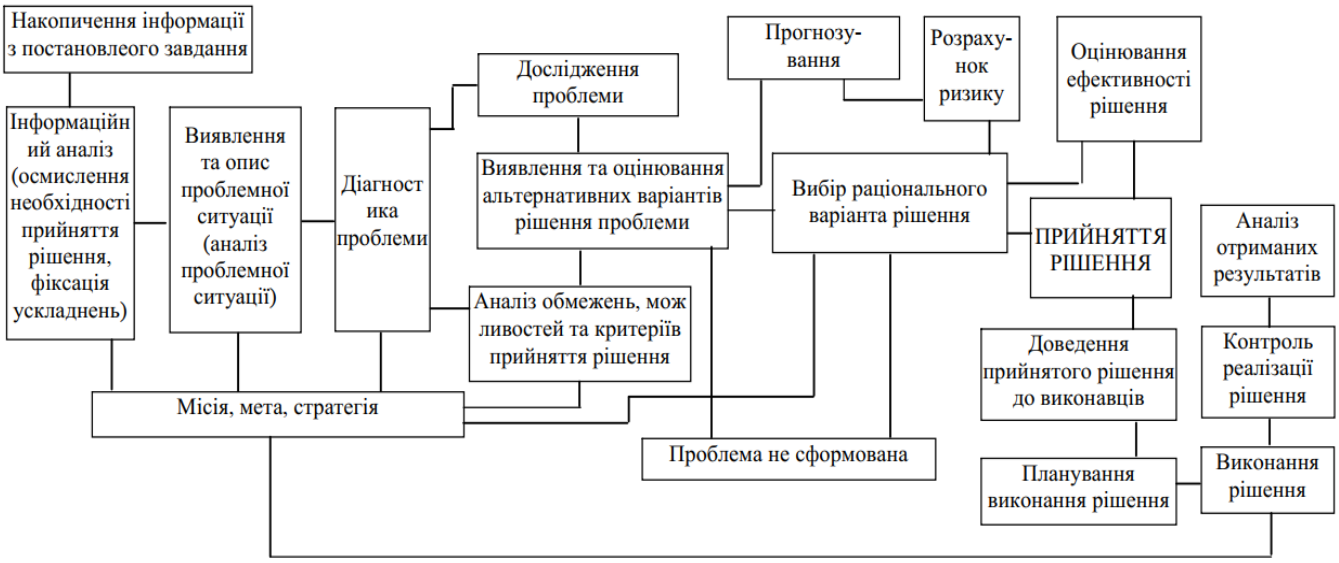

Рисунок 1.2 Етапи прийняття раціонального рішення

При цьому важливим і безперечно головним етапом при вирішенні проблеми – накопичення даних. Етап включає обробку і збір різноманітних інформаційних відомостей, матеріалів, знань та даних, що мають конкретне відношення до проблемної ситуації. Слід виокремити його головну важливість, оскільки рівень якості рішення проблеми повністю залежить від рівня якості апріорних даних про неї.

Головне завдання даного етапу – своєчасне знаходження сигналів ускладнень у діяльності певного об’єкта; підготовче визначення причин, що цьому допомагають; оповістка про виявлені ускладнення осіб, які мають право приймати рішення. [9]

Другий етап – аналіз та опис проблемної ситуації. Мета етапу – визначення ситуації проблемного характеру, що проявився як наслідок впливу

зовнішніх факторів, неврахованих суб'єктивною діяльністю або прогнозом системи безпеки. При цьому відбираються релевантні дані.

Третій етап – діагноз проблеми. Він включає наступні підетапи: опис та виявлення проблемної ситуації (вираження і усвідомлення у будь-якій спосіб протиріччя між несталим характером впливу внутрішніх та (або) зовнішніх чинників на систему, а також перспективами системи забезпечити здобутки в цих умовах); визначення мети розв'язання проблемної ситуації (визначення необхідного кінцевого результату розв'язання проблемної ситуації); визначення критеріїв прийняття рішення (отримання ознак, на базі яких створюється оцінювання шансу вирішення проблемної ситуації і упорядкування їх за рівнем важливості). [10]

На базі вхідної як внутрішньої, так і зовнішньої інформації фіксуються симптоми ускладнень та проводиться оцінка причини виникнення проблемної ситуації. Для оптимізації засобів і робіт на даному етапі намагаються не допускати надлишку даних й здійснювати збір тільки даних, які відповідають даному релевантному стану.

Четвертим етапом є формування множини альтернативних варіантів вирішення проблемної ситуації. Етап передбачає розробку, опис та складання переліку усіх можливих варіантів дій, що забезпечують вирішення проблемної ситуації. При цьому в процесі формування множини припустимих альтернатив з метою обмеження їх кількості необхідно враховувати такі вимоги до них: взаємовиключність (вибір можливий лише у випадку, коли альтернативи взаємно виключають одна одну); забезпечення однакових умов опису альтернатив (ресурсних, часових та інших). [26]

Для цього визначається діапазон (інтервал) у межах якого має прийматися рішення та визначаються стандарти (критерії його ухвалення), що дозволять оцінити альтернативні варіанти вибору.

Головними серед таких є:

- критерій задовільності (враховує можливості системи управління);
- критерій реалістичності (враховує навколишні обставини, незалежні від самої системи управління);
- критерій прийнятності наслідків реалізації.

На п’ятому етапі оцінюються альтернативні варіанти. Етап полягає у підборі та перевірці припустимих альтернатив з урахуванням відповідних обмежень на підставі проведених прогнозів, а також визначенні можливого ризику та імовірності реалізації кожної. Кінцевим результатом роботи є з’ясування системними аналітиками головних переваг порівнюваних альтернатив за певною проблемою. У цьому випадку існує небезпека, що частина кращих альтернатив може бути упущена.

При цьому на процес прийняття рішення здебільшого впливають:

- рівень ризику;
- можливість негативних наслідків;
- взаємозалежність рішень на різних рівнях ієрархії.

Шостий етап полягає у прийнятті рішення, тобто порівнянні альтернатив та виборі кращої з них на підставі критеріїв, ідентифікованих на четвертому етапі формування рішення. При цьому використовуються результати аналітичних розрахунків різних варіантів, можливих або припустимих ризиків. На цьому етапі формується судження про переваги альтернативних варіантів досягнення певної мети. При сумніві у виборі найкращої альтернативи проводиться експериментальна перевірка отриманих результатів. [11]

При цьому під раціональним рішенням розуміють таке допустиме рішення, за якого цільова функція $W = F[x1, x2,..., xn]$ за обмежень $Gi (x1, x2,..., xn) \geq 0$, $i = 1..m$ приймає максимальне або мінімальне значення. Для рішення цієї задачі застосовують такі відомі методи, як методи оптимізації цільової

функції та методи оптимізації цільового функціонала, класифікація яких являє собою надто складну задачу, носить умовний характер й тому, істотно, має явні недоліки. Так, наприклад, в класичних методах оптимізації серед обмежень відсутні нерівності, відсутні умови не позитивності та дискретності змінних, а цільова функція F[x1, x2 ,..., xn] та функції обмеження Gi (x1, x2,..., xn) ≥ 0 безперервні й мають часткові похідні як мінімум другого порядку.

Сьомим етапом є доведення рішень. Він полягає у передаванні змісту рішення систему управління інформаційною безпекою, перевірка одержаної інформації та за необхідності – зміна їх повноважень. Структура, зміст рішення та особливості його наступної реалізації визначається рівнем ієрархії, де воно прийнято. Восьмий етап передбачає спільне організаційне планування виконання рішення тобто розробку планів графіків виконання робіт, визначених для системи із залученням останніх. Дев'ятий етап – етап виконання рішення, передбачає здійснення дій, виконання розроблених оперативних та організаційних планів. На десятому етапі – етапі контролю, за рахунок розробки ефективного механізму проміжного і фінального контролю, забезпечують необхідною інформацією про хід виконання рішення. На останньому, одинадцятому етапі шляхом співставлення цілей, сформульованих в прийнятому рішенні аналізуються отримані результати, причини успіху (невдачі) та здійснюються заходи з оцінювання його ефективності.

1.2 Процеси та методи прийняття рішення

Процеси прийняття рішень у сферах інформаційної безпеки багато в чому аналогічні. Тому переважна більшість систем управління повинна мати універсальний метод їх формування та підтримки реалізації. З цією метою

процес підготовки прийняття рішення на всіх його етапах супроводжується кількісним вираженням таких категорій як «перевага», «важливість», «бажаність» тощо. Сукупність категорій становить певну структуру понять, у якій одні категорії, відбиваючи найбільш узагальнені поняття і зв'язки, є вузловими, опорними, інші є частиною більш загальної категорії. Представлений на рисунку 1.3 взаємозв'язок категорій дає можливість виділити мету та структуру системи управління.

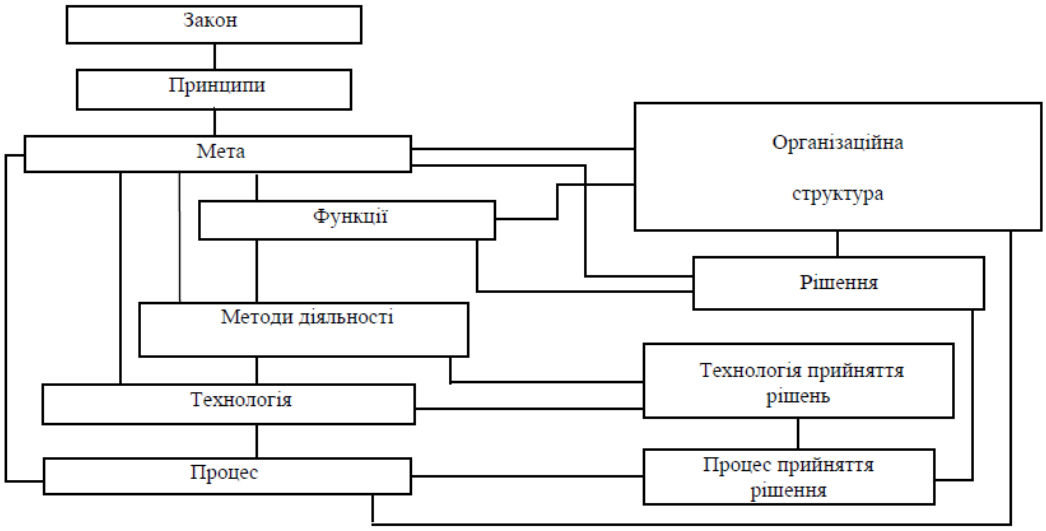

Рисунок 1.3 Взаємозв'язок категорій системи управління та теорії прийняття рішень

Мета, будучи важливою категорією процесу прийняття рішень, визначає функції і методи, а також хід формування, прийняття, реалізації та оцінювання рішень (рис. 1.4) й тому багато в чому впливає на ефективність останніх.

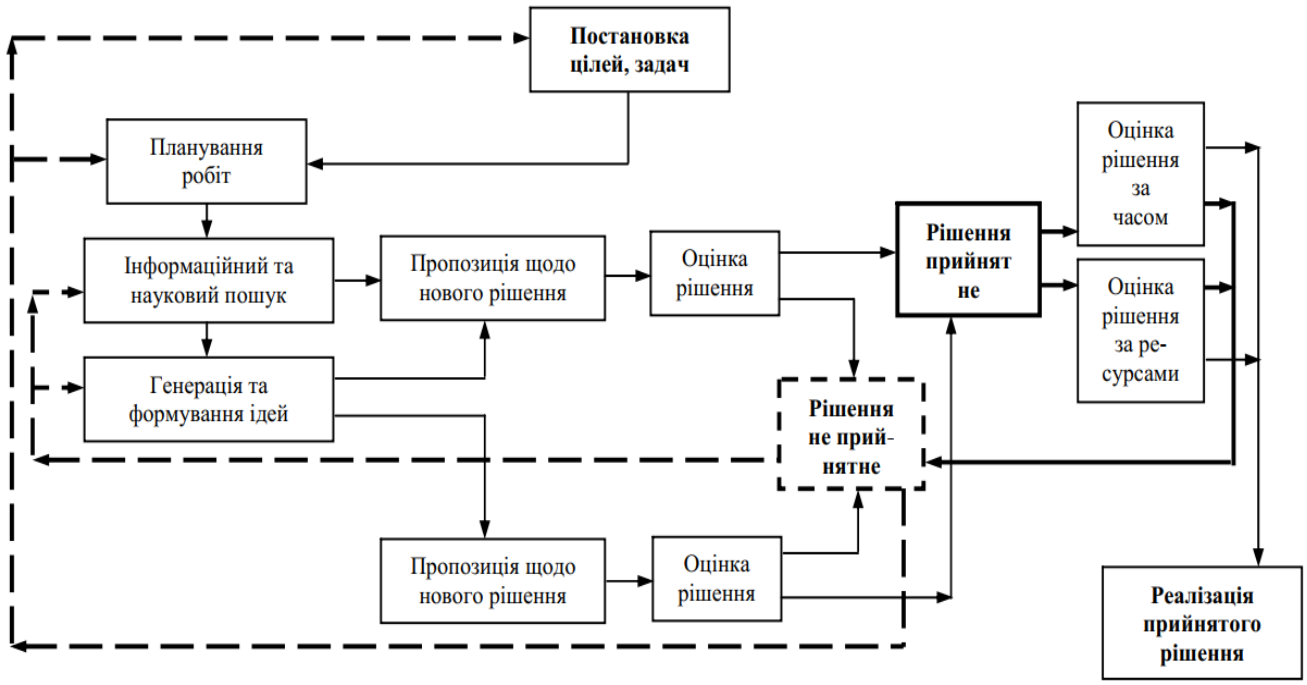

Рисунок 1.4 Процес прийняття рішень та його оцінювання

Власне хід формування, прийняття, реалізації та оцінювання рішень передбачає проведення заходів з:

- оцінювання показників об’єктів дослідження за кількісною шкалою;
- віднесення конкретного об’єкта дослідження до конкретної категорії за порядковою шкалою;
- групового оцінювання деякої множини об’єктів дослідження;
- виділення підмножини найкращих об’єктів з множини можливих. [19]

Перша і друга задачі є типовими для оцінювання альтернатив і прийняття рішень. Вони, як правило, полягають у виборі або відхиленні декількох варіантів з множини можливих. Третя задача безпосередньо відповідає типовому завданню прийняття рішення – упорядкованому розподілу альтернатив (кожний із розглядуваних варіантів ураховується в цьому випадку відповідно до його пріоритету). Четверта задача в деяких випадках розглядається як частковий випадок третього. При цьому кожна з наведених вище задач може бути розглянута в такий спосіб. Припустимо, що:

1) існує декілька однотипних альтернатив (об’єктів, дій і т.п.);

2) визначений головний критерій порівняння альтернатив;

3) обрано декілька груп однотипних факторів (часткових критеріїв), що відомим чином впливають на відбір альтернатив.

Кожній альтернативі необхідно поставити у відповідність пріоритет (число), тобто сформувати рейтинг альтернатив. Причому чим більш кращою є альтернатива за обраним критерієм, тим вищим буде її пріоритет. [23]

При виборі метода рішення конкретної задачі (рис. 1.5) враховуються, як правило, такі основні фактори: відповідність обираємого методу об’єктивним характеристикам вирішуваної задачі (варіант постановки задачі, умови та множина альтернативних рішень, кількість критеріїв та їх взаємозв’язок тощо); урахування об’єктивних (часових, обчислювальних) та суб’єктивних чинників.

