МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Метод оцінювання ризиків для систем управління інформаційною безпекою».

Виконавець: _____ Дмитро БІБІН
(підпис)

Керівник: _____ Володимир КЛИМЧУК
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Бібіна Дмитра Олексійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Метод оцінювання ризиків для систем управління інформаційною безпекою»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи: засоби аналізу і оцінювання ризиків
4. Зміст пояснювальної записки: засоби аналізу та оцінювання ризиків інформаційної безпеки, модель та методи аналізу та оцінювання ризиків інформаційної безпеки, експериментальне дослідження системи аналізу і оцінювання ризиків
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: результати дослідження ЗАОР, приклад визначення еталонних значень базових компонент, базовий алгоритм роботи систем аналізу і оцінювання ризиків ІБ, результати оцінювання ПЗ First-ЗАОР, гістограма середніх значень рівня ризику ПЗ First-ЗАОР

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Засоби аналізу та оцінювання ризиків інформаційної безпеки	12.09.2022-05.10.2022	Виконано
4	Модель та методи аналізу та оцінювання ризиків інформаційної безпеки	06.10.2022-15.10.2022	Виконано
5	Експериментальне дослідження системи аналізу і оцінювання ризиків	17.10.2022-05.11.2022	Виконано
6	Охорона праці	07.11.2022-12.11.2022	Виконано
7	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
8	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколиш-нього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Володимир КЛИМЧУК
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Дмитро БІБІН
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Метод оцінювання ризиків для систем управління інформаційною безпекою» містить 93 сторінки, 6 рисунків, 31 таблиця, 46 використаних джерел.

АВТОМАТИЗОВАНА СИСТЕМА, ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНИЙ АКТИВ, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ РЕСУРСИ, ІНФОРМАЦІЙНА СИСТЕМА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, КОРТЕЖНА МОДЕЛЬ БАЗОВИХ ХАРАКТЕРИСТИК РИЗИКУ, КОМПЛЕКСНА ЕКСПЕРТНА СИСТЕМА, ЛІНГВІСТИЧНА ЗМІННА, НЕЧІТКІ АРИФМЕТИЧНІ ОПЕРАЦІЇ, НЕЧІТКА МНОЖИНА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, НЕСАНКЦІОНОВАНА МОДИФІКАЦІЯ, НЕЧІТКІ ЧИСЛА, ОЦІНКА РИЗИКУ, ЗАСОБИ АНАЛІЗУ І ОЦІНЮВАННЯ РИЗИКІВ.

Мета кваліфікаційної роботи - розробка гнучких у використанні методів та засобів аналізу та оцінювання ризику (ЗАОР) ІБ, як на основі статистичних даних, так і на основі експертних оцінок, зроблених у нечітко визначеному слабо формалізованому середовищі.

Об'єкт – процес аналізу та оцінювання ризиків інформаційної безпеки;

Предмет – моделі, методи, системи, методики та програмні засоби аналізу та оцінювання ризиків у сфері інформаційної безпеки.

Наукова новизна отриманих результатів - набули подальшого розвитку методи аналізу та оцінювання ризику (ЗАОР) ІБ.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АС – автоматизована система;

ЗІ – захист інформації;

ІА – інформаційний актив;

ІБ – інформаційна безпека;

ІР – інформаційні ресурси;

ІС – інформаційна система;

ІТ – інформаційні технології;

КМР – кортежна Модель базових характеристик ризику;

КЕС – комплексна експертна система;

ЛП – лінгвістична змінна;

НАО – нечіткі арифметичні операції;

НМ – нечітка множина;

НСД – несанкціонований доступ;

НСМ – несанкціонована модифікація;

НЧ – нечіткі числа;

ОР – оцінка ризику;

ПК – персональний комп'ютер;

ПЗ – програмне забезпечення;

РІС – ресурс інформаційної системи;

РП – ризикоутворюючий потенціал;

ЗАОР – засоби аналізу і оцінювання ризиків;

СЗІ – система захисту інформації;

СМІБ – система менеджменту інформаційної безпеки;

ФП – функція приладдя;

ЦО – цільові об'єкти.

ВСТУП

Актуальність теми. Актуальність стрімкого розвитку IT-інфраструктури підприємств незмінно тягне за собою неконтрольоване зростання кількості загроз та вразливостей інформаційних ресурсів (ІР). У цих умовах оцінювання ризиків інформаційної безпеки (ІБ) дозволяє визначити необхідний рівень захисту інформації (ЗІ), здійснити його підтримку та розробити стратегію розвитку інформаційної структури об'єкта захисту. Аналіз та оцінювання ризиків є необхідною умовою при створенні системи управління ризиками та плану робіт із забезпечення ІБ. Відповідно до рекомендацій стандарту ISO/IEC 27001 для забезпечення ІБ на підприємстві будь-якої форми власності необхідно впроваджувати систему управління інформаційною безпекою (СМІБ). Основою такого стандарту є менеджмент ризиків, під яким мається на увазі аналіз, оцінювання та обробка ризиків ІБ. На сьогоднішній день існує безліч засобів аналізу та оцінювання ризику (ЗАОР), що використовуються для оцінювання, які представлені в досить широкому спектрі, що починається нормативними документами (стандартами) і конкретними програмними додатками [1-30].

Метою кваліфікаційної роботи є розробка гнучких у використанні методів та засобів аналізу та оцінювання ризику (ЗАОР) ІБ, як на основі статистичних даних, так і на основі експертних оцінок, зроблених у нечітко визначеному слабо формалізованому середовищі.

Для досягнення поставленої мети необхідно вирішити такі **основні завдання**:

1) Проаналізувати та дослідити базові поняття, пов'язані з ризиком, існуючі стандарти, методи, методики, методології та програмні ЗАОР, з метою визначення набору базових характеристик, що використовуються для створення і вибору найбільш ефективного інструментарію розв'язання відповідних завдань ЗІ;

2) На основі отриманих базових характеристик розробити модель кортежної моделі базових характеристик КМР, що дозволяє динамічно визначати набори величин і таким чином забезпечити гнучкість відповідних ЗАОР ІБ, що розробляються;

3) На основі запропонованої моделі КМР розробити методи аналізу та оцінювання ризиків ІБ, що дозволить створювати ефективні засоби оцінювання, що використовують як вхідні дані динамічно змінювані набори детермінованих і нечітко визначених базових характеристик;

Об'єкт – процес аналізу та оцінювання ризиків інформаційної безпеки;

Предмет – моделі, методи, системи, методики та програмні засоби аналізу та оцінювання ризиків у сфері інформаційної безпеки.

Наукова новизна отриманих результатів. Набули подальшого розвитку методи аналізу та оцінювання ризику (ЗАОР) ІБ.

Практичне значення отриманих результатів.

На основі запропонованої моделі КМР можна створювати ефективні засоби оцінювання ризиків ІБ, що використовують як вхідні дані динамічно змінювані набори детермінованих і нечітко визначених базових характеристик.

РОЗДІЛ 1
ЗАСОБИ АНАЛІЗУ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Аналіз визначень ризику

У літературі зустрічається визначення ризику як дія чи діяльність: реалізація якої ставить під загрозу задоволення якоїсь досить важливої потреби; яка полягає в невизначеності її результату та можливих несприятливих наслідках у разі неуспіху для суб'єкта в тому чи іншому відношенні загрожує суб'єкту втратою (програшем, травмою, збитком); в умовах невизначеності та діяльність суб'єкта, пов'язана з подоланням невизначеності; навмання в надії на щасливий результат [1].

Як відомо, дія чи діяльність, так само як і ймовірність (вимірювана чи розрахована), пов'язані з виникненнями будь-яких характерних для них подій. Також відомо, що будь-які дії призводять до подій та наслідків, які можуть бути як потенційними «позитивними» можливостями, так і «небезпеками». Виходячи зі сказаного, у цьому контексті простежується спільність зазначених понять.

Наступну базову характеристику можна визначити як подію, яка може статися, або не відбутися або очікування її наступу (потенційно небажаних впливів на актив або його характеристики, які можуть бути наслідком деякого минулого, сьогодення чи майбутньої події).

У більшості зазначених джерел [1, 2, 4-8] ризик часто відображається ймовірністю або пов'язаними з нею поняттями, наприклад, ймовірність, що вимірюється або розраховується: втрат, появи несприятливого результату або події (наприклад, в результаті якого можливі непередбачені втрати) можливості небезпеки, невдачі, отримання результату від прийнятого рішення, не досягнення мети, появи обставин, що зумовлюють невпевненість або неможливість отримання очікуваних результатів від реалізації поставленої мети зазнати збитків або упустити вигоду (кількісно вимірювана невпевненість у отриманні відповідного доходу); реалізації певної загрози, виду

та величини завданих збитків; заподіяння шкоди майну, навколишньому середовищу або життю (здоров'ю) громадян, тварин, рослин виникнення заданої загрози та потенційно несприятливих наслідків виникнення цієї загрози передбачає потенційну можливість порушення безпеки даної загрози, за допомогою якої будуть використовуватися вразливості активу або групи активів, щоб призвести до втрати та /або пошкодження майна, а також як, поєднання або комбінація ймовірності події і його наслідків. Відомо, що ймовірність пов'язана з настанням певної події, відповідно з ним тут пов'язаний і ризик.

Імовірність часто поділяють на «об'єктивну» (іноді звану фізичну) і «суб'єктивну». Під об'єктивною ймовірністю розуміється відносна частота появи будь-якої події у загальному обсязі спостережень чи відношення числа сприятливих результатів до загальної кількості. Вона, наприклад, формується під час аналізу результатів великої кількості спостережень. Під суб'єктивною ймовірністю розуміється міра впевненості деякої людини чи групи людей у тому, що ця подія станеться. Ця ймовірність може бути формально представлена різними способами, наприклад, імовірнісним розподілом або бінарним ставленням на безлічі подій, але найчастіше вона являє собою імовірнісний захід, отриманий експертним шляхом [2].

Також зустрічаються визначення ризику, що відображають його як небезпеку: передбачувана (відома); невідома на даний момент, але яка може виникнути; заподіяння шкоди за допомогою атаки (реалізації певної загрози з використанням уразливості активу або групи активів).

Відомі поняття ризику, що визначають його як частоту, витрати чи втрати, які безпосередньо пов'язані з виникненням тієї чи іншої події. Наведемо деякі з них, наприклад, ризик як: частота реалізації "небезпеки"; як добуток величини події на міру її можливості; витрати чи втрати економічного ефекту, пов'язані з реалізацією певного рішення (наприклад, планового варіанта) за умов, інших проти тими, у яких рішення було оптимальним. Також ризик у будь-якому контексті розглядається як сумарна величина загрози (тобто події, що завдають шкоди), уразливості (відкритість підприємства до загроз) та вартості майна (вартість активу за небезпеки). Збільшення

будь-якого з цих факторів відповідно збільшує ризики, а зниження призводить до його зменшення [1-3].

Після проведеного аналізу поняття ризику в різних сферах життєдіяльності людини можна виділити одну характеристику ризику, яка зустрічається во всіх визначеннях наведених вище і об'єднує їх – це подія, яка має відбутися і яку автори пов'язують із ймовірністю, дією або діяльністю, частотою, втратами, небезпекою тощо.

В аспекті ІБ ризик можна пов'язати з подією реалізації загрози ресурсам інформаційної системи, внаслідок якого відбулося порушення однієї чи більше базових характеристик безпеки – конфіденційності, цілісності, доступності. Також його можна описати як: ймовірність події, яка призвела до порушення характеристик безпеки; подія, що відбулася за участю або без участі суб'єкта – діяльність або бездіяльність суб'єкта; подія, що відбувається з певною частою тощо.

При розкритті поняття ризику також слід враховувати, що більшість рішень щодо ІБ приймаються в умовах невизначеності.

Проведений аналіз показує, що різні трактування поняття ризику мають загальну безліч характеристик, наприклад, зв'язок ризику з ймовірністю і настанням певної події та ін.

1.2. Методи і методики оцінки ризиків

ЗАОР 1 – Метод на основі байєсівських мереж (МБС) розроблений для побудови каузальних моделей оцінки операційних ризиків. В його основі лежить теорема Байєса, цінність якої стосовно оцінки таких ризиків полягає в її здатності комбінувати дані про ймовірність подій, одержуваних експертним та статистичним шляхом. Для окремих факторів ризику (загроз), які не мають статистики втрат, оцінки ймовірності ризикових подій можуть бути засновані лише на експертних знаннях, а для інших – на статистиці втрат, якщо обсяг зібраних даних достатній для цілей моделювання кожній пов'язаній з ризиком події (наприклад - «Хакерська атака», «Несанкціонований доступ (НСД)», «Несанкціонована модифікація (НСМ)» та і.н.), про-

водиться оцінка ймовірності її реалізації та (по ланцюжку) пов'язаних з нею операційних втрат. Імовірність реалізації події може бути зазначена у вигляді безперервної функції розподілу або у вигляді таблиці ймовірностей (дискретних ймовірностей). Оскільки безперервні функції розподілу вдається отримати лише в окремих випадках (через недостатність статистики), то використовуються дискретні розподіли. Для концептів, які на графі не мають вхідних стрілок (наприклад, подій, які є драйверами (факторами) ризику), повинна бути вказано абсолютна ймовірність кожного з можливих результатів події, а тих, куди впливають інші концепти, вказується умовна ймовірність кожної комбінації пов'язаних концептів [4]. Приклад експертного завдання умовної ймовірності показано у таблиці 1.1.

Таблиця 1.1

Формування ймовірності

	Виходи - умови			
Хакерська атака	ТАК		НІ	
Зараження вірусом	Так	Ні	Так	Ні
Ймовірність результату події «Зупинка сервера» для різних умов				
Відбудеться	0,3	0,15	0,10	0,02
Не відбудеться	0,7	0,85	0,90	0,98

Визначається абсолютна ймовірність та величина витрат. Розглядаються три категорії наслідків: порушення конфіденційності (К), цілісності (Ц) та доступності (Д). Для матеріальних активів збитки визначаються за шкалою – від повної втрати активу до збою (зупинки, неполадки) на несуттєвий проміжок часу.

ЗАОР 2 - Методологія NIST 800-30 (Risk Management Guide for Information Technology Systems, рекомендації NIST, розробник - National Institute of Standards and Technology, США) охоплює дев'ять первинних кроків: характеристика системи; ідентифікація загроз (таблиця 1.2); ідентифікація вразливостей; аналіз управління; визначення ймовірності; аналіз дії; визначення ризику; рекомендації щодо управління; документування результатів [4-5].

Таблиця 1.2

Приклад ідентифікації загроз

Джерело Загрози	Причина	Дія загрози
Хакер, крекер	Виклик, Его, Бунт	Хакінг, Соціоінжиніринг, Вторгнення в ІС, зломи, НСД в ІС.
Кібер-злочинець	Руйнування інформації, Інформаційне розкриття, Грошова вигода, НСМ даних	Комп'ютерний злочин (кібер-переслідування), Шахрайські дії, Інформаційний підкуп, Spoofing, Вторгнення в ІС

У процесі аналізу ризику збирається інформація, ідентифікація загроз (визначення джерела, причини та дії загрози). Для оцінки використовуються такі рівні ймовірності: високий «В», середній «С», низький «Н». При аналізі впливу визначаються події, пов'язані з втратою К, Ц та Д. Величина впливу визначається за шкалою: висока (В), середня (С), низька (Н). Для визначення ризику використовується матриця: «В»; «С»; «Н» [5].

Таблиця 1.3

Приклад ідентифікації пари вразливість- загроза

Вразливість	Джерело загрози	Дія загрози
ID звільнених службовців не видалені з ІС	Звільнені службовці	Проникнення в ІС на основі особистих даних
Брандмауер компанії дозволяє вхідні	Несанкціоновані користувачі (наприклад, хакери, звільнені службовці)	Використання telnet для доступу до сервера XYZ і читання системних файлів

ЗАОР 3 - Методика TRA (Threat and Risk Assessment, розробник – компанія Government (Communications Security Establishment), Канада) розроблена на основі трьох керівництв для IT- систем по: управлінню ризиком безпеки (Guide to

Security Risk Management for Information Technology Systems – MG-02); сертифікації і акредитації (Guide to Certification and Accreditation of Information Technology Systems – MG-01); оцінки ризику і вибору гарантій (Guide to risk assessment and safeguard selection for Information Technology Systems (MG-03). Для оцінки ризику, аналітик має розглянути опис IT-системи, ідентифікувати суттєві сценарії загроз, оцінити вплив (рис. 1.1) [7].

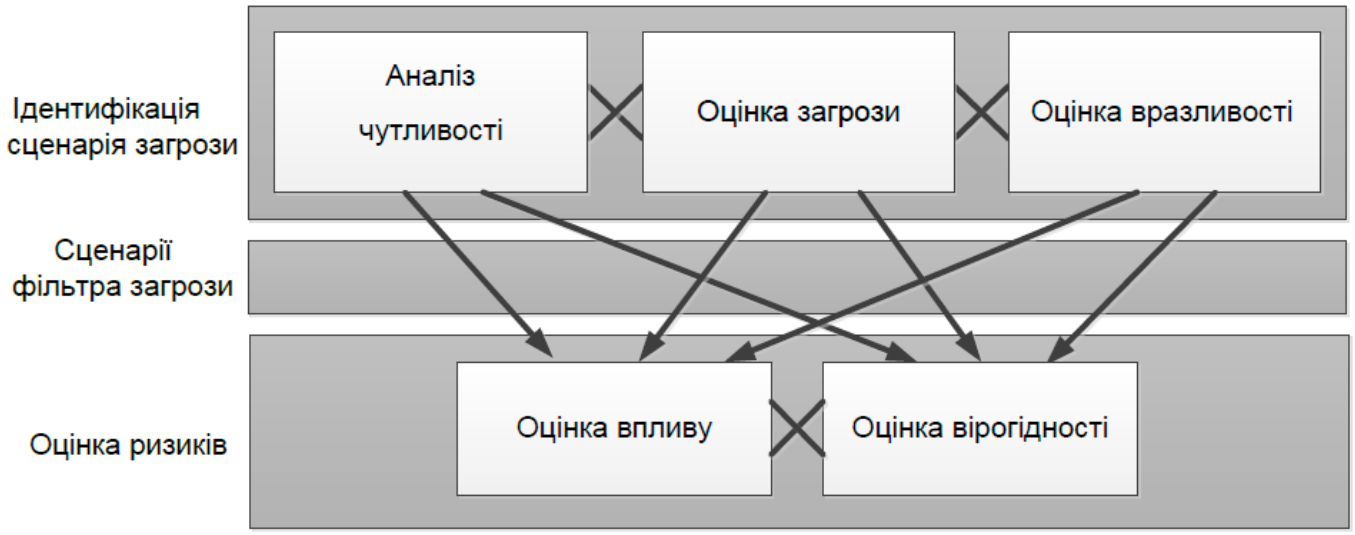


Рис. 1.1. Процес оцінки ризику

В процесі оцінки ризику для кожного сценарію загрози розраховуються її вплив та ймовірність. Такий підхід відображає середні очікувані втрати за певний час. По суті, ризик (R) описується як функціональний зв'язок між вартістю активів (A_{Val}), загрозою (T) і вразливістю (V): $R = f(A_{Val}, T, V)$. Оцінка загрози (наприклад, «Хакерська атака») для такої підгрупи активів, як корпоративні дані (КД) здійснюється на основі таблиці 1.4 де рівень порушення таких характеристик ІБ, як К, Ц і Д відображається трирівневою КЧ шкалою («В», «С», «Н») [8].

Таблиця 1.4

Приклад оцінки загрози

Клас загрози	Дія загрози	Категорія агента загрози (АУ)	АУ	Подія загрози	Рівень порушення			Підгрупа активів
					К	Ц	Д	
Умисна	Шпигунство	Хакери	-	НСД	В	-	-	Д
	Саботаж	Хакери	-	НСМ	-	-	В	Д
	Саботаж	Хакери	-	DoS	-	Н	-	Д

ЗАОР 4 - Методика FRAP (Facilitated Risk Analysis Process, розробник – компанія Peltier and Associates, США) орієнтована на забезпечення ІБ ІВ, що розглядається в рамках процесу управління ризиками, що складається з п'яти етапів [7-8].

Етап 1 – Визначення активів, що захищаються (проводиться на основі опитувальників, вивчення документації на систему, використання інструментів автоматизованого аналізу (сканування) мереж).

