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

ДОСЛІДЖЕННЯ ФАКТОРІВ ВПЛИВУ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ НА ЗАХИЩЕНІСТЬ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ЗАСТОСУВАННЯМ ІМОВІРНІСНОГО МЕТОДУ БАЄСОВИХ МЕРЕЖ ДОВІРИ.

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
Мойсеєнко Микола Григорович _____

Кваліфікаційна робота містить результати самостійного виконання навчального завдання. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

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: Мойсеєнко Микола Григорович

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: Дослідження факторів впливу Інформаційної та кібербезпеки на захищеність об'єкту критичної інфраструктури з застосуванням імовірнісного методу Баєсових мереж довіри.

затверджена наказом НУК від «14» 10 2025 р. № 1217-г

2. Вихідні дані до роботи: Моделі та алгоритми оцінки факторів Інформаційної та кібербезпеки на ОКІ.

1.Провести аналіз сучасних методів та способів оцінки факторів Інформаційної та кібербезпеки на ОКІ.

2.Розробити інформаційно – логічну модель оцінки впливу факторів інформаційної та кібербезпеки на стан захищеності ОКІ.

3.Виконати практичну реалізацію результатів дослідження з застосуванням імовірнісного методу Баєсових мереж довіри.

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 _____ М.Г. Мойсеєнко

АНОТАЦІЯ

У магістерській роботі досліджувалась актуальна проблема залежності захищеності об’єкту критичної інфраструктури від впливу *НЕ*-факторів які характеризуються високим ступенем невизначеності, складністю строгої формалізації та мають суб’єктивний характер.

В роботі досліджені проблемні питання оцінювання стану захисту об’єктів критичної інфраструктури, проведений аналіз та визначено основні *НЕ*-фактори загроз, що впливають на захищеність об’єктів. Проведено детальний аналіз сучасних методів і способів оцінки та підтримки захищеності об’єктів критичної інфраструктури. Для визначення рівня захищеності об’єкта критичної інфраструктури від факторів Інформаційної та кібербезпеки розроблено інформаційну та інформаційно – логічну моделі для оцінювання стану безпеки з використанням імовірнісного методу Баєсовських мереж довіри. Для прогнозування рівня безпекового стану критичного об’єкту побудована нечітка База знань з застосуванням знань експертів та теорії нечітких множин. В процесі дослідження залежності захищеності об’єкту критичної інфраструктури від впливу факторів Інформаційної та кібербезпеки використовувались системний аналіз, графо-аналітичні методи Байесовської мережі довіри та теорія експертних оцінок.

Застосування сукупності теоретичних і практичних засад розробки та досліджень нададуть можливість вирішення задач з оцінювання захищеності об’єкту критичної інфраструктури, в залежності від факторів які характеризуються високим ступенем невизначеності, складністю строгої формалізації та мають суб’єктивний характер.

Ключові слова: Байєсівська мережа довіри, об’єкт критичної інфраструктури, програмне забезпечення, особа, що приймає рішення, інформаційна безпека, кібербезпека, база знань.

ABSTRACT

The master's thesis investigated the current problem of the dependence of the security of a critical infrastructure object on the influence of non-factors that are characterized by a high degree of uncertainty, the complexity of strict formalization and are subjective in nature.

The work investigated the problematic issues of assessing the state of protection of critical infrastructure objects, analyzed and identified the main non-factors of threats that affect the security of objects. A detailed analysis of modern methods and methods of assessing and maintaining the security of critical infrastructure objects was carried out. To determine the level of security of a critical infrastructure object from factors of Information and cybersecurity, an information and information-logical model was developed for assessing the state of security using the probabilistic method of Bayesian trust networks. To predict the level of security of a critical object, a fuzzy Knowledge Base was built using expert knowledge and the theory of fuzzy sets. In the process of studying the dependence of the security of a critical infrastructure object on the influence of factors of Information and Cybersecurity, system analysis, graph-analytical methods of the Bayesian trust network and the theory of expert assessments were used.

The application of a set of theoretical and practical principles of development and research will provide an opportunity to solve problems of assessing the security of a critical infrastructure object, depending on factors that are characterized by a high degree of uncertainty, the complexity of strict formalization and are subjective in nature.

Keywords: Bayesian trust network, critical infrastructure facility, software, decision maker, information security, cybersecurity, knowledge base.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

БМД – Байєсівська мережа довіри.

ОКІ – Об’єкт критичної інфраструктури;

ПЗ – програмне забезпечення;

ОПР – Особа, що приймає рішення.

ІБ – Інформаційна безпека.

КБ – Кібербезпека.

СППР – Система підтримки прийняття рішень

БЗ – База знань.

ТНМ - Теорія нечітких множин.

ЗМІСТ

ВСТУП

На сьогодні важливим фактором розвитку сучасного суспільства є забезпечення захищеності інформаційних систем, які є ключовими елементами будь-яких процесів незалежно від сфери людської діяльності.

Функціонування об’єктів критичної інформаційної інфраструктури (КІІ) в такому специфічному середовищі, як кіберпростір, пов’язане з вразливостями системи кіберзахисту і кіберзагрозами, та вимагає розробки нового інструментарію по забезпеченню їх захищеності.

Управління системою забезпечення захисту інформації критичної інфраструктури, як і у разі управління будь-якою соціально-технічною структурою, пов'язане зі значними складнощами, спричиненими неповнотою інформації, конфліктами інтересів та цілей, швидкими та численними змінами у різних галузях здійснення інформаційної боротьби за їхню потенційну безпеку. Тому методики визначення, оцінки та прийняття рішень з підвищення стану захищеності, на всіх рівнях ієрархії з управління захистом ОКІ, мають відповідати сучасним технологіям щодо оптимізації їх захисту.

Актуальність теми: На сьогодні, методи моделювання загроз та ступінь їх впливу на рівень безпеки об’єкту критичної інфраструктури, потребують складних розрахунків, наявності достатньо повної статистичної інформації, тривалого часу для опрацювання необхідних даних.

