МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

Кафедра комп'ютерних технологій та інформаційної безпеки

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних технологій та інформаційної безпеки, к.т.н., доцент
_____ С.М. Нужний
«10» 12 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА

ПОБУДОВА ТА ДОСЛІДЖЕННЯ РЕЛЯЦІЙНОЇ МОДЕЛІ ВЗАЄМОВПЛИВУ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ЗАХИЩЕНІСТЬ ОБ'ЄКТУ ВОДНОГО ТРАНСПОРТУ

Ступінь вищої освіти: магістр
Галузь знань: 14 Електрична інженерія
Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»
Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки

Виконав: студент 6 курсу групи 6366м

Бондаренко Іван Юрійович _____

Керівник:
д.т.н., професор, професор кафедри комп'ютерних технологій та інформаційної безпеки

Передерій Віктор Іванович _____

Миколаїв – 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки

ЗАТВЕРДЖУЮ
Гарант освітньої програми,
д.т.н., професор,
професор кафедри КТІБ
_____ Передерій В.І.
«14» 10 2025 р.

ЗАВДАННЯ

на кваліфікаційну роботу

Студент: Бондаренко Іван Юрійович

Курс:6

Група: 6366м

Ступінь вищої освіти: магістр

Галузь знань: 14 Електрична інженерія

Спеціальність: 141 «Електроенергетика, електротехніка та електромеханіка»

Освітньо-професійна програма: Системи технічного захисту інформації, автоматизація її обробки.

1. Тема роботи: Побудова та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об'єкту водного транспорту
затверджена наказом НУК від «14» 10 2025 р. № 1217-ук

2. Вихідні дані до роботи: моделі, методи і інформаційні технології оцінки та забезпечення стану захищеності ОКІ.

1.Провести аналіз методів і способів побудови реляційної моделі взаємовпливу факторів вразливостей на захищеність об'єкту водного транспорту.

2.Розробити математичну модель оцінювання залежності взаємовпливу факторів вразливостей на захищеність об'єкту водного транспорту

3.Провести експерименти з оцінки впливу факторів вразливостей на об'єкт критичної інфраструктури.

4. Терміни виконання завдання:
термін видачі завдання: «01- 05» вересня 2025 р.
термін подання роботи: «18» грудня 2025 р.

6. План-графік виконання кваліфікаційної роботи

п/п	Заходи	Дата		Готовність
		Навч. тиждень	Контрольна дата	
1.	Наукове стажування	1 - 8	27.10.2025	Звіт з наукового стажування
2.	Організаційні збори	9	29.10.2025	Попередній варіант змісту КР
3.	Рубіжний контроль	10	05.11.2025	Попередній варіант оглядових розділів, звіт з практика
4.	Рубіжний контроль	13	27-28.11.2025	Доповідь на 13-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2025»
5.	Рубіжний контроль	14	3.12.2025	1. Попередній варіант повної КР 2. Попередній варіант презентації
6.	КЕ на рівень «магістра»	15	8,9.12.2025	Складання державного екзамену зі спеціальності на ступінь магістра
7.	Перевірка на плагіат	15	10.12.2025	Електронний варіант кваліфікаційної роботи, попередній захист (робота передається студентом на кафедру для внутрішньої рецензії).
8.	Оформлення КР та супутньої документації	16	15-17.12.2025	1. Оформлена КР (в форматі pdf) У разі отримання позитивної внутрішньої рецензії, КР подається на зовнішню рецензію. 2. Оформлена презентація (в форматі pdf).
9.	Подання документів на захист	16	18.12.2025	1. Подання щодо захисту КР: тема, успішність, висновок керівника та висновок кафедри про КР. 2. Зовнішня рецензія (окремо від КР). Резюме на КР. 3. Електронний варіант презентації. 4. Електронний варіант КР на диску
10.	Захист ДР	17	22,23,24 12.2025	1. Приєднання студента до засідання кваліфікаційної комісії (конференції) у встановлений час для проведення процедури дистанційного захисту 2. Процедура захисту КР.

Керівник
д.т.н., професор, професор кафедри комп'ютерних технологій
та інформаційної безпеки, _____ В.І. Передерій

Студент _____ І.Ю. Бондаренко

АНОТАЦІЯ

У магістерській кваліфікаційній роботі досліджується проблема побудови реляційної моделі взаємовпливу факторів вразливостей на рівень захищеності об’єкта водного транспорту в умовах невизначеності, складності формалізації та впливу суб’єктивних чинників.

Проаналізовано сучасний стан оцінювання та забезпечення захищеності об’єктів водного транспорту, визначено основні фактори впливу на захищеність за умов дії природних, техногенних і людських загроз, а також узагальнено підходи до ідентифікації вразливостей.

Обґрунтовано доцільність застосування інформаційно-когнітивних технологій і методів м’яких обчислень для оцінювання впливу випадкових і комбінованих факторів. Розроблено реляційну та інформаційно-логічну моделі оцінювання захищеності об’єкта водного транспорту й алгоритми функціонування модулів контролю з урахуванням взаємозалежностей між факторами вразливостей.

Методичну основу дослідження становлять системний аналіз, графо-аналітичні методи, Байєсівські мережі довіри, методи експертних оцінок та аналіз ризиків. Досліджено вплив сценаріїв функціонування об’єкта і застосування контрзаходів на інтегральний рівень його захищеності.

Результати роботи забезпечують підвищення обґрунтованості управлінських рішень щодо забезпечення захищеності об’єктів водного транспорту в умовах невизначеності та дії людського фактору.

Ключові слова: об’єкт водного транспорту, захищеність, фактори вразливостей, реляційна модель, інформаційно-когнітивні технології, м’які обчислення, Байєсівські мережі довіри, оцінювання ризиків, людський фактор.

ABSTRACT

This master's thesis examines the problem of constructing a relational model of the mutual influence of vulnerability factors on the level of security of water transport objects in conditions of uncertainty, complexity of formalisation, and the influence of subjective factors.

The current state of assessment and security of water transport facilities is analysed, the main factors affecting security in the face of natural, man-made and human threats are identified, and approaches to vulnerability identification are summarised.

The feasibility of using information and cognitive technologies and soft computing methods to assess the impact of random and combined factors is substantiated. Relational and information-logical models for assessing the security of water transport facilities and algorithms for the functioning of control modules, taking into account the interdependencies between vulnerability factors, have been developed.

The methodological basis of the study consists of system analysis, graph-analytical methods, Bayesian confidence networks, expert assessment methods, and risk analysis. The impact of facility operation scenarios and the application of countermeasures on the overall level of its security has been investigated.

The results of the work provide a more sound basis for management decisions on ensuring the security of water transport facilities in conditions of uncertainty and human factors.

Keywords: water transport facility, security, vulnerability factors, relational model, information and cognitive technologies, fuzzy computing, Bayesian belief networks, risk assessment, human factor.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОВТ – об’єкт водного транспорту;

КІ – критична інфраструктура;

ІС ОВТ – інформаційна система об’єкта водного транспорту;

СЗІ – система захисту інформації;

ФВ – фактор вразливості;

ЗБ – загроза безпеці;

РЗ – рівень захищеності;

РМ – реляційна модель;

ВФ – взаємовплив факторів;

ОПР – особа, що приймає рішення;

СППР – система підтримки прийняття рішень;

ІБ – інформаційна безпека;

КБ – кібербезпека;

КЗ – кіберзахищеність;

КІС – критична інформаційна система;

АСУ ТП – автоматизована система управління технологічними процесами;

КФС – кіберфізична система (Cyber-Physical System);

ЗМІСТ

ВСТУП

На сьогодні одним із ключових чинників сталого розвитку транспортної галузі є забезпечення належного рівня захищеності об’єктів водного транспорту, які відіграють важливу роль у функціонуванні економіки держави, міжнародній торгівлі, логістичних процесах та забезпеченні національної безпеки. Сучасні об’єкти водного транспорту являють собою складні соціально-технічні системи, що функціонують у динамічному та потенційно небезпечному середовищі, на яке впливають як технічні, так і природні, організаційні та людські фактори.

Функціонування об’єктів водного транспорту в умовах підвищеної інтенсивності судноплавства, складних гідрометеорологічних умов, цифровізації навігаційних та інформаційних систем, а також зростання кількості потенційних загроз, пов’язаних з техногенними аваріями та людським фактором, супроводжується появою численних вразливостей. Це зумовлює необхідність розробки нових підходів до оцінювання та підвищення рівня захищеності таких об’єктів на основі комплексного аналізу взаємовпливу факторів вразливостей.

Управління захищеністю об’єктів водного транспорту ґрунтується на знаннях про поточний стан об’єкта, умови його експлуатації, характеристики навколишнього середовища та впливи, що виникають у процесі функціонування. Важливим елементом систем управління безпекою є підсистеми підтримки прийняття рішень, ефективність яких безпосередньо залежить від здатності забезпечити особу, що приймає рішення, достовірною, узгодженою та структурованою інформацією щодо реальних і прогнозованих станів об’єкта водного транспорту.

Процес формування управлінських рішень у сфері забезпечення захищеності об’єктів водного транспорту ускладнюється наявністю невизначеності, неповноти інформації, впливом суб’єктивних чинників, а також складністю взаємозв’язків між окремими факторами вразливостей. Значну роль

відіграють помилки персоналу, психологічний стан екіпажу, рівень підготовки операторів, а також несприятливі погодні та навігаційні умови. У зв'язку з цим традиційні детерміновані методи аналізу не завжди дозволяють адекватно оцінити реальний рівень захищеності об'єкта.

Моделювання взаємовпливу факторів вразливостей та оцінювання їх сукупного впливу на захищеність об'єкта водного транспорту займає провідне місце при проєктуванні та вдосконаленні систем безпеки. Оскільки розв'язання даної задачі пов'язане з багатофакторністю, високим рівнем невизначеності та складністю формалізації причинно-наслідкових зв'язків, доцільним є використання методів м'яких обчислень, когнітивного моделювання та реляційного аналізу.

Актуальність теми: На сучасному етапі розвитку транспортної галузі методи оцінювання впливу факторів вразливостей на захищеність об'єктів водного транспорту часто потребують значних обсягів статистичних даних, складних обчислень та значного часу на обробку інформації. В умовах обмеженості даних та динамічної зміни експлуатаційних параметрів виникає потреба у використанні підходів, здатних працювати з нечіткою, якісною та експертною інформацією. Реляційні моделі у поєднанні з методами м'яких обчислень дозволяють формалізувати взаємозв'язки між факторами вразливостей, врахувати їх взаємний вплив та забезпечити адаптивність оцінювання рівня захищеності об'єкта. У зв'язку з цим дослідження, спрямоване на побудову та аналіз реляційної моделі взаємовпливу факторів вразливостей, є актуальним.

Виходячи з цього, у даній роботі пропонується підхід до побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об'єкта водного транспорту з використанням сучасних методів аналізу та підтримки прийняття рішень.

Мета дослідження: Метою магістерської роботи є побудова та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об'єкта водного транспорту.

Завдання дослідження:

- Проаналізувати сучасний стан методів та способів визначення факторів вразливостей на захищеність об’єкту водного транспорту.

- Проаналізувати сучасні способи і методи оцінки взаємовпливу факторів вразливостей на захищеність об’єкту водного транспорту.

-побудувати та дослідити реляційну модель взаємовпливу факторів вразливостей на захищеність об’єкту водного транспорту.

Об’єкт дослідження:

– процеси забезпечення захищеності об’єктів водного транспорту.

Предмет дослідження:

– методи та моделі оцінювання взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту з використанням реляційного підходу та методів м’яких обчислень.

***Методи дослідження*:** Системний аналіз, методи реляційного аналізу, теорія м’яких обчислень, методи експертних оцінок, когнітивне моделювання, байєсівські підходи до оцінювання ризиків.

Наукова новизна одержаних результатів: полягає у розробці реляційної моделі, що дозволяє формалізувати та досліджувати взаємовплив факторів вразливостей на захищеність об’єкта водного транспорту з урахуванням невизначеності та суб’єктивних чинників.

Очікуваний результат: Полягає у можливості використання запропонованої моделі для підтримки прийняття рішень щодо підвищення рівня захищеності об’єктів водного транспорту в умовах складної експлуатаційної обстановки.

Робота є самостійним дослідженням, що містить теоретичні та аналітичні розділи, практичну реалізацію реляційної моделі та оцінку ефективності отриманих результатів.

1 ОСНОВНІ ПІДХОДИ ДО ФОРМУВАННЯ ТА АНАЛІЗУ БЕЗПЕКИ ОБ'ЄКТІВ ВОДНОГО ТРАНСПОРТУ

1.1 Нормативно-правове забезпечення оцінювання захищеності об'єктів водного транспорту.

Нормативно-правове забезпечення оцінювання захищеності об'єктів водного транспорту в Україні формується на основі законодавчих та підзаконних актів, які регламентують питання національної безпеки, захисту критичної інфраструктури, інформаційної та кібербезпеки, а також охорони інформації з обмеженим доступом. Зазначені нормативні документи створюють правове підґрунтя для побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей на рівень захищеності об'єктів водного транспорту. Основними нормативно-правовими актами, що визначають правові засади забезпечення безпеки та проведення оцінювання захищеності, є:

Закон України «Про критичну інфраструктуру» від 16.11.2021:
Даний Закон встановлює правові та організаційні засади створення та функціонування національної системи захисту критичної інфраструктури, до складу якої належать об'єкти водного транспорту. Закон визначає принципи і підходи до ідентифікації вразливостей та оцінювання їх впливу на загальний рівень захищеності об'єктів [1].

- Закон України «Про національну безпеку України» від 24.11.2021:
Цей Закон визначає базові принципи та напрями державної політики у сфері національної безпеки і оборони, а також розмежовує повноваження органів державної влади у питаннях забезпечення безпеки. Його положення створюють методологічну основу для комплексного аналізу загроз і вразливостей об'єктів водного транспорту [2].

-Рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» та Указ Президента України від 26.08.2021:

Стратегія кібербезпеки визначає пріоритети та напрями захисту інформаційних і інформаційно-телекомунікаційних систем, що використовуються на об’єктах водного транспорту, і враховує взаємозв’язок між кіберзагрозами та фізичними вразливостями інфраструктури [3].

-Закон України «Про основні засади забезпечення кібербезпеки України» від 15.12.2021:

Закон регламентує правові та організаційні основи захисту національних інтересів у кіберпросторі, визначає повноваження суб’єктів забезпечення кібербезпеки та принципи координації їх діяльності, що є важливим для аналізу вразливостей інформаційних компонентів об’єктів водного транспорту [4].

-Закон України «Про інформацію»:

Нормує правовідносини у сфері створення, збирання, зберігання, використання та захисту інформації, що має суттєве значення для забезпечення інформаційної складової захищеності об’єктів водного транспорту [5].

-Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»:

Відповідно до статті 8, інформація з обмеженим доступом або така, що є власністю держави, повинна оброблятися із застосуванням комплексних систем захисту інформації з підтвердженою відповідністю, що безпосередньо впливає на рівень захищеності об’єктів водного транспорту [6].

-Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29 березня 2006 р. №373:

Дані Правила визначають необхідність створення комплексних систем захисту інформації для запобігання витоку даних технічними каналами, несанкціонованим діям та спеціальним впливам, що є важливими факторами при аналізі вразливостей об’єктів водного транспорту [7].