Етап 2 – **Ідентифікація загроз.** При складанні списку загроз можуть використовуватися різні підходи, наприклад: вибір актуальних для цієї ІС загроз з заздалегідь підготовлених експертами переліків (checklists); аналізується статистика інцидентів ІБ пов'язаних із даною ІВ; оцінюється їхня середньорічна частота (за низкою загроз, наприклад, виникнення пожежі, дані можна отримати у відповідних державних організацій); фахівці компанії вирішують завдання за допомогою «мозкового штурму» та ін.

Етап 3 – Оцінка ризику (ОР). Кожній загрозі зі складеного списку зіставляють її ВР, далі оцінюють збитки, які можуть бути завдані цією загрозою і за отриманими значеннями, оцінюється її рівень. При проведенні аналізу ризику зазвичай приймають, що на початковому етапі в системі відсутні засоби та механізми захисту. Таким чином оцінюється рівень ризику для незахищеної ІВ, що дозволяє показати ефект від впровадження засобів захисту інформації (ЗІ). Оцінка провадиться за ВР загрози та шкоди від її реалізації протягом року з використанням наступних шкал. Для ймовірності (Probability): висока (High Probability) - ймовірно; середня (Medium Probability)

- можливо; низька (Low Probability) – малоймовірна. Для шкоди (Impact – міра величини втрат або шкоди, що завдається активу): «В» (High Impact) – зупинка критично важливих бізнес-підрозділів, що призводить до істотних збитків для бізнесу, втрати іміджу або неотримання істотного прибутку; «С» (Medium Impact) – короткочасне переривання роботи критичних процесів чи систем, що призводить до обмежених фінансових втрат в одному бізнес-підрозділ; «Н» (Low Impact) – перерва в роботі, яка не викликає відчутних фінансових втрат. Оцінка здійснюється у відповідність до правила, що задається матрицею ризиків і може інтерпретуватися наступним чином: рівень А – пов'язані з ризиком заходи (наприклад, впровадження засобів ЗІ) повинні бути виконані негайно та в обов'язковому порядку; рівень В - пов'язані з ризиком заходи повинні бути вжиті; рівень С – потрібен моніторинг ситуації (але безпосередніх заходів щодо протидії загрозі вживати, можливо, не треба); рівень D - ніяких заходів зараз робити не треба.

Етап 4 – Визначення контрзаходів. Після ідентифікації загроз та оцінки ризику визначаються контрзаходи, що дозволяють усунути ризик або звести його до прийнятного рівня.

Етап 5 – Документування. Після аналізу та оцінювання ризику результати докладно документуються в стандартизований формат. Отриманий звіт може бути використаний щодо політик, процедур, бюджету ІБ і т.д.

PROBABILITY

IMPACT

	High	Medium	Low
High	*A*	*B*	*C*
Medium	*B*	*B*	*C*
Low	*B*	*C*	*D*

A – Corrective action must be implemented
B – Corrective action should be implemented
C – Requires monitor
D – No action required at this time

Рис. 1.2. Матриця ризиків FRAP

ЗАОР 5 - Методика BSI-Standard 100-3 (Risk Analysis IT-Grundschutz – аналіз ризиків на основі IT-Grundschutz, розроблена Федеральним Агентством по ІБ (Federal Office for Information Security - BSI) , Німеччина) на процесі аналізу і оцінювання ризику ІТ- безпеки , запропонованого в BSI-Standard 100-3-й, включає сім етапів [8-9].

Етап 1 – Попередня підготовка. На цьому етапі визначається область ІБ, вимоги до неї (нормальні, високі та дуже високі), які розглядаються з точки зору забезпечення К, Ц та Д. Також проводиться аналіз структури підприємства, додатковий аналіз ІБ, оцінюється її поточний рівень.

Етап 2 – Підготовка до опису загрози. За допомогою запропонованого у методиці списку загроз здійснюється їх аналіз для конкретного підприємства. Ідентифікуються модулі та цільові об'єкти (ЦО) захисту, які заносяться до таблиці (таблиці 1.5).

Таблиця 1.5

Приклад ідентифікації

№	Назва модуля	ЦО
B 2.4	Серверна кімната,	Каб. М. 723
B 2.6	Виробнича кімната,	Каб. М. 811
B 3.101	Сервер,	S3
B 3.207	Головний клієнт,	C4
B 3.301	Шлюз безпеки (FireWall)	N3

Кожен модуль ЗІ пов'язаний зі списком загроз, а номер та їхня назва відповідає конкретному ЦО. Результатом проходження етапу є перелік загроз конкретному об'єкту (таблиці 1.6).

Таблиця 1.6

Приклад описи загроз

Сервер S3
До: нормальна; Ц: висока; Д: висока
Т 1.2 Відмова ІТ- системи. Т 3.2 Ненавмисне знищення активу. Т 4.1 Перебій у електроживленні. Т 5.57 Мережеве сканування. Т 5.85 Втрата Ц інформації і т.д.

Далі узагальнені таблиці загрози сортуються по кожному ЦО.

Етап 3 – Визначення додаткових загроз. Тут використовується спеціальний набір запитів, наприклад: «Які потенційні форс-мажорні обставини представляють особливі загрози інформаційної області?»; «Яких організаційних недоліків потрібно уникнути за будь-яку ціну для гарантування ІБ?»; «Які помилки людини негативно впливають на ІБ?»; «Які спеціальні проблеми ІБ могли статися з ЦО, що розглядається, через технічну відмову?» і т.д.

Етап 4 – Оцінка загрози. Тут проводиться тематичне опитування фахівців з урахуванням базових запитів. Результати фіксуються в таблиці із зазначенням Y (якщо заходи ІБ (здійснені або передбачувані) забезпечують належний захист від відповідної загрози або, якщо загроза не важлива для поточного аналізу ступеня ризику) або N (якщо заходи ІБ (здійснені або передбачені) не забезпечують належний захист від відповідної загрози) для кожної окремої загрози (табл. 1.7)).

Таблиця 1.7

Загрози

Сервер S3	Оцінка загрози
К: нормальна; Ц: висока; Д: висока.	
Т 1.2 Відмова ІТ системи.	N
Заходи ІБ для сервера S3 не запобігають реалізацію загрози. ІТ - заходи по Каталогу Grundschutz не відповідають.	
Т 5.85 Втрата Ц інформації.	N
Інформація клієнта про замовлення не повинна піддаватися НСМ. Інакше це може привести до надлишкам (нестачі) поставок, тим самим накликаючи компанії високі Витрати.	

Етап 5 – Обробка ризиків. Тут використовується шкала: «А» - зниження ризику за допомогою додаткових заходів; «В» – запобігання ризику за допомогою реструктурування; «С» - прийняття ризику; «D» - передача ризику; (Таблиця 1.8).

Етап 6 – Консолідація концепції ІБ.

Етап 7 - Зворотний зв'язок.

Таблиця 1.8

Приклад таблиці обробки ризику

Сервер S3	
К: нормальна; Ц: висока; Д: висока	
Т 1.2	Відмова ІТ- системи
«*A*» S 6. U1	Додаткова ІТ-міра по ІБ: Здійснення повної заміни системи спілкування з клієнтом. Реалізується повна заміна системи зв'язку з клієнтами. Це стосується всіх технічних засобів, включаючи канали зв'язку. Резервна система знаходиться в приміщенні Е.3. З можливістю використання у будь-який момент часу, (не > 30 хв. затримки виробництва). Використовується модемний зв'язок із клієнтом. Вся система заміни, включаючи модемне з'єднання, перевіряється не рідше одного разу в квартал і всякий раз, при зміні конфігурації.
Т 5.85	Втрата Ц інформації
«*C*»	Прийняття ризику: Хоча ризик мінімізований до певної міри механізмами ІБ, які вбудовані в систему передачі та ІТ-систему, але можливі подальші інциденти, що призводять до НСМ інформації про вимогу замовлення, що наражає компанію на високий ризик. Цей залишковий ризик прийнятий керівництвом, оскільки ефективні протидії будуть неекономними.

1.3. Інші відомі підходи до оцінювання ризиків

ЗАОР 6 - Стандарт ISO/IEC 27005:2008 (Information technology – Security techniques – Information security risk management (Інформаційна технологія – Методи захисту – Менеджмент ризиків ІБ) представляє технічний перегляд стандартів, скасування та заміну ISO/IEC TR 13335-3:1998 та ISO/IEC TR 13335-4:2000, Швейцарія) надає рекомендації для менеджменту ризиків ІБ організації, в особливості підтримуючи вимоги «Системи менеджменту інформаційної безпеки» (ISMS) згідно з ISO/IEC 27001 [9-11]. Процес менеджменту реалізується у шість етапів.

Етап 1 – Створення контексту. Здійснюється загальний аналіз усієї інформації про організацію, що відноситься до створення контексту, а також проводиться встановлення основних критеріїв, необхідних для менеджменту ризиків ІБ та визначення для нього сфери застосування та меж здійснення.

Етап 2 – Оцінка ризиків. Тут здійснюється ідентифікація (активів, загроз, існуючих вимог, уразливостей та наслідків), оцінка та опис (КЛ, КЧ або їх комбінація), розташування за пріоритетами ризиків, що належать до організації. Якісна оцінка використовує шкалу кваліфікації атрибутів, щоб описати величину потенційних наслідків (наприклад: низькі, середні чи високі) та ймовірність, що ці наслідки відбудуться. Кількісна оцінка використовує масштаб із числовими значеннями, як наслідків, і ймовірності. Кількісна оцінка здебільшого використовує статистику інцидентів. Результатами проходження цього етапу будуть оцінки наслідків, ймовірності інциденту.

Етап 3 – Обробка ризиків. Включає загальний опис обробки, а також зниження, збереження, запобігання та перенесення ризику.

Етап 4 – Прийняття ризику. Плани обробки ризику повинні описати, як оцінені ризики були опрацьовані, до приймальних критеріїв.

Етап 5 – Комунікації ризику. Обмін інформацією про ризик між особами, які приймають рішення та іншими причетними сторонами з метою досягнення угоди щодо управління ризиками.

Етап 6 – Моніторинг та перегляд ризику ІБ. Тут здійснюється моніторинг та перегляд факторів ризику, а також покращення його менеджменту. У стандарті є рекомендації та приклади: визначення сфери застосування та меж процесу менеджменту ризиків; ідентифікації та визначення цінності активів, вартості впливу; типових загроз (де мітки мають наступне значення: D – навмисний (навмисні акції, націлені на ІА), A – випадковий (ненавмисні дії людини на ІА) і E – екологічний (інциденти, які не ґрунтуються на діях людини)); уразливостей та методи їх оцінювання; підходи до оцінки ризиків; обмеження щодо зниження ризику. Стандарт має реалізації у ПС, наприклад, Meycor KP (Knowledge Provider).

Таблиця 1.9

приклад типових погроз

Тип	Загрози	Мітки
НСД	Несанкціоноване використання Устаткування	D
	Шахрайське копіювання ПС	D
	Використання підроблених або скопійованих ПС	A, D
	Спотворення даних	D
	Незаконна обробка даних	D

В ISO/IEC 27005:2008 запропоновано високорівневу та детальну ОР ІБ. Для останньої може використовуватись матриця з певними значеннями. Для кожного активу розглядаються відповідні вразливості і загрози, наприклад, якщо цінність активу - ЦА = 3, ВВ загрози - ВВУ = «В» і простота використання вразливості - ППУ = «Н» то міра ризику - МР = 5 [7-16].

Також запропоновано матрицю визначення ймовірності сценарію інциденту. (ВСІ) (де «ВІН» (дуже низька), «Н» (низька), «С» (середня), «В» (висока), «ДВ» (дуже висока)), що відповідно означає (дуже малоймовірно), (малоймовірно), (можливо), (ймовірно), (часто). Отримуване в результаті значення ризику вимірюється по шкалою від 0 до 8 (наприклад, «Н» (0-2); «С» (3-5); «В» (6-8)), може бути оцінено щодо критеріїв прийняття ризику.

Таблиця 1.10

Матриця оцінки МР

ВВУ		Н			З			У		
ППУ		Н	З	У	Н	З	У	Н	З	У
ЦА	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5

Матриця може використовуватися для зв'язку факторів наслідків (ЦА) з ВВУ (беручи до уваги аспекти вразливості). Спочатку за певною шкалою (наприклад, 1

÷ 5) проводиться оцінка ЦА для кожного активу, що знаходиться під загрозою (колонка (b)). Далі, наприклад, за тією ж шкалою оцінюється ВВУ, для кожної загрози (колонка (c)) та за отриманими результатами обчислюється міра ризику (колонка (d)) шляхом множення d = b × c. Згодом проводиться ранжування загроз (колонка (e)) у порядку відповідного заходу ризику (у таблиці). 1.11 1 – найнижчий наслідок та найнижча ВВУ. У колонці (a) відображено ідентифікатори загрози.

Таблиця 1.15

Приклад ранжирування погроз

(a)	(b)	(c)	(d)	(e)
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	5
E	4	1	4	4
F	2	4	8	3

Розглянемо приклад (запропонований у стандарті) оцінки значення для ймовірності ризиків та їх можливих наслідків. Тут особлива увага приділяється наслідкам інцидентів ІБ (сценаріям інцидентів) та визначенню того, яким системам слід віддавати перевагу. Це виконується шляхом оцінки двох значень для кожного активу і загрози, комбінація яких визначатиме бали (B_{ij}), де і та j – відповідно номер активу та загрози. Підсумовування всіх балів активів дає можливість визначити МР. Спочатку кожному активу надається ЦА для кожного випадку виникнення відповідної загрози. Це значення пов'язане з можливими несприятливими наслідками, що можуть виникати при реалізації загрози. Далі визначається показник ймовірності ризику. Він оцінюється виходячи з комбінації ВВУ та ПІУ. Потім, після перетину ліній значень ЦА і ПВР присвоюються відповідні бали. Після чого вони підраховуються для отримання підсумкових значень по кожному активу [11].

У наступних прикладах усі значення вибрано випадковим чином. Припустимо, що система має три активи $А_1$, $А_2$, $А_3$ і існують дві загрози $З_1$, $З_2$ цій системі. Нехай $ЦА_1 = 3$, $ЦА_2 = 2$ і $ЦА_3 = 4$. Якщо для $А_1$ і $З_1$ $ВВУ_{11}$ = «Н» та $ПІУ_{11}$ = «С», то значення $ПВР_{11} = 1$. Бали для $А_1$ і $З_1$ можуть бути виведені на перетині ліній $ЦА_1 = 3$ та $ПВР_{11} = 1$, тобто. $Б_{11} = 4$. Аналогічним чином, нехай для $А_1$ і $З_2$ $ВВУ_{12}$ = «С», а $ПІУ_{12}$ = «В», то $ПВР_{12} = 3$ тобто. $Б_{12} = 6$. Тепер можуть бути обчислені підсумкові бали (БІ і) активу щодо всіх загроз $БІ_1 = Б_{11} + Б_{12} = 10$ (для кожного активу та його загрози). Обчислення підсумкових балів по всій системі (ВІС) здійснюється шляхом підсумовування всіх балів за кожному активу щодо всіх загроз $БІС = БІ_1 + БІ_2 + БІ_3$. У стандартах ISO/IEC 27001 та 27002 на етапі оцінки ризику ІБ дається посилання на документ ISO/IEC TR 13335-3, який тепер представлений як ISO/IEC 27005 [10-14].

Таблиця 1.12

Бальник

ПВР	ЦА				
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

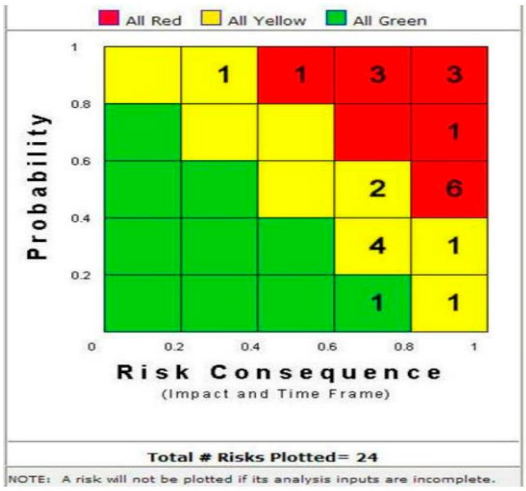
ЗАОР 7 - Методика Risk Matrix (Розробник компанія Mitre Corporation, США) орієнтована на оцінювання ризику і згодом була реалізована додатком для Microsoft Excel. Основний процес включає: - планування оцінки ступеня ризику; ідентифікацію завдань чи вимог; визначення; ранжування; складання рейтингу ризиків; управління планами дій; безперервну оцінку ризиків. Оцінка ризику полягає у плануванні діяльності. Початково Виготовляється ідентифікація ризику з допо-

могою застосування експертами «Мозкового штурму». Далі надаються різні атрибути кожному ризику, такі як, наприклад, період часу (дати початку та закінчення можливої реалізації) та ВР. За допомогою сценарію «Якщо ризик …, то наслідки …» складається матриця ризику. Для визначення впливу використовується шкала: С (критичне); S (серйозне); M_o (середні); M_i (Низьке); N (незначне), а ймовірності – ($ВС_3$): 0-10% (дуже низька); 11-40% (Низька); 41-60% (Середня); 61-90% (Вище середнього); 91- 100% (Висока) [15-17].

Таблиця 1.13

Шкала ризиків

ПВР (%)	Категорії впливу				
	N	M_i	M_o	S	С
0-10	Н	Н	Н	З	З
11-40	Н	Н	С	С	П
41-60	Н	С	С	С	П
61-90	С	С	С	С	П
91-100	С	П	П	П	П



All 5x5 Cells: Red

Risk ID	Risk Name	Consequence	Probability	Mitigation
INF.003	Platform System Integration	0.91	1.00	Yellow
MGT.001	Organizational Interfaces	0.89	0.90	White
OPS.003	Ground Sampling Collection and Analysis	0.84	1.00	Green
SE.016	Technology Readiness for Science Payload CIs	0.87	0.70	Red
SE.015	Cannot handle real-time transmission rate	0.91	0.60	Red
PROG.001	Stakeholder and Mission Partner Complexity	0.73	0.90	Red
SE.017	Balloon weight	0.89	0.50	White
OPS.006	Balloon inflation	0.82	0.60	Yellow
MGT.002	WBS	0.81	0.60	White
OPS.009	Accurately controlling vehicle altitude in the Venusian environment	0.84	0.50	White
SE.005	Component single point of failure	0.81	0.50	Green
APPS.001	SW Testing Enviroment	0.67	1.00	Yellow

Рис. 1.3. Діаграма частот

ВИСНОВКИ ДО РОЗДІЛУ 1

1) Проаналізовано базові поняття, пов'язані із ризиком. Проведений аналіз показує, що різні трактування ризику мають загальну безліч характеристик, наприклад, зв'язок ризику з ймовірністю і настанням певної події та ін.

2) Проведено аналіз і дослідження існуючих стандартів, методів, методик, методологій та програмних ЗАОР, з метою визначення вхідних, внутрішніх та вихідних параметрів, що використовуються для створення та вибору найбільш ефективного інструментарію розв'язання відповідних завдань ЗІ.

РОЗДІЛ 2
МОДЕЛЬ ТА МЕТОДИ АНАЛІЗУ ТА ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Кортежна модель базових характеристик ризику

Стрімкий розвиток ІТ-інфраструктури підприємств незмінно спричиняє неконтрольоване зростання кількості інформаційних загроз та вразливостей інформаційних ресурсів. У умовах оцінювання ризиків ІБ дозволяє визначити необхідний рівень ЗІ, здійснити його і розробити стратегію розвитку інформаційної структури компанії. Оцінювання та аналіз ризиків ІБ є необхідною умовою при створенні системи управління ризиками та плану забезпечення безперервності та поновлення бізнесу.

У п. 1.1 проведено аналіз тлумачень ризику у багатьох галузях людської діяльності з метою відображення його на сферу ІБ, а також виділено базові характеристики ризику.

У різних публікаціях існує безліч визначень ризику, які мають досить широке його трактування. Тільки в Інтернет-словниках міститься понад 1500 тлумачень ризику у багатьох сферах людської діяльності. Внаслідок цього виникають різні неоднозначності, пов'язані з розкриттям сутності самого ризику та пов'язаних з ним понять. Відповідно такий стан характерний і для сфери ІБ.

Враховуючи, що ризики торкаються різних предметних областей, то це поняття слід розглянути з погляду:

1) Безпеки;
2) Психології;
3) Економіки;
4) Страхування;
5) Медицини;
6) Геології;

і т.д., що розкривається як у монографіях, статтях, підручниках, словниках, так і різних нормативних, національних та міжнародних документах.