Тому, варто звернути увагу на підхід, який наддасть можливість вирішувати задачі, що не піддаються строгій формалізації, використовувати неповну, нечітку інформацію та суб’єктивні судження експертів предметної області, будувати гнучкі, конструктивні моделі, які адекватно реагують на зміни. В зв’язку з цим, даний напрям дослідження є актуальним.

Виходячи з цього, в даній роботі пропонується дослідження впливу *НЕ*-факторів Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури з застосуванням імовірнісного методу Баєсових мереж довіри

Мета дослідження. Мета магістерської роботи є дослідити вплив *НЕ*-факторів Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури з застосуванням імовірнісного методу Баєсових мереж довіри.

Завдання дослідження:

1. Провести аналіз сучасних методів та способів дослідження та оцінки факторів Інформаційної та кібербезпеки на об’єкті критичної інфраструктури.

2. Визначити особливості застосування імовірнісного методу Баєсових мереж довіри в дослідженні та оцінювані факторів впливу Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури.

3. Побудувати інформаційну модель впливу факторів інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури.

4. Визначити та провести оцінювання основних факторів впливу інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури.

5. Розробити інформаційно – логічну модель оцінки впливу факторів інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури із застосуванням імовірнісного методу Баєсових мереж довіри.

6. Виконати практичну реалізацію результатів дослідження захищеності об’єкту критичної інфраструктури із застосуванням імовірнісного методу Баєсових мереж довіри.

Об'єкт дослідження: моделі, методи і інформаційні технології оцінки та забезпечення стану захищеності ОКІ.

Предмет дослідження: сукупність теоретичних та практичних засад з використанням теорії м’яких обчислень для оцінки впливу факторів інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури.

Методи дослідження: Системний аналіз, теорія експертних оцінок, теорія нечітких множин, Байесовської мережі довіри.

Наукова новизна одержаних результатів: Побудова інформаційно – логічної моделі для оцінювання рівня захищеності об’єкту критичної

інфраструктури з використанням імовірнісного методу Баєсовських мереж довіри.

Очікуваний результат: Результати дослідження нададуть можливість вирішення задач з оцінювання захисту об’єкту критичної інфраструктури, які характеризуються високим ступенем невизначеності, складністю строгої формалізації та мають суб’єктивний характер.

Дипломна робота є самостійним дослідженням, яке включає теоретичні розділи, аналітичну частину, розробку практичних рекомендацій та оцінку їх ефективності. Робота базується на актуальних наукових публікаціях, а також даних, отриманих в результаті експертних опитувань.

1. ОСНОВНІ ОСОБЛИВОСТІ ФАКТОРІВ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Організаційно - правове забезпечення оцінювання захищеності об'єкту критичної інфраструктури.

Організаційно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури України є значущим аспектом для забезпечення безпеки та стійкості цих об'єктів перед сучасними кіберзагрозами. В Україні існують спеціальні нормативні акти, закони та положення, які регулюють захист критичної інфраструктури в кіберпросторі.

Інформаційна безпека стає все більш важливою та суттєвою сферою національної безпеки України, що відображено у Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 25 лютого 2017 року №47/2017. Відповідно до Доктрини, інформаційні технології набули глобального характеру і стали невід'ємною частиною всіх сфер діяльності держави, суспільства та особистості. З розширенням сфер застосування інформаційних технологій значно зростають і ризики нових інформаційних загроз та атак. Зарубіжні спеціальні служби використовують інформаційно психологічний вплив для дестабілізації соціальної та внутрішньо політичної ситуації в різних регіонах світу, що може призвести до порушення територіальної цілісності та підриву суверенітету інших держав. У сфері оборони держави, економіки, суспільної та державної безпеки, науки, освіти та технологій спостерігаються визначені державою стратегічні цілі для забезпечення ефективного стану безпеки конфіденційної інформації. Одночасно з розвитком інформаційних технологій зростає і кількість засобів та методів порушення безпеки конфіденційної інформації. Останні роки характеризуються різким зростанням кількості витоків конфіденційної інформації, як це видно зі звітів експертно-аналітичного центру групи компаній SafeNet. Для зміни ситуації на краще необхідно розробляти нові методи та

підходи, які можуть забезпечити надійний захист від сучасних загроз безпеці інформації. Задача забезпечення безпеки конфіденційної інформації стає найактуальнішою у зв'язку з ростом комп'ютерних атак та витоків інформації, що відображаються у статистичних даних про злочини у сфері високих технологій. У 2021 році зростання кримінальної активності з використанням SafeNet. Для зміни ситуації на краще необхідно розробляти нові методи тапідходи, які можуть забезпечити надійний захист від сучасних загроз безпеці інформації. Задача забезпечення безпеки конфіденційної інформації стає найактуальнішою у зв'язку з ростом комп'ютерних атак та витоків інформації, що відображаються у статистичних даних про злочини у сфері високих технологій. У 2021 році зростання кримінальної активності з використанням сучасних комунікаційних пристроїв та Інтернету склало 39%. Кожен двадцятий злочин кваліфікується як кіберзлочин. Лідерствують злочини, пов'язані з розповсюдженням комп'ютерних вірусів та неправомірним доступом до конфіденційної інформації. Друге місце займає шахрайство з використанням онлайн-платежів, кількість таких правопорушень у першому півріччі 2022 року зросла у 8 разів. Щорічні звіти міжнародної компанії Group-IB також відзначають активність проурядових організацій, які проводять кібератаки для досягнення своїх цілей. Для досягнення цілей забезпечення безпеки конфіденційної інформації необхідно організувати ефективне створення системи захисту інформації, моделювання актуальних загроз інформаційної безпеки, визначення актуальних порушників та проведення якісної оцінки ефективності системи захисту. Однією з найважливіших задач є оцінка ефективності системи захисту.

