Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин»

Виконав: студент 2-го курсу, групи 1БС-21м

спеціальності 125 – Кібербезпека

_____ Євгеній ЛИСЕНКО

Керівник: к.т.н., доц., доц. каф. ЗІ

_____ Наталія КОНДРАТЕНКО

Опонент: к.т.н., доц., доц. каф . ПЗ

_____Олекснdр ТКАЧЕНКО

«12» 12 _____2023 р.

Допущено до захисту

Завідувач кафедри ЗІ

д.т.н., проф.

_____Володимир ЛУЖЕЦЬКИЙ

«13» 12 2023 р.

Вінниця – 2023

Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра захисту інформації
Рівень вищої освіти ІІ-й (магістерський)
Галузь знань – 12 Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма – Безпека інформаційних і комунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗІ, д.т.н., проф.
_____ В. А. Лужецький
«19» 09 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
Лисенку Євгенію Максимовичу

1. Тема магістерської кваліфікаційної роботи Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин

Керівник магістерської кваліфікаційної роботи Кондратенко Наталія Романівна, к.ф.-м.н., доц. каф ЗІ, затверджені наказом ректора ВНТУ від 18 вересня 2023 року №247

2. Строк подання студентом роботи 11 грудня 2023 р.
3. Вихідні дані до роботи:
   - дані зібрані з опитувань працівників, вимоги до забезпечення безпеки згідно ISO/IEC 27000;
   - спосіб реалізації – гугл опитування, інтервальна нечітка модель за бальною шкалою, аналіз отриманих результатів, створення рекомендацій згідно результатів.
4. Зміст текстової частини: Вступ. 1. Аналіз предметної області. 2. Побудова нечітких моделей оцінки безпеки. 3. Реалізація експерементальної частини. 4. Економічна частина. Висновки. Список використаних джерел. Додатки.
5. Перелік ілюстративного матеріалу: Схема обробки даних за нечіткою моделю з бальною шкалою (плакат А4). Схема обробки даних за нечіткою моделю з лінгвістичною шкалою (плакат А4). Графічне представлення еталоних нечітких множин (плакат А4). Анкета анонімного оцінювання інформаційної безпеки (плакат А4).

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанти	Підпис, дата	
		завдання видав	виконання прийняв
1	Наталія Кондратенко, к.т.н., доц. каф. ЗІ	19.09	19.09
2	Наталія Кондратенко, к.т.н., доц. каф. ЗІ	19.09	29.09
3	Наталія Кондратенко, к.т.н., доц. каф. ЗІ	19.09	26.11
4	Ольга РАТУШНЯК, к.т.н., доц. каф ЕВПМ	19.09	21.11

7. Дата видачі завдання 01.09.2023 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примі
1	Аналіз завдання. Вступ	01.09.2023 – 10.09.2023	
2	Аналіз літературних джерел за напрямом магістерської кваліфікаційної роботи	10.09.2023 – 15.09.2023	
3	Науково-технічне обґрунтування	16.09.2023 – 22.09.2023	
4	Розробка технічного завдання	23.09.2023 – 29.09.2023	
5	Розробка рішень	30.09.2023 – 12.10.2023	
6	Практична реалізація, моделювання, експериментування, результати	14.10.2023 – 10.11.2023	
7	Розробка розділу економічного обґрунтування доцільності розробки	11.11.23 – 17.11.2023	
8	Аналіз виконання ТЗ, висновки	18.11.2023 – 24.11.2023	
9	Оформлення пояснювальної записки	25.11.2023 – 30.11.2023	
10	Попередній захист та доопрацювання МКР	28.11.2023 – 01.12.2023	
11	Перевірка магістерської роботи на наявність плагіату	02.12.2023 – 10.12.2023	
12	Представлення МКР до захисту	11.12.2023 – 14.12.2023	
13	Захист МКР	14.12.2023 – 21.12.2023	

Студент _____ Євгеній ЛИСЕНКО
(підпис)

Керівник роботи _____ Наталія КОНДРАТЕНКО

АНОТАЦІЯ

Магістерська робота присвячена вивченню моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин.

У першому розділі проведено аналіз предметної області, визначено ключові проблеми та виклики, пов'язані з безпекою інформації в умовах сучасного інформаційного суспільства.

Другий розділ присвячено детальному опису розроблених моделей оцінювання безпеки за допомогою інтервальних нечітких множин. В рамках цього розділу розглянуті дві основні шкали: бальна та інгвістична. Впровадження нечіткості в оцінювання безпеки дозволяє більш точно враховувати неоднозначність та невизначеність в оцінках безпеки інформації.

Третій розділ базується на результатів опитування користувачів, в якому аналізується їхнє сприйняття рівня безпеки. З використанням інтервальної моделі оцінки безпеки, розробленої у попередньому розділі, обчислено рівень безпеки за бальною шкалою. На основі цього проведено формулювання рекомендацій для підвищення рівня безпеки інформації в організації.

У четвертому розділі досліджено економічний аспект впровадження запропонованих моделей. Визначено витрати, пов'язані з реалізацією та підтримкою системи безпеки, що є важливим кроком для прийняття обґрунтованих рішень та ефективного управління ресурсами.

ABSTRACT

The master's thesis is devoted to the study of a model for assessing the level of information security using interval fuzzy sets.

The first chapter analyzes the subject area, identifies key problems and challenges related to information security in the modern information society.

The second section is devoted to a detailed description of the developed risk assessment models using interval fuzzy sets. Within this section, two main scales are considered: scoring and inguistic. The introduction of fuzziness in risk assessment allows for a more accurate accounting of ambiguity and uncertainty in information security assessments.

The third section is based on the results of a user survey that analyzes their perception of the level of security. Using the interval risk assessment model developed in the previous section, the security level is calculated on a point scale. Based on this, recommendations for improving the level of information security in an organization are formulated.

Section 4 examines the economic aspect of implementing the proposed models. The costs associated with the implementation and maintenance of the security system are determined, which is an important step for making informed decisions and effective resource management.

ЗМІСТ

ВСТУП

Актуальність теми. З високою швидкістю розвитку інформаційних технологій та зростання кількості цифрових загроз, питання забезпечення безпеки інформації набуває особливої актуальності. Сучасні комп'ютерні системи є складними екосистемами, в яких інформаційні ресурси переплітаються з технічними та технологічними аспектами. У цьому контексті, оцінювання рівня безпеки інформації стає стратегічно важливим завданням для організацій та підприємств. Актуальність теми визначається не лише зростанням кількості кіберзагроз, але й недоліками традиційних методів оцінювання безпеки. Традиційні математичні моделі часто не здатні врахувати нечіткість та невизначеність в контексті безпеки інформації. У цьому контексті, розробка нових підходів до оцінювання рівня безпеки, таких як використання інтервальних нечітких множин, стає необхідністю.

Метою цієї роботи є розширення можливостей для оцінювання рівня безпеки інформації в умовах недо визначених вхідних даних за рахунок використання інтервальних нечітких множин.

Завданнями дипломної роботи є:

- Аналіз предметної області;
- Побудова нечітких моделей оцінки рівня безпеки;
- Реалізація експеременьальної частини.

Об’єктом дослідження є процес оцінювання рівня безпеки інформації в умовах недо визначених вхідних даних

Предметом дослідження є моделі оцінювання рівня безпеки інформації на нечітких множин.

Практичне значення одержаних результатів. покращення стратегій управління ризиками та забезпечення більш ефективного захисту інформаційних активів в умовах сучасного цифрового середовища. Враховуючи величезне значення інформації у всіх сферах життя, висвітлення цих аспектів набуває особливого значення в сучасному інформаційному суспільстві.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Основні характеристики безпеки

Проблематика забезпечення безпеки інформації в комп'ютерних системах є різновіковою і набуває належної актуальності у зв'язку з постійним розвитком інформаційних технологій та широким поширенням комп'ютерних систем і мереж у всіх сферах суспільства. На сучасному етапі сформувалася сильна індустрія безпеки, що об'єднує наукові та виробничі напрями, і спрямована на розв'язання ключових проблем безпеки, які можна класифікувати у три основні групи [5]:

- фізичні (пов'язані здебільшого з об'єктивними чинниками);
- логічні (пов'язані з суб'єктивними факторами);
- соціальні.

З фізичною безпекою пов'язані питання захисту від стихійних лих, таких як: пожежа, землетруси, затоплення, урагани, вибухи промислових хімічних речовин, різна магнітні поля, збої устаткування, гризуни тощо.

Логічна безпека відображає питання захисту від несанкціонованого доступу, помилок у діях персоналу та програм, які негативно впливають на інформацію тощо.

До соціальної безпеки входять різні заходи з юридичного, організаційного та адміністративного захисту, а також питання, пов'язані з підготовкою кадрів, вихованням та спрямованими на формування конкретних норм поведінки та етичних стандартів. Сюди входять також обов'язки осіб, які взаємодіють у сфері інформаційних процесів та інші аспекти, пов'язані з обабічними взаємодіями в інформаційному середовищі. [4].

До базових характеристик безпеки інформації відносять:

- конфіденційність (Confidential),
- цілісність (Integrity)
- доступність (Accessibility).

Конфеденційність - характеристика безпеки інформації, яка відображає її властивість нерозкритості та доступності без відповідних повноважень.

По суті, інформація не може бути доступною або розкритою несанкціонованій стороні, тобто для неї вона нібито не існує. З іншого боку, авторизована сторона (наприклад, обслуговуючий персонал, користувачі, програми тощо), яка отримала відповідні повноваження, має повний доступ до інформації.

Цілісність - це характеристика безпеки інформації, що виражає її властивість протистояти несанкціонованій модифікації. Наприклад, користувач, який зберігає інформацію, може розраховувати на те, що вміст його файлів залишиться незмінним, незважаючи на спрямовані атаки або відмову програмних або апаратних засобів. За цією характеристикою інформація залишається непошкодженою від будь-яких спроб несанкціонованого впливу.

Доступність - це характеристика безпеки інформації, яка визначає її здатність бути використаною у заданий момент часу з використанням відповідних ресурсів та відповідно до наданих повноважень. По суті, авторизована сторона за необхідності отримує необмежений доступ до необхідної інформації.

Загалом ці атрибути можна застосовувати для відображення вказаних властивостей не лише окремих систем, але й будь-яких складових комп'ютерних систем, під якими розуміють сукупності програмних засобів, апаратури, рівні фізичні носії інформації, дані та обслуговуючий персонал.

Рівень безпеки інформації, основних її характеристик, напряму залежить від того, наскільки ефективно реалізується та чи інша загроза. Загроза в даному контексті означає потенційну можливість порушення безпеки. При створенні складних систем захисту проведення аналізу загроз є важливим етапом. На цьому етапі формується найповніша множина загроз з урахуванням фактора ризику та їхніх властивостей. Ґрунтуючись на публікаціях зарубіжних авторів класифікацію загроз можна виконати за такими базовими ознаками[7]:

Вплив на характеристики безпеки інформації може бути розглянутий через різні типи загроз:

- Тип "К" впливає на конфіденційність;
- Тип "Ц" викликає загрозу цілісності;
- Тип "Д" стосується доступності;
- Тип "КЦ" об'єднує загрози конфіденційності та цілісності;
- Тип "КД" включає загрози конфіденційності та доступності;
- Тип "ЦД" враховує загрози цілісності та доступності;
- Тип "КЦД" охоплює загрози конфіденційності, цілісності та доступності.

За природою джерела:

- Об'єктивна загроза виникає незалежно від прямого впливу людини і пов'язана з різноманітними природними явищами, такими як пожежі, блискавки, землетруси, радіоактивне випромінювання, напади гризунів та інші стихійні події.
- Суб'єктивна загроза, навпаки, виникає в результаті діяльності людини. Залежно від характеру, суб'єктивну загрозу можна розділити на активну, яка передбачає активну діяльність людини, та пасивну, що виникає без прямої участі людини у процесі виникнення загрози.

Суб'єктивну загрозу, своєю чергою, за мотивом поділяють на активну і пасивну. Активна – діяльність людини, направлена на отримання вигоди, а пасивна містить укванну складову і пов'язана з помилками людини, недбалістю, проєктно-технологічними недоліками в програмному або апаратному забезпеченні тощо.

Також передбачено допоміжні класифікаційні ознаки (до прикладу, частота появи загрози, наслідками її реалізації, можливістю виявлення та запобігання тощо), що допоможуть формалізувати перебіг ідентифікації та аналізу загроз і підвищити ефективність процесу побудови систем ЗІ.

1.2 Класифікація систем захисту

Галузь новітніх інструментів для забезпечення безпеки інформації (ЗЗІ) характеризується широким спектром доступних засобів. З практичної точки зору, ці засоби можна класифікувати на декілька категорій, таких як апаратні, програмні, програмно-апаратні, криптографічні, стеганографічні, організаційні, законодавчі та морально-етичні.

Фізичні засоби безпеки - це різноманітні пристрої і системи, які можуть бути механічними, електричними, електромеханічними, електронними тощо. Серед таких пристроїв можна виокремити джерела безперебійного живлення, криптографічні обчислювачі, процесори систем безпеки інформації (СБІС), електронні ідентифікатори та ключі, пристрої для виявлення шпигунського програмного забезпечення, генератори шуму, що можуть працювати автономно, а також вбудовуватися або з'єднуватися з іншим обладнанням для блокування впливу дестабілізуючих факторів та вирішення інших завдань забезпечення інформаційної безпеки[3].

Програмні засоби безпеки - це спеціальні програми, такі як антивіруси, інструменти для шифрування даних, які використовують алгоритми цифрового підпису, реалізують механізми розподілу доступу, проводять оцінку ризиків, визначають рівень безпеки, а також використовуються для проведення експертиз та вирішення інших завдань забезпечення інформаційної безпеки. Ці програми діють в межах комп'ютерних систем з метою вирішення завдань забезпечення інформаційної безпеки.

Програмно-апаратні засоби - взаємопов'язані апаратні та програмні засоби (наприклад, банківські системи захисту електронних платежів, комплексні системи конфіденційного зв'язку) зв'язку, автоматизовані системи контролю доступу персоналу і транспортних засобів у режимних зонах тощо), що функціонують автономно або у складі інших систем з метою вирішення завдань ЗІ.

Криптографічні засоби є інструментами для забезпечення інформаційної безпеки, використовуючи криптографічне перетворення інформації, таке як шифрування та дешифрування. Це відбувається за допомогою асиметричних або симетричних криптографічних систем. Асиметричні системи ґрунтуються на використанні криптографії з відкритим ключем, яка реалізована, наприклад, у системах Діффі-Хеллмана, RSA та Ель-Гамаля[3]. З іншого боку, симетричні криптографічні системи базуються на використанні криптографії з секретним ключем, представленою, наприклад, у системах DES, ГОСТ і інших.

Практичне використання сучасних засобів криптографії тісно пов'язане із фундаментальними дослідженнями у цій області та здійснюється за допомогою відповідних апаратних, програмних та апаратно-програмних рішень, які побудовані на основі цих досліджень. До цього класу засобів входять, наприклад, системи Криптон, Тессера, Кліппер та інші. Важливо відзначити, що криптоаналіз тісно пов'язаний з цими засобами і ефективно використовується для перевірки надійності криптографічних систем.

Останнім часом стеганографічні методи активно еволюють. Стеганографія, яка включає в себе техніку приховування інформації так, що сам факт її наявності залишається непомітним, розвивається інтенсивно. Наприклад, використання методів, які дозволяють приховати дані у звукових чи графічних файлах, що входять до складу операційної системи Windows 95, набуває популярності. Однак, на державному рівні, ці методи стеганографії ще не отримали широкого практичного застосування.

Органоорганізаційні засоби - організаційно-технічні та органоорганізаційно-правові заходи (наприклад, організація розроблення та використання систем ЗІ, контроль за знищенням носіїв та інформації). Останнім часом стеганографічні методи активно еволюють. Стеганографія, яка включає в себе техніку приховування інформації так, що сам факт її наявності залишається непомітним, розвивається інтенсивно. Наприклад, використання методів, які дозволяють приховати дані у звукових чи графічних файлах, що входять до складу операційної системи Windows 95, набуває

популярності. Однак, на державному рівні, ці методи стеганографії ще не отримали широкого практичного застосування.

Можна припустити, що основними методами створення організаційних засобів є неформальні та евристичні підходи. Законодавчі інструменти, які включають нормативно-правові акти, такі як конвенції, закони, укази, постанови, нормативні документи та інші, призначені для надання юридичної підтримки для вирішення завдань забезпечення інформаційної безпеки. Наприклад, ефективним засобом захисту від несанкціонованого копіювання програмного забезпечення може бути відповідний закон, який регулює захист авторських прав.