Для формалізації процесу формування базових характеристик ризику введемо багато всіх можливих характеристик [18].

$$\boldsymbol{BC} = \bigcup_{i=1}^{n} \boldsymbol{BC}_i = \{\boldsymbol{BC}_1, \boldsymbol{BC}_2, ..., \boldsymbol{BC}_n\}, \quad (2.1)$$

де n - кількість членів НД.

Наприклад, при n =6 множина НД може мати наступний вигляд [18].

$$\boldsymbol{BC} = \bigcup_{i=1}^{6} \boldsymbol{BC}_i = \{\boldsymbol{BC}_1, \boldsymbol{BC}_2, \boldsymbol{BC}_3, \boldsymbol{BC}_4, \boldsymbol{BC}_5, \boldsymbol{BC}_6\},$$

«ДІЯ», «ПОДІЯ», «ЙМОВІРНІСТЬ», «НЕБЕЗПЕКА», «ЧАСТОТА», "ВИТРАТИ"}.

Після проведеного аналізу поняття ризику у різних сферах життєдіяльності людини, можна назвати таку базову характеристику ризику – «ДІЯ» (BC_1), що призвело до події порушення ІБ. З погляду ІБ BC_2 пов'язане з реалізацією потенційних загроз базовим характеристикам безпеки ресурсів інформаційних систем (РІС), що призвели до виникнення небажаної події . У зв'язку з цим базову характеристику BC_1 можна відобразити безліччю ідентифікаторів [18].

$$\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i} = \{BC_{11}, BC_{12}, ..., BC_{1bc_1}\}, \quad (2.2)$$

(де bc_1 - кількість ідентифікаторів загроз), наприклад, при bc_1 =3 безліч НД може мати такий вигляд $\boldsymbol{BC_1} = \bigcup_{i=1}^{3} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}\}$ ={«Комп'ютерне шпигунство», «Шпигунство», «Збій програмного забезпечення»}.

Наступну базову характеристику можна визначити як, «ПОДІЯ» ($ВС_2$), яку можна відображати у вигляді символьної змінної, що приймає одне із значень кінцевої множини ідентифікаторів [19].

$$\boldsymbol{BC_2} = \bigcup_{i=1}^{bc_2} BC_{2i} = \{BC_{21}, BC_{22}, ..., BC_{2bc_2}\}, \quad (2.3)$$

(bc_2 – кількість ідентифікаторів подій). З урахуванням того, що в області ІБ ризик пов'язаний з такими базовими характеристиками безпеки РІС як конфіденційність, цілісність та доступність, то базові події при bc_2 =7 можуть ідентифікуватися як $\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i} = \{BC_{21}, BC_{22}, BC_{23}, BC_{24}, BC_{25}, BC_{26}, BC_{27}\}$ = {«Порушення конфіденційності», «Порушення цілісності», «Порушення доступності», «Порушення цілісності і конфіденційності», «Порушення цілісності та доступності», «Порушення конфіденційності та доступності», «Порушення конфіденційності, цілісності та доступності»}. Слід зазначити, що, коли виникають складнощі з отриманням статистичних даних, а також для простоти інтерпретації величин, експерти використовують логіко-лінгвістичний підхід. З його допомогою здійснюється відображення відповідної характеристики за допомогою ЛП «Вірогідність» з певною базовою терм-множиною, наприклад [19-20]:

$$\boldsymbol{BC_3} = \bigcup_{i=1}^{bc_3} \underset{\sim}{BC}_{3i}, \quad (2.4)$$

(bc_3 - кількість термів), для членів якого справедливо ставлення порядку $\underset{\sim}{BC}_{31} < \underset{\sim}{BC}_{32} < ... < \underset{\sim}{BC}_{3bc_3}$. Слід відзначити, що терми ЛП пов'язуються зазначеним ставленням у вигляді застосування методів порівняння нечітких чисел [19]. Наприклад, для зазначеної ЛП можна сформувати безліч термів.

$\boldsymbol{BC_3} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{3i} = \{\underset{\sim}{BC}_{31}, \underset{\sim}{BC}_{32}, \underset{\sim}{BC}_{33}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$, що відображаються нечіткими числами (НЧ) Н, С і В, мають лінгвістичний еквівалент «низьке» (Н), «середня» (С) та

«високе» (В) відповідно. Надалі для зазначених НЧ з урахуванням відомих методів формуються необхідні функції власності. Також можуть бути введені інші значення первинних термів, наприклад, «дуже низька» (ВІН), «Вище середнього» (НД), «Нижче середнього» (НС) та ін. Очевидно, що в цьому випадку характеристика $ВС_3$ відображається набором лінгвістичних значень, але як окремий випадок, вона може приймати чітке або інтервальне значення, тоді для її відображення будемо використовувати не напівжирний шрифт, наприклад, $ВС_3$. Визначимо ще одну базову характеристику ризику ($ВС_4$), яка розглядається як величина, що характеризує небезпеку події порушення ІБ, наприклад, за допомогою $ВС_{12}$.По аналогії з $ВС_3$, базова характеристика $ВС_4$ може відображатися у чіткій чисельній формі (наприклад, в відсотках) і позначається як $ВС_4$ або з допомогою ЛП - «НЕБЕЗПЕКА» з базовим набором термножин [20]:

$$\boldsymbol{BC_4} = \bigcup_{i=1}^{bc_4} \underset{\sim}{BC}_{4i} \ (\underset{\sim}{BC}_{41} < \underset{\sim}{BC}_{42} < \ldots < \underset{\sim}{BC}_{4bc_4}), \qquad (2.5)$$

Наприклад, при bc_4 =3 можемо визначити: $\boldsymbol{BC_4} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{4i} = \{\underset{\sim}{BC}_{41}, \underset{\sim}{BC}_{42}, \underset{\sim}{BC}_{43}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$ з відповідними лінгвістичними еквівалентами - «низька» (Н), «середня» (С) і «Висока» (В). Для досліджуваної вище безлічі тлумачень ризику можна виділити такі базові характеристики, як: частота ($ВС_5$), що у області ІБ можна пов'язати з частотою реалізації «загрози», що призвела до події порушення ІБ. Такий компонент можна відображати чисельно ($ВС_5$) або за допомогою ЛП – «ЧАСТОТА» [21-22]:

$$\boldsymbol{BC_5} = \bigcup_{i=1}^{bc_5} \underset{\sim}{BC}_{5i} \ (\underset{\sim}{BC}_{51} < \underset{\sim}{BC}_{52} < \ldots < \underset{\sim}{BC}_{5bc_5}), \qquad (1.6)$$

наприклад, якщо bc_5 =3, то $\boldsymbol{BC_5} = \bigcup_{i=1}^{3} \underset{\sim}{BC}_{5i} = \{\underset{\sim}{BC}_{51}, \underset{\sim}{BC}_{52}, \underset{\sim}{BC}_{53}\} = \{\underset{\sim}{H}, \underset{\sim}{C}, \underset{\sim}{B}\}$ де $\underset{\sim}{H}, \underset{\sim}{C}$ і $\underset{\sim}{B}$ мають відповідно лінгвістичні еквіваленти - «низька» (Н), «середня» (С) і «Висока» (В).

Визначимо базову характеристику витрати і втрати, яку в області ІБ доцільно визначити через термін витрати ($ВС_6$) та подати число ($ВС_6$), наприклад, на заданих інтервалах;

1) 0 - $100;
2) $100 - $1000;
3) $1000 - $10 000;
4) $10 000 - $100 000.

Також $ВС_6$ можна визначити за допомогою ЛП «ВИТРАТИ» [22]:

$$\boldsymbol{BC_6} = \bigcup_{i=1}^{bc_6} \underset{\sim}{BC}_{6i} \left(\underset{\sim}{BC}_{61} < \underset{\sim}{BC}_{62} < \ldots < \underset{\sim}{BC}_{6bc_6} \right), \quad (2.7)$$

де, наприклад, при $bc_6 = 5$ ЛП приймає вигляд $\boldsymbol{BC_6} = \bigcup_{i=1}^{5} \underset{\sim}{BC}_{6i} = \{\underset{\sim}{BC}_{61}, \underset{\sim}{BC}_{62}, \underset{\sim}{BC}_{63}, \underset{\sim}{BC}_{64}, \underset{\sim}{BC}_{65}\} = \{\underset{\sim}{H}, \underset{\sim}{HC}, \underset{\sim}{C}, \underset{\sim}{BC}, \underset{\sim}{B}\}$ а лінгвістичними еквівалентами використовуваних НЧ будуть відповідно «низькі» (Н), «нижче середнього» (НС), «середні» (С), «Вище середнього» (ВС) і «високі» (В). на практиці зустрічається і інтегроване подання $ВС_6$, наприклад;

1) Negligible (менше $100);
2) Minor (менше $1000);
3) Moderate (менше $10 000);
4) Serious (Істотне негативне вплив на бізнес);
5) Critical (Катастрофічний вплив, можливе припинення діяльності підприємства).

У цьому випадку Характеристики позначаються як $ВС_6$ / $ВС_6$. Для досліджуваної множини тлумачень ризику, були виділені його базові характеристики: ризик розглядається як ймовірність, що вимірюється або розраховується; ризик пов'язаний з настанням певної події (як правило, несприятливої); поняття ризику розкривається через діяльність суб'єкта; ризик розкривається через незалежну від діяльності суб'єкта подію; ризик сприймається як небезпека, частота, витрати та втрати.

Як узагальнення пропонується для інтегрованого використання базових характеристик ризику, відображених на сферу ІБ, представити їх у вигляді моделі з m-компонентним базовим кортежем < $ВС_1$, $ВС_2$, ..., $ВС_m$, де m(m≤n) – кількість членів у кортежі. Наприклад, при m= 6 шестикомпонентний кортеж може мати такий вигляд [23]:

$$<BC_1, BC_2, BC_3, BC_4, BC_5, BC_6>, \quad (2.8)$$

де $ВС_1$ – дія, $ВС_2$ – подія, $ВС_3$ – ймовірність, $ВС_4$ – небезпека, $ВС_5$ – частота, $ВС_6$ – витрати та втрати. В результаті конкретизації використовуваних характеристик утворюється приватна кортежна Модель, наприклад, для BC_{12}=«Шпигунство» $\hat{BC}_{22}$ = «НК», bc_3=3, $\hat{bc}_4$=3, bc_5=3 і bc_6=5 вона прийме наступний вигляд:

$$<BC_{12},BC_{21},BC_3,BC_4,BC_5,BC_6>=<BC_{12},BC_{21},\bigcup_{i=1}^{3}\underset{\sim}{BC}_{3i},\bigcup_{i=1}^{3}\underset{\sim}{BC}_{4i},\bigcup_{i=1}^{3}\underset{\sim}{BC}_{5i},\bigcup_{i=1}^{5}\underset{\sim}{BC}_{6i}>.$$

Як видно, якщо базові величини приймають чіткі або нечіткі значення, то в приватному кортежі (приватної кортежної моделі) вони позначаються відповідно не напівжирним або напівжирним шрифтом, наприклад, $ВС_{12}$, $ВС_{21}$, або $ВС_3$, $ВС_4$, $ВС_5$, $ВС_6$.

На основі представленої кортежної моделі можна здійснювати дослідження широкого спектру існуючих засобів аналізу і оцінювання ризику з позицій формування необхідних для їх функціонування вихідних даних, що дозволить визначити підходи до створення нових систем або використання існуючих для ефективного вирішення відповідних завдань ЗІ.

2.2. Базові характеристики, що використовуються у засобах аналізу та оцінювання ризиків

На сьогоднішній день існує досить багато інструментальних ЗАОР. Часто перед фахівцями компаній для підвищення ефективності розв'язання завдань ЗІ виникає питання щодо вибору відповідної методики, яка задовольнятиме адекватним вимогам. У п. 1.1 здійснено аналіз поняття ризику, у різних предметних сферах людської діяльності, для подальшої його інтерпретацій у галузі ІБ. Також у п. 2.1 було запропоновано кортежну модель базових характеристик ризику (КМР). Такий підхід дає можливість щодо КМР уніфікувати процес дослідження відповідних ЗАОР та підвищити ефективність здійснення їх вибору. Також є безліч інших подібних засобів, котрим не визначено набір характеристик ризику, оскільки здійснювався відповідний аналіз.

У зв'язку з цим проведено дослідження широкого спектра існуючих ЗАОР (з використанням запропонованого у п. 2.1 підходу) для визначення їх набору характеристик, по яким можна здійснити порівняльний аналіз таких засобів. Це підвищить ефективність вирішення завдань у сфері ІБ.

ЗАОР 1 - Методологія NIST 800-30 (Risk Management Guide for Information Technology Systems, рекомендації NIST, розробник –National Institute of Standards and Technology, США) [NIST 800].

Щодо КМР визначимо кортеж цієї методології. Характеристика $ВС_1$ відображається «Дією загрози» (таблиця 2.1), яка може привести до порушення характеристик ІБ, так наприклад, $ВС_{11}$ = «Проникнення в ІС на основі особистих даних» може привести до $ВС_{21}$ = «К». Для оцінки методології використовуються базові характеристики $ВС_3$ і побічні $ВС_4$, які відображають значення параметра «Вплив» (табл. 2.1). Отже, кортеж для методології має вигляд: <$ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$>.

Таблиця 2.1

Матриця рівня ризику

Ймовірність Загрози	Вплив		
	Н (10)	*З (50)*	*У (100)*
В (1,0)	Н 10 × 1,0 = 10	З 50 × 1,0 = 50	У 100 × 1,0 = 100
С (0,5)	Н 10 × 0,5 = 5	З 50 × 0,5 = 25	З 100 × 0,5 = 50
Н (0,1)	Н 10 × 0,1 = 1	Н 50 × 0,1 = 5	Н 100 × 0,1 = 10

ЗАОР 2 - Методика BSI-Standard100-3 (IT-Grundschutz – аналіз ризиків на основі IT-Grundschutz, розроблена Федеральним Агентством з ІБ (FederalOfficeforInformationSecurity – BSI), Німеччина). [Методика BSI] .

Щодо КМР відзначимо, що всі множини дій ($ВС_1$), представлено як загрози, що приводять до порушення ІБ, наприклад, $ВС_{11}$ = «Відмова ІТ-системи», $ВС_{12}$ = «Ненавмисне знищення активу», $ВС_{13}$ = «Втрата інформації» і т.д. Щодо характеристики $ВС_2$ слід зазначити, що розглянуті дії призводять до порушення певних характеристик ІБ і може бути опосередковано пов'язане зі значенням $ВС_{27}$ = «КЦД». З урахуванням КМР кортеж для цієї методики можемо подати у вигляді: <$ВС_1$, $ВС_2$>.

ЗАОР 3 - Стандарт ISO/IEC 27005:2008 (Informationtechnology - Securitytechniques - Informationsecurityriskmanagement (Інформаційна технологія - Методи захисту - Менеджмент ризиків ІБ) представляє технічний перегляд стандартів, скасування та заміну ISO/IEC TR 13335-3:1998 та ISO/IEC TR 13335-4:2000, Швейцарія). Стандарт ISO/IEC 27005:2008.

Зазначимо, що в ISO/IEC 27005:2008 як ризик розглядаються дії, які можуть привести до порушення ІБ, наприклад, $ВС_{11}$ = «Крадіжка носіїв або документів» може перебувати в логічному зв'язку з $ВС_{21}$ = «К» і тому характеристика $ВС_2$ у стандарті є побічною. У процесі аналізу та оцінки ризику можна додатково ідентифікувати компонент $ВС_3$ і побічно – $ВС_4$ (величина потенційних наслідків), отже, кортеж має вигляд: <$ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$>.

ЗАОР 4 - Стандарт AS/NZS 4360:2004 (стандарт ризик-менеджменту, Австралія та Нова Зеландія). Стандарт AS/NZS 4360:2004.

Розглянемо цей стандарт щодо КМР. Так, характеристиці $ВС_1$ відповідають дії які можуть призвести до ризику. Отже їх можна уявити як, наприклад, $ВС_{11}$ = «Відмова системи», що може призвести до порушення характеристик ІБ атакованих ресурсів і може бути пов'язане зі значенням $ВС_{25}$ = «ЦД». При оцінюванні ризику визначається ймовірність загроз ($ВС_3$) та вплив, який можна інтерпретувати як рівень небезпеки ($ВС_4$). Проведений аналіз показав, що кортеж для цього стандарту має вигляд: <$ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$>.

ЗАОР 5 - Стандарт ISO/FDIS 31000 (Riskmanagement – Principlesandguidelines (Управління ризиками – керівні принципи), Швейцарія).

Зазначимо, що щодо КМР у стандарті розглядається подія ризику, які можна відобразити як дію ($ВС_1$), що призводить до порушення ІБ, наприклад, $ВС_{11}$ = «Відмова в обслуговуванні веб-сервера через атаку хакера», $ВС_{12}$ = «Падіння криптосерверу через навантаження», $ВС_{13}$ = «Перехоплення паролів користувача» і т.д. Ці дії можуть бути пов'язані з подіями ($ВС_2$) порушення базових характеристик ІБ $ВС_{23}$ = «Д», $ВС_{27}$ = «КЦД», $ВС_{21}$ = «К» і т.д., отже характеристики $ВС_1$ і $ВС_2$ в стандарті присутні побічно. Характеристики, що використовуються в процесі аналізу ризику, є впливом, який можна відобразити через $ВС_4$ і ймовірністю ризику ($ВС_3$). Після проведеного аналізу з урахуванням КМР кортеж для стандарту буде <$ВС_1$,$ВС_2$, $ВС_3$, $ВС_4$>.

ЗОАР 6 - Методика COBRA (Consultative Objective and Bi-Functional Risk Analysis, розробник - C&A Systems Security Ltd , Великобританія).

Для методики COBRA можна отримати відображення таких складових: $ВС_1$, $ВС_2$. Так, компоненту $ВС_1$ (виходячи із зазначеного прикладу) відповідає, наприклад, значення $ВС_{11}$ = «Крадіжка». Ця дія призводить до порушення певних характеристик безпеки атакованих ресурсів та може бути пов'язана зі значенням $ВС_{27}$ = «КЦД».

Зазначимо, що в аналізованій методиці ризик відображається трьома базовими характеристиками, перша та остання з яких несуть у собі $ВС_1$ та $ВС_2$. Скла-

дові (назва категорії та коментарі до неї), а решта – складова, якій відповідає «РІВЕНЬ РИЗИКУ», представлений у відсотках (імовірність настання ризику), у зв'язку з цим рівень ризику можна відобразити через компонент $ВС_3$.

Усі аналізовані дії ($ВС_1$), які відображаються в запити, зібрані в категорії ризику, наприклад, дія розглянута в прикладі запиту $ВС_{11}$ входить до категорії ризику «Непередбачена ситуація в бізнесі (НСБ)», отже характеристику в даної категорії ризику можна, можливо уявити як $\boldsymbol{ВС_{1НСБ}} = \{ВС_{1НСБ1}, ВС_{1НСБ2}, ..., ВС_{1НСБbc_1}\}$, где $ВС_{1НСБ1}$ = «Крадіжка» (bc_1 - кількість ідентифікаторів загроз для категорії НСБ).

Аналіз показав, що пряме використання компонента $ВС_2$ у системі немає, але простежується логічний зв'язок із ним, тому вважаємо його присутність непрямим. Тут і далі для позначення непрямих показників кортежі буде використовуватися символ *, тобто. $НД_2$. Після проведеного аналізу з урахуванням КМР кортеж для цієї методики можемо подати у вигляді <$ВС_1$, $ВС_2$, $ВС_3$>.

ЗОАР 7 - Метод CRAMM (CCTA Risk Analysisand Management Method, розробник - Центральне агентство з комп'ютерів і телекомунікацій (CCTA - Central Computerand Telecommunications Agency), Великобританія).

Аналіз ризику проводиться на першому та другому етапах, після чого здійснюється його оцінювання. Під час аналізу пропонується проставити коефіцієнти для кожного ресурсу з точки зору частоти виникнення загрози та ймовірності реалізації загрози, тому з урахуванням п. 2.1 тут можна виділити компоненти $ВС_5$ та $ВС_3$.

Щодо уявлення КМР для CRAMM (аналогічно методиці COBRA) можна визначити значення: $ВС_1$, $ВС_2$. Компонент $ВС_1$ відображається дією, що призвела до порушення характеристик ІБ, що можна показати на прикладі «оцінки загрози», а саме $ВС_{12}$ = «Несанкціонований доступ» може призвести до $ВС_{21}$ = «Порушення конфіденційності (ПК)».

Після проведеного аналізу з обліком п. 2.1 складемо КМР для даного методу: <$ВС_1$, $ВС^*_2$, $ВС_3$, $ВС_5$, $ВС_6$>.