Наслідки кібератак можуть бути катастрофічними, тому важливо проводити регулярне оцінювання захищеності кіберпростору об’єктів критичної інфраструктури та приймати заходи для підвищення захищеності.

Це дає змогу зменшити ризики кібератак і забезпечити безпеку функціонування критичної інфраструктури.

Отже, враховуючи інформаційну війну як джерело загроз постає потреба детальніше проаналізувати загрози інформаційної безпеки для коректного розуміння можливих загроз та протидії їм.

Фактори впливу на стан кібербезпеки. Проведений аналіз існуючих систем захисту інформації [1-3], дає змогу визначити основні складові частини системи кіберзахисту інформаційних систем об’єктів критичної інфраструктури:

– нормативно-правова;

– організаційна;

– технічна;

На даний момент існує більше 30 міжнародних норм типу ISO/IEC 27000, що стосуються інформаційної безпеки,спільно опублікованих Міжнародною організацією зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC).

Зокрема:

- ISO 27001 – це світова норма,розроблена Міжнародною організацією зі стандартизації,яка визначає,як керувати інформаційною безпекою в компанії. Остання редакція цієї норми була випущенау2013 році, повна назва – ISO/IEC 27001:2013. Перша редакція норми, випущена у 2005 році, ґрунтувалася на Британському стандарті BS 7799-2;

- ISO/IEC 27004 містить настанови щодо оцінювання інформаційної безпеки. Ця норма добре взаємодіє з ISO 27001, оскільки пояснює, як з'ясувати, чи досягла система управління інформаційною безпекою своїх цілей;

-ISO/IEC27005 містить настанови для управління ризиками порушення інформаційної безпеки. Це надзвичайно корисне доповнення до стандарту ISO 27001, тому що містить подробиці того, як виконувати оцінку та обробку ризиків (а це, мабуть, найбільш складний етап впровадження). ISO 27005

виник на базі британського стандарту BS 7799-3. Також існують Українські Нормативні документи технічного захисту інформації:

- НД ТЗІ1.1-003-99

- НД ТЗІ 2.5-005-99

А також надано методологію оцінки рівня захищеності об'єктів критичної інфраструктури, закріплену Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 14 січня 2025 року N17. Ця Методологія націлена на реалізацію кроків із визначення рівня захищеності об'єктів критичної інфраструктури, а також вжитих і запланованих дій для гарантування захисту, безпеки та стійкості критичної інфраструктури [4-6].

Дані норми є обов'язковими, проте їх важливість у сучасному суспільстві важко переоцінити. По суті, вони відображають особливості поточного рівня інформаційних технологій, але не містять наскрізних шкал цінності та переліків умов безпеки систем захисту інформації, що супроводжує цим захисту критично важливих об'єктів (від методології розробки до етапу остаточної реалізації та подальшої експлуатації) бажано починати з експертної оцінки (ЕО) задіяних технічних, програмних та програмно-апаратних інструментів захисту інформації (ЗЗІ), що обслуговують ці об'єкти інфраструктури.

1.2 Напрями розвитку механізмів захисту критичної інфраструктури в Україні.

Захист критичної інфраструктури – це складне комплексне завдання для будь-якої держави, якими б великими не були її ресурси. Тому з розвитком і зростанням інформаційних технологій зростає і складність архітектури об'єктів критичної інфраструктури.

Сучасні об'єкти критичної інфраструктури. мають клієнт серверну територіально розподілену та багатокористувацьку архітектуру. Програмне забезпечення, засноване на відкритому інтерфейсі програмування, надає

можливість робити функціональні вдосконалення за допомогою поширених мов програмування (рис.1.1) [7-10].