Узагальнено визначаються права, обов'язки і відповідальність у взаємодії з інформацією за допомогою законодавчих засобів, і порушення цих норм може впливати на рівень захисту інформації. В світовій практиці відомі різноманітні закони та правові акти, такі як патентне та авторське право, національні закони про державну таємницю, правила обробки інформації в комп'ютерних системах, ліцензування, страхування, сертифікація, класифікаційні нормативні документи і т. д.

Морально-етичні засоби охоплюють моральні норми та етичні правила, що утворилися в суспільстві, колективі та серед об'єктів інформаційної діяльності, наприклад, у спільноті BBS (Bulletin Board System). Порушення цих норм вважається несуплікуванням із загальноприйнятими дисциплінарними правилами та професійними ідеалами. Прикладом таких морально-етичних засобів може бути кодекс професійної поведінки, етикет, або етичні принципи хакерів.

1.3 Стандарти інформаційної безпеки

В умовах стрімкого розширення комп'ютеризації в усіх сферах суспільства та для забезпечення надійної інформаційної безпеки в кіберпросторі виникла необхідність створення однієї вседостатньої системи

стандартів інформаційної безпеки. Ця система має гарантувати ефективність та універсальність, враховуючи відсутність на той момент єдиної теорії захищених систем, особливо універсальної для застосування в різних сферах, як у державному, так і в комерційному секторі[2]. Враховуючи широкий спектр викликів, які виникають у зв'язку з швидким впровадженням комп'ютерних технологій, важливо мати єдиний стандарт, що регулює питання інформаційної безпеки. Такий стандарт повинен бути гнучким і адаптованим до різних галузей та секторів, забезпечуючи високий рівень захисту як для державних структур, так і для комерційних підприємств. Перед вченими і фахівцями стоїть завдання розробити систему, яка не лише враховує сучасні технологічні виклики, але і має стійку архітектуру для майбутнього розвитку.

Однак, незважаючи на необхідність стандартів інформаційної безпеки, важливо також зрозуміти, що цей процес не є простим завданням і вимагає узгодженого підходу з урахуванням різноманітних потреб різних сфер та ринків. Розробка такої системи має базуватися на глибокому розумінні принципів безпеки, технологічних тенденцій та викликів, що постають перед інформаційним суспільством. Оскільки інформаційна безпека стає ключовим аспектом в умовах цифрової трансформації, розробка і впровадження таких стандартів стає актуальним завданням для глобальної інформаційної спільноти. Використання єдиної системи стандартів сприятиме створенню єдиної теорії захищених систем та підвищить загальний рівень інформаційної безпеки в сучасному світі.

Так, в період становлення інформаційної безпеки перші значущі внески в цю сферу здійснювалися через активну участь окремих національних та міжнародних форумів, зокрема, стоунфордських консорціумів, які фокусувалися на дослідженні питань інформаційної безпеки та розробці політики у 1990-х роках. Однак на сучасному етапі цей процес отримав новий імпульс завдяки спільним ініціативам Міжнародної організації зі стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC).

Міжнародна співпраця в області інформаційних технологій вибудована на основі спільного технічного комітету ISO/IEC JTC1, який був спеціально створений для координації та розробки міжнародних стандартів інформаційної безпеки. Основною місією цього комітету є визначення інтернаціональних норм та вимог, спрямованих на ефективне забезпечення інформаційної безпеки в різних сферах діяльності.

Такий спільний підхід до розробки стандартів інформаційної безпеки визнається ефективним механізмом, сприяючим створенню єдиної міжнародної системи, яка має високий ступінь узгодженості та широкий застосування. Організації ISO і IEC виконують ключову роль у забезпеченні консолідації зусиль світової спільноти для вирішення проблем інформаційної безпеки, створюючи фундаментальні стандарти, які визначають високі стандарти ефективності та надійності в цьому важливому аспекті сучасного світу.

Стандарти, розроблені для забезпечення захисту інформації в кіберпросторі, виступають як неоціненний орієнтир у справі кібербезпеки. У цифровому світі, як сучасному інформаційному просторі, де технології швидко розвиваються, система кібербезпеки, побудована на основі міжнародних стандартів інформаційної безпеки, виявляється вельми суттєвою. Ключовою складовою цієї системи є система управління інформаційною безпекою (СУІБ)[8], яка, в свою чергу, входить у склад основних категорій в цій сфері. Система управління інформаційною безпекою (СУІБ) є інтегральною частиною загальної системи управління, яка використовує підхід, що рахує бізнес-ризи та враховує їх в контексті інформаційної безпеки. Завдяки такому підходу, СУІБ охоплює в собі весь цикл дій: розроблення, впровадження, функціонування, моніторинг, перегляд, підтримку та постійне вдосконалення інформаційної безпеки (ІБ). Важливо відзначити, що ІБ включає три основні компоненти: конфіденційність, доступність і цілісність. Таким чином, використання стандартів у сфері інформаційної безпеки, особливо в контексті системи управління

інформаційною безпекою, визначає вагомий внесок у забезпечення ефективності та надійності захисту інформації в сучасному цифровому вимірі.

У щоденному тлумаченні інформаційна безпека (ІБ) розглядається як гарантована захищеність інформації та супутньої інфраструктури від випадкових або умисних впливів природного чи штучного характеру, спрямованих на завдання шкоди власникам або користувачам інформації та відповідної інфраструктурі. Однак, у більш глибокому розумінні, інформаційна безпека визначає стан захищеності ключових інтересів людини, суспільства та держави.

Цей стан передбачає попередження можливої шкоди через: неповноту, невчасність та невірогідність використаної інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформації. Враховуючи різноманіття аспектів, ІБ стає важливим елементом у врегулюванні взаємодії між особою, суспільством та державою. Забезпечення високого рівня інформаційної безпеки означає захист не лише самої інформації, а й життєво важливих інтересів, які можуть бути піддані небезпеці внаслідок різноманітних факторів. Такий підхід відображає значущість інформаційної безпеки у сучасному світі, де технології та обмін інформацією стають невід'ємною частиною життєдіяльності.

Так, ІБ забезпечується застосуванням та управлінням відповідними заходами забезпечення безпеки, які охоплюють широкий діапазон загроз з метою гарантування стійкого успіху бізнесу і мінімізації впливу інцидентів інформаційної безпеки. Таким чином, інформаційна безпека досягається за допомогою виконання відповідного набору засобів управління, сформованого в ході обраного процесу менеджменту ризику і керованого через СУІБ, включаючи політики, процеси, процедури, організаційні структури, програмне та технічне забезпечення для захисту виявлених інформаційних активів. Ці засоби управління повинні бути визначені, впроваджені, а також

контролюватися, аналізуватися і поліпшуватися, щоб гарантувати досягнення встановленого рівня інформаційної безпеки і бізнес-цілей.

Родина міжнародних стандартів управління безпекою інформації серії ISO/IEC 27000 активно розширює свій функціонал з метою ефективного забезпечення інформаційної безпеки в організаціях. Ця родина включає низку стандартів, які встановлюють вимоги до систем управління інформаційною безпекою (СУІБ), систему управління ризиками, метрики та критерії вимірювання ефективності контрольних механізмів, а також надає керівництво з впровадження. Стандарти СУІБ охоплюють такі аспекти:

1. Визначення вимог до СУІБ[9]: Стандарти визначають необхідні вимоги до систем управління інформаційною безпекою, а також стосовно сертифікації таких систем. Це сприяє створенню стійких та ефективних механізмів захисту інформації в організаціях.
2. Підтримка та деталізація: Стандарти забезпечують безпосередню підтримку, включаючи деталізовані рекомендації та/або інтерпретацію процесів розробки, впровадження, забезпечення працездатності та постійного вдосконалення СУІБ. Це дозволяє організаціям ефективно впроваджувати та підтримувати системи інформаційної безпеки.
3. Керівництво для різних галузей: Стандарти включають керівництва з управління інформаційною безпекою для конкретних галузей, що сприяє налагодженню та оптимізації заходів захисту, враховуючи специфіку кожного сектора.
4. Вказівки з оцінки відповідності: Стандарти містять вказівки з оцінки відповідності для систем управління інформаційною безпекою. Це дозволяє оцінювати ефективність та відповідність заходів інформаційного захисту.

Важливо зазначити, що терміни та визначення, використовувані в цій серії стандартів, включають найбільш вживані терміни та визначення в галузі

систем управління інформаційною безпекою. Вони не охоплюють всіх термінів та визначень, які використовуються в сфері СУІБ, а також не обмежують можливість серії стандартів визначати нові терміни.

Міжнародна стандартизація в області інформаційної безпеки (ІБ) включає в себе ряд стандартів, які умовно можна розділити на чотири ключові групи, кожна з яких спрямована на визначення, розвиток та забезпечення ефективності систем управління інформаційною безпекою (СУІБ).

1) Стандарти для огляду і введення в термінологію: Ця група стандартів має на меті визначити та узагальнити основні поняття та терміни, пов'язані з інформаційною безпекою. Вони служать основою для зрозуміння загальних принципів та підходів до захисту інформації.
2) Стандарти, які визначають обов’язкові вимоги до СУІБ: Ці стандарти встановлюють основні обов'язкові вимоги до систем управління інформаційною безпекою, надаючи рамки та структуру для ефективної імплементації інформаційного захисту в організаціях.
3) Стандарти, що визначають вимоги і рекомендації для аудиту СУІБ: Ця група стандартів надає вимоги та рекомендації для проведення аудиту систем управління інформаційною безпекою, забезпечуючи ефективний механізм контролю та перевірки дотримання вимог.
4) Стандарти, що пропонують кращі практики впровадження, розвитку та вдосконалення СУІБ: Ці стандарти містять рекомендації та кращі практики для успішного впровадження, розвитку та постійного вдосконалення систем управління інформаційною безпекою в організаціях.

Зазначені стандарти формують важливий фундамент для розбудови ефективної і стійкої системи інформаційної безпеки, забезпечуючи високий рівень захисту в сучасному цифровому середовищі.

Розглянемо стандарти, що визначають базові принципи та термінологію в сфері інформаційної безпеки.

Один із ключових документів у цьому контексті - стандарт ISO/IEC 27000 [12] «Інформаційні технології – Методи і засоби забезпечення безпеки – Система менеджменту інформаційної безпеки – Загальні відомості та словник». Цей стандарт становить важливий внесок у розуміння загальних концепцій систем управління інформаційною безпекою, а також надає інтерпретацію ключових термінів, що використовуються в цій області. Він відкриває широкі можливості для засвоєння важливих аспектів інформаційної безпеки.

За даним стандартом слідують нормативні документи, що встановлюють обов'язкові стандарти для систем управління інформаційною безпекою (СУІБ). Серед них основний - ISO/IEC 27001 «Інформаційна технологія – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги». Цей стандарт не лише комплексно описує найкращі світові практики у сфері управління інформаційною безпекою, але й ставить конкретні вимоги до процесів проектування, впровадження та підтримки СУІБ. Враховуючи індивідуальні потреби організації, стандарт також зосереджується на оцінці та управлінні ризиками інформаційної безпеки. Таким чином, ця система стандартів створює необхідні умови для впровадження та ефективного управління інформаційною безпекою в сучасному цифровому середовищі.

ISO/IEC 27001 [11] установлює вимоги, які є загальними та можуть бути застосовані до різноманітних організацій, незалежно від їхнього типу, розміру та природи [6]. Цей стандарт також визначає вимоги до системи менеджменту інформаційної безпеки з метою виявлення здатності організації ефективно захищати свої інформаційні ресурси. Важливо відзначити, що вимоги ISO/IEC 27001 [11] створені як загальний референс, доступний для застосування у різноманітних контекстах організаційного життя.

Ці вимоги не обмежуються конкретними видами організацій і можуть бути використані всіма, незалежно від їхньої галузі чи сфери діяльності. Крім того, ISO/IEC 27001 [11] не тільки встановлює рамки для захисту

інформаційних ресурсів, але й функціонує як ефективна модель для розробки та впровадження системи менеджменту інформаційної безпеки. Він забезпечує компроміс між загальноприйнятими принципами та можливістю адаптації до конкретних умов та вимог кожної конкретної організації. Таким чином, цей стандарт створює умови для впровадження, ефективного функціонування, моніторингу та постійного удосконалення системи менеджменту інформаційної безпеки в контексті великого спектру організаційних умов.

Стосовно стандартів, які уточнюють вимоги і надають рекомендації для аудиту систем управління інформаційною безпекою (СУІБ), важливо врахувати кілька ключових документів. До цієї категорії відносяться:

1) ISO/IEC 27006: "Інформаційні технології – Методи забезпечення безпеки – Вимоги до органів аудиту і сертифікації систем управління інформаційною безпекою." Цей стандарт значно розширює вимоги, які передбачені стандартом ISO 17021, спеціально для організацій, які здійснюють аудит та сертифікацію СУІБ.
2) ISO/IEC 27007: "Інформаційні технології – Методи забезпечення безпеки – Керівництво по аудиту – Систем менеджменту інформаційної безпеки." Цей стандарт пропонує рекомендації щодо проведення аудитів СУІБ з боку сертифікаційних організацій, що може бути корисним для аудиторів цих організацій.
3) ISO/IEC TR 27008: "Інформаційні технології – Методи забезпечення безпеки – Керівництво для аудиторів щодо механізмів контролю СУІБ." Це додатковий стандарт до ISO 19011: 2011, розроблений спеціально для СУІБ, і спеціалізований для аудиту механізмів управління інформаційною безпекою в організації.

Ці стандарти є важливими керівництвами та інструментами для ефективного аудиту та вдосконалення систем управління інформаційною

безпекою. З їхньою допомогою забезпечується відповідність та надійність СУІБ відповідно до встановлених міжнародних стандартів.

В контексті управління інформаційною безпекою в організації, існує різні стандарти, але одна з найбільш об'ємних груп стосується кращих практик впровадження та вдосконалення систем управління інформаційною безпекою (СУІБ). До цієї категорії входять такі стандарти, як ISO/IEC 27002 та ISO/IEC 27003.

1) ISO/IEC 27002: "Інформаційні технології – Методи забезпечення безпеки – Практичні правила управління інформаційною безпекою. Друга редакція 01.10.2013". Цей стандарт, який став популярним після ISO 27001, надає важливі вказівки щодо розробки, впровадження, підтримки і вдосконалення СУІБ. Він служить як міжнародний референс для організацій, які впроваджують заходи інформаційної безпеки на базі ISO/IEC 27001, або як настанова для організацій, які впроваджують загальноприйняті заходи інформаційної безпеки. Стандарт також може використовуватися для розроблення установчих документів з управління інформаційною безпекою, що специфічні для конкретних галузей та організацій, враховуючи їхні унікальні ризики інформаційної безпеки.
2) ISO/IEC 27003: "Інформаційні технології – Методи забезпечення безпеки – Керівництво по впровадженню системи управління інформаційною безпекою". Цей стандарт визначає вказівки та методологію для процесів розроблення і впровадження СУІБ, що надає організаціям конкретні інструменти для успішної реалізації та підтримки систем управління інформаційною безпекою.

Ці стандарти важливі для організацій різних типів та розмірів, враховуючи різноманіття їхніх операцій та ризиків інформаційної безпеки.

Забезпечення інформаційної безпеки на високому рівні стає можливим завдяки впровадженню ефективних практик та методологій, які визначають ці стандарти.

Стандарт ISO/IEC 27003 спрямований на надання ефективної допомоги при впровадженні системи управління інформаційною безпекою (СУІБ) в межах організації згідно з вимогами ISO/IEC 27001. Слід відмітити, що цей стандарт пропонує рекомендації та пояснення, не накладаючи при цьому жодних обов'язкових вимог. В той же час ISO/IEC 27003 детально визначає етапи планування проекту СУІБ.

Стандарт розрахований для використання в корпоративних системах, що реалізують СУІБ, і застосовний для організацій будь-якого типу та розміру. Основний акцент робиться на критичних аспектах, які є ключовими для успішного проектування та впровадження СУІБ.

ISO/IEC 27003 визначає такі ключові пункти:

1) Фази планування проекту СУІБ: Описується весь процес планування проекту, від початкового етапу розробки до подання конкретних планів впровадження системи управління інформаційною безпекою.
2) Застосування у корпоративних системах: Стандарт спроектований таким чином, щоб бути ефективним і придатним для застосування в комплексних корпоративних системах, які реалізують СУІБ.
3) Універсальність в застосуванні: Охоплює організації різних типів і розмірів, забезпечуючи узагальнені підходи для всебічного впровадження.

Стандарт також детально описує процес отримання затвердження від керівництва для впровадження СУІБ та визначає ключові етапи проекту впровадження, надаючи керівництво планом для успішної реалізації СУІБ.