ЗАОР 8 - Система RiskWatch (розробник - компанія RiskWatch, США).

Щодо КМР з урахуванням п. 2.1 для RiskWatch визначимо кортеж. Так компоненту $ВС_1$ (виходячи із зазначеного прикладу категорій втрат) відповідають, наприклад, значення $ВС_{11}$ = «Затримка та відмова в обслуговуванні», $ВС_{12}$ = «Розкриття інформації», $ВС_{13}$ = «Знищення обладнання» і т.д. Ці дії призводять до порушення певних характеристик ІБ атакованих ресурсів і відповідно пов'язуються зі значеннями $ВС_{23}$ = «Д», $ВС_{21}$ = «К», $ВС_{25}$ = «ЦД». Аналіз показав, що прямого використання компонента $ВС_2$ у системі немає, але простежується логічний зв'язок з ним, тому вважаємо його присутність непрямим. Аналіз ризику відбувається під час обробки даних, що ініціюються через ТБ, який використовується при проходженні фази 1. Для визначення ALE використовується компонент $ВС_5$ а ризиком є очікувані втрати за рік, які також можна інтерпретувати як витрати ($ВС_6$). З урахуванням КМР, кортеж для цієї методики можна подати у вигляді <$ВС_1$, $ВС_2$, $ВС_5$, $ВС_6$>.

ЗАОР 9 - Інструментарій RA2 artofrisk (RA SoftwareTool, розробник-компанії AEXIS SecurityConsultants і XiSECConsultantsLtd., Великобританія).

Щодо КМР визначимо значення $ВС_1$, $ВС_2$. Всі дії ($ВС_1$), що відображаються запитами, представлені у вигляді вимог стандарту, наприклад, «Чи було проведено оцінку для виявлення ризиків пов'язаних з доступом третіх осіб (ДТЛ)?», «Чи схвалено політику ІБ з керівництвом?». і т.д., компонент $ВС_1$ можна відобразити $ВС_{1i}$, $i = \overline{1, bc_1}$ (де bc_1 - кількість ідентифікаторів загроз). Так, наприклад, у запиті про ДТЛ при невиконанні цієї оцінки можуть виникнути дії, що приводять до порушення базових характеристик ІБ, тоді $ВС_1$ можна уявити безліччю $\boldsymbol{ВС_{1ДТЛ}} \in \{ВС_{1ДТЛi}\}\, i = \overline{1, bc_1}$, де, наприклад, $ВС_{1ДТЛ1}$ = «Крадіжка». Щодо компонента $ВС_2$ відзначити, що розглянуті дії (виходячи із зазначеного прикладу запитів) призводять до порушення певних характеристик ІБ і може бути опосередковано пов'язане зі значенням $ВС_{27}$ = «КЦД». Аналіз показав, що характеристика $ВС_2$ ПЗ присутня побічно. У методиці є характеристики $ВС_4$ (рівні небезпеки) і $ВС_3$ (імовірність ризику), отже, ризик відображається як небезпека ($ВС_4$) для організації (при настанні ризикової ситуації). З урахуванням КМР кортеж для цієї методики можемо подати у вигляді:<$ВС_1$, $ВС_2$, $ВС_3$, $ВС_4$>.

САОР 10 - Методика Information Security RA (Risk Assessment, розробник Centers for Medicare & Medicaid Services (CMS), США). Розглянемо цю методику

щодо КМР. Так, характеристиці $ВС_1$ відповідає всі загрози, які визначаються у фазі 2. Вони можуть призвести до порушення базових характеристик ІБ і отже, може бути пов'язано зі значеннями $ВС_2$. Аналіз показав, що прямого використання їх у методиці немає, але простежується з ним логічний зв'язок, отже є опосередковано. Оцінюючи ризику визначається ймовірність загроз ($ВС_3$) і вплив, який можна відобразити характеристикою $ВС^*_4$. Дослідження показали, що кортеж для цієї системи має вигляд: $<ВС_1, ВС_2, ВС_3, ВС_4>$. Таким чином, у роботі з урахуванням запропонованого у п. 2.1 підходу, проведено дослідження широкого спектра ЗАОР у вигляді відповідного ПЗ та визначено набір базових характеристик (таблиці 2.2), за якими можна здійснити порівняльний аналіз відповідних засобів оцінювання та вибрати найбільш підходящі для вирішення певного класу задач ЗІ.

Таблиця 2.2

Результати дослідження ЗАОР

ЗАОР	BC_1	BC_2	BC_3	BC_4	BC_5	BC_6
1	+	+*	+	+	-	-
2	+	+	-	-	-	-
3	+	+*	+	+	+	+
4	+	+*	+	+	-	-
5	+	+*	+	+*	-	-
6	+*	+*	+	+*	-	-
7	+	+*	+	-	-	-
8	+	+*	-	-	+	+
9	+	+*	+	+	-	-
10	+	+	+	+*	-	+*

2.3. Метод FirstM оцінювання ризиків для систем управління інформаційною безпекою

Відповідно до рекомендацій стандарту ISO/IEC 27001 для забезпечення ІБ на підприємстві будь-якої форми власності необхідно впроваджувати систему управління ІБ. Основою такого стандарту є менеджмент ризиків ІБ, під яким мається на увазі аналіз, оцінювання та обробка ризиків ІБ.

У роботі запропоновано кортежну модель базових характеристик ризику (п. 2.1), а також досліджено широкий спектр ЗАОР (п. 2.2) з визначенням їх базових характеристик, які надалі можна використовувати для аналізу та порівняння відповідних засобів. Таке дослідження показало, що в основному для аналізу та оцінювання ризиків використовуються статистичні дані про інцидентах і погроз ІБ. У багатьох країнах (у в тому числі і в Україні) на державному рівні подібна статистика не ведеться, що обмежує можливості існуючих засобів для національного використання. Також слід зазначити, що досліджуваний інструментарій встановлює експерту певні обмеження (набір параметрів, що використовується) і не дає йому можливості застосування для оцінювання більш широкого спектра величин.

У зв'язку з цим метою є розробка методів аналізу та оцінювання ризиків, що дозволяють використовувати широкий спектр базових характеристик, що дають можливість створювати більш гнучкі засоби оцінювання, а також визначати ризики, як на основі статистичних даних, так і на експертних оцінках, зроблених у невизначеній, слабо формалізованому середовищі, з урахуванням періоду часу, галузі, економічною та управлінської специфіки підприємства та ін. Крім цього, методи, що розробляються, дадуть можливість відображати результати, як у числовій, так і в словесній формі, наприклад, з використанням ЛП, що часто застосовується для опису складних систем, що описуються параметрами, представленими не тільки в кількісному, але і та в якісному вигляді. При цьому ЛП дозволяють поставити у відповідність якісним значенням певний кількісний еквівалент. Для вирішення поставленого завдання пропонується використовувати підхід, що базується на суджен-

нях експертів. При цьому враховуватимемо першу ситуацію, коли експерт має чіткі (бінарні) переваги щодо значень параметрів, що оцінюються, так і другу ситуацію – із зоною невпевненості, коли експерт сумнівається в однозначності своїх пріоритетів. Відповідно до цього пропонується два методи оцінювання – для детермінованої (FirstM).

Метод FirstM

Етап 1 – Визначення множин. На цьому етапі визначаються всі використовувані базові безлічі параметрів, які будуть задіяні у процесі аналізу та оцінювання ризиків. Для визначення множин як основу використовуємо кортежну Модель базових характеристик ризику (п. 2.1):

$\boldsymbol{BC_1} = \bigcup_{i=1}^{bc_1} BC_{1i}$ дія, яка може привести до BC_2 (наприклад, для і $bc_1 = 5$ експерти можуть ідентифікувати, наступні $\boldsymbol{BC_1} = \bigcup_{i=1}^{5} BC_{1i} = \{BC_{11}, BC_{12}, BC_{13}, BC_{14}, BC_{15}\}$ ={«Зараження вірусами», «Помилки програмування», «Порушення роботи операційної системи», «Порушення цілісності системи безпеки», «Відмова в обслуговуванні»});

$\boldsymbol{BC_2} = \bigcup_{i=1}^{7} BC_{2i}$ подія порушення ІБ (наприклад, BC_2 може відбиватися значенням BC_{27} = «КЦД»). Для відображення спільного результату оцінювання ризику скористаємося ЛП «РІВЕНЬ РИЗИКА» (LR), що визначається кортежем [21-29] $<LR, \underset{\sim}{T}_{LR}, X_{LR}>$, де базові терм- множини задаються m термами $\underset{\sim}{\boldsymbol{T}}_{LR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{LR_j}$ (наприклад, для $m=5 - \bigcup_{j=1}^{5} \underset{\sim}{T}_{LR_j}$ = {«Рівень ризику порушення ІБ дуже низький» (НР), «Рівень ризику порушення ІБ низький» (РН), «Рівень ризику порушення ІБ середній» (РС), «Рівень ризику порушення ІБ високий» (РВ), «Рівень ризик порушення ІБ дуже високий» (ВР)}, які можуть бути відображені на універсальній безлічі $X_{LR} \in \{0, max_{LR}\})$. Для кожного з термів $\underset{\sim}{T}_{LR_1}, \ldots, \underset{\sim}{T}_{LR_j}, \ldots, \underset{\sim}{T}_{LR_m}$ задається свій інтервал значень $[lr_{min}; lr_1[, \ldots, [lr_j; lr_{j+1}[, \ldots, [lr_m; lr_{max}]$ (наприклад, при m = 5 $\underset{\sim}{T}_{LR_1}$, $\underset{\sim}{T}_{LR_2}$, $\underset{\sim}{T}_{LR_3}$, $\underset{\sim}{T}_{LR_4}$, $\underset{\sim}{T}_{LR_5}$ визначимо інтервали з використанням шкали Харрінгтона [26], яку модифікуємо

збільшенням її градуйованих значень у два порядки, тобто $[lr_{min};\ lr_1[$, $[lr_2;\ lr_3[$, $[lr_4;\ lr_5[$, $[lr_6;\ lr_7[$, $[lr_8;\ lr_{max}]$ будуть відповідати наступним значенням - ([0; 20 [, [20; 40 [, [40; 60 [, [60; 80 [, [80; 100]])]). Далі, для створення можливості експерту при оцінюванні використовувати ширший спектр величин, скористаємося вищезгаданою моделлю базових характеристик ризику і поставимо безліч таких характеристик:

$$EC_{Fh} \in \{EC_i\} = \{BC_3, BC_4, BC_5, BC_6\} \ (i = \overline{1,g})$$

де Fh – шістнадцятковий код, бінарне значення якого наступним чином відображає порядковий номер характеристики у множині: BC_3 розташовується в розряді 2^3, BC_4 в 2^2, BC_5 – 2^1, BC_6 - 2^0 (наприклад, якщо експерти хочуть скористатися BC_3, BC_4 і BC_6 то:

$$g=3\ (i = \overline{1,3}),\ \text{а}\ EC_{Dh} \in \{EC_i\} = \{EC_1, EC_2, EC_3\} = \{BC_3, BC_4, BC_6\})$$

Введемо ЛП «РІВЕНЬ EC_i» (C_{ECi}), яка визначається кортежем $<C_{EC_i},\ T_{\sim C_{EC_i}},\ X_{EC_i}>$, де базові терм- множини задаються m термами: $T_{\sim C_{EC_i}} = \bigcup_{j=1}^{m} T_{\sim C_{EC_i j}}$ (наприклад, при m=5– $\bigcup_{j=1}^{5} T_{\sim C_{EC_i j}}$ = {«дуже низький» (ВІН), «низький» (Н), «середній» (С), «високий» (В), «дуже високий» (ОВ)}, які в лінгвістичної формі характеризують рівень Характеристики і можуть бути відображені на універсальну безліч $X_{EC_i} \in \{0,\ \max_{C_{EC_i}}\})$ Для кожного ЄС і $[c_{EC_i \min}; c_{EC_i 1}[, \ldots, [c_{EC_i j};\ c_{EC_i j+1}[, \ldots, [c_{EC_i m};\ c_{EC_i \max}]$ (наприклад, при m =5 для термів $T_{\sim C_{EC_3 1}}$, $T_{\sim C_{EC_3 2}}$, $T_{\sim C_{EC_3 3}}$, $T_{\sim C_{EC_3 4}}$, $T_{\sim C_{EC_3 5}}$ базової характеристики EC_3 = {BC_6}, здійснимо розбиття значення на інтервали - $[c_{EC_3 \min}; c_{EC_3 1}[$, $[c_{EC_3 2}; c_{EC_3 3}[$, $[c_{EC_3 4}; c_{EC_3 5}[$, $[c_{EC_3 6}; c_{EC_3 7}[$, $[c_{EC_3 8}; c_{EC_3 \max}]$ яким будуть відповідати значення ([0; 0,1[, [0,1; 0,2[, [0,2; 0,3[, [0,3; 0,4[, [0,4; 0,5]). Для зручності відобра-

ження базових характеристик через інтервали допустимих значень скористаємося табл. 2.3. Оцінка значимості EC_i здійснюється параметрами з безлічі $\boldsymbol{LS} \in \{LS_i\}\ (i = \overline{1,g})$, а оцінка поточного значення оцінного компонента - за допомогою безлічі $\boldsymbol{ec} \in \{ec_i\}\ (i = \overline{1,g})$.

Таблиця 2.3

Відображення значень базових характеристик

EC_i	Інтервали значень C_{EC_i} для $T_{\sim C_{EC_i 1}} - T_{\sim C_{EC_i m}}$				
	$T_{\sim C_{EC_i 1}}$	…	$T_{\sim C_{EC_i j}}$	…	$T_{\sim C_{EC_i m}}$
EC_1	$[c_{EC_1 \min}; c_{EC_1 1}[$	…	$[c_{EC_1 j}; c_{EC_1 j+1}[$	…	$[c_{EC_1 m}; c_{EC_1 \max}]$
…	…	…	…	…	…
EC_i	$[c_{EC_i \min}; c_{EC_i 1}[$	…	$[c_{EC_i j}; c_{EC_i j+1}[$	…	$[c_{EC_i m}; c_{EC_i \max}]$
…	…	…	…	…	…
EC_g	$[c_{EC_g \min}; c_{EC_g 1}[$	…	$[c_{EC_g j}; c_{EC_g j+1}[$	…	$[c_{EC_g m}; c_{EC_g \max}]$

Етап 2 – Опис базових характеристик. На цьому етапі проводиться опис набору використовуваних базових характеристик, які, на думку експерта-аналітика, з одного боку, впливають на оцінювання ризиків ІБ, а з іншого – оцінюють його різні за природою сторони, наприклад, що враховують особливості організації (банк, архів, силові відомства, завод та ін.). Для цього експерт повинен визначити шістнадцятковий код, за яким із $\{EC_i\}$ вибираються значення відповідних компонентів, наприклад, при коді:

$$Dh - g{=}3,\ a\ EC_{Dh} \in \{EC_i\} = \{EC_1, EC_2, EC_3\} = \{BC_3, BC_4, BC_6\}\ (i = \overline{1,3})$$

або при коді

$$Fh - g{=}4,\ a\ EC_{Fh} \in \{EC_i\} = \{EC_1, EC_2, EC_3, EC_4\} = \{BC_3, BC_4, BC_5, BC_6\}\ (i = \overline{1,4}).$$

Етап 3 – Оцінка рівня важливості базових показників. На цьому етапі кожному компоненту – ЄС і ставиться у відповідність до рівня його значущості – LS_i. Зазначимо, якщо для всіх LS справедливе відношення порядку:

$$LS_i \geq LS_{i+1}, \tag{2.9}$$

то значимість і-го компонента визначається по правилу Фішберна:

$$LS_i = \frac{2(g-i+1)}{(g-1)g}, \tag{2.10}$$

Згідно з цим правилом, у експерта відсутня інформація (крім умови (2.1)) про значущість компонента і тоді (2.2) відображає максимум ентропії інформаційної невизначеності про об'єкт дослідження. Якщо ж всі компоненти мають рівну значимість (Рівно переважні тобто $LS_i = LS_{i+1}$ або системи уподобань ні), то [30]:

$$LS_i = 1/g, \tag{2.11}$$

Етап 4 – Визначення еталонних значень рівня ризику. У цьому етапі експертами визначаються еталонні значення для LR, тобто, задається кількість термів у базовій терм-множині ЛП і ставитися їм у відповідність свій інтервал значень, що лежить в діапазоні [lr_{min}; lr_{max}].

Етап 5 – Визначення еталонних значень базових Показників. Тут експертами Виготовляється визначення еталонних значень для C_{EC}, тобто. задається кількість термів у терм-множині ЛП.

Таблиця 2.4

Приклад визначення еталонних значень базових компонент

EC_i	Інтервали значень для C_{EC_i} $T_{\sim C_{EC_i1}} - T_{\sim C_{EC_i5}}$				
	$T_{\sim C_{EC_i1}}$	$T_{\sim C_{EC_i2}}$	$T_{\sim C_{EC_i3}}$	$T_{\sim C_{EC_i4}}$	$T_{\sim C_{EC_i5}}$
EC_1= BC_3	$T_{\sim C_{BC_31}} \in [0; 20[$	[20; 40[	[40; 60[	[60; 80[	$T_{\sim C_{BC_35}} \in [80; 100]$
EC_2= BC_4	$T_{\sim C_{BC_41}} \in [0; 2[$	[2; 4[	[4; 6[	[6; 8[	$T_{\sim C_{BC_45}} \in [8; 10]$
EC_3= BC_5	$T_{\sim C_{BC_51}} \in [0;0,2[$	[0,2; 0,4[	[0,4; 0,6[	[0,6; 0,8[	$T_{\sim C_{BC_55}} \in [0,8; 1]$
EC_4= BC_6	$T_{\sim C_{BC_61}} \in [0; 0,1[$	[0,1; 0,2[	[0,2; 0,3[	[0,3; 0,4[	$T_{\sim C_{BC_65}} \in [0,4; 0,5]$

Етап 6 – Оцінка поточних значень характеристик. На цьому етапі за кожною базовою характеристикою $\{EC_i\}=\{BC_3, BC_4, BC_5, BC_6\}$ $(i=\overline{1,g})$ експерти відповідної предметної області визначають ЕС для всіх BC_1 при:

$$(bc_1=\overline{1,n}) \qquad \{ec_i^{BC_{1bc_1}}\}=\{ec_{BC_3}^{BC_{1bc_1}}, \quad ec_{BC_4}^{BC_{1bc_1}}, \quad ec_{BC_5}^{BC_{1bc_1}}, \quad ec_{BC_6}^{BC_{1bc_1}}\}$$

виставляються на підставі переваг експертів, статистичної інформації і ін. даних.

У табл. 2.5 показаний приклад визначення поточних значень для $\boldsymbol{BC_1}=\bigcup_{i=1}^{5} BC_{1i}$ описаних на етапі 1 при g=4, а:

$$EC_{Fh} \in \{EC_i\}=\{BC_3, BC_4, BC_5, BC_6\} \ (i=\overline{1,4})$$

Таблиця 2.5

Приклад 1 - Визначення поточних значень базових характеристик

EC_i	$ec_i^{BC_{11}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{12}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{13}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{14}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{15}}$	$T_{\sim C_{EC_i}}$
BC_3,(i=1)	72	В	58	С	64	С	70	В	66	С
BC_4,(i=2)	5,4	С	6	С	2,2	ОН	9	ОВ	5,5	С
BC_5,(i=3)	0,72	В	0,58	С	0,64	С	0,7	В	0,66	С
BC_6,(i=4)	0,23	С	0,33	С	0,12	Н	0,4	В	0,24	Н

Етап 7 – Класифікація поточних значень. При проходженні цього кроку визначається належність $ec_i^{BC_{1bc1}}$ заданому діапазону, за яким формується бінарне значення λ:

$$\lambda_{ij}^{(BC_{1bc1})} = \begin{cases} 1, \text{ при } ec_i^{BC_{1bc1}} \in [\, c_{EC_i(j-1)}; c_{EC_ij}[\\ 0, \text{ при } ec_i^{BC_{1bc1}} \notin [\, c_{EC_i(j-1)}; c_{EC_ij}[\end{cases}, \quad (2.12)$$

відображає перевагу експерта щодо значень оціночних параметрів, а результати обчислень для зручності заносяться до табл. 2.6.