-Закон України «Про захист персональних даних»:

Регулює правові відносини, пов’язані з обробкою та захистом персональних даних, що обробляються в інформаційних системах об’єктів водного транспорту, та спрямований на захист прав і свобод людини [8].

- Закон України «Про державну таємницю»:

Визначає порядок віднесення інформації до державної таємниці, її охорону та захист, що має ключове значення для забезпечення безпеки об’єктів водного транспорту, пов’язаних із виконанням завдань національної безпеки [9].

1.2 Роль та значення математичних методів у дослідженні загроз і вразливостей на об’єктах водного транспорту.

На сучасному етапі забезпечення захищеності об’єктів водного транспорту (морські порти, судна, перевантажувальні термінали, диспетчерські та навігаційні комплекси) дедалі більше залежить від якості обґрунтування управлінських рішень у сфері безпеки. З огляду на складну структуру таких об’єктів, багатоканальність інформаційних потоків та наявність великої кількості взаємопов’язаних факторів вразливостей, важливою стає математизація процесів оцінювання — застосування математичних методів і моделей для формалізації загроз, ризиків та рівня захищеності. У межах теми побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту, математичні методи виступають інструментом, який забезпечує: (1) перехід від описових суджень до кількісних оцінок; (2) встановлення причинно-наслідкових зв’язків між вразливостями; (3) визначення критичних комбінацій факторів, що формують найбільшу загрозу. Серед найбільш поширених підходів математичного аналізу, які застосовуються при дослідженні загроз на водному транспорті, доцільно виокремити такі.

-Методи теорії ймовірностей та математичної статистики застосовують для оцінювання частоти інцидентів, надійності технічних систем, а також для виявлення закономірностей у виникненні відмов і порушень (наприклад,

зв’язок між людським фактором, режимами експлуатації та кількістю інцидентів). На практиці це дає змогу формувати статистично обґрунтовані показники ризику та будувати прогностичні оцінки для різних сценаріїв загроз.

-Моделі ризик-аналізу та багатокритеріального оцінювання використовуються, коли захищеність не може бути описана одним параметром. Для об’єктів водного транспорту це особливо актуально, оскільки загрози можуть впливати одночасно на технологічні процеси, інформаційні системи, фізичну охорону і безпеку персоналу. Багатокритеріальні методи дозволяють узгоджувати різні показники (втрати, ймовірність реалізації загрози, час відновлення, критичність сервісів) в єдину оцінну шкалу.

-Графові та мережеві моделі є важливими для відображення структури взаємозв’язків між елементами інфраструктури: вузлами комунікацій, компонентами автоматизованих систем управління, каналами передачі даних, а також між вразливостями і загрозами. Саме мережеві моделі є природною основою для реалізації реляційного представлення: коли об’єкти (активи, загрози, вразливості, контрзаходи) описуються як сутності, а їх взаємодія — як відношення, що дозволяє аналізувати “ланцюги” впливу та поширення негативних наслідків.

-Методи теорії множин і реляційної алгебри застосовуються безпосередньо при побудові реляційної моделі взаємовпливу. Вони дозволяють формально описати множини факторів вразливостей, множини загроз та множини наслідків, а також операції над ними (перетини, об’єднання, композиції відношень). Це забезпечує строгість моделі та можливість реалізувати її у вигляді бази даних або знань, придатної до автоматизованого аналізу.

-Логіко-ймовірнісні методи та нечітка логіка є корисними у випадках, коли частина факторів не має точних числових характеристик (наприклад, “низька підготовка персоналу”, “недостатній контроль доступу”, “підвищена загроза соціальної інженерії”). Для об’єктів водного транспорту така невизначеність є типовою, тому поєднання експертних оцінок із формальними

процедурами (нечіткі множини, правила виводу) дозволяє отримувати узгоджені результати навіть за неповної інформації.

-Моделі оптимізації застосовуються для вибору найефективніших контрзаходів за обмежених ресурсів (бюджет, персонал, час простою об’єкта). В умовах водного транспорту це може бути оптимальний розподіл засобів охорони та кіберзахисту, пріоритизація оновлень, планування резервування каналів зв’язку чи відновлення критичних сервісів. Очевидно, що загрози реалізуються у разі наявності вразливостей, а характер вразливостей залежить від джерела виникнення, місця прояву в життєвому циклі об’єкта, умов експлуатації та рівня взаємодії підсистем (технічної, організаційної, інформаційної). Тому при моделюванні загроз на об’єктах водного транспорту важливою є не лише ідентифікація окремих вразливостей, а й встановлення взаємного впливу між ними, оскільки сукупний ефект декількох слабких місць часто перевищує суму їх ізольованого впливу.

З огляду на це, математичні методи дозволяють сформувати основу для подальшого дослідження та уточнення ключових понять. Якщо захищеність у контексті об’єкта водного транспорту розуміти як здатність протидіяти зовнішнім загрозам та обмежувати можливі збитки до прийнятного рівня, то оцінювання захищеності — це формалізований процес встановлення кількісних і якісних показників впливу вразливостей на конфіденційність, цілісність, доступність інформації та безперервність технологічних процесів. Таким чином, роль математичних методів у дослідженні загроз на об’єктах водного транспорту полягає в тому, що вони забезпечують формальний апарат для побудови реляційної моделі, аналізу взаємовпливу факторів вразливостей, оцінювання ризиків і підтримки прийняття рішень щодо підвищення рівня захищеності критично важливих компонентів транспортної інфраструктури.

1.3 Основні особливості застосування реляційних моделей у дослідженні загроз на об’єктах критичної інфраструктури.

Забезпечення захищеності об’єктів критичної інфраструктури, зокрема об’єктів водного транспорту, потребує системного підходу до аналізу загроз, вразливостей та можливих наслідків їх реалізації. У зв’язку з багаторівневою структурою таких об’єктів та значною кількістю взаємопов’язаних елементів, традиційні ізольовані методи оцінювання ризиків виявляються недостатніми. У цьому контексті важливу роль відіграють реляційні моделі, які дозволяють формалізувати взаємозв’язки між різними компонентами системи безпеки та досліджувати їх взаємовплив.

Методології оцінювання загроз і ризиків на об’єктах критичної інфраструктури мають враховувати всі ролі та функції, що реалізуються в системі, при цьому внутрішні фактори вразливостей не повинні розглядатися як ізольована категорія. У реляційних моделях доцільно розглядати типи загроз у поєднанні з людським фактором, включаючи інсайдерський компонент, який може проявлятися на різних рівнях функціонування об’єкта. Такий підхід дозволяє адекватно відобразити складні сценарії реалізації загроз та оцінити їх сукупний вплив на загальний рівень захищеності.

Важливу превентивну роль у зниженні ризиків відіграють оператори та експлуатуючі організації об’єктів критичної інфраструктури. У межах реляційної моделі персонал, його функції, повноваження та доступи розглядаються як окремі сутності, пов’язані відношеннями з інформаційними ресурсами, технічними засобами та технологічними процесами. Це дає змогу формалізувати ризики, пов’язані з помилковими або навмисними діями персоналу, починаючи з етапу відбору кадрів і завершуючи їх повсякденною діяльністю.

Оціночні моделі захищеності об’єктів критичної інфраструктури повинні враховувати можливість виникнення кіберінцидентів, які можуть мати ненавмисний або навмисний характер, бути зумовленими технічними

відмовами, помилками персоналу або цілеспрямованими кібератаками. Особливої актуальності це набуває для кіберфізичних систем (Cyber-Physical Systems), що широко застосовуються на об’єктах водного транспорту. У таких системах порушення цілісності чи достовірності інформації може призвести не лише до інформаційних втрат, а й до збоїв у технологічних процесах.

Застосування реляційних моделей дозволяє відобразити багаторівневу структуру захисту у вигляді сукупності взаємопов’язаних рубежів або «поясів» безпеки. Як правило, до них відносять правовий, організаційно-адміністративний, морально-етичний, фізичний та програмно-апаратний рівні захисту. Кожен із зазначених рівнів може бути представлений у моделі як окрема множина елементів, між якими встановлюються відношення залежності та взаємовпливу, що дає змогу аналізувати ефективність захисту як у цілому, так і за окремими напрямами.

З позицій мінімізації ймовірності реалізації загроз інформаційній безпеці, реляційні моделі доцільно застосовувати і для аналізу кадрових ризиків. Зокрема, процеси відбору та тестування персоналу можуть бути формалізовані у вигляді зв’язків між характеристиками кандидата, вимогами до посади та рівнями доступу до критичних ресурсів. Це дозволяє систематизувати результати експертних і психологічних оцінок та інтегрувати їх у загальну модель оцінювання захищеності об’єкта.

У практичній реалізації реляційних підходів важливим є врахування безпеки допоміжних інформаційних платформ і сервісів, що використовуються для збору та обробки даних, зокрема систем онлайн-тестування персоналу. Такі платформи можуть розглядатися у моделі як потенційні джерела вразливостей, що потребують окремих контрзаходів. У реляційній моделі це реалізується шляхом встановлення зв’язків між об’єктами тестування, персональними даними та механізмами автентифікації і захисту доступу.

Таким чином, застосування реляційних моделей у дослідженні загроз на об’єктах критичної інфраструктури дозволяє забезпечити комплексний і формалізований підхід до аналізу вразливостей, загроз і контрзаходів. Це

створює методологічну основу для побудови ефективних систем захисту та підтримки прийняття рішень щодо підвищення рівня захищеності об’єктів водного транспорту в умовах зростання складності та інтенсивності сучасних загроз.

1.4 Основні задачі та вимоги до моделювання взаємовпливу факторів вразливостей на захищеність об’єкту водного транспорту.

Моделювання взаємовпливу факторів вразливостей на захищеність об’єктів водного транспорту є складним багаторівневим процесом, який потребує врахування технічних, організаційних, інформаційних і людських складових. Методології оцінювання ризиків для таких об’єктів мають охоплювати всі ролі та функції, що реалізуються в системі, при цьому окремі фактори вразливостей не повинні розглядатися ізольовано. Навпаки, вони мають аналізуватися у взаємозв’язку з відповідними типами загроз, у тому числі з урахуванням інсайдерського компонента, що може проявлятися на будь-якому рівні функціонування об’єкта водного транспорту.

Однією з ключових задач моделювання є ідентифікація та формалізація факторів вразливостей, які виникають на різних етапах життєвого циклу об’єкта: під час проектування, впровадження, експлуатації та модернізації. У межах моделі необхідно враховувати вразливості, пов’язані з персоналом, технічними засобами, програмним забезпеченням, інформаційними ресурсами та організаційними процедурами. Особливу увагу слід приділяти людському фактору, оскільки саме персонал може одночасно виступати як елементом захисту, так і потенційним джерелом загроз.

Важливою вимогою до моделі є облік можливих кіберінцидентів, тобто подій ненавмисного або навмисного характеру, що можуть бути спричинені технічними відмовами, помилками персоналу або цілеспрямованими кібератаками. Для об’єктів водного транспорту, де широко використовуються автоматизовані та кіберфізичні системи управління, навіть незначне порушення

цілісності чи достовірності інформації може призвести до суттєвих збоїв у технологічних процесах або до загрози безпеці судноплавства. Тому модель повинна відображати як прямий, так і опосередкований вплив вразливостей на функціонування об’єкта.

Наступною задачею є структуризація рівнів захисту та відображення їх у моделі. Як правило, для об’єктів водного транспорту виділяють правовий, організаційно-адміністративний, морально-етичний, фізичний і програмно-апаратний рівні захисту. Кожен з цих рівнів має власні фактори вразливостей і механізми протидії загрозам, а їх взаємодія повинна бути формалізована у вигляді зв’язків та відношень. Це дозволяє оцінити, яким чином ослаблення одного рівня може впливати на загальну захищеність об’єкта.

З позицій мінімізації ризиків інформаційної та кіберзахищеності важливою задачею є включення до моделі кадрових процесів, зокрема відбору, навчання та контролю персоналу. Оцінювання професійної придатності працівників до виконання функцій на критичних ділянках об’єкта водного транспорту має бути формалізоване у вигляді показників, які відображають стресостійкість, відповідальність, уважність, здатність працювати з великими обсягами інформації та оперативно реагувати на події. Такі показники можуть формуватися на основі результатів тестування та експертних оцінок і бути включеними до реляційної моделі як окремі атрибути.

Важливою вимогою до моделювання є забезпечення достовірності та захищеності вхідних даних, що використовуються для аналізу. Інформаційні платформи та інструменти збору даних, зокрема системи онлайн-тестування персоналу, повинні розглядатися як потенційні об’єкти вразливостей. Тому модель має враховувати ризики витоку персональних даних, компрометації облікових записів та несанкціонованого доступу до інформації, а також передбачати відповідні контрзаходи.

Узагальнюючи викладене, можна визначити основні вимоги до моделювання взаємовпливу факторів вразливостей на захищеність об’єкту водного транспорту: комплексність, багаторівневість, урахування людського

фактора, можливість формалізації взаємозв’язків між загрозами та вразливостями, а також адаптивність до змін умов експлуатації. Реалізація таких вимог створює основу для побудови реляційної моделі, яка дозволяє здійснювати обґрунтоване оцінювання рівня захищеності та підтримувати прийняття рішень щодо підвищення безпеки об’єктів водного транспорту.

Висновок до розділу 1.

У першому розділі розглянуто нормативно-правові та методологічні засади оцінювання захищеності об’єктів водного транспорту. Встановлено, що правове регулювання у сфері критичної інфраструктури, національної та кібербезпеки, захисту інформації й персональних даних формує обов’язкову основу для ідентифікації вразливостей, визначення загроз і організації процедур оцінювання захищеності. Показано, що через багатофакторність і взаємозалежність технічних, природно-кліматичних, організаційних, інформаційних і людських чинників ефективна оцінка потребує застосування математичних методів, які забезпечують формалізацію ризиків, кількісне оцінювання впливів та підтримку прийняття рішень. Обґрунтовано доцільність використання реляційних моделей як інструменту системного подання сутностей предметної області та зв’язків між ними, що дає змогу аналізувати комбінований ефект вразливостей і встановлювати критичні ланцюги впливу на рівень захищеності. Сформульовано основні задачі та вимоги до моделювання взаємовпливу факторів вразливостей, що створює передумови для подальшої побудови та дослідження реляційної моделі захищеності об’єкта водного транспорту.

2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА СПОСОБІВ МОДЕЛЮВАННЯ ВЗАЄМОВПЛИВУ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ЗАХИЩЕНІСТЬ ОБ'ЄКТІВ ВОДНОГО ТРАНСПОРТУ

2.1 Аналіз сучасного стану методів та способів визначення факторів вразливостей на захищеність об'єкту водного транспорту.

Функціонування об'єктів водного транспорту (портові комплекси, судна, диспетчерські центри, навігаційні та інформаційно-керуючі системи) у сучасному інформаційному середовищі тісно пов'язане з наявністю численних вразливостей та загроз різної природи. Ці об'єкти одночасно перебувають під впливом фізичних, технічних, організаційних, інформаційних і кібернетичних факторів, що обумовлює необхідність застосування комплексних підходів до аналізу їх захищеності.

Управління захищеністю об'єктів водного транспорту ґрунтується на знаннях про поточний і прогнозований стан об'єкта, умови його функціонування, а також про характер і інтенсивність деструктивних впливів. Невід'ємною складовою таких систем управління є підсистеми підтримки прийняття рішень, ефективність яких безпосередньо залежить від якості моделей, що описують взаємовплив факторів вразливостей.