В нашій країні було створено широкий спектр нормативних актів у сфері технічного захисту інформації та визначено державні стандарти України (ДСТУ), що регулюють питання створення та оптимальної експлуатації систем

управління інформаційною безпекою (СУІБ). До числа цих нормативних документів належать [14]:

1) НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі"
2) Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі"
3) НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу"
4) НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу"
5) НД ТЗІ 2.5-008-02 "Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2"
6) НД ТЗІ 2.5-010-03 "Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу"
7) НД ТЗІ 3.7-001-99 "Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі"
8) НД ТЗІ 3.6-001-2000 "Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу"
9) ГОСТ 34.602- 89
10) НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу"

У додаток до внутрішніх нормативів, в Україні було акредитовано та впроваджено два галузеві міжнародні стандарти: ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 та ГСТУ СУІБ 2.0/ISO/IEC 27002:2010, що стосуються інформаційних технологій, методів захисту, та систем управління інформаційною безпекою з відповідними вимогами та стандартами.

Міжнародні нормативи інформаційної безпеки втілюють в собі вичерпну систему, що охоплює як примусові вимоги, так і рекомендації, спрямовані на гарантування надійного захисту інформаційної безпеки (ІБ). Процес створення нових стандартів є постійним інструментом, який реагує на неперервний стрім викликів та інцидентів інформаційної безпеки. Цей процес спрямований на розробку універсальної та надійної моделі захисту особистих даних та інформації, включаючи їх захист у кіберпросторі.

Сімейство міжнародних стандартів є не лише фундаментом для ефективного механізму забезпечення інформаційної безпеки, але також служить орієнтиром для подальшого розвитку програм захисту систем управління інформаційною безпекою (СУІБ) та гарантування ІБ на локальних рівнях.

Цей неперервний процес вдосконалення стандартів дозволяє адаптувати заходи безпеки до постійно зростаючих викликів і загроз, що забезпечує високий рівень захисту в умовах сучасного кіберпростору та інформаційного середовища.

1.4 Проблеми оцінювання стану безпеки

Пояснюючи сутність концепції безпечної системи, ми приймаємо позицію, згідно з якою безпека є важливою якісною характеристикою системи. Це створює виклики у вимірюванні безпеки в однакових одиницях та подальшому порівнянні рівнів безпеки, наприклад, між двома різними системами. Одним із ключових аспектів визначення захищеної системи є

усвідомлення, що безпека не є конкретним параметром, який можна виміряти або порівняти в стандартних одиницях.

Вона є складною і відносною величиною, яка залежить від конкретних умов, загроз та контексту взагалі. Такий підхід ускладнює створення однозначних метрик безпеки та вимагає розгляду безпеки як гнучкого та адаптивного аспекту, який може змінюватися залежно від потреб та умов даних систем [1] [2].

Не можна також ігнорувати той невідомий обставини, що ухвалення рішення під час експертизи неминуче підпорядковане суб'єктивним судженням експерта, а також його власним знанням і професійним досвідом. Запобігти або зменшити негативний вплив цього фактора можливо шляхом активного розвитку наукових та методичних підходів у даній галузі. У контексті прийняття експертних рішень слід враховувати, що суб'єктивність експертного оцінювання визначається індивідуальним сприйняттям та інтерпретацією експертом представленої інформації.

Це ставить під сумнів абсолютну об'єктивність таких рішень та підкреслює необхідність розвитку ефективних методів та наукових підходів для мінімізації впливу особистого експертного бачення. Зокрема, важливим є постійне вдосконалення методичного та теоретичного базису, що дозволить експертам зменшити ризик спотворення рішень під впливом особистих уподобань чи обмежень.

Продовження вивчення і розробка нових підходів також є важливим етапом у вдосконаленні якості експертних рішень. Сприяючи постійному розвитку методологій та забезпеченню експертів новими науковими знаннями, можна значно поліпшити об'єктивність і надійність їхніх експертних висновків. Таким чином, покращення якості експертних рішень вимагає комплексного підходу, що включає в себе не лише розвиток методичного та наукового забезпечення, але й стимулювання постійного самовдосконалення та професійного зростання експертного корпусу.

Із проведеного аналізу також випливає, що в галузі інформаційної безпеки недостатня теоретична база, яку можна застосовувати для розв'язання задач якісного оцінювання. Це особливо помітно тоді, коли немає повної інформації про систему, а також даних, які підлягають обробці, задані нечітко (розмито) і часто пов'язані з із судженнями та інтуїцією людини. Для роботи з нечітко детермінованими величинами зазвичай застосовують апарат теорії НМ, який оперує такими поняттями, як нечіткі множини, нечіткі або лінгвістичні змінні, тощо.

Розглядаючи концепцію захищеної системи, важливо враховувати, що безпека представляє собою якісну характеристику системи, і це ускладнює завдання вимірювання та порівняння безпеки між різними системами. Неможливо звести безпеку до конкретних одиниць вимірювання, що ускладнює об'єктивне порівняння наприклад, двох комп'ютерних систем. Також важливо враховувати, що рішення, прийняте під час експертизи, значно впливає на суб'єктивні судження та досвід експерта. Зменшення негативного впливу цього фактора можливе завдяки розвитку методичного та наукового забезпечення, що стандартизує процес оцінювання. Аналіз також вказує на те, що в галузі інформаційної безпеки існує дефіцит теоретичної бази, яку можна використовувати для якісного оцінювання.

Особливо це помітно, коли немає повної інформації про систему, а дані, що підлягають обробці, задані нечітко та пов'язані із судженнями та інтуїцією. Для роботи з нечітко детермінованими величинами часто застосовується апарат теорії нечітких множин, що оперує поняттями, такими як нечіткі множини, нечіткі або лінгвістичні змінні і т.д.

Важливо визначити, що якісне оцінювання безпеки інформації в сучасних комп'ютерних системах здійснюється в умовах постійного розвитку технологій та зміни загроз. Це вимагає постійного апдейту методів аналізу та впровадження нових стратегій безпеки. Однак велика частина інформаційної безпеки ґрунтується на суб'єктивних судженнях експертів, а це може призводити до ризиків та відхилень у процесі прийняття рішень. Для

зменшення впливу суб'єктивних факторів на результати оцінювання важливо активно розвивати методичне та наукове забезпечення, що базується на об'єктивних критеріях та стандартах.

Зокрема, інтеграція нечітких множин та нечіткої логіки в процес прийняття рішень може допомогти ефективніше враховувати неоднозначність та невизначеність в оцінці рівня безпеки. У світлі цього важливо акцентувати увагу на розвитку теоретичної бази інформаційної безпеки, зокрема для розв'язання завдань якісного оцінювання. Використання теорії нечітких множин є лише одним із можливих шляхів у роботі з нечітко визначеними даними, де експертні судження та інтуїція грають значущу роль. Такий підхід стає необхідним у випадках, коли інформація не повністю структурована, а аспекти безпеки пов'язані із складними ситуаціями, де важко визначити чіткі межі та параметри.

2 ПОБУДОВА НЕЧІТКИХ МОДЕЛЕЙ ОЦІНКИ РІВНЯ БЕЗПЕКИ

2.1 Нечітка модель оцінки рівня безпеки

Нечітка модель оцінки загрози - це аналітичний підхід, який використовує нечіткі логічні правила для оцінки рівня загрози в певній ситуації. Вона дозволяє враховувати неоднозначність, невизначеність та різні ступені впевненості в оцінках загроз. Такі моделі використовують нечіткі множини, які включають лінгвістичні терміни для опису рівня загрози, наприклад: "низький рівень", "середній рівень" та "високий рівень" [1].

Ці терміни можуть мати свої числові відповідники, які виражають ступені належності до цих категорій.

Наприклад, оцінка загрози для кібербезпеки може враховувати такі параметри, як рівень захисту мережі, сила паролів, частота виявлення потенційних атак тощо. Кожен параметр може мати свою нечітку оцінку, яка потім об'єднується для отримання загальної оцінки загрози. Це дозволяє аналізувати ризики та визначати, які аспекти потребують уваги чи покращень,

враховуючи не тільки чіткі параметри, а й неоднозначність та невизначеність в оцінках.

Такий підхід допомагає краще розуміти загрози та приймати обґрунтовані рішення з покращення безпеки.

У загальному визначенні, оцінка рівня інформаційної безпеки вимагає індивідуального розгляду кожного критичного бізнес-процесу та врахування лише тих уразливостей, які є суттєвими для конкретного бізнес-процесу. Важливо відзначити, що деякі вразливості можуть бути спільними для всіх бізнес-процесів. Кожній вразливості з переліку співвідноситься загроза, для реалізації якої існує ця вразливість.

Для кожної ідентифікованої пари проводиться оцінка ймовірності виникнення та впливу цієї пари на цілісність, конфіденційність, доступність та спостережуваність. Поглибимо аналіз та розглянемо процес побудови інтервальної нечіткої моделі для оцінювання рівня захищеності комп’ютерної системи, базуючись на знаннях експертів. Допоміжні кроки у цьому процесі включають складання експертного запиту, де компоненти ранжуються і визначається коефіцієнт важливості для кожної компоненти запиту (наприклад, за шкалою Сааті [1]). Крім того, експерти формують нечіткі еталони, що відображають лінгвістичну змінну "рівень безпеки".

Ці еталони використовуються для порівняння з нечіткими числами. Наприклад, терм-множина лінгвістичної змінної "рівень безпеки" може містити п'ять нечітких термів:

- Надзвичайно низький
- Низький
- Середній
- Високий
- Надзвичайно високий

Ці терміни визначаються в контексті інтервальної нечіткої моделі та слугують як лінгвістичні покажчики для оцінювання рівня захищеності системи:

$$T = \{T_1, T_2, T_3, T_4, T_5\}$$

Визначивши відповідні категорії як "Дуже низький" (ДН), "Низький" (Н), "Нижче середнього" (НС), "Середній" (С), "Вище середнього" (ВС), "Високий" (В) та використовуючи числові оцінки від 0 до 4, введемо число еталонів як L = 5. Розглянемо еталони для вказаних категорій, визначаючи їх на основі нечітких множин:

Н = {1/0, 0,5/1, 0,2/2, 0,1/3, 0,06/4};

НС = {0,5/0, 1/1, 0,5/2, 0,2/3, 0,1/4};

С = {0,1/0, 0,2/1, 0,5/2, 1/3, 0,5/4};

ВС = {1/0, 0,5/1, 0,2/2, 0,1/3, 0,06/4};

В = {0,06/0, 0,1/1, 0,2/2, 0,5/3, 1/4}.

Такий підхід дозволяє структурувати оцінку рівня захищеності за конкретними категоріями та числовими значеннями, надаючи більш глибокий та деталізований підхід до оцінювання безпеки.

В другому етапі відбувається процес оцінювання користувачами функціонального стану системи відповідно до їхніх конкретних запитів. Цей етап, безсумнівно, є суб’єктивним, оскільки від оцінок користувачів значною мірою залежить від багатьох суб’єктивних факторів.

Ці фактори вводять невизначеність у вихідні дані та можуть значно вплинути на результати обчислень. Споживачі взаємодіють з системою, визначаючи її поточний стан та ефективність відповідно до своїх потреб та очікувань. Цей процес оцінювання, що базується на відгуках користувачів, може бути важливим елементом вдосконалення функціональності системи. Слід відзначити, що врахування різноманітних суб’єктивних факторів, таких як особисті вподобання, індивідуальні сприйняття та очікування, робить оцінку більш точною та збалансованою.

Врахування різноманіття поглядів користувачів може призвести до вдосконалення якості обслуговування та надання продукту або послуги. Такий підхід відображає реальність та унікальність кожного користувача, сприяючи адаптації системи до індивідуальних потреб та очікувань своїх користувачів.

2.2 Нечітка модель з бальною шкалою

У даній моделі визначається основна група термінів лінгвістичної змінної, яка визначає рівень захищеності інформації в оцінюваній комп’ютерній системі, розподілений на п'ять нечітких категорій. Головний зміст оцінки за цією моделлю полягає в тому, що користувач, дав відповіді на передбачені попередньо впорядковані питання, які є складовими частинами експертного запиту, використовуючи N-бальну шкалу, яку попередньо розробив експерт (див. Рисунок 1.1).

Важливо відзначити, що межі цієї шкали можуть змінюватися та залежать від рівня складності потенційної загрози. Кожна категорія шкали відображає певний аспект рівня безпеки, і користувач, визначаючи свої відповіді, надає системі відомість про її поточний стан з точки зору безпеки. Цей метод оцінки створює можливість враховувати різноманітні фактори та аспекти, що впливають на загальний рівень захисту. Такий підхід не лише дозволяє користувачам ефективно висловлювати свої думки, але і надає зручність у визначенні конкретних аспектів інформаційної безпеки, які є важливими для них. Таким чином, шкала стає інструментом для споживачів у

вираженні їхнього сприйняття та оцінки рівня безпеки комп’ютерної системи.

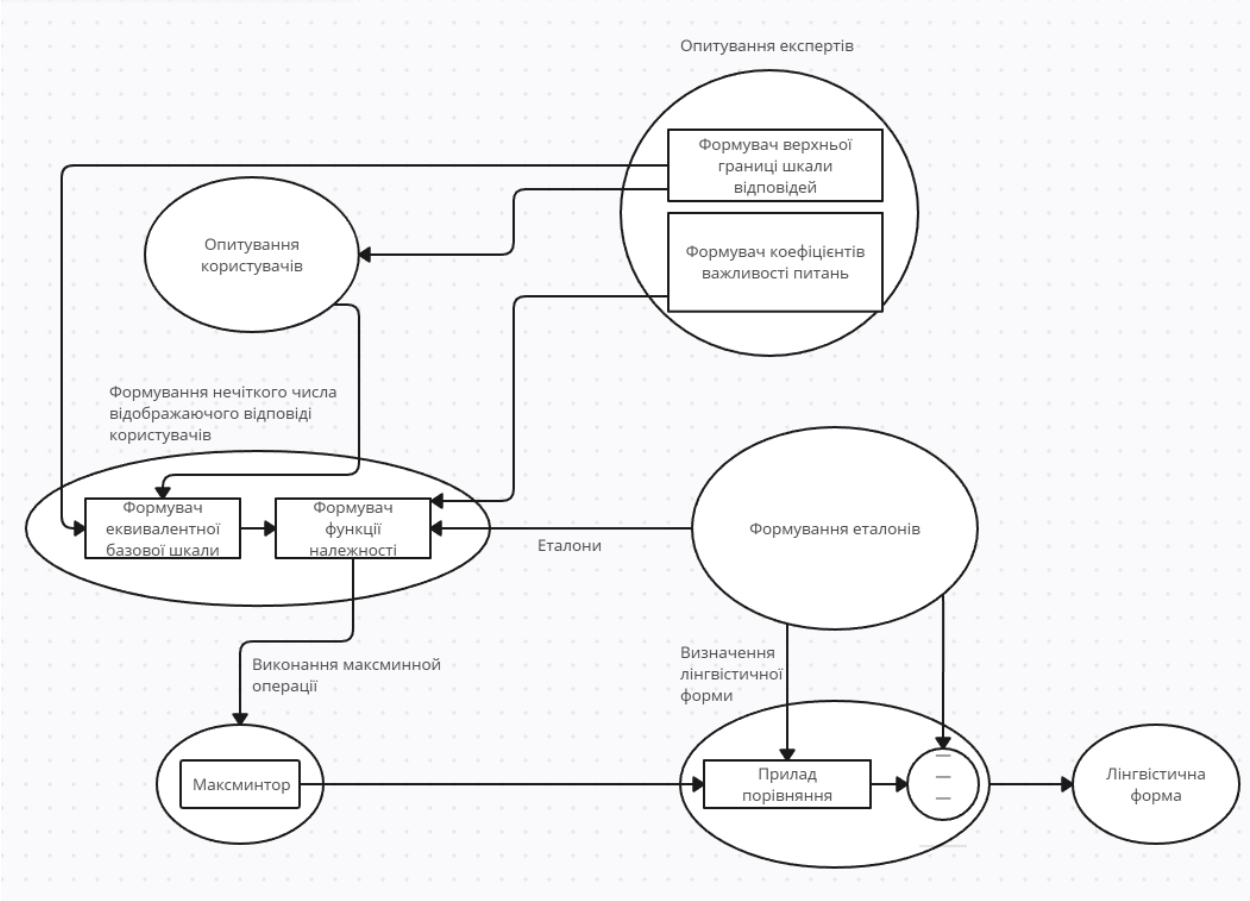


Рисунок 2.1 – Схема обробки даних за нечіткою моделю з бальною шкалою

Діапазон $\left[\underline{X_j},\ \overline{X_j}\right]$ $\left(\underline{X_j} = 0, \overline{X_j} = N_j\right)$ зміна параметра $X_j{}^*$, j = $\overline{1,n}$ (N_j – максимально можлива кількість балів по кожному питаню) відображається в універсальну множину еталоних нечітких чисел $U = [L-1]$ (L – кількість еталонів), для чого фіксоване значення $X_j^* \in \underline{X}_j,\ \overline{X}_j$ перераховуються в відповідний елемент $U_j^* \in [0, L-1]$ по формулі:

$$U_j^* = (L-1)\frac{X_j^* - \underline{X}_j}{\overline{X}_j - \underline{X}_j}$$

а функція приналежності $\mu_i^j\left(U_j^*\right), i = \overline{1,L}$ нечіткого терма з і-м номером вичислимо за допомогою виразу:

$$\mu_{ii}^j\left(U_j^*\right) = \left[\frac{1}{1 + (U_j^* - i + 1)^2}\right]^{PN_j \ldots n}$$

Де $PN_j, j = \overline{1,n}$ - коєфіцієнт важливості, обчислення по оцінкам експертів для кожного компоненту вищенаведаного експертного запросу.

