МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри кібербезпеки

_____Анна ІЛЬЄНКО
"_____"_____ 20__ р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ "МАГІСТР"

Тема: «Метод оцінювання ризиків інформаційної безпеки»

Виконавець: Євген НЕВОЙТ

Керівник: к.т.н., доцент Андрій ПЕТРЕНКО

Нормоконтролер: к.т.н., доцент Андрій ПЕТРЕНКО

Київ 2024

ДЕРЖАВНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Факультет комп'ютерних наук та технологій
Кафедра кібербезпеки
Освітній ступінь магістр
Спеціальність 125 «Кібербезпека та захист інформації»
Освітньо-професійна програма «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки

_____Анна ІЛЬЄНКО
«30»___08_____2024 р.

ЗАВДАННЯ

на виконання кваліфікаційної роботи

Невойта Євгена Миколайовича

1. Тема кваліфікаційної роботи: «Метод оцінювання ризиків інформаційної безпеки».

затверджена наказом ректора від 30.08.2024 р. №1696/ст.

2. Термін виконання роботи: з 30.08.2024 по 15.12.2024

3. Вихідні дані до роботи:

- аналіз ризиків у сфері інформаційної безпеки;
- ідентифікація та визначення величини ризиків;
- процес обробки ризиків інформаційної безпеки;
- методологія управління ризиками ІБ.

4. Зміст пояснювальної записки:

- Оцінка та обробка ризиків інформаційної безпеки.
- Інструментальні засоби управління ризиками.
- Методологія синтезу системи оцінювання рівня безпеки інформаційних ресурсів.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: презентація.

6.Календарний план-графік

№ з/п	Завдання	Термін виконання	Підпис керівника
1.	Провести аналіз літературних джерел	30.08.2024 – 05.09.2024	*Виконано*
2.	Обґрунтування вибору рішення	06.09.2024 – 15.09.2024	*Виконано*
3.	Дослідження технологій аналізу ризиків	16.09.2024 – 25.09.2024	*Виконано*
4.	Вдосконалення методологічного базису нечітких множин для вирішення задач оцінки ризиків	26.09.2024 – 02.10.2024	*Виконано*
5.	Вдосконалення методу оцінки ризиків в інформаційних системах	03.10.2024 – 25.10.2024	*Виконано*

7.Дата видачі завдання: «30» __08__ 2024 р.

Керівник кваліфікаційної роботи: _____ Андрій ПЕТРЕНКО
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання: _____ Євген НЕВОЙТ
(підпис здобувача вищої освіти) (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Метод оцінювання ризиків інформаційної безпеки».

Об’єкт дослідження – оцінювання та розрахунок ризиків в сфері ІБ.

Предмет дослідження – метод Мамдамі розрахунку ризику інформаційної безпеки засобами нечіткої логіки.

Мета роботи – вдосконалення методу для оцінки ризику ІБ засобами нечіткої логіки з використанням програмного забезпечення MatLab.

Методи дослідження: методи аналізу та оцінка ризиків, нечітка логіка, ідентифікація нелінійної залежності нечіткими базами знань.

Наукова новизна дипломної роботи полягає в наступному: вдосконалений метод нечіткої логіки Мамдамі для оцінювання ризиків інформаційної безпеки організації.

Практична цінність: проведено оцінку ризику інформаційної безпеки організації використовуючи засоби Optimization Toolbox MatLab.

Результати кваліфікаційної роботи рекомендується використовувати для оцінки ризику кібербезпеки підприємства та оцінювання рівня поточного стану ІБ автоматизованої системи для зниження потенційних втрат за рахунок підвищення стійкості функціонування корпоративної мережі.

Дипломна робота складається із списку скорочень, вступу, основної частини, що містить 4 розділи, висновку та списку літератури. Загальний обсяг роботи – 94 сторінки. Робота містить 17 рисунків та 2 таблиці. Список використаних джерел включає 50 джерел.

Ключові слова: АВТОМАТИЗОВАНА СИСТЕМА ОБРОБКИ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ, КОМПЛЕКС СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ, РИЗИК, ЦІЛІСНІСТЬ, ДОСТУПНІСТЬ, ЗАГРОЗА, ВРАЗЛИВІСТЬ, ОЦІНКА РИЗИКУ, НЕЧІТКА ЛОГІКА, МЕТОД МАМДАМІ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ……6
ВСТУП……..7
РОЗДІЛ 1 АНАЛІЗ РИЗИКІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……..9
1.1. Загальний огляд нормативних документів України про захист інформації….9
1.2. Міжнародні стандарти у сфері управління ризиками інформаційної безпеки…….....13
1.3. Система управління інформаційними ризиками…….……19
1.4. Висновок по розділу 1…….……..…..21
РОЗДІЛ 2 ОЦІНКА ТА ОБРОБКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ……..…..23
2.1. Ідентифікація та визначення цінності активів……..24
2.2. Аналіз загроз та вразливостей……29
2.3. Оцінювання та визначення величин ризиків……37
2.4. Процес обробки ризиків інформаційної безпеки……..39
2.5. Висновок по розділу 2……42
РОЗДІЛ 3 ІНСТРУМЕНТАЛЬНІ ЗАСОБИ УПРАВЛІННЯ РИЗИКАМИ …….43
3.1. Методології управління ризиками інформаційної безпеки ……43
3.2. Інструментарій базового рівня ……..47
3.3. Засоби повного аналізу ризиків ……49
3.4. Загальні недоліки та обмеження комерційних програмних продуктів……...58
3.5. Висновок по розділу 3……59
РОЗДІЛ 4 МЕТОДОЛОГІЯ СИНТЕЗУ СИСТЕМИ ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ …….……..…….61
4.1. Методологічний базис нечітких множин для вирішення задач оцінки ризиків …….... 61
4.2. Алгоритм нечіткого висновку Мамдані……77
4.3. Оцінка ризику інформаційної безпеки засобами нечіткої логіки……..79
4.4. Висновок по розділу 4……89
ВИСНОВОК ……..90
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ……91

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АСОІ – автоматизована система обробки інформації;

АС – автоматизована система;

ЕОМ – електронна-обчислювальна машина;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

ІР – інформаційні ресурси;

ІТ – інформаційні технології;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

ПБ – політика безпеки;

СЗІ – система захисту інформації.

КЗЗ – комплекс засобів захисту

ВСТУП

Розвинення та зміцнення, забезпечення найефективнішого та безперебійного функціонування будь-якої системи є цілями діяльності організації.

Для забезпечення реалізації визначених цілей є забезпечення необхідного та достатнього рівня інформаційної безпеки (ІБ) організацій, її інформаційних активів, які визначаються рівнем ІБ.

Актуальність теми. Особливість організації полягає в, тому що негативні наслідки збоїв в роботі наносять збиток інтересам клієнтам та власників. Тому для організацій загрози ІБ представляють небезпеку. Для протидії визначеним загрозам та ефективному забезпеченню заходів з нейтралізації несприятливих наслідків інцидентів ІБ в організаціях, необхідно забезпечити достатній рівень ІБ. Тому оцінювання ризиків та забезпечення ІБ є одним з важливих аспектів діяльності для організацій.

Діяльність в організації, що відноситься до забезпечення ІБ, повинна бути контрольована. Тому компанії регулярно проводять оцінку рівеня ризику ІБ в організаціях та застосовують заходи, які необхідні для управління цим ризиком.

Основними задачами забезпечення достатнього рівня ІБ організацій є встановлення єдиних вимог щодо забезпечення ІБ організацій, а також підвищення ефективності заходів по забезпечення та підтримки ІБ організації.

Ресурси, загрози, вразливі місця. ІС та оцінка загроз – визначають комплекс засобів захисту (КЗЗ), що забезпечить достатній рівень захищеності ІС. Під час оцінювання захищеності враховуються наступні чинники: цінність ресурсів, існуючи вразливості, рівень загроз, ефективність наявних та запланованих методів, способів та засобів захисту.

Мета і завдання виконання кваліфікаційної роботи. Запропонований метод дозволяють провести оцінку рівня поточного стану ІБ автоматизованої системи (АС), знизити потенційні збитки за рахунок підвищення стійкості функціонування корпоративної мережі, розробити концепцію й політику безпеки

АС, а також запропонувати та запровадити плани захисту від виявлених загроз та вразливих місць. На сьогоднішній день існують різноманітні й складні за структурою АС, для яких неможливо підібрати конкретну методику оцінювання ризиків, тому для отримання точних результатів необхідно розробити методику оцінювання ризиків засобами нечіткої логіки та провести розрахунок використовуючи програмне забезпечення Matlab.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

– дослідити методології проведення оцінювання ризику ІБ;

– проаналізувати програмне забезпечення, яке використовується для оцінки ризику та виявити недоліки та обмеження;

–визначити методологічний базис нечітких множин для оцінки ризику та провести розрахунок.

Об’єкт дослідження – оцінювання та розрахунок ризиків в сфері ІБ.

Предмет дослідження – метод Мамдамі розрахунку ризику інформаційної безпеки засобами нечіткої логіки.

Методи дослідження: методи аналізу та оцінки ризиків, нечітка логіка, ідентифікація нелінійної залежності нечіткими базами знань.

Наукова новизна отриманих результатів.

Наукова новизна дипломної роботи полягає в наступному: вдосконалений метод нечіткої логіки Мамдамі для оцінювання ризиків інформаційної безпеки організації.

Практична цінність: проведено оцінку ризику інформаційної безпеки організації використовуючи засоби Optimization Toolbox MatLab.

Результати кваліфікаційної роботи рекомендується використовувати для оцінки ризику кібербезпеки підприємства та оцінювання рівня поточного стану ІБ автоматизованої системи для зниження потенційних втрат за рахунок підвищення стійкості функціонування корпоративної мережі.

РОЗДІЛ 1
АНАЛІЗ РИЗИКІВ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Обов’язковою умовою для організації режиму інформаційної безпеки (ІБ) на підприємстві є існування системи управління ІБ (Information Security Management) та аналізу інформаційних ризиків, управління цими ризиками.

1.1. Загальний огляд нормативних документів України про захист інформації

На сьогоднішній час організація режиму ІБ є критично важливим стратегічним показником розвитку будь-якого підприємства. При цьому, за правилом, увага приділяється рекомендаціям і вимогам відповідної української нормативно-методичної бази в галузі захисту інформації.

Законодавчі заходи щодо захисту процесу оброблення інформації полягають у застосуванні діючих в країні або введенням нових розроблених законів, постанов, положень та інструкцій, які регулюють юридичну відповідальність уповноважених осіб, користувачів та персоналу, який обслуговує інформаційну систему, щодо витоку, втрату або модифікацію інформації що довірена їм, яка підлягає захисту, а також за спроби виконати аналогічні дії за межами своїх повноважень, а також відповідальності сторонніх осіб за намагання несанкціонованого доступу до інформації або апаратури.

Попередити та стримати потенційних зловмисників є головною метою законодавчих заходів.

Необхідність створення комплексної системи захисту інформації на підприємстві (КСЗІ) в автоматизованій системі (АС) визначається на базі аналізу нормативно-правових актів, на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями. Такими документами у нашому випадку є:

– Закон України «Про інформацію» [1].

У цьому законі встановлені загальні правові основи щодо отримання, використання, розповсюдження та зберігання інформації, закріплено право особи на інформацію в усіх сферах суспільного і державного життя України, а систему інформації, джерела, визначений статус учасників інформаційних відносин, регулює доступ до інформації та забезпечує її охорону, захищає особу та суспільство від неправдивої інформації.

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [2].

– Закон України «Про захист інформації в автоматизованих системах» (затверджено Президентом України від 5липня 1994 р.) [3].

В Законі визначені основи регулювання правових відносин у сфері захисту інформації в АС, за умови дотримання права власності громадян України і юридичних осіб на інформацію та права доступу до неї, права власника інформації на її захист, а також встановленого чинним законодавством обмеження на доступ до інформації.

– «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені постановою Кабінету Міністрів України від 29.03.2006 року № 373 [4].

– Положення про технічний захист інформації в Україні (затверджено Указом Президента України від 27.09.99 року № 1229) [5].

– НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу [6].

Цей документ установлює терміни і визначення понять у галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. Терміни, що установлюються цим документом, обов’язкові для застосування в усіх видах документації і літератури, що входять до системи технічного захисту інформації.

Для кожного поняття встановлено один термін. Застосування синонімів терміна не допускається.

– НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [7].

Цей нормативний документ технічного захисту інформації визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів, регламентуючих питання:

✓ визначення вимог щодо захисту комп'ютерних систем від несанкціонованого доступу;

✓ створення захищених комп'ютерних систем і засобів їх захисту від несанкціонованого доступу;

✓ оцінки захищеності комп'ютерних систем і їх придатності для вирішення завдань споживача.

– НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [8].

Цей нормативний документ технічного захисту інформації визначає методологічні основи (концепцію) вирішення завдань захисту інформації в комп'ютерних системах і створення нормативних і методологічних документів.

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу [9].

Цей нормативний документ установлює критерії оцінки захищеності інформації, оброблюваної в комп'ютерних системах, від несанкціонованого доступу.

– НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [10].

Цей документ установлює принципи класифікації автоматизованих систем і утворення стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу.

– НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 [11].

Цей документ визначає вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2 і установлює згідно з визначеними НД ТЗІ 2.5-004 специфікаціями мінімально необхідний перелік функціональних послуг безпеки та рівнів їх реалізації у комплексах засобів захисту інформації (стандартний функціональний профіль захищеності).

– НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [12].

Цей нормативний документ встановлює вимоги до порядку розробки, складу і змісту технічного завдання на створення комплексної системи захисту інформації а автоматизованій системі, призначеній для оброблення, зберігання і передачі інформації з обмеженим доступом, або інформації, захист якої гарантується державою.

– НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [13].

Цей документ визначає основи організації та порядок виконання робіт із захисту інформації в інформаційно-телекомунікаційних системах (далі - ІТС) - порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування ІТС і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

1.2. Міжнародні стандарти у сфері управління ризиками інформаційної безпеки

Стандартом де-факто в області побудови систем управління інформаційною безпекою (ІБ) є Британський стандарт BS 7799, він був розроблений Британським Інститутом Стандартів і затверджений як державний у Великобританії в 1995 році. BS 7799 Part 1 // Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою) [14]. У документі описані 127 механізмів контролю, які є необхідні для побудови системи управління інформаційною безпекою (СУІБ) організації, що основуються на прикладах світового досвіду (best practices) в даній області. Цей документ слугує практичним керівництвом зіо створенню СУІБ. BS 7799 Part 2 // Information Security management – Specification for ISMS (Специфікація системи управління інформаційною безпекою), налає специфікацію СУІБ.

Основною метою цього стандарту – створення загальної методології для розробки, впровадження та оцінки ефективності СУІБ, застосовну як в умовах комерційних компаній, так і державних і некомерційних структур [14].

Стандарт BS 7799 складається з наступних частин:

Частина 1: Практичні рекомендації, 2000 р. Визначаються і розглядаються наступні аспекти організації режиму ІБ:

- політика безпеки (ПБ);
- організація захисту;
- класифікація інформаційних ресурсів і керування ними;
- управління персоналом;
- фізична безпека;
- адміністрування комп'ютерних систем і мереж;
- управління доступом до систем;
- розробка і супровід систем;
- планування безперебійної роботи організації;
- перевірка системи на відповідність вимогам ІБ.

Частина 2: Специфікації, 2000 р. Присвячена тим же аспектам, але з точки зору сертифікації режиму ІБ на відповідність вимогам стандарту.

В 2000 р. міжнародний інститут стандартів ISO на базі британського BS 7799 розробив та випустив міжнародний стандарт менеджменту безпеки ISO/IEC 17799 «Інформаційна технологія. Практичні правила управління інформаційною безпекою» встановлює рекомендації з управління інформаційною безпекою особам, відповідальним за планування, реалізацію або підтримку рішень безпеки в організації. Він призначений для забезпечення загальних основ для розробки стандартів безпеки та вибору практичних заходів з управління безпекою в організації, а також в інтересах забезпечення довіри в ділових відносинах між організаціями [14].

Основні розділи стандарту ISO 17799:

1. Область застосування,
2. Терміни та визначення,
3. Політика безпеки,
4. Організаційні питання безпеки,
5. Класифікація та управління активами,
6. Питання безпеки, які стосуються персоналу,
7. Фізичний захист та захист від впливу навколишнього середовища,
8. Управління передачею даних и операційною діяльністю,
9. Контроль доступу,
10. Розробка та обслуговування систем,
11. Управління неперервністю бізнесу,
12. Відповідність вимогам.

У Німеччині в 1998 р. вийшло «Керівництво щодо захисту інформаційних технологій для базового рівня захищеності». Можна виділити наступні блоки цього документа:

- Методологія управління ІБ (організація менеджменту в області ІБ , методологія використання керівництва);
- Компоненти інформаційних технологій:

– Основні компоненти (організаційний рівень ІБ, процедурний рівень, організація захисту даних, планування дій у надзвичайних ситуаціях);

– Інфраструктура (будівлі, приміщення, кабельні мережі, організація віддаленого доступу);

– Клієнтські компоненти різних типів (DOS, Windows, UNIX, мобільні компоненти, інші типи);

– Мережі різних типів (з'єднання «точка - точка», мережі Novell NetWare, мережі з ОС UNIX та Windows, різнорідні мережі);

– Елементи систем передачі даних (електронна пошта, модеми, між мережеві екрани і т.д.);

– Телекомунікації (факси, автовідповідачі, інтегровані системи на базі ISDN, інші телекомунікаційні системи);

– Стандартне ПЗ;

– Бази даних ;

– Каталоги загроз безпеки і контрзаходів (близько 600 найменувань у кожному каталозі).

При цьому всі каталоги структуровані таким чином:

– Загрози по класах;

– Форс-мажорні обставини;

– Недоліки організаційних заходів;

– Помилки людини;

– Технічні несправності;

– Навмисні дії.

Контрзаходи по класах:

– Поліпшення інфраструктури;

– Адміністративні контрзаходи;

– Процедурні контрзаходи;

– Програмно-технічні контрзаходи;

– Зменшення вразливості комунікацій;

– Планування дій у надзвичайних ситуаціях.

Всі компоненти розглядаються за таким планом: загальний опис, можливі сценарії загроз безпеки (перераховуються застосовні до даного компонента загрози з каталогу загроз безпеки), можливі контрзаходи (перераховуються можливі контрзаходи з каталогу контрзаходів). Фактично зроблена спроба описати з точки зору ІБ найбільш поширені компоненти інформаційних технологій і максимально врахувати їх специфіку. Передбачається оперативне поповнення та оновлення стандарту в міру появи нових компонентів. Каталоги загроз безпеки і контрзаходів, що містять по 600 позицій, є найбільш докладними із загальнодоступних. Ними можна користуватися самостійно - при розробці методик аналізу ризиків, управління ризиками та при аудиті інформаційної безпеки.

Стандарт ISO/IEC 15408. «Критерії оцінки безпеки інформаційних технологій» [15].

Стандарт розроблений таким чином, щоб задовольнити потреби трьох груп фахівців: розробників, експертів з сертифікації і користувачів об'єкта оцінки. Універсальність стандарту виявляється в тому, що об'єктом оцінки (ОО) може бути виріб інформаційних технологій ІТ, в якості якого можуть виступати продукт ІТ і система ІТ, а також автоматизована система (АС).

Стандарт 15408 складається з трьох частин:

Частина 1 «Введення і загальна модель» є введенням в ІСО 15408. У ній визначено загальні принципи і концепції оцінки безпеки ІТ і наведена загальна модель оцінки. Представлені конструкції для вираження цілей безпеки ІТ, вибору та визначення вимог безпеки ІТ.

Частина 2 «Функціональні вимоги безпеки» встановлюють сукупність функціональних компонентів як стандартний спосіб вираження функціональних вимог до ОО і містить каталог всіх функціональних компонентів, сімейств і класів.

Частина 3 «Вимоги довіри до безпеки» встановлюють сукупність компонентів довіри як стандартний спосіб вираження вимог довіри до ГО і містить каталог всіх компонентів, сімейств і класів довіри. Також визначено

критерії оцінки профілів захисту і завдань з безпеки і представлені оціночні рівні довіри, які встановлюють зумовлену в стандарті шкалу ранжування довіри до ГО. У міжнародному стандарті ІСО 27001 «Інформаційні технології - Методи забезпечення безпеки - Системи менеджменту інформаційної безпеки», формально визначає систему управління інформаційною безпекою (СУІБ), набір заходів, пов'язаних з управлінням ризиками інформаційної безпеки. Оцінка інформаційних ризиків полягає в розрахунку ризиків, який виконується з урахуванням відомостей про критичність активів, а також ймовірностей реалізації вразливостей [15].

Прийняття ризиків здійснюється в тому випадку, якщо рівень ризиків визнається прийнятним. Тобто компанія не вважає за доцільне застосовувати будь-які заходи по відношенню до цих ризиків і готова понести збитки.

Ухилення від ризиків - це повне усунення джерела ризику.

Передача ризиків - перенесення відповідальності за ризик на треті особи (наприклад, постачальника обладнання або страхової компанії) без усунення джерела ризику.

Зниження ризиків - це вибір і впровадження заходів щодо зниження ймовірності нанесення збитку.

У процесі обробки ризиків спочатку потрібно визначити, які ризики вимагають подальшої обробки, а які можна прийняти.

За результатами оцінки і обробки ризиків розробляється Положення про застосовність. Наявність цього документа обов'язково для проходження сертифікації [15].