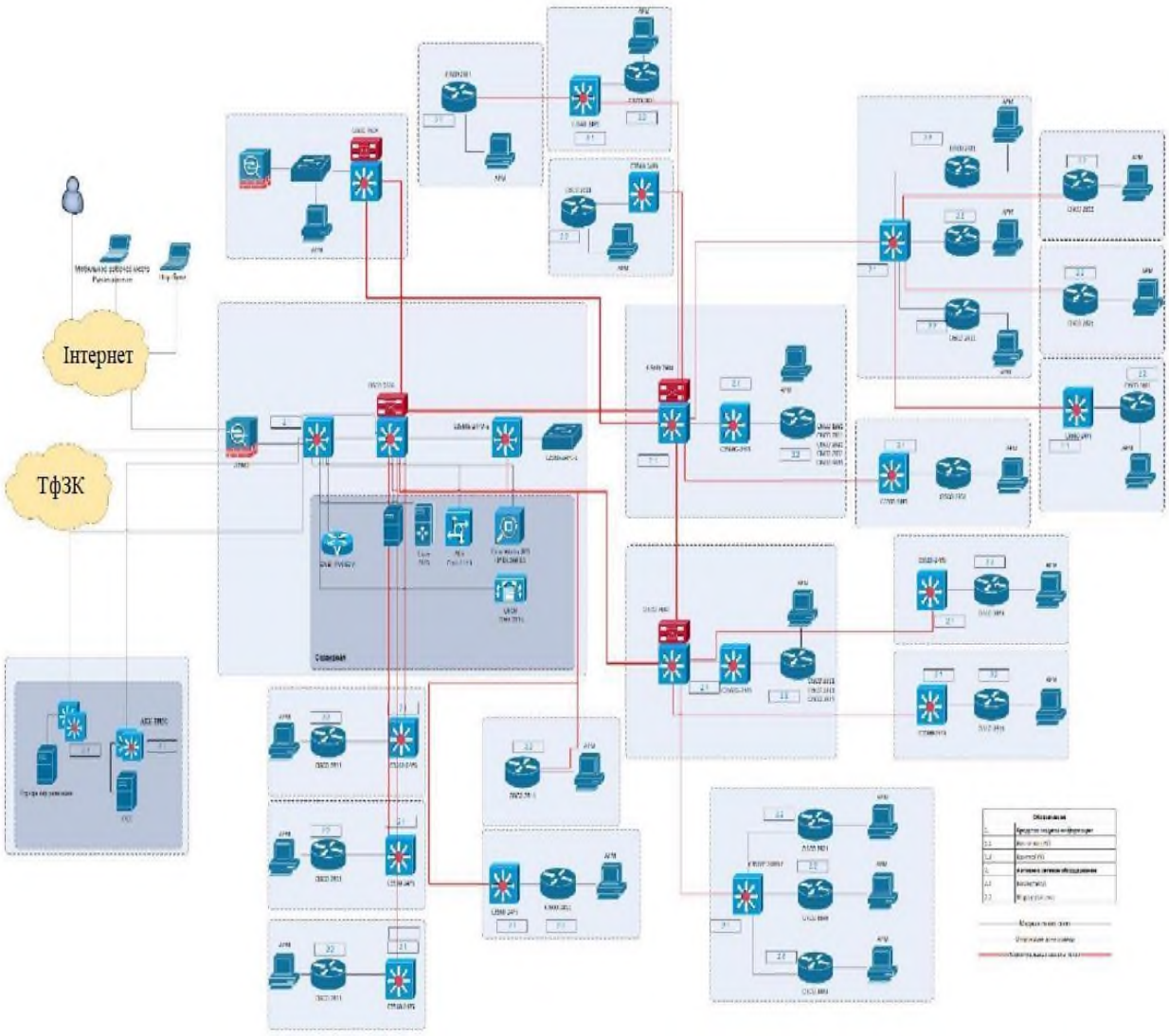

Рисунок 1.1 – Типова схема комплексу технічних засобів розподіленого об'єкту критичної інфраструктури.

Широка доступність сучасних технологій, поява нових запитів і активна позиція споживача, глобалізація ринків і скорочення ресурсів роблять питання інформаційної безпеки пріоритетними. З такої позиції сутнісні характеристики категорії «безпека» складають поняття «протиріччя», «стан», «загроза» Погляд на причину загрози безпеці розвитку через виникнення та загострення

протиріч визначає необхідність вивчення та виділення об’єктів загроз, що проявляються у конфліктах, кризових станах й ситуаціях, катастрофах При цьому слід враховувати інформаційні, людські, організаційні та техніко-технологічні можливості, що забезпечують умови економічної безпеки - стійку реалізацію цілей розвитку через здатність вирішувати протиріччя, передбачувати, оцінювати та активно протистояти загрозам (табл.1.1).

Таблиця 1.1 - Актуальні загрози критично-важливих об’єктів.

Загроза	**Пояснення**
Несанкціоноване використання точок доступу для віддаленого обслуговування	Пункти доступу для технічного обслуговування це спеціально створені зовнішні входи у мережу ІКТ, які часто недостатньо захищені
Мережеві атаки через офісні чи корпоративні мережі	Офісні ІТ зазвичай пов'язані із мережею декількома шляхами. У більшості випадків мережеві з'єднання з офісів у мережу ІКТ також існують, тому зловмисники можуть отримати доступ до цього маршруту
Атаки на стандартні компоненти, що використовуються в мережі КВО	Стандартні ІТ-компоненти (COTS), як-от системне програмне забезпечення, сервери додатків або бази даних, часто містять недоліки чи вразливості, які можуть бути використані зловмисниками. Якщо такі стандартні компоненти також застосовують у мережі ІКТ, небезпека успішної атаки на мережу ІКТ зростає.
Атаки типу "відмова в обслуговуванні"	(Розподілені) атаки типу "відмова в обслуговуванні" можуть послабити мережеві з'єднання та найважливіші ресурси та призвести до відмови систем, наприклад, для порушення роботи ІКТ
Людська помилка або саботаж	Умисні дії, що здійснюються як внутрішніми, так і зовнішніми зловмисниками, є серйозною небезпекою для усіх цілей захисту. Недбалість і людська помилка також є великою загрозою, особливо щодо конфіденційності та доступності цілей захисту
Впровадження шкідливого ПЗ через знімні носії та зовнішнє обладнання	Використання знімних носіїв та мобільних ІТ-компонентів зовнішнього персоналу завжди тягне за собою великий ризик зараження шкідливим ПЗ
Читання та опублікування новин у мережі ІКТ	Більшість компонентів управління нині використовують протоколи з відкритим текстом, тому зв'язок не захищений. Це дозволяє відносно легко читати та вводити команди управління

Несанкціонований доступ до ресурсів	Внутрішні зловмисники та наступні атаки після первинного зовнішнього проникнення роблять це особливо простим, якщо служби та компоненти у мережі процесів не використовують методи автентифікації та авторизації або якщо ці методи є небезпечними
Атаки на мережеві компоненти	Зловмисники можуть маніпулювати мережевими компонентами, наприклад, для проведення атак «зловмисник усередині» або для полегшення прослуховування
Технічні несправності або форс-мажорні обставини	Перебої, спричинені екстремальною погодою або технічними несправностями, можуть статися у будь-який час - ризик і потенційні збитки можуть бути зведені до мінімуму тільки в момент виникнення таких випадків

На основі аналізу досвіду провідних країн світу щодо захисту критичних інфраструктур, які застосовуються в ЄС з одного боку, а також аналізу положення щодо захисту таких інфраструктур в Україні, з іншого боку, запропоновано наступні ключові напрями розвитку механізмів захисту критичної інфраструктури [8]:

–вдосконалення нормативно-правових та організаційних механізмів захисту критичної інфраструктури;

– визначення пріоритетних секторів критичної інфраструктури та органів державної влади, які відповідають за формування та реалізацію державної політики щодо забезпечення захисту відповідних об'єктів критичної інфраструктури.