На завершувальній стадії визначаємо показник рівня захищеності по наступному логічному виразу:

$$\mu_S(X_j^*) = \bigvee_{i=1}^{L} \bigwedge_{j=1}^{n} \mu_i^j$$

де i = $\overline{1,L}$ – номер терма з базового терм-множини T, а j = $\overline{1,n}$ – номер компонента експертного запросу.

Змоделюємо експертний запит, але нехай відповіді на нього будуть сформовані в балах. Межі зміни діапазону відповідей задає експерт для кожного компонента окремо. Так, наприклад, для першого, другого, третього і четвертого компонент межі дорівнюють [0;3], [0;5], [0;10] і [0;4] відповідно. Використовуючи матрицю парних порівнянь і перетворену матрицю, обчислимо коєфіцієнт важливості для кожного компонента експертного запиту.

Формула матриці попарних порівнянь:

$$i < j,\ v = i,\ w = j\text{: } avw\text{ `} = (\ 100/aij{+}1\ ) * aij$$

$$i > j,\ v = i,\ w = j\text{: } avw\text{ `} = (\ 100/aji{+}1\ )$$

Припустимо, що матриця парних порівнянь має такий вигляд (рис 1.2):

$$A = (a_{ij}) = \begin{vmatrix} 1 & 3 & 4 & 9 \\ 1/3 & 1 & 5 & 7 \\ 1/7 & 1/5 & 1 & 5 \\ 1/9 & 1/7 & 1/5 & 1 \end{vmatrix},$$

Рисунок. 2.2 - матриця попарних порівнянь

Тоді елементи перетвореної матриці матимуть такі значення (рис 1.3):

$$A' = (a'_{ij}) = \begin{vmatrix} 1 & 75 & 87,5 & 90 \\ 25 & 1 & 83,3 & 87,5 \\ 12,5 & 16,7 & 1 & 83,3 \\ 10 & 12,5 & 16,7 & 1 \end{vmatrix}.$$

Рисунок. 2.3 – матриця перетворених значень

Формула Коєфіцієнта важливості:

$$P_j = \sum_{i=1}^{n} a_i$$

Після проведення всіх обчислень та визначення коєфіцієнта важливості для кожного з компонентів, занесемо в таблицю результати обчислення коєфіцієнта важливості для всіх компонентів, нормалізовані та відповіді користувачів, значення які ми отримали мають вагому частину у наступних обчислень в даній моделі (табл. 1.1).

Номер компонента	$P_j, j = \overline{1,4}$	$PN_j, j = \overline{1,4}$	Відповіді в балах $X_j^*, j = \overline{1,4}$
1	75+87,5+90=252,5	0,421	1,5
2	25+83,3+87,5=195,8	0,326	3,5
3	12,5+16,7+83,3=112,5	0,188	2
4	10+12,5+16,7=39,2	0,065	3,6

Таблиця 2.1 – результати опитування користувачів та експертів

Використаємо апарат нечітких множин. Відобразимо діапазон [Xj ,Xj] (Xj = 0, $Xj = Nj$) зміни параметру $Xj*$, j = 1, n (Nj – максимально можлива кількість балів по кожному питанню) на універсальну множину нечітких еталонів U = [0, $L-1$] (L – кількість еталонів).

Тоді фіксоване значення $Xj* \in Xj$, Xj перераховується у відповідний елемент $Uj* \in [0, L-1]$ по формулі:

$$U_j^* = (L-1)\frac{X_j^* - \underline{X}_j}{\overline{X}_j - \underline{X}_j}$$

Функцію приналежності нечіткого терма з і-тим номером обчислюємо за допомогою формули:

$$\mu_i^j(U_j^*) = \left[\left[\frac{1}{1 + \left(U_j^* - i + 1\right)^2}\right]^{PN_j * n}\right]$$

Значення PN_j відповідає коефіцієнту важливості, де j змінюється від одиниці до n. Значення рівня захисту в системі буде визначатися за допомогою логічного виразу. Обчислюємо результати (табл. 2.2).

Номер компонента (j)	$U_j^*, (j = \overline{1,4})$	$\mu_1^j(U_j^*)$	$\mu_2^j(U_j^*)$	$\mu_3^j(U_j^*)$	$\mu_4^j(U_j^*)$	$\mu_5^j(U_j^*)$
1	2	0,07	0,31	1	0,31	0,07
2	2,8	0,06	0,15	0,52	0,95	0,31
3	0,8	0,69	0,97	0,51	0,27	0,16
4	3,6	0,5	0,59	0,72	0,92	0,96

Таблиця 2.2 – результати опитування користувачів та експертів

Згідно результатів знаходимо показник рівня захищеності за формолою:

$$\mu_S(X_j^*) = \bigvee_{i-1}^{L} \bigwedge_{j-1}^{n} \mu_i^j$$

Проводимо обчислення рівня захищеності:

$\mu_S(X_j^*) = \bigvee_{i=1}^{L} \bigwedge_{j=1}^{n} \mu_i^j = [\mu_1^1(2)$

$\wedge\, \mu_1^2(2{,}8) \wedge \mu_1^3(0{,}8) \wedge \mu_1^4(3{,}6)] \vee [\mu_2^1(2) \wedge \mu_2^2(2{,}8) \wedge \mu_2^3(0{,}8) \wedge \mu_2^4(3{,}6)]$

$\vee\, \mu_3^1(2) \wedge \mu_3^2(0{,}8) \wedge \mu_3^4(0{,}8)] \vee \mu_3^4(3{,}6)] \vee$

$[\mu_4^1(2) \wedge \mu_4^2(2{,}8) \wedge \mu_4^3(2{,}8) \wedge \mu_4^3(0{,}8) \wedge \mu_4^4(3{,}6)] \vee [\mu_5^1(2) \wedge \mu_5^2(0 = 2{,}8) \wedge \mu_5^3(0{,}8) \wedge \mu_5^4(3{,}6)] = 0{,}51$

Згідно результатів показник рівня захищеності дорівнює $0{,}51$ (μ_3^j), тому для прийняття рішення вибирається нечіткий терм ТЗ – “Середній”, що і визначає рівень захищеності в даній роботі.

2.3 Нечітка модель з лінгвістичною шкалою

Розглянем нечітку модель з лінгвістичною шкалою. Визначення стану безпеки відповідності з нечіткою моделю з лінгвістичною шкалою реалізується по результатам опитування користувачів системи відповідно складеного експертного запиту, компоненти якого зачасно ранжовані через визначення КВ $P_j(j = \overline{1,n};)$ (n – кількісний елемент). Для досягнення цієї цілі використовують метод відносного ранжування, в якому список всіх компонентів запиту заносяться в таблицю відносно ранжування (попарного порівняння). Експерт приймає рішення на основі голосування за один з компонентів або ділення голосу, наприклад, якщо значимість компонентів, за його думкою відноситься як 1:3, то втаблицю заносяться числа 0,25 та 0,75.

Для ранжування також можно використати метод на основі перетвореної матриці A` = $(a`_{vw})$, отриманий на основі матриці парних зрівнянь A = (a_{ij}). Елемент перетворенної матриці визначають так:

$$a`_{vw} = \begin{cases} \dfrac{100}{a_{ij}+1} * a_{ij}, & \forall i < j: v = i, w = j; \\ 1, & \forall i < j: v = w = \ i = j; \\ \dfrac{100}{a_{ij}+1}, & \forall i < j: v = j, w = i; \end{cases}$$

Де i = j = $\overline{1,n}$,

a, n – кількість компонентів запиту

Для більш детального опису роботи важливим етапом є побудова детальної схеми, яка систематизує ключові компоненти та взаємодії у моделі, від формування еталонів обчислення рівня безпеки.

Схема нечіткої моделі з лінгвістичною шкалою (рис. 2.4).

Рисунок 2.4 – Схема обробки даних за нечіткою моделю з лінгвістичною шкалою

Значення коєфіцієнта важливості $(P_i, i = \overline{1,n},)$ для кожних з питань експертного запиту обчислюється за формулою:

$$P_i = \sum_{j=1}^{n} a`_{ij} \; \forall i \neq j$$

Після визначення коєфіцієнту важливості здіснюється їх нормалізація за вираженням:

$$PN_i = P_i / (\sum_{i=1}^{n} P_i)$$

Таким чином щоб виконати умову:

$$\sum_{i=1}^{n} PN_i = 1$$

На відміну від запропонованого в роботі способу опрацювання сформованої матриці парного порівняння метод побудови перетвореної матриці не вимагає обчислення її власного значення, процес знаходження якого значно ускладнюється зі зростанням кількості ранжируваних компонент, процес знаходження якого значно ускладнюється зі зростанням кількості ранжованих компонентів.

Описані вище методи ранжування дають змогу порівнювати два елемента, ігноруючи інші, що істотно полегшує процес ухвалення рішення.

Крім ранжування складових за ступенем небезпеки, експерти мають будувати нечіткі еталони, які відображають лінгвістичну змінну "РІВЕНЬ БЕЗПЕКИ", які будуть зразком для порівняння нечітких множин.

Визначемо, наприклад, базову терм-множину лінгвістичних змінних п’ятьма нечіткими термами T = {T1, T2, T3, T4, T5} з відповідними назвами: “Низький” (Н), “Нижче середнього” (НС), “Середній” (С), “Вижче середнього” (ВС), ”Високий” (В). Виконаємо побудову еталоних нечітких множин, використовуя один із способів побудови функції належності нечітких множин. Діапазон зміни носія $X_i, i = \overline{1, L}$ (L = 5 = число термів) відобразимо на універасальну множину U = [0, 4], в результаті отримуємо еталонні нечіткі множини, представлені виразом:

$$\begin{cases} \text{Н} = \left\{\frac{1}{0}; \frac{05}{1}; \frac{0,2}{2}; \frac{0,1}{3}; \frac{0,06}{4}\right\}; \\ \text{НС} = \left\{\frac{0,5}{0}; \frac{1}{1}; \frac{0,5}{2}; \frac{0,2}{3}; \frac{0,1}{4}\right\}; \\ \text{С} = \left\{\frac{0,2}{0}; \frac{0,5}{1}; \frac{1}{2}; \frac{0,5}{3}; \frac{0,2}{4}\right\}; \\ \text{ВС} = \left\{\frac{0,1}{0}; \frac{0,2}{1}; \frac{0,5}{2}; \frac{1}{3}; \frac{0,5}{4}\right\}; \\ \text{В} = \left\{\frac{0,06}{0}; \frac{0,1}{1}; \frac{0,2}{2}; \frac{0,5}{3}; \frac{1}{4}\right\}; \end{cases}$$

А також представлення графічного зображення нечітких еталонів (рис. 1.5).

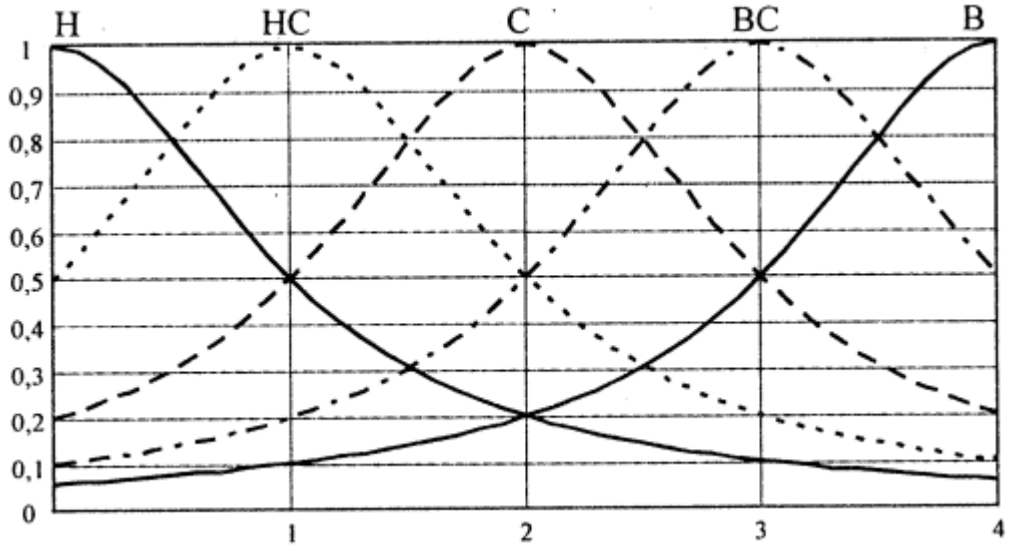


Рисунок 2.5 – Графічне представлення еталоних нечітких множин

Нечітка модель з лінгвістичною шкалою припускає, що група N користувачів відповідає на n питань (n-компонентний експертний запит) відповідно поставлено експертом нечіткої шкали. По відповідям користувачів, формується нечітка множина $Z_t, t = \overline{1,n}$, в якому ставиться у відповідності одне з еталонів. Значення нечіткого вичислювачаб відповідно оцінки відповідей всієї групи користувачів на j-й ($j = \overline{1,n},$) питання (компонент) визначається по формулі:

$$L_j = (\sum_{t=1}^{N} Z_t)/N$$

Сумарну оцінку безпеки КС визначаюь з урахуванням раннє обчислених коєфіцієнів важливості:

$$LS = \sum_{j=1}^{n} (PN_i * L_j)$$

Створене LS порівнюється з еталоним нечітким вичислювачем, для використовують a-рівневу відстань:

$$d(X,Y) = (\sum_{j=1}^{k}\sum_{i=1}^{m}|x_i - y_j|)/k$$

Де a це задане значення a-рівня ($0 \leq \text{a} \leq 1$), x_i та y_j відповідно носії отриманого еталоного нечіткого вичислювача X та Y; m – кількість компонентів нечіткого вичислювача X; k – кількість компонентів нечіткого вичислювача Y з функцією приналежності $\mu_y \geq a$.

Критерії відповідно LS одному з еталонних нечітких вичислювачів є мінімальна a-рівнева відстань, яке і визначає рівень захищеності:

$$dmin_i = \bigwedge_{j=1}^{5} d(L_i, LV_j), (i = \overline{1,4})$$

3 РЕАЛІЗАЦІЯ ЕКСПЕРЕМЕНТАЛЬНОЇ ЧАСТИНИ

Відомо, що знання, які отримують від експертів, є суб'єктивними та можуть містити різні види невизначеностей. Іншими словами, терміни, які використовуються експертами у висловленнях антецедентів та консеквентів правил, можуть мати різні тлумачення, залежно від особистого сприйняття кожного експерта. Крім того, значення консеквентів висловлень можуть розподілятися залежно від групи експертів, чия думка може бути розходженням, і інші невизначеності можуть виникати через шуми вхідних даних.

У зв'язку з цим актуальним є розробка методів, спрямованих на вирішення проблем подання та обробки невизначених або майже суперечливих вхідних даних. Найбільш ефективними для такого роду даних є методи теорії нечітких множин. Зокрема, для подальших вивчень розглянемо

нечітку модель з бальною шкалою як базовий інструмент для оцінювання рівня захищеності комп’ютерної системи. Ця модель будується на основі нечітких множин типу-1 та враховує різноманітність та невизначеність, які властиві експертному знанню.

Розглянемо детальніше процес побудови інтервальної нечіткої моделі для комплексного оцінювання рівня захищеності комп’ютерної системи, що базується на знаннях експертів. Для цього проведемо аналіз допоміжних етапів конструювання цієї моделі. По-перше, ініціюємо експертний запит, в якому компоненти передбачено попередньо ранжувати. Далі проводиться обчислення коефіцієнта важливості для кожного компонента запиту. Наприклад, цей коефіцієнт може бути визначений за допомогою шкали Сааті або іншими відповідними методами.