Стандарт ISO/IEC 27003:2010 «Інформаційні технології - Методи забезпечення безпеки - посібник з впровадження системи управління інформаційною безпекою». У даному міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження системи менеджменту інформаційної безпеки (СМІБ) відповідно до стандарту ISO/IEC 27001:2005 [16]. У ньому описується процес визначення і розробки СМІБ, від запуску до складання планів впровадження. Впровадження системи

менеджменту інформаційної безпеки (СМІБ) є важливим видом діяльності і зазвичай здійснюється в організації, як проект. У даному документі пояснюється впровадження СМІБ з докладним описом запуску, планування та визначення проекту [16]. Процес планування кінцевого впровадження СМІБ включає п'ять фаз, наступні:

a) Отримання схвалення керівництва для запуску проекту СМІБ;

b) Визначення області дії і політики СМІБ;

c) Проведення аналізу організації;

d) Проведення аналізу ризиків та планування обробки ризиків;

e) Розробка СМІБ.

Відповідно до четвертої фазою даного стандарту необхідно визначити методологію оцінки ризику, визначити, проаналізувати і оцінити ризики для інформаційної безпеки, з метою вибору варіантів обробки і засоби управління ризику.

Спеціальні рекомендації з менеджменту ризику інформаційної безпеки міститься в стандарті ISO / IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Менеджмент ризику інформаційної безпеки», який являє собою керівництво з менеджменту ризику ІБ в організації, підтримуючи вимоги до СМІБ відповідно до ICO 27001 [17].

Менеджмент ризику ІБ повинен сприяти:

- Ідентифікації ризиків;
- Оцінці ризиків виходячи з наслідків їх реалізації для організації та ймовірності їх виникнення;
- Усвідомленню та інформування про вірогідність і наслідки ризиків;
- Встановленню пріоритетів у рамках обробки ризиків;
- Встановленню пріоритетів заходів щодо зниження наявних ризиків;
- Ефективності проведеного моніторингу обробки ризиків;
- Проведення регулярного моніторингу та перегляду процесу менеджменту ризику.

Процес менеджменту ризику ІБ може бать застосований до всієї організації, до будь-якої окремої частини організації, до будь-якої інформаційної системи, до наявним, планованим або специфічним аспектам управління.

1.3. Система управління інформаційними ризиками

Управління ризиками розглядається на адміністративному рівні ІБ, оскільки тільки керівництво організації здатне виділити необхідні ресурси, ініціювати і контролювати виконання відповідних програм.

Управління ризиками, як і вироблення власної політики безпеки, актуально тільки для тих організацій , інформаційні системи оброблювані дані яких можна вважати нестандартними. Звичайну організацію цілком влаштує типовий набір захисних заходів , вибраний на основі уявлення про типових руських або взагалі без будь-якого аналізу ризиків (особливо це вірно з формальної точки зору, у світлі проаналізованого нами раніше законодавства в галузі ІБ) [18].

Використання інформаційних систем пов'язане з певною сукупністю ризиків. Коли можливий збиток неприйнятно великий, необхідно прийняти економічно виправдані заходи захисту. Періодична переоцінка ризиків необхідна для контролю ефективності діяльності в галузі безпеки і для врахування змін обстановки .

З кількісної точки зору рівень ризику є функцією вірогідності реалізації певної загрози (що використовує деякі вразливі місця), а також величини можливого збитку.

Таким чином , суть заходів щодо управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків, а потім переконатися, що ризики укладені в прийнятні рамки (і залишаються такими). Отже, управління ризиками включає в себе два види діяльності, які чергуються циклічно:

- переоцінка (вимірювання) ризиків;

- вибір ефективних і економічних захисних засобів (нейтралізація ризиків).

По відношенню до виявлених ризиків можливі наступні дії:

- ліквідація ризику (наприклад, за рахунок усунення причини);
- зменшення ризику (наприклад, за рахунок використання додаткових захисних засобів);
- прийняття ризику (і вироблення плану дії у відповідних умовах);
- переадресація ризику (наприклад, шляхом укладення страхової угоди).

Процес управління ризиками можна розділити на наступні етапи:

1. Вибір аналізованих об'єктів і рівня деталізації їх розгляду.
2. Вибір методології оцінки ризиків.
3. Ідентифікація активів.
4. Аналіз загроз та їх наслідків, виявлення вразливих місць в захисті.
5. Оцінка ризиків.
6. Вибір захисних заходів.
7. Реалізація та перевірка вибраних заходів.
8. Оцінка залишкового ризику.

Етапи 6 і 7 ставляться до вибору захисних засобів (нейтралізації ризиків), решта - до оцінки ризиків.

Вже перерахування етапів показує, що управління ризиками - процес циклічний. По суті, останній етап - це оператор кінця циклу, що приписує повернутися до початку. Ризики потрібно контролювати постійно, періодично проводячи їх переоцінку. Відзначимо, що сумлінно виконана і ретельно документована перша оцінка може істотно спростити подальшу діяльність [21].

Управління ризиками, як і будь-яку іншу діяльність у галузі інформаційної безпеки, необхідно інтегрувати в життєвий цикл ІС. Тоді ефект виявляється найбільшим, а витрати - мінімальними. Раніше ми визначили п'ять етапів життєвого циклу. Коротко опишемо, що може дати управління ризиками на кожному з них.

На етапі ініціації відомі ризики слід врахувати при виробленні вимог до системи взагалі і засобам безпеки зокрема.

На етапі закупівлі (розробки) знання ризиків допоможе вибрати відповідні архітектурні рішення , які грають ключову роль в забезпеченні безпеки.

На етапі установки виявлення ризики слід враховувати при конфігурації, тестуванні та перевірці раніше сформульованих вимог, а повний цикл управління ризиками повинен передувати впровадженню системи в експлуатацію.

На етапі експлуатації управління ризиками має супроводжувати всі істотні зміни в системі.

При виведенні системи з експлуатації управління ризиками допомагає переконатися в тому, що передача, зберігання, обробка даних відбувається безпечним чином [22].

1.4. Висновок по розділу 1

Згідно з метою роботи та завданням у роботі був проведений загальний огляд нормативних документів України про захист інформації:

1. Закон України «Про інформацію».
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
3. Закон України «Про захист інформації в автоматизованих системах»
4. «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».
5. Положення про технічний захист інформації в Україні.
6. НД ТЗІ 1.1-003-99.
7. НД ТЗІ 1.1-002-99.
8. НД ТЗІ 2.5-004-99.
9. НД ТЗІ 2.5-005-99.
10. НД ТЗІ 2.5-008-2002.
11. НД ТЗІ 3.7-001-99.

12.НД ТЗІ 3.7-003-05.

Були розглянуті міжнародні стандарти у сфері управління ризиками інформаційної безпеки:

- Стандарт BS 7799;
- Стандарт ISO/IEC 17799;
- Стандарт ISO/IEC 15408;
- Стандарт ISO / IEC 27001;
- Стандарт ISO / IEC 27003.

Також була розглянута система управління інформаційними ризиками.

РОЗДІЛ 2
ОЦІНКА ТА ОБРОБКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Опубліковані документи різних організацій і положення описаних вище стандартів у галузі захисту інформації, присвячені питанням аналізу інформаційних ризиків та управління ними , не містять низки важливих деталей, які треба обов'язково конкретизувати при розробці застосовних на практиці методик. Необхідний ступінь конкретизації цих деталей залежить від рівня зрілості організації, специфіки її діяльності і ряду інших чинників. Таким чином, неможливо запропонувати якусь єдину, прийнятну для всіх вітчизняних компаній і організацій, універсальну методику, відповідну певної концепції управління ризиками. У кожному окремому випадку доводиться адаптувати загальну методику аналізу ризиків та управління ними під конкретні потреби підприємства з урахуванням специфіки його функціонування та ведення бізнесу [24].

Згідно з усталеною термінології, яка використовується в стандартах, оцінка ризиків включає два послідовних етапи: аналіз ризиків та оцінювання ризиків [18-25].

Аналіз ризиків включає в себе:

- Ідентифікацію активів;
- Ідентифікацію бізнес-вимог та вимог законодавства, застосовних до ідентифікованим активам;
- Оцінювання активів з урахуванням ідентифікованих бізнес-вимог і вимог законодавств, а також наслідків порушення їх конфіденційності цілісності та доступності;
- Ідентифікацію значущих загроз і вразливостей ідентифікованих активів;
- Оцінка ймовірності реалізації загроз і величини вразливостей.

Оцінювання ризиків полягає у визначенні їх кількісних і якісних значень, формуванні реєстру ризиків і ранжирування.

2.1. Ідентифікація та визначення цінності активів

Важливі активи всередині області дії СУІБ повинні бути чітко ідентифіковані і належним чином оцінені, а реєстри, що описують різні види активів, повинні бути взаємопов'язані і підтримуватися в актуальному стані [27].

Активи (ресурси) - це все, що має цінність або знаходить корисне застосування для організації, її ділових операцій і забезпечення їх безперервності. Тому активи потребують захисту для того, щоб забезпечити коректність ділових операцій і безперервність бізнесу.

Ідентифікація активів:

- формування моделі бізнес-процесів;
- інвентаризація активів;
- формування реєстрів активів;
- визначення взаємозв'язків між реєстрами активів;
- визначення власників активів та їх обов'язків;
- класифікація та категорування активів;
- визначення правил допустимого використання активів.

Активи необхідно структурувати, категорувати і класифікувати за рівнем конфіденційності, критичності та іншими ознаками. Групування схожих або зв'язкових активів дозволяє спростити процес оцінки ризиків. Для кожного з ідентифікованих активів або групи активів повинен бути визначений власник, на якого покладається відповідальність за здійснення контролю виробництва, розробки, супроводу, використання та безпеки цих активів.

Власник активу повинен нести відповідальність за визначення відповідної класифікації і прав доступу до цього активу, підтримання відповідних механізмів контролю. В обов'язки власника активу також входить періодичний перегляд прав доступу і класифікацій безпеки [28].

Ідентифікацію (інвентаризацію) активів слід починати зверху вниз, тобто з ідентифікації та опису бізнес-процесів, які розглядаються в якості основних активів організації. Вони являють собою комбінацію різнорідних активів, таких як інформація, технічні та програмні засоби, кадрові ресурси, юридичні та договірні зобов'язання і т.д. Всі ці активи представляють цінність для організації в контексті бізнес-процесів.

Для цілей управління ризиками ділимо всі процеси на зовнішні і внутрішні, а також на основні і допоміжні. Під основними розуміємо бізнес-процеси які дозволяють організації безпосередньо отримувати дохід і досягати поставлених бізнес-цілей. Оскільки цілі будь-якої організації полягають у виробництві деяких продуктів чи послуг та надання їх зацікавленим зовнішнім сторонам, такі процеси називаються зовнішні. Ці процеси або складаються у взаємодії із зовнішніми сторонами, або орієнтовані на зовнішні сторони [27].

Наступні ризики є специфічними для окремих зовнішніх процесів організації:

- продажі та маркетинг;
- виробництво та експлуатація;
- підтримка клієнтів;

Під допоміжними процесами розуміємо такі процеси які необхідні для підтримки (забезпечення умов виконання) основних процесів організації. Ці процеси надають інформацію, послуги та інші ресурси зовнішнім бізнес-процесам, тому ми віднесемо такі процеси до внутрішніх, наступні:

- управління кадрами;
- дослідження і розробки;
- адміністрування та IT;
- фінанси, бухгалтерія;
- забезпечення безпеки (фізичної, економічної, інформаційної);
- аудит;
- ризик-менеджмент і т.п.

Інформація про бізнес-процеси витягується в ході інтерв'ювання власників та учасників цих процесів. Кожен процес характеризується певним алгоритмом дій , які виконуються в ручному , автоматичному чи напівавтоматичному режимі. Для виконання цих дій використовуються різні ресурси : обладнання , програмне забезпечення, сервіси, приміщення, кадри. Одним з основних видів ресурсів є інформація, представлена в різних формах, тобто інформаційний актив, який повинен бути захищений, від різних видів загроз і атак.

Кінцевою метою етапу ідентифікації активів є формування реєстру інформаційних активів. Це ключовий документ є найпершим і одним з важливих результатів на шляху усвідомлення інформаційних ризиків і встановлення контролю над ними. Реєстр також необхідний для вирішення інших завдань, таких як планування резервного копіювання або аварійного відновлення, розподілу відповідальності за активи, облік активів і розподіл прав доступу до них, класифікація активів за критеріями конфіденційності, цілісності та доступності. Разом з формуванням реєстру активів в організації повинен бути реалізований безперервний процес інвентаризації активів, що забезпечують актуальність цього документа і його взаємозв'язок з іншими реєстрами: програмними, апаратними [30,31].

Ідентифікація та визначення цінності активів, виходячи з потреб організації, є основними факторами в оцінці ризику. Для того щоб визначити необхідний рівень захисту активів, необхідно визначити їх цінність з точки зору важливості цих активів для бізнесу. Важливо враховувати ідентифіковані законодавчі вимоги, вимоги бізнесу і договірних зобов'язань, а також порушення конфіденційності, цілісності та доступності цих активів.

Етапи визначення цінності активів:

- визначення шкали цінності активів;
- визначення критеріїв оцінки збитку;
- отримання вихідних даних для оцінки від власників і користувачів активів;

– визначення наслідків для бізнесу в результаті порушення конфіденційності, цілісності та доступності активу;

– визначення цінності активу окремо для кожного з трьох властивостей.

Обчислення сумарної цінності активів проводиться з урахуванням взаємозв'язків між різними видами активів. Сумарна цінність фізичних активів визначається власною цінністю, а також цінністю пов'язаних з ними інформаційних активів і програмного забезпечення. Сумарна програмного забезпечення визначається власною цінністю, а також цінністю пов'язаних з ними інформаційних активів [33].

Сумарна цінність кожного окремого взятого активу може бути представлена матрицею цінності активу (табл. 2.1), де по вертикалі вказуються наслідки впливу загроз на актив, по горизонталі - категорія вимог, які при цьому порушуються, а на перетині - якісне або кількісне значення цінності активу.

Для заповнення цієї матриці, необхідно визначити якісну шкалу цінності активів і критерії оцінки збитку.

Цінність інформаційних активів визначається величиною прямого або непрямого збитку, що виникає в результаті інцидентів безпеки, пов'язаних з розкриттям, несанкціонованою модифікацією, тимчасової недоступністю або з руйнуванням активів (табл. 2.1).

Таблиця 2.1.

Матриця цінності активу

	Вимоги бізнесу	Вимоги законодавства	Контрактні зобов'язання
Конфіденційність	+		
Цілісність		+	
Доступність		+	+
Автентичність	+		+

Наслідки таких інцидентів можуть виражатися в упущеної вигоди , втрати конкурентних переваг, погіршення іміджу організації, заподіянні шкоди

інтересам третьої сторони, штрафах, прямих фінансових збитках або дезорганізації діяльності. Для кожного активу слід розглядати найгірший сценарії розвитку подій.

Критерії оцінки збитку для різних організацій можуть істотно різнитися. Вони визначаються областю , характером і масштабами діяльності організації, політикою керівництва, формою власності та низкою інших факторів.

Після ідентифікації активів повинні бути визначені вимоги безпеки для цих активів [36].

У будь-якій організації вимоги безпеки відбуваються з трьох основних джерел:

1. Унікальний для даної організації набір загроз і вразливостей, які можуть призвести до значних втрат, в разі їх реалізації;
2. Застосовні до організації, її комерційним партнерам, підрядникам вимоги законодавства, нормативної бази та договорів;
3. Унікальний набір принципів, цілей і вимог до обробки інформації, який організація розробила для підтримки операцій і процесів, який застосовується до інформаційних систем організації.

Застосовні до організації вимоги законодавчої та нормативної бази, вимоги бізнесу, а також вимоги випливають з контрактних зобов'язань організації визначаються з метою ідентифікації юридичних, репутаційних, фінансових та бізнес ризиків, пов'язаних з порушенням обов'язкових вимог, оформляються у вигляді реєстру вимог безпеки.

Після ідентифікації активів, визначення критеріїв і шкал оцінки збитку, вимог безпеки необхідно розробити таблицю цінності активів (табл. 2.2.).

Заповнення табл. 2.2. виробляється експертом з оцінки ризиків впід час інтерв'ювання власників і користувачів активів, яким пропонується розглянути різні сценарії інцидентів, в ході яких порушується конфіденційність, цілісність або доступність активу.

Результати опитування мають бути зафіксовані в письмовій формі і узгоджені з опитуваним. На основі даної інформації керівництву організації доведеться приймати важливі для організації рішення.

Таблиця 2.2.

Оцінка величини можливого збитку і цінності активів

Назва активу	Наслідок загрози	Вимога безпеки	Тип збитку	Цінність активу (величина збитку)	Примітка (опис можливих наслідків загрози та шкоди)
Корпоративний веб-сайт	к	+			+
	ц		+		
	д	+		+	
Персональні дані співробітників	к				
	ц	+			
	д				+
і т.д.					

2.2. Аналіз загроз та вразливостей інформаційної безпеки

Вразливості представляють собою недостатність (Недоліки) захисту, асоційована з активами організації. Ці слабкості можуть використовуватися однією або декількома загрозами, які є причиною небажаних інцидентів. Вразливість як така не завдає шкоди, ця умова або набір умов, що дозволяють загрозу заподіяти шкоду активам.

Інакше, вразливості - це будь-які фактори , що роблять можливою успішну реалізацію загроз. Тому для оцінки вразливостей необхідно ідентифікувати існуючі механізми безпеки і оцінити їх ефективність.

Ідентифікація вразливостей повинна визначати пов'язані з активами слабкості в наступних областях:

– Фізичному оточенні;

– Персоналі, процедурах управління, адміністрування і механізмах контролю;

– Ділових операціях та наданні сервісів;

– Технічних засобах, програмному забезпеченні, телекомунікаційному обладнанні і підтримуючої інфраструктурі.

Існуючі вразливості діляться на дві групи: організаційні та технічні [32].

Організаційні вразливості полягають у відсутності або неправильному застосуванні механізмів контролю. Тому основним джерелом ідентифікації організаційних вразливостей служить стандарт ISO 27001, так як цей стандарт містить найбільш повне високорівневий опис того, що повинно бути зроблено для захисту інформаційних активів.

Джерела ідентифікації потенційних організаційних вразливостей:

– ISO 27001, розділи 4-8, визначають вимоги і процеси СУІБ;

– ISO 27001, додаток А, - визначає 11 областей і 137 механізмів контролю;

– ISO 27002 - докладно описує 11 областей і 137 механізмів контролю;

– BIP 0072 - містить опитувальники для перевірки відповідності вимогам ISO 27001;

– BIP 0073 - надає додаткове керівництво з впровадження та аудит механізмів контролю;

– Застосовна законодавча і нормативна база.

Результатом ідентифікації організаційних вразливостей є звіт про невідповідності, в якому для кожної галузі контролю визначається ступінь відповідності, перераховуються існуючі механізми безпеки, сильні і слабкі сторони, а також видаються рекомендації щодо посилення захисту [30].

Ідентифікація технічних вразливостей проводиться для зовнішнього і внутрішнього периметра корпоративної мережі. Зовнішній периметр - це

сукупність всіх точок входу в мережу. До внутрішнього периметру відносимо хости і додатки, доступні з нутрії .

Для ідентифікації технічних вразливостей проводяться наступні організаційно-технічні заходи з аналізу захищеності:

– ручні перевірки системної конфігурації;
– мережеве та хостове сканування;
– тестові випробування;
– соціальні тести;
– аналіз програмних кодів.

Аналіз загроз інформаційній безпеці.

Активи є об'єктом для багатьох загроз. Загроза може стати причиною небажаного інциденту, в результаті якого організації буде завдано шкоди. Цей збиток може виникнути в результаті атаки на інформацію, що приводить до її несанкціонованого розкриття, модифікації, пошкодження, знищення, недоступності або втрати. Загрози можуть виходити від випадкових або навмисних джерел або подій. При реалізації загрози використовується одна або більше вразливостей систем, додатків або сервісів. Загрози можуть виходити як зсередини організації, так і ззовні [27].

Для кожного інформаційного активу або групи активів визначається список загроз щодо конфіденційності, цілісності та доступності. За основу береться модель загроз, що є частина політики безпеки організації .

Перелік, що містить приклади загроз і вразливостей, пов'язаних з цілями і механізмами контролю представлений в стандарті ISO / IEC 27002:2005 [17, 25]. Цей перелік не є вичерпним і повинен розглядатися як приклад, проте його достатньо для проведення високорівневої оцінки ризиків.

Для кожної ідентифікованої загрози визначається список вразливостей, через які реалізуються загрози. При цьому враховується результати аудитів безпеки і контролю захищеності інформаційних систем організації, вплив людського фактору, а також факти відсутності або недостатності застосовуваних механізмів контролю (організаційних і технічних).

Класифікація загроз безпеки: по об'єкту впливу, за джерелом загрози, способом здійснення, можливим наслідкам та видами збитку.

За видами активів, на які спрямовані загрози (об'єктах впливу) поділяються на:

– загрози, спрямовані проти інформаційних активів;
– загрози, спрямовані проти програмного забезпечення;
– загрози, спрямовані проти технічних засобів;
– загрози кадрових ресурсів;
– загрози приміщенням організації.

За джерелом загрози можна розділити на класи:

– загрози з боку різних класів зовнішніх порушників;
– загрози з боку різних класів внутрішніх порушників;
– загрози з боку партнерів і підрядників;
– антропогенні катастрофи;
– техногенні аварії;
– природні катаклізми;
– нещасні випадки.

За типом порушення загрози можна розділити на класи:

– загрози порушення конфіденційності інформації;
– загрози порушення цілісності інформації;
– загрози порушення доступності інформації;
– загрози відмови від вчинених дій з інформацією (загрози неспростовності);
– загрози, пов'язані з неможливістю встановлення авторства електронних документів (загрози автентичності);
– загрози порушення вимог законодавства.