–розробка та затвердження критеріїв та методології віднесення об'єктів (незалежно від їх форми власності) до переліку критичної інфраструктури;

–вдосконалення системи моніторингу стану об’єктів критичної інфраструктури, аналізу та прогнозування загроз критичній інфраструктурі, визначення шляхів та засобів зменшення ризиків, пов'язаних з функціонуванням критичної інфраструктури та запобігання виникненню на них надзвичайних ситуацій;

–вдосконалення механізмів державно-приватного партнерства;

– впровадження інноваційних розробок та вдосконалення існуючих засобів забезпечення безпеки та захисту об’єктів критичної інфраструктури;

–розробка та впровадження стандартів, правил, технічних умов захищеності об'єктів критичної інфраструктури;

–покращення систем та режимів охорони об’єктів критичної інфраструктури;

– залучення експертного співтовариства громадськості, поширення інформації та передових досягнень, підготовка кадрів, проведення 17 тренувань та навчань;

– усунення джерел загроз, зменшення рівня загроз шляхом застосування комплексних безпекових заходів (наприклад, в рамках протидії тероризму);

– розвиток міжнародної співпраці з питань захисту критичної інфраструктури

1.3 Основні особливості методів і засобів дослідження та оцінювання захищеності об’єкту критичної інфраструктури.

Наслідки кібератак можуть бути руйнівними, тому важливо проводити регулярне оцінювання захищеності кіберпростору установ критичної інфраструктури та вживати заходів для її укріплення.

Виконання цієї процедури вимагає вирішення наступних завдань: збір інформації про компоненти ОКІ; обробка цієї інформації і побудова прийнятної моделі на основі отриманих результатів для подальшого використання при оцінці ризиків. В свою чергу забезпечення безпечного функціонування ОКІ представляє собою безперервний процес прийняття рішення з оцінювання стану безпеки об’єкту критичної інфраструктури, ефективності реалізованих засобів захисту та впливу дестабілізуючих факторів [11-14].

Вважається, що основою забезпечення безпеки об’єкту критичної інфраструктури є три складові у вигляді конфіденційності, цілісності, доступності, а процес успішного захисту залежить від рівня розвитку

апаратного забезпечення, програмного забезпечення та рівня комунікації (забезпечення зв'язку). Використані процедури (механізми) захисту від потенційних загроз поділяють на фізичний рівень захисту, на рівень захисту персоналу та організаційний рівень, а саме поняття «інформаційна безпека» вводять з погляду або діяльності, спрямованої на забезпечення захищеного стану об'єкта, або стану певного об'єкта (інформація, дані, ресурси, автоматизованої системи, інформаційна система підприємства, суспільства, держави тощо) [9,10].

Регулярне дослідження та оцінювання захищеності об’єкту критичної інфраструктури дасть змогу знівелювати загрози кібератак та гарантувати безпечне функціонування важливої інфраструктури.

Головні аспекти дослідження впливу інформаційної та кібербезпеки на критичну інфраструктуру містять: системний підхід до з'ясування зв'язків між кіберзагрозами та функціональною стійкістю, оцінка вразливостей комунікаційних та технологічних систем, комп'ютерне моделювання наслідків кібератак для життєво значущих послуг, формування та втілення комплексних засобів захисту згідно з державними стандартами та передовими практиками, а також визначення ступеня важливості об'єкта для першочергового виконання заходів безпеки.

Математичні апарати для визначення стану захищеності об'єктів критичної інфраструктури (ОКІ) охоплюють методи аналізу загроз, моделювання, теорії стійкості, теорії ігор, а також методи оцінки вразливостей та аналітики кібербезпеки. Ці методи сприяють виявленню слабких ланок, прогнозуванню результатів атак та оптимізації дій захисту, беручи до уваги як фізичні, так і цифрові аспекти (рис. 1.2)