Другий етап передбачає конструювання нечітких еталонів експертами, які наочно відображають лінгвістичну змінну «рівень безпеки». Ці нечіткі еталони використовуються для подальших порівнянь з нечіткими числами. Так, терм-множина лінгвістичної змінної «рівень безпеки» може бути розширена до п'яти нечітких термів, що надає більше можливостей для точного вираження експертних думок та врахування різноманітних контекстів.

3.1 Складання експертних запитів

Основною складовою моделі є опитування користувачів/співробітників, які не є експертами з питань безпеки. Їхні спостереження та досвід можуть допомогти виявити певні аспекти безпеки, які можуть бути упущені технічними експертами.

Наприклад:

1. Отримання неформальної інформації: Експертні запитання дозволяють звертатися до користувачів/співробітників з неформальним

підходом, щоб отримати цінні відомості, які можуть бути важливими для безпеки, але не завжди виявляються у формальних процесах;

2. Виявлення соціальних аспектів безпеки: Експерти з різних галузей можуть надати інформацію про соціальні аспекти безпеки, такі як соціальна інженерія, яка може бути важливою для виявлення загроз, пов'язаних із людською діяльністю;

3. Аналіз робочих потоків та процесів: Користувачі, які щоденно працюють у конкретних областях, можуть надати унікальні відомості про робочі потоки та процеси, які потребують додаткового захисту;

4. Оцінка реального часу та непередбачених сценаріїв: Запитання, які спрямовані на отримання відгуків щодо оцінки загроз в реальному часі та виявлення непередбачених сценаріїв, допомагають у створенні гнучких та адаптивних стратегій безпеки;

5. Знання процесів та робочих потоків: Дозволяє більш ефективно уловити проблемні місця, які можуть виникати під час робочого процесу.

При свторені експертних запитів, задача експерта - сприяти відповідності організаційної безпеки міжнародним стандартам, зокрема ISO/IEC 27001, під час розробці запитів, які враховують їхні вимоги та враховувати особливості діяльності компанії та її інфраструктури при побудові запитів для найточнішого визначення загроз та ризиків а також, сприяти відсутності взаємовиключних питань та порівнянянь альтернатив які не можуть порівнюватись в одному експерному запиті.

В даній роботі обьєкт дослідження це айті компанія яка надає рішення для бізнес-аналітики на основі даних та допомагають світовому туристичному та готельному бізнесу оптимізувати дистрибуцію, формувати попит і максимізувати доходи.

Згідно діяльності компанії, інструментів та сервісів для реалізації рішень та володіння співпрацівниками критичної інформації будуються екпертні запити на основі вимог згідно стандарту ISO/IEC 27001.

Експертні запити:

1)

- як ви оцінюєте своє ознайомлення з політикою безпеки компанії?

- оцініть частоту проведення оновлення політики безпеки компанії.

- чи використовуються процедури для моніторингу порушень політики безпеки?

- чи доступна політика безпеки для всіх співробітників?

2)

- як ви оцінюєте процедури повідомлення про події з безпекою?

- як ви оцінюєте складність стандарту паролів від робочої пошти співробітників?

- чи використовується двофакторна аутентифікація для доступу до робочої пошти співробітників?

- як часто ви змінюєте пароль від робочої пошти?

3)

- чи є в компанії фізичні бар'єри для захисту від несанкціонованого доступу?

- чи використовуються системи контролю доступу до офісу?

- чи є в компанії процедури забезпечення безпеки при допуску до офісу сторонніх осіб?

- чи часто виконується резервне копіювання?

4)

- чи проводиться антивірусний контроль?

- оцініть ефективність системи ідентифікації та аутентифікації визначення вашої особи та доступу до ресурсів компанії.

- як ви оцінюєте процес керування правами доступу, який визначає, які ресурси та операції які ви можете використовувати у своїй роботі?

- наскільки ефективно здійснюється моніторинг доступу до інформаційних ресурсів компанії, у тому числі виявлення аномальної активності?

5)

- як ви оцінюєте процес завершення доступу до інформаційних ресурсів для працівників, які покидають компанію або змінюють свою роль?

- наскільки ви вважаєте ефективними навчання та інформаційні кампанії для підвищення свідомості працівників щодо безпеки доступу?
- наскільки ефективно реалізовані заходи захисту від витоку конфіденційної інформації в хмарному середовищі?
- як часто проводяться аудити безпеки для перевірки відповідності хмарних сервісів вимогам безпеки?

6)

-як ви оцінюєте систему ідентифікації та аутентифікації в хмарному середовищі для забезпечення безпеки доступу?

- Як часто проводяться аудити безпеки для перевірки відповідності хмарних сервісів вимогам безпеки?

-На скільки ефективно здійснюється моніторинг доступу до інформаційних ресурсів компанії, у тому числі виявлення аномальної активності?

Опитування співробітників відбувається завдяки гугл формам:

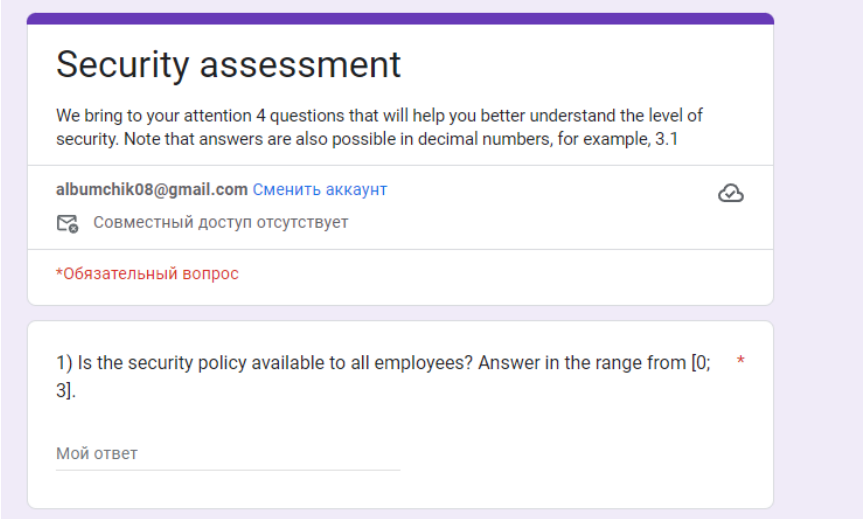


Рисунок 3.1 – Гугл форма опитування

3.2 Інтервальна нечітка модель з бальною шкалою

Використання інтервалів дозволяє враховувати варіативність та коливання в даних. Це особливо важливо, коли точні значення можуть змінюватися або коливатися в межах певного діапазону.

На основі двух попредньо ранжованих запитів будується матриці попарних порівнянь

- як ви оцінюєте процедури повідомлення про події з безпекою?	[0-5]	- як ви оцінюєте своє ознайомлення з політикою безпеки компанії?	[0-3]
- як ви оцінюєте складність стандарту паролів від робочої пошти співробітників?	[0-4]	- оцініть частоту проведення оновлення політики безпеки компанії.	[0-5]
- як ви оцінюєте процедуру двофакторної аутентифікації для доступу до робочої пошти співробітників?	[0-4]	- як ви оцінюєте процедури для моніторингу порушень політики безпеки?	[0-10]
- як часто ви змінюєте пароль до внутрішніх систем?	[0-6]	- чи доступна політика безпеки для всіх співробітників?	[0-4]

Рисунок 3.2 – Ранжовані експертні запити

Під час використання цієї моделі користувач взаємодіє з системою, реагуючи на передбачені та відсортовані запитання, які мають N-бальну шкалу. Тобто, у користувача є можливість відповідати на питання, використовуючи числову шкалу заздалегідь визначених значень. Цей процес дозволяє зібрати об'єктивні дані щодо оцінки важливості кожного компонента запиту в контексті визначення рівня захищеності системи:

$i < j,\ v = i,\ w = j$: $avw\ ` = (\ 100/aij+1\ ) * aij$

$i > j,\ v = i,\ w = j$: $avw\ ` = (\ 100/aji+1\ )$

Отримані результати:

Матриця першого запиту

Матриця попарного порівняння				
Питання	П1	П2	П3	П4
П1	1	3	7	9
П2	1/3	1	3	7
П3	1/7	1/3	1	3
П4	1/9	1/7	1/3	1

Нормалізації матриці				
Питання	П1	П2	П3	П4
П1	1	75	87,5	90
П2	25	1	75	87,5
П3	12,5	25	1	75
П4	10	12,5	25	1

Рисунок 3.3 – Матриця попарних порівнянь для першого запиту

Матриця другого запиту

Матриця попарного порівняння				
Питання	П1	П2	П3	П4
П1	1	3	4	9
П2	1/3	1	5	7
П3	1/7	1/5	1	5
П4	1/9	1/7	1/5	1

Нормалізації матриці				
Питання	П1	П2	П3	П4
П1	1	75	87,5	90
П2	25	1	83,3	87,5
П3	12,5	16,7	1	83,3
П4	10	12,5	16,7	1

Рисунок 3.4 – Матриця попарних порівнянь для другого запиту

Результати опитування десяти користувачів першого та другого запитів на основі інтервальної нечіткої моделі з бальною шкалою заносимо в таблиці:

j	1	2	3	4	5	6	7	8	9	10	м	σ	м - σ	м + σ
1.	1	3	1	1	2	1	3	1	1	2	1,6	0,84	0,76	2,44
2.	2	4	4	4	2	2	4	4	4	2	3,2	1,03	2,17	4,23
3.	2	3	4	2	2	1	3	4	2	2	2,6	0,97	1,63	3,57
4.	4	3	4	4	3	4	3	4	4	2	3,4	0,71	2,69	4,11

Рисунок 3.5 – Результати обчислень першого запиту

j	1	2	3	4	5	6	7	8	9	10	м	σ	м - σ	м + σ
1.	1	1	2	1	1	1	2	2	1	1	1,3	0,38	0,92	1,68
2.	2	3	2	2	3	2	2	2	2	2	2,2	0,42	1,78	2,62
3.	3	2	2	2	2	3	2	2	3	2	2,3	0,48	1,82	2,78
4.	1	1	2	1	1	1	1	1	2	1	1,2	0,36	0,84	1,56

Рисунок 3.6 – Результати обчислень другого запиту

Обчислюємо математичне сподівання M:

$$M_x = \frac{1}{n}\sum_{--=1}^{n} x_i * P(X = x_i)$$

Обчислюємо σ – Середньоквадратичне відхилення отриманих відповідей:

$$\sigma = \sqrt{E((X - M(X))^2)}/(\text{n-1})$$

На основі отриманих результатів обчислюємо відповіді користувачів у вигляді інтервалу:

M_x - σ

M_x + σ

Вписуємо в таблицю результати коєфіцієнту важливості, нормованого еоєфіцієнту важливості а також відповіді користувачів у вигляді інтервалів:

Номер компонента (j)	$P_j, j = \overline{1,4}$	$PN_j, j = \overline{1,4}$	Відповіді в балах $X_j^*, j = \overline{1,4}$	
1	75+87,5+90=252,5	0,421	0,92	1,68
2	25+83,3+87,5=195,8	0,326	1,78	2,62
3	12,5+16,7+83,3=112,5	0,188	1,82	2,78
4	10+12,5+16,7=39,2	0,065	0,84	1,56

Рисунок 3.7 – Коєфіцієнт важливості та результати опитування першого запиту

Номер компонента (j)	$P_j, j = \overline{1,4}$	$PN_j, j = \overline{1,4}$	Відповіді в балах $X_j^*, j = \overline{1,4}$	
1	75 + 87,5 + 90 = 252,5	0,421	0,76	2,44
2	25 + 75 + 87,5 = 187,5	0,312	2,17	4,23
3	12,5 + 25 + 75 = 112,5	0,188	1,63	3,57
4	10 + 12,5 + 25 = 47,5	0,079	2,69	4,11

Рисунок 3.8 – Коєфіцієнт важливості та результати опитування другого запиту

Коєфіцієнт важливості обчислюємо за формолою:

$$P_j = \sum_{i=1}^{n} a_i$$

Відповіді в балах:

M_x - σ

M_x + σ

Перерахування Фіксованого значення $X_j^* \in [\underline{X}_j, \overline{X}_j]$, $[\underline{X}_j, \overline{X}_j]$ – діапазон шкали відповідей на попередньо ранжовані результати:

Номер компонента j	U_j^* $(j=1,4)$		$\mu_1^j(U_j^*)$		$\mu_2^j(U_j^*)$		$\mu_3^j(U_j^*)$		$\mu_4^j(U_j^*)$		$\mu_5^j(U_j^*)$	
1	0,6	1,95										
2	1,74	3,38										
3	1,3	2,81										
4	2,15	3,3										

Рисунок 3.9 – Перерахування Фіксованого значення першого запиту

Номер компонента j	U_j^* $(j=1,4)$		$\mu_1^j(U_j^*)$		$\mu_2^j(U_j^*)$		$\mu_3^j(U_j^*)$		$\mu_4^j(U_j^*)$		$\mu_5^j(U_j^*)$	
1	0,74	1,34										
2	1,78	2,62										
3	1,82	2,78										
4	0,56	1,04										

Рисунок 3.10 – Перерахування Фіксованого значення другого запиту

Проводимо обчислення:

$$U_2^* = (5-1)\frac{2,17}{5} = 1,74$$

$$U_2^* = (5-1)\frac{4,23}{5} = 3,38$$

$$U_3^* = (5-1)\frac{1,63}{5} = 1,30$$

$$U_3^* = (5-1)\frac{3,57}{5} = 2,81$$

Функція належності і-того нечіткого терму (PN_j - коєфіцієнт важливості):

$$\mu_i^j(U_j^*) = \left[\left[\frac{1}{1+\left(U_j^* - i + 1\right)^2}\right]^{PN_j * n}\right]$$

Приклад обчислення:

$$U_1^* = 0{,}6 : \mu_1^1(U_1^*) = \left[\frac{1}{1+(0{,}6-1+1)^2}\right]^{0{,}42*4} = 0{,}6$$

Записумо результати в таблицю:

Номер компонента j	U_j^* $(j=1,4)$		$\mu_1^j(U_j^*)$		$\mu_2^j(U_j^*)$		$\mu_3^j(U_j^*)$		$\mu_4^j(U_j^*)$		$\mu_5^j(U_j^*)$	
1	0,6	1,95	0,07	0,6	0,38	0,78	0,1	0,16	0,04	0,29	0,01	0,06
2	1,74	3,38	0,04	0,18	0,09	0,59	0,27	0,97	0,3	0,85	0,11	0,66
3	1,3	2,81	0,19	0,47	0,33	0,94	0,68	0,74	0,36	0,97	0,2	0,51
4	2,15	3,3	0,46	0,76	0,55	0,61	0,1	0,73	0,84	0,97	0,62	0,88

Рисунок 3.11 – Таблиця з результатами

Визначеємо рівень захищеності за формолою:

$$\mu_S(X_j^*) = \bigvee_{i-1}^{L} \bigwedge_{j-1}^{n} \mu_i^j$$

Номер компонента j	U_j^* $(j=1,4)$		$\mu_1^j(U_j^*)$		$\mu_2^j(U_j^*)$		$\mu_3^j(U_j^*)$		$\mu_4^j(U_j^*)$		$\mu_5^j(U_j^*)$	
1	0,6	1,95	0,07	0,6	0,38	0,78	0,1	0,16	0,04	0,29	0,01	0,06
2	1,74	3,38	0,04	0,18	0,09	0,59	0,27	0,97	0,3	0,85	0,11	0,66
3	1,3	2,81	0,19	0,47	0,33	0,94	0,68	0,74	0,36	0,97	0,2	0,51
4	2,15	3,3	0,46	0,76	0,55	0,61	0,1	0,73	0,84	0,97	0,62	0,88

Рисунок 3.12 – Діапазон для першого запиту

Номер компонента j	U_j^* $(j=1,4)$		$\mu_1^j(U_j^*)$		$\mu_2^j(U_j^*)$		$\mu_3^j(U_j^*)$		$\mu_4^j(U_j^*)$		$\mu_5^j(U_j^*)$	
1	0,74	1,34	0,18	0,49	0,84	0,89	0,54	0,2	0,048	0,11	0,02	0,03
2	1,78	2,62	0,06	0,15	0,18	0,54	0,66	0,93	0,3	0,83	0,09	0,24
3	1,82	2,78	0,19	0,33	0,34	0,68	0,7	0,97	0,51	0,96	0,26	0,5
4	0,56	1,04	0,83	0,93	0,1	0,53	0,74	0,84	0,6	0,66	0,51	0,55

Рисунок 3.13 – Діапазон для другого запиту

Нечіткі еталони в контексті лінгвістичних змінних, наприклад, "рівень безпеки", є представленням ступеня належності об'єктів чи ситуацій до різних лінгвістичних термінів, таких як "низький", "середній" або "високий". Для кожного з термів може бути встановлено нечіткий еталон, що вказує на те, які значення належать до певної категорії рівня безпеки.