Загрози ІБ, реалізовані з використанням програмних засобів - найбільш численний клас загроз щодо конфіденційності, цілісності та доступності інформаційних активів, пов'язаних з отриманням внутрішніми або зовнішніми порушниками несанкціонованого доступу до інформації, а також блокуванням

або руйнуванням цієї інформації з використанням можливостей, що надаються загальносистемним і прикладним програмним забезпеченням.

До цього класу загроз можна віднести наступні:

– використання помилок проектування, кодування, або конфігурації для отримання НСД;

– використання закладок ПО, залишених для налагодження, або зумисне впроваджених;

– збій в роботі засобів захисту інформації;

– маскарад, перехоплення паролів або злом паролів користувачів;

– нецільове використання ПЗ;

– аналіз мережевого трафіку з метою перехоплення інформації;

– заміна, вставка, видалення або зміну даних користувача в інформаційному потоці;

– помилки користувачів і технічного персоналу;

– впровадження шкідливого ПЗ;

– витік конфіденційної інформації з електронних каналів зв'язку;

– і т.п.

Більшість розглянутих в цьому класі загроз реалізуються шляхом здійснення локальних або віддалених атак на інформаційні активи системи внутрішніми і зовнішніми порушниками.

Витік інформації по технічним каналам зв'язку - це специфічний клас загроз, що вимагає для своєї реалізації спеціальних навичок і устаткування для проведення технічної розвідки.

До даного класу загроз відносяться наступні:

– побічні електромагнітні випромінювання;

– наведення сигналу на дроти та лінії зв'язку, заземлення, електроживлення;

– радіовипромінювання, модульовані інформативним сигналом, паразитні випромінювання;

– радіовипромінювання, зумовлені впливом на технічні засоби високочастотних сигналів, що створюються за допомогою розвідувальної апаратури;

– апаратні закладки;

– акустичне випромінювання мовного сигналу;

– виброакустичне випромінювання мовного сигналу;

– телевізійна й фотографічна розвідка.

Відносно програмних засобів можуть реалізовуватися такі види загроз:

– інше ПЗ і резервних копій;

– внесення несанкціонованих змін до вихідні тексти ПО;

– використання неліцензійного ПЗ;

– порушення ліцензійних угод ;

– порушення конфіденційності програмних кодів.

До загроз технічних засобів ставляться загрози інформації, яка обробляється і передається по каналах зв'язку, пов'язані з пошкодженнями і відмовами технічних засобів системи і пошкоджень ліній зв'язку [28].

До них відносять такі основні види загроз:

– Навмисне або ненавмисне фізичне пошкодження технічних засобів внутрішніми порушниками;

– Фізичне пошкодження мережевого і каналоутворюючого обладнання внутрішніми порушниками;

– Фізичне пошкодження ліній зв'язку зовнішніми або внутрішніми порушниками;

– Перебої в системі електроживлення;

– Відмови технічних засобів;

– Установка неперевірених технічних засобів або заміна що вийшли з ладу апаратних компонентів на неідентичні компоненти;

– Розкрадання носіїв конфіденційної інформації внутрішніми порушниками внаслідок відсутності контролю за їх використанням та зберіганням.

Оцінка загроз і вразливостей.

Після ідентифікації загроз і вразливостей необхідно оцінити вірогідність їх об'єднання і виникнення ризику. Це включає в себе оцінку ймовірності реалізації загроз, а також того, наскільки легко вони можуть використовувати наявні вразливості. При оцінюванні ймовірності загроз необхідно враховувати особливості, притаманні різним групам загроз.

Імовірність навмисних загроз залежить від мотивації, знань, компетентності та ресурсів, доступних потенційному зловмиснику, а також від привабливості активів для реалізації атак [27].

Вірогідність випадкових загроз може оцінюватися з використанням статистики і досвіду. Ймовірність таких загроз може залежати від близькості організації до джерел небезпеки. Географічне положення організації також впливає на можливість виникнення екстремальних погодних умов. Імовірність людських помилок (одна з найбільш поширених випадкових загроз) і поломки устаткування також повинні бути оцінені.

Інциденти, що відбувалися в минулому, що показують проблеми в існуючих захисних заходах.

Нові розробки та тенденції включають в себе звіти, новини і тенденції, отримані з Інтернет, груп новин, від інших організацій і консультантів.

Для оцінки ймовірності реалізації загрози може використовуватися трьох рівнева якісна шкала:

– Н – низька ймовірність. Малоймовірно, що ця загроза здійснюється, не існує інцидентів, статистики, мотивів і т.п., які вказували б на те, що це може статися. Очікувана частота реалізації загрози не перевищує 1 разу на 5-10 років.

– С – середня ймовірність. Можливо, ця загроза здійснитися або існує статистика або інша інформація, яка вказує на те, що такі або подібні загрози іноді здійснювалися перш, або існують ознаки того, що у атакуючого можуть бути певні причини для реалізації таких дій. Очікувана частота реалізації загрози - приблизно один раз на рік.

– В – висока ймовірність. Ця загроза, швидше за все, здійсниться. Існують інциденти, статистика або інша інформація, яка вказує на те, що загроза, швидше за все, здійсниться, або можуть існувати серйозні причини або мотиви для атакуючого, щоб здійснити такі дії. Очікувана частота реалізації загрози - щотижня або частіше.

Трирівневої шкали зазвичай достатньо для первісної оцінки загроз. Надалі її можна розширити, додавши ще пару проміжних рівнів.

Загальна ймовірність інциденту також залежить від вразливостей активів, тобто наскільки легко слабкості активів можуть бути використані для успішного здійснення загроз.

Вразливості, так само як і загрози, можуть бути оцінені за трирівневою якісної шкалою. Значення рівня вразливості показує, наскільки ймовірно успішне здійснення загрози з використанням даної вразливості в разі, якщо ця буде реалізовуватися. Відповідні якісні рівні вразливості можуть бути визначені, наприклад, наступним чином:

– В – ймовірно. Вразливість легко використовувати, і існує слабкий захист або захист відсутній. Імовірність успішної реалізації загрози ≈0.9-1.

– С – можливо. Вразливість може бути використана, але існує певна захист. Імовірність успішної реалізації загрози ≈ 0.5.

– Н – малоймовірно. Вразливість складно використовувати, і існує достатній захист. Імовірність успішної реалізації загрози ≈ 0-0.1.

Для визначення підсумкового рівня вразливості, розглянутої для конкретної групи загроз, використовуються експертні оцінки. З одного боку представлені механізми контролю, з іншого – вразливості. Якщо сильно переважують вразливості, тоді підсумковий рівень буде високим. Якщо існуючий перевага на боці механізмів контролю, які здатні нівелювати наявні вразливості, тоді підсумковий рівень буде низьким. Якщо між механізмами контролю та вразливості спостерігається приблизний паритет, тоді підсумковий рівень вразливості оцінюється як середній.

Така оцінка навряд чи може вважатися об'єктивною, так як все ціле залежить від думки того чи іншого експерта про вразливості і механізмах контролю. Для підвищення об'єктивності оцінки слід застосовувати підтвердили свою ефективність методи експертної оцінки, такі як, наприклад, метод Дельфі. Треба влаштовувати колективні обговорення загроз, вразливостей і механізмів контролю, на які слід запрошувати представників різних бізнес-підрозділів, власників активів і бізнес-процесів, експертів з безпеки і зовнішніх консультантів. Це підвищує не тільки об'єктивність оцінок, а й, що не менш важливо, обізнаність всіх учасників таких обговорень [26].

2.3. Оцінювання та визначення величин ризиків

У будь-якій методиці необхідно ідентифікувати ризики, як варіант - їх складові (загрози та вразливості). Природним при цьому є вимога повноти списку. Складність завдання складання списку і докази його повноти залежить від того, які вимоги пред'являються до деталізації списку [22, 24].

При оцінюванні ризиків необхідно розглянути наступні аспекти:

- шкали та критерії, за якими можна вимірювати ризики;
- оцінку ймовірностей подій;
- технології вимірювання ризиків.

Шкали й критерії, за якими вимірюються ризики. Для вимірювання якої-небудь властивості необхідно вибрати шкалу. Шкали можуть бути прямими (природними) або непрямими (похідними). Приклад - шкала для вимірювання суб'єктивного властивості «цінність інформаційного ресурсу». Ця цінність може вимірюватися в одиницях виміру похідних шкал, таких як вартість відновлення ресурсу, час відновлення ресурсу та інший варіант - визначити шкалу для отримання експертної оцінки, наприклад має три значення:

- малоцінний інформаційний ресурс: від нього не залежать критично важливі завдання і він може бути відновлений з невеликими витратами часу і фінансів;

- ресурс середньої цінності: від нього залежить ряд важливих завдань, але в разі втрати він може бути відновлений за час, що не перевищує критично допустимий, але вартість відновлення - висока;
- цінний ресурс: від нього залежать критично важливі завдання, у разі втрати час відновлення перевищує критично допустимий або вартість надзвичайно висока.

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. Приклад суб'єктивного критерію - оцінка власником інформаційного ресурсу ризику виходу з ладу ПК. У методиках аналізу ризиків, як правило, використовуються суб'єктивні критерії, вимірювані в якісних одиницях, оскільки:

- оцінка повинна відображати суб'єктивну точку зору власника інформаційних ресурсів;
- слід враховувати різні аспекти - не тільки технічні, але й організаційні, психологічні і т.д.

Процес отримання суб'єктивної ймовірності зазвичай поділяють на три етапи: підготовчий етап, отримання оцінок, етап аналізу отриманих оцінок.

Перший етап. Під час цього етапу формується об'єкт дослідження - безліч подій, а також виконується попередній аналіз властивостей цієї множини (встановлюється залежність чи незалежність подій, дискретність або неперервність випадкової величини, що породжує дане безліч подій). На основі такого аналізу вибирається один з відповідних методів визначення суб'єктивної ймовірності. На цьому ж етапі проводиться підготовка експерта або групи експертів, ознайомлення їх з методом і перевірка розуміння ними поставленого завдання [27].

Другий етап. Полягає у 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 остаточним розподілом, оскільки нерідко виявляється суперечливим.

Третій етап. На цьому етапі досліджуються результати опитування. Якщо ймовірності, представлені експертами, не узгоджуються з аксіомами ймовірності, то на це звертається увага експертів та відповіді уточняються з метою приведення їх у відповідність до вибраної системи аксіом.

Для деяких методів отримання суб'єктивної ймовірності третій етап виключається, оскільки сам метод полягає у виборі підкоряється аксіомам ймовірності ймовірного розподілу, яке в тому чи іншому сенсі найбільш близько до оцінок експертів. Особливу важливість третій етап набуває при агрегування оцінок, запропонованих групою експертів.

2.4. Процес обробки ризиків інформаційної безпеки

Оцінка ризиків дозволяє отримати відповіді на три питання, а саме - які інформаційні активи, від чого і навіщо слід захищати. Після цього успішність організації за лежатиме від того, які заходи вона буде застосовувати для обробки виявлених ризиків [23,31].

Метою обробки ризиків є їх зменшення до прийнятного рівня шляхом зменшення ймовірності інциденту або мінімізації можливих збитків. Процес обробки ризиків включає в себе підготовку, вибір і прийняття рішень по способам обробки ризиків. На вхід процесу обробки ризиків надходять результати оцінки ризиків у вигляді звіту і додається до нього реєстру інформаційних ризиків. Якщо ці дані є достатніми, тоді для кожної групи ризиків приймається рішення по їх обробці шляхом вибору одного з чотирьох способів обробки ризиків або їх комбінації. При цьому використовуються критерії прийняття ризиків, що визначаються політикою організації в галузі управління ризиками. Результатом процесу обробки ризиків є план оброблення ризиків, що містить переліки заходів для кожної групи ризиків та оцінку остаточних ризиків (рис. 2.1.)

Обираєте для зменшення ризиків механізми контролю повинні бути економічно обгрунтовані, тобто забезпечити позитивний повернення інвестицій. Після того як ризик був оцінений, керівництвом організації має бути прийняте рішення про спосіб обробки цього ризику.

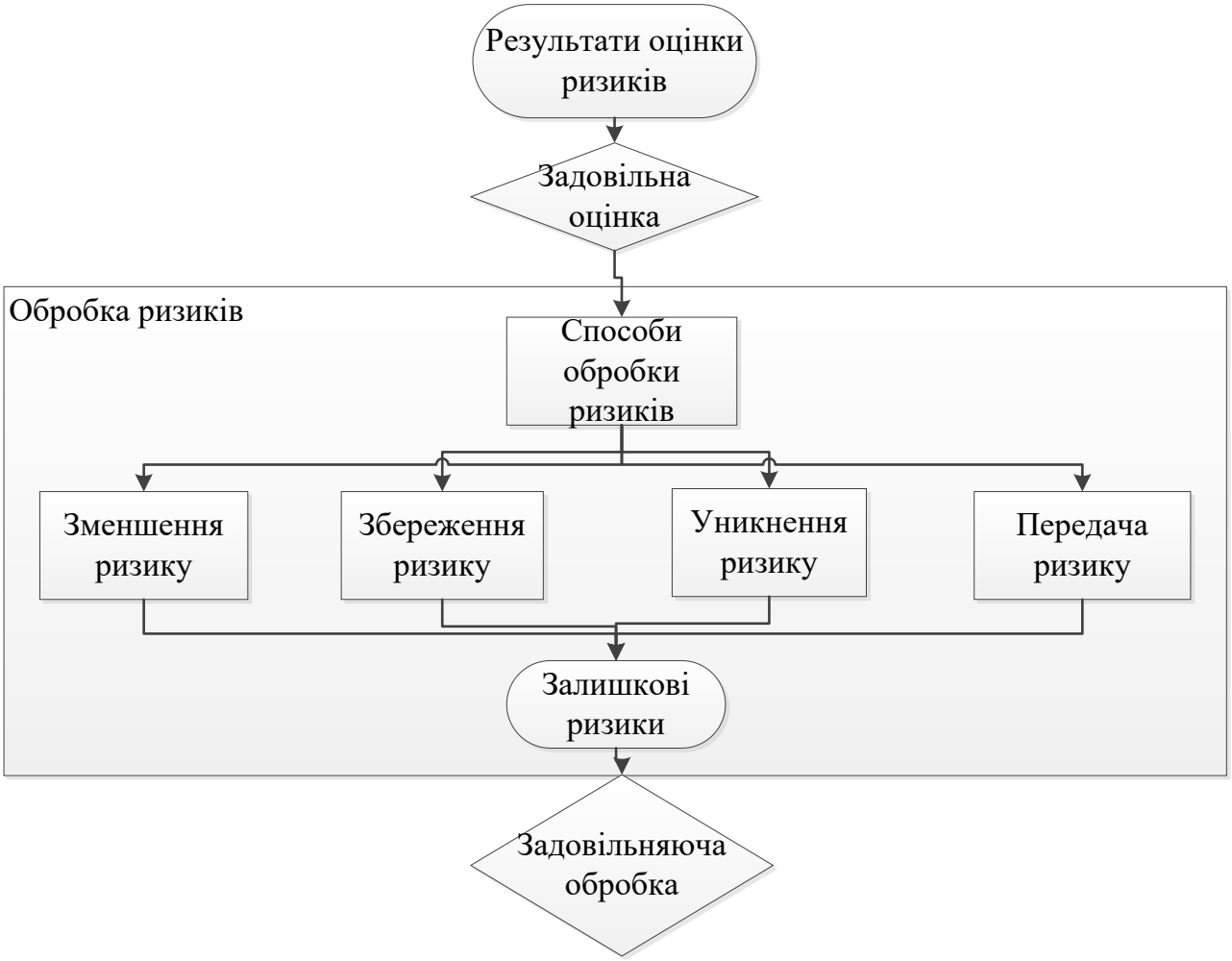

Рис. 2.1. Блок-схема обробки ризиків ІБ

Існує чотири можливі способи обробки ризику:

- прийняття (збереження) ризику;
- зменшення ризику;
- передача ризику;
- уникнення ризику.

На рішення про прийняття ризику впливають різні обставини.

Основні фактори, що впливають на рішення про прийняття ризиків:

- можливі наслідки здійснення ризику;

- очікувана частота подібних подій.

До числа суб'єктивних факторів, що впливають на прийняття рішень з ризиків можна віднести:

- готовність до прийняття ризику;
- простота реалізації механізму контролю;
- доступні фінансові, кадрові та інформаційні ресурси;
- існуючі ділові / технологічні пріоритети;
- політика організації та керівництва.

Багато ризиків не можна довести до нехтовно малої величини. На практиці після прийняття стандартного набору контрзаходів деякі ризики зменшуються, але залишаються все ще значущими. Необхідно знати залишкову величину ризику. Кожна організація повинна встановити критерій прийняття ризиків, що визначають максимально допустимий рівень залишкового ризику, а також можливі винятки для певних ризиків при певних обставинах. Ризики, що перевищують встановлений керівництвом допустимий рівень, - це ті ризики, які є неприйнятними для організації, а пов'язана з ними діяльність - занадто ризикованою. Всі інші ризики нижче цього рівня, є допустимими і можуть бути прийняті без подальшої обробки [32,33].

Якщо ризик неприйнятний, то розглядається питання про його зменшенні до рівня, який був визначений як максимально допустимий. Багато ризики вдається значно зменшити шляхом застосування відповідних механізмів контролю. Переліки, яких, наведені в стандарті ISO 27001 (додаток А) і ISO 27002, що надають опис і посібник з впровадження для кожного механізму контролю [36]. У стандарті ISO 15408 і розроблених на його основі профілях захисту можливе визначити відповідні вимоги і підібрати специфікацію будь-яким програмно-технічним механізмам контролю.

Зменшувати ризики можна наступними способами:

- зменшенням ймовірності впливу загрози на активи;
- ліквідацією наявних вразливостей;
- зменшенням імовірності використання вразливості;

- зменшенням можливого збитку в разі здійснення ризику шляхом виявлення небажаних подій, реагування та відновлення після них.

Передача ризику може бути обрана в разі, якщо складно зменшити ризик до прийнятного рівня або якщо передача цього ризику третій стороні економічно більш виправдана.

Основними механізмами передачі ризику є страхування та аутсортинг.

Уникнення ризику – деякі дії, при яких змінюються способи ведення бізнесу для того, щоб уникнути здійснення ризику, наприклад, шляхом вибору інших способів передачі, зберігання або обробки інформації.

В результаті виконання даного етапу для прийнятих до уваги інформаційних ризиків керівництво організації повинне розробити стратегію управління ризиками.

2.5. Висновок по розділу

Згідно з метою роботи було проведена ідентифікація та визначення цінності активів. Був проведений аналіз загроз та вразливостей. Був розглянутий процес оцінювання та визначення величин ризиків, шкал і критерій, за якими вони можуть вимірюватись. Також був розглянутий процес обробки ризиків інформаційної безпеки та способи зменшення ризиків. Були описані основні та суб’єктивні фактори, що впливають на рішення про прийняття ризиків.

РОЗДІЛ 3.
ІНСТРУМЕНТАЛЬНІ ЗАСОБИ УПРАВЛІННЯ РИЗИКАМИ

Управління IT-ризиками складається з їх періодичної оцінки та виконання заходів щодо зниження виявлених ризиків до прийнятного рівня. При цьому величини виявлених ризиків використовуються для визначення розмірів розумних інвестицій в ІБ.

Інструментальні засоби аналізу ризиків дозволяють автоматизувати роботу спеціалістів в галузі захисту інформації, що здійснюють оцінку або переоцінку інформаційних ризиків підприємства.

3.1. Методології управління ризиками інформаційної безпеки

Методологія CORAS побудована на базі програми Information Society Technologies. Суть методики: адаптація, визначення і поєднання методів аналізу ризиків, Event-Tree-Analysis, ланцюги Маркова, HazOp і FMECA [39].

CORAS базується на моделі UML та на австралійському / новозеландському стандарті AS / NZS 4360: 1999 Risk Management і ISO / IEC 17799-1: 2000 Code of Practice for Information Security Management. В стандарті поєднані рекомендації, що визначені в ISO / IEC TR 13335-1: 2001 Guidelines for the Management of IT Security і IEC 61508: 2000 Functional Safety of Electrical / Electronic / Programmable Safety Related. Проміжні результати та подання про аналіз ризиків ІБ, використовуються спеціальні діаграми CORAS, які вбудовані в UML.

Метод CORAS - це програмний інструмент, шо документує, генерує звіти про результати аналізу за допомогою моделювання ризику [39].

Роботи аналізу ризиків базуються на наступних етапах:

1) заходи з підготовки – загальні відомості про об'єкт аналізу;

2) представлення клієнтом переліку об'єктів, що необхідно проаналізувати;

3) опис завдання аналітиком;

4) перевірка на коректність та повноту документів, які представлені для аналізу;

5) визначення переліку заходів з виявлення ризиків, (можливо організувати семінар) аналітиком;

6) оцінювання наслідків інцидентів і ймовірностей ІБ;

7) виявлення ризиків, які прийнятні та тих ризиків для оцінювання для подальшого усунення;

8) нейтралізація загроз, з метою зменшення ймовірності та (або) наслідків інцидентів в сфері ІБ.

Інформаційні систем розглядаються відповідно до CORAS не тільки з точки зору технологій, які використовуються, а в загальному, як складний комплекс, а також враховується фактор людини. Правила методології CORAS представленні у вигляді додатків для Windows і Java.

Методологія CRAMM (CCTA Risk Analysis and Management Method) розроблена британським Центральним комп'ютерним і телекомунікаційним агентством використовується урядовими організаціями та комерційними підприємствами [40]. Програмний засіб CRAMM має різні версії, які підходять до різних типів організацій, відрізняться базами знань, та «профілями». Метод CRAMM здійснює аналіз ризиків визначаючи ідентифікацію та розрахунок рівнів ризиків на основі оцінок, присвоєних ресурсам, вразливостям та загрозам ресурсів.