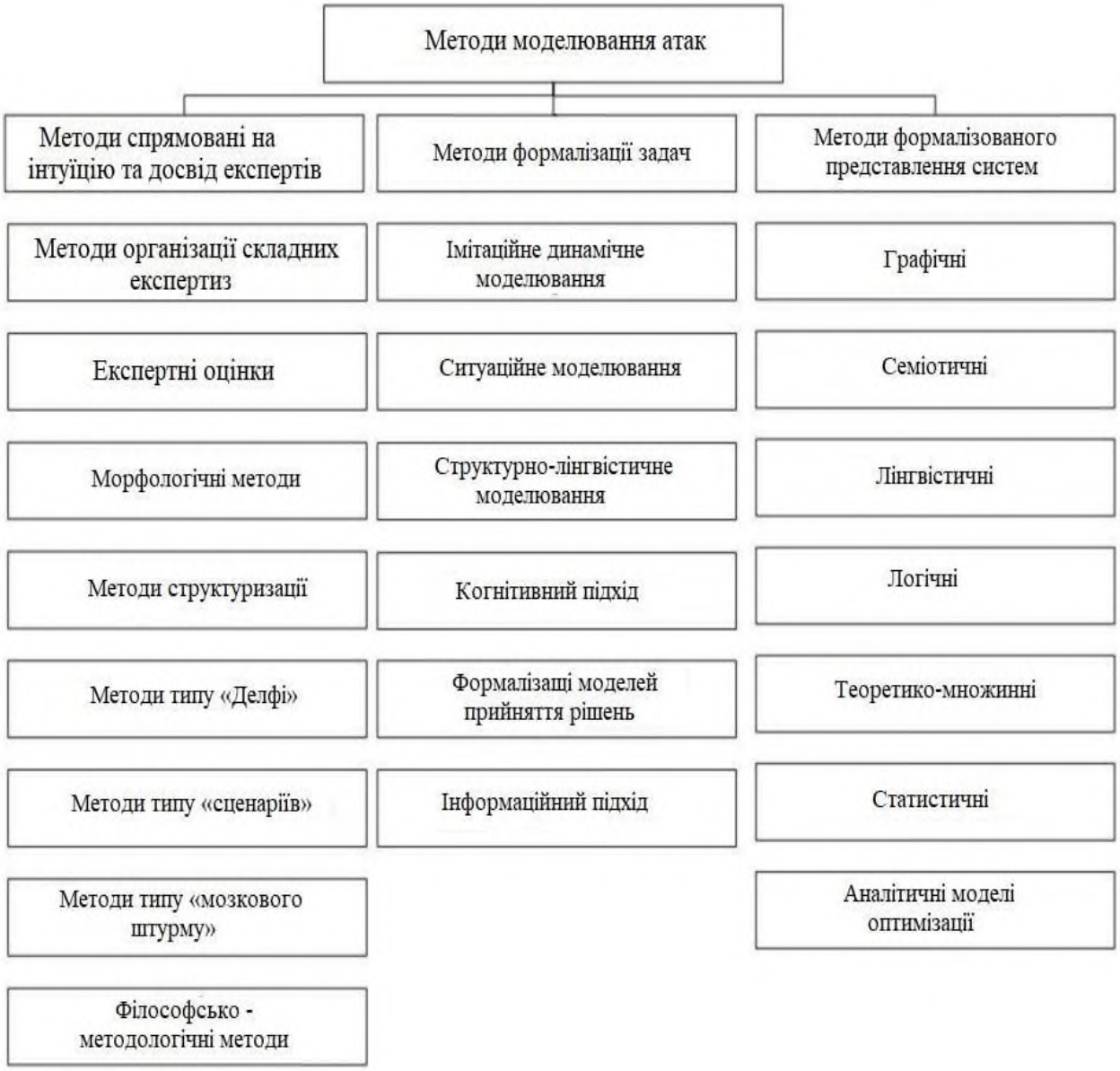

Рисунок 1.2 - Математичні апарати для визначення стану захищеності об'єктів критичної інфраструктури.

Головні чинники дослідження:

• Комплексний підхід: Важливо розуміти взаємозв'язок між кіберзагрозами та функціональною міцністю. Кібератака на комунікаційну чи технологічну систему критичної інфраструктури може прямо позначитися на сталому функціонуванні об'єкта загалом.

• З'ясування вразливостей: Необхідно проводити детальний аналіз комунікаційних та технологічних систем, які є складовою об'єкта критичної

інфраструктури, з метою виявлення прогалин, які можуть бути використані зловмисниками.

• Моделювання наслідків: Важливо передбачати та відтворювати потенційні наслідки успішних кібератак для збереження безперервності життєво важливих послуг. Це допомагає з'ясувати, які системи є найбільш життєво необхідними.

• Формування та втілення заходів захисту: На підставі проведеного аналізу створюються та вводяться в дію комплексні заходи кібербезпеки, які мають відповідати нормативним вимогам та усталеним нормам.

• Паспорт безпеки: Створення та узгодження паспорта безпеки є одним із ключових документів, що обумовлює заходи захисту у випадках виникнення загроз.

• Визначення ступеня важливості: Процес дослідження починається з визначення ступеня важливості об'єкта, що дає змогу надати пріоритет його захисту та коштам, які виділяються на кібербезпеку. Протоколи нарад робочих груп використовуються для фіксації ухвалених рішень щодо класифікації об'єктів.

Дослідження та оцінка чинників вразливостей — це процес виявлення, аналізу та визначення пріоритетів слабких місць у комп'ютерних системах, мережах чи додатках для запобігання кіберзагрозам. Це систематичне сканування, яке допомагає визначити потенційні слабкості безпеки, що можуть бути задіяні зловмисниками, однак воно не передбачає активного зламу. Основне завдання — надати пропозиції щодо усунення виявлених проблем та зниження ризиків.

Процедура оцінки вразливостей

• Ідентифікація: Виявлення слабких місць у налаштуваннях, програмному забезпеченні та мережевій структурі.

• Аналіз: Застосування спеціалізованих інструментів (сканерів вразливостей) для автоматизованого або ручного пошуку відомих слабкостей.

• Кількісна оцінка: Визначення ступеня важливості кожної вразливості, наприклад, за допомогою Загальної системи оцінки вразливостей (CVSS).

• Пріоритизація: Розподіл черговості для усунення вразливостей відповідно до їхньої серйозності.

• Рекомендації: Формування плану дій для усунення або зменшення загроз, пов'язаних з ідентифікованими вразливостями.

Головні відмінності від перевірки на проникнення

• З'ясування вразливостей: Визначає потенційні слабкості та надає поради щодо їх виправлення. Це більш перестрахувальний, ніж прямий, процес.

• Перевірка на проникнення: Імітує справжню атаку, щоб з'ясувати, наскільки легко зловмисник може скористатися визначеними слабкостями.

Особливості методів і засобів дослідження та оцінювання захищеності об’єкту критичної інфраструктури представлено у таблиці 1.2.

Висновки до першого розділу.

У даному розділі наведені нормативні вимоги і критерії до оцінювання захищеності об’єкту критичної інфраструктури. Проведений аналіз основних особливостей факторів інформаційної і кібербезпеки на об’єктах критичної інфраструктури, та визначені основні особливості дослідження впливу факторів Інформаційної та кібербезпеки на захищеність критичного об’єкту.

В розділі розглянуті основні критерії застосування математичних методів та моделей в дослідженні факторів вразливостей на об’єктах критичної інфраструктури.

Проведений загальний аналіз вимог до оцінювання захищеності об’єкту критичної інфраструктури та визначена постановка задачі на дослідження.

Таблиця 1.2 - Особливості методів та засобів дослідження та оцінювання захищеності об’єкту критичної інфраструктури.