В результаті першого запиту маємо діапазон [0,19; 0,61], що відповідає μ_1^j , та μ_2^j, тому для прийняття рішення вибирається нечіткий терм Т1та Т2 – “Низький”, “Нище середнього”, що і визначає рівень захищеності в даній роботі.

В результаті другого запиту маємо діапазон [0,19; 0,53] , що відповідає μ_1^j та μ_2^j , тому для прийняття рішення вибирається нечіткий терм Т1та Т2 – “Низький”, “Нище середнього”, що і визначає рівень захищеності в даній роботі.

3.3 Рекомендації згідно результатів оцінки безпеки

Згідно результатам експертного запиту пропонується рекомендації для покращення ситуації:

- Забезпечити доступність та зрозумілість політики безпеки для всіх працівників. Розгляньте проведення обов'язкового навчання та тестування з цього питання.
- Забезпечити регулярні оновлення політики безпеки відповідно до змін у загрозах та технологічних змінах. Визначте конкретний графік оновлень та повідомляйте співробітників.
- Покращити процедури повідомлення про події. Забезпечте ефективний механізм для виявлення та повідомлення про інциденти з безпеки.
- Розглянути посилення вимог до складності паролів та введення двофакторної аутентифікації. Забезпечте регулярну зміну паролів та надійні методи аутентифікації.
- Організувати регулярні тренінги та навчання з питань безпеки для всіх працівників, щоб підвищити їх свідомість та розуміння ризиків.

Всі вищезгадані рекомендації були створені відповідно до строгих вимог і стандартів ISO 27001.

4 ЕКОНОМІЧНА ЧАСТИНА

Виконання наукових досліджень завжди передбачає отримання результатів та вимагає витрат ресурсів. Отримані результати відкривають нові можливості для подальшого вдосконалення технологій, процесів та програмного забезпечення.

Дослідження на тему " Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин " відноситься до фундаментальних наукових досліджень та спрямоване на вирішення актуальних проблем у сфері оцінки безпеки. Ці дослідження мають на меті покращення наукового розуміння проблеми. Це сприяє розвитку наукових знань та теоретичній базі в цій галузі, що може призвести до виявлення нових закономірностей, корисних для практичного застосування. Для цього випадку виконаємо такі етапи робіт:

1) здійснимо проведення наукового аудиту досліджень, тобто встановлення їх наукового рівня та значимості;
2) проведемо планування витрат на проведення наукових досліджень;
3) здійснимо розрахунок рівня важливості наукового дослідження та перспективності, визначимо ефективність наукових досліджень.

4.1 Оцінювання наукового ефекту

Основними характеристиками наукового внеску науково-дослідної роботи є наступні аспекти: новизна дослідження, рівень теоретичного аналізу, перспективність результатів, розповсюдження результатів та можливість їхньої практичної реалізації. У випадку дослідження на тему " Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин " можна визначити два основні критерії оцінки наукового внеску: ступінь новизни дослідження та рівень теоретичного аналізу.

Значення показників ступеня новизни і рівня теоретичного опрацювання науково-дослідної роботи в балах наведені в табл. 4.1 та 4.2.

Таблиця 4.1 – Показники ступеня новизни науково-дослідної роботи виставлені експертами

Ступінь новизни	Характеристика ступеня новизни	Значення ступеня новизни, бали		
		Експерти (ПІБ, посада)		
		1	2	3
Принципово нова	Робота якісно нова за постановкою задачі і ґрунтується на застосуванні оригінальних методів дослідження. Результати дослідження відкривають новий напрям в даній галузі науки і техніки. Отримані принципово нові факти, закономірності; розроблена нова теорія. Створено принципово новий пристрій, спосіб, метод	0	0	0
Нова	Отримана нова інформація, яка суттєво зменшує невизначеність наявних значень (по-новому або вперше пояснені відомі факти, закономірності, впроваджені нові поняття, розкрита структура змісту). Проведено суттєве вдосконалення, доповнення і уточнення раніше досягнутих результатів	0	0	0
Відносно нова	Робота має елементи новизни в постановці задачі і методах дослідження. Результати дослідження систематизують і узагальнюють наявну інформацію, визначають шляхи подальших досліджень; вперше знайдено зв’язок (або знайдено новий зв’язок) між явищами. В принципі відомі положення розповсюджені на велику кількість об’єктів, в результаті чого знайдено ефективне рішення. Розроблені більш прості способи для досягнення відомих результатів. Проведена часткова раціональна модифікація (з ознаками новизни)	28	31	25
Традиційна	Робота виконана за традиційною методикою. Результати дослідження мають інформаційний характер. Підтверджені або поставлені під сумнів відомі факти та твердження, які потребують перевірки. Знайдено новий варіант рішення, який не дає суттєвих переваг в порівнянні з існуючим	0	0	0
Не нова	Отримано результат, який раніше зафіксований в інформаційному полі, та не був відомий авторам	0	0	0
Середнє значення балів експертів		28		

Згідно отриманого середнього значення балів експертів ступінь новизни характеризується як відносно нова, тобто отримана нова інформація, яка суттєво зменшує невизначеність наявних знань (по-новому або вперше

пояснені відомі факти, закономірності, розкрита структура змісту) та проведено доповнення і уточнення раніше досягнутих результатів.

Таблиця 4.2 – Показники рівня теоретичного опрацювання науково-дослідної роботи виставлені експертами

Характеристика рівня теоретичного опрацювання	Значення показника рівня теоретичного опрацювання, бали		
	Експерт (ПІБ, посада)		
	1	2	3
Відкриття закону, розробка теорії	0	0	0
Глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу	62	66	60
Розробка способу (алгоритму, програми), пристрою, отримання нової речовини	0	0	0
Елементарний аналіз зв'язків між фактами та наявною гіпотезою, класифікація, практичні рекомендації для окремого випадку тощо	0	0	0
Опис окремих елементарних фактів, викладення досвіду, результатів спостережень, вимірювань тощо	0	0	0
Середнє значення балів експертів	62,7		

Згідно отриманого середнього значення балів експертів рівень теоретичного опрацювання науково-дослідної роботи характеризується як глибоке опрацювання проблеми: багатоаспектний аналіз зв'язків, взаємозалежності між фактами з наявністю пояснень, наукової систематизації з побудовою евристичної моделі або комплексного прогнозу.

Показник, який характеризує рівень наукового ефекту, визначаємо за формулою [38]:

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор},$$

де $k_{нов}, k_{теор}$ - показники ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи, $k_{нов} =$ 53,7, $k_{теор} =$ 62,7 балів;

0,6 та 0,4 – питома вага (значимість) показників ступеня новизни та рівня теоретичного опрацювання науково-дослідної роботи.

$$E_{нау} = 0,6 \cdot k_{нов} + 0,4 \cdot k_{теор} \quad = 0,6 \cdot 53,7 + 0,4 \cdot 62,7 = 57,3 \text{ балів.}$$

Визначення характеристики показника $E_{нау}$ проводиться на основі висновків експертів виходячи з граничних значень, які наведені в табл. 4.3.

Таблиця 4.3 – Граничні значення показника наукового ефекту

Досягнутий рівень показника	Кількість балів
Високий	70…100
Середній	50…69
Достатній	15…49
Низький (помилкові дослідження)	1…14

Відповідно до визначеного рівня наукового ефекту проведеної науково-дослідної роботи на тему " Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин ", даний рівень становить 57,3 балів і відповідає статусу - середній рівень. Тобто у даному випадку можна вести мову про потенційну фактичну ефективність науково-дослідної роботи.

4.2 Розрахунок витрат на здійснення науково-дослідної роботи

Витрати, пов’язані з проведенням науково-дослідної роботи на тему " Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин ", під час планування, обліку і калькулювання собівартості науково-дослідної роботи групуємо за відповідними статтями.

4.2.1 Витрати на оплату праці

До статті «Витрати на оплату праці» належать витрати на виплату основної та додаткової заробітної плати керівникам відділів, лабораторій, секторів і груп, науковим, інженерно-технічним працівникам, конструкторам,

технологам, креслярам, копіювальникам, лаборантам, робітникам, студентам, аспірантам та іншим працівникам, безпосередньо зайнятим виконанням конкретної теми, обчисленої за посадовими окладами, відрядними розцінками, тарифними ставками згідно з чинними в організаціях системами оплати праці.

Основна заробітна плата дослідників

Витрати на основну заробітну плату дослідників ($З_о$) розраховуємо у відповідності до посадових окладів працівників, за формулою [38]:

$$З_о = \sum_{i=1}^{k} \frac{M_{ni} \cdot t_i}{T_p}, \quad (4.2)$$

де k – кількість посад дослідників залучених до процесу досліджень;

M_{ni} – місячний посадовий оклад конкретного дослідника, грн;

t_i – число днів роботи конкретного дослідника, дн.;

T_p – середнє число робочих днів в місяці, T_p=21 дні.

$$З_о = 17400{,}00 \cdot 21 / 21 = 17400{,}00 \; грн.$$

Проведені розрахунки зведемо до таблиці 4.4.

Таблиця 4.4 – Витрати на заробітну плату дослідників

Найменування посади	Місячний посадовий оклад, грн	Оплата за робочий день, грн	Число днів роботи	Витрати на заробітну плату, грн
Керівник проекту	17 400,00	828,57	21	17 400,00
Системний адміністратор	17 150,00	816,67	10	8 166,7
Спеціаліст з безпеки	17 050,00	811,90	18	14 614,2
Всього				40 180,9

Основна заробітна плата робітників

Витрати на основну заробітну плату робітників ($З_р$) за відповідними найменуваннями робіт НДР на тему " Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин " розраховуємо за формулою:

$$З_р = \sum_{i=1}^{n} C_i \cdot t_i \quad , \tag{4.3}$$

де C_i – погодинна тарифна ставка робітника відповідного розряду, за виконану відповідну роботу, грн/год;

t_i – час роботи робітника при виконанні визначеної роботи, год.

Погодинну тарифну ставку робітника відповідного розряду C_i можна визначити за формулою:

$$C_i = \frac{M_M \cdot K_i \cdot K_c}{T_p \cdot t_{зм}} \quad , \tag{4.4}$$

де M_M – розмір прожиткового мінімуму працездатної особи, або мінімальної місячної заробітної плати (в залежності від діючого законодавства), приймемо *Мм*=6700,00 грн;

K_i – коефіцієнт міжкваліфікаційного співвідношення для встановлення тарифної ставки робітнику відповідного розряду [38];

K_c – мінімальний коефіцієнт співвідношень місячних тарифних ставок робітників першого розряду з нормальними умовами праці виробничих об’єднань і підприємств до законодавчо встановленого розміру мінімальної заробітної плати.

T_p – середнє число робочих днів в місяці, приблизно T_p = 21 дн;

$t_{зм}$ – тривалість зміни, год.

$C_1 = 6700{,}00 \cdot 1{,}10 \cdot 1{,}65 / (21 \cdot 8) = 72{,}38$ *грн.*

$З_{р1} = 72{,}38 \cdot 2{,}5 = 180{,}95$ *грн.*

Таблиця 4.5 – Величина витрат на основну заробітну плату робітників

Найменування робіт	Тривалість роботи, год	Розряд роботи	Тарифний коефіцієнт	Погодинна тарифна ставка, грн	Величина оплати на робітника грн
Визначення можливих проблем для оцінювання безпеки	2,5	2	1,10	72,38	180,95
Розробка експертних запитів	8,5	3	1,35	88,83	755,05
Практичне застосування моделі	18	4	1,50	98,71	1 776,78
Формування рекомендацій на основі результатів	16	2	1,10	72,38	1 158,08
Всього					3 870,86

Додаткова заробітна плата дослідників та робітників

Додаткову заробітну плату розраховуємо як 10 … 12% від суми основної заробітної плати дослідників та робітників за формулою:

$$З_{дод} = (З_о + З_р) \cdot \frac{Н_{дод}}{100\%}, \quad (4.5)$$

де $Н_{дод}$ – норма нарахування додаткової заробітної плати. Приймемо 12%.

$З_{дод}$ = (40180,9+ 3870,86) · 12 / 100% = 5286,21 грн.

4.2.2 Відрахування на соціальні заходи

Нарахування на заробітну плату дослідників та робітників розраховуємо як 22% від суми основної та додаткової заробітної плати дослідників і робітників за формулою:

$$З_н = (З_о + З_р + З_{дод}) \cdot \frac{Н_{зп}}{100\%} \quad , \qquad (4.6)$$

де $Н_{зп}$ – норма нарахування на заробітну плату приймаємо 22%.

Зн = (40180,9 + 3870,86 + 5286,21) · 22 / 100% = 10854,35 грн.

4.2.3 Сировина та матеріали

До статті «Сировина та матеріали» належать витрати на сировину, основні та допоміжні матеріали, інструменти, пристрої та інші засоби і предмети праці, які придбані у сторонніх підприємств, установ і організацій та витрачені на проведення досліджень за темою "Методи захисту від атак на смарт-контракти в блокчейні Ethereum".

Витрати на матеріали на даному етапі проведення досліджень в основному пов’язані з використанням моделей елементів та моделювання роботи і досліджень за допомогою комп’ютерної техніки та створення експериментальних математичних моделей або програмного забезпечення, тому дані витрати формуються на основі витратних матеріалів характерних для офісних робіт.

Витрати на матеріали ($М$), у вартісному вираженні розраховуються окремо по кожному виду матеріалів за формулою:

$$М = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j - \sum_{j=1}^{n} В_j \cdot Ц \quad , \qquad (4.7)$$

де $Н_j$ – норма витрат матеріалу j-го найменування, кг;

n – кількість видів матеріалів;

$Ц_j$ – вартість матеріалу j-го найменування, грн/кг;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ = *1,1 … 1,15*);

$В_j$ – маса відходів j-го найменування, кг;

$Ц_{вj}$ – вартість відходів *j*-го найменування, грн/кг.

$M_1 = 1,0 \cdot 225,00 \cdot 1,1 - 0 \cdot 0 = 247,50$ *грн.*

Проведені розрахунки зведемо до таблиці 4.6.

Таблиця 4.6 – Витрати на матеріали

Найменування матеріалу, марка, тип, сорт	Ціна за 1 кг, грн	Норма витрат, кг	Величина відходів, кг	Ціна відходів, грн/кг	Вартість витраченого матеріалу, грн
Папір канцелярський офісний (А4)	225,00	1,0	0	0	247,50
Папір для заміток (А5)	116,00	2,0	0	0	255,20
Начиння канцелярське	195,00	1,0	0	0	214,50
Органайзер офісний	183,00	2,0	0	0	402,60
Картридж для принтера	950,00	1,0	0	0	1045,00
Всього					2 164,80

4.2.4 Розрахунок витрат на комплектуючі

Витрати на комплектуючі *($К_в$)*, які використовують при проведенні НДР на тему "Методи захисту від атак на смарт-контракти в блокчейні Ethereum", розраховуємо, згідно з їхньою номенклатурою, за формулою:

$$К_в = \sum_{j=1}^{n} Н_j \cdot Ц_j \cdot К_j \tag{4.8}$$

де $Н_j$ – кількість комплектуючих *j*-го виду, шт.;

$Ц_j$ – покупна ціна комплектуючих *j*-го виду, грн;

$К_j$ – коефіцієнт транспортних витрат, ($К_j$ *= 1,1 … 1,15*).

$К_в = 1 \cdot 3079,00 \cdot 1,1 = 3386,90$ *грн.*

Проведені розрахунки зведемо до таблиці 4.7.

Таблиця 4.7 – Витрати на комплектуючі

Найменування комплектуючих	Кількість, шт.	Ціна за штуку, грн	Сума, грн
Зовнішній жорсткий диск 2.5" 2TB Seagate (STGD2000200)	1	3079,00	3386,90
Оперативная память Kingston Fury DDR4-3200 8192MB PC4-25600 (KF432C16BB/8)	2	1029,00	2263,80
Всього			4216,30

4.2.5 Спецустаткування для наукових (експериментальних) робіт

До статті «Спецустаткування для наукових (експериментальних) робіт» належать витрати на виготовлення та придбання спецустаткування необхідного для проведення досліджень, також витрати на їх проектування, виготовлення, транспортування, монтаж та встановлення.