Таблиця 2.6

Класифікація поточних значень базових характеристик

EC_i	$\lambda_{ij}^{(BC_{1bc1})}$ для $T_{\sim C_{EC_ij}}$ $(i=\overline{1,g},\ j=\overline{1,m})$				
	$T_{\sim C_{EC_i1}}$	…	$T_{\sim C_{EC_ij}}$	…	$T_{\sim C_{EC_im}}$
EC_1	λ_{11}	…	λ_{1j}	…	λ_{1m}
…	…	…	…	…	…
EC_i	λ_{i1}	…	λ_{ij}	…	λ_{im}
…	…	…	…	…	…
EC_g	λ_{g1}	…	λ_{gj}	…	λ_{gm}

Аналогічні проводиться перетворення для всіх BC_1, наприклад, для тих, що визначені на етапі 1. Усі обчислені значення $\lambda_{ij}^{(BC_{11})}, \lambda_{ij}^{(BC_{12})} \ldots \lambda_{ij}^{(BC_{15})}$ занесемо в табл. 2.7.

Етап 8 – Оцінка рівня ризику. На цьому етапі проводиться обчислення показника рівня ризику порушення ІБ $lr^{(BC_{1bc_1})}$ по формулі:

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m}\left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right), \qquad (2.13)$$

де lr_j=90-20(j-1) $\lambda_{ij}^{(BC_{1bc_1})}$ визначається по формулі (2.4) для кожною BC_{1bc_1} $(bc_1 = \overline{1,n})$, а $LS_i (i = \overline{1,g})$ - по формулі (2.2) або (2.3) $(j = \overline{1,m})$.

Таблиця 2.7

Приклад 1 - класифікація поточних значень характеристик

EC_i	Значення λ для $BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$																									
	$\lambda_{ij}^{(BC_{11})}$ для $T_{\sim C_{EC_i m}}$ $(i = \overline{1,4}, j = \overline{1,5})$					$\lambda_{ij}^{(BC_{12})}$ для $T_{\sim C_{EC_i m}}$ $(i = \overline{1,4}, j = \overline{1,5})$					$\lambda_{ij}^{(BC_{13})}$ для $T_{\sim C_{EC_i m}}$ $(i = \overline{1,4}, j = \overline{1,5})$					$\lambda_{ij}^{(BC_{14})}$ для $T_{\sim C_{EC_i m}}$ $(i = \overline{1,4}, j = \overline{1,5})$					$\lambda_{ij}^{(BC_{15})}$ для $T_{\sim C_{EC_i m}}$ $(i = \overline{1,4}, j = \overline{1,5})$				
BC3	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	
BC4	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	
BC5	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	
BC6	0	0	1	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	

Етап 9 – Лінгвістичне розпізнавання. На завершальному етапі здійснюється лінгвістичне розпізнавання отриманого значення за допомогою терм-множин $lr^{(BC_{1bc_1})}$, наприклад, за формулою (2.6) при m =5:

$$\underset{\sim}{T}_{LR} = \begin{cases} HP, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_{\min}; lr_1[\\ PH, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_2; lr_3[\\ PC, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_4; lr_5[\\ PB, \text{ при } lr^{(BC_{1bc_1})} \in [\, lr_6; lr_7[\\ OP, \text{ при } lr^{(BC_{1bc_1})} \in [lr_8; lr_{\max}] \end{cases}, \quad (2.14)$$

де LR відображає обчислене $lr^{(BC_{1bc_1})}$ за допомогою значень терм-множин ЛП «РІВЕНЬ РИЗИКУ». Також по виразу (2.7) можна обчислити середнє значення $lr^{(cp)}$ за оцінюваним ресурсом:

$$lr^{(cp)} = \left(\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})}\right) / m, \quad (2.15)$$

Розглянемо приклад аналізу та оцінювання ризику на основі використання такого ресурсу (активу) інформаційної системи, як поштовий сервер, скориставшись при цьому прикладом для параметрів BC_1 і BC_2 визначених на етапі 1. Їх ідентифікацію найбільш часто здійснюють на основі суджень експертів або за допомогою запитів, за допомогою складених експертами опитувальників. Наведемо приклад запитів у відповідність до стандарту ISO/IEC 27002:

1) Чи існує в організації певна, впроваджена та затверджена процедура отримання дозволу щодо використання нових засобів обробки інформації? (Пункт 6.1.4 стандарту). Для відповіді на цей запит пропонується вибрати відповідь ТАК або НІ. Якщо експерт відповідає ТАК, то відбувається уточнення, як ця процедура організована на підприємстві.

1.1 Чи схвалено нові засоби обробки інформації зі сторони:

а) керівництва користувачів; якщо відповідь ТАК - перехід до наступного, якщо НІ - можуть бути реалізовані всі $BC_{1bc_1}\ (bc_1 = \overline{1,5})$;

б) адміністраторів засобів управління; якщо відповідь ТАК – перехід до наступного, якщо НІ – може бути реалізовано BC_{13}- BC_{15};

в) менеджером локальної інформаційної системи. Якщо експерт відповів ТАК - перехід до наступного, якщо НІ - можуть бути реалізовані BC_{12}- BC_{15};

1.2 Чи перевірено сумісність з іншими компонентами системи? Якщо ТАК – перехід до наступного, якщо НІ – може бути реалізовано BC_{13}- BC_{15};

1.3 Чи використовуються засоби обробки інформації особистої чи приватної власності: портативні комп'ютери, домашні комп'ютери або прилади для обробки ділової інформації та визначено, чи впроваджені необхідні заходи контролю? Якщо відповідь ТАК - перехід до наступного, якщо НІ - можуть бути реалізовані всі BC_{1bc_1}.

У разі якщо експертом була дана відповідь НІ на запит 1, то це може призвести до BC_{17} і всім BC_1. Проведемо опитування за цим запитом та опрацюємо варіанти відповідей. Припустимо, що на запит 1 експерт дав позитивну відповідь, отже, перейшов до уточнення даних, на що дав наступні відповіді: 1.1а - ТАК; 1.1б - ТАК; 1.1в - НІ; 1.2 ТАК; 1.3 НІ.

Етап 1. Зробимо обробку відповідей та визначення базових характеристик. І так, щодо даного активу можуть бути спрямовані всі $BC_{1bc_1}.(bc_1 = \overline{1,n})$, при реалізації яких можливі наступи певних BC_1, що описується зв'язками:

$$BC_{11} => BC_{25} = \text{«НЦД»};\ BC_{12} => BC_{27} = \text{«НКЦД»};\ BC_{13} => BC_{25} = \text{«НЦД»};\ BC_{14} => BC_{27} = \text{«НКЦД»};\ BC_{15} => BC_{23} = \text{«НД»}$$

(наприклад, остання зв'язка інтерпретується так: щодо поштового сервера може бути реалізована дія (реалізація потенційних загроз), що призводить до відмови в обслуговуванні та події, що ініціює порушення доступності ресурсу). Таким чином, безліч

BC_2 для даного активу, відображається як $BC_2 = \{BC_{23}, BC_{25}, BC_{27}\}$. При оцінці ступеня ризику використовуємо відповідну ЛП з терм-множиною та інтервалами значень, які як приклад, розглянуті на етапі 1.

Етап 2. Скористаємося базовими характеристиками, визначеними в прикладі етапу 1 при g=4, $EC_{Fh} \in \{EC_i\}=\{EC_1$ - ймовірність (BC_3), EC_2 - небезпека $(BC_4 =)$, EC_3 – частота (BC_5), EC_4 – Витрати $(BC_6)\}$, $(i = \overline{1,g})$.

Етап 3. Оцінку LS здійснимо по формулі (2.3) $LS_i = 1/g = 0{,}25$ $(i = \overline{1,4})$.

Етап 4. Для визначення еталонних значень рівня ризику скористаємося прикладом, описаним на етапі 1 де $[lr_{min}; lr_{max}]$ відповідає [0; 100].

Етап 5. На основі попереднього експертного аналізу отримуємо еталонні значення C_{EC_i} з заданими інтервалами. Для цього скористаємося даними з прикладу етапу 1 та таблиця. 2.4 де розбиття на інтервали компонента BC_5 ґрунтується на шкалі Харрінгтона, а BC_3 – на її модифікації шляхом збільшення у два порядки градуйованих значень. Діапазон значень BC_4 та BC_6 визначається на розсуд експертів.

Етап 6. Поточний стан ІБ активу характеризується значеннями базових характеристик ЕС по кожному BC_1 (таблиця. 2.5), які визначаються на основі експертних суджень. Для подальших розрахунків будуть використовуватися дані з табл. 2.6.

Етап 7. Для кожного BC_{1bc_1} $(bc_1 = \overline{1,5})$ на підставі вирази (2.4) щодо заданих діапазонів (див. табл. 2.4) здійснюється класифікація поточних значень $ec_i^{BC_{1bc_1}}$ за допомогою бінарної змінної $\lambda_{ij}^{(BC_{1bc_1})}$ конкретні значення якої занесені в таблиці. 2.7.

Етап 8. Виробимо обчислення показника рівня ризику порушення ІБ по формулі (2.5), де:

$$m = 5,\ j = \overline{1,5}, i = \overline{1,4},\ bc_1 = \overline{1,5}, lr_1=10,\ lr_2=30,\ lr_3=50,\ lr_4=70, lr_5=90,$$

Тоді:

$$lr^{(BC_{11})}=0+35+25+0+0=60,\quad lr^{(BC_{12})}=60,\quad lr^{(BC_{13})}=50,\quad lr^{(BC_{14})}=80,$$

$$lr^{(BC_{15})}=50.$$

Етап 9. Для лінгвістичного розпізнавання отриманого значення $lr^{(BC_{1bc_1})}$ скористаємося формулою (2.6), де $[lr_{min};lr_{max}]$ відповідає [0; 100], а:

$$\underset{\sim}{T}_{LR}=\begin{cases} HP, при\ lr^{(BC_{1bc_1})}\in[\ 0;\ 20[\\ PH, при\ lr^{(BC_{1bc_1})}\in[20;\ 40[\\ PC, при\ lr^{(BC_{1bc_1})}\in[\ 40;\ 60[\\ PB, при\ lr^{(BC_{1bc_1})}\in[60;\ 80[\\ OP, при\ lr^{(BC_{1bc_1})}\in[\ 80;\ 100] \end{cases}, \qquad (2.16)$$

Тоді показниками $lr^{(BC_{11})}, lr^{(BC_{12})}$, $lr^{(BC_{13})}$, $lr^{(BC_{14})}, lr^{(BC_{15})}$ відповідно певні значення ЛП: «РВ», «РВ», «РС», «ОР», «РС».

Також для даного активу по виразу (2.7) обчислюється середнє значення рівня ризику $lr^{(cp)}=(\sum_{bc_1=1}^{5} lr^{(BC_{1bc_1})})/5=(60+60+50+80+50)/5=60$ далі, по формулі (2.6) визначається його лінгвістичний еквівалент – «РВ». У цілях верифікації методу виконаємо аналогічні обчислення при середовищі оточення заданого ресурсу з підвищеним рівнем ризику, то є експертами було оцінено поточний значення $ec_i^{BC_{1bc_1}}$ для всіх BC_{1bc_1} на рівні $\underset{\sim}{T}_{C_{EC_i 4}}=\{«В»\}$ і $\underset{\sim}{T}_{C_{EC_i 5}}=\{«ОВ»\}$. Результати обчислень (за аналогії з табл. 2.5) занесемо в таблиці. 2.8.

Таблиця 2.8

Приклад 2 – визначення поточних значень базових характеристик

EC_i		$T_{\sim C_{EC_i}}$	$ec_i^{BC_{12}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{13}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{14}}$	$T_{\sim C_{EC_i}}$	$ec_i^{BC_{15}}$	$T_{\sim C_{EC_i}}$
BC_3, (i=1)	0	В	9	В	5	ОВ	6	ОВ	1	В
BC_4, (i=4)	4	В		ОВ		В	3	ОВ	9	ОВ
BC_5, (i=2)	92	ОВ	83	В	9	ОВ	61	В	2	В
BC_6, (i=3)	44	ОВ	39	В	45	ОВ	48	В	43	ОВ

Далі проводиться класифікація поточних значень $ec_i^{BC_{1bc_1}}$ по формулі (2.4), а результати заносяться до таблиці 2.9.

Таблиця 2.9

Приклад 2 - класифікація поточних значень характеристик

	Значення λ для $BC_1 \in \{BC_{1bc_1}\}$ $(bc_1 = \overline{1,5})$																									
C_i	$\lambda_{ij}^{(BC_{11})}$ для $T_{\sim C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{12})}$ для $T_{\sim C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{13})}$ для $T_{\sim C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{14})}$ для $T_{\sim C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$					$\lambda_{ij}^{(BC_{15})}$ для $T_{\sim C_{EC_i m}}$ $(i=\overline{1,4}, j=\overline{1,5})$				
C_3																										
C_4																										
C_5																										
C_6																										

Здійснимо обчислення показника рівня ризику за формулою (2.5):

$$lr^{(BC_{11})}=85,\quad lr^{(BC_{12})}=80,\quad lr^{(BC_{13})}=85,\quad lr^{(BC_{14})}=80,\quad lr^{(BC_{15})}=85$$

і для лінгвістичного розпізнавання отриманих результатів скористаємося формулою (2.6), тоді всім показникам $lr^{(BC_{11})}$, $lr^{(BC_{12})}$, $lr^{(BC_{13})}$, $lr^{(BC_{14})}$, $lr^{(BC_{15})}$ відповідають значення ЛП: «ОР». Далі обчислюється середнє значення рівня ризику $lr^{(ср)}=(85+80+85+80+85)/5=83$ і за формулою (2.6) визначається його лінгвістичний еквівалент – «ОР». Як видно, зі збільшенням агресивності середовища оточення відповідно збільшився, як середній ризик, так і окремі значення по BC_{1bc_1} $(bc_1=\overline{1,5})$.

ВИСНОВОК ДО РОЗДІЛУ 2

Кортежна модель базових характеристик ризику, яка за рахунок композиції базових характеристик, відображених шестикомпонентним кортежем, дозволяє будувати гнучкіші та ефективніші методи аналізу та оцінювання ризиків щодо динамічно змінюваних наборів характеристик.

Проведено дослідження широкого спектру існуючих ЗАОР з урахуванням запропонованої моделі та визначено набір базових характеристик, за якими можна здійснити порівняльний аналіз таких ЗАОР та вибрати найбільш підходящі для вирішення відповідних завдань ЗІ.

РОЗДІЛ 3
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СИСТЕМИ АНАЛІЗУ І ОЦІНЮВАННЯ РИЗИКІВ

3.1. Базовий алгоритм роботи системи аналізу та оцінювання ризиків інформаційної безпеки

На підставі запропонованих структурних схем First-ЗАОР та Second-ЗАОР систем можна реалізувати програмні продукти, що дозволяють проводити аналіз та оцінювання ризиків ІБ в автоматизованому режимі, їх базовий алгоритм роботи (рис. 3.1) можна описати наступними етапами:

1) Створення нового ПП або відкриття існуючого;

2) Вказівка імені існуючого ПП;

3) Відкриття ПП з збереженими налаштуваннями та наявними даними, що зберігаються у БДПП;

4) Вказівка імені нового ПП і здійснення вибору методу FirstM або SecondM;

5) Створення проєкту з вибраними параметрами, що реалізується за допомогою створення таблиці ПП у БД та завантаження порожнього проєкту;

6) Вибір $IR,\ BC_{1bc_1}$ та вказівка значення $ec_i^{BC_{1bc_1}}$;

7) Оцінка $lr^{(BC_{1bc_1})}$ для зазначеного набору $IR_h,\ BC_{1bc_1}$ і BC_{2bc_2};

8) Запис в БД користувальницьких даних і розрахованого $lr^{(BC_{1bc_1})}$;

9) Розрахунок $lr^{(cp)}$ для кожного ІР зазначеного в ПП;

10) Генерація звітів з вказівкою всіх IR_h і відповідних їм BC_{1bc_1}, а також інформації про $lr^{(cp)}$, для ІР в числовій і лінгвістичної формі і $lr^{(BC_{1bc_1})}$ для кожної загрози в окремо.

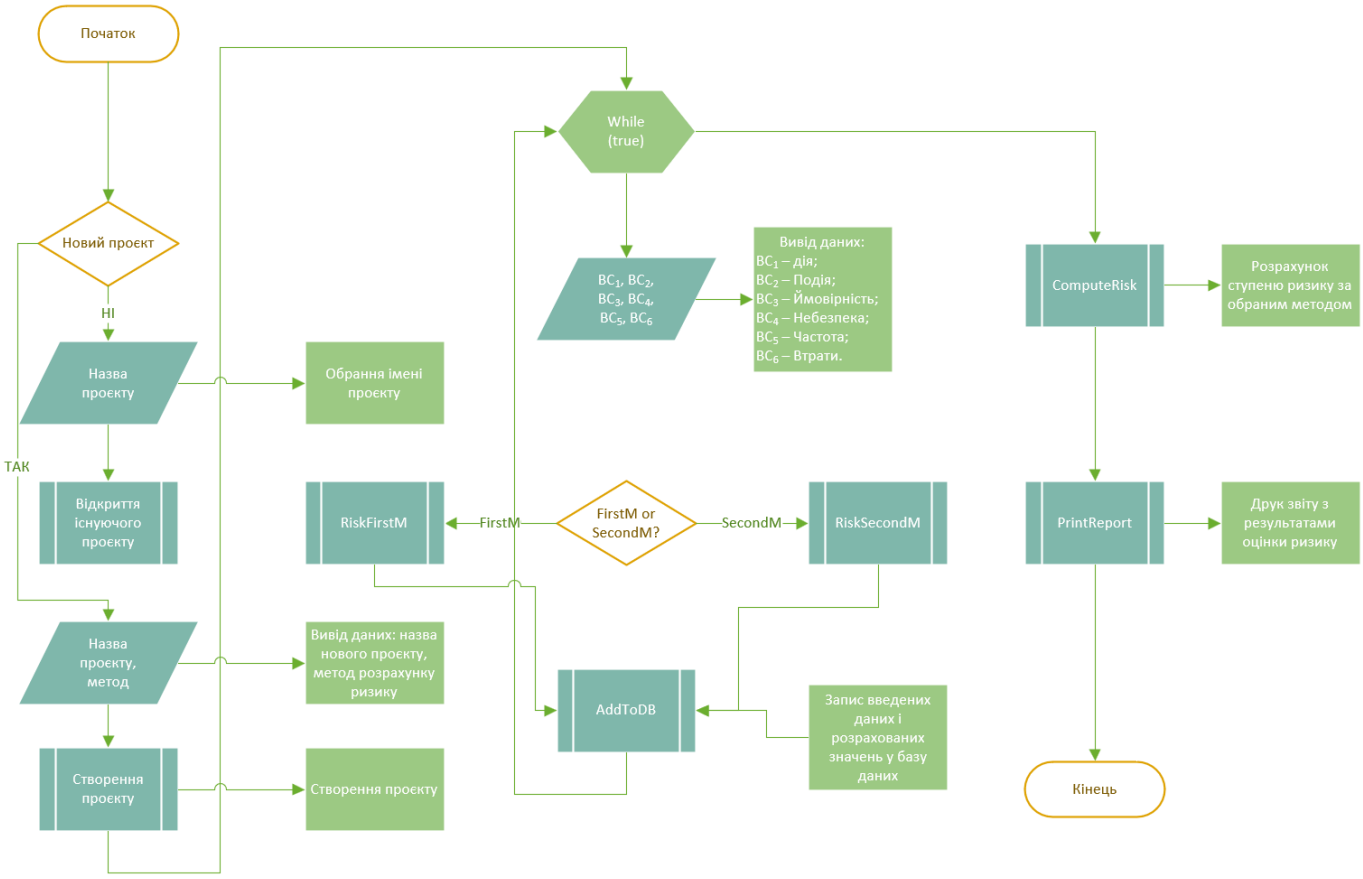


Рис. 3.1. Базовий алгоритм роботи систем аналізу і оцінювання ризиків ІБ

На підставі запропонованої методології можна будувати як програмні, так і програмно-апаратні системи, призначені для ефективного аналізу та оцінювання ризику ІБ, які використовують як вхідні дані різні набори базових характеристик, що дозволяє підвищити гнучкість і розширює можливості проєктованих ЗАОР, що функціонують як в детермінованому, так і в нечітко визначеному слабоформалізованому середовищі. З використанням цієї методології було представлено структурні рішення ЗАОР.

На основі розроблених структур First-ЗАОР систем створено програмні засоби, які на відміну від відомих п. 2.2 використовують як вхідні дані різні набори базових характеристик, що підвищує гнучкість, зручність використання, інтеграцію можливостей та розширює можливість проєктованих засобів аналізу та оцінювання ризиків ІБ функціонуючих як у детермінованому, так і в нечіткому, слабо формалізованому середовищі.