Ідентифікація та вибір контрдій дозволяють зменшити ризик до прийнятного рівня і таким чином здійснюється контроль ризиків.

Формальний метод який базується на цій концепції дозволяє впевнитись, що захищена вся система, а також що:

• всі ризики існуючі визначені;

• ідентифіковані вразливості та визначені їх рівні;

• ідентифіковані загрози та оцінені їх рівні;

• ефективно діють контрзаходи;

• виправдані витрати на ІБ.

З використанням методу CRAMM, дослідження стану ІБ системи здійснюється в три етапи:

1) на першому етапі –визначення цінності ресурсів, які захищаються. Результатом завершення стадії замовник повинен знати, чи вистачить для захисту базового рівня захисту з поточними функціями безпеки, чи необхідний детальний аналіз;

2) на другому – оцінюються вразливості, визначаються рівнів загроз для груп ресурсів. Результатом цього етапу є ідентифікація і оціпеніння рівні ризиків для замовника;

3) на третьому етапі – розглядаються адекватні контрзаходи. Тобто це розробляються варіанти системи безпеки, які будуть відповідати вимоги замовника. На цьому етапі замовник буде знати, як необхідно покращити систему захисту для ухилення від впливу ризику, а також які заходи протидії спеціальні, вплинуть га зменшення та мінімізації впливу інших ризиків.

Метод CRAMM використовує технологію оцінювання загроз та вразливостей неопосередкованим чином, існує можливість результати перевірити. Тобто, використовується моделювання інформаційної системи з точки зору безпеки з використанням бази даних по контр діям. CRAMM метод направлений на детальне оцінювання ризику, а також на ефективне використання декількох комбінацій різних контрзаходів. Існують комерційні програмні засоби, що базуються на методиці CRAMM. Зокрема, компанія Siemens розробила програми CRAMM Expert і CRAMM Express [40].

Методологія OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) розроблена в університеті Карнегі-Меллона при Інституті програмної інженерії і активно залучає власників інформації для визначення інформаційних активів, які критичні для ІБ та асоційованих з ними ризиків [41].

Методика ґрунтується на створенні групи аналізу, яка досліджує ІБ. Група аналізу (ГА) складається з співробітників підрозділів, які експлуатують систему, та співробітників відділів ІТ.

Методика OCTAVE – базується на трьох етапному підході оцінювання ризиків ІБ.

На першому етапі оцінюються організаційні аспекти. На цьому етапі ГА визначаються критерії або показники оцінки збитку або неприйнятні наслідки, які потім можуть бути використані для оцінки ризиків. Також на першому етапі, визначаються найбільш важливі організаційні ресурси та проводиться оцінка поточного стану ІБ на підприємстві.

Результатом цього етапу є вимоги безпеки за критеріями, і розробляється для кожного критичного ресурсу профіль загроз.

На другому етапі – аналізується за рівнями ІТ-інфраструктура організації, приділяється увага на ступінь, з якою питання безпеки вирішуються і підтримуються підрозділами й співробітниками, відповідальними за експлуатацію інфраструктури.

На третьому етапі розробляється стратегія щодо забезпечення безпеки та плану захисту інформації організації.

На цьому етапі визначаються та аналізуються ризики та розробляються стратегії забезпечення ІБ та план зменшення ризиків. Під час визначення та аналізу ризиків проводять оцінювання збитків від реалізації загроз, розраховують імовірнісні критерії оцінки загроз, оцінюють ймовірність реалізації загроз.

При розробці стратегії ІБ та плану зменшення ризиків необхідно:

• описати існуючу стратегію безпеки,

• визначитись з підходами до зменшення ризиків,

• розробити план зменшення ризиків,

• визначити необхідні зміни в стратегії забезпечення ІБ,

• розробити перспективні напрями забезпечення ІБ.

Метод OCTAVE має певну ступінь гнучкості, за рахунок вибору критеріїв, які організація може застосувати для адаптації цієї методології під певні особливості організації. Методологія була розроблена для використання

великими компаніями, а для невеликих підприємств була створена версії OCTAVE-S.

3.2. Інструментарій базового рівня

Відповідно ISO 17799 проаналізуємо існуючий інструментарій:

– Довідкові та методичні матеріали;

– ПЗ аналізу ризиків та аудиту Cobra.

Британські оранізації пропонують наступні продукти:

– Політика інформаційної безпеки (Information Security Police)

– Довідники щодо захисту інформації (SOS - INTERACTIVE "ONLINE" SECURITY POLICIES AND SUPPORT);

– Настанова для співробітників служб безпеки (Security Professionals Guide).

Ці продукти є довідниками, для реалізації практичної частини реалізації політики безпеки відповідно до ISO 17799. Демонстраційні версії (Evaluation version) можна завантажити з сайту [28].

Представлені методичні матеріали детально описують вимоги стандарту ISO 17799 і виконані в стилі цього стандарту. Перевагою є зручна навігація та гіпертекстова структура.

COBRA програмний засіб для аналізу та управління ризиками, виробником є C&A Systems Security Ltd., він дозволяє формалізувати і швидше перевіряти на відповідність ІБ вимогам Британського стандарту BS 7799 (ISO 17799), а також проводити аналіз ризиків простий. Існують база знань загальних вимог BS 7799 (ISO 17799) і спеціалізовані бази, які зосереджені на відповідну сферу застосування. Доступна демонстраційна версія цього ПЗ.

ПЗ COBRA представляє вимоги стандарту як тематичні «опитальники» з деяких напрямків діяльності організації [27].

За даним методом, аналіз ризиків, відповідає базовому рівню безпеки, тобто не визначаються рівні ризику. Перевагою цієї методики є її простота у

використанні. Необхідно надати відповіді на кілька десятків питань, потім відбудеться формування звіту автоматично.

Цей програмний продукт використовувати для проведення аудиту ІБ організації, а також у роботі спеціалістів служб, що відповідають за забезпечення ІБ.

Простота цього методу та відповідність міжнародному стандарту, малий перелік питань дозволяють достатньо легко адаптувати для роботи у вітчизняних умовах.

Ще один метод, який можливо віднести до базового рівня це RA Software Tool. Даний метод базується на британському стандарті BS 7799, частинах 1 і 2, а також на методичних матеріалах Британського інституту стандартів (BSI) PD 3002 (Керівництво з оцінки та управління ризиками), PD 3003 (Оцінка готовності компанії до аудиту відповідно до BS 7799), PD 3005 (Керівництво з вибору системи захисту), а також стандарті ISO 13335, частини 3 і 4 (Керівництво з управління режимом інформаційної безпеки, технології управління безпекою і вибір засобів захисту) [35].

Основні модулі методу:

– основні модулі;
– аналіз;
– ідентифікація вимог безпеки;
– базове/детальне оцінювання ступеня ризику;
– базова оцінка;
– детальне оцінювання ступеня ризику;
– вибір засобів управління;
– сертифікація.

Кожний модуль розбивається на ряд етапів

Досліджуваний інструментарій виконує оцінювання ризиків відповідно до вимог базового рівня, також з деталізованими специфікаціями PD 3002 Британського інституту стандартів.

3.3. Засоби повного аналізу ризиків

Чітко визначити границі між методами базового та повного аналізу ризиків достатньо складно. Наприклад, згаданий вище RA Software Tool має перелік найпростіших засобів, що дозволяють формально віднести до засобів повного аналізу ризиків. Нижче розглядається інструментарій з більш розвиненими засобами аналізу ризиків та управління ними.

Програмні засоби, що здатні проводити повний аналіз ризиків, створюються на базі структурних методів системного аналізу і проектування (SSADM - Structured Systems Analysis and Design), також відносяться до категорії засобів автоматизації розробки або CASE-засобів (Computer Aided System Engineering) [28,42].

Такі методи є інструментом для:

– розробки моделі ІС з позиції ІБ;
– категорування цінності ресурсів;
– розробки модулі загроз та оцінки їх ймовірностей;
– вибору контрзаходів та аналізу їх ефективності;
– аналізу варіантів побудови системи захисту;
– документування (генерації звітів).

Використовуючи методологію CRAMM розроблено програмний засіб для оцінювання ризиків, включає в себе наступне:

– база даних більше 3000 контрзаходів, що включає всі аспекти ІБ, відповідно до BS 7799, ISO 15408 та іншими стандартами;
– має 400 типів ресурсів ІС, більше 25 описів збитків, більше 10 способів оцінювання збитку, більше 38 типів моделей загроз, 150 існуючих комбінацій збитку, загрози та вразливості, 7 рівнів ризику;
– має набір засобів інструментальних для проведення аудиту та проходження сертифікації на відповідність стандарту BS 7799;
– містить набір типових політик безпеки та документів, що налаштовуються для кожної організації окремо;

– існують засоби планування забезпечення безперервності бізнесу;

– існують засоби аналізування ризиків застосовуючи CRAMM v.5 Express;

– існують засоби відображення та документування механізмів безпеки і результатів аудиту.

Цей метод має необхідну певну універсальність, яка дозволяє застосовувати його в проектах будь-якої складності.

Але цей продукту має деякі недоліки:

– вимагається спеціальна підготовка спеціаліста і його висока кваліфікація;

– частіше підходить для аудиту вже існуючих систем безпеки, для розроблюваних систем є певні складнощі;

– проведення аудиту ІБ системи потребує багато часу;

– створює багато паперової документації, яка не завжди приносить користь на практиці;

– існують деякі труднощі з відображенням кирилиці;

– користувач не може заносити доповнення до бази знань, а це впливає негативно вразі необхідності адаптації до потреб організації;

– будувати свій шаблон звіту або модифікувати існуючий неможливо.

Компанія RiskWatch пропонує два інструменти: один стосується до інформаційної, інший - до фізичної безпеки. ПЗ цієї компанії ідентифікує та оцінює захист ресурсів, загроз, вразливостей і заходів захисту в сфері комп'ютерної та фізичної безпеки підприємства.

RiskWatch проводить аналіз ризиків і має можливість запропонувати обґрунтований вибір заходів і засобів захисту. Методика, яка використовується в програмі складається з чотирьох етапів [38].

Перший етап - визначення предмета дослідження. На цьому етапі повинні бути описані параметри організації: склад системи, що досліджується, її тип, описані базові вимоги в сфері ІБ. Описання повинно формалізовано у переліку підпунктів, які можна використати для подальшої деталізації або пропустити. В

шаблонах представлені списки категорій ресурсів, які захищаються, вразливостей, загроз, втрат і переліку заходів захисту для полегшення роботи аналітика. З них аналітик вибирає ті, які реально існують в організації.

Другий етап – заповнення даних, які відносяться до конкретних характеристик системи. Ці дані вводяться вручну або можуть бути імпортовані із звітів, які були створені з використанням інструментальних засобів дослідження вразливостей комп'ютерних мереж та систем.

На цьому етапі:

- детально описані ресурси, класи інцидентів і втрати. Класи інцидентів обчислюють використовуючи зіставлення категорії втрат і категорії ресурсів;
- використовуючи опитувальник, виявляють можливі вразливості, його база містить більше 600 запитань. Питання відносяться до категорій ресурсів. Існує можливість корегувати, видаляти питання або додавати нові;
- за кожною з виділених загроз визначається частота її появи, ступінь вразливості і цінність ресурсів. Потім все це дає змогу надалі розрахувати ефективність засобів захисту, які були впроваджені в систему [38].

Третій етап – оцінювання ризику. На початку необхідно встановити зв'язки між ресурсами, які захищаємо, вразливостями, загрозами, збитком, які були визначені на попередніх етапах.

Для розрахунку ризиків використаємо формулу математичного очікування втрат за рік:

$$m = p \times v, \qquad (3.1)$$

де p – частота виникнення загрози протягом року,

v – вартість ресурсу, на яку направлена загроза.

Четвертий етап – генерація звітів. Існують наступні типи звітів:

- короткий підсумок;
- звіти про елементи повні і короткі, які описаних на етапах 1 і 2;

– звіт щодо вартості ресурсів, які захищаємо та втрат від реалізації загроз, які очікуються;
– звіти про загрози та перелік заходів протидії;
– звіт про результати аудиту безпеки.

До основних переваг програмного продукту RiskWatch, можна віднести:

– простота використання;
– методологія аналізу ризиків;
– поєднання кількісної та якісної оцінки ризиків;
– велика база знань щодо загроз, вразливостей і контрзаходів;
– існує можливість редагувати і вдосконалювати базу знань;
– існує можливість налаштовувати звіти.

Такий метод дуже зручний, вразі якщо необхідно аналізувати ризики на програмно-технічному рівні системи захисту не враховуючи організаційні та адміністративні складові. Але потрібно усвідомити, що отримані оцінки ризиків (математичне очікування втрат) не достатньо з точки зору розуміння ризику з системних позицій.

Компанія AEXIS Security Consultants і XiSEC Consultants Ltd розробила програмний продукт RA2 the art of risk, який здійснює оцінювання і дозволяє управляти інформаційними ризиками. Його призначення в першу чергу полягає для того, щоб полегшити створення СУІБ у відповідності до вимог міжнародного стандарту ISO 27001. В RA 2 реалізовано достатньо простий для процесний підхід, в стандарті ISO 27001 визначені загальні вимоги і більш докладно описані в стандарті BS 7799-3. Фахівці в галузі управління безпекою Тед Чамфріз та Анжеліка Плейт є розробниками цього програмного засобу. Вони займались редактуванням британського стандарту BS 7799 та міжнародних стандартів ISO 27001 та ISO 17799, а також є авторами серії книжок BIP 0071-0074, що є офіційними посібниками з впровадження стандартів серії 27000 Британського інституту стандартів [28,35,43].

Процес побудови СУІБ в RA2 має на чотири етапи:

– збір інформації (Information Gathering).

– оцінка ризиків (ISMS Risk).

– обробка ризиків (Risk Management Decisions).

– впровадження механізмів контролю (Implementation of Controls).

Кожен етап програми докладно пояснений у відповідності зі стандартом BS 7799.

Програмний продукт RA2 містить засоби щодо вирішення завдань:

– визначення переліку дій, бізнес-вимоги, політики та мету СУІБ;

– реєстр активів СУІБ;

– оцінка ризиків СУІБ;

– ухвалення рішення щодо обробляння ризиків використовуючи вибір відповідних контрзаходів з програми А до стандарту BS 7799-2;

– дослідження розбіжностей зі стандартом ISO 27002;

– розробка Декларації про використання та інших документів СУІБ.

Недоліком цього програмного продукту при практичному використанні в якості засобу для управління ризиками в організації є те що недостатньою відпрацьований інтерфейс користувача, примітивні засобів, що використовуються для роботи з моделями активів, загроз і вразливостями, а також існують певні недоліки щодо відображення кирилиці в звітах.

Британською компанією IT Governance спільно з Vigilant Software розроблений програмний продукт vsRisk Risk Assessment Tool. Він є сучасним засобом оцінювання ризиків, як і ПЗ RA2, повністю відповідає вимогам міжнародного стандарту ISO 27001 [27,43].

Дане ПЗ пропонує простий і зрозумілий інтерфейс на основі візард і має наступні властивості:

– оцінює ризики щодо порушення цілісності, конфіденційності та доступності інформації для бізнесу, а також дотримання вимог законодавства і контрактних зобов'язань відповідно до ISO 27001;

– базується на стандартах: ISO / IEC 27002, BS 7799-3:2006, ISO / IEC TR 13335-3:1998, NIST SP 800-30;

– містить базу знань загроз і вразливостей, яка інтегрована і регулярно оновлюється.

Програмний продукт пропонує засоби для якісної оцінювання всіх факторів ризиків, а також включає вразливості, загрози, активи і механізми контролю.

Відповідно до вимог стандарту ISO 27001 за результатами оцінки ризиків vsRisk формує декларацію про використання механізмів контролю та надає план оброблення ризиків.

До переваг даного програмного продукту віднесемо, те що інтерфейс пропонує всі необхідні пояснення, він простий у використанні, і повністю задовольняє вимоги міжнародного стандарту ISO 27001, які стосуються до оцінки ризиків.

Існує декілька недоліків, що характерні для vsRisk:

– символи кирилиці некоректно відображаються.

– засоби для побудови моделі активів відсутні (наразі, такі засоби передбачені, наприклад в CRAMM).

– загрози не відповідають типами вразливостей і категоріями активів.

– відсутня можливість додавати пояснення і обґрунтувати вибір тих чи інших значень величини вразливості і ймовірності загрози. В результаті, неможливо визначити, чому були обрані ті чи інші значення під час аналізу результатів оцінки ризиків.

– опис механізмів контролю включає в себе тільки назва і цілі.

Компанія MethodWare випускає перелік програмних засобів, які можуть бути корисними для аналітиків в області ІБ для проведення аналізу ризиків, управлінні ризиками, аудиті ІБ [42]:

– ПЗ з аналізу та управління ризиками Operational Risk Builder і Risk Advisor. Методологія базується на австралійському стандарту Australian / New Zealand Risk Management Standard (AS / NZS 4360:1999). Також розроблена версія, відповідно до ISO 17799;

– ПЗ управління життєвим циклом інформаційної технології відповідно з відкритим стандартом в сфері IT CobiT Advisor 3rd Edition (Audit) і CobiT 3rd Edition Management Advisor. У посібниках CobiT особливе місце приділяється управління та аналізу ризиками;

– ПЗ для автоматизації розробки різноманітних листів опитування Questionnaire Builder.

Розглянемо ПЗ Risk Advisor, яке є інструментарієм для аналітика або менеджера в сфері ІБ. Методика, яка реалізована в ПЗ, дозволяє задати модель інформаційної системи з точки зору інформаційної безпеки, ідентифікувати загрози, ризики та втрати в наслідок інцидентів ІБ.

Основні етапи роботи ПЗ Risk Advisor:

– описання контексту (існує кілька аспектів моделі взаємодії організації із зовнішнім середовищем: організаційний, бізнес-цілі, стратегічний, критерії оцінювання ризиків та управління ризиками);

– описання ризиків (складається матриця ризиків, описуються у відповідності з розробленим шаблоном і виявляються зв'язки цих ризиків з іншими елементами моделі);

– описання загроз (складається список загроз, класифікуються, потім виявляється зв'язок між ризиками та загрозами. Описання також проводиться на якісному рівні що дозволяє зафіксувати ці взаємозв'язки);

– оцінювання втрат (перелік подій (наслідки), які пов'язані з порушенням режиму ІБ. Втрати оцінюються у визначеній системі критеріїв);

– аналіз управляючих впливів;

– розробка пропозицій контрзаходів та плану дій.

Результатом розробки моделі формується докладний звіт з 100 розділів, на екрані агреговані опису можна подивитися у вигляді графіка ризиків [42].

Це ПЗ документує багато аспектів, які пов'язані з управлінням ризиком, на адміністративному та організаційному, тобто верхніх рівнях. На нижньому рівні програмно-технічні аспекти фіксувати в цій моделі не дуже зручно. Оцінки представлені в якісних шкалах, детального аналізу факторів ризиків не має.

Перевагою даного методу є можливість подання різнопланових взаємозв'язків, адекватного врахування багатьох факторів ризику та суттєва менша трудомісткість в порівнянні з CRAMM.

ПЗ «Авангард» позиціонується як експертна система управління інформаційною безпекою. Структура і функції комплексу наведено на рис. 3.1.

Типовий пакет програмних засобів «Авангард» включає два програмних комплексів – «Авангард-Аналіз» і «Авангард-Контроль». Кожен з цих комплексів використовує на своє методику оцінювання ризиків.

У першому передбачається оцінка ризиків на основі розрахунку ризикостворюючих потенціалів компонентів системи. При цьому, під ризикостворюючих потенціалом розуміється та частина сукупного ризику, пов'язаного з системою, яка може бути віднесена на рахунок цього компонента.

Рис. 3.1. Структура і функції ПЗ «АванГард»

Методика передбачає, що будь-який ризик виникне за рахунок реалізації деякої безлічі загроз, кожна з них, може бути визначена як загроза безпеці будь-

якого компонента системи. Таким чином, можливо визначити ризикостворюючий потенціал кожної із загроз в залежності від її впливу в події ризику, а також ризикостворюючі потенціали тих компонентів, до яких ці загрози відносяться, і розрахувати ризики за всіма структурними складовими оцінюваної системи і по системі взагалі. Програмний комплекс «Аван-Гард-Аналіз» може виконувати допоміжну роль для вирішенні задач управління ІБ, а саме: провести всебічний аналіз, що дозволить повноцінно визначити перелік цілей безпеки, обґрунтувати політику безпеки, гарантувати повний перелік вимог безпеки, контролювати виконання. Відповідно оцінювання ризиків в цьому ПЗ обчислюється з метою вирішення перерахованих проблем.

Завдання контролю рівня захищеності АІС вирішує методика оцінки ризиків комплексу «Авангард-Контроль» і тому відрізняється від методики комплексу «Авангард-Аналіз». Якщо методика комплексу «Авангард-Аналіз» відноситься до ризиків можливих порушень безпеки оцінюваної системи, то методика комплексу «Авангард-Контроль» призначена ризикам, які є результатом невиконання вимог забезпечення безпеки оцінюваної системи і її компонентів.

При використанні ПЗ «Авангард-Контроль» необхідно, щоб кожний компонент оцінюваної системи мав повний набір вимог, виконання яких дорівнює нульовому ризику порушення безпеки системи. Тобто, мається на увазі, що порушення безпеки системи буде 100-відсотковим вразі невиконання всіх вимог [32,33].

При розробці повних наборів вимог можливе використання профілів захисту для окремих компонентів оцінюваної системи, заснованих на основі ISO 15408-2002 за критеріями оцінки безпеки інформаційних технологій.