Балансову вартість спецустаткування розраховуємо за формулою:

$$B_{спец} = \sum_{i=1}^{k} Ц_i \cdot C_{пр.i} \cdot K_i \quad , \tag{4.9}$$

де $Ц_i$ – ціна придбання одиниці спецустаткування даного виду, марки, грн;

$C_{пр.i}$ – кількість одиниць устаткування відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує доставку, монтаж, налагодження устаткування тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань устаткування.

$B_{спец} = 84750,00 \cdot 1 \cdot 1,1 = 93225,0$ *грн.*

Отримані результати зведемо до таблиці 4.8.

Таблиця 4.8 – Витрати на придбання спецустаткування по кожному виду

Найменування устаткування	Кількість, шт	Ціна за одиницю, грн	Вартість, грн
Ноутбук MacBook Pro 14" Silver 2021 (Z15J001WF). Apple M1	1	84 750,00	93 225,00
Всього			93 225,00

4.2.6 Програмне забезпечення для наукових (експериментальних) робіт

До статті «Програмне забезпечення для наукових (експериментальних) робіт» належать витрати на розробку та придбання спеціальних програмних засобів і програмного забезпечення, (програм, алгоритмів, баз даних) необхідних для проведення досліджень, також витрати на їх проектування, формування та встановлення.

Балансову вартість програмного забезпечення розраховуємо за формулою:

$$B_{прг} = \sum_{i=1}^{k} Ц_{iпрг} \cdot C_{прг.i} \cdot K_i \quad , \qquad (4.10)$$

де $Ц_{iпрг}$ – ціна придбання одиниці програмного засобу даного виду, грн;

$C_{прг.i}$ – кількість одиниць програмного забезпечення відповідного найменування, які придбані для проведення досліджень, шт.;

K_i – коефіцієнт, що враховує інсталяцію, налагодження програмного засобу тощо, ($K_i = 1,10…1,12$);

k – кількість найменувань програмних засобів.

$B_{прг} = 0 \cdot 1 \cdot 1,1 = 0$ грн.

Отримані результати зведемо до таблиці 4.9.

Згідно результатів, витрат на придбання програмних засобів не було.

4.2.7 Амортизація обладнання, програмних засобів та приміщень

В спрощеному вигляді амортизаційні відрахування по кожному виду обладнання, приміщень та програмному забезпеченню тощо, розраховуємо з використанням прямолінійного методу амортизації за формулою:

$$A_{обл} = \frac{Ц_б}{T_в} \cdot \frac{t_{вик}}{12}, \quad (4.11)$$

де $Ц_б$ – балансова вартість обладнання, програмних засобів, приміщень тощо, які використовувались для проведення досліджень, грн;

$t_{вик}$ – термін використання обладнання, програмних засобів, приміщень під час досліджень, місяців;

$T_в$ – строк корисного використання обладнання, програмних засобів, приміщень тощо, років.

$A_{обл} = (8200{,}00 \cdot 1) / (2 \cdot 12) = 341{,}67$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.10 – Амортизаційні відрахування по кожному виду обладнання

Найменування обладнання	Балансова вартість, грн	Строк корисного використання, років	Термін використання обладнання, місяців	Амортизаційні відрахування, грн
Робоче місце спеціаліста	8200,00	2	1	341,67
Офісна оргтехніка	9600,00	4	1	200,00
Дослідницька лабораторія	500000,00	20	1	2 083,33
Всього				2 625,00

4.2.8 Паливо та енергія для науково-виробничих цілей

Витрати на силову електроенергію (B_e) розраховуємо за формулою:

$$B_e = \sum_{i=1}^{n} \frac{W_{yi} \cdot t_i \cdot Ц_e \cdot K_{вni}}{\eta_i}, \quad (4.12)$$

де W_{yi} – встановлена потужність обладнання на визначеному етапі розробки, кВт;

t_i – тривалість роботи обладнання на етапі дослідження, год;

$Ц_e$ – вартість 1 кВт-години електроенергії, грн; (вартість електроенергії визначається за даними енергопостачальної компанії), приймемо $Ц_e = 8,19$ грн;

$K_{вni}$ – коефіцієнт, що враховує використання потужності, $K_{вni} < 1$;

η_i – коефіцієнт корисної дії обладнання, $\eta_i < 1$.

$B_e = 0,04 \cdot 250,0 \cdot 8,19 \cdot 0,95 / 0,97 = 60,72$ *грн.*

Проведені розрахунки зведемо до таблиці.

Таблиця 4.11 – Витрати на електроенергію

Найменування обладнання	Встановлена потужність, кВт	Тривалість роботи, год	Сума, грн
Ноутбук MacBook Pro 14" Silver 2021 (Z15J001WF). Apple M1	0,04	250,0	80,21
Робоче місце програміста	0,10	250,0	200,53
Офісна оргтехніка	0,60	5,0	24,06
Всього			304,80

4.2.9 Службові відрядження

До статті «Службові відрядження» дослідної роботи на тему «Захищена система збирання та аналізування даних для спеціальних задач. Частина 1. Підсистема аналізу» належать витрати на відрядження штатних працівників, працівників організацій, які працюють за договорами цивільно-правового характеру, аспірантів, зайнятих розробленням досліджень, відрядження, пов'язані з проведенням випробувань машин та приладів, а також витрати на відрядження на наукові з'їзди, конференції, наради, пов'язані з виконанням конкретних досліджень.

Витрати за статтею «Службові відрядження» розраховуємо як 20…25% від суми основної заробітної плати дослідників та робітників за формулою:

$$B_{св} = (З_о + З_р) \cdot \frac{Н_{св}}{100\%}, \quad (4.13)$$

де $Н_{св}$ – норма нарахування за статтею «Службові відрядження», приймемо $Н_{св}$ = 20%.

$B_{св} = (40180,9 + 3870,86) \cdot 20 / 100\% = 8810,35$ *грн.*

4.2.10 Витрати на роботи, які виконують сторонні підприємства, установи і організації

Витрати за статтею «Витрати на роботи, які виконують сторонні підприємства, установи і організації» відсутні.

4.2.11 Інші витрати

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками.

Витрати за статтею «Інші витрати» розраховуємо як 50…100% від суми основної заробітної плати дослідників та робітників за формулою:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (4.14)$$

де $Н_{ів}$ – норма нарахування за статтею «Інші витрати», приймемо $Н_{ів}$ = 70%.

$I_в$ = (40180,9+ 3870,86) · 70 / 100% = 30836,23 грн.

4.2.12 Накладні (загальновиробничі) витрати

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов'язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов'язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов'язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін.

Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуємо як 100…150% від суми основної заробітної плати дослідників та робітників за формулою:

$$В_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (4.15)$$

де $Н_{нзв}$ – норма нарахування за статтею «Накладні (загальновиробничі) витрати», приймемо $Н_{нзв}$ = 100%.

$В_{нзв}$ = (47464,29 + 3870,86) · 100 / 100% = 51335,15 грн.

Витрати на проведення науково-дослідної роботи на тему "Методи захисту від атак на смарт-контракти в блокчейні Ethereum"розраховуємо як суму всіх попередніх статей витрат за формулою:

$$В_{заг} = З_о + З_р + З_{дод} + З_н + М + К_в + В_{спец} + В_{прг} + А_{обл} + В_е + В_{св} + В_{сп} + І_в + В_{нзв} \quad (4.16)$$

$B_{заг}$=

17400+760,03+5286,21+10854,35+2164,8+4216,3+93225+0+1492,92+304,8+8810,35+30836,23+51335,15 = 248 391,34 грн.

Загальні витрати *ЗВ* на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховується за формулою:

$$ЗВ = \frac{B_{заг}}{\eta}, \quad (4.17)$$

де η - коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи, приймемо η=0,95.

ЗВ = 248 391,34 / 0,95 = 261 464,57 грн.

4.3 Оцінювання важливості та наукової значимості науково-дослідної роботи

Оцінювання та доведення ефективності виконання науково-дослідної роботи фундаментального чи пошукового характеру є достатньо складним процесом і часто базується на експертних оцінках, тому має вірогідний характер.

Для обґрунтування доцільності виконання науково-дослідної роботи на тему “Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин” використовується спеціальний комплексний показник, що враховує важливість, результативність роботи, можливість впровадження її результатів у виробництво, величину витрат на роботу.

Комплексний показник K_P рівня науково-дослідної роботи може бути розрахований за формулою:

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t}, \quad (4.18)$$

де I – коефіцієнт важливості роботи. Приймемо $I = 4$;

n – коефіцієнт використання результатів роботи; $n = 0$, коли результати роботи не будуть використовуватись; $n = 1$, коли результати роботи будуть використовуватись частково; $n = 2$, коли результати роботи будуть використовуватись в дослідно-конструкторських розробках; $n = 3$, коли результати можуть використовуватись навіть без проведення дослідно-конструкторських розробок. Приймемо n=2;

T_C – коефіцієнт складності роботи. Приймемо $T_C = 3$;

R – коефіцієнт результативності роботи; якщо результати роботи плануються вище відомих, то $R = 4$; якщо результати роботи відповідають відомому рівню, то $R = 3$; якщо нижче відомих результатів, то $R = 1$. Приймемо $R = 3$;

B – вартість науково-дослідної роботи, тис. грн. Приймемо *B = 230 950,26* грн;

t – час проведення дослідження. Приймемо t = 0,08 років, (1 міс.).

Визначення показників *I, n, T_C, R, B, t* здійснюється експертним шляхом або на основі нормативів [22].

$$K_P = \frac{I^n \cdot T_C \cdot R}{B \cdot t} = 4^2 \cdot 3 \cdot 3 \,/\, 261{,}46 \cdot 0{,}08 = 6{,}73.$$

Якщо $K_P > 1$, то науково-дослідну роботу на тему “ Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин можна вважати ефективною з високим науковим, технічним і економічним рівнем.

Витрати на проведення науково-дослідної роботи на тему “ Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин ” складають *261 464,57* грн. Відповідно до проведеного аналізу та розрахунків рівень науково-економічного ефекту проведеної науково-

дослідної роботи на тему “ Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин ” є середній, а дослідження актуальними, рівень доцільності виконання науково-дослідної роботи $K_P > 1$, що свідчить про потенційну ефективність з високим науковим, технічним і економічним рівнем.

Висновки до розділу

Згідно проведених досліджень рівень комерційного потенціалу розробки за темою «Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин» становить 57,3 бали, що, свідчить про комерційну важливість проведення даних досліджень оскільки рівень комерційного потенціалу розробки високий.

Отже можна зробити висновок про доцільність проведення науково-дослідної роботи за темою «Інформаційна технологія моніторингу безпеки даних програмного забезпечення».

ВИСНОВКИ

В контексті даної магістерської досліджено суттєвий аспект управління інформаційною безпекою, а саме – моделі оцінювання рівня безпеки за допомогою інтервальних нечітких множин.

Проведені дослідження дали висновок про великий потенціал цього підходу для вдосконалення процесів оцінювання та управління безпекою інформації в організаціях. Серед ключових внесків роботи варто відзначити розробку та використання інтервальних нечітких множин для визначення рівня безпеки.

Цей підхід дозволяє враховувати неоднозначність та невизначеність у визначенні безпеки інформації, що є важливим умовою в умовах сучасного кіберзлочинності та технічних загроз.

Проведені експерименти та аналіз результатів підтверджують ефективність запропонованої моделі оцінювання. Використання інтервальних нечітких множин дозволяє уникнути жорсткості традиційних методів оцінювання та створює можливість для більш гнучкого та адаптивного управління безпекою інформації.

Результати дослідження можуть служити основою для розвитку нових методів оцінювання рівня безпеки в умовах зростаючих викликів та складності інформаційного середовища.

Важливо врахувати, що дана модель не є універсальною, і її ефективність може залежати від конкретних умов та контексту використання. У цілому, метою цієї роботи є сприяння подальшому розвитку та вдосконаленню стратегій управління безпекою інформації, з урахуванням динаміки сучасного цифрового середовища та викликів, що виникають у зв'язку з цим.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Liang, Q. Interval Type-2 fuzzy logic systems: theory and design [Text] / Q. Liang, J. M. Mendel // IEEE Trans. on Fuzzy Syst. – 2000. –V. 8. – P. 535–550.
2. Кондратенко, Н. Р. Дослідження адекватності інтервальних нечітких моделей типу-2 в задачах ідентифікації складних об’єктів [Текст] / Н. Р. Кондратенко, О. О. Снігур // Системні дослідження та інформаційні технології. – 2019. – № 4. – С. 94–104
3. Бабак В. П., Корченко А. Г. Інформаціна безпека та сучасні мережеві технології. Англ.-укр. слів. термінів. – К.: НАУ, 2003. - 670 с.
4. Шевченко В. Л. Несанкціонований доступ до інформаційних ресурсів ERP-системи [Електронний ресурс] / В. Л. Шевченко, В. І. Кулажський, О.
5. Методи захисту системи управління інформаційною безпекою: ДСТУ ISO/IEC 27001:2015. – 2016. – Чин. 2017.01.01. – Київ.: ДП «УкрНДНЦ», 2016. – 22с.
6. Kruglov V.V., Borisov V.V., FedulovA.S.(2012) Fuzzy models and networks. Hotline -Telecom,. 284p
7. Нечітка модель оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем — Режим доступу: https://tit.dut.edu.ua/index.php/telecommunication/article/view/2311
8. Захист March 2017 Web Server Survey [Електронний ресурс]. — 2017. — Режим доступу: http://news.n etcraft.com/archives/2017/03/24/march-2017 -web-server-survey.html. (дата звернення: 27.09.2022)
9. Ekhlakov Yu.P.(2014) Fuzzy model for assessing the risks of software product promotion.Business informatics.3 (29):P. 69-78.REGMIC
10. Давиденко А. Н. Проблеми аналізу та моделювання національних та міжнародних критеріїв оцінки безпеки інформації // Зб. наук. пр. Ін-

ту пробл. Моделювання в енергетиці НАН України. – Львів: Світ, 2002. – Вип 18. – С.171-175.

11. International standard BS ISO/IEC 27005:2008, 2008-06-15.
12. ISO / IEC 27005 - Information security risk management
13. James J. Cebula A Taxonomy of Operational Cyber Security Risks / James J. Cebula, Lisa R. Young. – Hanscom AFB, MA: Carnegie Mellon University. – 47 p.
14. Maria Garnaeva. Kaspersky Security Bulletin 2015. Overall statistics for2015 / [Maria Garnaeva, Jornt van der Wiel, Denis Markushin and etc.]. – Kaspersky Lab, 2015. – 86p
15. RiskWatch International. Global Leader in Risk Assessment Solutions [Электронный ресурс]. – Режим доступа: www.riskwatch.com.
16. Thomas R. Peltier. Facilitated Risk Analysis Process (FRAP) [Электронный ресурс]. – Режим доступа: www.ittoday.info/AIMS/DSM/85- 01-21.pdf
17. Visintine V. An Introduction to Information Risk Assessment / Visintine V. – Bethesda, Maryland: SANS Institute, 2009. – 13 p.
18. Wayne Jansen. Directions in Security Metrics Research , NISTIR 7564, April 2009 [Електронний ресурс] // NIST.gov - Computer Security Division - Computer Security Resource Center [сайт] / Wayne Jansen ; Computer Security Division , Information Technology Laboratory , National Institute of Standards and Technology — Режим доступу: http://csrc.nist.gov/publications/nistir/ir7564/nistir7564_metrics-research.pdf
19. Про інформацію: [закон України: офіц. текст: за станом на 2 жовтня 1992 р., із змінами, внесеними Законом України від 10 січня 2012р.]: [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12.

20. Козловський В. О., Лесько О. Й., Кавецький В. В. Методичні вказівки до виконання економічної частини магістерських кваліфікаційних робіт. Вінниця : ВНТУ, 2021. - 42 с.
21. Про основи національної безпеки України: [закон України: офіц. текст: за станом на 19 червня 2003р., із змінами, внесеними Законом України від 13 жовтня 2012 р.] // Відомості Верховної Ради України (ВВР). – 2012. – № 7. – ст. 53.
22. Світлична В.Ю., Інформаційна безпека: багатогранність сутності, види загроз та шляхи забезпечення http://economy.kname.edu.ua/images/files/publishing/360-369_%D0%A1%D0%B2%D1%96%D1%82%D0%BB%D0%B8%D1%87%D0 %BD%D0%B0_2.pdf
23. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки. – 2008. – № 10. – С. 220-225.

ДОДАТКИ

Додаток А

ПРОТОКОЛ ПЕРЕВІРКИ МАГІСТЕРСЬКОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Моделі оцінювання рівня безпеки інформації за допомогою інтервальних нечітких множин

Автор роботи: Лисенко Євгеній Максимович

Тип роботи: магістерська кваліфікаційна робота

Підрозділ кафедра захисту інформації ФІТКІ
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність – 91,13 %. Схожість – 8,87 %.