Сучасні методи аналізу безпеки об'єктів критичної інфраструктури базуються на розумінні категорії «захищеність» як складного стану системи, що формується під впливом протиріч, загроз і поточних умов функціонування. У цьому контексті ключовими поняттями є стан об'єкта, загроза, вразливість та *ризик*, які перебувають у тісному причинно-наслідковому зв'язку. (Рис.2.1.)

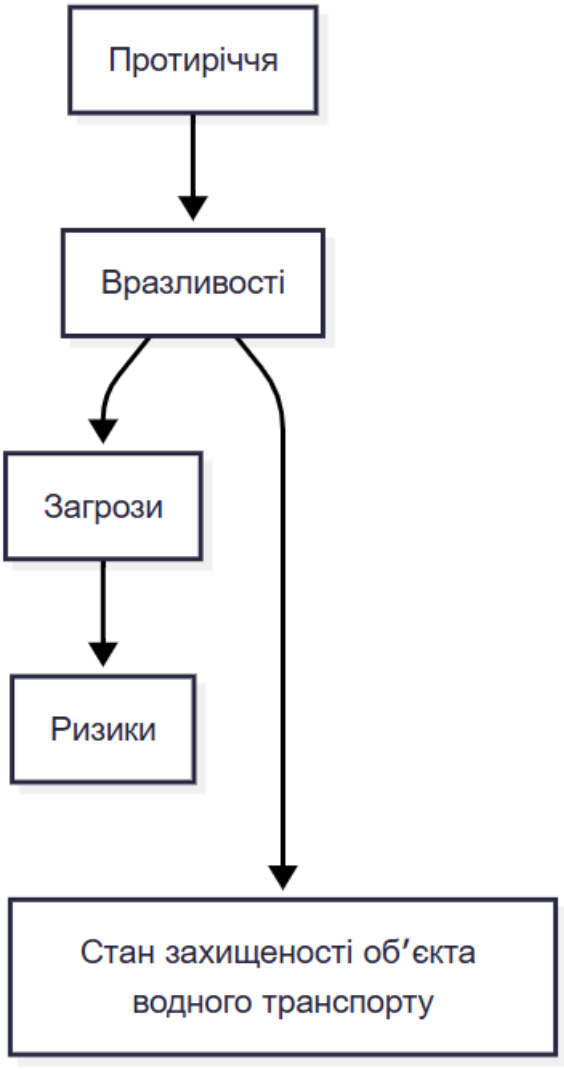

Рисунок 2.1 - Сутнісні складові захищеності об’єкта водного транспорту

Погляд на загрози через призму виникнення та розвитку вразливостей зумовлює необхідність систематизації факторів, які можуть призводити до порушення захищеності об’єкта водного транспорту. До таких факторів належать інформаційні, людські, організаційні та техніко-технологічні складові, що формують умови безпечної або небезпечної експлуатації.

На основі аналізу сучасних джерел можна виділити найбільш актуальні загрози для об’єктів водного транспорту, що реалізуються через виявлені вразливості (табл. 2.1).

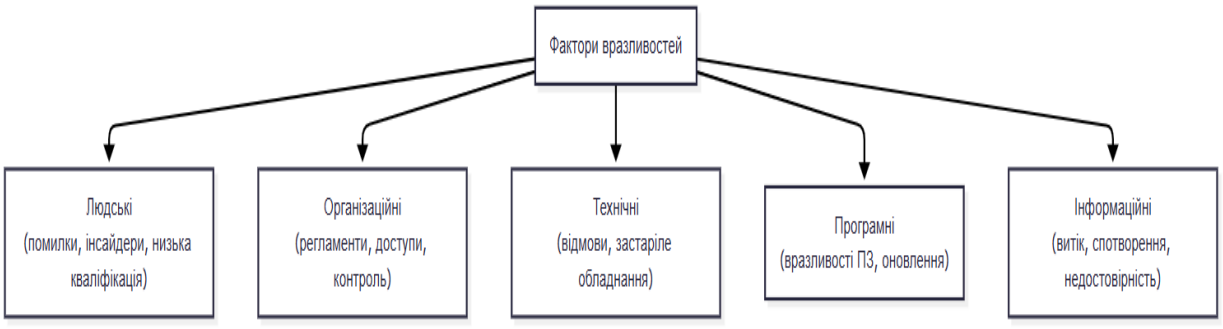

Рисунок 2.2 -Класифікація факторів вразливостей об’єкта водного транспорту.

Таблиця 2.1 – Основні загрози об’єктам водного транспорту

Загроза	**Характеристика**
Несанкціонований доступ	Отримання доступу до навігаційних або керуючих систем
Мережеві атаки	Використання корпоративних або службових мереж
Атаки на стандартні компоненти	Вразливості типових IT-рішень
DDoS-атаки	Порушення доступності сервісів
Людський фактор	Помилки персоналу або навмисні дії
Шкідливе ПЗ	Інфікування через зовнішні носії
Порушення цілісності даних	Спотворення навігаційної або технологічної інформації
Техногенні та природні фактори	Аварії, погодні умови, відмови обладнання

Аналіз сучасних підходів показує, що більшість існуючих методик зосереджені на локальному аналізі окремих загроз або вразливостей і недостатньо враховують їх взаємовплив. Це обмежує можливості комплексної оцінки захищеності складних багатокомпонентних об’єктів водного транспорту.

Особливої уваги потребують кіберфізичні системи, в яких порушення інформаційної складової може безпосередньо впливати на фізичні процеси управління. У таких умовах захищеність об’єкта доцільно розглядати як багатовимірну характеристику, що формується сукупним впливом декількох взаємозалежних факторів.

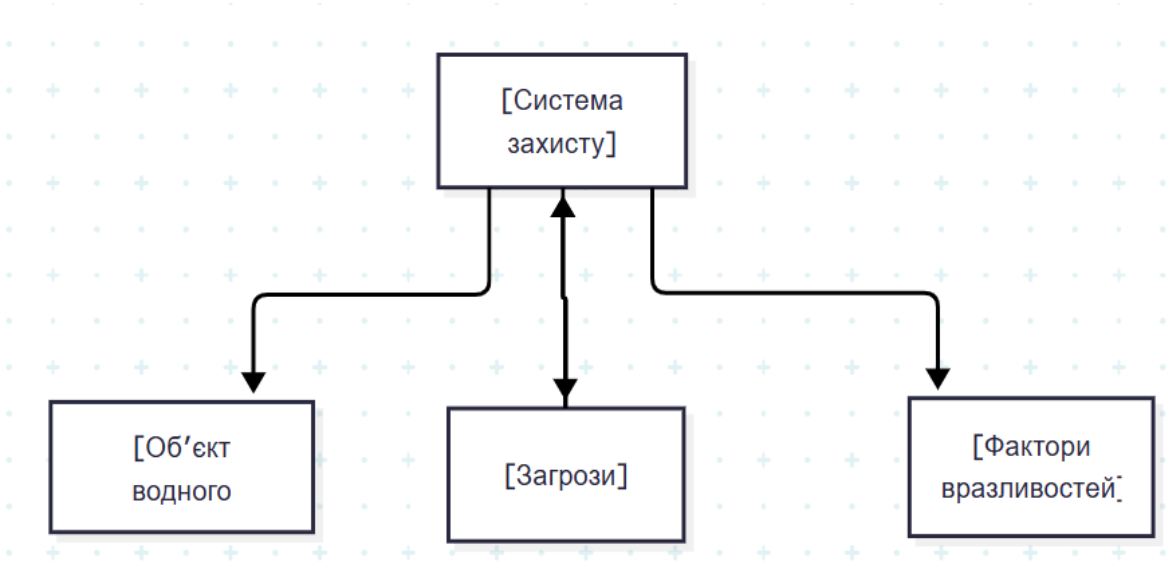

Рисунок 2.3 - Узагальнена модель протиборства в кіберфізичному середовищі водного транспорту

Таким чином, виникає потреба у застосуванні реляційних та когнітивних моделей, які дозволяють формалізувати взаємозв'язки між факторами вразливостей, загрозами та показниками захищеності. Особливо перспективними є підходи, що використовують нечіткі когнітивні карти, байєсівські мережі та реляційні бази знань, які здатні працювати в умовах невизначеності та неповноти вхідних даних.

Отже, проведений аналіз сучасного стану методів і способів визначення факторів вразливостей свідчить про доцільність переходу від фрагментарних оцінок до комплексного реляційного моделювання, що дозволяє враховувати багатокритеріальний характер захищеності об'єктів водного транспорту та забезпечує науково обґрунтовану підтримку прийняття рішень.

Рисунок 2.4 - Узагальнений алгоритм аналізу взаємовпливу факторів вразливостей

2.2 Аналіз сучасних способів і методів оцінки взаємовпливу факторів вразливостей на захищеність об'єкту водного транспорту.

Процес формування обґрунтованих рішень щодо підвищення рівня захищеності об'єктів водного транспорту здійснюється в умовах дії значної кількості різнорідних факторів вразливостей, які мають складний, нелінійний та взаємозалежний характер. До таких факторів належать людський фактор, програмні та технічні вразливості, організаційні недоліки, технічні відмови та кібератаки на інформаційні й навігаційні системи. Особливістю

зазначених факторів є наявність суттєвої невизначеності, неповноти статистичної інформації та значного впливу суб’єктивних чинників.

В умовах, коли побудова строгих аналітичних моделей є ускладненою або неможливою, доцільним є застосування експертного методу оцінювання, який дозволяє формалізувати знання та досвід фахівців предметної області й використати їх для аналізу взаємовпливу факторів вразливостей. Згідно з підходами, викладеними в навчальному посібнику НУК, експертні методи є ефективним інструментом підтримки прийняття рішень у слабоструктурованих системах, де домінують якісні залежності та суб’єктивні оцінки.

Для подальшої формалізації результатів експертного оцінювання та урахування імовірнісної природи реалізації загроз у роботі обрано байєсівські мережі як інструмент моделювання взаємовпливу факторів вразливостей. Байєсівські мережі дозволяють подати систему у вигляді орієнтованого ациклічного графа, вершини якого відповідають факторам або подіям, а дуги відображають умовні залежності між ними. Такий підхід забезпечує можливість врахування комбінованого впливу декількох факторів, обчислення ймовірності реалізації інцидентів та оновлення оцінок у разі надходження нової інформації.

Таким чином, поєднання експертних оцінок і байєсівських мереж створює методичну основу для комплексного оцінювання взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту в умовах невизначеності та обмеженості вихідних даних.

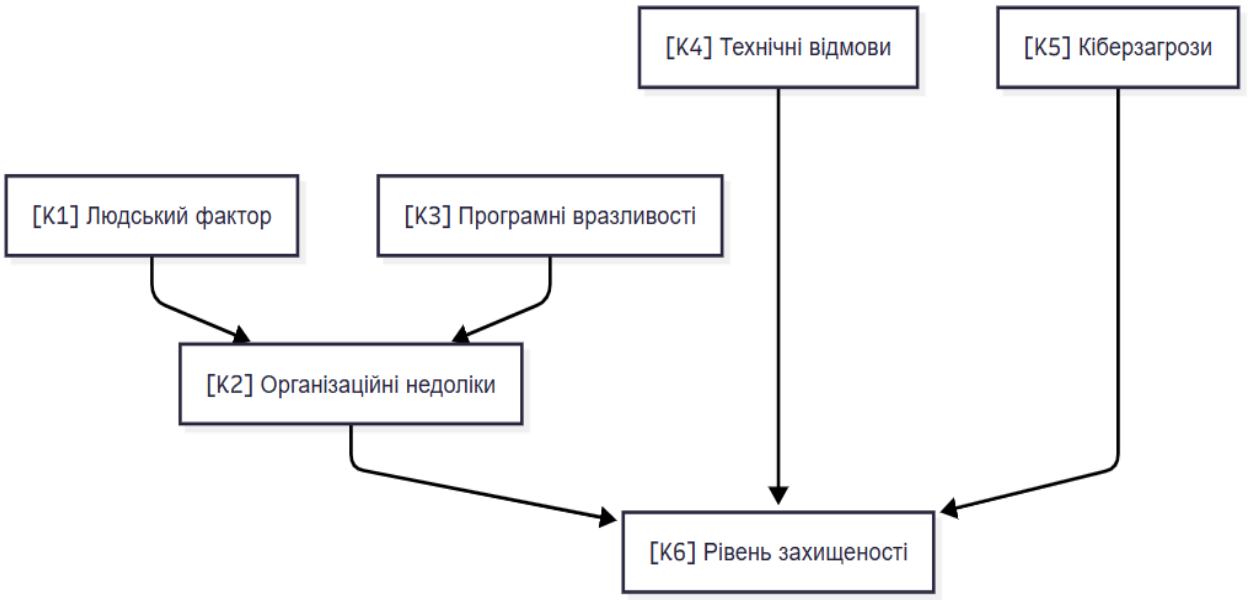

Рисунок 2.5 Схема взаємовпливу факторів вразливостей, що використовується в сучасних методах оцінювання захищеності об’єктів водного транспорту

Нехай задано множину факторів вразливостей:

$$K = \{K_1, K_2, \ldots, K_n\}, \tag{2.1}$$

де Ki— окремий фактор, що впливає на рівень захищеності об’єкта водного транспорту.

Експертне оцінювання полягає у визначенні:

- значущості кожного фактора;
- сили впливу одного фактора на інший;
- інтегрального впливу факторів на рівень захищеності.

Вагові коефіцієнти факторів визначаються на основі узагальнення думок групи експертів:

$$w_i = \frac{1}{m} \sum_{j=1}^{m} w_{i} \tag{2.2}$$

де:

- wij — оцінка важливості і-го фактора, надана j-м експертом;
- m — кількість експертів.

Для забезпечення порівнянності результатів здійснюється нормування:

$$\sum_{i=1}^{n} w_i = 1. \tag{2.3}$$

Взаємовплив факторів вразливостей описується матрицею експертних оцінок:

$$A = [a_{ij}], \tag{2.4}$$

де αij — експертна оцінка впливу фактора Ki на фактор Kj.

Елементи матриці можуть набувати значень у нормованій шкалі:

$$a_{ij} \in [0; 1], \tag{2.5}$$

де 0 відповідає відсутності впливу, а 1 — максимальному впливу.

Узагальнене значення взаємовпливу визначається шляхом усереднення експертних оцінок:

$$\bar{a}_{ij} = \frac{1}{m} \sum_{k=1}^{m} a_{ij}^{(k)}. \tag{2.6}$$

Інтегральна оцінка рівня захищеності

Інтегральний рівень захищеності об’єкта водного транспорту визначається як функція сукупного впливу факторів вразливостей:

$$Z = 1 - \sum_{i=1}^{n} w_i \cdot k_i, \tag{2.7}$$

де: ki — експертна оцінка рівня прояву iii-го фактора вразливості.

Отримане значення Z дозволяє кількісно оцінити поточний стан захищеності та використовується для порівняння альтернативних сценаріїв управління безпекою.

Переваги експертного методу для об’єктів водного транспорту

Застосування експертного методу оцінювання взаємовпливу факторів вразливостей має низку суттєвих переваг:

- можливість роботи за відсутності повної статистичної інформації;
- урахування досвіду та інтуїції фахівців галузі водного транспорту;
- гнучкість та адаптивність до змін умов функціонування об’єкта;
- простота інтеграції в системи підтримки прийняття рішень.