Вважають, що рішення приймається в умовах повної визначеності, якщо мають повні і точні дані про ефективність кожного з можливих варіантів дії. Проблема може бути тільки у великій кількості можливих варіантів та відсутності зайвого часу на їхній аналіз. Такі задачі формулюються як оптимізаційні і вирішуються методами лінійного, нелінійного, динамічного і дискретного програмування. [4]

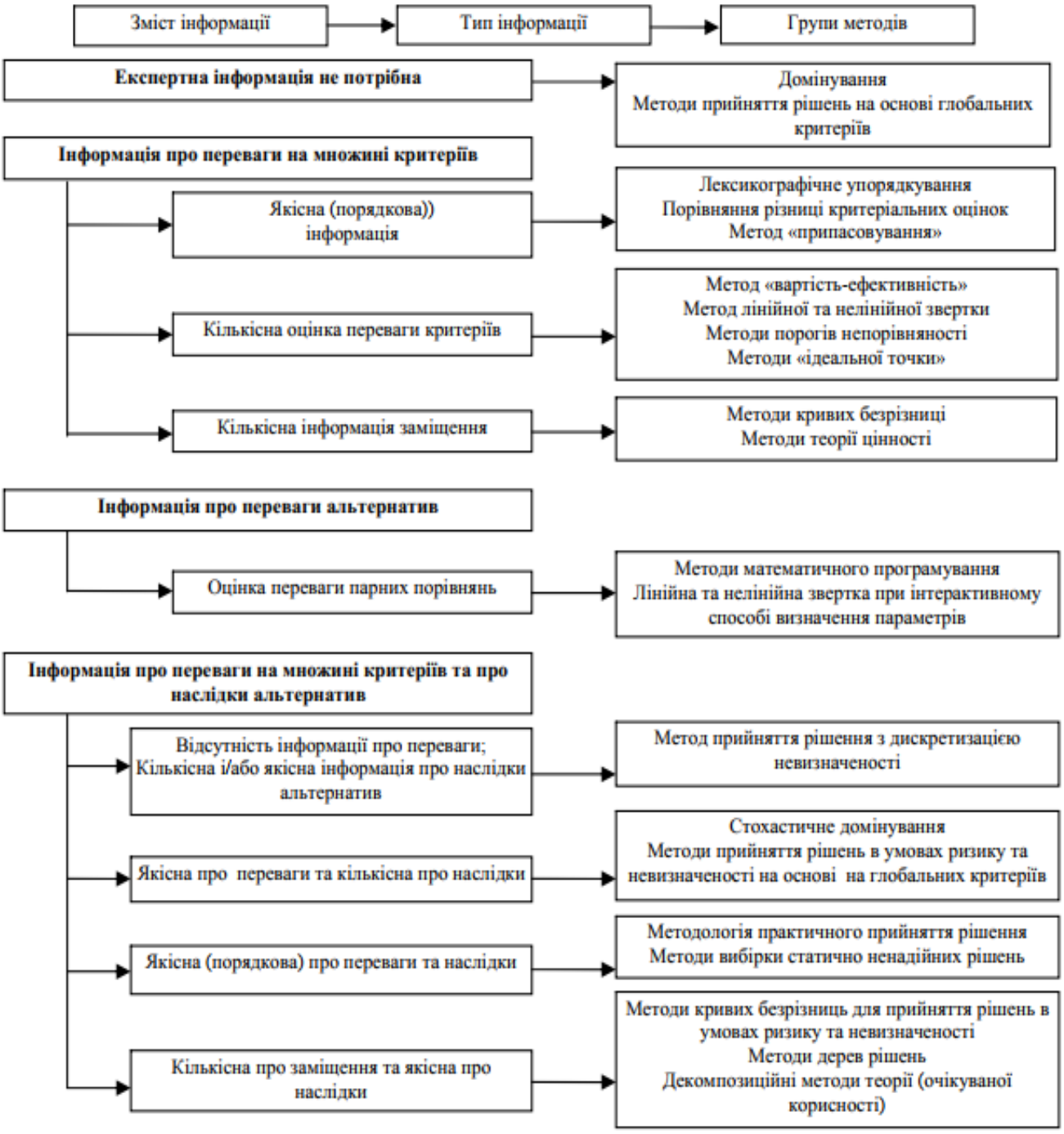

Рисунок 1.5 Класифікація методів прийняття рішень

Класифікацію методів прийняття рішень в умовах визначеності можна представити таким чином:

- методи на основі глобальних критеріїв домінування (експертна інформація не потрібна);

- методи лексикографічного впорядкування шляхом порівняння різниць критеріальних оцінок (використовується якісна впорядкована інформація про перевагу критеріїв);
- метод «ефективність-вартість», лінійна та нелінійна згортки, методи порогів непорівнянності та “ідеальної точки” (використовується якісна (впорядкована) інформація про перевагу критеріїв);
- методи кривих безрізниці та методи теорії цінності (використовується якісна впорядкована інформація про заміщення при визначенні переваги критеріїв);
- людино-машинні процедури на базі математичного програмування, а саме лінійна та нелінійна звертки при інтерактивному способі визначення параметрів (використовується оцінка переваги парних порівнянь при визначенні переваги критеріїв). [18]

Рішення приймається в умовах ризику, якщо у момент прийняття рішення не відомо в яких саме умовах буде функціонувати об’єкт, однак відомо імовірності появи тих або інших умов. Імовірності появи умов можна знайти статистичними методами на підставі тривалих спостережень або досліджень.

Рішення приймається в умовах невизначеності, якщо відома ефективність варіантів побудови або функціонування досліджуваного проекту, але не має інформації про поводження зовнішнього середовища. При описі складних систем, наприклад, розрізняють невизначеності цільової функції, невизначеності середовища та невизначеності системи. Невизначеність цільової функції проявляється у випадку неможливості подання мети системи у вигляді скалярної цільової функції. Невизначеності системи викликані неповною інформації про їхні стани. [25]

Таким чином сутність задачі прийняття рішень полягає у виборі деякої підмножини з безлічі альтернатив (альтернативних рішень) або в їхньому

упорядкуванні. При цьому рішенням називають обрану підмножину або упорядковану множину альтернатив, раціональним рішенням – рішення, що за певним критерієм (критеріями) дає можливість вирішити поставлене завдання, ухваленням рішення – акт вибору або упорядкування, а відповідну процедуру – процедурою прийняття рішень. [17]

Основні моделі прийняття рішень

Існують три основні моделі прийняття рішень:

- класична модель;
- поведінкова модель;
- ірраціональна модель.

Класична модель спирається на поняття «раціональності» у прийнятті рішень. Передбачається прийняття рішення повинна бути об’єктивним і логічним, мати чітку ціль, а усі її дії в процесі прийняття рішень мають бути спрямовані на вибір найкращої альтернативи.

Отже, основні характеристики класичної моделі є такими:

існує чітка ціль щодо прийняття рішення;

повна інформація відносно ситуації, що склалася;

повна інформація відносно можливих альтернатив і наслідків їх реалізації;

раціональна система впорядкування переваг в ієрархії важливості;

мета завжди полягає у тому, щоб здійснити такий вибір, який надав би системі управління максимальний ефект.

Діяти згідно з поданою моделлю можна в умовах наявності повного масиву інформації, що є достатньо проблематичним на практиці. Крім того, значний вплив на прийняття рішень можуть спричинити суб’єктивні фактори. [2]

Поведінковій моделі притаманні у свою чергу такі основні характеристики:

неповна інформація відносно ситуації прийняття рішення;

неповна інформація відносно можливих альтернатив;

не має можливості передбачити наслідки реалізації кожної можливої альтернативи.

Ірраціональна модель базується на припущенні, що система в більшості ірраціональна у процесі прийняття рішень. Цей підхід орієнтований на те, що рішення приймається задовго до того, як досліджуються альтернативи. Використовується така модель частіш за все у випадках, які стосуються принципово нових, складно вирішуваних і надзвичайних рішень. [12]

1.3 Порівняльний аналіз методів прийняття рішень в системах управління інформаційною безпекою

Існує безліч класифікацій методів і моделей прийняття рішень, заснованих на застосуванні різних ознак. При класифікації кожен з елементів може служити її ознакою і характеризуватися такими властивостями:

По виду відображення. Відображення може мати детермінований характер, імовірнісний або невизначений вид, відповідно до чого завдання прийняття рішень можуть бути розділені на завдання в умовах ризику і завдання в умовах невизначеності.

За насиченістю. Множина критеріїв вибору може містити один елемент або кілька, що дає підставу визначити завдання прийняття рішень як завдання зі скалярним критерієм або завдання з векторним критерієм (багатокритеріальне прийняття рішень)

За типом системи переваги. Переваги можуть формуватися однією особою або колективом, і в залежності від цього завдання прийняття рішень можна класифікувати на завдання індивідуального прийняття рішень і завдання колективного прийняття рішень. [27]

Методи і моделі індивідуального прийняття рішень при багатьох критеріях можна розділити на наступні основні групи:

Блоки першої групи:

- лексикографічні методи;
- аксіоматичні методи багатокритеріальної теорії корисності;
- методи порівняння багатовимірних альтернатив (методи домінування, компенсації, порогів непорівнянності).

Блоки другої групи:

- методи побудови узагальненого критерію;
- вербальні методи;
- методи теорії нечітких множин;
- інтелектуальні методи.

Методи прийняття колективних рішень можна розділити на наступні групи:

Блоки першої групи:

- методи колективного безконфліктного вибору;
- методи групового вибору;
- методи кооперації.

Блоки другої групи:

- динамічні методи колективного вибору в конфліктних ситуаціях;
- задачі про призначення;
- методи формування колективної поведінки.

Використовуваний принцип класифікації дозволяє наочно, досить чітко виділити чотири великі групи методів, причому три групи відносяться до прийняття рішень в умовах визначеності, а четверта – до прийняття рішень в умовах невизначеності. [16]

В області теорії прийняття рішень за останні роки опубліковано багато наукових робіт, присвячених як вибору варіантів при створенні системи управління інформаційної безпеки, так і безпосередньо розвитку методів теорії прийняття рішень. Серед них можна відзначити методи теорії

прийняття рішень, що включають методи аналізу ієрархій і аналітичних мереж, методи, засновані на теорії нечітких множин, метод кластерного аналізу та комбінаторно-морфологічного аналізу і синтезу систем, евристичні методи пошуку нових рішень, інтелектуальні методи і системи для підтримки процедур прийняття стратегічних рішень та методи теорії корисності і теорії ігор. [18]

Аналіз літератури з теорії прийняття рішень та науково-технічної літератури з проектування системи управління інформаційної безпеки показав, що при виборі основних напрямків розвитку об'єктів інформаційної безпеки, в тому числі при оцінці їх технічного рівня можуть бути використані такі методи прийняття рішень:

- методи згортки векторного критерію;
- метод мінімізації поступок;
- метод оптимізації по домінуючому критерію;
- методи ранжування (метод парних (бінарних) відносин), метод послідовних поступок);
- метод вагових коефіцієнтів;
- метод ідеальної точки;
- метод ЕЛЕКТРА;
- метод аналізу ієрархій;
- статистичні методи оцінки (кореляційний аналіз та регресійний аналіз);
- спектральний метод ранжування альтернативних варіантів;
- метод аналізу ієрархій;
- метод нечіткого відношення переваги;
- метод переваги;
- метод вирішальних матриць;

- метод документацій;
- метод тестів;
- метод Парето;
- метод оцінки несуперечності суджень,
- метод змішаної альтернативи;
- метод узгодження оцінок;

експертні методи (метод Дельфі, метод комісій, метод суду, метод «мозкової атаки» або «мозкового штурму», або «колективної генерації ідей» і різновиди – індивідуальний «мозковий штурм», масовий «мозковий штурм», письмовий «мозковий штурм», подвійний «Мозковий штурм», зворотний «мозковий штурм», конференція ідей); метод взаємної оцінки і самооцінки, метод складних експертиз). [31]

У таблиці 1.1 наведені в стислому вигляді основні властивості відомих експертних методів прийняття рішення, які широко використовуються на практиці.

Таблиця 1.1 Порівняльний аналіз методів прийняття рішень

Назва методу	Сутність методу	Сфери застосування	Переваги методу	Недоліки методу	Примітка
1. Метод суду	Робота колективу Експертів здійснюється згідно з правилами ведення судового процесу	Вибір найкращої альтернативи	Процедура розгляду обговорюваного питання дозволяє виявити слабкі і сильні сторони кожної альтернативи, складність організації процесу	Прийняття рішення за оцінкою альтернатив	Метод корисний при наявності декількох підгруп експертів, кожна з яких відстоює свою точку зору

2. Метод комісій	Метод комісій полягає в тому. що на базі сукупних індивідуальних знань експертів знаходиться саме об'єктивна думка за рішенням питання. Спочатку експерти виставляють оцінку незалежно один від одного. Після обговорення незалежних оцінок експерти знову дають оцінку кожному параметру якості	Вибір найкращої альтернативи	Метод дозволяє виробити колективну думку щодо вирішення проблеми, уникнути упереджень і суб'єктивізм окремих експертів	1. Значний вплив авторитетів на думку учасників обговорення 2. Небажання експерта відмовитися від публічного висловлених раніше думок. 3. Труднощі організації проведення експертизи по підбору провідних фахівців	
3. Метод Дельфі	Метод полягає в заповненні експертами анкет з відповіддю на поставлені питання. Згода між учасниками опитування досягається шляхом ряду ітерацій, в процесі яких позиції експертів зближуються	Вибір найкращої альтернативи Метод Дельфі вважається основним інструментом при оцінці нових пропозицій в інституті майбутнього (США)	Збіжність оцінки експертів спостерігається після 3-5 сеансів обговорення проблеми	1. Необхідно мати попередні оцінки для кращого з'ясування експертами їх завдань. 2. Для здійснення процедури з рядом ітерацій необхідні значні витрати часу. 3. Може скластися ситуація, коли експерту потрібно висловити судження	

				по питанню, що не відносяться до сфери його діяльності	
4. Метод мозкової атаки (мозкового штурму) або метод генерації ідей	Суть методу полягає в генеруванні ідей, причому забороняється осуд ідей при висуненні і в процесі обговорення. Далі проводиться відбір. Число генераторів ідей має бути не більше 8-12.	Застосовується при рішенні не занадто складних задач загального організаційного характеру, коли проблема добре знайома всім учасникам засідання	Висунуті в процесі обговорення ідеї можуть базуватися на ідеях інших учасників або служити для них фундаментом, каталізатором	Можуть бути помилки в селекції ідей - невідома або традиційна	Протягом декількох нарад необхідно синтезувати 400-500 ідей для порівняльного аналізу завдання. Експерти повинні бути одного і того ж статусу.

На основі проведеного аналізу випливає висновок, що:

– кожен метод має свої обмеження і дослідник повинен отримати уявлення про метод перед тим, яким чином далі застосувати метод;

– основною проблемою багатокритеріального вибору є вибір критеріїв, а також можливі способи обчислення інтегральних оцінок;

1.4 Висновки з розділу

Сутність задачі прийняття рішень полягає у виборі деякої підмножини з безлічі альтернатив (альтернативних рішень) або в їхньому упорядкуванні. При цьому рішенням називають обрану підмножину або упорядковану множину альтернатив, раціональним рішенням – рішення, що за певним критерієм (критеріями) дає можливість вирішити поставлене завдання, а відповідну процедуру – процедурою прийняття рішень.

В ході проведених досліджень показана значимість методів і моделей прийняття рішень при формуванні нових напрямків розвитку техніки і технічного вигляду. Розглянута одна з процедур і можлива математична модель прийняття рішень, наведені поняття про ефективність прийняття рішень і основні критерії ефективності, розглянуті різні типи класифікації методів прийняття рішень, представлені основні властивості деяких відомих методів і моделей прийняття рішень.

Аналіз джерел з проблем теорії і практики прийняття рішень показав, що порівняльний аналіз методів прийняття рішень є важливим фактором вибору оптимального способу прийняття рішень для проведення конкретних практичних робіт і недостатньо представлений в науково-методичній літературі в інтересах оцінки технічного рівня.

Процеси прийняття рішень у сферах інформаційної безпеки багато в чому аналогічні. Тому переважна більшість систем управління повинна мати універсальний метод їх формування та підтримки реалізації. Мета, будучи важливою категорією процесу прийняття рішень, визначає функції і методи,

а також хід формування, прийняття, реалізації та оцінювання рішень і тому багато в чому впливає на ефективність останніх.

РОЗДІЛ 2. ЕКСПЕРТНІ МЕТОДИ В ОЦІНЦІ РИЗИКІВ У СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

2.1 Ризики в системі забезпечення інформаційної безпеки

В умовах дедалі більшої складності і інтеграції інформаційних систем питання інформаційної безпеки (ІБ) набуває все більшого значення. З одного боку, потрібна побудова єдиного інформаційного простору, швидкої інтеграції наявних і впроваджуваних інформаційних систем і комплексів в єдине рішення, що дозволяє здійснювати оперативне і стратегічне управління компанією і виробництвом. З іншого боку, крайня нерівномірність розвитку IT-служб та інфраструктури і різнорідність експлуатованих інформаційних систем перешкоджають забезпеченню необхідного рівня ІБ. Забезпечення ІБ стає одним із пріоритетних завдань з метою підтримки її нормальної діяльності. В умовах, що склалися необхідна побудова дійсно комплексної корпоративної системи інформаційної безпеки, що є однією з найбільш важливих складових в загальній системі компанії.

Для сучасної СУІБ характерний підхід, який передбачає вирішення проблем не "по мірі їх надходження", коли буває вже надто пізно ними займатися, а передбачає завчасний аналіз і попередження можливих проблем, на основі оцінки можливих ризиків ІБ. Тому фундаментом для успішного впровадження і функціонування СУІБ є оцінка та аналіз ризиків ІБ. [34]

У роботі визначимо ризик порушення ІБ як потенційну можливість використання вразливостей активів загрозами ІБ для заподіяння шкоди, яка вимірюється з урахуванням ймовірності реалізації загроз ІБ і величини збитку від реалізації загроз ІБ.

Таким чином, в представленому визначенні ризик ІБ є функція як мінімум двох змінних: величини потенційного (негативного) впливу – шкоди для організації і ймовірності реалізації загрози ІБ. Друга величина є комплексним показником.