3.2. Вивчення First-ЗАОР системи

Паралельно зі стрімким розвитком та впровадженням ІТ-технологій у всі сфери діяльності людства зростає і кількість загроз, пов'язаних з порушенням конфіденційності, цілісності та доступності ІР, які обробляються за допомогою цих технологій. Тому безпека таких ресурсів стає пріоритетним завданням як для підприємницької діяльності, так і для держави загалом. На сьогоднішній день вирішувати таке завдання доцільно за допомогою системи управління ІБ. Для побудови такої системи необхідно проводити аналіз та оцінювання ризиків ІБ, які часто характеризуються високою невизначеністю.

На даний момент існує необхідність в ефективних засобах, які б дозволили в автоматизованому режимі здійснювати оцінювання ризиків. Для вирішення такого завдання, використовуючи методологію синтезу ЗАОР ІБ п. 3.1, яка заснована на логіко-лінгвістичному підході, відомих методах п. 2.3 та п. 2.4 та кортежної моделі базових характеристик ризику п. 2.1, було запропоновано нові відповідні структурні рішення систем оцінювання п. 3.2. і п. 3.3.

Для практичного застосування розроблених методів та відповідних структурних реалізацій систем необхідно вирішити актуальне завдання з розробки ПЗ ЗАОР, які дозволять на практиці здійснювати оцінювання за різних вихідних величин, а також враховувати можливості експерта щодо чіткого детермінування оцінюваних базових характеристик та його невпевненості у своїх судженнях.

У зв'язку з цим, метою роботи є створення та верифікація засобів оцінювання, які дозволять проводити аналіз та оцінювання ризиків ІБ на основі обраного базису характеристик у детермінованому та нечіткому, слабоформалізованому середовищі.

Досягнення поставленої мети здійснимо на основі запропонованих структурних рішень First-ЗАОР систем п. 3.2 та п. 3.3. Відповідні ПЗ ґрунтуються на розробках, які на відміну від відомих п. 2.2 використовують як вхідні дані різні набори базових характеристик. Це підвищує гнучкість, зручність використання, інтеграцію можливостей та розширює спектр функцій інструментальних засобів працюючих у детермінованому середовищі, для якої більшою мірою характерна визначеність та стабільність

і вона досить стійка до впливу різноманітних збурень у часі. Також ці засоби орієнтовані до роботи у нечіткому середовищі, яке характеризується великим ступенем невизначеності, випадковості, нестабільності, впливом різноманітних збурень у часі тощо, а формалізації її процесів використовується математичний апарат теорії нечітких множин.

Розроблені ПЗ були реалізовані на основі методології синтезу систем аналізу та оцінювання ризиків ІБ п. 3.1, згідно з якою на першому етапі необхідно здійснити вибір методу оцінювання. Далі згідно з методологією, для ідентифікації ІР, а також дій та подій порушення ІБ здійснюється формування відповідних баз даних (БД):

- дій $BC_{1bc_1}(bc_1 = \overline{1,n})$ складеною на основі переліку загроз з ISO / IEC 27002:2005;

- інформаційних ресурсів IR_h, містить в собі перелік ресурсів згідно з методом CRAMM для профілю Commercial;

- базових характеристик $ec_i^{BC_{1bc_1}}$ (БХ).

Для зручності та подальшого використання отриманих результатів у ПЗ усі дані зберігаються у проєктах користувачів, які у свою чергу зібрані у БД. Зазначимо, що тут як вхідні дані виступають:

$$IR \in \{IR_h\}\ (h = \overline{1,\ 20});$$
$$BC_1 \in \{BC_{1bc_1}\}\ (bc_1 = \overline{1,\ 60});$$
$$BC_2 \in \{BC_{2bc_2}\}\ (bc_2 = \overline{1,7}),$$

а значення:

$$ec_i^{BC_{1bc_1}}:\ \ \{ec_i^{BC_{1bc_1}}\} = \{ec_{BC_3}^{BC_{1bc_1}},\ \ ec_{BC_4}^{BC_{1bc_1}},\ \ ec_{BC_5}^{BC_{1bc_1}},\ \ ec_{BC_6}^{BC_{1bc_1}}\},\ \text{де}\ i = \overline{1,4}.$$

Ідентифікатори IR_h і BC_{1bc_1} набувають текстових значень відповідні найменуванням з зазначених переліків.

Розглянемо роботу First-ЗАОР системи. Для наступного оцінювання УР, що відображається параметром LR згідно методології п. 3.1, здійснюється формування еталонних значень РР. У запропонованому ПЗ діапазон числових значень рівня ризику лежить у межах від 0 до 100. У лінгвістичній формі LR може відображатися такими значеннями:

- «Рівень ризику порушення ІБ дуже низький» (НР);
- «Рівень ризику порушення ІБ низький» (РН);
- «Рівень ризику порушення ІБ середній» (РС);
- «Рівень ризику порушення ІБ високий» (РВ);
- «Рівень ризику порушення ІБ високий» (ВР).

Для визначення відповідності (лінгвістичне розпізнавання) отриманого числового значення РР $lr^{(BC_{1bc1})}$ лінгвістичному, застосовується формула (3.1):

$$\underset{\sim}{T}_{LR} = \begin{cases} HP, \text{ при } lr^{(BC_{1bc1})} \in [\, lr_{\min}; lr_1[\\ PH, \text{ при } lr^{(BC_{1bc1})} \in [\, lr_2; lr_3[\\ PC, \text{ при } lr^{(BC_{1bc1})} \in [\, lr_4; lr_5[\\ PB, \text{ при } lr^{(BC_{1bc1})} \in [\, lr_6; lr_7[\\ OP, \text{ при } lr^{(BC_{1bc1})} \in [lr_8; lr_{\max}] \end{cases}, \quad (3.1)$$

Де $[lr_{min};\ lr_1[,\ [lr_2;\ lr_3[,\ [lr_4;\ lr_5[,\ [lr_6;\ lr_7[,\ [lr_8;\ lr_{max}]$ наприклад, відповідатимуть значення [0; 20 [, [20; 40 [, [40; 60 [, [60; 80 [, [80; 100]. Формування еталонних значень для БХ в ПЗ було реалізовано в наступному вигляді:

- BC_3 (Приймає значення в діапазоні від 0 до 100, крок дискретизації - 1);
- BC_4 (Приймає значення від 0 до 10, крок дискретизації - 1);
- BC_5 (перебуває в діапазоні від 0 до 1, крок дискретизації - 0,01);
- BC_6 (лежить в межах від 0 до 0,5, крок дискретизації - 0,01).

На етапах формування рівня значимості і визначення поточного значення БХ ПЗ для введення даних використовується інтерактивний інтерфейс. Класифікація поточних значень та оцінка РР у ПЗ здійснюється у автоматизованому режимі. При цьому, для кожної дії (Загрози) реалізується розрахунок значення $lr^{(BC_{1bc_1})}$ по виразу:

$$lr^{(BC_{1bc_1})} = \sum_{j=1}^{m}\left(lr_j \sum_{i=1}^{g} LS_i \lambda_{ij}^{(BC_{1bc_1})} \right), \tag{3.2}$$

де lr_j=90-20(j-1),

$$\lambda_{ij}^{(BC_{1bc_1})} = \begin{cases} 1, \text{при } ec_i^{BC_{1bc_1}} \in [\, c_{EC_i(j-1)}; c_{EC_ij}[\\ 0, \text{при } ec_i^{BC_{1bc_1}} \notin [\, c_{EC_i(j-1)}; c_{EC_ij}[\end{cases} (bc_1 = \overline{1,n}), \tag{3.3}$$

$$LS_i = \frac{2(g-i+1)}{(g-1)g}\ (i=\overline{1,g}) \text{ або } LS_i = 1/g\ (j=\overline{1,m}).$$

Для ІР значення $lr^{(cp)}$ обчислюється на основі виразу:

$$lr^{(cp)} = \left(\sum_{bc_1=1}^{m} lr^{(BC_{1bc_1})}\right) / m\,. \tag{3.4}$$

Отримані результати мають відповідну інтерпретацію, а ПЗ створює необхідний звіт.

Для тестування основних функцій та відображення принципу роботи ПЗ ЗАОР виконаємо його верифікацію за допомогою комп'ютера під керуванням операційної системи Microsoft Windows 11 Professional x64. Розроблений додаток для своєї роботи не вимагає додаткових бібліотек та системних файлів, оскільки при компіляції проєкту були вказані такі опції:

```
Usedynamic RTL = false; Buildwithruntimepackages = false.
```

Також додатково для функціонування БД було встановлено сервер MySQL 5.1.60 x64. За допомогою розробленого ПЗ створено тестовий проєкт «test24», а як IR_1 для верифікації вибрано «мережевий файл-сервер» з категорії «Мережеві сервери». Тестування проводилося за чітко визначених вихідних даних, тобто, у так званому детермінованому середовищі.

Для даного IP були встановлені наступні $BC_{1bc_1}(bc_1 = \overline{1,3})$:

BC_{11} = «Зловживання засобами обробки інформації» (з категорії «Нецільове використання комп'ютерного обладнання та мережі Інтернет співробітниками організації»);

BC_{12} =«Перехоплення інформації на лініях зв'язку шляхом використання різних видів аналізаторів мережевого трафіку» (з категорії «Загрози витоку конфіденційної інформації»);

BC_{13} = «Ушкодження носіїв інформації» (з категорії «Загрози доступності IT-сервісів та руйнування (втрати) інформаційних активів»).

Після цього за кожною загрозою здійснюються розрахунки значень $lr^{(BC_{1bc_1})}$, результати яких представлені в табл. 3.1, з якої видно, що значення рівня ризику для даного IP з усіх загроз низьке.

Таблиця 3.1

Результати оцінювання ПЗ First- ЗАОР

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$\tilde{T}_{LR}$
BC_{11}	42	1	0,67	0,05	35	*PH*
BC_{12}	25	4	0,13	0,31	35	*PH*
BC_{13}	33	3	0,07	0,17	25	*PH*

Далі проводиться розрахунок середнього $lr^{(cp)}$ для даного IP, в результаті чого отримуємо $lr^{(cp)} = 31,67$, що відповідає $\tilde{T}_{LR} - PH$.

Подальша верифікація ПЗ виконувалася на основі моделювання для кількох станів оцінювання:

1-й стан – початкові умови із встановленою кількістю загроз IP;

2-й стан – збільшено кількість загроз для IP;

3-й стан – блоковано одну загрозу для IP;

4-й стан – зміна значень базових характеристик (зменшення чи збільшення).

1-й стан з початковими умовами, і навіть результати обчислення РР, наведено у таблиці 3.2. Розглянемо результати моделювання наступних станів.

2-й стан.

До ПП були внесені зміни шляхом введення додаткового BC_{14} для IR_1 = «Мережевий файл-сервер», тобто, BC_{14} =«Нелегальне використання програмного забезпечення», яке входить в категорію «Юридичні загрози». У табл. 3.2 наведено значення $ec_i^{BC_{1bc_1}}$, які були визначено по оцінках експертів. У результаті цього здійснено розрахунок значення РР для BC_{14}, тобто $lr^{(BC_{14})}=45$, а середнє $lr^{(cp)}$ після інтегрування з BC_{14} складає $lr^{(cp)}=35$, що відповідає значенню $\underset{\sim}{T}_{LR}$ - РН

Таблиця 3.2

Значення $ec_i^{BC_{1bc_1}}$ ПЗ First-ЗАОР

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_5
BC_{11}	42	1	0,67	0,05
BC_{12}	25	4	0,13	0,31
BC_{13}	33	3	0,07	0,17
BC_{14}	69	5	0,45	0,07

3-й стан.

Далі було проведено моделювання в умовах, коли на оцінюваному об'єкті захисту проведено заходи щодо усунення BC_{12} =«Перехоплення інформації на лініях зв'язку шляхом використання різних видів аналізаторів мережевого трафіку». Тут також

виконано повторний вимір $lr^{(BC_{1bc_1})}$ та $lr^{(cp)}$. Використовуючи розроблену систему та враховуючи модельовану ситуацію, отримане значення $lr^{(cp)}$ для IR_1 зменшилося до 30, тобто $lr^{(cp)} \underset{\sim}{T}_{LR} = 30$ (РН). Значення $lr^{(cp)}$ змінюється при зміні кількості BC_{1bc_1}, а РР порушення ІБ во всіх випадках, визначається як низьке. Подальше експериментальне дослідження показало, що при значному збільшенні або зменшенні числа BC_{1bc_1} значення $lr^{(cp)}$ може відповідно адекватно змінитись.

4-й стан.

Після виконаних розрахунків, згідно з 1-м станом, було проведено моделювання для двох ситуацій:

- перша (на об'єкті захисту враховано попередні результати аналізу та оцінювання ризиків ІБ та впроваджено заходи для мінімізації ризиків);
- друга (на об'єкті захисту не враховано попередні результати оцінювання – не прийнято рішень щодо впровадження заходів для зниження ризиків).

З урахуванням першої ситуації на об'єкті захисту було проведено низку заходів, спрямованих на зменшення рівня загроз для заданого ІР, а саме:

- впроваджено систему розмежування доступу, користувачам надано права та привілеї відповідно до їх посадових обов'язків для мінімізації BC_{11} = «Зловживання засобами обробки інформації»;
- розроблено систему шифрування мережевого трафіку для усунення BC_{12} = «Перехоплення інформації на лініях зв'язку шляхом використання різних видів аналізаторів мережного трафіку»;
- реалізовано системи моніторингу стану жорстких дисків, настроєно політику регулярного створення резервних копій критичної інформації, впроваджено технології RAID 1 для нейтралізації BC_{13} = «Ушкодження носіїв інформації».

Після повторної реалізації аналізу та оцінювання ризиків ІБ експертами було встановлено величини базових характеристик, значення яких наведено у табл. 3.3.

Для кожного BC_{1bc_1} був повторно здійснено розрахунок значень $lr^{(BC_{1bc_1})}$, результати якого відображені в таблиці 3.3.

Таблиця 3.3

Значення оціночних компонент і $lr^{(BC_{1bc_1})}$ ПЗ First-ЗАОР

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$T_{\sim LR}$
BC_{11}	12	1	0,37	0,01	15	НР
BC_{12}	25	2	0,13	0,04	15	НР
BC_{13}	5	2	0,05	0,03	10	НР

Також з урахуванням першого та другого стану було здійснено оцінювання ризиків для додаткових трьох ІР. У таблиці 3.5 показано значення $lr^{(cp)}$ для цих ІР.

Таблиця 3.4

Результати оцінювання ПЗ First- ЗАОР

BC_{1bc_1}	BC_3	BC_4	BC_5	BC_6	$lr^{(BC_{1bc_1})}$	$T_{\sim LR}$
BC_{11}	52	1	0,81	0,05	40	*РН*
BC_{12}	45	4	0,23	0,31	45	*РС*
BC_{13}	43	3	0,47	0,27	45	*РС*

Порівнюючи отримані результати, можна дійти висновку, що з зміні значень базових характеристик розроблене ПЗ First-ЗАОР адекватно реагує на відповідні умови середовища оцінювання.

Таблиця 3.5

Значення $lr^{(cp)}$ ПЗ First-ЗАОР

ІР	$lr^{(cp)}$		
	Середній рівень ризику початкові умови	Знижений рівень ризику	Підвищений рівень ризику
IR_1	31,67 (*PH*)	13,33 (*HP*)	43,33 (*PC*)
IR_2	20 (*HP*)	15 (*HP*)	26,5 (*PH*)
IR_3	28,33 (*PH*)	23,33 (*PH*)	30 (*PH*)
IR_4	28,33 (*PH*)	22,5 (*PH*)	31,25 (*PH*)

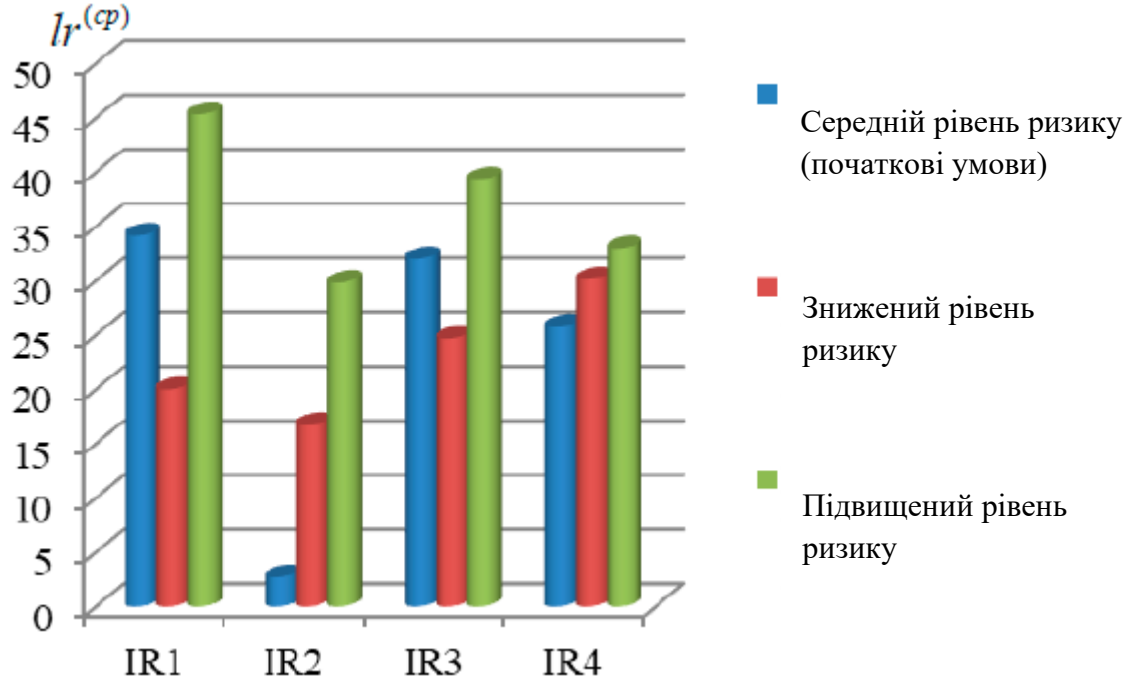


Рис. 3.2. Гістограма середніх значень рівня ризику ПЗ First -ЗАОР

ВИСНОВОК ДО РОЗДІЛУ 3

Проведено експериментальне дослідження з розробленим ПЗ ЗАОР, з метою верифікації розроблених методів, моделі, структурних рішень та ПЗ. Експериментальне дослідження ЗАОР показало, що з будь-якому базисі показників можна реалізо-

вувати адекватну оцінку. Також було проведено розрахунки за різних умов середовища оцінювання: на початковому етапі стану об'єкта захисту; з реалізацією заходів щодо зниження ризику.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ

Результатом даної дипломної робота є розроблена принципова схема комутаційного обладнання для оптимізації потоків трафіку.

Суб'єкт дипломної роботи інженер – проектувальник, який здійснює розробку і аналіз принципової схеми абонентського приймача кабельного цифрового телебачення.

Робоче місце інженера-проектувальника знаходиться в проектувальному відділі на другому поверсі.

4.1. Аналіз небезпечних і шкідливих факторів, що впливають на інженера

Відділ проектування знаходиться на другому поверсі п'ятиповерхового будинку. Приміщення має розміри: довжина 8 м, ширина 4 м, висота 4. Загальна площа - 32 м^2, загальний об'єм – 128 м^3. У відділі знаходиться 5 робочих місць інженерів-проектувальників, оснащені комп'ютерами.

Робоча площа одного співробітника становить:

$$S_{\text{роб}} = \frac{S_{\text{заг.пл}}}{N} = \frac{32}{5} = 6{,}4 \text{ м}^2$$

Робочий об'єм одного співробітника:

$$V_{\text{роб}} = \frac{V_{\text{заг.об}}}{N} = \frac{128}{5} = 25{,}6 \text{ м}^3$$

N- кількість співробітників у відділі

$S_{\text{заг.пл}}$ – загальна площа;

$V_{\text{заг.об}}$ – загальний об'єм.

Відповідно до [31] площа на одне робоче місце має становити не менше ніж 6 м^2, а об'єм не менше ніж 20 м^3. Робоче місце інженера-проектувальника відповідає вимогам.

В проектному відділі інженера-проектувальника знаходяться: комп'ютери, принтер. У даному приміщенні температура повітря у теплий період року становить 30°С, використовується природне та штучне освітлення. Штучне освітлення виконано у вигляді перериввчастих ліній світлодіодних світильників. Рівень шуму в приміщенні становить 54 дБ, а згідно з Державними санітарними нормами [32] не повинен перевищувати 50 дБ.