Таким чином, експертний метод оцінювання є доцільним і ефективним інструментом аналізу взаємовпливу факторів вразливостей на захищеність об’єктів водного транспорту в умовах невизначеності та обмеженості формалізованих даних, що повністю узгоджується з методологічними положеннями, викладеними у навчальному посібнику НУК.

Байєсівські мережі обрано як інструмент імовірнісного моделювання, що забезпечує формалізацію причинно-наслідкових залежностей між факторами вразливостей та інцидентами, а також дозволяє враховувати їх комбінований вплив. Застосування байєсівського підходу дає змогу працювати в умовах невизначеності, оновлювати оцінки при надходженні нової інформації та отримувати ймовірнісні характеристики рівня захищеності об’єкта водного транспорту.

Формально байєсівська мережа задається як пара ⟨G, P⟩, де G — направлений ациклічний граф, а P — множина таблиць умовних імовірностей для кожної вершини відносно її батьківських вершин.

У межах мережі сукупний (спільний) імовірнісний розподіл для множини випадкових змінних X1,…Xn обчислюється за співвідношенням

$$P(X_1, \ldots, X_n) = \prod_{i=1}^{n} P\big(X_i \mid Pa(X_i)\big), \tag{2.1}$$

де Pa(Xi) — множина батьківських вершин для Xi.

Застосування у задачі оцінювання ризику для об’єкта водного транспорту дає можливість не “складати” незалежні ризики, а враховувати умовні залежності, тобто те, як один фактор змінює ймовірність прояву іншого, а разом — імовірність цільової події.

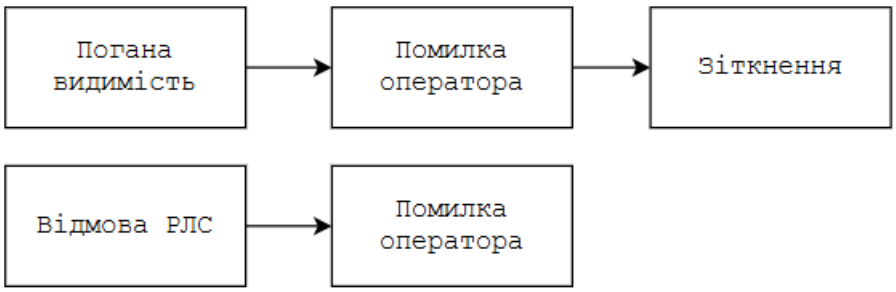

Рисунок 2.6 - Фрагмент причинно-наслідкової структури оцінки ризику інциденту.

У відповідності до структури на рис. 2.6 подія “Зіткнення” може розглядатися як змінна C, що залежить від сукупності причинних факторів: видимості V, відмови РЛС R та помилки оператора E. Узагальнена залежність задається у вигляді:

$$P(C) = f\big(P(V), P(R), P(E)\big). \tag{2.2}$$

При використанні байєсівської мережі така функція конкретизується через

правила розкладу спільної ймовірності. Зокрема, якщо структура мережі визначена як:

- V→E
- R→E
- E→C

То спільний розподіл може бути поданий як:

$$P(V, R, E, C) = P(V)\, P(R)\, P(E \mid V, R)\, P(C \mid E). \tag{2.3}$$

Звідси ймовірність інциденту “Зіткнення” визначається шляхом маргіналізації (підсумовування) за всіма можливими станами причинних змінних:

$$P(C) = \sum_{v} \sum_{r} \sum_{e} P(C \mid e)\, P(e \mid v, r)\, P(v)\, P(r). \tag{2.4}$$

Співвідношення є принципово важливим, оскільки воно показує, що оцінка ризику формується не на основі одного параметра (наприклад, лише видимості), а як результат комбінації факторів. Саме тому в реальних умовах навіть за несприятливої видимості ризик може бути зменшений (або збільшений) за рахунок зміни ймовірності помилки оператора через технічну підтримку (РЛС) або навпаки — зростає у разі відмови системи.

Додатково, при оцінюванні впливів у межах моделі можуть застосовуватися узагальнені ймовірнісні показники. Зокрема, у посібнику

НУК для інтегральної оцінки ступеня впливу використовується середнє значення ймовірності:

$$P(y_j) = \frac{1}{m} \sum_{i=1}^{m} P_i(y_j), \tag{2.5}$$

де Pi(yj) - оцінка (ймовірність) впливу за і-м фактором/критерієм, m — кількість врахованих факторів.

Тому застосування є доцільним у випадках, коли необхідно отримати узагальнену оцінку впливу певної властивості/показника (наприклад, загального рівня небезпеки або рівня реалізації вразливостей) на основі набору часткових оцінок.

Таким чином, байєсівська мережа у задачі оцінювання ризику дозволяє:

- формалізувати причинно-наслідкові зв’язки між факторами;
- обчислювати ймовірність інциденту на основі умовних ймовірностей;
- враховувати комбінований вплив факторів;
- уточнювати оцінки при зміні вихідних даних (оновлення вхідних ймовірностей)

2.3 Постановка задачі побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкту водного транспорту

У різних галузях критичної інфраструктури та для різних типів об’єктів застосовується широкий спектр підходів до оцінювання рівня захищеності інформаційних систем і технологічних процесів. Для об’єктів водного транспорту, до яких належать порти, судна, термінали, диспетчерські та навігаційні комплекси, задача оцінювання захищеності істотно ускладнюється через багатофакторний характер загроз і вразливостей. Вони

можуть проявлятися одночасно у кіберпросторі, фізичному середовищі та внаслідок дій або помилок персоналу.

Особливістю об’єктів водного транспорту є тісна взаємопов’язаність інформаційних, технічних і організаційних компонентів. Порушення функціонування окремого елемента або наявність вразливості в одній підсистемі може призводити до каскадних ефектів і зниження захищеності інших елементів, включаючи критичні технологічні процеси. Тому коректне оцінювання захищеності таких об’єктів потребує врахування не лише окремих факторів вразливостей, а й їх взаємовпливу.

Аналіз існуючих методик оцінювання захищеності показує, що їх умовно можна поділити на три основні класи підходів, які застосовуються в практиці забезпечення безпеки об’єктів водного транспорту:

- Підходи стандартного аудиту та відповідності (compliance-based), орієнтовані на перевірку виконання вимог нормативних документів і наявності визначених заходів безпеки.
- Ризик-орієнтовані підходи (risk-based), що спрямовані на ідентифікацію загроз, оцінювання ризиків та визначення пріоритетів їх зменшення.
- Структурно-орієнтовані модельні підходи (model-based), які базуються на формалізованому описі об’єкта у вигляді сутностей та відношень між ними.

Порівняльний аналіз зазначених підходів наведено в таблиці 2.2.

Проведений аналіз свідчить, що для задачі дослідження взаємовпливу факторів вразливостей на захищеність об’єктів водного транспорту найбільш доцільним є застосування структурно-орієнтованого модельного підходу, реалізованого у вигляді реляційної моделі. Така модель дозволяє впорядкувати інформацію про активи, компоненти, вразливості, загрози, інциденти та контрзаходи, а також формалізувати їх взаємозалежності у вигляді відношень.

У межах даного дослідження реляційна модель розглядається як формалізований опис предметної області, у якому фактори вразливостей та елементи об’єкта водного транспорту представлені у вигляді множин сутностей з визначеними атрибутами та відношеннями між ними. Це створює основу для аналізу як прямих, так і непрямих впливів факторів на інтегральний рівень захищеності.

- оцінювання сукупного прямого та непрямого впливу факторів вразливостей на інтегральний показник захищеності;
- реалізації сценарного аналізу розвитку інцидентів і можливих каскадних ефектів;
- формування рекомендацій щодо вибору контрзаходів і пріоритизації заходів підвищення захищеності.

Таким чином, актуальною є задача розробки та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту**,** яка поєднує структурний опис предметної області з можливостями кількісного та якісного аналізу. Результати такого моделювання можуть бути використані для підвищення обґрунтованості управлінських рішень, удосконалення системи контролю стану захищеності та підтримки прийняття рішень в умовах невизначеності та динамічної зміни загроз.

Таким чином, за результатами проведеного аналізу сучасного стану методів і способів визначення факторів вразливостей, а також методів оцінювання їх взаємовпливу на захищеність об’єктів водного транспорту встановлено, що значна увага у наукових дослідженнях приділяється проблемам безпеки критичної транспортної інфраструктури в умовах багатофакторності та невизначеності. Разом із тим, більшість існуючих підходів орієнтовані на ізольований аналіз окремих загроз або вразливостей і не забезпечують комплексного урахування їх взаємозалежностей та можливих каскадних ефектів.

Таблиця 2.2 – Порівняльний аналіз підходів до оцінювання захищеності об’єктів водного транспорту.

Підхід клас. методик	**Переваги**	**Недоліки**
Аудит відповідності (compliance-based)	забезпечує базову перевірку виконання вимог; зручний для регулярного контролю; орієнтований на стандарти	Слабко враховує взаємовплив факторів; не відображає каскадні ефекти; не дає оцінки впливу
Ризик-орієнтовані (risk-based)	дозволяють ранжувати загрози; підтримують пріоритизацію заходів; формують основу управління ризиками	залежать від якості вихідних даних; складно відобразити структурні залежності; потребують постійної актуалізації
Модельні структурні (реляційні)	формалізують сутності та зв’язки; дозволяють аналізувати взаємовплив вразливостей; придатні для сценарного аналізу та автоматизації	потребують чіткої постановки предметної області; складність зростає зі збільшенням кількості елементів

З огляду на це, задачі оцінювання захищеності об’єктів водного транспорту, які характеризуються високим ступенем невизначеності, складністю формалізації та наявністю значної частки суб’єктивних чинників, доцільно вирішувати із застосуванням структурно-орієнтованих модельних підходів. Найбільш придатним у цьому контексті є реляційний підхід, що дозволяє формалізувати множину факторів вразливостей, загроз і контрзаходів, а також описати їх взаємовплив у вигляді відношень.

Виходячи з наведеного, у даній роботі поставлено задачу побудови і дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту, яка створює методичну основу для подальшого оцінювання рівня захищеності та підтримки прийняття управлінських рішень у сфері безпеки водного транспорту.

Висновок до розділу 2.

У другому розділі проаналізовано сучасні методи визначення факторів вразливостей та оцінювання їх взаємовпливу на захищеність об’єктів водного транспорту. Встановлено, що функціонування таких об’єктів відбувається в динамічному середовищі під дією технічних, організаційних, інформаційних, природних і людських чинників, що зумовлює багатофакторний характер вразливостей та необхідність комплексного підходу до оцінювання захищеності. Показано, що більшість існуючих підходів орієнтовані на аналіз окремих загроз і недостатньо враховують взаємозалежності та каскадні ефекти, притаманні кіберфізичним системам водного транспорту. Обґрунтовано доцільність застосування реляційного моделювання як засобу структуризації предметної області та формалізації відношень між факторами в умовах невизначеності. Отримані результати сформували методичне підґрунтя для постановки задачі побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей, що реалізується в наступних розділах роботи.

3.ЗАСТОСУВАННЯ МЕТОДІВ М'ЯКИХ ОБЧИСЛЕНЬ В ПОБУДОВІ ТА ДОСЛІДЖЕННІ РЕЛЯЦІЙНОЇ МОДЕЛІ ВЗАЄМОВПЛИВУ ФАКТОРІВ ВРАЗЛИВОСТЕЙ НА ЗАХИЩЕНІСТЬ ОБ'ЄКТУ ВОДНОГО ТРАНСПОРТУ

3.1 Розробка інформаційної моделі впливу факторів вразливостей на захищеність об'єкта водного транспорту.

Функціонування об'єктів водного транспорту відбувається в умовах складного та динамічного середовища, що характеризується одночасною дією технічних, природно-кліматичних, організаційних, інформаційних і людських факторів. Сукупний вплив зазначених чинників формує багатовимірний простір вразливостей, який безпосередньо визначає рівень захищеності об'єкта та його здатність до безпечного і стійкого функціонування. У таких умовах традиційні детерміновані підходи до оцінювання безпеки виявляються недостатньо ефективними, оскільки не дозволяють у повному обсязі врахувати нелінійність взаємозв'язків, невизначеність вихідних даних та суттєвий вплив людського фактору.

Аналіз наукових джерел і навчальних посібників із системного аналізу, безпеки судноплавства та інформаційно-когнітивних технологій свідчить про доцільність побудови інформаційної моделі, яка відображає не лише перелік окремих факторів вразливостей, а й причинно-наслідкові зв'язки між ними. Така модель створює концептуальне підґрунтя для подальшої формалізації у вигляді реляційної, ймовірнісної або когнітивної моделі та забезпечує підтримку прийняття рішень у сфері управління захищеністю об'єктів водного транспорту.

Інформаційна модель впливу факторів вразливостей на захищеність об'єкта водного транспорту розглядається як формалізований опис предметної області, у межах якого визначено склад факторів, їх ієрархію та характер взаємодії. Основною ідеєю побудови такої моделі є припущення, що більшість

інцидентів і аварій не є наслідком дії одного ізольованого фактору, а виникають у результаті поєднання декількох несприятливих умов.

Наприклад, відмова навігаційного обладнання сама по собі не обов'язково призводить до аварійної ситуації, однак у поєднанні з обмеженою видимістю, високою інтенсивністю руху у фарватері, несприятливими погодними умовами та недостатньою кваліфікацією оператора рівень ризику суттєво зростає. Саме такі комбіновані впливи і мають бути відображені в інформаційній моделі.

Відповідно до цього, інформаційна модель повинна:

- Структурувати фактори вразливостей за змістовими групами;
- Відображати взаємозв'язки між окремими факторами та їх агрегованими групами;
- Дозволяти аналізувати вплив комбінацій факторів на інтегральний рівень захищеності;
- Слугувати основою для побудови реляційної моделі взаємовпливу факторів.

У межах розробки інформаційної моделі виділено низку базових сутностей, характерних для предметної області водного транспорту, а саме: об'єкт водного транспорту, фактори вразливостей, потенційні загрози, середовище функціонування, контрзаходи та інциденти. Фактори вразливостей розглядаються як первинні елементи, що формують імовірність реалізації загроз та визначають рівень захищеності об'єкта.

Для впорядкування предметної області всі фактори згруповано за змістовою ознакою, що відповідає логіці побудови наведеної інформаційної моделі.

Група природно-кліматичних факторів описується множиною:

$$F_{nt} = \{R_{Vb}, R_{Wc}, R_{Tr}, R_{Fc}\} \tag{3.1}$$

Де:

- RVb - Visibilyty - рівень видимості,

- RWc – Wether Conditions – Погодні умови

- RTr – Trafic Intensiti – Інтенсивність руху

- RFc- Fairway Condition – Стан фарватеру

Дані фактори формують природне середовище функціонування об’єкта водного транспорту та безпосередньо впливають на складність навігаційної обстановки.

Організаційно-управлінські фактори представлені множиною:

$$F_{org} = \{R_{Rq}, R_{Acl}, R_{Etl}\} \tag{3.2}$$

Де:

- RRq - Regulation Quality - якість нормативного та регламентного забезпечення,

- RAcl - Acces Control Level - Рівень контролю доступу

- REtl - Emeregency Training Level - Рівень підготовки до дій у надзвичайних ситуаціях.