Аналіз ризиків – це процедури виявлення факторів ризиків ІБ і оцінки їх вагомості. Аналіз ризиків ІБ включає оцінку ризиків і методи зниження ризиків або зменшення пов'язаних з ними несприятливих наслідків. При аналізі спочатку проводиться виявлення відповідних факторів і оцінка їх вагомості, повнота виявлених чинників збільшує якість і точність прогнозованих ризиків. До таких факторів належать безліч активів, вразливостей і загроз. Основна мета створення класифікації загроз ІБ – повна, детальна класифікація, що описує всі існуючі загрози ІБ і яка найбільш застосовна для аналізу ризиків реальних інформаційних систем. [23]

Аналіз і управління інформаційними ризиками - один з базових процесів, що визначають ефективність системи забезпечення інформаційної безпеки. При організації системи безпеки, що включає різнорідні заходи і способи забезпечення інформаційної безпеки, саме аналіз інформаційних ризиків визначає якість і ефективність функціонування цієї системи.

Користуючись поняттям ризику, можна кількісно і якісно визначити і такі поняття, як ефективність системи захисту інформації, рівень безпеки дій і оптимальність прийнятих рішень. [8]

Незалежно від розмірів організації і специфіки її інформаційної системи, роботи по забезпеченню режиму ІБ зазвичай складаються з наступних етапів (рис. 2.1):

- Визначення політики безпеки.
- Визначення сфери (кордонів) системи управління інформаційною безпекою та конкретизація цілей її створення.
- Оцінка ризиків.
- Вибір контрзаходів, що забезпечують режим ІБ.
- Управління ризиками.
- Аудит системи управління ІБ.

Як правило, визначення політики безпеки зводиться до наступних практичних кроків:

1. Вибір національних і міжнародних керівних документів і стандартів в області ІБ, і визначення на їх основі основних вимог і положень політики ІБ компанії, включаючи:

- управління доступом до засобів обчислювальної техніки (ЗОТ), програмам і даним;
- антивірусний захист;
- питання резервного копіювання;
- проведення ремонтних і відновлювальних робіт;
- інформування про інциденти в області ІБ та ін.

2. Визначення підходів до управління інформаційними ризиками та прийняття рішення про вибір рівня захищеності ІС. Рівень захищеності відповідно до зарубіжними стандартами може бути мінімальним (базовим) або підвищеним. Цим рівням захищеності відповідають мінімальний (базовий) або повний варіант аналізу інформаційних ризиків. [17]

3. Структуризація контрзаходів щодо захисту інформації за такими основними рівнями: нормативно-правовий, організаційно-управлінський, технологічний і апаратно-програмний.

4. Визначення порядку сертифікації та акредитації ІС на відповідність стандартам в області ІБ. Визначення періодичності проведення нарад за тематикою ІБ на рівні керівництва, включаючи періодичний перегляд положень політики ІБ, а також порядок навчання всіх категорій користувачів інформаційної системи з питань ІБ.

5. Визначення меж системи управління інформаційною безпекою і конкретизація цілей її створення.

На цьому етапі визначаються межі системи, для якої повинен бути забезпечений режим ІБ. Відповідно, система управління ІБ будуватися саме в цих межах. [29]

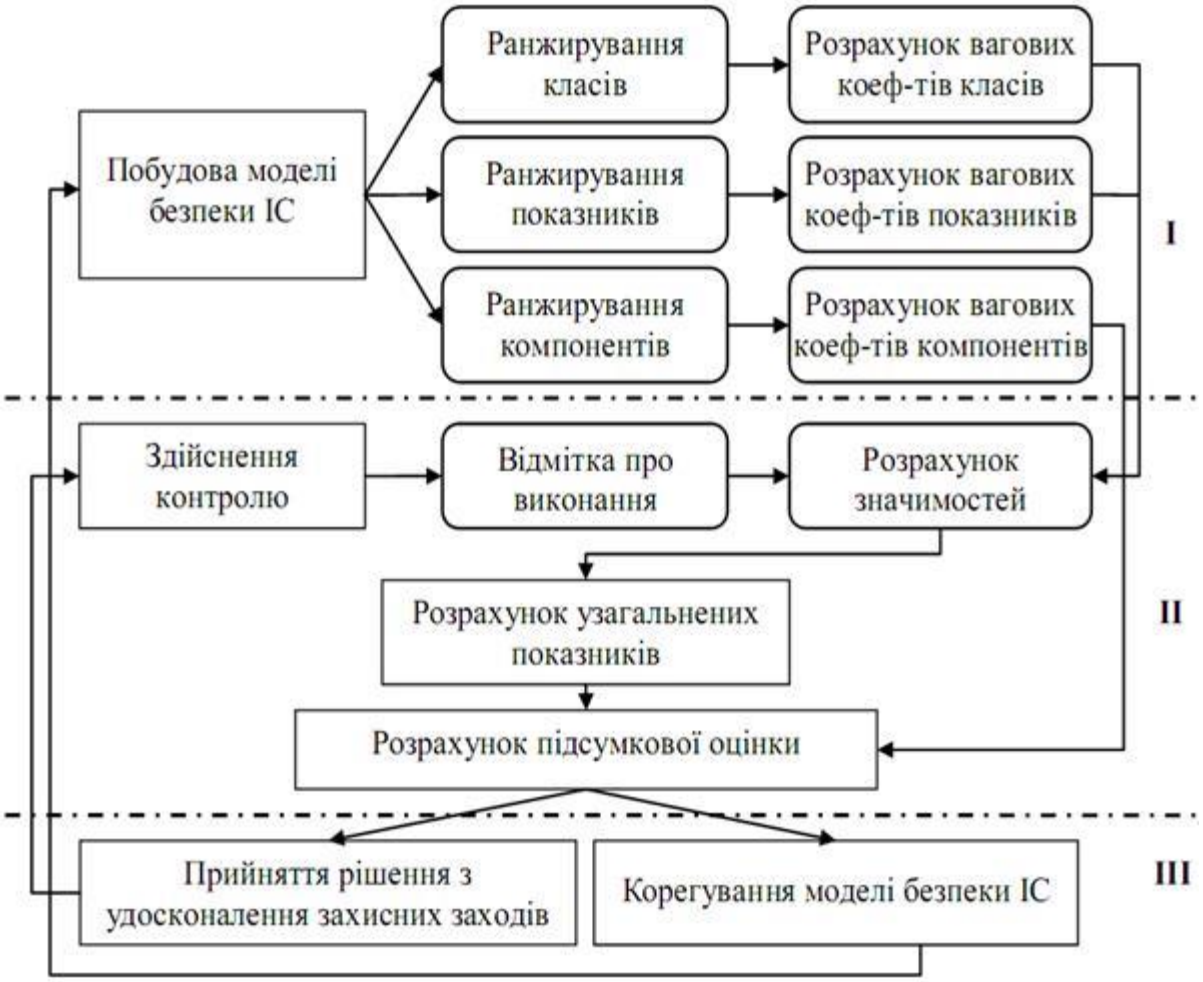

Рисунок 2.1 Основні етапи забезпечення інформаційної безпеки

6. Постановка завдання оцінки ризиків обґрунтовуються вимогами до методики оцінки інформаційних ризиків компанії. Вибір підходу залежить від рівня вимог, що пред'являються в організації до режиму інформаційної безпеки, характеру взятих до уваги загроз (спектра дії загроз) і ефективності потенційних контрзаходів щодо захисту інформації. Розрізняють мінімальні або базові, а також підвищені або повні вимоги до режиму ІБ.

Мінімальним вимогам до режиму ІБ відповідає базовий рівень ІБ. Такі вимоги застосовуються, як правило, до типових проектних рішень. Існує ряд стандартів і специфікацій, в яких розглядається мінімальний (типової) набір найбільш ймовірних загроз, таких як: віруси, збої устаткування,

несанкціонований доступ тощо. Для нейтралізації цих загроз обов'язково повинні бути прийняті контрзаходи незалежно від ймовірності їх здійснення і уразливості ресурсів. [21]

7. Управління ризиками. Розробляється деяка стратегія управління ризиками. Можливі такі підходи до управління інформаційними ризиками компанії:

Зменшення ризиків. Більшість ризиків можуть бути істотно зменшені шляхом використання досить простих і дешевих контрзаходів.

Ухилення від ризику. Від деяких класів ризиків можна ухилитися.

Зміна характеру ризику. Якщо не вдається ухилитися від ризику або ефективно його зменшити, можна прийняти деякі заходи страховки.

Прийняття ризику. Більшість ризиків не можуть бути зменшені до незначної величини. На практиці, після прийняття стандартного набору контрзаходів, ряд ризиків зменшується, але залишається все ще значним. Необхідно знати залишкову величину ризику.

В результаті виконання етапу для інформаційних ризиків компанії, що беруться до уваги, повинна бути запропонована стратегія управління ризиками.

8. Вибір контрзаходів, що забезпечують режим ІБ. На цьому етапі обґрунтовано вибирається комплекс різних контрзаходів щодо захисту інформації, структурованих по нормативно-правовому, організаційно управлінському, технологічному і апаратно-програмному рівнях забезпечення інформаційної безпеки. Надалі пропонований комплекс контрзаходів реалізується відповідно до обраної стратегії управління інформаційними ризиками. Якщо проводиться повний варіант аналізу ризиків, для кожного ризику додатково оцінюється ефективність комплексу контрзаходів щодо захисту інформації. [18]

9. Аудит системи управління ІБ. Перевіряється відповідність обраних контрзаходів щодо захисту інформації цілям і задачам бізнесу, декларованим в політиці безпеки компанії, проводиться оцінка залишкових ризиків і, в разі необхідності, оптимізація ризиків.

Технологія аналізу ризиків

Мета процесу аналізу ризиків полягає у визначенні характеристик ризиків по відношенню до інформаційної системи (ІС) і її ресурсів (активів). На основі отриманих даних можуть бути обрані необхідні засоби захисту. При аналізі ризиків враховується багато факторів: цінність ресурсів, оцінки значущості загроз і вразливостей, ефективність існуючих і планованих засобів захисту і багато іншого. Аналіз ризиків може бути базовим та повним [2,9,10]

Базовий аналіз ризиків – аналіз ризиків, що проводиться відповідно до вимог базового рівня захищеності. Базовий рівень безпеки – обов'язковий мінімальний рівень захищеності для ІС. Критерій досягнення базового рівня безпеки це виконання заданого набору вимог. Прикладні методи аналізу ризиків, орієнтовані на даний рівень, зазвичай не розглядають цінність ресурсів і не оцінюють ефективність контрзаходів. Методи даного класу застосовуються у випадках, коли до інформаційної системи не пред'являється підвищених вимог в області ІБ.

Повний аналіз ризиків – аналіз ризиків для інформаційних систем, що пред'являють підвищені вимоги в області ІБ. Включає в себе визначення цінності інформаційних ресурсів, оцінку загроз і вразливостей, вибір адекватних контрзаходів, оцінку їх ефективності.

При аналізі ризиків порівнюється з витратами на заходи і засоби захисту, після чого приймається рішення щодо оцінюваного ризику, який може бути:

- знижений, наприклад, за рахунок впровадження засобів і механізмів захисту, що зменшують ймовірність реалізації загрози або коефіцієнт руйнування;
- усунутий за рахунок відмови від використання схильного до загрози ресурсу;
- перенесений, наприклад, застрахований, в результаті чого в разі реалізації загрози безпеки, втрати буде нести страхова компанія, а не власник ресурсу;

Найбільш трудомістким є процес оцінки ризиків, який умовно можна розділити на наступні етапи: ідентифікація ризику; аналіз ризику; оцінювання ризику. На рисунку1.2 схематично зображено процес оцінки ризиків інформаційної безпеки.

Рисунок 2.2 Процес оцінки ризиків інформаційної безпеки

Ідентифікація ризиків

Ідентифікація ризику полягає в складанні переліку та описі елементів ризику: об'єктів захисту, загроз, вразливостей. [13]

Прийнято виділяти такі типи об'єктів захисту:

− інформаційні активи;

− програмне забезпечення;

− фізичні активи;

− сервіси;

− люди, а також їх кваліфікації, навички і досвід;

− нематеріальні ресурси, такі як репутація та імідж організації.

Як правило, на практиці розглядають перші три групи. Решта об'єктів захисту не розглядаються в силу складності їх оцінки.

Складність задачі складання переліку і доказ його повноти залежить від того, які вимоги пред'являються до деталізації списку. На базовому рівні безпеки спеціальних вимог до деталізації класів, як правило, не пред'являється і досить використовувати будь-який відповідний в даному випадку стандартний список класів ризиків.

Списки класів ризиків містяться в деяких посібниках, в спеціалізованому ПО аналізу ризиків. Прикладом є стандарт BSI, в якому є каталог загроз стосовно до різних елементів інформаційної технології. Як правило, для оцінки загроз та вразливостей використовуються різні методи, в основі яких можуть лежати:

− Експертні оцінки.

− Статистичні дані.

− Облік чинників, що впливають на рівні загроз і вразливостей.

Один з можливих підходів до розробки подібних методик – накопичення статистичних даних про події, що реально трапилися, аналіз і класифікація їх причин, виявлення чинників, від яких вони залежать. На основі цієї

інформації можна оцінити загрози та вразливості в інших інформаційних системах. [27]

Практичні складності в реалізації цього підходу такі:

По-перше, повинен бути зібраний досить великий матеріал про події в цій галузі.

По-друге, застосування цього підходу виправдано далеко не завжди. Якщо інформаційна система досить велика (містить багато елементів, розташована на великій території), має давню історію, то подібний підхід, швидше за все, можна застосувати. Якщо система порівняно невелика, використовує новітні елементи технології (для яких поки немає достовірної статистики), оцінки загроз і вразливостей можуть виявитися недостовірними.

Найбільш поширеним в даний час є підхід, заснований на обліку різних факторів, що впливають на рівні загроз і вразливостей. Такий підхід дозволяє

абстрагуватися від малоістотних технічних деталей, врахувати не тільки програмно-технічні, а й інші аспекти.

Оцінювання ризиків

Оцінка ризику полягає у визначенні його рівня (якісної або кількісної величини) і порівнянні цього рівня з максимально допустимим (прийнятним) рівнем, а також з рівнем інших ризиків.

Рівень ризику визначається шляхом комбінування двох величин: ймовірності події та розмірів його наслідків. Подія полягає в реалізації загрози, що використовує уразливість активу для впливу на цей актив і порушення його безпеки.

Всі відомі методики оцінки ризиків можна розділити на:

методики, що використовують оцінку ризику на якісному рівні (наприклад, за шкалою «високий», «середній», «низький»), до таких методик, зокрема, відноситься FRAP;

кількісні методики (ризик оцінюється через числове значення, наприклад, розмір очікуваних річних втрат).

До прийняття рішення про впровадження тієї чи іншої методики управління ризиками ІБ слід переконатися, що вона досить повно враховує бізнеспотреби компанії, її масштаби, а також відповідає кращим світовим практикам і має досить докладний опис процесів і необхідних дій. [6]

Якісне визначення величини ризику

Точно визначити ймовірність загрози, величину уразливості або розмір збитку на практиці зазвичай не представляється можливим, тому мова може йти тільки про числові оцінки в деякому діапазоні величин. Кожному кількісному діапазону можна зіставити певний якісний рівень ризику. В результаті отримаємо якісну шкалу оцінки ризику, якій зіставляються деякі приблизні кількісні оцінки, без яких будь-яка якісна шкала позбавляється сенсу, тому що перестає бути пов'язаною з реальними втратами організації.

Матриця виникає в результаті розгляду ймовірності сценарію інциденту з урахуванням впливу на бізнес. У цій матриці по горизонталі відкладаються якісні значення ймовірності успішної реалізації загрози (сценарію інциденту), а по вертикалі - якісні рівні збитку (впливу на бізнес). Результуючий ризик вимірюється за шкалою від 0 до 8, який може оцінюватися за критеріями прийняття ризиків, тобто порівнюватися з максимально допустимим рівнем ризику, в якості якого може бути вибрано, наприклад, значення 3. Мінімальний рівень ризику, що дорівнює 0, відповідає дуже низькій ймовірності інциденту і дуже низькому впливу цього інциденту на бізнес, а максимальний рівень ризику, що дорівнює 8, відповідає дуже високій ймовірності інциденту і дуже високому впливу на

бізнес. Дана шкала ризиків також може бути зведена до простого загального рейтингу ризику, наприклад: низький ризик: 0-2, середній ризик: 3-5, високий ризик: 6-8. Всі ризики, значення яких перевищує 3, потребуватимуть обробки. [32]

Вибір конкретного табличного методу і налаштування відповідних шкал є прерогативою конкретної організації.