Робоче місце розташоване так, щоб природне світло падало з лівої сторони, при цьому відстань зі світлом до робочого місця - 1 м. Висота робочої поверхні столу над підлогою 750 мм, глибина столу – 800 мм, ширина столу 1300мм. Робочий стіл має простір для ніг висотою 650 мм та шириною 600 мм.

Перелік шкідливих та небезпечних виробничих чинників.

Створення сприятливих умов праці, в роботі інженера-проектувальника, має велике значення як для полегшення , так і для підвищення продуктивності праці. Відповідно до [33] шкідливими виробничими факторами є:

1. Підвищена температура робочого приміщення
2. Недостатня освітленість робочої поверхні
3. Виробничий шум
4. Електромагнітні випромінювання радіочастотного діапазону
5. Іонізуючі випромінювання

Відповідно до [34] робота інженера-проектувальника у приміщенні з енерговитратами 90-120 ккал/год. відносяться до категорії легких фізичних робіт Іа (роботи, що виконуються сидячи і не потребують фізичного напруження).

Таблиця 4.1

Оптимальні величини температури

Період року	Категорія робіт	Температура повітря,°С
Холодний період року	Легка Іа	22-24
Теплий період року		23-25

Допустимі величини температури на постійних робочих місцях:

Період року	Категорія робіт	Температура повітря,°С	
		Верхня межа	Нижня межа
Холодний період року	Легка Іа	25	21
Теплий період року		28	22

У проектному відділі температура повітря становить 30℃ в теплий період року,що перевищує допустиму на 2 ℃. Забезпечили температуру приміщення 23 ℃,за допомогою механічної вентиляції з вентилятором VORTICE VARIO, повітрообмін якого становить 680 $м^3$ /год.

Недостатня освітленість. В приміщенні встановлені персональні комп'ютери, присутнє природне та штучне освітлення . За вимогами [35], величина коефіцієнта природної освітленості повинна бути не менше 1.5%. В проектному відділі порушенні вимоги, освітленість робочої поверхні складає 370 лк , а коефіцієнт освітленості складає 1.2%. Природне світло проникає у приміщення через бічні світло прорізи. Вікна мають жалюзі. Штучне освітлення виконано у вигляді переривчастих ліній світлодіодних світильників, розташованих паралельно лінії зору інженера-проектувальника. Для місцевого освітлення використовувати галогенні лампи розжарювання

Виробничий шум. Шум на робочому місці створюється: комп'ютером та периферійним пристроєм. Допустимі рівні звукового тиску на робочому місці повинні відповідати вимогам [36]:

Таблиця 4.2

Санітарні норми виробничого шуму, ультразвуку та інфразвуку

Вид трудової діяльності, робоче місце	Рівні шуму та еквівалентні рівні шуму, ДБА, дБАекв
Конструювання та проектування.	50

Реальний рівень шуму в проектному відділі становить 54 дБ, що перевищує допустимий рівень.

Для зменшення рівня шуму рекомендується використовувати місцеву та загальну звукоізоляцію, шумопоглинаючі екрани, поглинаючі фільтри.

4.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів

Нормалізація повітря робочої зони. Для створення й автоматичної підтримки в ІТ відділі незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря [37].

Виробниче освітлення. Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення шляхом встановлення 5 додаткових світильників, щоб загальна кількість лам відповідала розрахованому вище значенню, а саме 36 світлодіодних ламп. Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік [38].

Електробезпека. Електробезпечність у приміщенні ІТ відділу пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЭ) для електроустановок з напругою до 1000 В. А також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки [39].

Ергономіка та організація робочого місця. Після проведення аналізу робочого місця програміста в ІТ Відділі було з'ясовано, що воно відповідає встановленим вимогам.

Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви сумарний час яких повинен складати 50 хвилин при 8-ми годинному робочому дні [40].

4.2.1. Розрахунок повітрообміну за надлишком тепла у проектному відділі

Приміщення має розміри 4×8×4, яке розміщується на другому поверсі п'ятиповерхового будинку з південного боку. Площа вікон F = 2,88 м^2. На вікнах розміщенні жалюзі. У приміщенні 5 інженерів-проектувальників, розташовано $N_{пк} = 5$ персональних комп'ютерів та принтер. Для штучного освітлення використовується 4 офісних світлодіодних світильника потужністю 125 Вт.

1. Розраховуємо загальну кількість тепла:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад,} \text{ Вт} \quad (4.1)$$

$Q_{над}$ – загальна кількість тепла

$Q_{осв}$ - кількість тепла від джерел штучного освітлення

$Q_{облад}$ - кількість тепла від обладнання

$Q_{ін\text{-}пр.}$ - кількість тепла від інженерів-проектувальників

$Q_{рад,}$ - кількість тепла від сонячної радіації

2. Розраховуємо кількість тепла від джерел штучного освітлення:

$$Q_{осв} = N \cdot \eta, \quad (4.2)$$

де N - сумарна потужність джерел освітлення, Вт; η - коефіцієнт теплових витрат (η = 0,55 – для світлодіодних ламп).

$$Q_{осв.} = 125 \cdot 4 \cdot 0,55 = 275 \text{ Вт}$$

2. Розраховуємо кількість тепла при роботі обладнання: 5 комп'ютерів і принтера (в режимі друку):

$$Q_{облад} = n \cdot P_{комп.} + P_{пр.}, \quad (4.3)$$

де n – кількість комп'ютерів (обладнання);

$P_{комп}$ – встановлена потужність комп'ютерів, $P_{комп} = 400$ Вт

$P_{пр.}$ – потужність принтера в режимі друку, $P_{пр} = 465$ Вт

$$Q_{облад} = 5 \cdot 400 + 465 = 2.5 \text{ кВт}$$

3. Розраховуємо кількість тепла від інженерів-проектувальників:

$$Q_{ін\text{-}пр.} = n \cdot q \text{ , Вт} \quad (4.4)$$

n – кількість інженерів-проектувальників

q – кількість тепла, що виділяється одним інженером-проектувальником

Кількість тепла, що виділяється одним інженером-проектувальником, який виконує легку фізичну роботу дорівнює 99 Вт.

$$Q_{ін\text{-}пр} = 5 \cdot 99 = 495 \text{ Вт}$$

4. Розраховуємо кількість тепла від сонячної радіації:

$$Q_{рад} = m \cdot S \cdot k \cdot q_{скл} \quad (4.5)$$

де m – число вікон; $S_{вікна}$ – площа одного вікна, $S_{вікна}$ =2,88 $м^2$;

k – коефіцієнт, віконного переплетення: k = 0,6 матові;

$q_{скл.}$ – надходження тепла через 1 $м^2$ вікна при різній орієнтації вікон: $q_{скл.}$ = *150* – південь;

$$Q_{рад} = 1 \cdot 2{,}88 \cdot 0{,}6 \cdot 150 = 259{,}2 \text{ Вт}$$

5. Загальна кількість тепла в проектному відділі:

$$Q_{над} = Q_{осв} + Q_{облад} + Q_{ін\text{-}пр.} + Q_{рад} = 275 + 2500 + 495 + 259{,}2 = 3{,}529 \text{ кВт}$$

6. Потрібний повітрообмін за надлишком тепла:

$$L = \frac{Q}{c \cdot \rho \cdot (t_{вид} - t_{зовн})} \text{ , м}^3/\text{год} \quad (4.6)$$

Q - кількість тепла, яке виділяється в приміщення за годину, Дж:

$$Q = 3600 \cdot Q_{надл} = 3600 \cdot 3529 = 12704 \text{ Вт} = 5328 \text{ кДж};$$

c – теплоємність повітря, Дж/кг (в інтервалі температур від 0ºС до 100ºС приймається рівною $1{,}01 \cdot 10^3$Дж/кг);

ρ – густина повітря, кг/м^3(дорівнює $\rho_{внт}$=1,2 кг/м^3);

$t_{вид}$– температура повітря, що видаляється, $t_{вид}$=*30*℃

$t_{зовн.}$- температура повітря, що подається до робочої зони, $t_{зовн.}$=23℃

$$L = \frac{5328}{1{,}01 \cdot 10^3 \cdot 1{,}2 \cdot (30 - 23)} = 628 \text{ м}^3/\text{год}$$

Оскільки, в проектному відділі підвищена температура повітря на 2 ℃ від допустимого значення 28℃, встановили механічну вентиляцію з вентилятором

VORTICE VARIO , яка забезпечила надходження до приміщення температури повітря 23 ℃, дане значення є оптимальним.

4.3. Пожежна безпека

Відповідно до [39-40] дане приміщення відноситься до категорії В по вибухово-пожежній та пожежній небезпеці із-за використання у ньому твердих горючих матеріалів з температурою спалаху понад 61℃.

Проектний відділ оснащено:

- Двома безпровідними датчиками детектування диму SD-02 (оповіщає при задимленні приміщення; площа обслуговування: до 20 м^2);
- двома порошковими вогнегасниками ВП-5 (для приміщення категорії В за відсутності горючих газів і рідин, площею до 50 м^2 і масою вогнегасної речовини – 5 кг, мінімальна кількість порошкових вогнегасників 2).
- LifeSOS LS-30LR бездротова пожежно-охоронна система (при детектуванні вторгнення, датчики передають на центральний блок сигнал тривоги по радіоканалу без проводів. Централь приймає сигнал від датчиків, включає сирену, відправляє інформацію на пульт централізованого нагляду, дзвонить на зазначені телефонні номери та відправляє SMS повідомлення з повідомленнями про тривогу.)

Для попередження виникнення пожеж проводяться організаційно-технічні заходи пожежної безпеки, які включають:

- включення питань пожежної безпеки у всі інструкції по техніці безпеки;
- виконання встановленого режиму експлуатації електричних мереж та обладнання;
- заборона куріння в недозволеному місці;
- видання необхідних інструктажів, планів евакуації

План евакуації складається з графічної і текстової частин. Графічна частина являє собою схематичний план поверху (рис. 5.1), в якому зеленими суцільними стрілками вказують шляхи евакуації, що ведуть до основних евакуаційних виходів, а пун-

ктирними зеленими стрілками - до аварійних виходів. Двері на шляху евакуації відчиняються назовні у напрямку виходу з будівлі. На плані евакуації умовними знаками показано розміщення вогнегасників, пожежних гідрантів, телефонів, аптечок медичної допомоги, електрощитів, датчиків диму, системи охоронно-пожежної сигналізації.

Умовні позначення											
	- телефон		- пожежний гідрант		- аптечка	ЗАПАСНЫЙ ВЫХОД	- евакуаційний вихід		напрямок руху до виходу		- датчики диму
									місце інженера-проектувальника		
	- Вогнегасник		- електрощитова		місце для куріння	ЗАПАСНЫЙ ВЫХОД	- запасний вихід		- шлях до евакуаційного виходу		охоронно-пожежна система
									шлях до запасного виходу		

Рис 5.1. План евакуації 2 поверх

4.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Вимоги безпеки перед початком роботи.

- Перед початком роботи працівник повинен зовнішнім оглядом перевірити цілісність корпусів системного блоку, відео монітора, принтера, клавіатури.
- Перевірити цілісність кабелів живлення, місць їх підключення (розеток електромережі, продовжувачів електромережі, розгалужувальних коробок, штепсельних вилок).
- Підготувати своє робоче місце, прибравши речі, які можуть заважати при виконанні роботи.
- Ввімкнути живлення ПК.
- У випадку, якщо після ввімкнення ПК не проходить загрузка або комп'ютер не виходить на робочий режим, працівник повинен повідомити керівника чи спеціаліста відділу інформаційних технологій.
- При виявленні ушкодження або яких-небудь інших недоліків повідомити безпосереднього керівника. Не приступати до роботи без його вказівки.

Вимоги безпеки під час роботи

- Необхідно стійко розташувати всі складові пристрої на столі, в тому числі і клавіатуру. Разом з тим повинна бути передбачена можливість переміщення клавіатури. ЇЇ розташування і кут нахилу повинні відповідати побажанням користувача ПК. Якщо в конструкції клавіатури не передбачений простір для опору долонь, то її слід розташовувати на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля. При роботі на клавіатурі слід сидіти прямо, не напружуватись.
- Для зменшення несприятливого впливу на користувача пристроїв типу "миша" (вимушена поза, необхідність постійного контролю за якістю дій) слід забезпечити вільною більшу площу поверхні столу для переміщення "миші" і зручного упору ліктьового суглоба.
- Не припустимі сторонні розмови, роздратовуючи шуми тощо.

- Періодично при вимкнутому ПК слід видаляти злегка зволоженою мильним розчином хлопко-паперовою салфеткою пил з поверхонь апаратури. Екран і захисний екран протирають ватою, зволоженою спиртом.
- Не дозволяється використовувати рідинні або аерозольні засоби чистки поверхонь ПК.

Забороняється:

- самостійно ремонтувати апаратуру, в яких кінескоп та інші елементи можуть знаходитись під високою напругою (до 25 кВ0.)
- класти будь-які речі на апаратуру ПК, бутерброди та напої на клавіатуру або поруч з нею. Це може вивести її з ладу;
- затуляти вентиляційні отвори в апаратурі, це може призвести до її перегріву і виходу з ладу.

- Для зменшення негативного впливу на стан здоров'я працівників різних факторів ризику, пов'язаних з роботою на ПК, передбачаються додаткові регламентовані перерви для відпочинку користувачів ПК:

- через кожний час безперервної роботи – 10 хвилин;
- через кожні 2 години – 15 хвилин.

- При можливості слід чергувати зміну діяльності з іншою, не пов'язаною з роботою на ПК.
- З метою зменшення негативного впливу монотонності доцільно застосовувати чергування операцій введення тексту і введення даних (зміна змісту і темпу роботи) і т.п.
- При роботі на лазерних принтерах:
- Розташовувати принтер необхідно поряд з системним блоком так, щоб з'єднувальні шнури не були натягнуті. Забороняється ставити принтер на системний блок.
- Перш, ніж програмувати роботу принтера, впевніться, що він знаходиться в режимі зв'язку з системним блоком.
- Для досягнення високоякісного, чистого, з високою роздільною здатністю зображення щоб не зіпсувати апарат, потрібно використовувати папір, марка якого вказана в інструкції до принтера (найчастіше папір вагою 60-135 г/м^2, типу Canon або Xerox 4024).

- Обрізання країв паперу повинно бути виконаним гострим лезом ножа, без зазусенців – це зменшить вірогідність загинання паперу.
- При виконанні роботи (більше 20 хвилин), коли втручання користувача в роботу програми не потрібне, бажано вимикати живлення відео монітора.
- Для підтримки загального тонусу м'язів, профілактики кістково-м'язових порушень, зорового дискомфорту та інших несприятливих суб'єктивних почуттів під час регламентованих перерв необхідно виконувати комплекси рекомендованих вправ для очей, для хребта, для рук.
- Кількість мікро пауз до 1-2 хвилин слід визначити індивідуально. Форма та зміст перерв можуть бути різними виконання допоміжних робіт, не пов'язаних з роботою ПК , приймання їжі, виконання рекомендованих вправ.
- Виконання фізичних вправ протягом дня рекомендується індивідуально, залежно від почуття втоми. Гімнастика повинна біти на корекцію вимушеної пози покращення кровообігу, часткову компенсацію, дефіциту рухової активності.
- Про виявлені несправності (іскріння, пробоїв, запаху гару, ознак горіння тощо) негайно припинити роботу, відключити все обладнання від електромережі і терміново повідомити безпосереднього керівника або спеціаліста по ремонту ПК.

Вимоги безпеки при закінчення роботи на ПК.

- Закінчити і зберегти в пам'яті ПК файли, які знаходились у роботі. Виконати всі дії для коректного завершення роботи в оперативній системі.
- Вимкнути принтер та інші периферійні пристрої, вимкнути системний блок. При наявності пристрою безперебійного живлення (ПБЖ) вимкнути його живлення.
- Вимкнути ПК кнопкою «POWER" (ЖИВЛЕННЯ) та вийняти штепсельну вилку кабелю живлення з розетки
- Накрити клавіатуру кришкою для попередження попадання в неї пилу.
- Навести порядок на робочому місці.

Вимоги безпеки в аварійних ситуаціях.

- Якщо після ввімкнення ПК відчувається запах горілого або при доторканні до металевих частин ПК відчувається дія електричного струму, потрібно негайно відключити ПК від електромережі та повідомити про це своєму керівникові.
- У випадку виникнення пожежі негайно розпочати гасіння наявними засобами пожежогасіння і повідомити за телефоном 101 (міська пожежна охорона) та начальнику ДПД підприємства. Пам`ятайте, що загашувати електроустановки слід вуглекислотними вогнегасниками, сухим піском, щоб уникнути ураження електричним струмом.

У разі виникнення інших аварійних ситуацій слід припинити роботу і повідомити про це керівника робіт.

ВИСНОВОК ДО РОЗДІЛУ 4

На підставі виконаного розрахунку повітрообміну за надлишком тепла, значення якого 628 $м^3$/год, встановили механічну вентиляцію з вентилятором VORTICE VARIO, оскільки використання природної вентиляції є малоефективним. Механічна вентиляція здатна забезпечити виведення з проектного відділу температури 30℃ і підтримувати температуру повітря допустимого та навіть оптимального значення.

РОЗДІЛ 5
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

На сьогоднішній день радіотехнічне та електронне виробництво є досить розвинутим і без нього суспільство не уявляє свого життя. Електронна і радіотехнічна промисловість грає провідну роль в науково-технічній революції. Впровадження електронних приладів в різні сфери людської діяльності значною мірою сприяє успішній розробці складних науково-технічних проблем, підвищенню продуктивності фізичної і розумової праці, поліпшенню економічних показників виробництва.

В кваліфікаційній роботі розроблена система захисту з використанням серверного обладнання, що може здійснювати негативний вплив на навколишнє середовище.

5.1. Аналіз впливу техногенних чинників

Широке використання електричного та електронного обладнання дозволило не тільки підвищити якість життя людей, але й призвело до негативних наслідків для навколишнього середовища та здоров’я людини. Можна виділити основні шкідливі та небезпечні чинники, які впливають на навколишнє середовище [42]:

- шумове забруднення;
- вібраційне забруднення;
- електромагнітне забруднення
- теплове забруднення
- радіаційне забруднення

Шумове забруднення. У сучасному світі в умовах науково-технічного прогресу шум став однією з форм фізичного (хвильового) забруднення природного середовища. Шумом прийнято вважати усі неприємні та небажані звуки або їх сукупність, які заважають нормально працювати, сприймати потрібну звукову інформацію та відпочивати.

Адаптація до нього практично неможлива. Фоновий рівень шуму навколишнього середовища становить 30-60 децибел. До цього природного фону за сучасних умов додаються виробничі й транспортні шуми, рівень яких нерідко перевищує 100 децибел. Джерелами шуму є: промислові об'єкти, транспорт, гучномовні пристрої, телевізори, радіоприймачі, музичні інструменти, юрби людей тощо. Шум у виробничих умовах негативно впливає на працівника: послаблює увагу, посилює розвиток втоми, сповільнює реакцію на небезпеку. Внаслідок цього знижується працездатність та підвищується ймовірність нещасних випадків. Допустимі рівні звукового тиску в октавних смугах частот на робочих місцях у виробничих приміщеннях наведені в таблиці 5.1 [42]:

Таблиця 5.1

Допустимі рівні звукового тиску в октавних смугах частот

Рівні звукового тиску в дБ, в октавних смугах частот, Гц								
31,5	63	125	250	500	1000	2000	4000	8000
107	95	87	82	78	75	73	71	69

Встановлено, що рослини під впливом шуму знижують енергію до зростання, у них спостерігається надмірне (навіть повне, що призводить до загибелі) виділення вологи через листя, можливі порушення у клітинах. Гинуть листя і квіти рослин, які розташовані близько до джерела інтенсивного шуму (звуку). Відсутність шуму особливо необхідний для тварин, які обмінюються звуковою інформацією, а також аналізуючи звуки навколишнього середовища з метою покращання отримання інформації, в тому числі сигналів тривоги. Аналогічно діє шум на тварин. Від шуму реактивного літака гинуть личинки бджіл, самі

вони втрачають здатність орієнтуватися, у пташиних гніздах дає тріщини шкаралупа яєць. Від коливань повітря, які утворюються звуками переносної радіоапаратури, не можуть піднятися у повітря жуки, джмелі та інші комахи.