Метод	Переваги	Недоліки
Алгоритми кластеризації	ефективні для розріджених мереж	надзвичайно повільні для щільних мереж
Алгоритм полідерев	дозволяє описувати взаємозв’язки вищого порядку	працює тільки для полідерев
Алгоритми узгодження	ефективні для розріджених мереж з невеликими циклічними розрізами	мінімізація циклічних розрізів є NP-складною задачею
Алгоритм реверсування ребра	гарантує знаходження оптимального рішення	реверсування дуг потребує неформального перевизначення ймовірностей подій в окремих вузлах
Алгоритм елімінації	оптимальне впорядкування елімінації дозволяє зменшити складність алгоритму	проблема знаходження оптимального впорядкування елімінації є NP-складною задачею
Символічний алгоритм	дає можливість працювати з параметрами у символічній формі без визначення їх числових оцінок	потребує використання спеціальних програм для здійснення символьних обчислень, дуже неефективний при роботі з великими мережами та/або великою кількістю символьних параметрів
Диференціальний метод	дає можливість обчислити відповіді на дуже широкий клас імовірнісних запитів за сталий час	поліноміальна мережа має експоненціальний розмір
Алгоритми стохастичного вибору	ефективні у випадку відповідності вибіркового розподілу реальному спільному розподілу ймовірностей	потребують багато часу на сходження
Алгоритми спрощення моделі	обчислюваний час зменшується зі зменшенням станів вершини	зменшення станів вершини може суттєво впливати на точність результатів
Алгоритм циклічного поширення	ефективний для ациклічних графів	для графів з циклами може давати слабкі результати або навіть не сходитися
Алгоритми пошуку	ефективні тільки для сильно асиметричних поширень	неефективні для складних багатозв’язних та багаторівневих мереж, що мають вершини з багатьма значеннями

2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА СПОСОБІВ ДОСЛІДЖЕННЯ ТА ОЦІНКИ ФАКТОРІВ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

2.1. Аналіз сучасних методів та засобів дослідження та оцінки факторів Інформаційної та кібербезпеки на об'єкті критичної інфраструктури.

Величезна кількість інформаційних загроз та їх складність спонукає до досліджень та "моделювання" нових методологій і систем "охорони" інформації. Розробка та удосконалення систем інформаційної та кібернетичної безпеки включає в себе створення та обробку математичних моделей з допомогою інформаційних технологій. Сучасний розвиток інформаційних технологій сприяє широкому впровадженню алгоритмів Data Mining для обробки великих масивів інформації у різних галузях, зокрема і в сфері кібербезпеки.

Обсяги інформаційних загроз постійно зростають, а самі вони стають більш складнішими та більш витонченими. Для протистояння у цьому процесі науковці досліджують та моделюють різні методології та системи захисту інформації. Розробка та удосконалення систем інформаційної та кібернетичної безпеки включає в себе створення та обробку математичних моделей з використанням сучасних інтелектуальних інформаційних технологій. Математичні методи та технології є підґрунтям для створення та покращення показників у сфері захисту інформації [15,16]. Сучасний стан потребує такі методи, які б дозволили прораховувати та прогнозувати можливі ризики використання загрозами вразливостей інформаційних активів з метою забезпечення конфіденційності, цілісності та доступності інформації. Обробка ризиків буде результативною, якщо ефективним буде процес аналізу, ідентифікації та оцінки ризиків. Для інформаційних та кібернетичних систем властива якісна оцінка ризиків, яка здійснюється на основі експертних оцінок фахівців. І хоча ця процедура містить математичну обробку цих оцінок,

обчислюється узгодженість експертів, проте існує висока ймовірність отримати даний результат суб’єктивним.

Математичні апарати для оцінки стану захищеності об'єктів критичної інфраструктури (ОКІ) включають методи аналізу ризиків, моделювання, теорії надійності, теорії ігор, а також методи оцінки вразливостей та аналізу кібербезпеки. Ці методи допомагають виявляти слабкі місця, передбачати наслідки атак та оптимізувати заходи захисту, враховуючи як фізичні, так і цифрові аспекти [17].

Основні математичні апарати

• Теорія надійності: Використовується для оцінки ймовірності збою системи або її окремих компонентів. Це дозволяє розрахувати показники надійності, ремонтопридатності та живучості, що є критичними для довготривалого функціонування ОКІ.

• Теорія графів та мережевого моделювання: Застосовується для моделювання складних мереж, аналізу їхньої структури та виявлення критично важливих вузлів або зв’язків. Це допомагає зрозуміти, як порушення роботи одного компонента може вплинути на всю систему.

• Методи оцінки ризиків: Включають кількісний та якісний аналіз загроз та вразливостей. Математичні моделі використовуються для визначення ймовірності реалізації загрози та оцінки потенційних збитків (наприклад, за формулою: Ризик = Ймовірність = Збиток).

• Теорія ігор: Дозволяє змоделювати взаємодію між захисником та нападником. Це допомагає розробляти оптимальні стратегії захисту, враховуючи можливі дії супротивника.

• Теорія прийняття рішень: Використовується для вибору найбільш ефективних заходів захисту з-поміж багатьох альтернатив, зважаючи на наявні ресурси, вартість, ефективність та ризики.

• Методи аналізу кібербезпеки:

Мережевий аналіз: Оцінка захищеності комп'ютерних мереж шляхом аналізу трафіку, виявлення вразливостей та аналізу логів.

Моделювання атак: Симуляція різних типів кібератак для оцінки ефективності існуючих механізмів захисту та виявлення нових вразливостей.

Приклади застосування

• Кіберзахист: Використання математичних методів для оцінки ризиків кібератак, аналізу вразливостей програмного забезпечення та розробки ефективних систем виявлення вторгнень.

• Фізичний захист: Застосування теорії надійності для оцінки стійкості будівель, систем охоронної сигналізації та протидії фізичним атакам.

• Управління інцидентами: Моделювання сценаріїв розвитку подій та визначення оптимального порядку дій у разі аварії чи терористичного акту.