Будь-якому якісному рівню, що виражається числовими значеннями або словами «низький», «середній», «високий» тощо, повинні відповідати певні діапазони оціночних кількісних величин. Без такого зіставлення використання якісних шкал для оцінки ризиків, звичайно, можливе, проте в цьому випадку оцінка ризиків втрачає економічний сенс.

Тому на практиці кількісний підхід завжди перетворюється в якісний і навпаки [2], в зв'язку з чим протиставлення якісних і кількісних методів оцінки ризиків є, взагалі кажучи, заняттям досить безглуздим.

Процес зіставлення якісних рівнів ризиків з відповідними кількісними діапазонами прогнозованого середньорічного збитку організації буде розглянуто далі у відповідному розділі.

Кількісне визначення величини ризику може здійснюватися різними методами. Вибір того чи іншого способу залежить, в першу чергу, від обсягу доступної, в тому числі статистичної, інформації про ризик і необхідної точності оцінок. Також доводиться враховувати фактичний рівень ризику. Чим менша ймовірність настання, тим важче виміряти ризик.

Загальний принцип при виборі методів вимірювання зводиться до максимально можливого використання доступних статистичних даних. Якщо їх немає, вони недостатні або непридатні, фактичний матеріал замінюється теоретичними гіпотезами або експертними оцінками. [3]

Всього можна виділити чотири групи методів кількісної оцінки ризиків інформаційної безпеки:

1. статистичні методи;
2. ймовірносно-статистичні;
3. теоретико-імовірнісні;
4. експертні.

В основі статистичних методів лежить оцінка ймовірності настання випадкової події виходячи з відносної частоти появи даної події в серії спостережень. Дані методи є найбільш переважними, оскільки, по-перше, вони досить прості, і, по-друге, їх оцінки базуються на фактичних даних. [1]

Використання комбінації статистичних даних і теоретичних гіпотез для оцінки ризику становить основну ідею ймовірносно-статистичних методів. Це розширює сферу застосування даної групи методів, але надійність отриманих результатів може виявитися нижче, ніж при використанні статистичних методів.

При управлінні ризиками інформаційної безпеки доводиться стикатися з необхідністю оцінки рідкісних подій, таких як розкриття інформації, прослуховування, заміна тощо, які допускають важкі наслідки. В цьому випадку статистика або взагалі відсутня, або відноситься до інших об'єктів, які суттєво відрізняються від досліджуваного. Це робить неможливим застосування статистичних і ймовірносно-статистичних методів.

Доводиться використовувати теоретико-імовірнісні методи, в основі яких лежить побудова математичної моделі досліджуваного ризику і теоретичної оцінки його параметрів. Дані методи дуже трудомісткі і мають відносно невисоку точність, але в ряді випадків є єдиним можливим науково обґрунтованим способом оцінки. Зокрема, вони застосовуються при розробці декларацій промислової безпеки підприємств. [18]

При оцінюванні ризиків рекомендується розглядати такі аспекти:

- Шкали і критерії, за якими можна вимірювати ризики.
- Оцінка ймовірностей подій.

- Технології вимірювання ризиків.

Шкали й критерії, за якими вимірюються ризики

Для вимірювання якої-небудь властивості необхідно вибрати шкалу. Шкали можуть бути прямими (натуральними) або непрямими (похідними). Прикладами прямих шкал є шкали для вимірювання фізичних величин, наприклад – літри для вимірювання об'єму, метри для вимірювання довжини. У ряді випадків прямих шкал не існує, доводиться використовувати або прямі шкали інших властивостей, пов'язаних з тими, що нас цікавлять, або визначати нові шкали. Прикладом є шкала для вимірювання суб'єктивної властивості «цінність інформаційного ресурсу». Вона може вимірюватися в похідних шкалах, таких як вартість відновлення ресурсу, час відновлення ресурсу та інших. Інший варіант – визначити шкалу для отримання експертної оцінки, що, наприклад, має три значення:

- Малоцінний інформаційний ресурс: від нього не залежать критично важливі завдання і він може бути відновлений з невеликими витратами часу і грошей.
- Ресурс середньої цінності: від нього залежить ряд важливих завдань, але в разі його втрати він може бути відновлений за час, що не перевищує критично допустимий, вартість відновлення – висока.
- Цінний ресурс: від нього залежать критично важливі завдання, в разі втрати час відновлення перевищує критично допустимий або вартість надзвичайно висока. [17]

Для вимірювання ризиків не існує природної шкали. Ризики можна оцінювати з об'єктивних або суб'єктивних критеріїв. Прикладом об'єктивного критерію є ймовірність виходу з ладу будь-якого обладнання,

наприклад ПК, за певний проміжок часу. Прикладом суб'єктивного критерію є оцінка власником інформаційного ресурсу ризику виходу з ладу ПК. Для цього зазвичай розробляється якісна шкала з декількома градаціями, наприклад: низький, середній, високий рівень.

Оцінка ймовірностей порушення ІБ

Процес отримання ймовірності подій порушень ІБ зазвичай поділяють три етапи: підготовчий етап, отримання оцінок, етап аналізу отриманих оцінок.

Перший етап. Під час цього етапу формується об'єкт дослідження – безліч подій, наводиться попередній аналіз властивостей цієї множини (встановлюється залежність або незалежність подій, дискретність або неперервність випадкової величини, що породжує дану множину подій). На основі такого аналізу вибирається один з відповідних методів отримання ймовірності. На цьому ж етапі проводиться підготовка експерта або групи експертів, ознайомлення їх з методом і перевірка розуміння поставленого завдання експертами. [4]

Другий етап полягає в застосуванні методу, обраного на першому етапі. Результатом цього етапу є набір чисел, який відображає суб'єктивний погляд експерта або групи експертів на ймовірність тієї чи іншої події, проте далеко не завжди може вважатися остаточно отриманим розподілом, оскільки може бути суперечливим.

Третій етап полягає в дослідженні результатів опитування. Якщо ймовірності, отримані від експертів, не узгоджуються з аксіомами ймовірності, то на це звертається увага експертів і проводиться уточнення відповідей з метою приведення їх у відповідність до вибраної системи аксіом.

Для деяких методів отримання ймовірності третій етап не проводиться, оскільки сам метод полягає у виборі ймовірного розподілу, що підкоряється

аксіом ймовірності, яке в тому чи іншому сенсі найближче до оцінок експертів. Особливу важливість третій етап набуває при агрегуванні оцінок, отриманих від групи експертів. [12]

2.2 Аналіз методик управління ризиками інформаційної безпеки

Проаналізуємо три найвідоміші світові методики управління ризиками ІБ, які можна застосувати для аналізу ризиків ІБ у процесі забезпечення неперервності функціонування СЗІ в КМЗ, визначимо переваги та недоліки кожної з них. Аналізу підлягають: методика оцінки NIST 800-30 [4], методика CRAMM [5] та методика OCTAVE [6].

Однією з найпопулярніших та широковживаних методик управління ризиками є методика оцінки ризиків Національного інституту стандартів і технологій США (National Institute of Standards and Technology) NIST, зазначена в Керівництві з управління ризиками в інформаційних технологіях NIST 800-30 (NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems). Ця методика передбачає попереднє оцінювання двох параметрів: потенційного збитку та ймовірності реалізації загрози [7].

Призначення системи управління ризиками безпосередньо пов’язане з можливістю компанії виконувати свої основні функції за умов постійного розширення сфери використання інформаційних технологій.

Методика оцінки ризиків, яка наведена в спеціальних рекомендаціях 800-30, охоплює широке коло завдань, що пов’язані зі стратегією управління ризиками і є основою для розроблення власної системи управління ризиками. Проте запропонований процес оцінювання ризику ІБ, який представлений у вигляді таблиці, що відображає залежність ризику від двох вхідних змінних: потенційного збитку і ймовірності можливого

інциденту. При цьому значення кожної змінної, зокрема ризику, оцінюється за трирівневою шкалою. Такий “жорсткий” механізм отримання оцінок ризику суттєво обмежує точність результатів, забезпечуючи їх оперативність та відтворюваність [7].

Алгоритм цієї методики зображено на рис. 2.3.

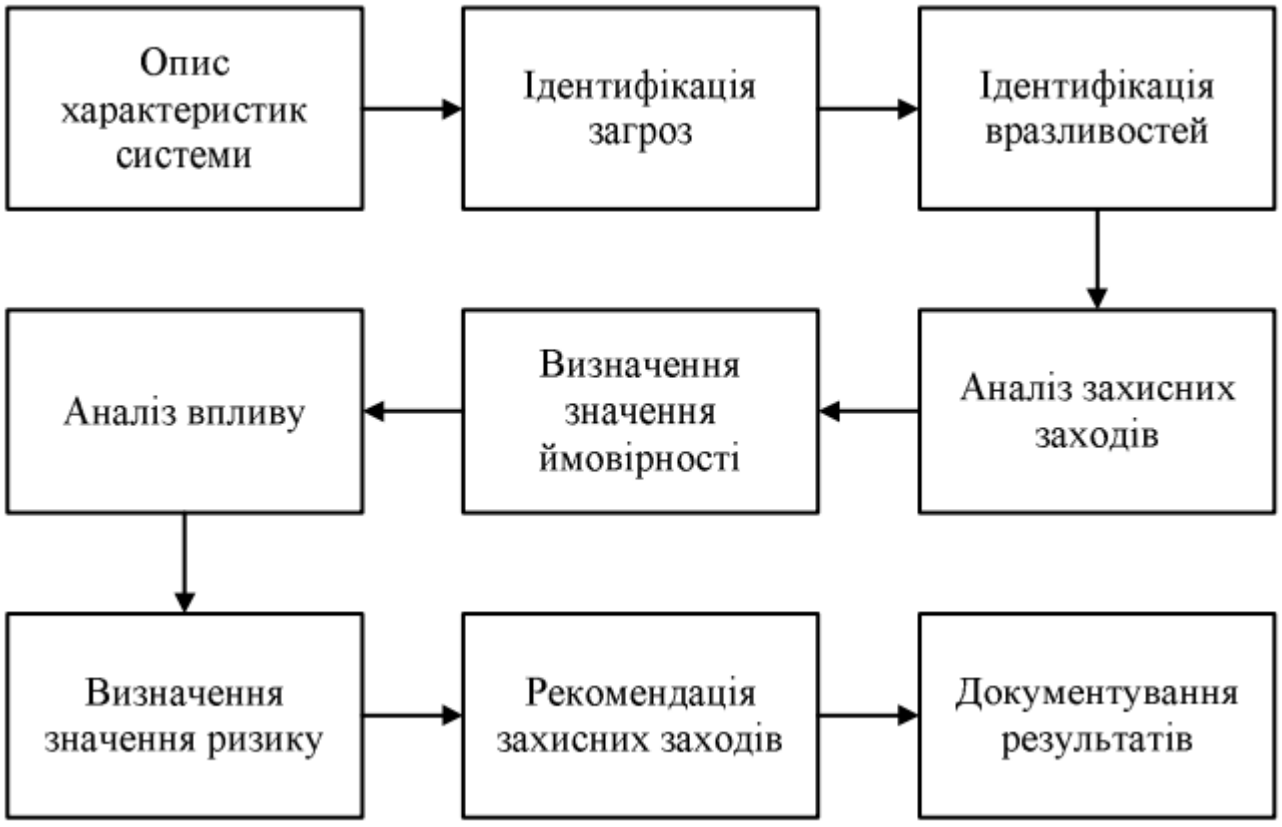

Рисунок 2.3 Алгоритм методики управління ризиками

Використання такої методики передбачає такі етапи:

- опис характеристик системи;
- ідентифікація загроз;
- ідентифікація вразливостей;
- аналіз наявних засобів/заходів захисту;
- визначення значення ймовірності;

- аналіз впливу;
- визначення значення ризику;
- вибір засобів/заходів захисту;
- документування отриманих результатів.

Наступною методикою, яку аналізують автори статті, є методика CRAMM (CCTA Risk Analysis and Managment Method), яку розробило Агентство з комп'ютерів і телекомунікацій Великобританії (Central Computer and Telecommunications Agency) за поданням Британського уряду і яка прийнята за державний стандарт. Цю методику використовують, починаючи з 1985 року, державні та комерційні організації Великобританії. За цей час CRAMM набула популярності у всьому світі. Фірма Insight Consulting Limited займається розробленням і супроводом однойменного програмного продукту, що реалізує метод CRAMM [8].

В основу методики CRAMM покладено комплексний підхід до оцінки ризиків, що поєднує кількісні та якісні методи аналізу. Методика є універсальною і придатна як для великих, так і для малих організацій, як державного, так і комерційного сектору. Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються своїми базами знань (profiles). Для комерційних організацій є комерційний профіль (Commercial Profile), для державних організацій – державний профіль (Government profile). Державний варіант профілю також дає змогу проводити аудит на відповідність вимогам американського стандарту ITSEC ("Помаранчева книга") [8].

Правильне використання методики CRAMM дає змогу економічно обґрунтувати витрати організації на забезпечення інформаційної безпеки та неперервності функціонування. Економічно обґрунтована стратегія

управління ризиками ІБ дає змогу, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Методика CRAMM припускає поділ всієї процедури на три послідовні етапи. Завданням першого етапу є відповідь на запитання: “Чи достатньо для захисту системи застосування засобів базового рівня, що реалізують традиційні функції ІБ, чи необхідне проведення детальнішого аналізу?” На другому етапі здійснюється ідентифікація ризиків і оцінюється їх величина. На третьому етапі вирішується завдання про вибір адекватних контрзаходів. Методика CRAMM для кожного етапу визначає набір вихідних даних, послідовність заходів, анкети для проведення інтерв’ю, списки перевірки і набір звітних документів [8].

Алгоритм методики CRAMM подано на рис. 2.4.

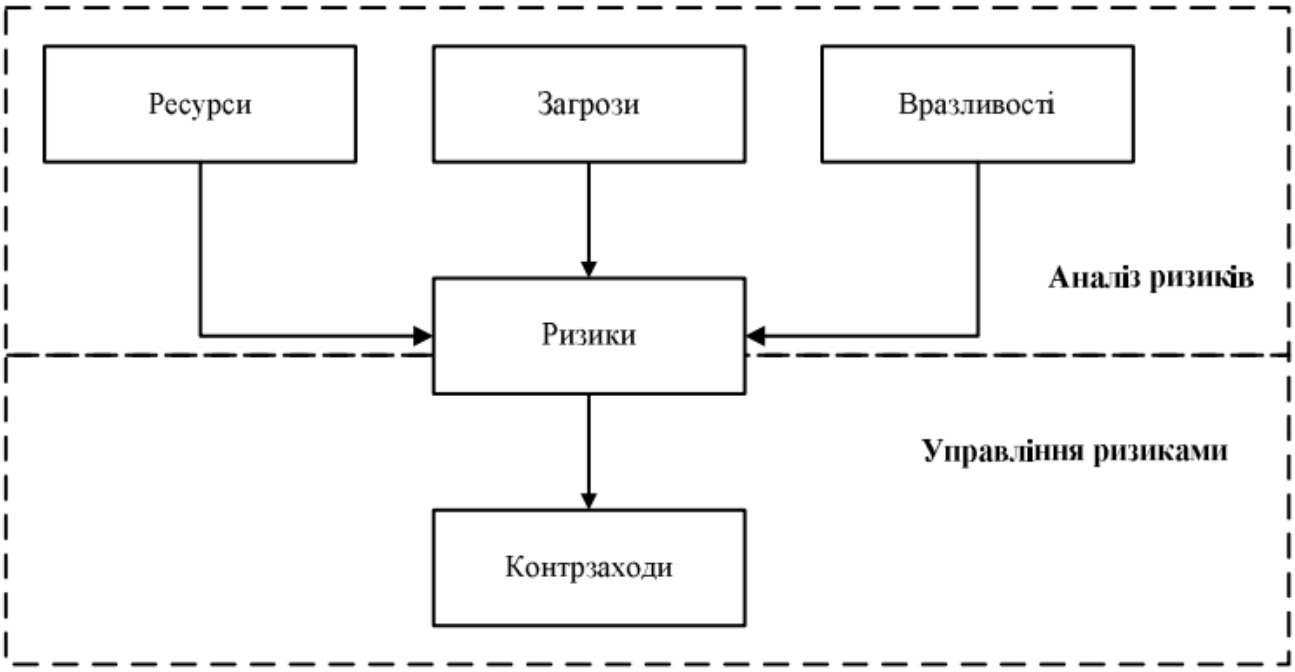

Рисунок 2.4 Алгоритм методики управління ризиками CRAMM

Методика OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в Університеті Карнегі-Мелон (США) і передбачає оцінювання критичності загроз, активів і вразливостей.

Цю методику широко використовують у всьому світі, виконуючи роботи з оцінки ризиків ІБ та впровадження процесів управління ризиками в компанії загалом. Методика має ряд модифікацій, які розраховані на організації різного розміру та галузі діяльності [9].