Ця група визначає здатність організації своєчасно реагувати на загрози та мінімізувати наслідки інцидентів.

Інформаційні та кібернетичні фактори подані множиною:

$$F_{cf} = \{R_{Cv}, R_{Car}, R_{Ndi}\} \tag{3.3}$$

Де:

- RCv - Cyber Vulnerability - Вразливість кібербезпеки

- RCar - Cyber Atack Risk - Ризик кібератаки

- RNdi - Nav data integrity - Цілісність навігаційних даних

Зазначені фактори відображають вплив цифрового середовища та інформаційних систем на загальний рівень захищеності об’єкта.

Група контрзаходів і захисних механізмів описується множиною:

$$F_{cm} = \{RS_r, RM_{sm}, RI_{sl}\}, \tag{3.4}$$

Де: - RSr – System Redundancy - Резервування системи

- RMsm – Monitoring system matunity - Зрілість системи моніторингу

- RIsl – IT security level - Рівень IT-безпеки

Ці фактори мають компенсуючий характер і здатні зменшувати негативний вплив інших вразливостей.

Фактори ризиків та інцидентів формалізуються множиною:

$$F_{ri} = \{RN_{er}, RIn, RP_l\} \tag{3.5}$$

Де:- RNer - Navigation Error risk - Ризик навігаційної помилки

- RIn - Incident - Інцидент

- RPl - Protection level - Рівень захисту

Технічні фактори описуються множиною:

$$F_{tl} = \{RH_i, RP_{ss}, RN_{ss}, RC_{ss}\} \tag{3.6}$$

Де:RHi - HullIntegrity - Цілісність корпусу

RPss - Power system state - Стан енергосистеми

RNss - Navigation system state - Стан навігаційної системи

RCss - Comm system state - Стан системи зв'язку

Людський фактор описується множиною:

$$F_{hn} = \{RP_c, RC_f, RC_q, RO_e\} \tag{3.7}$$

Де:- RPc - Procedure compliance - Процедури дотримання вимог

- RCf - Crew Fatigue - Втома екіпажу

- RCq - Crew Qualification - Кваліфікація екіпажу

- Roe - Oprerator Error - Помилка оператора

Ця група факторів відіграє ключову роль у формуванні кінцевого рівня захищеності, оскільки саме людина виступає центральним елементом системи прийняття рішень.

Фактори впливають на загрози та визначають імовірність прояву інциденту.

Враховуючи всі фактори було побудовано таку інформаційну модель:

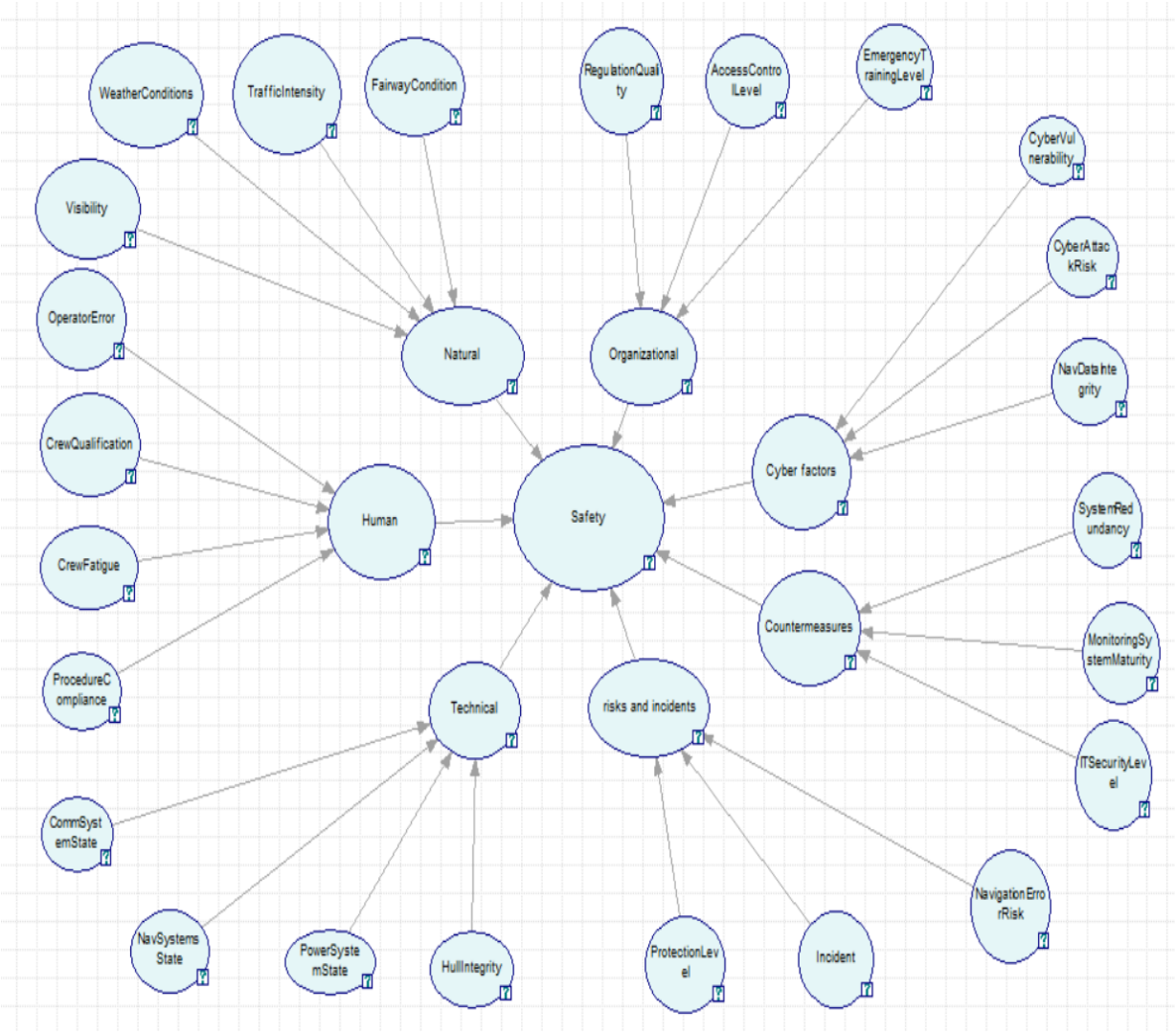

Рисунок 3.1 – Інформаційна модель впливу на безпеку об’єкта водного транспорту.

Логіка взаємозв’язків та формування інтегрального показника.

Згідно з інформаційною моделлю, окремі групи факторів впливають на узагальнений показник захищеності S через систему причинно-наслідкових зв’язків. У загальному вигляді рівень захищеності поданий як функція сукупності факторів:

$$S = F(F_{nt}, F_{org}, F_{cf}, F_{cm}, F_{ri}, F_{tl}, F_{hn}), \tag{3.8}$$

де:

функція F(·) відображає агрегування впливів з урахуванням їх взаємозалежностей.

Такий підхід відповідає рекомендаціям навчальних посібників та дозволяє перейти від ізольованого аналізу факторів до комплексної оцінки захищеності об’єкта водного транспорту.

Таким чином, розроблена інформаційна модель є логічно обґрунтованим відображенням предметної області, забезпечує структуризацію факторів вразливостей та створює методичну основу для подальшої побудови реляційної моделі взаємовпливу факторів на захищеність об’єкта водного транспорту.

3.2 Визначення та оцінка впливу основних факторів вразливостей на захищеність об’єкту водного транспорту.

Було проведено оцінювання впливу факторів вразливостей на захищеність об’єкта водного транспорту, оскільки дана задача є складною багатокритеріальною та характеризується значною невизначеністю вихідної інформації. Різнорідність факторів впливу, що охоплюють природні, технічні, організаційні, кібернетичні та людські аспекти функціонування об’єкта, зумовлює необхідність застосування методичного підходу, здатного

забезпечити отримання кількісних оцінок за відсутності повної статистичної бази.

У межах даного дослідження основним методом оцінювання обрано експертний метод, який дозволяє формалізувати знання та практичний досвід фахівців галузі водного транспорту щодо ступеня прояву факторів вразливостей і сили їх впливу на захищеність об’єкта. Експертні оцінки використовуються як вихідні дані для подальших розрахунків, що підтверджується наведеною далі таблицею експертних оцінок (табл. 3.1) та відповідною графічною інтерпретацією результатів рис. (3.4).

Для кількісної обробки отриманих експертних даних та врахування взаємовпливу факторів застосовується імовірнісний апарат як допоміжний інструмент. На його основі формуються апріорні імовірності станів факторів та реалізується причинно-наслідкова залежність типу «фактор → проміжний стан → інцидент», що дозволяє перейти від окремих оцінок до розрахунку імовірності виникнення небажаних подій за правилами умовної та повної ймовірності.

З метою узагальнення результатів оцінювання використовується інтегральний показник ризику, який формується на основі часткових оцінок впливу факторів із урахуванням їх вагових коефіцієнтів. Отримане значення інтегрального ризику використовується для оцінювання загального рівня захищеності об’єкта водного транспорту та порівняння можливих сценаріїв його функціонування.

Таким чином, у даному підрозділі експертний метод є основним інструментом оцінювання, тоді як імовірнісні розрахунки та реляційне подання результатів застосовуються як допоміжні засоби обробки, узагальнення та інтерпретації експертних даних, що забезпечує логічну цілісність і практичну спрямованість виконаного дослідження.

Для проведення оцінювання було сформовано експертну групу, до складу якої увійшли спеціалісти з експлуатації об’єктів водного транспорту, інформаційної та кібербезпеки, автоматизованих систем управління, а також

фахівці з організації та управління безпекою. Добір експертів здійснювався з урахуванням їхнього професійного стажу, рівня компетентності та практичного досвіду роботи з об’єктами критичної інфраструктури водного транспорту.

Кожному експерту було запропоновано здійснити незалежне оцінювання визначеної множини факторів вразливостей, що впливають на рівень захищеності об’єкта водного транспорту. Оцінювання проводилося за уніфікованою шкалою, що дозволяє привести суб’єктивні судження до порівнюваного вигляду. Експертам пропонувалося визначити ступінь прояву кожного фактора та оцінити його вплив на загальний рівень захищеності.

Отримані індивідуальні експертні оцінки підлягали агрегуванню шляхом усереднення, що дозволило зменшити вплив суб’єктивних відхилень та сформувати узагальнені значення для кожного фактора. Сформовані таким чином експертні оцінки були використані для побудови ймовірнісних та реляційних характеристик факторів вразливостей, а також для подальшого аналізу їх взаємовпливу.

Застосування експертного підходу забезпечило можливість формалізації слабоструктурованої інформації та отримання вихідних даних, необхідних для побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту в умовах невизначеності та мінливості загроз.

За результатами експертного опитування (5 експертів) імовірність кожного стану визначається як середнє арифметичне.

Експериментальні дослідження в межах даної роботи виконано у формі модельного експерименту, що базується на експертних оцінках факторів вразливостей та їх подальшій імовірнісній обробці. Такий підхід є доцільним для об’єктів критичної інфраструктури водного транспорту, для яких проведення натурних експериментів є обмеженим або неможливим.

Таблиця 3.1 – Надані Експертні оцінки.

Вузол	**Стан**	**E 1**	**E 2**	**E 3**	**E 4**	**E 5**	**Сер.**
Natural	Favourable	0.60	0.55	0.50	0.45	0.40	0.50
	Unfavourable	0.40	0.45	0.50	0.55	0.60	0.50
Organizational	ReadinessLevel	0.60	0.55	0.50	0.45	0.40	0.50
	RiskExposure	0.40	0.45	0.50	0.55	0.60	0.50
Cyber factors	ResilienceLevel	0.60	0.55	0.50	0.45	0.40	0.50
	RiskExposure	0.40	0.45	0.50	0.55	0.60	0.50
Technical	Serviceability	0.65	0.55	0.50	0.45	0.35	0.50
	Malfunction	0.35	0.45	0.50	0.55	0.65	0.50
Human	PerformanceState	0.60	0.55	0.50	0.45	0.40	0.50
	RiskLevel	0.40	0.45	0.50	0.55	0.60	0.50

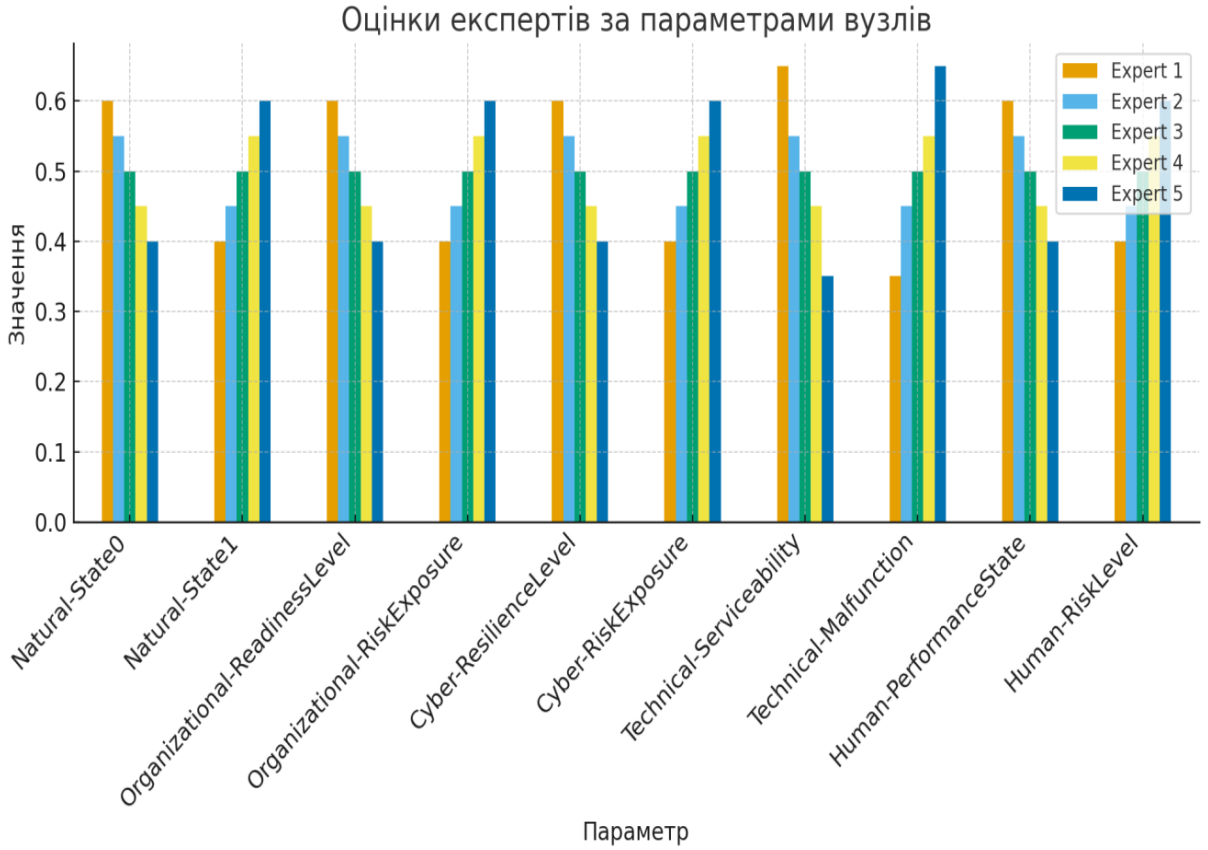

Рисунок 3.2 – Оцінки експертів за параметрами вузлів

:

$$P(\text{state}) = \frac{1}{m}\sum_{k=1}^{m} P_k(\text{state}), \qquad m = 5 \tag{3.9}$$

де Pk(state)— оцінка k-го експерта для відповідного стану.