Вібраційне забруднення. Вібрація – це механічні коливання твердого тіла. Вібрацію поділяють на природну та штучну. Джерелами природної вібрації є землетруси,

що викликаються природними чинниками. Джерелами штучної вібрації є промисловість, транспорт. Тривалі вібрації завдають великої шкоди здоров'ю людини – від сильної втоми до змін багатьох функцій організму: порушення серцевої діяльності, нервової системи, спазмів судин, деформації м'язів, струсу головного мозку тощо. Особливо небезпечна вібрація з частотою, яка є резонансною з частотою коливання окремих органів чи частин тіла людини, що може призвести до їх пошкодження. Тривала дія вібрації може спричинити професійне захворювання – вібраційну хворобу [42].

Електромагнітне забруднення. У процесі еволюції біосфера постійно знаходилася і знаходиться під впливом електромагнітного поля (ЕМП) природного походження (природний фон): електричного й магнітного поля Землі, космічного електромагнітного випромінювання, насамперед того, що генерується Сонцем. У період науково-технічного прогресу людство створювало і дедалі ширше використовувало штучні (антропогенні) джерела ЕМП. У наш час ЕМП антропогенного походження значно перевищують природний фон і є тим несприятливим чинником, вплив якого на людину та довкілля рік за роком зростає. Ступінь впливу ЕМП на організм людини залежить від діапазону частот, інтенсивності та тривалості дії, характеру випромінювання (неперервного чи модульованого), режиму опромінювання, розміру поверхні тіла, що зазнає опромінювання, індивідуальних особливостей організму. Електромагнітні поля можуть викликати біологічні та функціональні порушення у функціонуванні організму. Функціональні ефекти проявляються у передчасній втомлюваності, частих болях голови, погіршенні сну, порушенні функцій серцево-судинної та центральної нервової систем. Тривалий та інтенсивний вплив ЕМП призводить до стійких порушень та захворювань. Біологічні негативні ефекти впливу ЕМП проявляються у тепловій та нетепловій діях. Теплова дія призводить до підвищення температури тіла та місцевого вибіркового нагрівання органів і тканин організму внаслідок переходу електромагнітної енергії в теплову. Таке нагрівання особливо небезпечне для органів із слабкою терморегуляцією (головний мозок, очі, нирки, шлунок тощо). Наприклад, випромінювання сантиметрового діапазону призводить до появи катаракти, тобто до поступової втрати зору [42].

Теплове забруднення. Теплове забруднення – це результат розсіювання в навколишнє середовище теплоти, яка виділяється у багаточисельних теплових процесах, насамперед пов’язаних зі згоранням палива. Під час згорання палива щорічно витрачається до 23% кисню, що утворюється в процесі фотосинтезу на Землі за рік. За підрахунками під час спалювання вугілля в навколишнє середовище викидається радіоактивних компонентів більше, ніж за той самий час на всіх атомних електростанціях у разі безаварійної роботи. Теплове забруднення гідросфери відбувається переважно внаслідок скидання у водойми підігрітих вод від ТЕС, АЕС та інших енергетичних об’єктів. Тепла вода змінює термічні та біологічні режими водойм і шкідливо впливає на їхніх мешканців [42].

5.2. Вплив приймальних пристроїв на навколишнє середовище

Абонентський приймач – телевізійний приймач (приставка), пристрій, що приймає сигнал цифрового телебачення, декодує його і перетворює в аналоговий сигнал для виведення через роз'єми RCA або SCART або перетворює в цифровий сигнал для виведення через роз'єм HDMI , і передає його далі на телевізор.

Перехід до цифрового телебачення призвів до зростання виробництва цифрових абонентських приймачів, що в свою чергу може негативно впливати на навколишнє середовище. Приймач продукує слабкі електричні і магнітні змінні поля в широкому діапазоні частот. Проте проблема впливу електромагнітних випромінювань, що продукуються заслуговує на особливу увагу. Наукові дослідження показали, що ЕМВ мають у своєму складі чинник, котрий впливає на користувачів при наявності сучасних екранів від ЕМВ. Вчені України ідентифікували цей чинник як торсіонові поля, котрі супроводжують будь-яке електромагнітне випромінювання та являються його інформаційною компонентою [45]. Робоча група Всесвітньої організації охорони здоров’я з гігієнічних аспектів користування моніторами та радіо терміналами виявили порушення стану здоров’я при користуванні пристроями, які мають електромагнітне випромінювання, найсерйозніші з яких:

- погіршення зору;

- порушення імунної системи;
- порушення психоемоційної сфери (стресовий синдром, агресивність)

Для забезпечення безпеки здоров'я користувачів в Україні діють Державні санітарні норми і правила при роботі з джерелами електромагнітних полів «ДСанПіН 3.3.6.096-2002». Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових залежно від тривалості їх дії наведені в таблиці 5.2.

Таблиця 5.2

Значення ГДР напруженості електричної ($E_{гд}$) і магнітної ($H_{гд}$) складових

Час перебування персоналу, год	$E_{гд}$, В/м					$H_{гд}$, А/м			
	1-10 кГц	10-60 кГц	0,063 МГц	3-30 МГц	30-300 МГц	1-10 кГц	10-60 кГц	0,06-3 МГц	30-50 МГц
8	120	70	50	30	10	9	7	5	0,3
7	130	75	53	32	11	9,8	7,5	5,3	0,32
6	140	82	58	34	12	10,6	8,1	5,8	0,34
5	155	90	63	37	13	11,6	8,8	6,3	0,38
4	175	110	71	42	14	13	9,9	7,1	0,42
3	200	115	82	48	16	15	11,4	8,2	0,49
2	250	140	100	59	20	18,4	14	10	0,6
1	350	200	141	84	28	26	19,7	14,2	0,85
0,5	500	280	200	118	40	37,6	27,9	20	1,2

У результаті дії на організм людини електромагнітних випромінювань в діапазоні 30 кГц - 300 МГц (НЧ) спостерігається: загальна слабкість, підвищена втома, сонливість, порушення сну, головний біль та біль в ділянці серця. З'являється роздратованість, втрачається увага, сповільнюються рухово-мовні реакції. Виникає ряд симптомів, які свідчать про порушення роботи окремих органів - шлунку, печінки, підшлункової залози.

Для того, щоб зменшити рівень електромагнітного випромінювання потрібно обмежити безперервний час роботи абонентського приймача [43-46].

В Україні норми електромагнітної безпеки регламентуються Державними санітарними нормами і правилами захисту населення від впливу електромагнітного випромінювання, згідно з якими допустимі рівні інтенсивності електромагнітного випромінювання для цивільного населення становлять 2,5 мкВт/см^2.

Абонентський приймач під час роботи створює шум, рівень якого становить 54 дБ. Допустимий рівень звукового тиску повинний відповідати «ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку», а саме 50 дБ.

Велика кількість звукових сигналів, що поступають до кори головного мозку, викликають переживання, страх, передчасну втому. Дія шуму на людину виражається в широкому діапазоні - від суб'єктивного роздратування до об'єктивних змін в ЦНС, органах слуху, серцево-судинних та ендокринній системах, травному акті та інших органів і систем. Першим показником шкідливої дії шуму є скарги на роздратованість, переживання, порушення сну [45].

5.3. Засоби для захисту від електромагнітного випромінювання та шуму, проблема електронних відходів

Захист від електромагнітного випромінювання. Для зменшення впливу ЕМП на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів, потрібно вжити ряд захисних заходів. До їх числа можуть входити організаційні, інженерно-технічні та лікарсько-профілактичні.

До заходів щодо зменшення впливу на працівників ЕМП належать: організаційні, інженерно-технічні та лікарсько-профілактичні.

Організаційні заходи здійснюють органи санітарного нагляду. Вони проводять санітарний нагляд за об'єктами, в яких використовуються джерела електромагнітних випромінювань.

Інженерно-технічні заходи передбачають таке розташування джерел ЕМП, яке б зводило до мінімуму їх вплив на працюючих, використання в умовах виробництва

дистанційного керування апаратурою, що є джерелом випромінювання, екранування джерел випромінювання, застосування засобів індивідуального захисту (халатів, комбінезонів із металізованої тканини, з виводом на заземлюючий пристрій). Для захисту очей доцільно використовувати захисні окуляри ЗП5-90. Скло окулярів вкрито напівпровідниковим оловом, що послаблює інтенсивність електромагнітної енергії при світлопропусканні не нижче 75%.

Взагалі, засоби індивідуального захисту необхідно використовувати лише тоді, коли інші захисні засоби неможливі чи недостатньо ефективні: при проходженні через зони опромінення підвищеної інтенсивності, при ремонтних і налагоджувальних роботах в аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання трудових операцій, погіршують гігієнічні умови.

У радіочастотному діапазоні засоби індивідуального захисту працюють за принципом екранування людини з використанням відбиття і поглинання ЕМП. Для захисту тіла використовується одяг з металізованих тканин і рідіопоглинаючих матеріалів. Металізовану тканину роблять із бавовняних ниток з розміщеним всередині них тонким проводом, або з бавовняних чи капронових ниток, спірально обвитих металевим дротом. Така тканина, наче металева сітка, при відстані між нитками до 0,5 мм значно послаблює дію випромінювання. При зшиванні деталей захисного одягу треба забезпечити контакт ізольованих проводів. Тому електрогерметизацію швів здійснюють електропровідними масами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок безконтактних проводів.

Лікарсько-профілактичні заходи передбачають проведення систематичних медичних оглядів працівників, які перебувають у зоні дії ЕМП, обмеження в часі перебування людей в зоні підвищеної інтенсивності електромагнітних випромінювань, видачу працюючим безкоштовного лікарсько-профілактичного харчування, перерви санітарно-оздоровчого характеру.

Захист від шуму. Для зменшення і ліквідації шуму застосовується цілий комплекс заходів, що називається шумозахистом. Це застосування звукопоглинаючих ма-

теріалів, раціональне розміщення будівельних об'єктів, створення вздовж вулиць екранів у вигляді земляних валів, стін різних конструкцій, шумовідбиваючих, як правило не житлових будівель - магазинів, складів, гаражів.

Проблема електронних відходів. Згідно Закону України «Про відходи» з метою запобігання або зменшення обсягів утворення відходів потрібно здійснювати системи збирання та утилізації електричного та електронного обладнання [30]. Вирішення проблеми електронних відходів в Україні мав би забезпечити «Технічний регламент з поводження з відходами електричного та електронного обладнання», розробка якого в Україні здійснюється з 2008 року. Згідно з проектами цих законодавчих актів імпортери і виробники можуть як самостійно утилізувати електровідходи, так і підписувати договори на виконання робіт з організації збирання, заготівлі та утилізації відповідних видів техніки з уповноваженими підприємствами. Розроблено також проект Постанови Кабінету Міністрів України «Про затвердження Технічного регламенту з поводження з відходами електронного та електричного устаткування». Цим регламентом передбачається створення пунктів збору відходів електронного та електричного обладнання, які повинні розташовуватися у місцях, зручних для користувачів, та забезпечувати безоплатність послуг, що надаються цими пунктами для користувачів. Наразі обговорюється ще один варіант вирішення проблеми, а саме проект внесення змін до Податкового Кодексу, в якому передбачає централізоване стягнення коштів з імпортерів та виробників різних споживчих товарів з метою забезпечення за рахунок цих коштів належної організації збирання, заготівлі та утилізації відходів від зазначених товарів.

Однак, загалом проблему електронних відходів в Україні необхідно вирішити як в організаційно-правовому аспекті – створення фондів виробників, підтримка держави підприємств з утилізації відходів, так і в соціально-інформаційному: українців треба переконати в тому, що виносити на звичайний смітник поламаний електронний пристрій – не можна.

ВИСНОВОК ДО РОЗДІЛУ 5

Телекомунікаційні ресурси створюють негативний вплив на навколишнє середовище. Вони є джерелами електромагнітного випромінювання та шумового забруднення. Для мінімізації ризику виникнення захворювань, ефективними є інженерно-технічні заходи, які зменшать дію шкідливих чинників. Також були розглянута проблема електронних відходів, одним зі шляхом вирішення якої є створення пунктів збору відходів електронного та електричного обладнання.

ВИСНОВКИ

У кваліфікаційній роботі виконані дослідження, які використані при розробці ефективних ЗАОР ІБ за запропонованою методологією синтезу, заснованою на створених у роботі методах та складеною моделлю КМР ризику. У ході вирішення поставлених завдань було отримано такі результати:

1) На підставі проведеного аналізу ЗАОР та його базових понять, розроблена кортежна модель базових характеристик ризику, яка за рахунок узагальнення базових характеристик, відображених шестикомпонентним кортежем, дозволяє формувати необхідні множини даних для забезпечення гнучкості та необхідної функціональності ЗАОР, що розробляються.

2) Запропоновано методи аналізу та оцінювання ризиків ІБ, які на основі використання узагальненої моделі КМР та логіко-лінгвістичного підходу, дозволяють створювати відповідні засоби оцінювання з інтегрованими можливостями, що використовують як вхідні дані динамічно змінювані набори детермінованих та нечітко визначених базових характеристик з урахуванням періоду часу, галузі, економічної та управлінської специфіки об'єкта захисту та ін.

3) Розроблено методи реалізації функції n-кратного інкрементування числа термів з використанням першого та другого приватного розширення бази, в якому за рахунок модифікації n-кратного розширення функції інкрементування термів на один порядок, розширюється можливість формалізації процесу еквівалентного трансформування числа еталонних термів ЛП на n порядків без залучення експертів відповідної предметної галузі.

4) Набула подальшого розвитку методологія синтезу ЗАОР, яка дозволила, за рахунок формалізації та узагальнення процесу використання сформованої моделі характеристик та запропонованих методів, детермінувати процес побудови інструментальних засобів з гнучкими можливостями використання заданих множин величин при аналізі та оцінювання ризиків ІБ.

5) Розроблено структури систем ЗАОР, які за рахунок підсистем обробки базових характеристик та формування даних, що реалізують запропоновані FirstM методи, дозволяють перетворити та формувати дані, як і якісної, і у кількісної інтерпретації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Dmitry S. Vorunichev, Mihail S. Kostin and Sergey N. Zamuruev, "Classification of Methods of Reverse Engineering inthe Configuration Management of OriginalHigh-Tech Radio Electronic Products", 2018 IEEE International Conference “Quality Management Transport and Information Security Information Technologies” (IT &QM&IS), 24–28 Sept. 2018.
2. Jia-Hui HUANG, Dong-Qin FENG and Hong-Jian WANG, "A Method for Quantifying Vulnerability of Industrial Control System Based on Attack Graph[J]", ACTA AUTOMATICA SINICA, vol. 42, no. 5, pp. 792-798, 2017.
3. Chi-qian JIA and Dong-qin FENG, "Security assessment for industrial control systems based on fuzzy analytic hierarchy process[J]", Journal of Zhejiang University(Engineering Science), vol. 50, no. 4, pp. 759-765, 2016.
4. YL Zheng and S Zheng, "Cyber Security Risk Assessment for Industrial Automation Platform[C]", 2017 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 341-344.
5. Y Chen, J Hong and CC Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations[J]", IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 2541-2552, 2018.
6. F Zhang and B Chen, "Risk Assessment for Substation Operation Based on Triangular Fuzzy Number AHP and Cloud Model[C]", 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), pp. 1-5, 2018.
7. A. F. Apriliana, R. Sarno and Y. A. Effendi, "Risk analysis of IT applications using FMEA and AHP SAW method with COBIT 5", 2018 International Conference on Information and Communications Technology ICOIACT 2018, 2018.
8. Balqis Lembah Mahersmi et al., "Analisis Risiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE Dan Kontrol ISO 27001 Pada Dishubkominfo Kabupaten Tulungagung", Seminar Nasional Sistem Informasi Indonesia, 2019.

9. A. Cahyapratama and R. Sarno, "Application of Analytic Hierarchy Process (AHP) and Simple Additive Weighting (SAW) methods in singer selection process", 2018 International Conference on Information and Communications Technology ICOIACT 2018, 2018.

10. ISO, 27001/ISO 27002, "4th edition IT GOVERNANCE A Manager's Guide to Data Security", Alan Calder and Steve Watkins, 2008.

11. R. A. Caralli et al., Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Carnegie Mellon University, 2017.

12. M. T. Jufri, M. Hendayun and T. Suharto, "Risk-assessment based academic information System security policy using OCTAVE Allegro and ISO 27002", Proceedings of the 2nd International Conference on Informatics and Computing ICIC 2019, 2019.

13. Khairul et al., "Decision Support System in Selecting The Appropriate Laptop Using Simple Additive Weighting", IJRTER, 2019.

14. J. Kittur, "Optimal generation evaluation using SAW WP AHP and PROMETHEE multi - Criteria decision making techniques", Proceedings of IEEE International Conference on Technological Advancements in Power and Energy TAP Energy 2021, 2021.

15. Lisa Yeo et al., "Risk Mitigation Decisions for IT Security", TMIS, 2020.

16. M. Masky, S. S. Young and T. Y. Choe, "A novel risk identification framework for cloud computing security", 2019 IEEE 2nd International Conference on InformationScience and Security ICISS 2019, 2019.

17. R. dan Levy Mattioli, Cedric. Methodologies for the identification of Critical Information Infrastructure assets and services, ENISA, 2021.

18. Mona Jaberidoost, "Pharmaceutical Supply Chain Risk Assessment in Iran Using Analytic Hierarchy Process (AHP) and Simple Additive Weighting (SAW) methods", Journal of Pharmaceutical Policy and Practice, 2021.

19. Nadher et al., "A Multiple Attribute Decision Making for Improving Information Security Control Assessment", International Journal of Computer Applications (0975-8887), vol. 89, no. 3, 2020.

20. Matondang Nurhafifah, I. I. Nurlaili and M. Anita, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)", Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi), 2018.

21. P. Pangaribuan and A. Beniyanto, "SAW TOPSIS PROMETHEE Method as a Comparison Method in Measuring Procurement of Goods and Services using Procurement of Goods and Auction Services", IOP Conference Series: Materials Science and Engineering, pp. 1-6, 2018.

22. Rosini et al., "Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode OCTAVE Allegro", Jurnal Pustakawan Indonesia, vol. 14, no. 1, 2021.

23. W. Sardjono and M. I. Cholik, "Information Systems Risk Analysis Using OCTAVE Allegro Method Based at Deutsche Bank", Jayapura 2018 International Conference on Information Management and Technology (ICIMTech), 2018.

24. J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with OCTAVE Allegro at Education Institution", Procedia Computer Science, 2018.

25. A. Suryana, E. Yulianto and K. D. Pratama, "Perancangan Sistem Pendukung Keputusan Penilaian Prestasi Pegawai Menggunakan Metode SAW AHP DAN TOPSIS", Jurnal Ilmiah Teknologi Informasi Terapan, 2017.

26. M. Talabis and J. Martin, "Information Security Risk Assessment: A Practical Approach", Information Security Risk Assessments, 2021.

27. F. Tscheikner-Gratl et al., "Comparison of multi-criteria decision support methods for integrated rehabilitation prioritization", Water (Switzerland), 2017.

28. Wayne S. Goodridge, "Sensitivity Analysis Using Simple Additive Weighting Method", I.J. Intelligent Systems and Applications, 2020.

29. Evan Wheeler, Security Risk Management Building an Information Security Risk Management Program from the Ground Up, USA:Syngress, 2021.

30. M. M. D. Widianta et al., "Comparison of Multi-Criteria Decision Support Methods (AHP TOPSIS SAW & PROMENTHEE) for Employee Placement", Journal of Physics: Conference Series, 2018.

31. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин.

32. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

33. Державні санітарні норми та правила «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу».

34. «ДСН 3.3.6.042-99 Санітарних норми мікроклімату виробничих приміщень».

35. ДБН 13.2.5-28-2006 «Природне і штучне освітлення».

36. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

37. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

38. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».

39. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».

40. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

41. НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

42. Прогнозування екологічних ризиків з використанням аналізу ієрархів та теорії нечітких множин: міжнародна науково-практична конференція «І-й всеукраїнський з'їзд екологів»: Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. – 2016. – С.25.

43. Клап Я. А., Яремкевич О. С., Червецова В. Г., Заярнюк Н. Л., Новіков В. П., Дослідження впливу електромагнітних, постійних магнітних та акустичних полів на організм людини // Вісник Нац. ун-ту "Львівська політехніка". – 2016 – № 812. – С. 365–372.

44. Сучасний стан досліджень впливу електромагнітних випромінювань на організм людини [Електронний ресурс]/[А. П. Чорний, В. В. Никифоров, Д. І. Родькін, В. Ю. Ноженко] // Інженерні та освітні технології в електротехнічних та комп'ютерних системах: щоквартальний науково-практичний журнал. – Кременчук: КрНУ, 2013.

45. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с.

46. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с.