Зміст методики OCTAVE полягає в тому, що для оцінки ризиків використовується послідовність відповідно організованих внутрішніх семінарів (workshops). Оцінка ризиків здійснюється в три етапи, яким передує набір підготовчих заходів: узгодження графіка семінарів, призначення ролей, планування, координація дій учасників проектної групи [9].

На першому етапі, в межах практичних семінарів, здійснюється розроблення профілів загроз, що містять в собі інвентаризацію та оцінку цінності активів, ідентифікацію застосовних вимог законодавства та нормативної бази, ідентифікацію загроз та оцінку їх ймовірності, а також визначення системи організаційних заходів з підтримки режиму інформаційної безпеки.

На другому етапі проводиться технічний аналіз вразливостей систем організації щодо загроз, чиї профілі розроблено на попередньому етапі, який містить ідентифікацію наявних вразливостей компанії та оцінювання їх величини.

На третьому етапі виконується оцінка та оброблення ризиків інформаційної безпеки, що містить визначення величини та ймовірності завданої шкоди внаслідок реалізації загроз ІБ з використанням вразливостей, які ідентифіковано на попередніх етапах, визначення стратегії ІБ, а також вибір варіантів і прийняття рішень з оброблення ризиків.

Величина ризику визначається як середнє значення річних втрат компанії в результаті реалізації загроз ІБ.

Алгоритм цієї методики зображено на рис. 2.5.

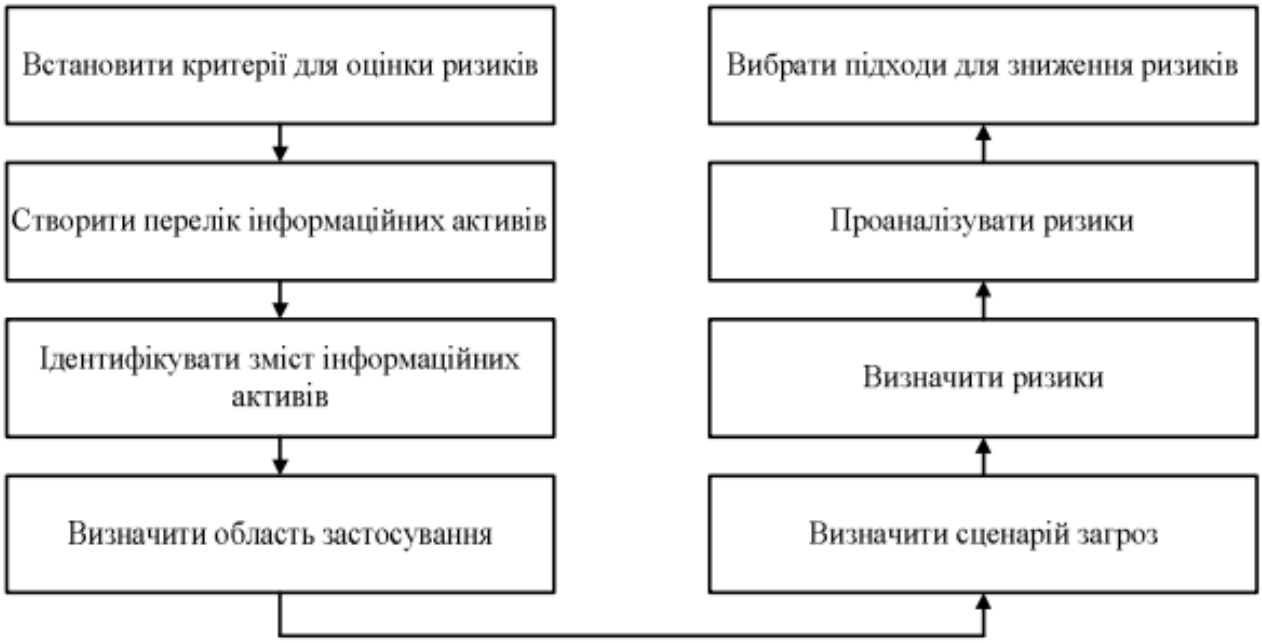

Рисунок 2.5 Алгоритм методики управління ризиками OCTAVE

Отже, коротко охарактеризувавши три найпоширеніші методики з управління ризиками в сфері інформаційної безпеки [8, 10, 11] та здійснивши аналіз основних властивостей цих методик, автори визначили основні переваги та недоліки перелічених вище методик. Їх подано у вигляді табл. 2.1.

Таблиця 2.1 Переваги та недоліки методик з управління ризиками ІБ

Методика	Переваги	Недоліки
NIST	– порівняно проста в реалізації; – придатна для підприємств різного розміру; – детально описує всі можливі ризики для інформаційних активів; – припускає використання як способів зниження ризиків всіх можливих варіантів (зниження, прийняття, перенесення, уникнення ризику); – існує автоматизоване програмне забезпечення, що реалізовує принципи методики; йому властива відносна легкість та зручність використання.	– довготривалий процес аналізу; – розроблена для використання у федеральних організаціях США; – оцінювання ризиків проводиться за трирівневою шкалою, що істотно обмежує можливості методики загалом.

CRAMM	– є універсальною і підходить для організацій як державного, так та комерційного сектору; – використовує кількісні і якісні способи оцінки ризиків; – розроблені комерційні програмні продукти, що реалізовують положення CRAMM;	– використання методики потребує спеціальної підготовки і високої кваліфікації спеціаліста; – довготривалий процес аналізу; – програмний інструментарій генерує велику кількість паперової документації, яка не завжди виявляється корисною на практиці; – не дає змоги створювати власні шаблони звітів або модифікувати наявні; – припускає використання лише методів зниження рівня ризиків ІБ, такі способи управління ризиками, як “уникнення” або “прийняття”, не розглядаються.
OCTAVE	– швидко впроваджується; – можливе застосування для організацій різного розміру та галузей зайнятості; – є комерційні програмні продукти, що реалізовують положення методики; – високий рівень гнучкості.	– не дає кількісної оцінки ризиків; – припускає використання як способів зниження ризиків лише його зниження і прийняття.

У випадку забезпечення неперервності функціонування СЗІ в МЗ, що є довготривалим та ресурсомістким процесом, аналіз ризиків ІБ, які можуть стати загрозою для неперервності функціонування СЗІ, є лише одним з багатьох етапів, що повинні бути успішно виконані. Саме тому дуже важлива можливість швидкого та порівняно простого управління ризиками

ІБ, що входять у сферу впливу неперервності функціонування СЗІ в МЗ. Так, на основі проведеного аналізу, автори статті зробили висновок, що оптимальним варіантом для вибору методики управління ризиками ІБ в контексті забезпечення неперервності функціонування МЗ та СЗІ зокрема є адаптація та удосконалення відомих методик логічним поєднанням їх переваг та мінімізацією недоліків. [11]

2.2 Експертні методи оцінки ризику

В сучасних умовах стає все більш складно забезпечувати зростання ефективності інформаційної безпеки. Це пов'язано з постійним підвищення жорсткості вимог до систем управління. Саме тому в даний час питання про вдосконалення систем управління є досить актуальним.

Важливим фактором підвищення рівня інформаційної безпеки є використання при підготовці рішень математичних методів і моделей в цілях оцінки ризиків і можливого їх запобігання. Однак використання даних методів при вирішенні різноманітних задач часто є неможливим внаслідок їх складності. Тому більш широке поширення набув метод експертних оцінок. [17]

Метод експертних оцінок зазвичай реалізується шляхом обробки думок досвідчених експертів (кваліфікованих фахівців). Тобто даний спосіб передбачає збір і вивчення оцінок, зроблених різними фахівцями на основі їх власної інтуїції, знань і досвіду, ймовірностей виникнення різних рівнів втрат. Ці оцінки базуються на обліку всіх факторів ризику, а також статистичних даних. Реалізація способу експертних оцінок значно ускладняється, якщо кількість показників оцінки невелика.

Основними вимогами до залучення до аналізу експертам є:

– високий рівень креативності мислення;

- наявність спеціалізованих знань в залежності від сфери проведення експертизи;
- повна незалежність від системи;
- можливість проведення оцінки будь-якої кількості ідентифікованих ризиків;
- доступ до всієї необхідної інформації.

Ситуації, до яких застосовується даний метод, часто виникають в розробках сучасних систем управління інформаційної безпеки, а також при прогнозуванні та довгостроковому плануванні.

Для того щоб забезпечити умови для підвищення якості та ефективності експертних оцінок, необхідна активна і цілеспрямоване участь фахівців на кожному етапі (стадії) прийняття рішень.

Післястадійний підхід до оцінки ризиків заснований, перш за все, на те, що ризики визначаються для кожної стадії проекту окремо, а потім знаходиться підсумковий сумарний результат по всьому проекту. [9]

Для отримання кінцевого результату (експертних оцінок) використовують різні методи, найбільшого поширення з яких отримали анкетні методи і методи групової експертизи. Тобто кожному експерту, що працює окремо, подається перелік первинних ризиків на основі опитувальних листів по всіх стадіях проекту і пропонується оцінити ймовірність настання ризиків у відповідності за наступною системою оцінок:

0 – ризик розглядається як несуттєвий;

25 – велика ймовірність, що ризик не реалізується;

50 – про настання події нічого певного сказати не можна;

75 – велика ймовірність, що ризик виявиться;

100 – ризик з повною упевненістю реалізується.

Оцінки експертів піддаються аналізу на несуперечливість, який виконується за певними правилами:

Максимально допустима різниця між оцінками двох експертів з будь-якого фактора не повинна перевищувати 50. Порівняння проводяться по модулю (знак плюс або мінус не враховується). Це дозволяє усунути неприпустимі відмінності в оцінках експертами ймовірності настання окремого ризику. Якщо кількість експертів три і більше, то оцінками піддаються попарно порівняльні думки.

Для оцінки узгодженості думок експертів по всьому набору ризиків, як правило, виявляється два експерта. Основним правилом при цьому є максимальне розбіжність думок цих експертів (мінімальна спільність). Для розрахунків розбіжності оцінки підсумовуються по модулю і результат ділиться на кількість простих ризиків. Частка від ділення не повинна перевищувати 25.

У разі виявлення між думками експертів протиріч (НЕ виконується хоча б одне з наведених правил), вони обговорюються на зборах з експертами. При відсутності протиріч всі оцінки експертів зводяться в середню (середньоарифметична), яка використовується в подальших розрахунках.

Існують і інші способи експертної оцінки ризику. Одним з них є метод ранжування, алгоритм реалізації якого наступний:

На першому етапі при обробці інформації необхідно впорядкувати всі оцінки по спадаючій.

Далі за формулою середнього арифметичного знаходиться середня величина всіх оцінок.

Отримані значення розбиваються на чотири рівних інтервали.

У разі потрапляння оцінок експертів в крайні інтервали, цих експертів просять обґрунтувати свою думку.

З їх обґрунтуванням знайомлять інших експертів (з умовою повної конфіденційності).

Врахування в наступних турах обговорення тих чинників, які були випадково втрачені фахівцями в першому турі опитування. В наслідок цього у другому турі менший розкид думок.

Також до числа найбільш поширених методів експертних оцінок ризику відносять метод Дельфі, попарне порівняння, метод бальних оцінок і інші.

Метод Дельфі передбачає виключення в процесі дослідження безпосереднього спілкування між експертами. Тобто суть даного методу полягає в індивідуальному опитуванні всіх членів групи за допомогою анкет з метою з'ясування їх думок на основі особистого досвіду і знань щодо майбутніх гіпотетичних подій. [20]

Метод бальної оцінки ризику полягає в експертизі ризику на основі узагальнюючого показника, який визначається по ряду експертно оцінюваних приватних показників (факторів) ступеня ризику. При цьому передбачається проходження наступних етапів:

- вибір чинників, які безпосередньо впливають на ступінь ризику проекту;
- визначення узагальненого критерію і приватних показників, які характеризують кожен фактор;
- оцінка даного критерію щодо ступеня ризику;
- вироблення рекомендацій з управління ризиком.

Очевидно, що висока якість експертизи досягається в разі високої узгодженості думок експертів за кількома факторами. Однак при використанні будь-якого методу експертних оцінок виникає проблема, пов'язана з неточністю отриманих результатів внаслідок таких чинників як: неякісний підбір фахівців, домінування думки (як правило, «авторитетного лідера») і т.д. Саме тому необхідне проведення експертизи на достовірність

отриманих оцінок. Одним з таких показників оцінок є коефіцієнт конкордації Кендала, або коефіцієнт множинної рангової кореляції. Розраховується наступним чином:

$$W = \frac{12S}{m^2(n^3 - n)}$$

де:

m – кількість експертів в групі,

n – кількість досліджуваних факторів,

S – сума квадратів різниць рангів (відхилень від середнього).

Результати налізу знаходяться в наступних межах:

- W <0,2-0,4 – узгодженість експертів слабка;
- W> 0.6 - 0.8 – узгодженість експертів сильна;
- W = 1 – думки всіх експертів збігаються.

Розберемо розрахунок коефіцієнта на прикладі, в якому 5 експертів попросили проранжувати за важливістю 4 різних фактори. Вони розставили ранги від 1 до 4 і тепер необхідно це проаналізувати.

	Фактор 1	Фактор 2	Фактор 3	Фактор 4
Експерт 1	1	3	2	4
Експерт 2	3	2	1	4
Експерт 3	4	3	1	2
Експерт 4	2	3	4	1
Експерт 5	2	4	1	3

Рисунок 2.6 Результати опитування думок п'яти експертів по 4 факторам

На основі прикладу отримуємо: m = 5, n = 4.

Оскільки всі дані відомі, залишається тільки знайти суму квадратів різниць рангів (S), яка розраховується за однією з формул:

$$S = \sum_{i=1}^{n}(\sum_{j=1}^{m} R_{ij})^2 - \frac{(\sum_{i=1}^{n}\sum_{j=1}^{m} R_{ij})^2}{n}$$

$$S = \sum_{i=1}^{n}(\sum_{j=1}^{m} A_{ij} - \frac{1}{2}m(n+1))^2$$

Для обчислення потрібно додати два рядки: суму по стовпцю (сума оцінки експертів по кожному фактору) і квадрат цієї суми.

Сума	12	15	9	14	50
Квадрат суми	144	225	81	196	646

Рисунок 2.7 Приклад розрахунку коефіцієнта конкордації Кендала на основі думок п'яти експертів по 4 факторам

Таким чином, отримуємо:

$$S = 646 - 50^2/4 = 21$$

Далі отримуємо:

$$S = (12 - 12,5)^2 + (15 - 12,5)^2 + (9 - 12,5)^2 + (14 - 12,5)^2 = 21$$

Далі розраховується сам коефіцієнт Кендала:

$$W = (12 * 21) / (25 * (64 - 4)) = 0,168$$

Отримуємо дуже слабку узгодженість експертів (W <0,2).

Такий результат може бути зумовлений двома причинами:

1. в розглянутій групі фахівців практично відсутня спільність думок;
2. всередині даної групи існують коаліції з високою узгодженістю думок, однак, узагальнені думки таких коаліцій протилежні. [10]

Також, слід узагальнити основні переваги та недоліки даного методу.

Таблиця 2.2 Переваги та недоліки метода експертних оцінок ризику

Переваги	**Недоліки**
Простота організації	Неповнота відповідей
Використання статистичної обробки	Можливість неправильного розуміння
Можливість охоплення великих груп	Суб'єктивний фактор опитуваних експертів

Таким чином, можна зробити висновок про те, що експертні оцінки ризику є досить ефективним і нескладним методом аналізу настання ймовірних несприятливих подій, особливо в таких сферах як системи управління інформаційною безпекою. Більш того, даний метод за рахунок своєї простої організації дозволяє охопити великий діапазон досліджуваних факторів. [5]

Однак в силу виняткової суб'єктивності відповідей експертів, необхідно дотримуватися певних правил проведення експертизи, а також проводити аналіз ступеня узгодженості думок фахівців з метою виявлення якості цієї експертизи.

2.3 Висновки з розділу

Забезпечення інформаційної безпеки стає одним із пріоритетних завдань з метою підтримки її нормальної діяльності. В умовах, що склалися необхідна побудова дійсно комплексної системи інформаційної безпеки, що є однією з найбільш важливих складових в загальній системі управління безпекою.

У роботі визначимо ризик порушення як потенційну можливість використання вразливостей активів загрозами для заподіяння шкоди, яка вимірюється з урахуванням ймовірності реалізації загроз ІБ і величини збитку від реалізації загроз ІБ. Оцінка ризику полягає у визначенні його рівня і порівнянні цього рівня з максимально допустимим рівнем, а також з рівнем інших ризиків. Ризики можна оцінювати з об'єктивних або суб'єктивних критеріїв.

Розглянуто процес управління ризиком ІБ в контексті забезпечення неперервності функціонування СЗІ. Здійснено аналіз трьох поширення методик в сфері управління ризиками ІБ, що дало змогу визначити їх основні особливості, встановити переваги та недоліки.