Отримані оцінки (середні значення) для вузлів моделі мають вигляд

- Natural:

P(N=Favourable)=0.60, P(N=Unfavourable)=0.40;

- Technical:

P(T=Serviceability)=0.70, P(T=Malfunction)=0.30;

Human:

P(H=PerformanceState)=0.60, P(H=RiskLevel)=0.40

Organizational:

P(O=ReadinessLevel)=0.50, P(O=RiskExposure)=0.50

Cyber factors:

P(Cy=ResilienceLevel)=0.60, P(Cy=RiskExposure)=0.40

Коректність імовірнісного задання станів перевіряється умовою нормування:

$$\sum_{j} P(X = s_j) = 1, \tag{3.10}$$

Що в наведених даних виконується (наприклад, 0.50+0.50=1).

Ці оцінки виконують роль апріорних імовірностей для вузлів моделі і використовуються як вихідні значення при розрахунку імовірностей інцидентів.

Для демонстрації методики оцінювання використовується фрагмент причинно-наслідкової структури.:

Імовірність інцидента

У межах цього фрагмента вводяться змінні:

- V — **Visibility** (стан видимості): Favourable / Unfavourable;

- R — **Radar** (РЛС): Serviceability / Malfunction;

- E — **OperatorError** (помилка оператора): Yes / No;

- Z — **Collision** (зіткнення): Yes / No.

Залежність імовірності інциденту подається у вигляді функціонального співвідношення.

$$P(Z) = f\big(P(V), P(R), P(E)\big) \tag{3.11}$$

Однак для розрахунку необхідно конкретизувати f(·) через умовні імовірності. Згідно з базовими правилами ймовірнісного моделювання, імовірність помилки оператора визначається як повна ймовірність за станами причинних факторів:

$$P(E) = \sum_{v} \sum_{r} P(E \mid v, r)\, P(v)\, P(r). \tag{3.12}$$

Імовірність інцидента визначається через умовні імовірності при наявності/відсутності помилки:

$$P(Z) = P(Z \mid E)\, P(E) + P(Z \mid \overline{E})\, P(\overline{E}) \tag{3.13}$$

Таким чином, для виконання розрахунку необхідно задати:

- апріорні ймовірності P(V), P(R);

- таблицю умовних імовірностей P(E|V,R)

- таблицю P(Z|E).

Апріорні ймовірності приймаються з експертних даних як:

$$P(V = \text{Unfavourable}) = 0.50, \quad P(V = \text{Favourable}) = 0.50,$$

$$P(R = \text{Malfunction}) = 0.50, \quad P(R = \text{Serviceability}) = 0.50.$$

Далі формується таблиця P(E|V,R). Для практичної реалізації (з урахуванням логіки предметної області: погана видимість та відмова РЛС підвищують ризик помилки) приймаємо такі значення:

$$P(E{=}1 \mid V{=}\text{Favourable}, R{=}\text{Serviceability}) = 0.02,$$
$$P(E{=}1 \mid V{=}\text{Unfavourable}, R{=}\text{Serviceability}) = 0.10,$$
$$P(E{=}1 \mid V{=}\text{Favourable}, R{=}\text{Malfunction}) = 0.08,$$
$$P(E{=}1 \mid V{=}\text{Unfavourable}, R{=}\text{Malfunction}) = 0.25.$$

Формула P(Z|E) задає ризик зіткнення за умови помилки оператора. Приймаємо:

$$P(Z{=}1 \mid E{=}1) = 0.15, \qquad P(Z{=}1 \mid E{=}0) = 0.01. \tag{3.14}$$

Формування інтегральної оцінки ризику об’єкта.

Для узагальнення результатів оцінювання використовується інтегральний показник ризику. У роботі інтегральний ризик формується як зважена сума часткових оцінок:

Наведені вище співвідношення утворюють математичну модель оцінювання залежності взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту, яка поєднує експертні оцінки з імовірнісним апаратом та дозволяє перейти від окремих факторів до інтегрального показника ризику.

$$R = \sum_i \omega_i \cdot Risk_i, \tag{3.15}$$

Де: Risk(i)— частковий ризик, пов’язаний із і-м фактором/групою факторів, ωі— ваговий коефіцієнт значущості (визначений експертно або прийнятий згідно пріоритетів об’єкта).

Інтегральний показник R використовується для порівняння сценаріїв функціонування об’єкта та оцінювання ефективності контрзаходів: зменшення R інтерпретується як підвищення загального рівня захищеності об’єкта водного транспорту.

3.3. Розробка та дослідження реляційної моделі оцінки взаємовпливу факторів вразливостей на захищеність об’єкту водного транспорту.

Після аналізу і вивчення факторів була побудована графічна реляційна модель

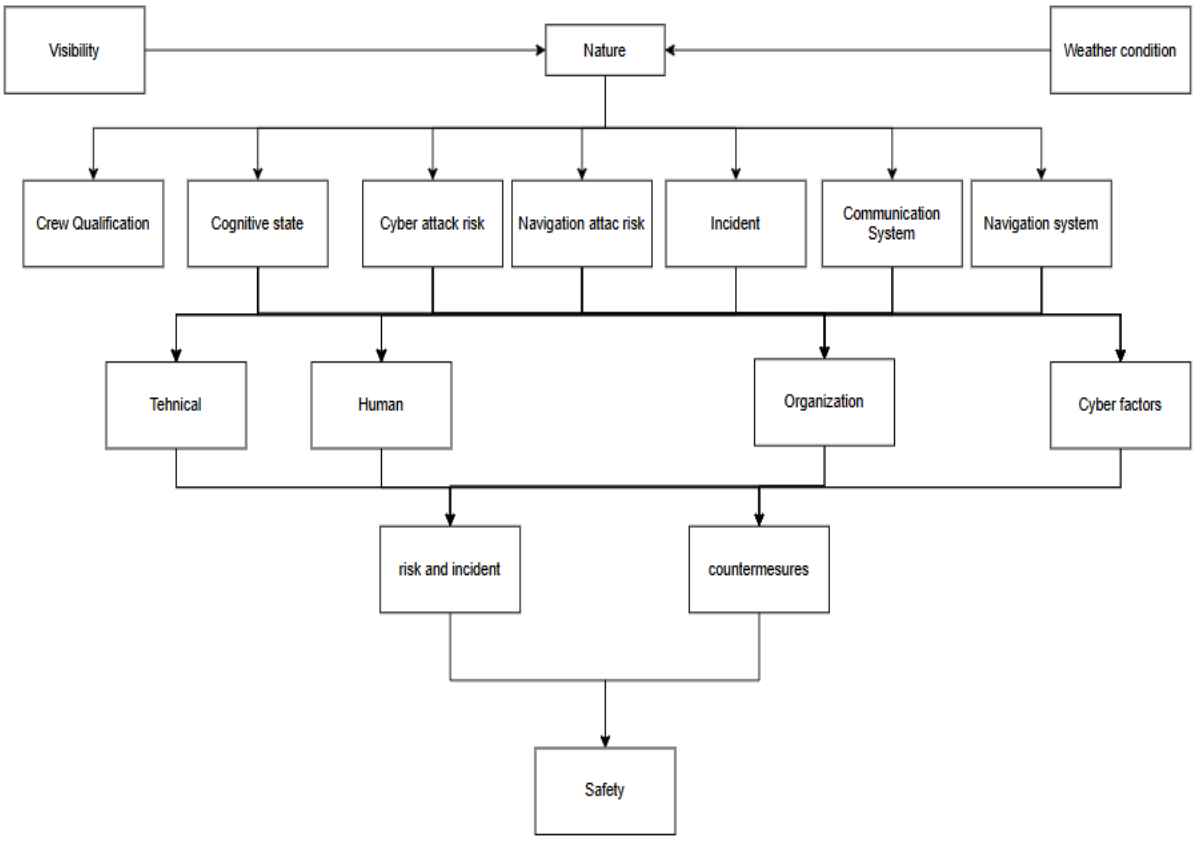

Рисунок 3.3 – Графічна Реляційна модель взаємовпливу факторів на об’єкт морського транспорту

Інформаційна модель безпеки базується на взаємодії природних умов, технічних, людських, організаційних та кіберфакторів, що формують сукупний ризик інцидентів.

Згідно з інформаційно-логічною моделлю взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту (рис. 3.3), для оцінювання та корекції рівня його захищеності розроблено Байєсівську мережу довіри (БМД), спрощена структура якої наведена на рисунку 3.1.

На сучасному етапі одним із найбільш ефективних інструментів аналізу складних систем у умовах неповної, неточної та суперечливої інформації є саме Байєсівські мережі довіри. Вони базуються на ймовірнісному підході та дозволяють максимально повно використовувати інформацію, що надходить з різнорідних джерел, для оцінювання стану захищеності об’єкта водного транспорту та прогнозування можливих інцидентів.

Байєсівські мережі являють собою графові моделі імовірнісних і причинно-наслідкових зв’язків між змінними, які використовуються у статистичному та інформаційному моделюванні. У таких мережах органічно поєднуються емпіричні дані щодо частоти реалізації подій, експертні оцінки очікуваних станів системи та теоретичні уявлення про ймовірності наслідків на основі апріорної інформації. Це є суттєвою практичною перевагою БМД і відрізняє їх від інших методів моделювання взаємовпливу факторів вразливостей.

Повна спільна ймовірність Байєсівської мережі довіри визначається за співвідношенням:

$$P_B(X^{(1)},\ldots,X^{(N)}) = \prod_{i=1}^{N} P_A\left(X^{(i)}\right) \tag{3.16}$$

Де: A – Безліч станів середовища; N=(x1,….,xn) – вектор параметрів їх розподілів

Умовна ймовірність події визначається співвідношенням:

$$p(E|H_k) = \frac{p(E \cap H_k)}{p(H_k)} \tag{3.17}$$

Де: E й H_k – зв'язані між собою змінні. Ця залежність дозволяє визначити, яка буде ймовірність події E, якщо має місце конкретна подія H_k.

Взаємовиключні події формують вичерпну безліч, якщо

$$\bigcup_{i=1}^{n} E_i = \Omega \tag{3.18}$$

Дві змінні не перетинаються, якщо вони не мають однакових значень. Теорія побудови мереж Байеса ґрунтується на припущенні, що події є вичерпними і не перетинаються. У цьому випадку ймовірність події E можна обчислити за допомогою умовних імовірностей:

$$p(E) = \sum_{i=1}^{n} p(E \cap H_i) = \sum_{i=1}^{n} p(E|H_i) \cdot p(H_i) \tag{3.19}$$

Використовуючи формулу (3.19), імовірність перетинання подій E і H

можна виразити в такий спосіб:

$$p(E \cap H_k) = p(E|H_k) \cdot p(H_k) = p(H_k|E) \cdot p(E) \tag{3.20}$$

Звідки одержуємо:

$$p(H_k|E) = \frac{p(E|H_k) \cdot p(H_k)}{p(E)} \tag{3.21}$$

З урахуванням формули (3.20) і (3.21) можна представити так:

$$p(H_k \mid E) = \frac{p(E \mid H_k) \cdot p(H_k)}{\sum_{i=1}^{n} p(E \mid H_i) \cdot p(H_i)} \tag{3.22}$$

Оскільки значна частина факторів вразливостей об’єкта водного транспорту має якісний характер та не може бути однозначно описана на основі статистичних даних, у роботі було застосовано метод експертних оцінок. Залучення експертів предметної області дозволяє формалізувати знання та практичний досвід фахівців щодо впливу природних, технічних, організаційних, кібернетичних і людських факторів на рівень захищеності об’єкта.

Експертні оцінки використовувалися для визначення початкових імовірнісних характеристик станів вершин байєсівської мережі довіри, що надалі слугують вхідними даними для побудови та дослідження моделі. Оцінювання здійснювалося групою з п’яти експертів, кожен з яких незалежно визначав імовірності можливих станів відповідних факторів. Для підвищення об’єктивності результатів підсумкове значення для кожного стану визначалося як середнє арифметичне експертних оцінок.

Результати експертного оцінювання для всіх вершин байєсівської мережі довіри наведено у таблиці 3.2.

Таблиця 3.2 – Результати експертного оцінювання станів вершин байєсівської мережі довіри для об’єкта водного транспорту

Вузол	Стан	E 1	E 2	E 3	E 4	E5	Сер.
Visibility	normal	0.46	0.48	0.50	0.52	0.54	0.50
Visibility	limited	0.26	0.28	0.30	0.32	0.34	0.30
Visibility	very_low	0.16	0.18	0.20	0.22	0.24	0.20
WeatherConditions	favorable	0.46	0.48	0.50	0.52	0.54	0.50
WeatherConditions	difficult	0.26	0.28	0.30	0.32	0.34	0.30
WeatherConditions	extreme	0.16	0.18	0.20	0.22	0.24	0.20
CrewQualification	high	0.66	0.68	0.70	0.72	0.74	0.70
CrewQualification	medium	0.16	0.18	0.20	0.22	0.24	0.20
CrewQualification	low	0.06	0.08	0.10	0.12	0.14	0.10
Cognitive state	high	0.61	0.63	0.65	0.67	0.69	0.65
Cognitive state	medium	0.21	0.23	0.25	0.27	0.29	0.25
Cognitive state	low	0.06	0.08	0.10	0.12	0.14	0.10
CyberAttackRisk	low	0.51	0.53	0.55	0.57	0.59	0.55
CyberAttackRisk	medium	0.26	0.28	0.30	0.32	0.34	0.30
CyberAttackRisk	high	0.11	0.13	0.15	0.17	0.19	0.15
Natural	favourable	0.46	0.48	0.50	0.52	0.54	0.50
Natural	unfavourable	0.46	0.48	0.50	0.52	0.54	0.50
NavigationErrorRisk	low	0.11	0.13	0.15	0.17	0.19	0.15
NavigationErrorRisk	medium	0.26	0.28	0.30	0.32	0.34	0.30
NavigationErrorRisk	high	0.51	0.53	0.55	0.57	0.59	0.55
Incident	none	0.06	0.08	0.10	0.12	0.14	0.10
Incident	minor	0.16	0.18	0.20	0.22	0.24	0.20
Incident	serious	0.26	0.28	0.30	0.32	0.34	0.30
Incident	catastrophic	0.36	0.38	0.40	0.42	0.44	0.40
CommSystemState	stable	0.11	0.13	0.15	0.17	0.19	0.15
CommSystemState	interference	0.26	0.28	0.30	0.32	0.34	0.30
CommSystemState	failure	0.51	0.53	0.55	0.57	0.59	0.55
NavSystemsState	normal	0.51	0.53	0.55	0.57	0.59	0.55
NavSystemsState	partial_failure	0.31	0.33	0.35	0.37	0.39	0.35
NavSystemsState	failure	0.06	0.08	0.10	0.12	0.14	0.10
Technical	Serviceability	0.52	0.54	0.56	0.58	0.60	0.56
Technical	Malfunction	0.40	0.42	0.44	0.46	0.48	0.44
Human	Performance	0.49	0.51	0.53	0.55	0.57	0.53
Human	RiskLevel	0.43	0.45	0.47	0.49	0.51	0.47
Organizational	ReadinessLevel	0.48	0.50	0.52	0.54	0.56	0.52
Organizational	RiskExposure	0.44	0.46	0.48	0.50	0.52	0.48
Cyber factors	ResilienceLevel	0.47	0.49	0.51	0.53	0.55	0.51
Cyber factors	RiskExposure	0.45	0.47	0.49	0.51	0.53	0.49
risks and incidents	SeverityLevel	0.65	0.67	0.69	0.71	0.73	0.69
risks and incidents	RiskLevel	0.27	0.29	0.31	0.33	0.35	0.31
Countermeasures	CapabilityLevel	0.54	0.56	0.58	0.60	0.62	0.58
Countermeasures	Effectiveness	0.38	0.40	0.42	0.44	0.46	0.42
Safety	SafetyIndex	0.68	0.70	0.72	0.74	0.76	0.72
Safety	ResilienceLevel	0.24	0.26	0.28	0.30	0.32	0.28

Графічна Реляційна модель була побудована у середовищі GeNIe.