Програмний комплекс «Авангард-Контроль», має дві частини – програмного комплексу «Авангард-Центр» і «Авангард-Регіон». Перший призначений для розробки профілів захисту (ПЗ), підготовка і розсилання ПЗ допомогою електронної пошти за підконтрольним частинам АІС, автоматизований збір звітності про виконання вимог безпеки в частинах АІС,

оцінка ризиків вразі невиконання вимог безпеки в АІС, ідентифікація проблемних місць в захисті. Другий – для отримання профілів захисту в окремих частинах АІС, автоматизації ведення звітності про виконання ПЗ та надсилання цієї звітності для її обробки ПК «Авангард-Центр».

Розробка профілів захисту в ПК «Авангард-Центр» проводиться в розділі ведення каталогів програмного комплексу. Спочатку в «Авангард» було визначено основні поняття, метаклас, клас, міра, вимога. Метакласи призначені для групування класів об'єктів АІС за конкретними ознаками. Класи визначають класи об'єктів, для яких розробляються типові набори вимог (профілі захисту). Заходи встановлюють функціональні класи і класи гарантій вимог у термінології ІСО 15408-2002. Вимоги включають функціональні сімейства, сімейства гарантій, функціональні компоненти, компоненти гарантій, функціональні елементи і елементи гарантій відповідно до ІСО 15408-2002 [28].

За результатами аналізу виконання вимог «АванГард-Центр» дозволяє оцінити ризики невиконання вимог в інформаційній системі. Інформація представляються у вигляді гістограм оцінок ризиків невиконання вимог. Чим більше вимог не виконується, тим більше ризики і тим вище стовпчики гістограми.

Таким чином, ПЗ «Авангард» автоматизує процес розробки профілів захисту відповідно до стандарту ISO 15408-2002, а також використовувати ПЗ для оцінювання виконання цих вимог в ІС організації.

3.4. Загальні недоліки та обмеження комерційних програмних продуктів

Загальні недоліки, які присутні у багатьох програмних продуктів, призначеним для управління ризиками, обмежують їх практичне застосування. До числа найбільш поширених недоліків слід віднесемо:

– не в повній мірі сумісні з міжнародними стандартами – наприклад, мало продуктів було розроблено спеціально для ISO 27001.

– неповний перелік активів. Більшість продуктів зосереджуються тільки на IT активах, інші види активів ігнорують, які однак, не менш важливі для ІБ;

– складність використання. Багато продуктів занадто складні у використанні непідготовленому працівникові;

– утруднення процесу усвідомлення ризиків, так як розрахунок ризиків виконується автоматично і прихований від користувача;

– притаманні ті чи інші проблеми з відображенням української мови, що характерно для більшості імпортних програмних продуктів.

Багато відомих продукти або не дозволяють проводити повноцінної оцінки ризиків, а швидше за все, є засобами для аналізу невідповідностей вимог стандарту ISO 27001, або включають в себе недостатні кошти оцінки ризиків, які не повністю відповідають вимогам ISO 27001, хоча в них багато функціоналу, або є занадто складними у використанні і мають високу вартість.

Можна було б виділити зі списку програмних продуктів, аналізованих раніше, RA2 the art of risk як інструмент, повністю відповідає вимогам ISO 27001, оскільки його розробники є авторами цього міжнародного стандарту, однак він не має можливості порівнювати між собою результати оцінок, містить примітивні засоби побудови моделі активів і редагування текстової інформації, що утрудняє його використання.

Можливо використовувати Risk Watch, однак він, як і багато інших програмних засобів, що не був спеціально розроблений відповідно до стандарту ISO 27001, має високу вартість.

Можна було б звернути увагу на новий продукт vsRisk британської компанії IT Governance. Він дозволяє за результатами оцінювання ризиків отримувати повноцінну декларацію про застосовність в повній відповідності з вимогами стандарту ISO 27001. Однак vsRisk також неправильно відображає українські літери і містить ряд інших суттєвих недоліків, що утрудняють його практичне використання, описаних в попередньому підрозділі.

3.5. Висновок по розділу

В даному розділі були розглянуті методології управління ризиками інформаційної безпеки:

- Методологія CORAS;
- Методологія CRAMM;
- Методологія OCTAVE.

Був проаналізований інструментарій базового рівня:

- COBRA;
- RA Software Tool;

та засоби повного аналізу ризиків:

- RiskWatch;
- RA2 the art of risk;
- vsRisk;
- Risk Advisor;
- «Авангард».

Знайти інструментарій, який позбавлений перерахованих недоліків і в той же час повністю відповідає вимогам міжнародних стандартів, досить складно. Проблема також полягає в тому, що багато програмних продуктів, які позиціонуються розробниками як засоби для оцінки або управління ризиками, по суті такими не є, оскільки не реалізують ні методології оцінки ризиків, ні алгоритму їх обчислення, а надають лише засоби представлення та зберігання даних про ризики, залишаючи аналіз і оцінювання користувачеві.

Були досліджені загальні недоліки та обмеження комерційних програмних продуктів.

РОЗДІЛ 4
МЕТОДОЛОГІЯ СИНТЕЗУ СИСТЕМИ ОЦІНЮВАННЯ РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ РЕСУРСІВ

4.1. Методологічний базис нечітких множин для вирішення задач оцінки ризиків

Насамперед, слід зазначити, що методологія нечіткого моделювання не замінює і виключає методологію системного моделювання, а конкретизує останню стосовно процесу побудови та використання нечітких моделей складних систем. Процес нечіткого моделювання представляє аналогічну послідовність взаємопов'язаних етапів, як і процес системного моделювання. При цьому кожен із етапів виконується з метою побудови та використання нечіткої моделі системи для вирішення вихідної проблеми [44].

У випадку під нечіткою моделлю розуміється інформаційно-логічна модель системи, побудована з урахуванням теорії нечітких множин і нечіткої логіки.

Таким чином, окремими етапами процесу нечіткого моделювання є .

– Аналіз проблемної ситуації.
– Структуризація предметної області та побудова нечіткої моделі.
– Виконує обчислювальні експерименти з нечіткою моделлю.
– Застосування результатів обчислювальних експериментів.
– Корекція чи доопрацювання нечіткої моделі.

Оскільки до справжньому часу запропоновані нечіткі узагальнення для найрізноманітніших розділів математики і логіки , кожне з них потенційно може служити основою для побудови відповідної нечіткою моделі.

Однією з характерних ознак складності побудови моделі є невизначеність у поданні структури або поведінки системи-оригіналу. У цьому сама категорія невизначеності можна розглянути з різних точок зору. У рамках сучасної

методології системного моделювання невизначеність може характеризувати такі аспекти модельних уявлень [44,45].

Неясність чи нечіткість межі системи. Так, наприклад, використання дихотомічних ознак "високий-низький", "великий-маленький", "дорогою-дешевий", "швидкий-повільний" і подібних їм для визначення складу елементів системи стикається з принциповою складністю уявлення структури моделі системи. Характерний приклад цього аспекту невизначеності – власне клас складних систем у тих відповіді питання: "Які системи слід вважати складними?"

Неоднозначність семантики окремих термінів, що використовуються при побудові концептуальних моделей систем. Йдеться про властиву природні мови полісемії або неоднозначність сенсу понять (модель зачіски і математична модель, гральний автомат і автомат як стрілецька зброя, географічна карта місцевості та гральна карта, стріла баштового крана і стріла, пущена з лука).

Неповнота модельних уявлень про деяку складну систему, особливо у зв'язку з вирішенням проблем, що слабо формалізуються. У цьому випадку сама спроба побудувати адекватну модель складної системи або предметної області стикається з принциповою неможливістю врахувати всі релевантні особливості проблеми, що вирішується [47].

Суперечливість окремих компонентів модельних уявлень чи вимог, яким має задовольняти модель складної системи. Так, наприклад, вимога вирішити проблему за мінімальний час і з мінімальними фінансовими витратами містить у собі елемент протиріччя. Елементи протиріч містяться у законодавчих актах та є предметом юридичної практики.

Невизначеність настання тих чи інших подій, що належать до можливості знаходження системи-оригіналу в тому чи іншому стані в майбутньому . Йдеться про те, що аналіз процесу поведінки системи не дає підстав для однозначної відповіді на запитання: "Чи буде система- оригінал в деякому стані в момент часу, який відноситься до її майбутнього?" Цей аспект невизначеності часто називають стохастичним, оскільки він традиційно досліджувався засобами теорії ймовірностей та математичної статистики.

Таким чином, нечітка модель системи-оригіналу, або нечітка система в першу чергу характеризується невизначеністю типу неясності (непарність кістки) межі системи, а також, можливо, окремих її станів, вхідних та вихідних впливів. У цьому випадку вихідна структуризація нечіткої системи може бути зображена графічно у вигляді фігури з розпливчастими межами (рис. 4.1).

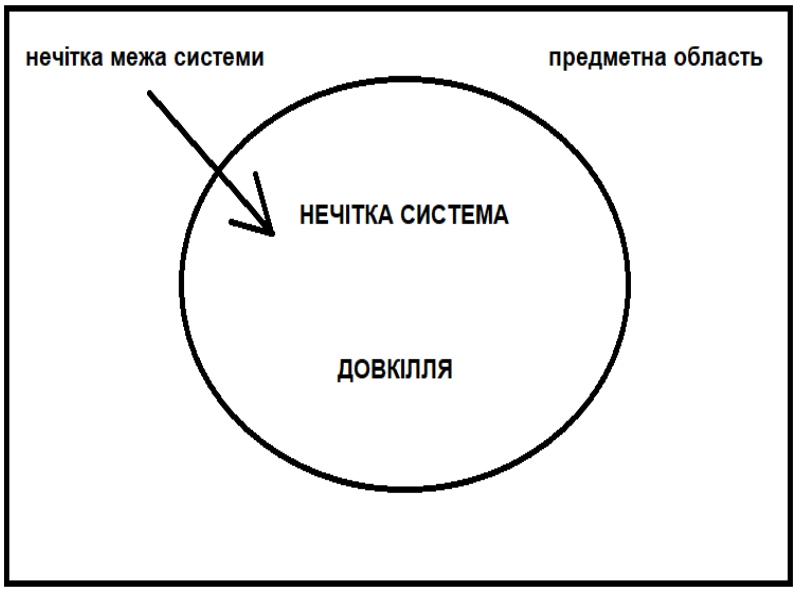

Рис. 4.1. Графічна ілюстрація нечіткої системи як системи з нечітким кордоном

Як було зазначено вище, базовою методологією побудови нечітких моделей є власне теорія нечітких множин та нечітка логіка, які, у свою чергу, є узагальненням класичної теорії множин та класичної формальної логіки [48].

Основні поняття теорії нечітких множин

До теперішнього часу запропоновано найрізноманітніші визначення нечітких теоретико-множинних понять. Розглянемо той матеріал, який безпосередньо застосовується для вирішення практичних завдань і тією чи іншою мірою реалізований у відповідних інструментальних засобах.

Нечітка множина (fuzzy set) представляє собою бій сукупність елементів довільної природи, щодо яких не можна з певністю стверджувати - належить той чи інший елемент аналізованої сукупності даному безлічі чи ні. Іншими словами, нечітка множина відрізняється від звичайної множини тим, що для всіх або частини його елементів не існує однозначної відповіді на запитання: "Належить

або не належить той чи інший елемент, що розглядається, не чіткій множині?" Можна це питання поставити і по-іншому: "Мають чи ні його елементи деякою характеристичною властивістю, яка може бути використана для завдання цієї нечіткої множини?"

Для побудови нечітких моделей систем саме поняття нечіткої множини слід визначити суворо, щоб унеможливити неоднозначність тлумачення тих чи інших його властивостей. Виявилося, що існують кілька варіантів формального визначення нечіткої множини, які, по суті, відрізняються між собою способом завдання характеристичної функції цих множин. Серед цих варіантів найбільш природним та інтуїтивно зрозумілим є завдання області значень подібної функції як інтервал дійсних чисел, укладених між 0 та 1 (включаючи самі ці значення).

Математичне визначення нечіткої множини. Формально нечітка множина A визначається як безліч упорядкованих пар або кортежів виду: $< x, \mu_A(x) >$, де x є елементом деякої універсальної множини або універсуму X, а $\mu_A(x)$ – функція приналежності, яка ставить у відповідність кожному з елементів $x \in X$ деяке дійсне число з інтервалу [0, 1], тобто дана функція визначається у формі відображення:

$$\mu_A : X \to [0,1]. \qquad (4.1)$$

При цьому значення $\mu_A(x) = 1$ для деякого $x \in X$ означає, що елемент x безперечно належить нечіткому множині X, а значення $\mu_A(x) = 0$ означає, що елемент x безумовно не належить нечіткому множині X.

У літературі по теорії нечітких множин , яка обчислюється величезним до особистістю робіт, можна зустріти не тільки різні визначення, а також різноманітні позначення для нечітких множин [47,48]. Найбільш загальні з визначень нечіткого безлічі припускають , що в якості області значень функції приладдя можуть виступати інші нечіткі безлічі або довільні цілком упорядковані безлічі .

Оскільки існуючі відмінності у формах запису не мають принципового значення, в наступному тексті нечіткі множини для зручності будуть позначатися рукописними великими літерами: A, B, C, D.

З усіх нечітких множин виділимо два окремі випадки, які по суті збігаються зі своїми класичними аналогами і використовуються в подальшому при визначенні інших нечітких понять.

Теоретично нечітких множин зберігають свій сенс деякі спеціальні класичні множини. Так, наприклад, порожня нечітка множина або безліч, яка не містить жодного елемента, як і раніше позначається через $\varnothing$ і формально визначається як така нечітка множина, функція приналежності якого тотожно дорівнює нулю для всіх без винятку елементів: $\mu_{\varnothing} = \varnothing$. У цьому характеристична функція звичайної порожньої множини також тотожно дорівнює нулю для будь-яких елементів: $X_{\varnothing} = \varnothing$.

Універсум. Що стосується іншої спеціальної множини, то так званий універсум, що позначається через X, вже був використаний вище як звичайна множина, що містить в рамках деякого контексту всі можливі елементи. Формально зручно вважати, що функція приналежності універсуму як нечіткої множини тотожно дорівнює одиниці для всіх без винятку елементів: $\mu_X = 1$. При цьому характеристична функція звичайної універсальної множини також тотожно дорівнює одиниці для будь-яких елементів: $X_X = 1$ [48].

Для того щоб визначити кінцеві та нескінченні нечіткі множини, необхідно ввести в розгляд одне з основних понять, яке використовується для характеристики довільної нечіткої множини, а саме – поняття носія нечіткої множини.

Носій нечіткої множини. Носієм нечіткої множини A називається звичайна множина A_S, яка містить ті і тільки ті елементи універсуму, для яких значення функції належності відповідної нечіткої множини відмінні від нуля. Математично носій нечіткого множини визначається наступною умовою:

$$A_S = \{x \in X | \mu_A(x) > 0\} \qquad \forall x \in X. \tag{4.2}$$

Очевидно, порожня нечітка множина має порожній носій, оскільки $\mu_\varnothing = \varnothing$ для будь-якого його елемента. Носій універсуму, що розглядається як нечітка множина, збігається з самим універсумом. Для зручності і скорочення запису довільної нечіткої множини часто вказують лише значення його функції приналежності для елементів носія, неявно припускаючи, що всі інші значення функції приналежності дорівнюють нулю.

Залежно від кількості елементів у нечіткій множині за аналогією зі звичайними множинами можна визначити кінцеві та нескінченні нечіткі множини.

Кінцеві нечіткі множини. Нечітка множина називається кінцевою, якщо її носій є кінцевою множиною. При цьому цілком доречно говорити, що така нечітка множина має кінцеву потужність, яка чисельно дорівнює кількості елементів його носія як звичайної множини. Зручно вважати потужність порожньої множини, що дорівнює 0 [48,49].

Нескінченні нечіткі множини . Аналогічним чином можна визначити і нескінченні нечіткі множини як такі нечіткі множини, носій яких не є кінцевою множиною. При цьому лічильною нечіткою множиною будемо називати нечітку множину з лічильним носієм, тобто носій якого має лічильну потужність $\aleph_0$ у звичному значенні. Численним нечітким безліччю будемо називати нечітке безліч з незліченним носієм, тобто носій якого має незліченну потужність або потужність континууму з (або $\aleph$) у звичайному розумінні.

Дане вище визначення носія нечіткої множини коректно, оскільки як для кінцевих, так і для нескінченних нечітких множин вираз має сенс.

Щоб навести деякі приклади нечітких множин і розпочати визначення їх основних властивостей, слід розглянути основні способи, якими формально можуть бути задані довільні нечіткі множини.

Нечіткі множини можуть бути задані двома основними способами:

1. У формі списку з явним перерахуванням всіх елементів і відповідних їм значень функції приналежності, що утворюють нечітку множину, що розглядається. При цьому часто елементи з нульовими значеннями функції приладдя просто не вказуються в цьому списку. Цей спосіб підходить для завдання нечітких множин з кінцевим дискретним носієм і невеликим числом елементів. У цьому випадку нечітка безліч зручно записувати у вигляді: $A = \{< x_1, \mu_A(x_1) >, \ < x_2, \mu_A(x_2) >, \ < x_n, \mu_A(x_n) >\}$, де n - Розглянуте число елементів нечіткої множини A (його носія).

2. Аналітично у формі математичного виразу для відповідної функції власності. Цей спосіб може бути використаний для завдання довільних нечітких множин як з кінцевим, так і з нескінченним носієм . У цьому випадку нечітку множину зручно записувати у вигляді: $A = \{< x, \mu_A(x) >\}$ або $A = \{x, \mu_A(x)\}$ де μ_A - деяка функція, задана аналітично у формі математичного виразу $f(x)$ або графічно у формі деякої кривої. Найчастіше використовувані види функцій власності буде розглянуто нижче [48].

Для формальної строгості при завданні нечітких множин необхідно явно вказувати відповідний універсум X елементів, з яких формується та чи інша конкретна нечітка множина. У загальному випадку ніяких припущень щодо елементів цієї множини не робиться. Проте з практичної точки зору доцільно обмежити універсум елементами предметної області, що розглядається, або розв'язуваної задачі. Оскільки при побудові нечітких моделей систем використовуються кількісні змінні, то найчастіше як універсум X використовується деяке підмножина дійсних чисел R, наприклад, безліч невід'ємних дійсних чисел $R+$ або натуральних чисел N.

Основні етапи нечіткого висновку

Говорячи про нечітку логіку, найчастіше мають на увазі системи нечіткого висновку, які широко використовуються для керування технічними пристроями та процесами. Розробка та застосування систем нечіткого виведення включають

ряд етапів, реалізація яких виконується за допомогою розглянутих раніше основних положень нечіткої логіки.

Інформацією, яка надходить на вхід системи нечіткого виведення, є вимірювані деяким чином вхідні змінні. Ці змінні відповідають реальним змінним процесам управління. Інформація, яка формується на виході системи нечіткого виведення, відповідає вихідним змінним, якими є управляючі змінні процесу управління.

Системи нечіткого висновку призначені для перетворення значень вхідних змінних процесу управління у вихідні змінні на основі використання нечітких правил виведення. Для цього системи нечіткого висновку повинні містити базу правил нечітких виведення та реалізовувати нечіткий висновок висновків на основі посилок або умов, представлених у формі "чітких лінгвістичних висловлювань" [49].

Отже, основними етапами нечіткого висновку є (рис. 4.2.):

– Формування основи правил систем нечіткого висновку.
– Фаззифікація вхідних змінних.
– Агрегування умов у нечітких правилах виведення.
– Активізація або композиція для складання у нечітких правилах виведення.
– Акумулювання висновків нечітких правил виведення.

Формування бази правил систем нечіткого висновку

База правил систем нечіткого висновку призначена для формального подання емпіричних знань або знань експертів у тій чи іншій проблемній галузі. У системах нечіткого виведення використовуються правила нечіткого виведення, у яких умови та висновки сформульовані у термінах нечітких лінгвістичних висловлювань розглянутих вище видів. Сукупність таких правил будемо далі називати базами правил нечіткого виведення.