Експертні оцінки ризику є досить ефективним і нескладним методом аналізу настання ймовірних несприятливих подій, особливо в таких сферах як системи управління інформаційною безпекою. Більш того, даний метод за рахунок своєї простої організації дозволяє охопити великий діапазон досліджуваних факторів.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ОЦІНКИ РИЗИКІВ НА ОСНОВІ ЕКСПЕРТНИХ МЕТОДІВ

3.1 Модель прийняття рішень оцінки ризиків експертними методами

Колективні рішення – формування елементів і параметрів моделі командою (експертами) під загальним керівництвом особи, що приймає рішення (ОПР), яка визначає вхідні та вихідні дані і приймає за результат найбільш ефективне рішення. Існує множина методів класифікації прийняття рішень. Процеси розробки і прийняття рішень є досить складними і трудомісткими, вони стосуються практично всіх аспектів людської діяльності. Узагальнена послідовність прийняття рішень будь-якої досліджуваної проблеми представлена на рис. 1. Це структурований поетапний процес підготовки та прийняття рішень, тобто структурований життєвий цикл рішень управління. Прийняття рішень є основною функцією управління. [1]

Експертна інформація відіграє важливу роль при застосуванні сучасних методів підтримки прийняття рішень. Методи її отримання, уявлення й обробки складають невід’ємну частину технології підтримки прийняття рішень. Ефективність використання цієї інформації істотно залежить від коректності і обґрунтованості використовуваних методів. Експертні оцінки є інформацією для особи, що приймає рішення (ОПР), необхідною при

прийнятті зважених обґрунтованих рішень, переважно в складних ситуаціях прийняття рішень. На жаль, до цих пір сформованих теоретично обґрунтованих технологій підготовки і прийняття колективних рішень немає. [2]

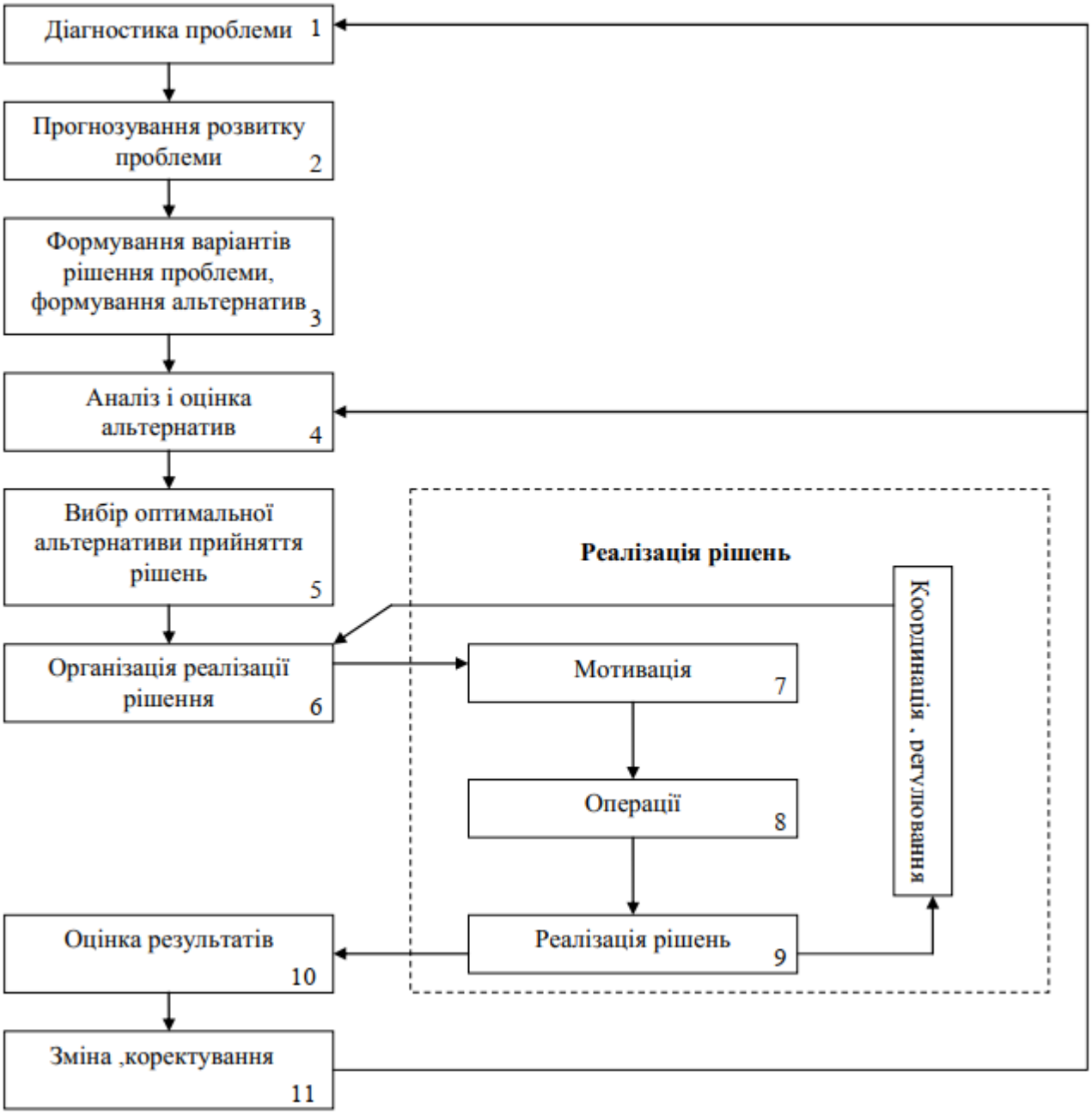

Рисунок 3.1 Послідовність прийняття і реалізації рішень з будь-якої досліджуваної проблеми

Структуризації проблеми представлено схемою на рис. 3.2, а далі опишемо поетапний структурований процес колективного експертного оцінювання.

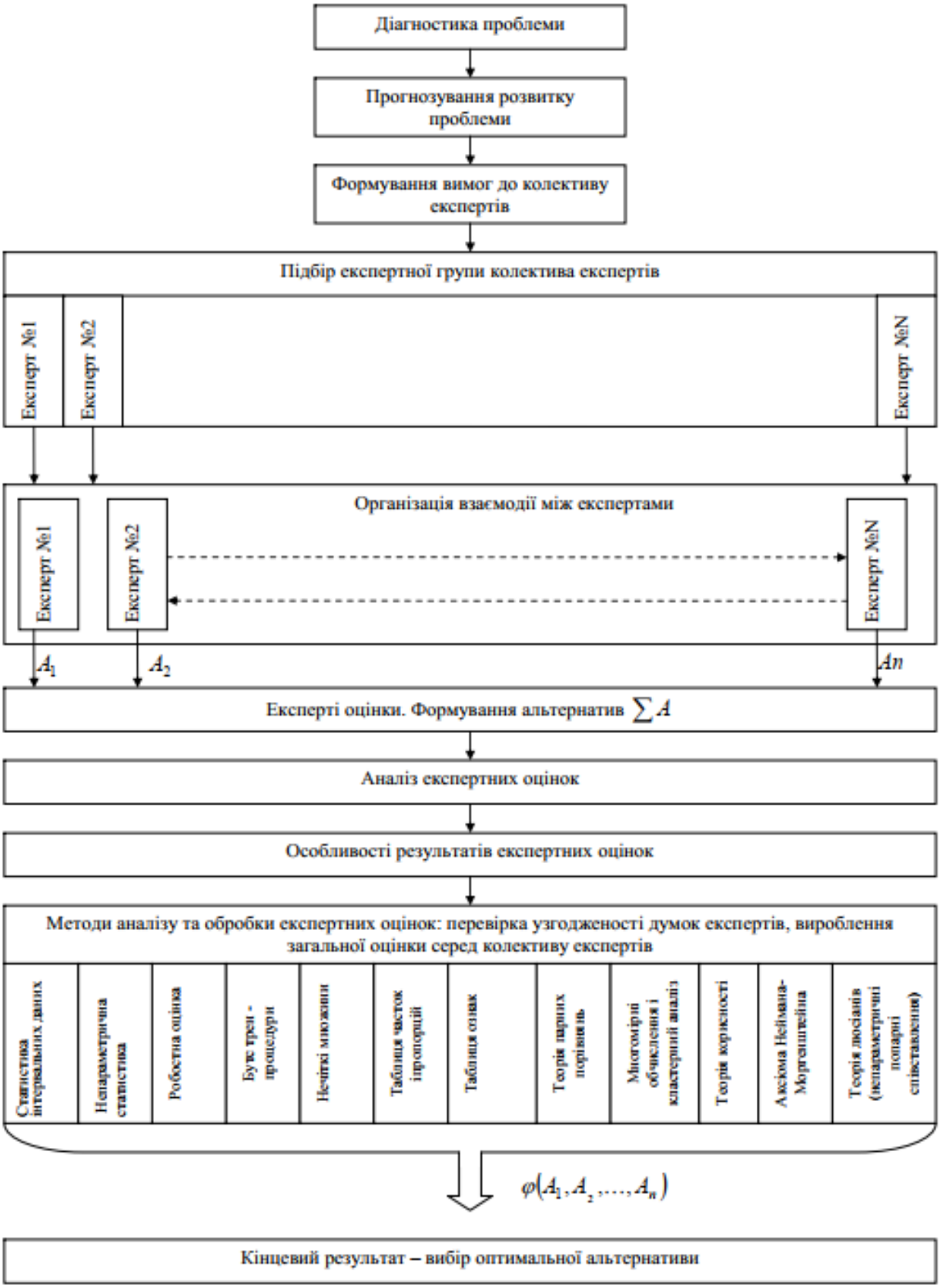

Рисунок 3.2 Структуризація завдань підготовки й прийняття рішень

Виходячи з викладеного, введемо деякі поняття. Під підготовкою колективної експертизи розумітимемо попередню поетапну розробку концептуальної схеми експертизи і підбір фахівців для вирішення проблему в даній області – експертів, а реалізацією експертизи назвемо процес рішення поставленої задачі перед експертами і методи її рішення. Підбір експертів є важливим, якщо не найважливішим, завданням колективного прийняття рішень. [6]

У колективному експертному оцінюванні (КЕО) роботу з відбору експертів зазвичай починають із визначення областей наукових, технічних, адміністративних та інших інтересів, які зачіпають дану проблемну тематику, а далі визначається чисельність групи; як правило, для кожного завдання регламентується своя кількість експертів. Окрім дослідження особистих якостей експертів в КЕО, слід враховувати так само особливості діяльності групи експертів. Відомо, що:

- коли кількість об’єктів складає від 3 до 12 одиниць, узгодженість між експертами є дуже високою;
- доречно включати в групу від 10 до 30 експертів, хоча можливі деякі відхилення, як на збільшення, так і на зменшення чисельності, а при великій чисельності групи виникають проблеми з організацією експертизи;
- експерти чутливі до зворотного зв’язку і наближають свої оцінки до середньогрупової оцінки, яка їм повідомляється, хоча вона може бути і фіктивною;
- у проміжних ситуаціях найбільшою мірою виявляється відмінність між оцінками експертів [9];
- для забезпечення стабільності оцінок експертів у серіях експериментів необхідно розглядати невелику кількість об’єктів, які порівнюватимуться: від 5 до 9 об’єктів;

надійним правилом зупинки експертної процедури [22] вважається не узгодженість оцінок експертів, а їх стабілізація від етапу до етапу, мірою якої може бути, наприклад,

частина експертів, які змінили оцінки між сусідніми етапами експертизи.

Для того, щоб отримувана експертна інформація була якісною, необхідне виконання наступних умов:

наявність експертної групи, що складається з фахівців, професійно знайомих з об’єктом експертизи і що мають досвід експертної роботи;

наявність аналітичної групи, що професійно володіє технологією організації і проведення експертиз, методами отримання і аналізу експертної інформації;

отримання достовірної експертної інформації;

організація взаємодії між експертами;

коректна обробка й аналіз експертної інформації.

До основних способів формування експертних груп можна віднести [3, 4, 22]:

- спосіб призначення. (Керівник проекту або ОПР призначає і формує групу експертів самостійно. Виділяють два основні способи: складають експертну групу з фахівців, зацікавлених в проведенні експертизи і схильних до колективного обговорення; призначення авторитетних осіб, вирішення яких не викликає сильних заперечень у інших співробітників);
- висунення експертів науковими колективами. Висунення фахівців до складу експертної групи може здійснюватися колективами підрозділів даної організації шляхом відкритого або таємного голосування. У такий спосіб можуть бути відібрані експерти, що користуються загальною довірою і пошаною, незалежно від їх службового положення. Цей спосіб формування експертної групи

доцільний, коли рішення задачі експертизи зачіпає інтереси або престиж окремих осіб, наприклад, при оцінці якості виконаних НДР з метою їх преміювання [22]. Рішення, вироблене експертною групою, створеною методом висунення, враховує не тільки об’єктивні показники значущості робіт, але і сумлінність експертів, складність поставленого завдання та інші додаткові чинники;

- документаційний спосіб. Спосіб відбору експертів за об’єктивними (документаційними) характеристиками: стажем роботи, посадою, вченим ступенем, кількістю успішних проектів і т. п. Вирішення експертної групи, створеної у такий спосіб, володіє певною авторитетністю. З погляду керівництва підприємства авторитетність такої групи нижче, ніж експертної групи, сформованої способом призначення. Яких-небудь особливих переваг щодо очікуваної якості результатів документаційний спосіб не представляє;
- спосіб тестування. Відбір експертів може бути проведений з деякої сукупності можливих експертів за наслідками виконання ними серії тестів (вирішення серії завдань) [3]. Застосування цього способу доцільне в тих випадках, коли надалі відібраним експертам доведеться багато разів вирішувати однотипні вузькоспеціальні завдання;
- спосіб послідовних рекомендацій. Один експерт, що є крупним фахівцем з аналізованої проблеми, повинен вказати умови, за яких проблема може бути вирішена, і він особисто міг би узяти на себе її рішення. Після того, як ці умови встановлені, експерт повинен назвати експертів, які могли б забезпечити досягнення вказаних їм проміжних цілей. Експерти виступають в другому етапі опиту,

коли з’ясовуються умови досягнення проміжних цілей і визначаються експерти, які можуть забезпечити досягнення проміжних цілей другого рівня та ін.;

- спосіб взаємних рекомендацій або метод «сніжної грудки». Спочатку опитують одного фахівця з проблеми експертизи. Він повинен назвати інших експертів, які, на його думку, увійдуть до складу експертної групи. Ці експерти називають ще ряд осіб (можливе включення і особи того, що рекомендував їх) і т. д. У результаті поступовий круг взаємних рекомендацій замикається, і формується група потенційних експертів.

Що стосується організації взаємодії між експертами, то виділяють три види взаємодії:

- вільний обмін;
- регламентований обмін;
- експерти, ізольовані один від одного.

При обробці результатів використовуються різні методи. Це, перш за все, систематизація чисельних різновидів методу Делфі, вдосконалення процедур обміну інформацією між експертами в процесі експертизи, а також подальший розвиток методу «мозкової атаки», сценаріїв, ситуаційного аналізу. При проведенні експертизи складних об’єктів, зокрема, для експертизи і прогнозування науково-технічних об’єктів, розвивалися і удосконалювалися такі методи, як ПАТЕРН, методи Глушкова і Поспелова, система АСАС, різні різновиди використання методу «дерева цілей» і критеріїв, розроблялися механізми виявлення експертних знань і оцінок. У даний час все більшого значення набуває проведення комплексних експертиз при оцінці складних об’єктів. [35]

Різні види експертної інформації вимагають як різних методів її отримання, так і різних методів обробки. При практичному використанні значна увага

приділяється як якісним, так і кількісним методам отримання експертної інформації. Достатньо широко використовується і розвивається мова бінарних відносин для одноманітного представлення кількісної та якісної експертної інформації. Розробляються методи вимірювання експертної інформації [9]. До основних проблем належать:

- проблема уявності експертної інформації;
- проблема єдиності вимірювань;
- проблема адекватності.

Остання особливо важлива для визначення коректних перетворень експертної інформації при розрахунках результуючих експертних оцінок – результату роботи експертних комісій. Проблема єдиності вимірювань експертної інформації тісно пов'язана з введенням основних шкал теорії вимірювань: шкал інтервалів, різниць, відносин, порядкових шкал і т. д.

Основні етапи аналізу експертної інформації представлені на рис.3.

Отримання опису альтернатив вимагає розробки методів вирішення завдань: побудови множини можливих і допустимих альтернатив, формування наборів аспектів, істотних для оцінки альтернатив, критерійного простору, впорядковування альтернатив за критеріями, що характерні загальним завданням оцінювання. Сенс завдання експертного оцінювання (ЕО) полягає в зіставленні даній системі вектора з Em.