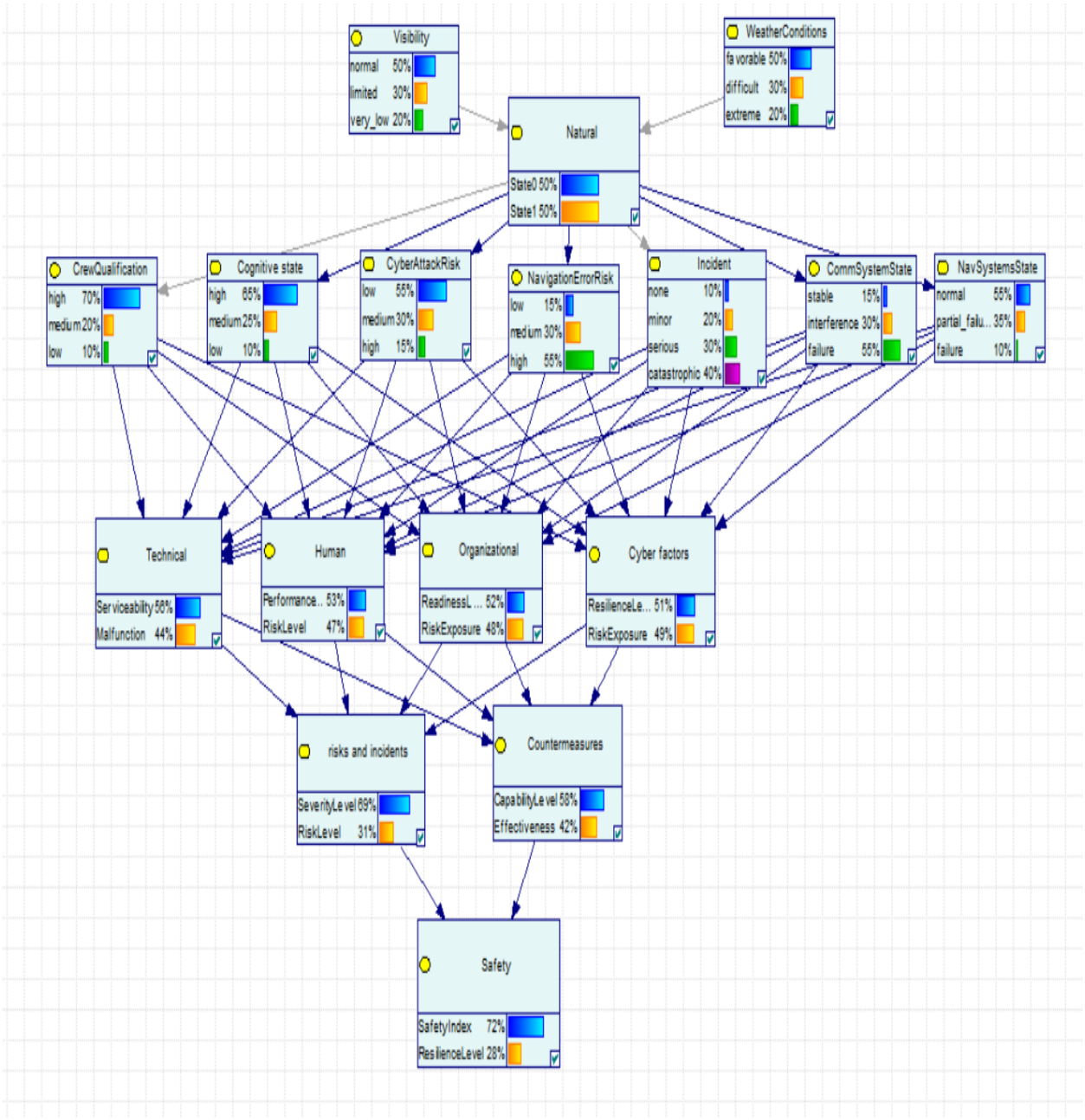

Рисунок 3.5 – Реляційна модель взаємодії факторів на об’єкт морського транспорту побудована в середовищі GeNIe на основі експертних оцінок.

Для відображення цієї структури у реляційній моделі застосовано такі основні сутності:

Основні таблиці:

- Nature – зовнішні умови впливу (погодні умови, видимість, навігаційна обстановка).

- VulnerabilityFactor – фактори вразливостей, згруповані згідно моделі:

-Technical (технічний стан систем та обладнання),

-Human (кваліфікація та когнітивний стан екіпажу),

-Organizational (процедури, управління, комунікації),

-Cyber (ризики кібератак, вразливості IT/ІКС систем),

-Natural (природні фактори: туман, вітер тощо).

- Incident – інциденти та небезпечні події.

- Threat – загрози, що виникають внаслідок сукупності факторів (зіткнення, навігаційні аварії, кібератаки тощо).

Control – контрзаходи (технічні, організаційні, кіберзахист, людський фактор).

- Safety – захищеність об’єкту критичної морської інфраструктури.

Зв’язкові таблиці (багато-до-багатьох):

- Environment_VF – вплив природних умов на фактори вразливості.

- Asset_VF – відповідність факторів конкретним активам.

- Threat_VF – сила впливу факторів на загрози.

- Control_VF – відповідність контрзаходів факторам.

Таким чином, реляційна модель відтворює логіку наданої ієрархії: середовище → фактори → ризики/загрози → інциденти → контрзаходи → безпека.

3.4 Практична реалізація моделі.

Практична реалізація реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту була спрямована на перевірку її працездатності, адекватності та можливостей використання для аналізу реальних експлуатаційних ситуацій. Реалізація моделі здійснювалася шляхом формалізованого опису факторів вразливостей, зовнішніх умов, людського фактору та контрзаходів у вигляді взаємопов’язаних сутностей

реляційної структури з подальшим обчисленням інтегрального показника захищеності.

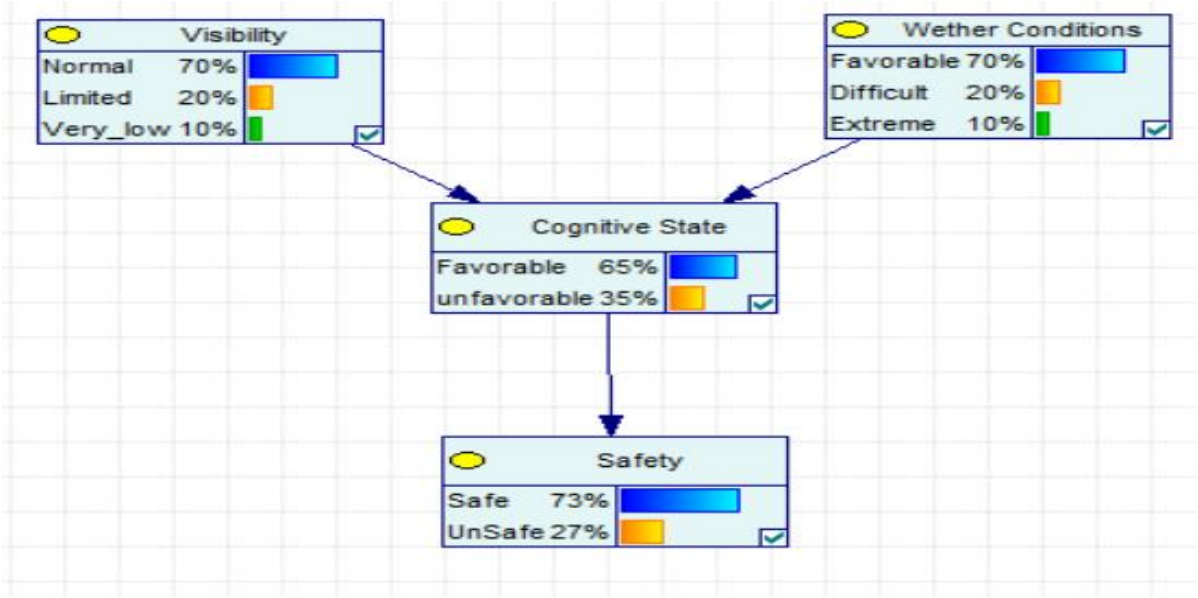

Рисунок 3.5 -Реляційна модель взаємодії факторів на об’єкт морського транспорту побудована в середовищі GeNIe для експеремента без змін.

Для експеримента було вибрано декілька факторів для перевірки зміни захищеності при зміні деяких факторів вразливостей. На рис.(3.5) приведено модель без змін.

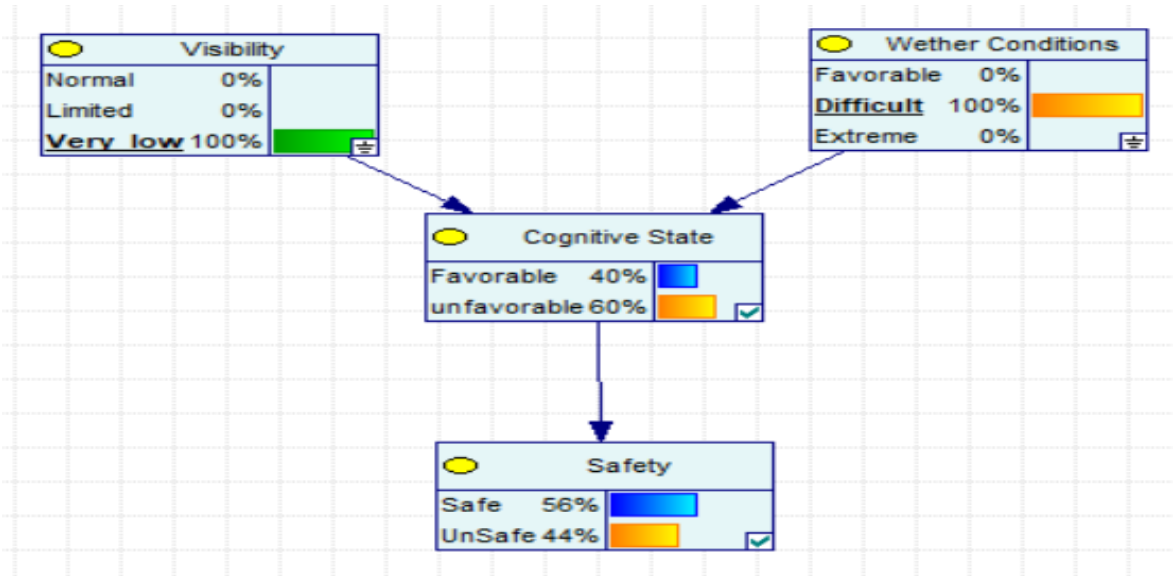

Рисунок 3.6- -Реляційна модель взаємодії факторів на об’єкт морського транспорту побудована в середовищі GeNIe для експеремента з наведенням змін в параметрах.

На рис.(3.6) було вказано такі параметри як, Видимість=дуже низька, Погодні умови=скрутні.

Сукупний ризик загрози формується за схемою моделі: природні фактори →технічні + людські + ризики та інциденти → вплив на безпеку.

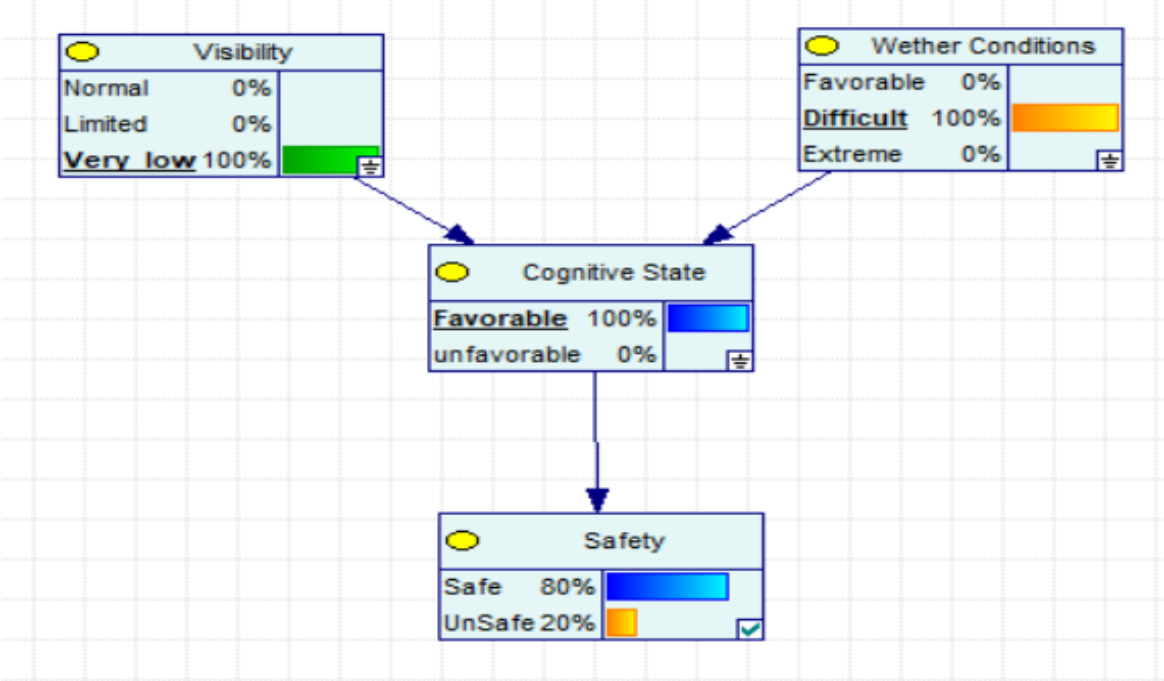

Рисунок 3.7 – Перший сценарій.

У межах першого сценарію практичної реалізації було розглянуто ситуацію, що характеризується значним негативним впливом зовнішніх умов. Зокрема, вихідні параметри відповідали дуже низькому рівню видимості та складним погодним умовам, які традиційно розглядаються як чинники підвищеного ризику для об’єктів водного транспорту. Такі умови, за відсутності компенсуючих факторів, призводять до суттєвого зниження рівня захищеності та зростання ймовірності аварійних ситуацій.