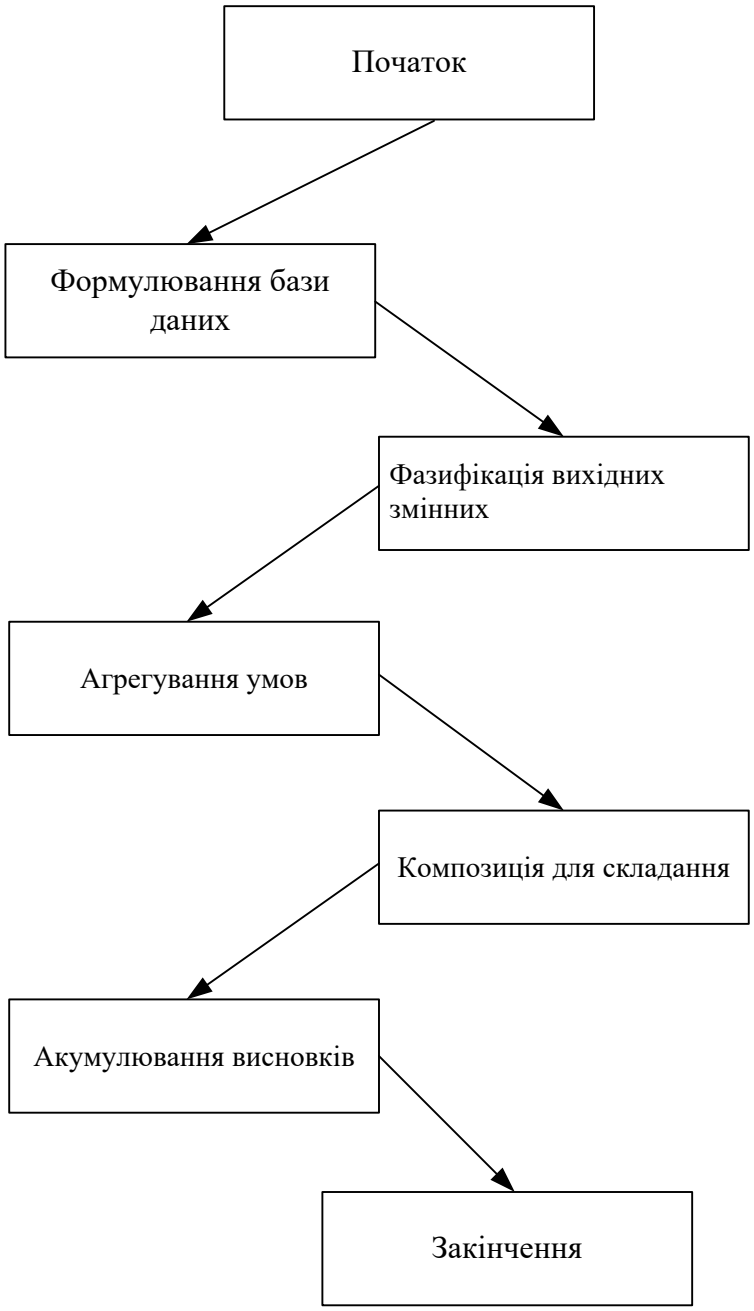

Рис. 4.2. Діаграма діяльності процесу нечіткого виведення у формі діаграми діяльності мови UML

База правил нечіткого виведення є кінцевою множиною правил нечіткого виведення, узгоджених щодо використовуваних у них лінгвістичних змінних. Найбільш часто база правил представляється у формі структурованого тексту:

ПРАВИЛО_1: ЯКЩО "Умова_1" ТО "Укладання_1" (F_1);

ПРАВИЛО_2: ЯКЩО "Умова_2" ТО "Укладання_2" (F_2)

…. (4.3)

ПРАВИЛО_ n: ЯКЩО " Умова_ n " ТО " Укладання_ n " (F_n)

або в еквівалентній формі:

UKR_1: IF Condition_l THEN Conclusion_1 (F_1)

UKR_2: IF Condition_2 THEN Conclusion_2 (F_2)

…..

UKR_ n: IF Condition_ n THEN Conclusions (F_n) (4.4)

Тут через $F_i (i \in \{1,2,...,n\})$ позначені коефіцієнти визначеності або вагові коефіцієнти відповідних правил. Ці коефіцієнти можуть набувати значень з інтервалу [0, 1]. Якщо ці вагові коефіцієнти відсутні, зручно прийняти, що й значення рівні 1.

Узгодженість правил щодо лінгвістичних змінних, що використовуються , означає, що в якості умов і висновків правил можуть використовуватися тільки нечіткі лінгвістичні висловлювання, при цьому в кожному з нечітких висловлювань повинні бути визначені функції належності значень терм-множини для кожної з лінгвістичних змінних [48].

Вхідні та вихідні лінгвістичні змінні, системах нечіткого виведення лінгвістичні змінні, які використовується в нечітких висловлюваннях під умов правил нечіткого виведення, часто бувають вхідними лінгвістичними змінними, а змінні, які використовуються в нечітких висловлюваннях під складанням правил.

Таким чином, при завданні або формуванні бази правил нечітких продуктів необхідно визначити: безліч правил нечіткого виведення: $P = \{R_1, R_2, ..., R_n\}$ у формі (4.4), безліч вхідних лінгвістичних змінних: $V = \{\beta_1, \beta_2, ..., \beta_m\}$множина вихідних лінгвістичних змінних: $W = \{\omega_1, \omega_2, ..., \omega_s\}$. Тим самим було база правил нечіткого виведення вважається заданої, якщо заданий множини P, V, W.

На формування бази правил систем нечіткого виведення часто впливають деякі додаткові фактори, які визначаються специфікою розв'язуваної задачі або алгоритму нечіткого виведення, що використовується.

Фаззифікація (Fuzzification)

У контексті нечіткої логіки під фазифікацією розуміється як окремий етап виконання нечіткого висновку, а й власне процес чи процедура знаходження значень функцій належності нечітких множин (термів) з урахуванням звичайних (не нечітких) вихідних даних. Фаззифікацію ще називають запровадженням нечіткості.

Метою етапу фазифікації є встановлення відповідності між конкретним (зазвичай – чисельним) значенням окремої вхідної змінної системи нечіткого виведення та значенням функції належності їй терму вхідної лінгвістичної змінної. Після завершення цього етапу для всіх вхідних змінних повинні бути визначені конкретні значення функцій приналежності по кожному з лінгвістичних термів, які використовуються в умовах бази правил системи нечіткого виведення [48,50].

Формально процедура фазифікації виконується в такий спосіб. До початку цього етапу передбачаються відомими конкретні значення всіх вхідних змінних системи нечіткого висновку, тобто безліч значень $V' = \{a_1, a_2, ..., a_m\}$. У загальному випадку кожне $a_i \in X_i$ де X_i, - Універсум лінгвістичної перемінної β_i,. Ці значення можуть бути отримані або від датчиків, або деяким іншим, зовнішнім по відношенню до системи нечіткого виведення способом.

Далі розглядається кожна з умов виду "$\beta_i \epsilon \alpha'$"правил системи нечіткого висновку, деα' - деякий терм з відомою функцією приналежності $\mu(x)$. При цьому значення a_i використовується як аргумент $\mu(x)$, тим самим знаходиться кількісне значення $b_i' = \mu(a_i)$. Це значення і є результатом фазифікації під умови "$\beta_i \epsilon \alpha'$".

p align="justify"> Етап фазифікації вважається закінченим, коли будуть знайдені всі значення $b_i' = \mu(a_i)$ для кожного з умов всіх правил, що входять в аналізовану базу правил системи нечіткого висновку. Це безліч значень позначимо через $B = \{b_i'\}$. У цьому якщо певний терм α'' лінгвістичної змінної β_i

, немає у жодному з нечітких висловлювань, то відповідне йому значення функції власності перебуває у процесі фазифікації.

Агрегування (Aggregation)

Агрегування є процедуру визначення ступеня істинності умов за кожним із правил системи нечіткого висновку.

Формально процедура агрегування виконується в такий спосіб. До початку цього етапу передбачаються відомими значення істинності всіх під умов системи нечіткого висновку, тобто безліч значень $B = \{b_i'\}$. Далі розглядається кожна з умов правил системи нечіткого виводу. Якщо умова правила є нечітким висловлюванням виду 1 або 2, то ступінь його істинності дорівнює відповідному значенню b_i'.

Якщо ж умова складається з кількох умов виду (4.2), причому лінгвістичні змінні в умовах попарно не рівні один одному, то визначається ступінь істинності складного висловлювання на основі відомих значень істинності під умов. При цьому значення b_i' використовуються як аргументи відповідних логічних операцій. Тим самим є кількісні значення істинності всіх умов правил системи нечіткого висновку [50].

Етап агрегування вважається закінченим, коли будуть знайдені всі значення b_k'' для кожного з правил R_k, що входять до бази правил, що розглядається P системи нечіткого висновку. Це безліч значень позначимо через $B'' = \{b_1'', b_2'', ..., b_n''\}$.

Активізація (Activation)

Активізація у системах нечіткого висновку є процедуру чи процес знаходження ступеня істинності кожного з під заключень правил нечіткого виведення. Активізація в загальному випадку багато в чому аналогічна композиції нечітких відносин, але не тотожна їй. При формуванні бази правил системи нечіткого виведення задаються вагові коефіцієнти F_i для кожного

правила (за умовчанням передбачається, якщо ваговий коефіцієнт не заданий явно, його значення дорівнює 1).

Формально процедура активізації виконується в такий спосіб. На початок цього етапу передбачаються відомими значення істинності всіх умов системи нечіткого висновку, тобто. безліч значень $B'' = \{b_1'', b_2'', ..., b_n''\}$ та значення вагових коефіцієнтів F_i для кожного правила. Далі розглядається кожне із висновків правил системи нечіткого висновку. Якщо висновок правила є нечітким висловом виду 1 або 2, то ступінь його істинності дорівнює твору алгебри відповідного значення b_i'' на ваговий коефіцієнт F_i.

Якщо ж висновок складається з кількох під в'язків виду (4.3), причому лінгвістичні змінні в підв'язненнях попарно не рівні один одному, то ступінь істинності кожного з ув'язнень дорівнює алгебраїчному твору відповідного значення b_i'' на ваговий коефіцієнт F_i. Таким чином , знаходяться всі значення c_k ступенів істинності під закладів для кожного з правил R_k, що входять до бази правил, що розглядається P системи нечіткого виведення. Це безліч значень позначимо через $C = \{c_1, c_2, ..., c_q\}$, де q – загальна кількість під складання в базі правил [48,50].

Після знаходження множини $C = \{c_1, c_2, ..., c_q\}$ визначаються функції приналежності кожного з під заключень для аналізованих вихідних лінгвістичних змінних. Для цієї мети можна використовувати один з методів, що є модифікацією того чи іншого методу нечіткої композиції:

min-активізація:

$$\mu'(y) = \min\{c_i, \mu(y)\}; \tag{4.5}$$

prod-активізація:

$$\mu'(y) = c_i \cdot \mu(y); \tag{4.6}$$

average-активізація:

$$\mu'(y) = 0.5 \cdot (c_i + \mu(y)), \tag{4.7}$$

де $\mu(y)$ – функція приналежності терму, який є значенням деякої вихідної змінної ω_j заданої на універсумі Y.

Етап активізації вважається закінченим, коли кожної з вихідних лінгвістичних змінних, які входять у окремі під складання правил нечіткого виведення, будуть визначено функції належності нечітких множин їх значень, тобто. сукупність нечітких множин: $C_1, C_2, ..., C_q$ де q – загальна кількість під складання в основі правил системи нечіткого висновку.

Акумуляція (Accumulation)

Акумуляція або акумулювання в системах нечіткого виводу являє собою процедуру або процес знаходження функції приналежності для кожної з вихідних лінгвістичних змінних множини $W = \{\omega_1, \omega_2, ..., \omega_s\}$.

Мета акумуляції полягає в тому, щоб об'єднати або акумулювати всі ступеня істинності висновків (під заключень) для отримання функції належності кожної вихідних змінних. Причина необхідності виконання цього етапу полягає в тому, що під складання. що належать до однієї й тієї ж вихідної лінгвістичної змінної, належать різним правилам системи нечіткого висновку [48,50].

Формально процедура акумуляції виконується в такий спосіб. На початок цього етапу передбачаються відомими значення істинності всіх під заключень кожному за правил R_k, які входять у аналізовану базу правил P системи нечіткого висновку, у формі сукупності нечітких множин: $C_1, C_2, ..., C_q$ де q – загальна кількість під заключень у основі правил. Далі послідовно розглядається кожна з вихідних лінгвістичних змінних $\omega_j \in W$ і нечіткі множини, що відносяться до неї: $C_{j1}, C_{j2}, ..., C_{jq}$. Результат акумуляції для вихідних лінгвістичної змінної ω_j визначається як поєднання нечітких множин $C_{j1}, C_{j2}, ..., C_{jq}$.

Етап акумуляції вважається закінченим, коли кожної з вихідних лінгвістичних змінних буде визначено підсумкові функції належності нечітких множин їх значень, т. е. сукупність нечітких множин: $C'_1, C'_2, ..., C'_s$, де s – загальна

кількість вихідних лінгвістичних змінних з урахуванням правил системи нечіткого виводу.

Дефаззифікація (Defuzzification)

Дефаззифікація в системах нечіткого виведення є процедуру або процес знаходження звичайного (не нечіткого) значення для кожної з вихідних лінгвістичних змінних множини $W = \{\omega_1, \omega_2, ..., \omega_s\}$.

Мета дефазифікації полягає в тому, щоб, використовуючи результати акумуляцію всіх вихідних лінгвістичних змінних, отримати звичайне кількісне значення (crisp value) кожної з вихідних змінних, яке може бути використане спеціальними пристроями, зовнішніми по відношенню до системи нечіткого виведення.

Дійсно, що застосовуються в сучасних системах управління пристроєм і механізмами здатні сприймати традиційні команди у формі кількісних значень відповідних керуючих змінних. Саме з цієї причини необхідно перетворити нечіткі множини в деякі конкретні значення змінних. Тому дефаззифікацію називають також приведенням до чіткості [50].

Формально процедура дефазифікації виконується в такий спосіб. На початок цього етапу передбачаються відомими функції власності всіх вихідних лінгвістичних змінних у вигляді нечітких множин: $C_1', C_2', ..., C_s'$, де s – загальна кількість вихідних лінгвістичних змінних з урахуванням правил системи нечіткого виводу. Далі послідовно розглядається кожна з вихідних лінгвістичних змінних $\omega_j \in W$ і те, що відноситься до неї, наче безліч C_j'. Результат дефазифікації для вихідної лінгвістичної змінної ω_j визначається у вигляді кількісного значення $y_j \in R$, одержуваного за однією з формул, що розглядаються нижче.

Етап дефазифікації вважається закінченим, коли для кожної з вихідних лінгвістичних змінних буде визначено підсумкові кількісні значення у формі деякого дійсного числа, тобто у вигляді $y_1, y_2, ..., y_s$, де s - загальна кількість вихідних лінгвістичних змінних в основі правил системи нечіткого висновку.

Для виконання чисельних розрахунків на етапі дефазифікації можуть бути використані наступні формули, що отримали назву методів дефазифікації.

Метод центру тяжкості

Центр тяжкості (CoG, COG, Centre of Gravity) або центроїд площі розраховується за формулою:

$$y = \frac{\int_{\min}^{\max} x \cdot \mu(x) dx}{\int_{\min}^{\max} \mu(x) dx}, \quad (4.8)$$

У формулі використовуються такі позначення: y – результат дефаззифікації ; x – змінна, відповідна вихідний лінгвістичної змінної ω; $\mu(x)$ – функція приналежності нечіткої множини, що відповідає вихідній змінній ω після етапу акумуляції; $\min$ і $\max$ – ліва і права точки інтервалу носія нечіткої множини розглянутої вихідний перемінної ω.

При дефазифікації методом центру тяжкості звичайне (не нечітке) значення вихідної змінної дорівнює абсцисі центру тяжкості площі, обмеженою графіком кривої функції належності відповідної вихідний змінної .

Метод центру тяжкості для одноточкових множин

Центр тяжкості (COGS, Centre of Gravity for Singletons) для одноточкових множин розраховується за формулою:

$$y = \frac{\sum_{i=1}^{n} x_i \cdot \mu(x_i)}{\sum_{i=1}^{n} \mu(x_i)}, \quad (4.9)$$

де n – число одноточкових (одноелементних) нечітких множин, кожна з яких характеризує єдине значення вихідної лінгвістичної змінної.

Метод центру площі

Центр площі (u CoA, COA, Centre of Area, Bisector of Area) дорівнює $y = u$ де значення визначається з рівняння:

$$\int_{\min}^{u} \mu(x)dx = \int_{u}^{\max} \mu(x)dx, \tag{4.10}$$

Іншими словами, центр площі дорівнює абсцисі, яка ділить площу, обмежену графіком кривої функції належності вихідної змінної, на дві рівні частини. Іноді центр площі називають бісектрисою площі. Цей метод не може бути використаний у разі однокрапкових множин [48].

Метод лівого модального значення

Ліве модальне значення (LM, Left Most Maximum) розраховується за такою формулою:

$$y = \min\{x_m\}, \tag{4.11}$$

де x_m – модальне значення (мода) нечіткої множини, що відповідає вихідній змінній ω після акумуляції.

Іншими словами, значення вихідної змінної визначається як мода нечіткої множини для відповідної вихідної змінної або найменша з мод (найліва), якщо нечітка множина має кілька модальних значень.

Метод правого модального значення

Праве модальне значення (RM, Right Most Maximum) розраховується за формулою:

$$y = \max\{x_m\}, \tag{4.12}$$

де x_m – модальне значення (мода) нечіткої множини для вихідної змінної після ω акумуляції . У цьому випадку значення вихідної змінної також визначається як мода деякої множини для відповідної вихідної змінної або найбільша з мод (найправіша), якщо нечітка множина має кілька модальних значень.

4.2. Алгоритм нечіткого висновку Мамдані

Розглянуті вище етапи нечіткого виведення можуть бути реалізовані неоднозначним чином, оскільки включають окремі параметри, які повинні бути фіксовані або специфіковані. Тим самим вибір конкретних варіантів параметрів

кожного з етапів визначає деякий алгоритм, який у повному обсязі реалізує нечіткий висновок у системах правил нечіткого виведення. Наразі запропоновано кілька алгоритмів нечіткого висновку, більш детально розглянемо алгоритм Мамдані (Mamdani).

Алгоритм Мамдані є одним із перших, який знайшов застосування в системах нечіткого виведення. Він був запропонований в 1975 р. англійським математиком Е. Мамдані (Ebrahim Mamdani) як метод для управління паровим двигуном. За своєю суттю цей алгоритм породжує розглянуті вище етапи, оскільки найбільшою мірою відповідає їх параметрам [48].

Формально алгоритм Мамдані можна визначити так.

Формування основи правил систем нечіткого висновку. Особливості формування бази правил збігаються з розглянутими вище при описі даного етапу.

Фаззифікація вхідних змінних. Особливості фазифікації збігаються з розглянутими вище при описі цього етапу.

Агрегування умов у нечітких правилах виведення. Для знаходження ступеня істинності умов кожного з правил нечітких виведення використовуються парні нечіткі логічні операції. Ті правила, ступінь істинності умов яких відмінна від нуля, вважаються активними і використовуються для подальших розрахунків.

Активізація під укладень у нечітких правилах виведення. Здійснюється за формулою (4.5), при цьому скорочення часу виведення враховуються лише активні правила нечіткого виведення.

Акумуляція висновків нечітких правил виведення. Здійснюється для об'єднання нечітких множин, що відповідають терм під заключень, що належать до тих самих вихідних лінгвістичних змінних.

Дефаззифікація вихідних перемінних. Традиційно використовується метод центра тяжкості в формі (4.8)-(4.9) чи метод центра площі (4.10) [48,50].

4.3. Оцінка ризику інформаційної безпеки засобами нечіткої логіки

Опис вхідних і вихідних змінних.

Змістовна інтерпретація нечіткої моделі передбачає вибір та специфікацію вхідних та вихідних змінних відповідної системи нечіткого виведення. При цьому в нечіткій моделі передбачається використовувати 7 вхідних змінних та одну вихідну змінну.

Як перша вхідна змінна використовується оцінка цінності інформації та активів, що захищаються, якими володіє організація. Очевидно, чим вища вартість активів та конфіденційної інформації, тим більші збитки внаслідок інциденту у сфері ІБ, а тому ризик вищий.

Як другий вхідний змінної використовується оцінка вразливості автоматизованої системи організації, де зберігається, обробляється, звертається конфіденційна інформація. Оскільки порушник, використовуючи вразливість, реалізує загрозу і завдає шкоди організації. Тому, що вище вразливість системи, то більший ризик ІБ.

В якості третьої вихідної змінної розробляється модель порушника і проводиться оцінка. Згідно, НД ТЗИ 1.1-003-99, рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами АС, наприклад, поділити на чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього [5]:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;
- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;
- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

В якості четвертої вхідної змінної використовується оцінка забезпечення рівня конфіденційності інформації, що захищаються засобами захисту (апаратними, апаратно-програмними, програмними). Чим вищий рівень забезпечення конфіденційності, тим ризик інциденту ІБ нижче.

Як п'ята вхідна змінна використовується оцінка забезпечення рівня цілісності інформації, що захищається засобами захисту (апаратними, апаратно-програмними, програмними). Що рівень забезпечення цілісності, то ризик інциденту ІБ нижче.

Як шостий вхідний змінної використовується оцінка забезпечення рівня доступності інформації засобами захисту (апаратними, апаратно-програмними, програмними). Що рівень забезпечення доступності, то ризик інциденту ІБ нижче.

Практика показує, що в АС, призначених для обробки даних, не для всієї інформації необхідно забезпечення всіх характеристик, наприклад, для відкритої інформації не потрібно забезпечувати конфіденційність, необхідно забезпечити доступність. Тому визначається необхідний набір показників.

Як вихідна змінна використовується оцінка ризику ІБ, яка є основою для прийняття рішення керівництвом організації та служби безпеки щодо забезпечення необхідного рівня безпеки ресурсів та активів підприємства. Даний параметр характеризує ступінь ефективності проведених заходів та реалізованих системою захисту згідно з поставленим завданням. Розрахувавши рівень ризику можуть бути прийняті рішення щодо підвищення або посилення системи захисту, або прийняття залишкового ризику.

Нечітка модель оцінювання ризику інформаційної безпеки.

При побудові нечіткої моделі оцінки ризику ІБ було зроблено припущення про те, що всі змінні, що розглядаються, вимірюються в балах в інтервалі дійсних

чисел від 0 до 10. При цьому найнижча оцінка значення кожної зі змінних є 0, найвищою - 10.

Фаззифікація вхідних та вихідних змінних

Як терм-множини першої вхідної змінної «Актив» використовуватимемо безліч T_1= { низький, середній, високий } з функціями приналежності термів, зображених на рис. 4.3.

Як терм-множини другої вхідної змінної «Вразливість» будемо використовувати безліч T_2= { низька, середня, висока } з функціями приналежності термів, зображених на рис. 4.4.