Основні етапи вирішення ЕО:

1) Визначення множини допустимих оцінок (МДО). На даному етапі визначається підмножина множини $E = \bigcup_{m=1}^{\infty} E_m$, в якій шукається оцінка системи [3].

2) Визначення найбільш точної оцінки. З МДО вибирається оцінка, яка найточнішевідображає властивості оцінюваної системи, що дозволяє представити ЕО у вигляді завдання прийняття рішень <Ω, ОП>, де Ω є

МДО, а ОП – принцип оптимальності, що виражає уявлення про найбільш оптимальну оцінку і задається функцією вибору:

$$C_{оп}(X)=\begin{cases} a, & якщо\ a \in X \subseteq \Omega, \\ \varnothing, & якщо\ a \notin X \subseteq \Omega, \end{cases}$$

де *a* – оцінка системи, яка є рішенням задачі < Ω, ОП>.

Рисунок 3.3 Основні етапи аналізу експертної інформації

Відповідно до етапів, рішення ЕО зводиться до послідовного вирішення двох завдань вибору: <E,ОП1> і <Ω,ОП> , де ОП1 – принцип оптимальності, що задає допустимість оцінки; ОП – принцип оптимальності, що задає точність оцінки з Ω ; рішенням першої задачі є Ω = СОП1 (E) ; рішенням другої задачі є оцінка a = СОП (Ω).

Принципи оптимальності ОП1 і ОП залежать як від самої оцінюваної системи, так і від оцінюючої особи, роль якої аналогічна до ролі, особи що приймає рішення (ОПР) у загальному завданні прийняття рішень (рис. 3.4).

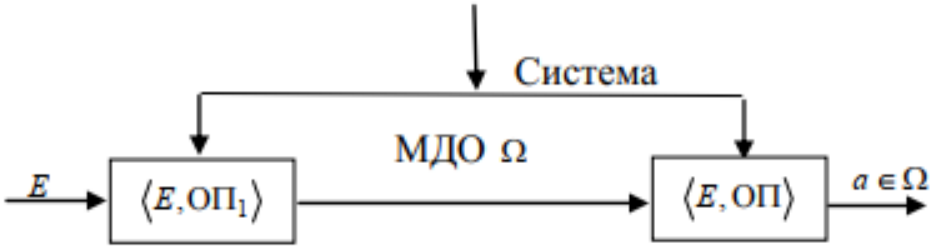

Рисунок 3.4 Модель прийняття рішень

Аналіз поширених експертиз показує [3], що в процесі їх побудови можна виділити певну послідовність дій:

-експерт знаходить множину допустимих оцінок Ω , у якій міститься оцінка, що шукається;

-експерт визначає множину допустимих оцінок , з якої визначають вибір експертизи;

-кожен експерт визначає свою оцінку, вирішується завдання оптимального вибору оцінки (при цьому допускається обмін думок експертів між собою);

-за визначеним раніше алгоритмом ОПР проводить обробку отриманої від експертів інформації і обчислюється результуюча оцінка з Ω , що є вирішенням початкової ЕО;

-при незадовільному вирішенні експертів ОПР може надати додаткову інформацію з можливістю організації зворотного зв’язку, після чого необхідно провести повторну процедуру експертизи (рис. 3.5.)

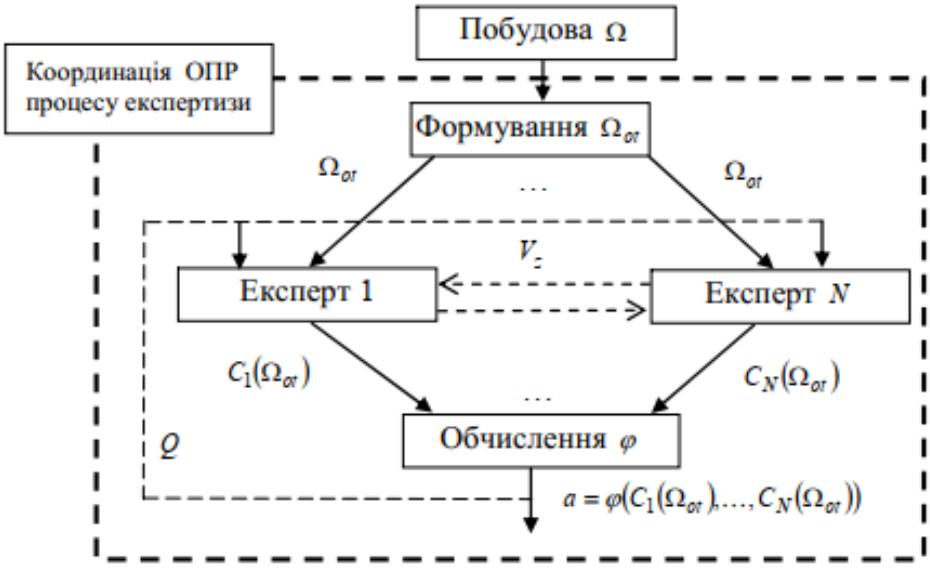

Рисунок 3.5 Узагальнена послідовність дій експертизи

Для того, щоб отримувана експертна інформація була якісною, необхідне виконання наступних умов:

- наявність експертної комісії, що складається з фахівців, які професійно знайомі з об’єктом експертизи і мають досвід експертної роботи;
- наявність аналітичної групи, що професійно володіє технологією організації і проведення експертиз методами отримання й аналізу експертної інформації;
- отримання достовірної експертної інформації;
- коректна обробка й аналіз експертної інформації

Одним з важливих завдань обробки експертної інформації є визначення результуючих експертних оцінок – результату колективної роботи експертів. Для цієї мети може бути введений аналог відстані – міра близькості між ранжируваннями, класифікаціями і т. д. Це дозволяє розробити коректні способи визначення результуючих експертних оцінок, таких як медіана Кемені, метод рядкових сум та ін. У багатьох випадках

оцінки експертів об’єктів експертизи виявлялися точнішими при використанні методів багатокритерійного оцінювання, при застосуванні методів визначення чинників, що характеризують об’єкти експертизи, зокрема, багатовимірне шкалування, факторний аналіз, статистичні методи визначення істотних чинників. Розвивалися методи оцінки їх порівняльної ваговитості, принципи прийняття рішень на основі оцінок об’єктів за багатьма критеріями, що далеко не завжди зводяться до згортків. [16]

3.2 Методика оцінювання інформаційних ризиків в системі управління інформаційною безпекою

Оцінювання ризику полягає у визначенні його рівня та порівнянні з максимально допустимим. За основу методики оцінювання інформаційного ризику в ІС обрано наступну методику, але для оцінювання системи управління ІБ використаємо оцінні вимоги, визначені в стандарті ISO/IEC 27001 (табл. 3.1). Безпосередню модель загроз та вразливостей побудуємо, виходячи з типових вразливостей ІБ згідно з ISO/IEC 27002 (табл. 3.2). У методиці описано процес оцінювання ризиків ІБ, а також розглянуто спосіб кількісного оцінювання ризиків ІБ. Вона призначена для оцінювання ризиків ІБ у рамках побудови або вдосконалення системи ІБ на підприємствах малого і середнього бізнесу. [12]

Основним завданням методики є визначення кількісного показника ризику ІБ з метою прийняття ефективних заходів щодо захисту інформації (ЗІ). Запропонована методика оцінювання ризиків дозволяє виконати повноцінний аналіз й оцінку ризиків без допомоги висококваліфікованих фахівців і може бути адаптованою для оцінювання ризиків ІБ.

Таблиця 3.1 Вимоги до інформаційної безпеки

№	Розділ основних вимог до ІБ	Вимоги до ІБ
1	2	3
1.	Загальні вимоги до СУІБ	1.1. СУІБ створена
		1.2. СУІБ впроваджена
		1.3. СУІБ знаходиться в експлуатації
		1.4. Здійснюється моніторинг СУІБ
		1.5. СУІБ аналізується
		1.6. СУІБ удосконалюється
2.	Створення й управління СУІБ	2.1. Визначені сфери дії та межі СУІБ
		2.2. Визначення дій СУІБ у виняткових ситуаціях
3.	Політика безпеки	3.1. Містить у собі основу для визначення її цілей
		3.2. Встановлює загальні напрямки та принципи діяльності щодо ІБ
		3.3. Враховує вимоги підрозділу
		3.4. Враховує вимоги законодавства та нормативної бази
		3.5. Враховує конкретні обов’язки в сфері безпеки
		3.6. Поєднується зі стратегічним контекстом управління ризиками в організації, у якій буде створюватися СУІБ
		3.7. Встановлює критерії для оцінювання ризиків
		3.8. Затверджена керівництвом

4.	Активи	4.1. Наявні реєстри інформаційних активів
		4.2. Власники активів правильно ідентифіковані
		4.3. Наявні правила маркування конфіденційних документів
		4.4. Наявні правила поведінки з конфіденційними документами
		4.5. Наявна схема класифікації документів

Таблиця 3.2 Характеристика невідповідності вимогам нормативно-правової бази в сфері ІБ

Сума виконаних вимог	Ризик невідповідності ІС вимогам законодавства (Rn)
16–21	0,01
11–15	0,25
<10	0,5
Не виконуються	0,9

Загальний алгоритм оцінювання ризику згідно з даною методикою наведено на рис. 3.6. Для його розуміння слід розглянути кожну процедуру окремо.

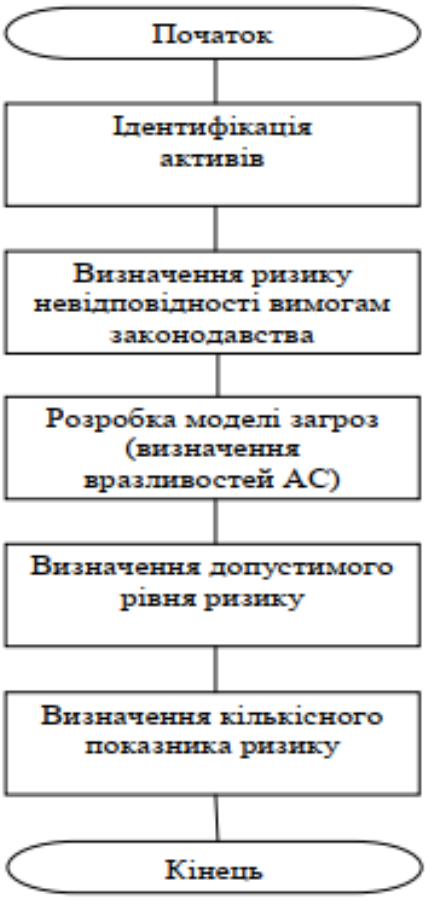

Рисунок 3.6 Схема алгоритму оцінювання ризику ІБ

Ідентифікація активів. На даному етапі експерти проводять інтерв'ю з особовим складом підрозділу або відділу з метою виявлення використовуваних активів. Активи системи інформаційних технологій є компонентом або частиною загальної системи, у яку підрозділ безпосередньо вкладає кошти, що, відповідно, потребують захисту з боку підрозділу. При ідентифікації активів слід мати на увазі, що будь-яка система інформаційних технологій включає в себе не тільки апаратні засоби, але й програмне забезпечення. [9]

Існують такі види активів: інформація (файли, що містять дані про діяльність організації); апаратні засоби (комп'ютери, принтери); програмне

забезпечення, включаючи прикладні програми (обробки текстів, цільового призначення); обладнання для забезпечення зв'язку (телефони, мідні та оптико-волоконні кабелі); персонал; престиж організації.

Визначення ризику невідповідності вимогам законодавства в галузі ІБ. Будь-який інформаційних технологій, повинен дотримуватися вимог законодавчих актів у цій галузі. Їх невиконання може спричинити цивільну, кримінальну, адміністративну, дисциплінарну та іншу, передбачену законодавством відповідальність. Ризик невиконання нормативних вимог впливає на загальний ризик ІБ. Алгоритм визначення ризику невідповідності вимогам законодавства у сфері ІБ включає в себе проведення всебічного аналізу стану системи інформаційного захисту з метою виявлення невідповідності. У ході аналізу всім вимогам, які не порушують, присвоюють значення "1", в іншому випадку – "0". Усі значення, яким присвоєно "1", додають, решту – не враховують.

Дізнавшись (підрахувавши) кількість виконаних вимог, можна визначити ризик невідповідності ІС вимогам законодавства. Для цього використаємо табл. 2. Оскільки не існує визначеної кількості вимог, а є лише перелік тих (описаний в [11]), що повинні бути виконані, нам слід підібрати їх (їхню кількість) саме під нашу ІС. У табл. 3.3 наведено вимоги до ІБ згідно зі стандартом ISO/IEC 27001 (відповідно до чотирьох розділів, а саме: "Загальні вимоги до системи управління інформаційною безпекою (СУІБ)", "Створення і управління СУІБ", "Політика безпеки", "Активи"), загальна їх кількість становить 21. За методикою, викладеною в [6], отримаємо характеристики невідповідності вимогам нормативно-правової бази у сфері ІБ (табл. 2).

Розробка моделі загроз. При розробці моделі загроз слід визначити вразливості (організаційні та технічні), притаманні визначеній ІС. У нашому випадку кількість організаційних та технічних вразливостей обираємо,

виходячи з табл. 3.3, яка описує модель загроз та вразливостей, передбачених стандартом ISO/IEC 27002:2005 [12]. Можливість використання організаційних вразливостей встановлюють експертним методом, аналізуючи застосування організаційних заходів ЗІ. У ході проведення аналізу всім організаційним заходам, які виконують, присвоюють значення “1”, в іншому випадку – “0”. Усі значення, яким присвоєно “1”, додають, решту – не враховують. Використовуючи методику, викладену в [6], отримаємо характеристики організаційних вразливостей ІБ ІС (табл. 3.4).

Таблиця 3.3 Модель загроз та вразливостей

№	Галузь безпеки	Вразливість	Загроза, що використовує дану вразливість
	Безпека кадрових ресурсів (ISO/IEC 27002:2005, розділ 8)	1.1. Недостатній рівень навчання персоналу щодо безпеки	1.1. Помилка персоналу технічної підтримки
		1.2. Неосвіченість користувачів у питаннях безпеки	1.2. Помилка користувачів
		1.3. Відсутність політики безпеки в сфері коректного використання засобів телекомунікацій та передачі повідомлень	1.3. Відсутність політики безпеки в сфері коректного використання засобів телекомунікацій та передачі повідомлень
		1.4. Права доступу залишаються в працівника навіть після звільнення	1.4. Несанкціонований доступ
		1.5. Невмотивований та незадоволений персонал	1.5. Зловживання засобами обробки інформації
		1.6. Робота без нагляду персоналу, що працює в неробочий час	1.6. Грабіж

		1.7. Відсутність механізмів моніторингу	1.7. Несанкціоноване використання програмного забезпечення
	Фізична безпека і безпека навколишнього середовища (ISO/IEC 27002:2005, розділ 9)	2.1. Відсутність фізичного захисту будівлі, дверей та вікон	2.1. Грабіж
		2.2. Розміщення обладнання в зоні, якій загрожує затоплення	2.2. Затоплення
		2.3. Незахищене зберігання інформації	2.3. Грабіж
		2.4. Відсутність схеми періодичної заміни обладнання	2.4. Закінчення терміну експлуатації засобів зберігання інформації
		2.5. Стрибки напруги	2.5. Флуктуація електроживлення
		2.6. Нестабільне електроживлення (подача електроенергії)	2.6. Флуктуація електроживлення
	Управління комунікаціями та операціями (ISO/IEC 27002:2005, розділ 10)	3.1. Складний користувацький інтерфейс	3.1. Помилка персоналу
		3.2. Передача або повторне використання засобів зберігання інформації без потрібного очищення	3.2. Несанкціонований доступ
		3.3. Неадекватний контроль змін	3.3. Збій системи безпеки
		3.4. Неадекватне керування мережею	3.4. Перенавантаження трафіка
		3.5. Відсутність розподілу обов’язків	3.5. Зловживання системою (випадкове чи навмисне)
		3.6. Відсутність процедур резервного копіювання	3.6. Відсутність процедур резервного копіювання

		3.7. Відсутність оновлень програмного забезпечення, яке використовують для захисту від шкідливих кодів (вірусів)	3.7. Вірусне ураження
		3.8. Неконтрольоване копіювання	3.8. Грабіж
		3.9. Незахищене з’єднання з мережами загального користування	3.9. Використання програмного забезпечення неавторизованими користувачами
	Контроль доступу (ISO/IEC 27002:2005, розділ 11)	4.1. Некоректне розмежування доступу в мережах	4.1. Несанкціоноване під’єднання до мережі
		4.2. Відсутність механізмів ідентифікації та аутентифікації	4.2. Присвоєння чужого користувацького ідентифікатора
		4.3. Відсутня чи некоректна політика контролю доступу	4.3. Несанкціонований доступ до інформації, системи чи програмного забезпечення
		4.4. Відсутність чи недостатнє тестування програмного забезпечення	4.4. Використання програмного забезпечення неавторизованими користувачами
		4.5. Незадовільне керування паролями	4.5. Присвоєння чужого користувацького ідентифікатора
		4.6. Відсутність захисту мобільного комп’ютерного устаткування	4.6. Відсутність захисту мобільного комп’ютерного устаткування
		4.7. Відсутність “виходу із системи”, коли залишають робоче місце	4.7. Відсутність “виходу із системи”, коли залишають