Разом із тим у даному сценарії було враховано високий рівень когнітивного стану людини-оператора, який відображає підвищену концентрацію уваги, адекватне сприйняття обстановки, швидкість прийняття рішень та здатність до прогнозування розвитку ситуації. У межах реляційної моделі цей фактор було пов’язано з іншими сутностями через відповідні

відношення, що дозволило формалізувати його компенсуючий вплив на негативні зовнішні умови. Результати моделювання показали, що навіть за несприятливих погодних факторів інтегральний рівень захищеності об’єкта водного транспорту у даному випадку виявився вищим порівняно з базовим сценарієм, у якому людський фактор не мав достатнього позитивного впливу.

Отриманий результат підтвердив важливість урахування людського фактору як одного з ключових елементів системи захищеності. Практична реалізація моделі продемонструвала, що високий когнітивний стан оператора здатний істотно зменшувати негативний ефект зовнішніх факторів та вразливостей технічного характеру. Це свідчить про доцільність інтеграції показників, що характеризують підготовку, психофізіологічний стан та когнітивні можливості персоналу, до моделей оцінювання захищеності об’єктів водного транспорту.

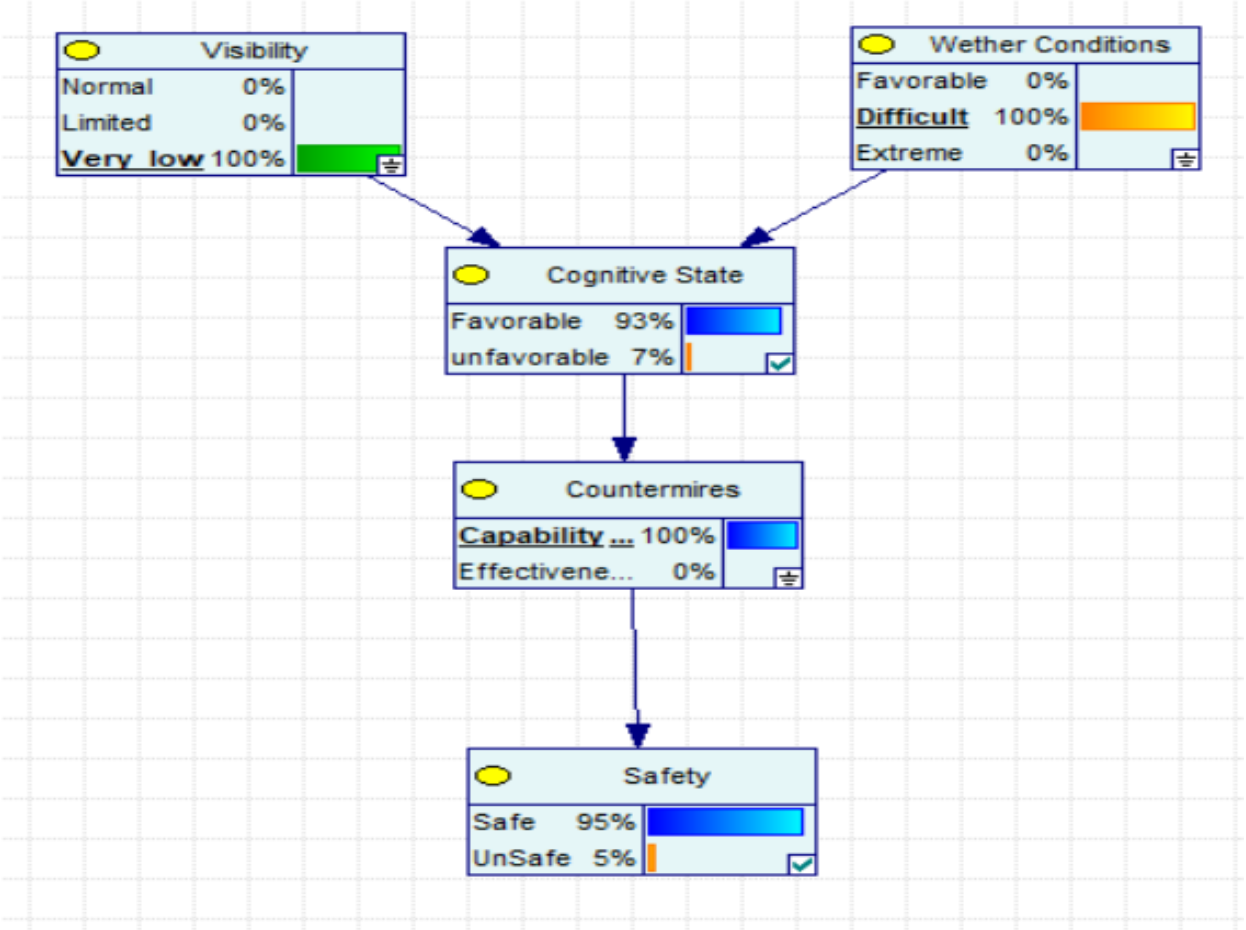

Рисунок 3.8 – Другий сценарій.

У другому сценарії практичної реалізації реляційної моделі було змодельовано вплив впровадження контрзаходів, спрямованих на зниження рівня вразливостей та підвищення загальної захищеності об’єкта. Контрміри розглядалися як окрема група сутностей реляційної моделі, пов’язаних з факторами вразливостей та ризиків через відношення, що відображають їх стримувальний або компенсуючий характер. Це дозволило формалізувати вплив контрзаходів не ізольовано, а у взаємозв’язку з усією системою факторів.

Результати моделювання другого сценарію засвідчили, що введення ефективних контрзаходів призводить до суттєвого зниження інтегрального ризику та формування дуже високого рівня захищеності об’єкта водного транспорту. При цьому позитивний ефект був досягнутий навіть за наявності несприятливих зовнішніх умов, що свідчить про здатність системи протидії компенсувати вплив критичних факторів вразливостей. Практична реалізація моделі показала, що саме комплексний характер контрзаходів, а не окремі ізольовані рішення, є визначальним для досягнення високого рівня захищеності.

Порівняльний аналіз двох розглянутих сценаріїв дозволяє зробити висновок, що реляційна модель забезпечує адекватне відображення взаємовпливу факторів вразливостей, людського фактору та контрзаходів. У першому випадку модель продемонструвала здатність виявляти компенсуючий ефект високого когнітивного стану оператора, тоді як у другому – ефективність системних контрзаходів у формуванні максимально можливого рівня захищеності об’єкта.

Таким чином, практична реалізація реляційної моделі підтвердила її придатність для оцінювання захищеності об’єктів водного транспорту в умовах різної комбінації факторів. Модель дозволяє не лише оцінювати поточний рівень захищеності, але й аналізувати альтернативні сценарії, визначати критичні фактори та обґрунтовувати вибір заходів щодо підвищення безпеки.

Отримані результати свідчать про те, що запропонований підхід може бути використаний як інструмент підтримки прийняття рішень у сфері

забезпечення захищеності об’єктів водного транспорту та має потенціал для подальшого розвитку й практичного впровадження.

Висновки до розділу 3

У третьому розділі магістерської кваліфікаційної роботи було реалізовано практичну частину дослідження, спрямовану на побудову, формалізацію та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту. Основною метою даного розділу було створення науково обґрунтованої інформаційно-аналітичної основи для оцінювання рівня захищеності об’єкта в умовах багатофакторності, невизначеності та складної структури взаємозв’язків між факторами ризику. Всі завдання було виконано, реляційна модель побудована та протестована.

ВИСНОВКИ

У магістерській роботі вирішено актуальне науково-практичне завдання побудови та дослідження реляційної моделі взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту. Актуальність дослідження зумовлена зростанням складності функціонування об’єктів водного транспорту, підвищенням ролі технічних, інформаційних і людських чинників у формуванні ризиків, а також необхідністю формалізованого оцінювання рівня захищеності в умовах невизначеності.

У процесі виконання роботи виконано всі поставлені завдання. Проведено аналіз сучасних методів і способів побудови реляційних моделей взаємовпливу факторів вразливостей, за результатами якого встановлено обмеженість традиційних підходів та обґрунтовано доцільність застосування реляційного підходу для формалізації взаємозв’язків між факторами різної природи. Розроблено математичну модель оцінювання залежності взаємовпливу факторів вразливостей на захищеність об’єкта водного транспорту, що базується на реляційному поданні сутностей і відношень та дозволяє формувати інтегральний показник захищеності з урахуванням умовних залежностей. Проведено експерименти з оцінки впливу факторів вразливостей на об’єкт критичної інфраструктури водного транспорту, які підтвердили адекватність і практичну придатність розробленої моделі для аналізу різних сценаріїв функціонування.

Отримані результати забезпечують можливість узагальненої оцінки захищеності, порівняльного аналізу сценаріїв та підтримки прийняття управлінських рішень у сфері безпеки водного транспорту. Запропонована реляційна модель є універсальною та може бути адаптована для використання на інших об’єктах критичної інфраструктури, що визначає практичну значущість виконаного дослідження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. International Maritime Organization. International Ship and Port Facility Security (ISPS) Code. IMO Publishing, London, 2018. Форма доступу - https://www.imo.org/en/OurWork/Security/Pages/ISPSCode.aspx

2. International Maritime Organization. International Convention for the Safety of Life at Sea (SOLAS), Consolidated Edition. IMO Publishing, London, 2020. Форма доступу -: https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS).aspx

3. International Maritime Organization. Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). IMO, London, 2017. Форма доступу - https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

4. European Union. Directive (EU) 2022/2557 on the Resilience of Critical Entities (CER Directive). Official Journal of the European Union, Brussels, 2022.\ Форма доступу - https://eur-lex.europa.eu/eli/dir/2022/2557/oj

5. Верховна Рада України. Закон України «Про критичну нфраструктуру» №1882-IX від 15.10.2021. Форма доступу - https://zakon.rada.gov.ua/laws/show/1882-20

6. Верховна Рада України. Закон України «Про транспорт». Відомості Верховної Ради України, Київ, 1994. Форма доступу - https://zakon.rada.gov.ua/laws/show/232/94-%D0%B2%D1%80

7. Міністерство інфраструктури України. Морська безпека та охорона портів. Офіційні матеріали, Київ, 2022. Форма доступу - https://mtu.gov.ua

8. Державна служба спеціального зв’язку та захисту інформації України. Кіберзахист критичної інфраструктури України: методичні рекомендації. Київ, 2021. Форма доступу - https://cip.gov.ua/ua

9. CERT-UA. Аналітика кіберзагроз для транспортного сектору України. Київ, 2022.
Форма доступу - https://cert.gov.ua

10. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity (CSF), Version 1.1. NIST, 2018. Форма доступу - https://www.nist.gov/cyberframework

11. National Institute of Standards and Technology. Guide for Conducting Risk Assessments (NIST SP 800-30). NIST, 2012.
Форма доступу - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

12. National Institute of Standards and Technology. Guide to Industrial Control Systems (ICS) Security (NIST SP 800-82). NIST, 2021.
Форма доступу - https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final

13. International Organization for Standardization. ISO/IEC 27001:2022 Information Security Management Systems. ISO, Geneva, 2022. Форма доступу - https://www.iso.org/standard/27001.html

14. International Organization for Standardization. ISO 28000:2007 Security Management Systems for the Supply Chain. ISO, Geneva, 2007. Форма доступу - https://www.iso.org/standard/44641.html

15. International Organization for Standardization. ISO 31000:2018 Risk Management — Guidelines. ISO, Geneva, 2018. Форма доступу - https://www.iso.org/standard/65694.html

16. Reniers G., Khakzad N. Safety and Security Science: Interlinking Risk Management in Process Industries. Springer, 2019. Форма доступу - https://link.springer.com/book/10.1007/978-3-030-00217-6

17. Zeng X., Yang Z., Oladokun M. Maritime Transport Vulnerability Assessment Using Integrated Risk Modelling. Safety Science, Elsevier, 2020. Форма доступу - https://www.sciencedirect.com/science/article/pii/S0925753520300184

18. Bichou K. Port Security Management: Technological Systems and Operational Perspectives. Taylor & Francis, 2014. Форма доступу - https://www.taylorfrancis.com/books/mono/10.4324/9781315885775

19. Ventikos N., Spanos D. Maritime Infrastructure Vulnerability and Risk Assessment. Journal of Marine Engineering & Technology, 2019. Форма доступу - https://www.tandfonline.com/doi/full/10.1080/20464177.2019.1583215

20. CyberRoad Project. Maritime Critical Information Infrastructure Vulnerabilities Report. EU FP7 Project, 2015. Форма доступу - https://cordis.europa.eu/project/id/653566

21. Synectics Global. Security Technologies for Offshore and Port Infrastructure. Industry Review, 2021. Форма доступу - https://www.synecticsglobal.com

22. Cambridge Pixel Ltd. Integrated Radar and Sensor Protection Systems for Maritime Infrastructure. Technical White Paper, 2020. Форма доступу - https://cambridgepixel.com

23. National Institute for Strategic Studies. Cybersecurity of Maritime Ports: Analytical Report. Kyiv, 2021. Форма доступу - https://niss.gov.ua

24. UkraineWorld. Critical Infrastructure of Ukraine: Threat Analysis. Kyiv, 2022. Форма доступу - https://ukraineworld.org

25. National Security and Defense Council of Ukraine. National System for Critical Infrastructure Protection. Kyiv, 2021. Форма доступу - https://www.rnbo.gov.ua

26. State Service of Maritime and River Transport of Ukraine. Port Security and ISPS Code Implementation. Kyiv, 2020. Форма доступу - https://marad.gov.ua

27. Adedeji O., Ajiwumi O., Daramola O. Modeling Interdependencies and Vulnerabilities in Maritime Transportation Systems. Marine Policy, Elsevier, 2021. Форма доступу - https://www.sciencedirect.com/science/article/pii/S0308597X21000447

28. U.S. Government Accountability Office. Critical Infrastructure Protection: Key Challenges. GAO Report, 2019.

Форма доступу - https://www.gao.gov/products/gao-19-332

29. Hwang J., Lee S. Relational Models for Vulnerability Factor Interaction in Maritime Safety. Journal of Transportation Security, 2020.

Форма доступу - https://link.springer.com/article/10.1007/s12198-020-00216-7

30. Holubka O., Serhiienko V. Risk and Vulnerability Modelling of Maritime Transport Systems. Bulletin of ONMU, 2021. Форма доступу - http://journals.onmu.edu.ua

31. Литвиненко А., Коваленко І. Методи оцінювання ризиків об’єктів водного транспорту. Техногенно-екологічна безпека, 2022. Форма доступу - https://teb-journal.org.ua

32. State Environmental Inspectorate of Ukraine. Prevention and Response to Marine Pollution Accidents. Kyiv, 2021. Форма доступу - https://dei.gov.ua

33. United States Coast Guard. Maritime Security Risk Analysis Model (MSRAM). Technical Documentation, 2020. Форма доступу - https://www.dco.uscg.mil/MSRAM

34. Kristensen S., Haugen S. Risk Modelling in Maritime Operations: Human, Technical and Environmental Factors. Elsevier, 2019.

Форма доступу - https://www.sciencedirect.com/book/9780128162810

35. International Maritime Organization. Maritime Safety Committee Reports on Threats and Vulnerabilities in Ports. IMO, 2020.

Форма доступу - https://www.imo.org/en/MediaCentre/MeetingSummaries/MSC