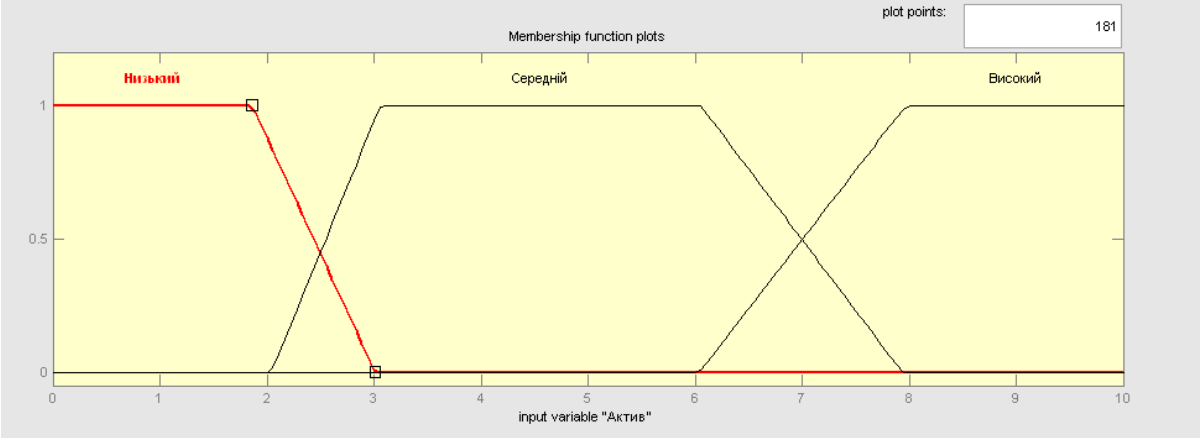

Рис. 4.3. Графік функції приладдя для термо лінгвістичної змінної «Актив»

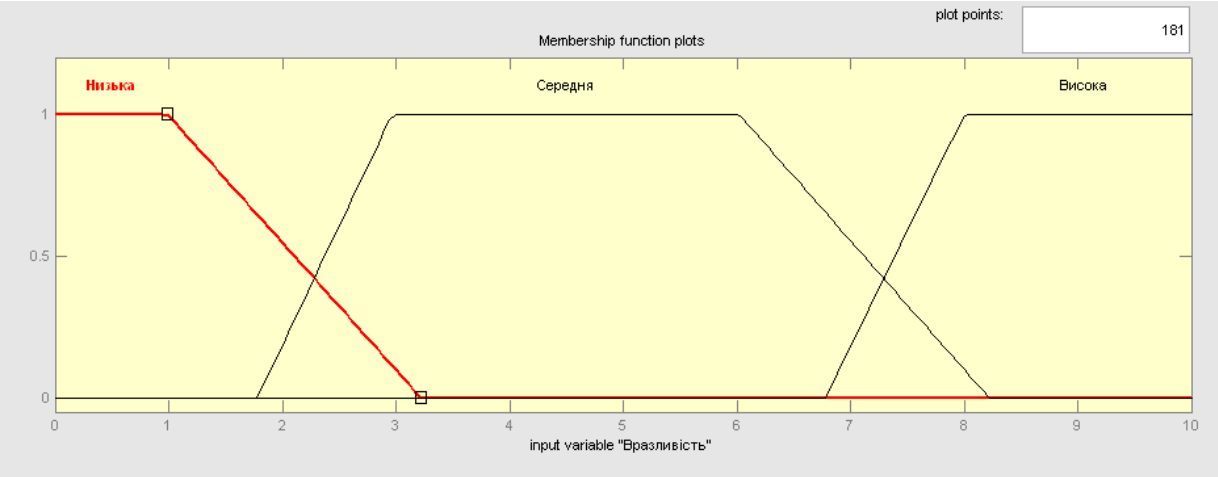

Рис. 4.4. Графік функції приладдя для термо лінгвістичної змінної «Вразливість»

Як терм-множини третин вхідної змінної «Загрози» використовуватимемо безліч T_3= { низькі, середні, високі } з функціями приналежності термів, зображених на рис. 4.5.

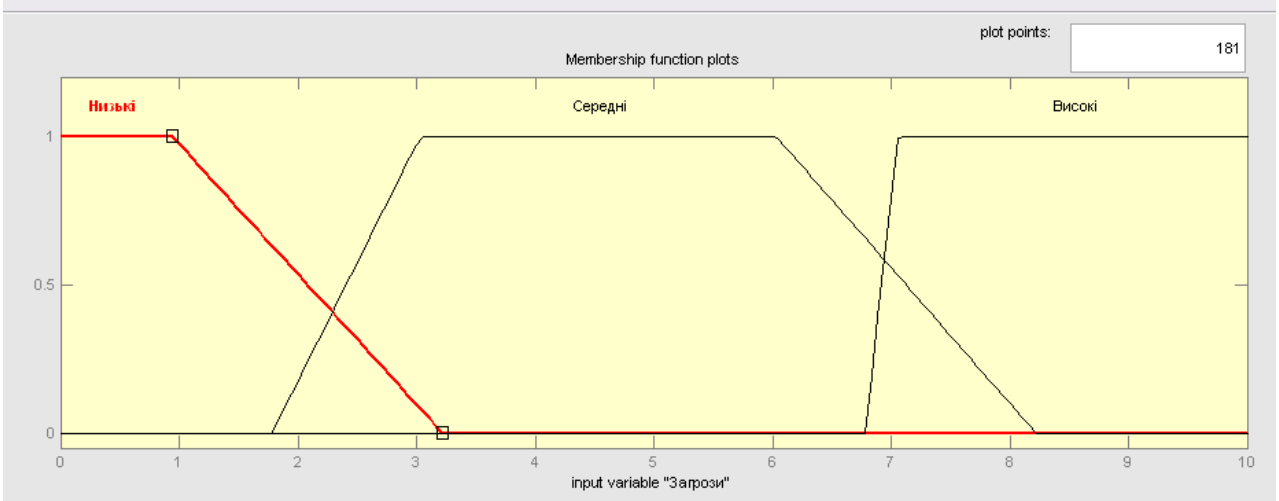

Рис. 4.5. Графік функції приладдя для термо лінгвістичної змінної «Загрози»

Як терм-множини четвертої вхідної змінної «Порушник» використовуватимемо безліч T_4= { низький, середній, високий, дуже високий } з функціями приналежності термів, зображених на рис. 4.6.

Як терм-множини п'ятої вхідної змінної «Конфіденційність» використовуватимемо безліч T_5= { низький, середній, високий } з функціями приналежності термів, зображених на рис. 4.7.

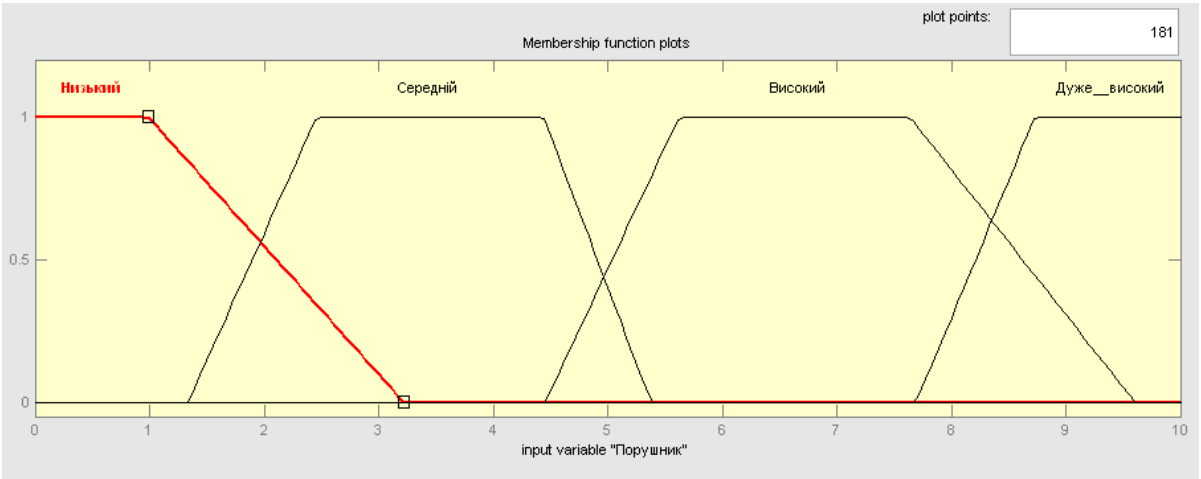

Рис. 4.6. Графік функції приладдя для термо лінгвістичної змінної «Порушник»

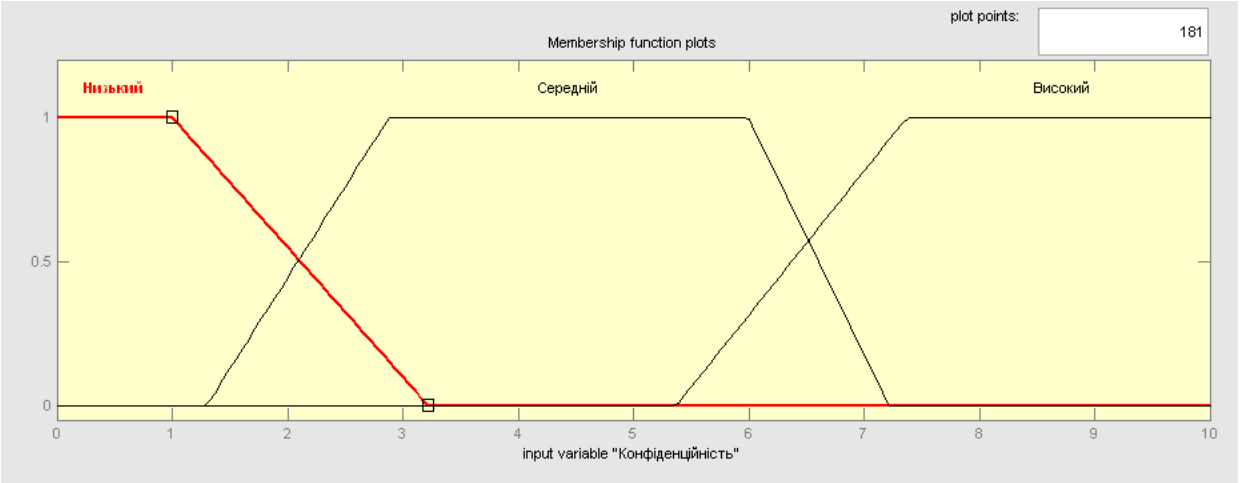

Рис. 4.7. Графік функції приналежності для термо лінгвістичної змінної «Конфіденційність»

Як терм-множини шостої вхідної змінної «Цілісність» використовуватимемо безліч $T_6 =$ { низька, середня, висока } з функціями приналежності термів, зображених на рис. 4.8.

Як терм-множини сьомої вхідної змінної «Доступність» використовуватимемо безліч $T_7 =$ { низька, середня, висока } з функціями приналежності термів, зображених на рис. 4.9.

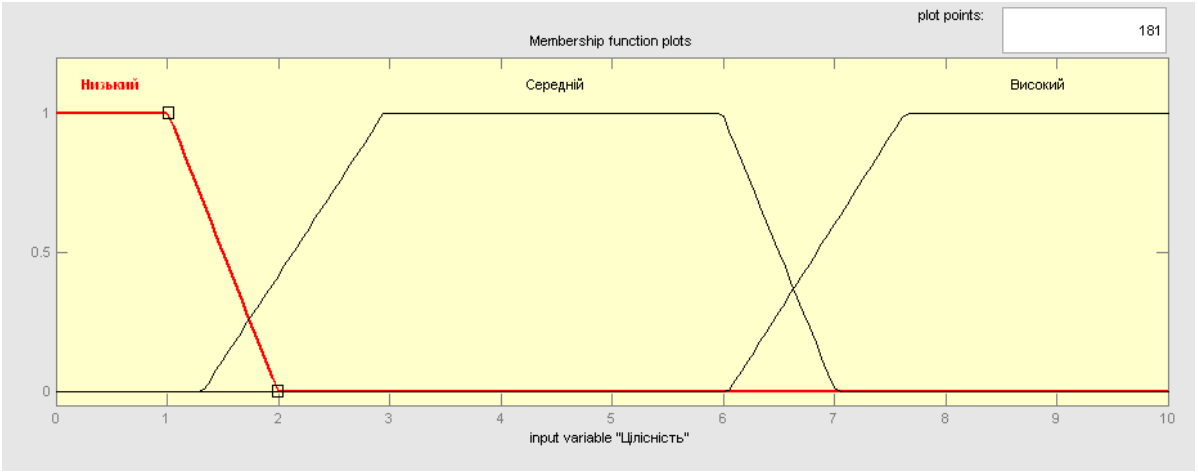

Рис. 4.8. Графік функції приналежності для термо лінгвістичної змінної «Цілісність»

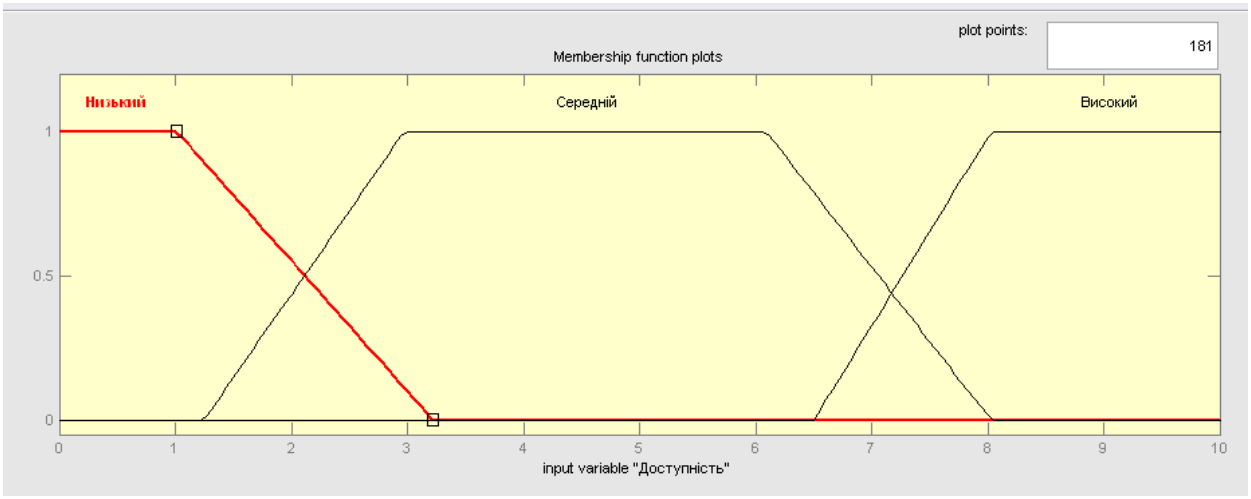

Рис. 4.9. Графік функції приналежності для термо лінгвістичної змінної «Доступність»

Як терм-множини вихідної лінгвістичної змінної «Рівень ризику» використовуватимемо безліч $T_8 =$ { дуже низький, низький, середній, високий, дуже високий } з функціями приналежності термів, зображених на рис. 4.10.

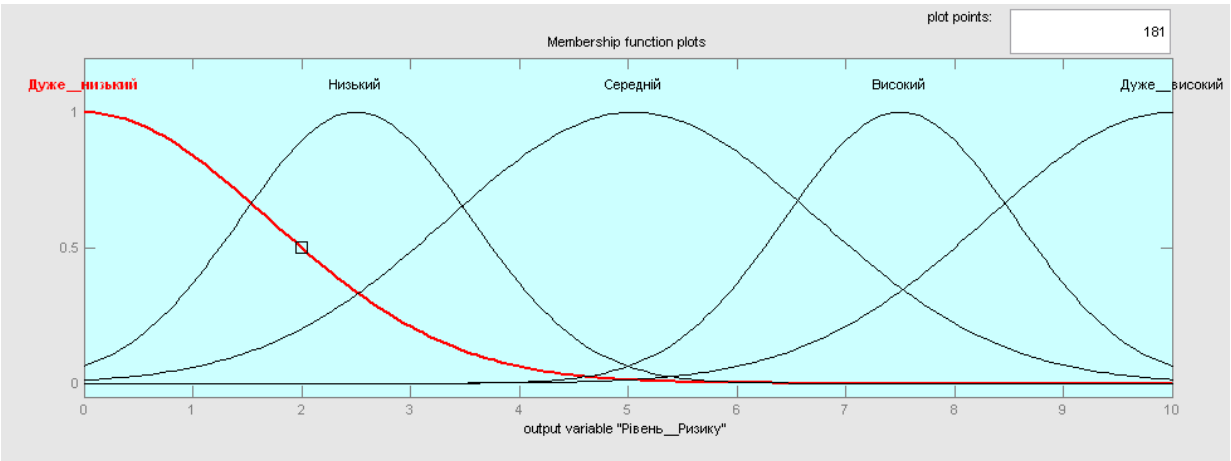

Рис. 4.10. Графік функції приналежності для термо лінгвістичної змінної «Рівень ризику»

Формування бази правил систем нечіткого висновку

Наступним етапом побудови моделі є побудова бази правил. З цією метою використовуємо 60 правил нечіткого виведення вбудованими засобами системи MatLab. Приклад представлено на рис. 4.11.

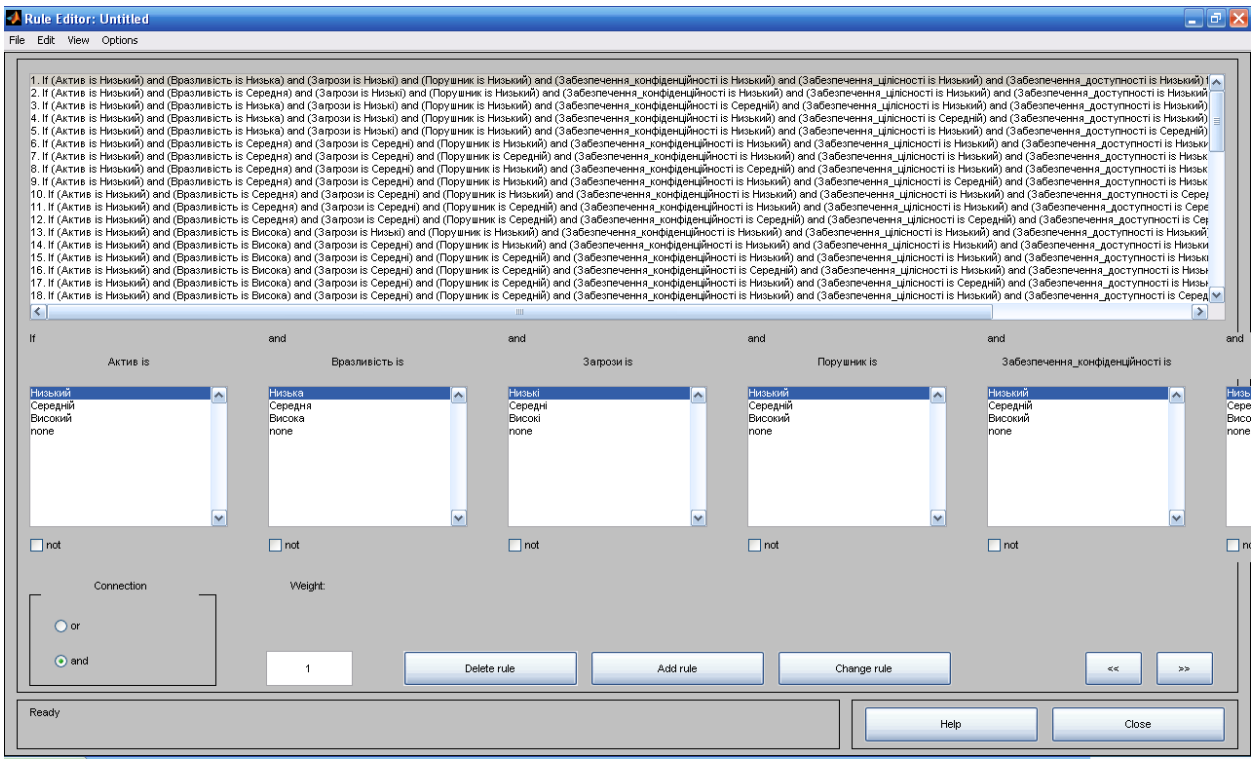

Рис. 4.11. Графічний інтерфейс редактора правил після завдання бази правил системи нечіткого виводу

Як схему нечіткого висновку використовуватимемо метод Мамдані, тому методом активації буде MIN, який розраховується за формулою:

$$\mu_{Q'}(< x_1, x_2, ..., x_k >) = \frac{\mu_Q(< x_1, x_2, ..., x_k >)}{h_Q}. \qquad (4.13)$$

Далі необхідно визначити методи агрегування умов. Оскільки у всіх правилах 1-60 як логічна зв'язка для умов застосовується тільки нечітка кон'юнкція (операція «І»), то як метод агрегування будемо використовувати операцію min-кон'юкції. Для акумуляції висновків правил використовуватимемо метод max-диз'юкції, який також застосовується у разі схеми нечіткого виведення методом Мамдані. Як метод дефазифікації використовуємо метод центру тяжкості (4.9).

Побудова нечіткої моделі засобами Fuzzy Logik Toolbox та аналіз отриманих результатів.

Розробку нечіткої моделі (назвемо mortgage) виконуватимемо з використанням графічних засобів системи MatLab. З цією метою в редакторі Fis

визначимо 7 вхідних змінних з іменами «Актив», «Вразливість» , «Загрози», «Порушник», «Конфіденційність», « Цілісність», «Доступність» та одну вихідну змінну «Рівень ризику». Вигляд графічного інтерфейсу редактора Fis цих змінних зображений на рис. 4.12.