Аналіз звіту подібності (відмітити потрібне):

√ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

□ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Валентина КАПЛУН
(підпис)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Євгеній ЛИСЕНКО
(підпис)

Керівник роботи _____ Наталія КОНДРАТЕНКО

Додаток В

ІЛЮСТРАТИВНА ЧАСТИНА
СИСТЕМА АВТОМАТИЗОВАНОГО КЕРУВАННЯ БЕЗПЕКОЮ ЗАСТОСУНКІВ У ХМАРНОМУ СЕРЕДОВИЩІ. ЧАСТИНА 1. ПІДСИСТЕМА МОНІТОРИНГУ ЗАСТОСУНКІВ

СХЕМА ОБРОБКИ ДАНИХ ЗА НЕЧІТКОЮ МОДЕЛЮ З БАЛЬНОЮ ШКАЛОЮ

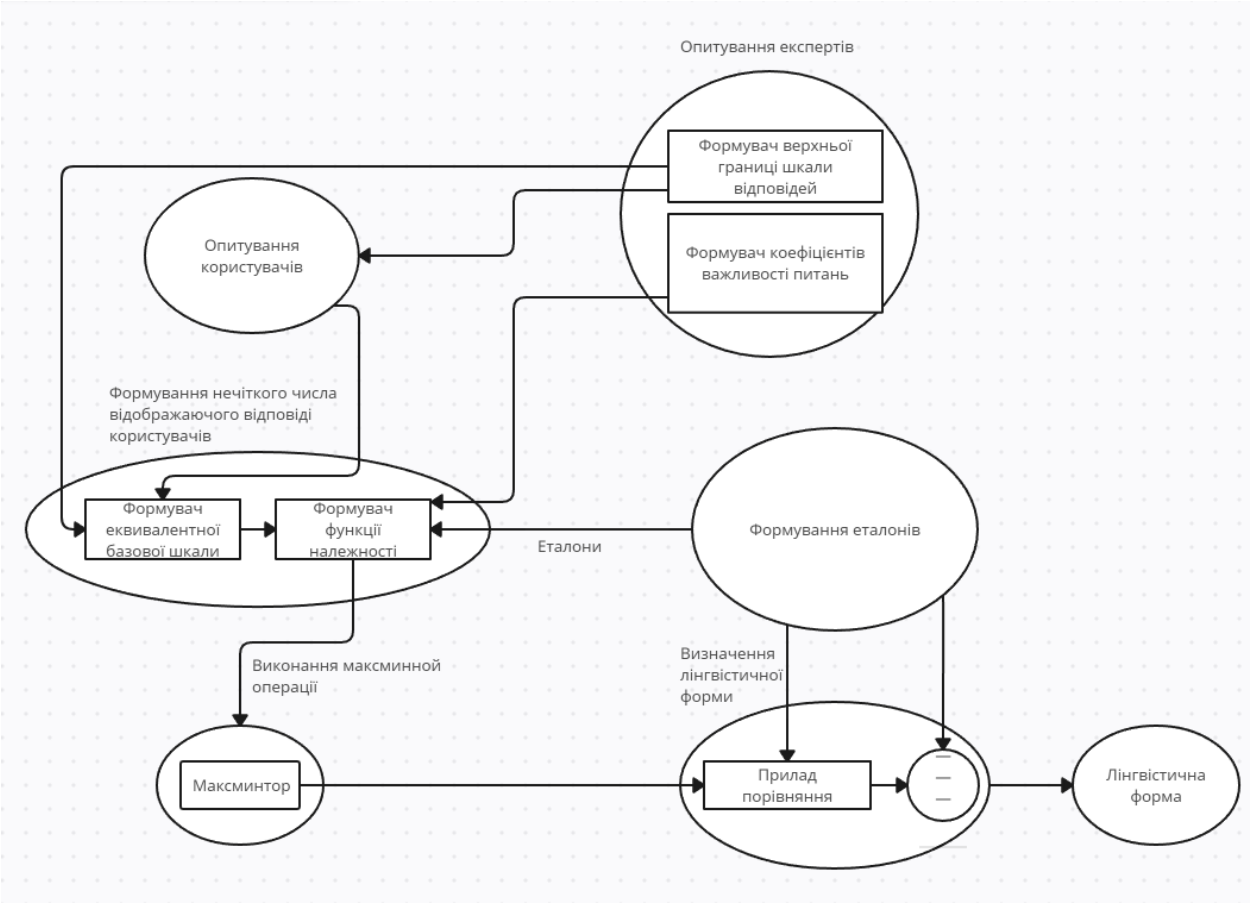
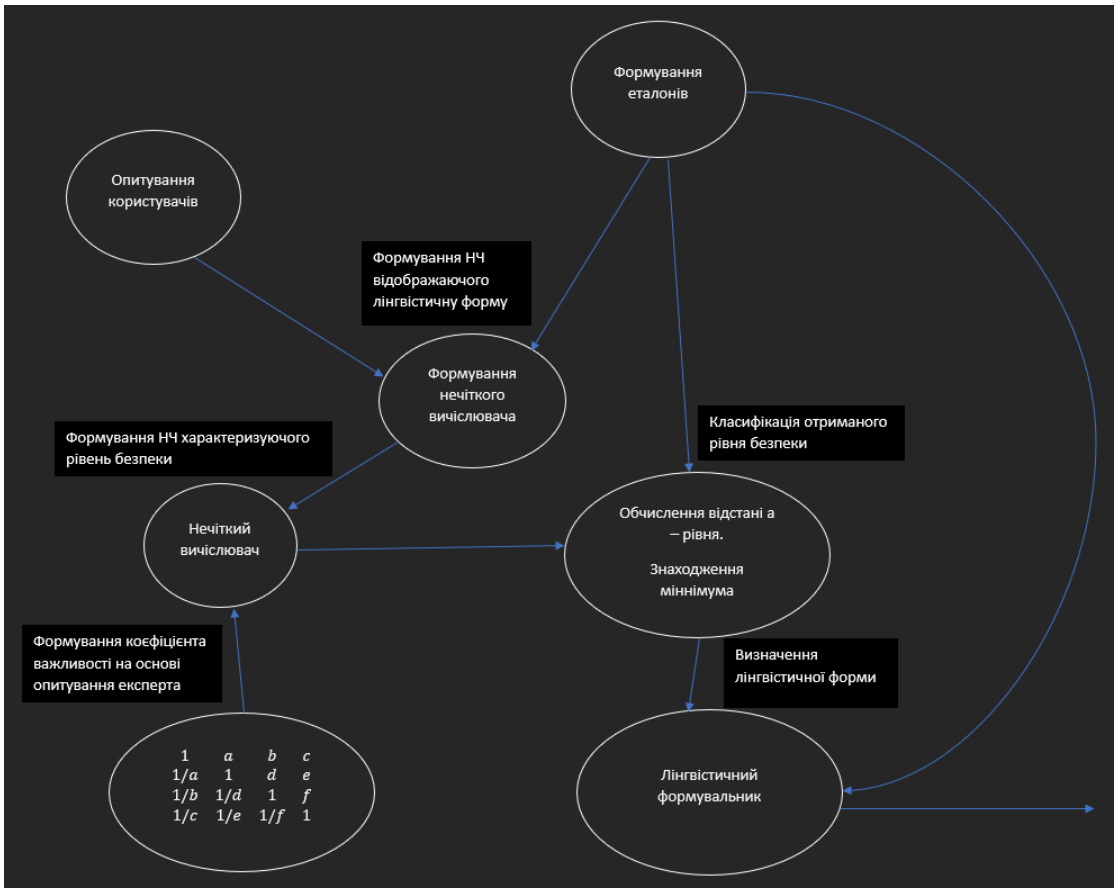
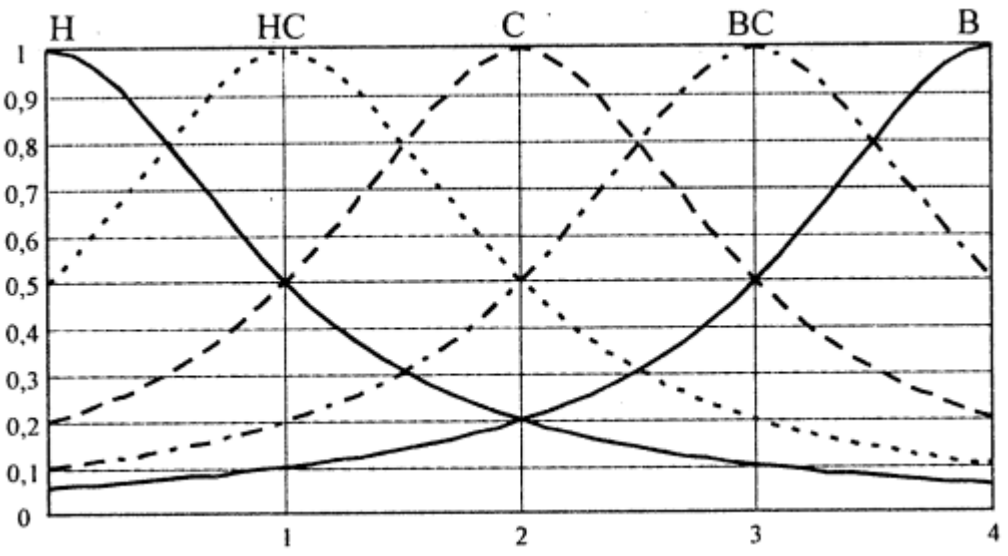


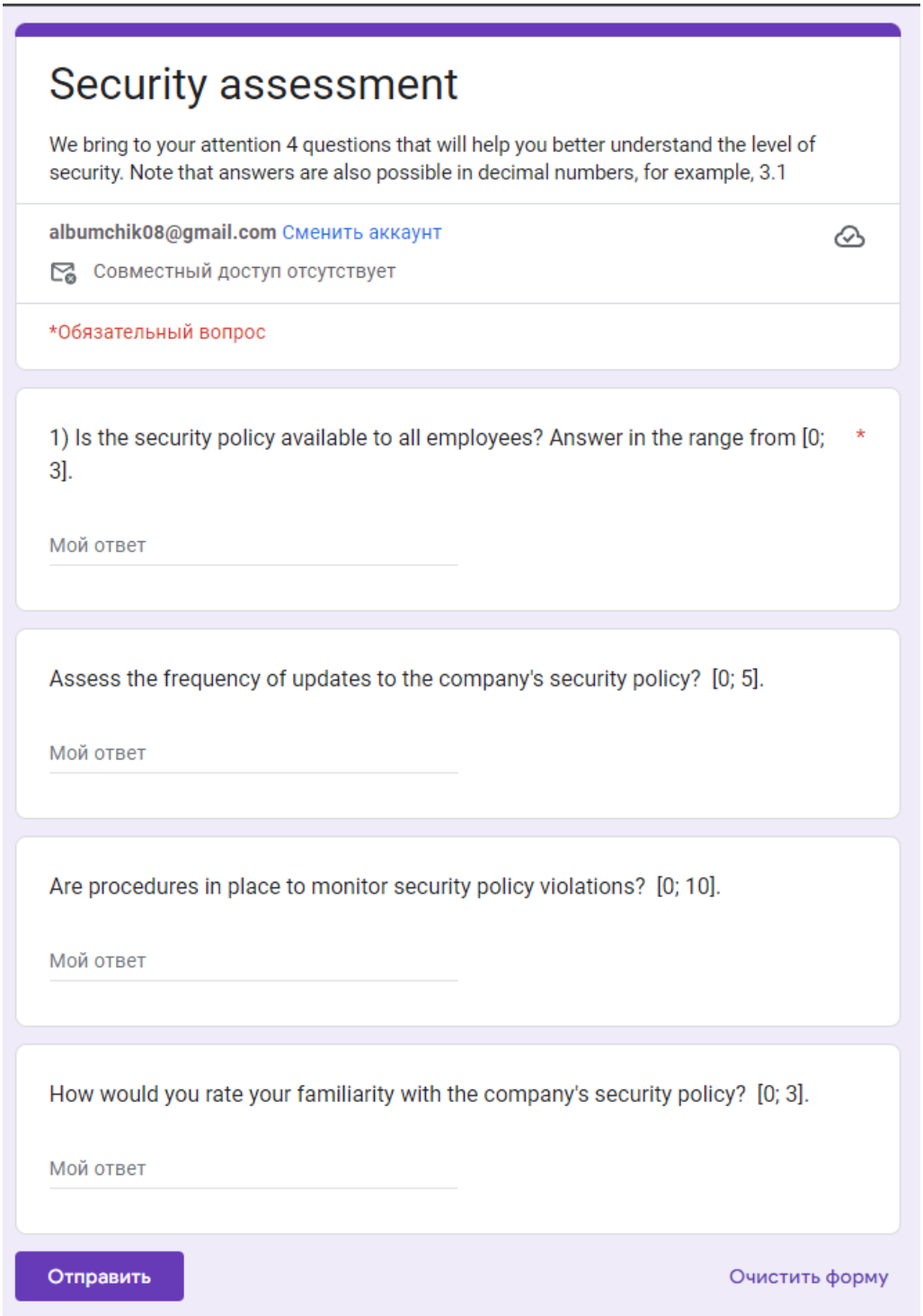
СХЕМА ОБРОБКИ ДАНИХ ЗА НЕЧІТКОЮ МОДЕЛЮ З ЛІНГВІСТИЧНОЮ ШКАЛОЮ



ГРАФІЧНЕ ПРЕДСТАВЛЕННЯ ЕТАЛОНИХ НЕЧІТКИХ МНОЖИН



АНКЕТА АНОНІМНОГО ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ



Security assessment

We bring to your attention 4 questions that will help you better understand the level of security. Note that answers are also possible in decimal numbers, for example, 3.1

albumchik08@gmail.com Сменить аккаунт

Совместный доступ отсутствует

*Обязательный вопрос

1) Is the security policy available to all employees? Answer in the range from [0; 3]. *

Мой ответ

Assess the frequency of updates to the company's security policy? [0; 5].

Мой ответ

Are procedures in place to monitor security policy violations? [0; 10].

Мой ответ

How would you rate your familiarity with the company's security policy? [0; 3].

Мой ответ

Отправить

Очистить форму

ВИКОРИСТАНІ РАНЖОВАНІ ЕКСПЕРТНІ ЗАПИТИ

- як ви оцінюєте процедури повідомлення про події з безпекою?	[0-5]	- як ви оцінюєте своє ознайомлення з політикою безпеки компанії?	[0-3]
- як ви оцінюєте складність стандарту паролів від робочої пошти співробітників?	[0-4]	- оцініть частоту проведення оновлення політики безпеки компанії.	[0-5]
- як ви оцінюєте процедуру двофакторної аутентифікації для доступу до робочої пошти співробітників?	[0-4]	- як ви оцінюєте процедури для моніторингу порушень політики безпеки?	[0-10]
- як часто ви змінюєте пароль до внутрішніх систем?	[0-6]	- чи доступна політика безпеки для всіх співробітників?	[0-4]

МАТРИЦЯ ПОПАРНИХ ПОРІВНЯНЬ

Матриця попарного порівняння

Питання	П1	П2	П3	П4
П1	1	3	7	9
П2	1/3	1	3	7
П3	1/7	1/3	1	3
П4	1/9	1/7	1/3	1

Нормалізації матриці

Питання	П1	П2	П3	П4
П1	1	75	87,5	90
П2	25	1	75	87,5
П3	12,5	25	1	75
П4	10	12,5	25	1

РЕЗУЛЬТАТИ ОБЧИСЛЕНЬ ПЕРШОГО ЗАПИТУ

j	1	2	3	4	5	6	7	8	9	10	м	σ	М - σ	М + σ
1.	1	3	1	1	2	1	3	1	1	2	1,6	0,84	0,76	2,44
2.	2	4	4	4	2	2	4	4	4	2	3,2	1,03	2,17	4,23
3.	2	3	4	2	2	1	3	4	2	2	2,6	0,97	1,63	3,57
4.	4	3	4	4	3	4	3	4	4	2	3,4	0,71	2,69	4,11

РЕЗУЛЬТАТИ ОБЧИСЛЕНЬ ДРУГОГО ЗАПИТУ

j	1	2	3	4	5	6	7	8	9	10	м	σ	М - σ	М + σ
1.	1	1	2	1	1	1	2	2	1	1	1,3	0,38	0,92	1,68
2.	2	3	2	2	3	2	2	2	2	2	2,2	0,42	1,78	2,62
3.	3	2	2	2	2	3	2	2	3	2	2,3	0,48	1,82	2,78
4.	1	1	2	1	1	1	1	1	2	1	1,2	0,36	0,84	1,56