			робоче місце
		4.8. Відсутність контролю прав доступу користувачів	4.8. Доступ зі сторони користувачів, які звільнились з організації, або перевелися на інше місце роботи
		4.9. Відсутність відключення та зміни стандартних попередньо встановлених облікових записів та паролів	4.9. Несанкціонований доступ до інформації, системи чи програмного забезпечення
		4.10. Неконтрольоване використання системних утиліт	4.10. Обхід механізмів контролю системи чи додатка
	Придбання, розробка та супровід інформаційних систем (ISO/IEC 27002:2005, розділ 12)	5.1. Недосконала політика безпеки в сфері використання криптографії	5.1. Порушення законодавства або нормативної бази
		5.2. Невиконання або виконання в недостатньому обсязі тестування програмного забезпечення	5.2. Використання програмного забезпечення неавторизованими користувачами
		5.3. Відомі дефекти в програмному забезпеченні	5.3. Використання програмного забезпечення неавторизованими користувачами
		5.4. Недостатній захист криптографічних ключів	5.4. Недостатній захист криптографічних ключів
		5.5. Відсутність контролю вхідних та вихідних даних	5.5. Помилка
		5.6. Відсутність перевірки даних, що обробляються	5.6. Викривлення інформації

		5.7. Неконтрольоване завантаження та використання програмного забезпечення	5.7. Шкідливе програмне забезпечення

Таблиця 3.4. Характеристика організаційних вразливостей ІБ ІС

Загальна кількість заходів захисту, що виконують (організаційні вразливості, які відсутні для даної інформаційної системи)	Коефіцієнт вразливості (K_0)
19–23	0,01
11–18	0,25
Менше 10	0,5
Не виконують	0,9

Можливість використання технічних вразливостей встановлюють експертним методом, аналізуючи технічні заходи ЗІ, що застосовують у даній ІС. Під час проведення аналізу всім технічним заходам, які виконують, присвоюється значення “1”, в іншому випадку – “0”. Усі значення, яким присвоєно “1”, додають, решту – не враховують. Відповідно до методики, викладеної в [6], отримаємо характеристики технічних вразливостей ІБ ІС (табл. 5).

Визначення допустимого рівня ризику. Допустимим ризиком прийнято вважати той, який у даній ситуації є прийнятним при існуючих суспільних цінностях. Для ІС рекомендоване значення допустимого ризику не повинне перевищувати 5%. Це обумовлюється, у першу чергу, тим, що кошти, вкладені за звітний період (наприклад, 1 рік), можуть становити десятки мільйонів гривень. У разі реалізації однієї з актуальних загроз завданий

збиток може становити більше 5%, а отже, є неприпустимим і вимагає вжиття ефективних заходів.

Визначення кількісного значення ризику. Кількісне значення інформаційного ризику реалізації певної загрози з усього переліку актуальних загроз з урахуванням наявності вразливостей розраховуємо за такою формулою [6]:

$$R = P_{загр} \cdot R_n \cdot C \cdot \frac{K_o + K_t}{2},$$

де R – кількісна величина інформаційного ризику;

Рзагр– імовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз;

R_n – ризик невідповідності вимогам законодавства;

C – цінність активу;

K_0 – імовірність використання організаційних вразливостей;

K_t – імовірність використання технічних вразливостей.

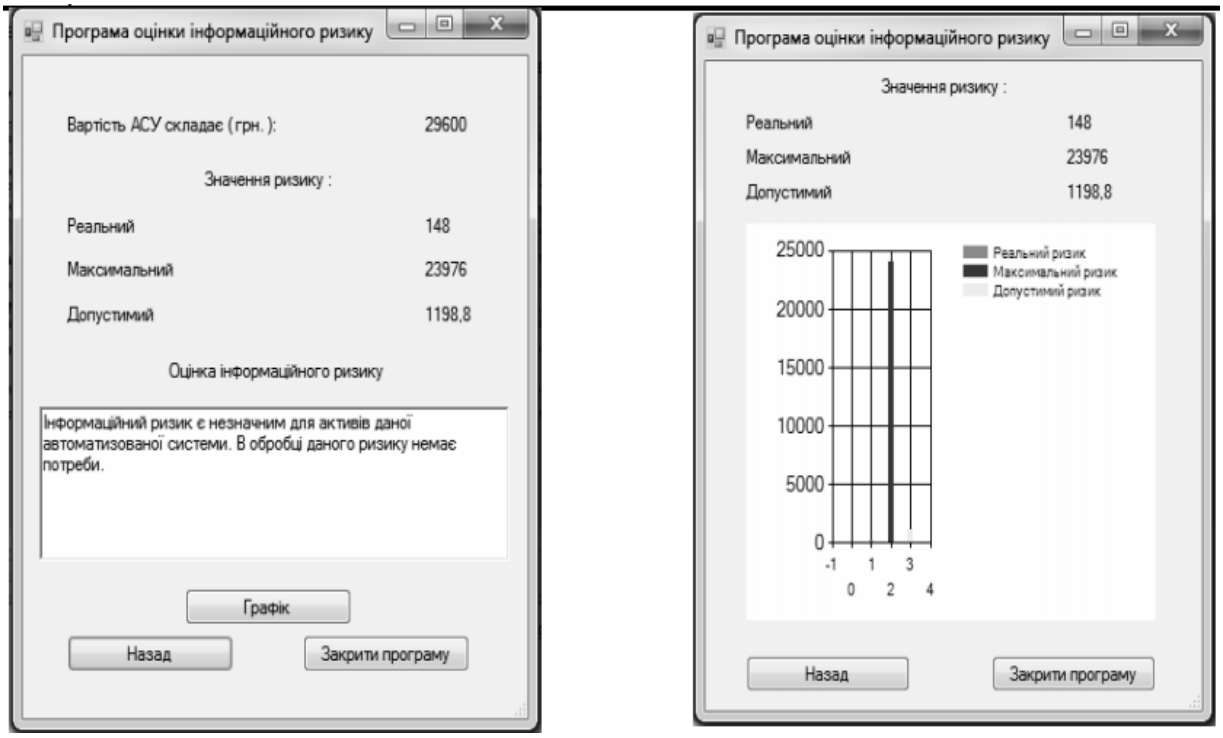

Рис. 3.7. Кінцевий результат (оцінка інформаційного ризику)

Реалізація прототипу експертної системи оцінювання інформаційного ризику. Результатом перевірки працездатності даної методики є розроблений програмний продукт, який є прототипом експертної системи оцінювання інформаційного ризику в ІС. Кінцеві результати роботи програми висвітлені у двох формах (рис. 3.7), причому на одній з них показано повідомлення, що містить рекомендації щодо необхідної кількості заходів ІБ, а на іншій – графічне зображення отриманих результатів оцінювання.

3.3 Висновок з розділу

Експертна інформація відіграє важливу роль при застосуванні сучасних методів підтримки прийняття рішень. Методи її отримання, уявлення й обробки складають невід'ємну частину технології підтримки прийняття рішень. Ефективність використання цієї інформації істотно залежить від коректності і обґрунтованості використовуваних методів.

Одним з важливих завдань обробки експертної інформації є визначення результуючих експертних оцінок – результату колективної роботи експертів. Для цієї мети може був введений аналог відстані – міра близькості між ранжируваннями, класифікаціями. Це дозволяє розробити коректні способи визначення результуючих експертних оцінок. Реалізовано прототип експертної системи оцінювання інформаційного ризику. Результатом перевірки працездатності даної методики є розроблений програмний продукт, який є прототипом експертної системи оцінювання інформаційного ризику в ІС. Кінцеві результати роботи програми висвітлені у двох формах, причому на одній з них показано повідомлення, що містить рекомендації щодо необхідної кількості заходів ІБ, а на іншій – графічне зображення отриманих результатів оцінювання.

ВИСНОВКИ

В цілому застосування експертного методу оцінки ризику дозволяє наочно простежити вплив окремих вихідних факторів на кінцевий результат системі управління, виявити на попередній стадії найбільш важливі чинники ризику, вжити заходів по їх мінімізації.

Більшість рішень приймаються в умовах ризику, що обумовлено рядом факторів: відсутністю повної інформації, наявністю протиборчих тенденцій, елементами випадковості і багатьом іншим. В умовах нестабільності проблема ризику має велике значення при обґрунтуванні рішень не тільки стратегічного характеру, але і на стадії короткострокового планування.

У зв'язку з цим проблема оцінки ризиків набуває самостійне теоретичне і прикладне значення як важлива складова частина теорії і практики системи управління інформаційною безпекою. Під ризиком слід розуміти наслідок дії або бездії, в результаті якого існує реальна можливість отримання невизначених результатів різного характеру, як позитивного, так і негативного впливу на систему управління інформаційною безпекою.

Більшість дослідників відзначають, що слід не уникати ризику на етапі прийняття рішення, а вміти грамотно, професійно керувати ним. Призначення аналізу ризику – дати необхідні дані для прийняття рішень про доцільність участі в проекті і передбачити заходи щодо захисту від можливих втрат.

В даний час найбільш поширеними є наступні методи аналізу ризиків:

- статистичний;
- експертних оцінок;
- аналітичний;
- аналіз наслідків накопичення ризику;
- метод використання аналогів;

– комбінований метод.

Метод експертних оцінок відрізняється способом збору інформації для побудови кривої ризику. При цьому методі передбачаються збір і вивчення оцінок, зроблених різними фахівцями (внутрішніми або зовнішніми експертами), що стосуються ймовірності виникнення різних рівнів втрат. Оцінки базуються на врахуванні всіх факторів ризику, а також на статистичних даних.

У процесі роботи було проведено аналіз зовнішнього ризику. Для цього розроблені математична модель і методика розрахунку інтегрального показника впливу зовнішнього ризику, а також показано взаємозв'язок даного показника з вибором оптимальної стратегії розвитку. Її висока динамічність і невизначеність чинників вимагають величезних ресурсів для створення потенціалу протидії загрозам. У зв'язку з цим для збереження основних параметрів діяльності системи управління інформаційною безпекою, створення передумов до підвищення ефективності може здійснювати прогнозування впливу різних чинників на основі розрахунку інтегрального показника.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alberts C. J. Operationally Critical Threat, Asset and Vulnerability Evaluation / C. J. Alberts, S. G. Behrens, R. D. Pethia, W. R. Wilson. – 2018. – P. 84.
2. Endorf C. F. Measuring ROI on security / Carl F. Endorf // Information security management handbook / Edited by Harold F. Tipton and Micki Krauze. – 6th edition. – Boca Raton: Auerbach Publications, 2017. – Part 1, Section 1.1, Ch. 12. – P. 133-137.
3. Henry K. Risk management and analysis / Kevin Henry // Information Security Management Handbook / Edited by Harold F. Tipton, Micki Krauze. – 6th edition. – Boca Raton : Auerbach Publications, 2017. – Part 1, Section 1.4, Ch. 28. – P. 321-329.
4. ISO/IEC 27035. Information technology. Security techniques. Information security incedent management. – 2011. – 78 p.
5. Landoll D. The security risk assessment handbook: a complete guide for performing security risk assessments / Douglas J. Landoll. – Boca Raton: Auerbach Publications, 2016. – 504 p.
6. Rittinghouse J. W. Business continuity and disaster recovery for infosec managers / John W. Rittinghouse, James F. Ransome. – Oxford: Elsevier, 2015. – 408 p.
7. Spedding L. Business risk management handbook: a sustainable approach / Linda Spedding, Adam Rose. – Oxford: Elsevier, 2018. – 768 p.
8. Андрианов В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов. – М.: ЦИПСиР, 2016. – 373 с.
9. Балашов П. А. Оценка рисков информационной безопасности на основе нечеткой логики / П. А. Балашов, В. П. Безгузиков, Р. И. Кислов //

[Електронний ресурс]. – режим доступу: http://www.nwaktiv.ru/textstat2/index.html

10. Баранова Е. К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2013. № 1(49). –С. 15-26.
11. Владимирцев А. В., Марцынковский О. А. Использование метода экспертных оценок при анализе и оценке рисков системы менеджмента. – Ассоциация по сертификации «Русский Регистр» – Санкт-Петербург: 2017. – 425 с.
12. Гарасим Ю. Р. Аналіз систем захисту, які мають властивість живучості / Ю. Р. Гарасим // Військово-технічний збірник. – 2016. № 1 (4). – С. 87–95.
13. Гарасим Ю. Р. Забезпечення живучості та неперервності функціонування систем захисту інформації / Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій // Вісник Нац. ун-ту “Львівська політехніка” “Автоматика, вимірювання та керування”. – 2014. – № 741. – С. 105-112.
14. Дубинин Е. А. Оценка относительного ущерба безопасности информационной системы: монография / Е. А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – 192 с.
15. Замула О. А. Аналіз міжнародних стандартів в галузі оцінювання ризиків інформаційної безпеки / О. А. Замула, В. І. Черниш // Системи обробки інформації: збірних наукових праць. – Х.: ХУ ПС, 2014. – Вип. 2(92). – С. 53-56.
16. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. - Наука і техніка Повітряних Сил Збройних Сил Украіни, 2017, – № 2(15). – С. 47-52.

17. Киселева И. А., Искаджян С. О. Информационные риски: методы оценки и анализа // ИТпортал, 2017. №2 (14). – С.142-146.
18. Козлова Е. А. Оценка рисков информационной безопасности с помощью метода нечеткой кластеризации и вычисления взаимной информации. Молодой учёный. Ежемесячный научный журнал №5 (52)/2015. – С. 45-51.
19. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения – К.: МК-Пресс, 2016. – 324 с.
20. Легчекова Е. В., Титов О. В. Метод расчета риска информационной безопасности. [Електронний ресурс]. – Режим доступу: http://lib.ibteu.by/bitstream/handle/22092014/3600/Легчекова%20Е.В.%2C%20Титов%20О.В.%20 Метод%20расчета.pdf
21. Малюк А. А. Теория защиты информации. – М.: Гор. линия-Телеком, 2015. – 184 с.
22. Методология OCTAVE для оценки информационных рисков [Електронний ресурс]. – Режим доступу: http://www.risk24.ru/octave.htm
23. Методологии управления ИТ-рисками [Електронний ресурс]. – Режим доступу:http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi bezopasnosti/metodologii-upravleniya-it-riskami
24. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Управление рисками информационной безопасности. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2016.– 245 с.
25. Петренко С. А., Петренко А. А. Аудит безопасности Intranet.– М.: ДМК Пресс, 2016. – 416 с.
26. Петренко С. А. Анализ рисков в области защиты информации. Методическое пособие. – ООО «Издательский Дом «Афина» г. СанктПетербург, 2016. – 456 с.

27. Плетнев П. В., Белов В. М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУРа № 1 (25), часть 2, июнь 2016. – С. 35-38.
28. Прокопенко А. В. Синтез систем реального времени с гарантированной доступностью программно-информационных ресурсов: монография / А. В. Прокопенко, М. А. Русаков, Р. Ю. Царев. – Красноярск: Сиб. федер. ун- т, 2016. – 92 с.
29. Саати Т. Принятие решений. Метод анализа иерархий / Томас Саати: Пер. с англ. Р. Вачнадзе. – М.: Радио и связь, 2013. – 320 с.
30. Сердюк В. А. Анализ современных тенденций построения моделей информационных атак / В. А. Сердюк // Информационные технологии. – 2014. – № 5. – С. 94-101.
31. Сердюк В. А. Организация и технологии защиты информации. Обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. – М.: Высшая Школа Экономики (Государственный Университет), 2015. – 576 с.
32. Ткаченко В. Современные подходы к оценке рисков информационных технологий / В. Ткаченко, В. Сысоев // [Електронний ресурс]. – Режим доступу: http://www.cbz.com.ua/resources/files/12224515494d0f29e1cacc9.pdf
33. Харитонов Е. В. Согласование исходной субъективной информации в методах анализа иерархий // Математическая морфология. –2017. – Т. 3. – Вып. 2. – С. 41-51.
34. Черныш В. И. Методы оценивания информационных рисков компании / В.И.Черныш // Материалы XV Международного юбилейного молодёжного форума «Радиоэлектроника и молодежь в XXI веке»: Сб. тезисов, 18–20 апреля 2015 р., Т.5. – Х.: ХНУРЭ, 2015. – С. 195.

35. Шаньгин В. Ф. Информационная безопасность и защита информации. – М.: ДМК Пресс, 2016. – 702 с.