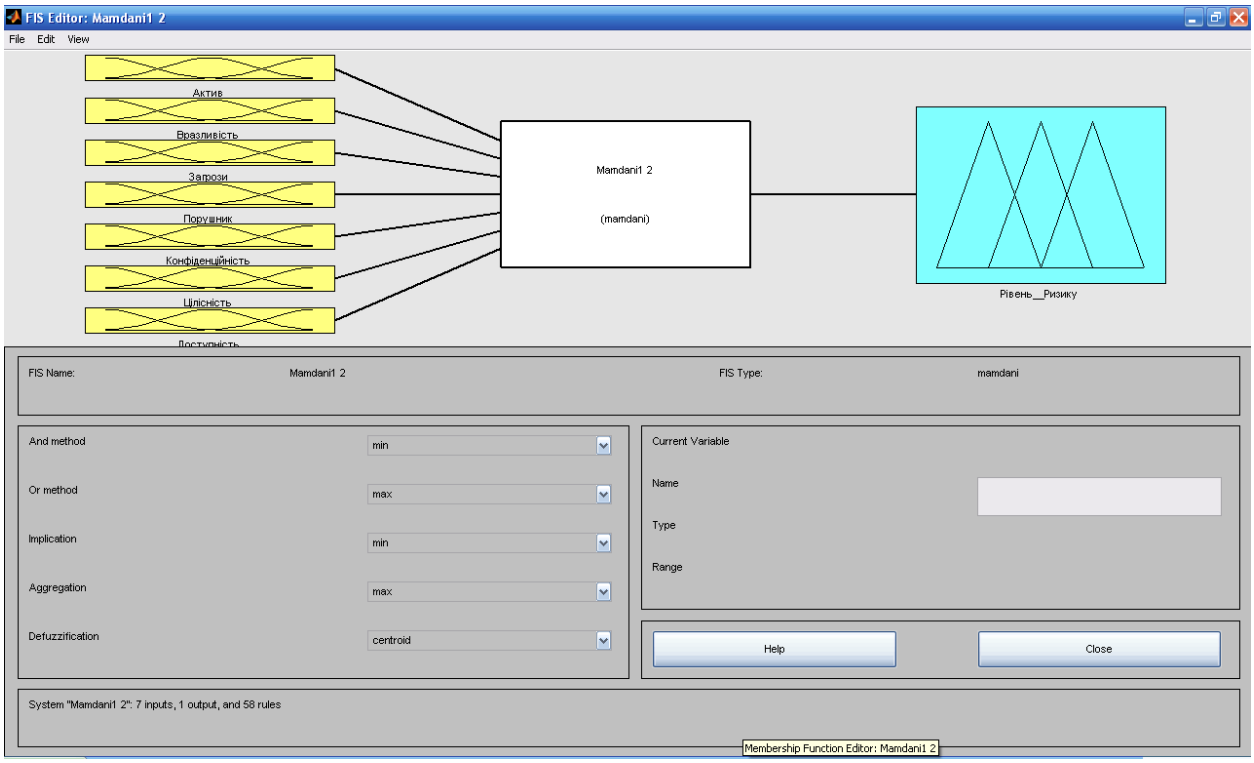

Рис.. 4.12. Графічний інтерфейс редактора Fis після визначення вхідних та вихідних змінних системи нечіткого виводу

Для вирішення поставленої задачі нечіткого моделювання використовуватимемо систему нечіткого виведення типу Мамдамі. Залишимо без зміни параметри нечіткої моделі, запропонованої системою MatLab за умовчанням, а саме, логічні операції ($\min$ – для нечіткого логічного І, $\max$ – для нечіткого логічного АБО), метод імплікації ($\min$), метод агрегування ($\max$) і метод дефазифікації (centroid).

Далі визначаємо функції належності термів для кожної з 7 вхідних і єдиної вихідний змінних аналізованої системи нечіткого виведення. З цією метою скористаємося редактором функцій належності системи MatLab. Будемо використовувати типи функцій приналежності для відповідні чисельні значення

їх параметрів, які зображені на рис. 4.3-4.9. Графічний інтерфейс редактора функцій належності вихідної змінної «Рівень ризику» зображено на рис. 4.13.

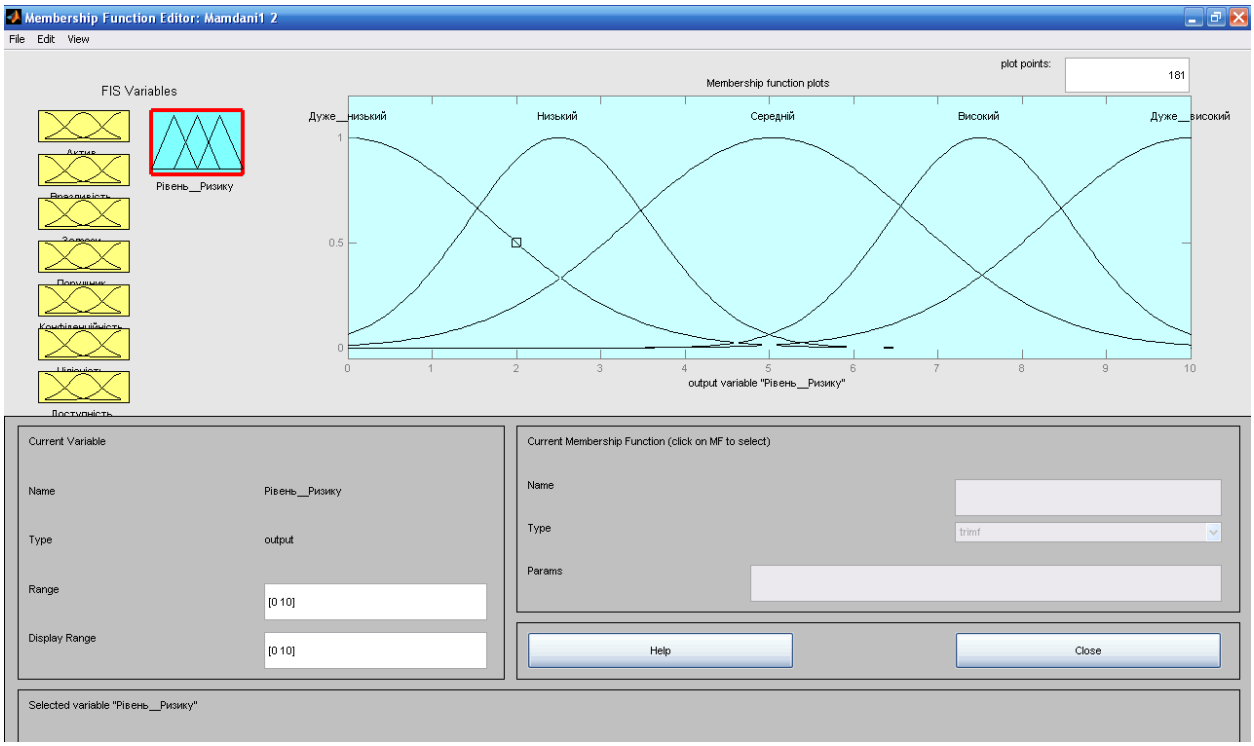

Рис.. 4.13. Графічний інтерфейс редактора функцій приладдя для вихідної змінної «Рівень ризику»

Далі поставимо 60 правил для системи нечіткого висновку, що розробляється. З цією метою використовуємо редактор правил MatLab. Вигляд графічного інтерфейсу редактора правил після завдання 60 правил нечіткого виводу зображено на рис. 4.11.

Виконуємо аналіз побудованої системи нечіткого висновку для аналізованого завдання оцінки рівня ризику ІБ організації. З цією метою відкриваємо вікно перегляду правил системи MatLab і вводимо значення вхідних змінних для окремого випадку, коли значення вхідної змінної «Актив» оцінюється в 3 бали, значення вхідної змінної «Вразливість» оцінюється в 7 балів, значення вхідної змінної «Загроза» оцінюється в 8 балів , значення вхідної змінної «Порушник» оцінюється у 8 балів, значення вхідної змінної «Конфіденційність » оцінюється у 3 бали, значення вхідної змінної «Цілісність»

оцінюється в 5 балів , значення вхідної змінної «Доступність» оцінюється у 3 бали. Процедура нечіткого висновку, виконана системою MatLab для розробленої нечіткої моделі, розраховує значення вихідної змінної «Рівень ризику» дорівнює 7,44 бали (рис. 4.14). Це досить високий рівень ризику ІБ, при якому можливе завдання шкоди організації і є підставою для перегляду керівником служби безпеки системи захисту.

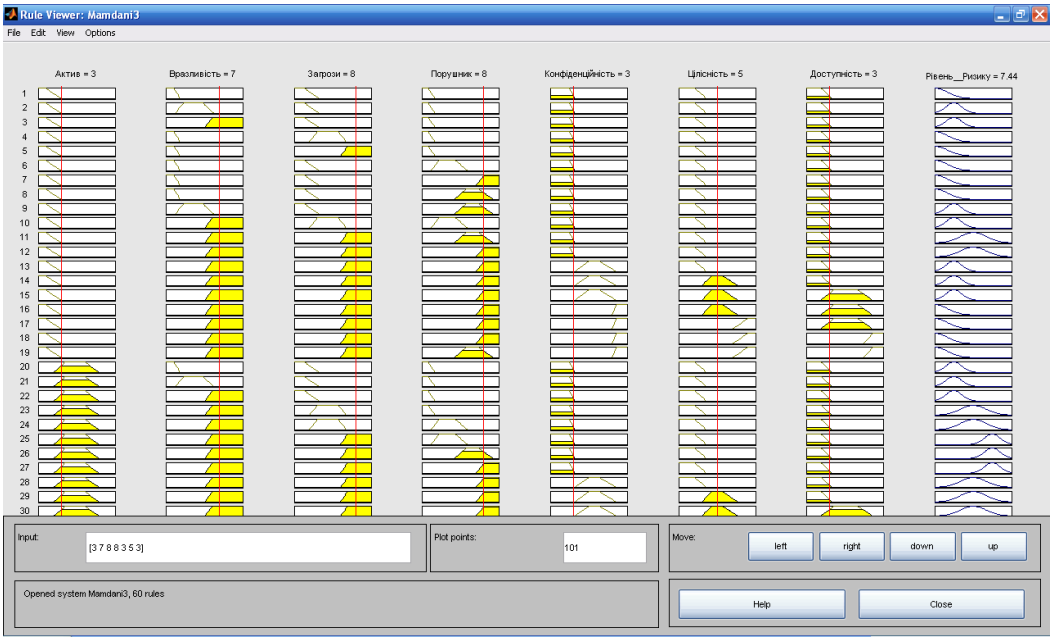

Рис. 4.14. Графічний інтерфейс програми перегляду правил після виконання процедури нечіткого виведення для першого варіанта значень вхідних змінних

Далі виконаємо аналіз побудованої системи нечіткого висновку другого варіанта вихідних даних. З цією метою змінимо значення вхідних змінних: значення вхідної змінної «Актив» оцінюється в 5 балів, значення вхідної змінної «Вразливість» оцінюється в 3 бали, значення вхідної змінної «Загроза» оцінюється в 7 балів, значення вхідної змінної «Порушник» оцінюється у 2 бали, значення вхідної змінної «Конфіденційність» оцінюється у 8 балів, значення вхідної змінної «Цілісність» оцінюється у 6 балів, значення вхідної змінної «Доступність» оцінюється в 9 балів.

Процедура нечіткого висновку, виконана системою MatLab, видає в результаті значення вихідної змінної «Рівень ризику», що дорівнює 5 балам (рис. 4.15).

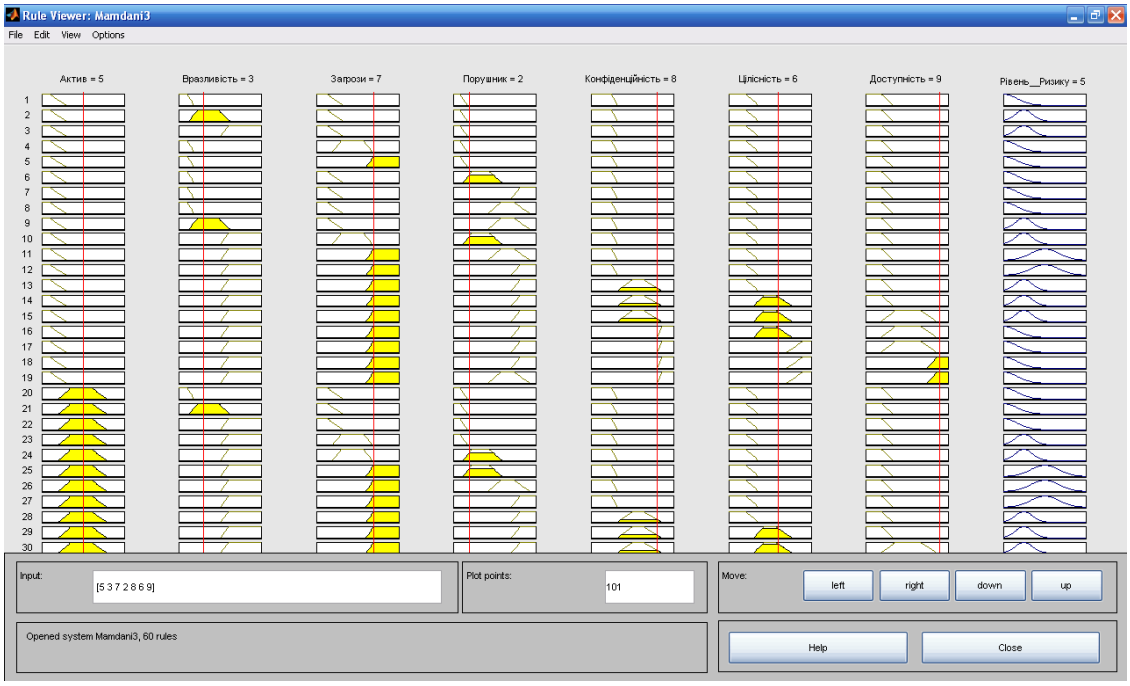

Рис. 4.15. Графічний інтерфейс програми перегляду правил після виконання процедури нечіткого виведення для другого варіанта значень вхідних змінних

4.4. Висновок до розділу 4

В розділі описані основні етапи нечіткого виведення відповідно до основних положень нечіткої логіки. Детально розглянутий алгоритм Мамдані нечіткого висновку. Запропоновано використовувати 7 вхідних змінних та одну вихідну змінну в нечіткій моделі. Проведена фаззифікація вхідних змінних: актив, вразливість, загрози, порушник, конфіденційність, цілісність, доступність та вихідної змінної – рівень ризику.

Сформовані бази правил системи. Використовується 60 правил нечіткого виведення вбудованими засобами системи MatLab. Для розрахунку ризику ІБ нечіткого моделювання використовуватимемо систему нечіткого виведення типу Мамдамі.

ВИСНОВОК

В роботі було проведено огляд нормативно-правової бази у сфері захисту інформації. Досліджено методології проведення оцінювання ризику ІБ. Проаналізовано програмне забезпечення, яке використовується для оцінки ризику. Виявлено недоліки та обмеження та визначений методологічний базис нечітких множин для оцінки ризику та проведена оцінка ризику засобами нечіткої логіки із використанням програмного забезпечення MatLab.

В першому розділі був проведений загальний огляд нормативних документів України про захист інформації. Були розглянуті міжнародні стандарти у сфері управління ризиками інформаційної безпеки. Також була розглянута система управління інформаційними ризиками.

В другому розділі була проведена ідентифікація та визначення цінності активів. Був проведений аналіз загроз та вразливостей. Був розглянутий процес оцінювання та визначення величин ризиків, шкал і критерій, за якими вони можуть вимірюватись. Також був розглянутий процес обробки ризиків інформаційної безпеки та способи зменшення ризиків. Були описані основні та суб’єктивні фактори, що впливають на рішення про прийняття ризиків.

В третьому розділі були розглянуті методології управління ризиками інформаційної безпеки. Був проаналізований інструментарій базового рівня та засоби повного аналізу ризиків. Були досліджені загальні недоліки та обмеження комерційних програмних продуктів.

В четвертому розділі була розглянута методологія нечіткого моделювання та основні поняття теорії нечітких множин. Були досліджені основні етапи нечіткого виводу. Була сформована база правил систем нечіткого виводу. Також був досліджений алгоритм нечіткого висновку Мамдані (Mamdani). Була проведена Оцінка ризику інформаційної безпеки засобами нечіткої логіки. Проведений опис вхідних і вихідних змінних, побудована нечітка модель оцінювання ризику інформаційної безпеки засобами Fuzzy Logik Toolbox та проведений аналіз отриманих результатів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Закон України «Про інформацію».
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
3. Закон України «Про захист інформації в автоматизованих системах».
4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені постановою Кабінету Міністрів України від 29.03.2006 року № 373
5. Положення про технічний захист інформації в Україні (затверджено Указом Президента України від 27.09.99 року № 1229).
6. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
7. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
9. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
10. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
11. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.
12. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

13. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

14. Стандарт BS 7799.

15. Стандарт ISO/IEC 15408. «Критерії оцінки безпеки інформаційних технологій».

16. Стандарт ISO/IEC 27003:2010 «Інформаційні технології - Методи забезпечення безпеки - посібник з впровадження системи управління інформаційною безпекою».

17. ISO / IEC 27005 «Інформаційні технології. Методи забезпечення безпеки. Менеджмент ризику інформаційної безпеки».

18. Методология анализов рисков в информационных системах. С.В. Симонов. – Конфидент/ январь-февраль 1/2001. С. 72-76.

19. «Common Criteria for Information Technology Security Evolution» (Part 1).

20. Анализ рисков, управление рисками. С.В. Симонов. – Jet Info. – 28 с.

21. В.М. Богуш, О.К. Юдін. Основи інформаційної культури. – Київ, 2003.

22. Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ - Петербург, 2003. – 752 с.

23. Доценко СМ. Аналитические компьютерные технологии и обеспечение безопасности компьютерных сетей // Конфидент. Защита информации. - № 2 - 2000. - С. 45-52.

24. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. -М.: Горячая линия - Телеком, 2000. – 354.

25. Липаев В.В. Стандарты на страже безопасности информационных систем // PC WEEC/RE. - № 30. - 2000.

26. Лобанов А.Ф. Основная модель оценки защиты продуктов и систем информационных технологий в стандарте ISO/IEC 15408 // Безопасность информационных технологий. - № 4. - 1998. - С. 71-75.

27. Медведовский И.Д., Петренко С.А., Нестеров С.А. CD «Руководство по управлению информационными рисками корпоративных информационных систем Internet/Intranet». - Domina Security, 2002.

28. Нестеров С.А., Петренко С.А. Программные средства анализа информационных рисков компании // Экспресс-электроника. - № 10. - 2002. - С. 84-86.

29. Норткат С, Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях: Пер. с англ. - М.: Издательский дом «Вильямс», 2001. – 487 с.

30. Петренко А.А., Петренко С.А. Оцени свой риск // IT Manager. - № 6. - 2002. -С. 42-48.

31. Симонов С.В. Методология анализа рисков в информационных системах // Конфидент. Защита информации. - № 1. - 2001. - С. 72-76.

32. Астахов А. Как управлять рисками информационной безопасности? — IS027000 RU, 2006http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami inlormacionnoi-bezopasnnsti/kak-upravlyai-riskami-informacionnoi bezopasnosti/

33. Астахов А. Особенности обеспечения информационной безопасности промышленных систем. — ISO27000 RU, 2006, http://www.iso27000.ru/ chitalnyi zai/kiberugrozy-i-kiberterrorizm/osobennosti-obespecheniya-informacionnoi-bezopasnosti-promyshlennyh-sistem/

34. Кэтрин Уолш. Хаки, фрики и черви: события, которые изменили безопасность Интернет. - ISO27000 RU, http://www.iso27000.ru/chilalnvi-zai/ kiberugrozy-i-kiberterrorizm/haki-friki-i-chervi-sobytiya-kotorye-izmenili-bezopasnost-inernet.

35. Стандарт BS 7799-3 , «Системи управління інформаційною безпекою. Керування ризиками інформаційної безпеки» https://uk.wikipedia.org/wiki/BS_7799-3

36. A1an Caldcr & Steve Watkins. Information Security Risk Management for ISO 27001/ISO 17799. — IT Governance Publishing, 2007, http://gtrust.ru/show_good.php?idtov=1254.

37. Бібліотека – The ISO 17799 Service & Software Directory http:/Avww.iso 17799software.com.

38. http://www.riskwatch.com - сайт компанії Risk Watch.

39. https://coras.sourceforge.net/.

40. http://ww1.cramm.com/.

41. www.cert.org/octave.

42. http://www.methodware.com - сайт компанії MethodWare.

43. https://riskadvisor.insure/.

44. Зайченко Ю. П. Дослідження операцій / Ю. П. Зайченко. – К. : Слово, 2006. – 688 с.

45. Кондратенко Ю. П. Методи обробки нечіткої лінгвістичної інформації в задачах багатокритерійного прийняття рішень / Ю. П. Кондратенко, Є. В. Сіденко // Матер. 6-ї Міжн. наук.-практ. конф. Сучасні інформаційні та інноваційні технології на транспорті MINTT2014. – Херсон, Травень 2014. – С. 161–163.

46. Куссуль Н. М. Інтелектуальні обчислення. Навчальний посібник (навчальний посібник з грифом МОН України) / Н. М. Куссуль, А. Ю. Шелестов, А. М. Лавренюк. – К. : «Наукова думка», 2006. – 186 с.

47. Ямпольський Л. С. Системи штучного інтелекту в плануванні, моделюванні та управлінні / Л. С. Ямпольський, Б. П. Ткач, О. І. Лісовиченко. – Київ : ДП «Видавничий дім «Персонал», 2011. – 544 с.

48. Fuzzy Logic Toolbox. User’s Guide. The MathWorks, Inc., 1999. – 134 p.

49. https://elearning.sumdu.edu.ua/free_content/lectured:5de5178bb62ca7a97fe35cba8b92d1b337ee8101/latest/8080/index.html.

50. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень : навчальний посібник. – Запоріжжя: ЗНТУ, 2008. – 341 с