Системний аналіз оцінки стану захищеності об'єкта критичної інфраструктури (ОКІ) — це процес, що охоплює виявлення вразливостей, визначення рівня загроз та розробку заходів для забезпечення стійкості об'єкта. Він ґрунтується на аналізі зв'язків між усіма елементами ОКІ, включаючи технологічні, фізичні та інформаційні аспекти, з метою забезпечення безперебійного функціонування об'єкта під час будь-яких загроз.

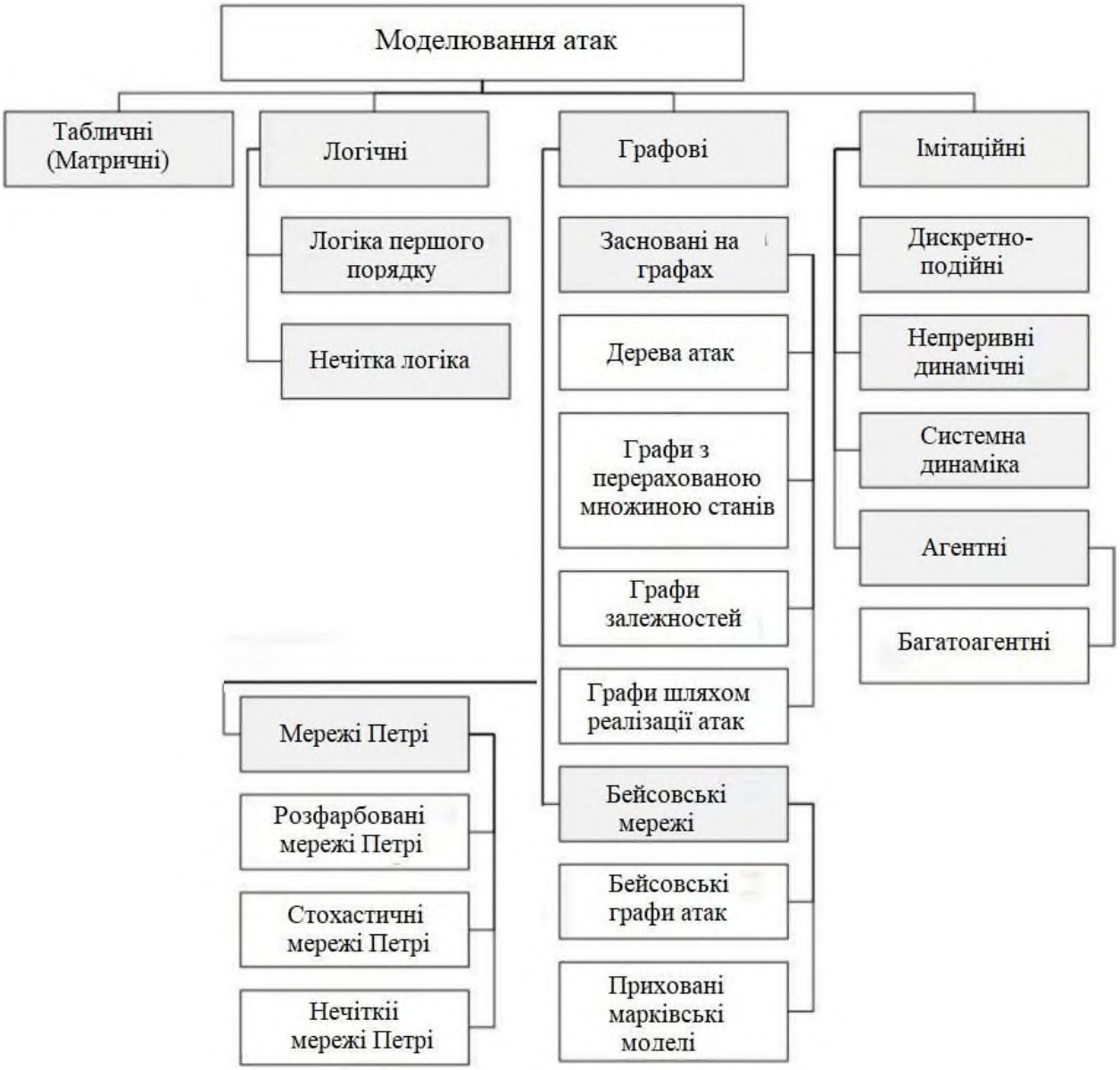

Рисунок 2.1 - Методи аналізу кібербезпеки

Виконаний аналіз досліджень засвідчив, що наявні методи оцінювання дієвості системи захисту мають низку вад, що спричиняє потребу у покращенні характеристик наявних на даний час методів.

Виходячи з цього в даній магістерській роботі пропонується застосувати Ймовірнісний метод оцінки системи захисту, який дозволяє досліджувати повне коло загроз, використовувати реалістичну позицію, зв'язків між частинами системи у явному вигляді.

Таблиця 2.1 —Недоліки та переваги методів оцінки ефективності СЗ.

Спосіб оцінки системи захисту	**Переваги**	**Мінуси**
Статистичний	Дає змогу здобувати результати, коли невідомі параметри СЗ, дозволяє оцінювати систему будь-якої складності	Результати надійні з певною вірогідністю, значний обсяг опрацювання статистичних даних
Імовірнісний	Аналізується повний спектр загроз, застосування реалістичного підходу, взаємозв'язки між елементами системи беруться до уваги у явному вигляді	Хитромудрість розрахунків, неможливо виявити зміну ймовірнісних характеристик спостережень
Експертний	Використання за браку статистичних даних, прудкість здобуття результатів	Надійність результатів залежить від знань експертів
Багатокритеріальний(нейромережний)	Дозволяє брати до уваги велику кількість критеріїв оцінки системи. Дає змогу враховувати кількісні, якісні показники	Труднощі добору оптимальної структури, відсутність формалізованих порядків
Комбінаторний (оптимізаційний)	Найбільш влучний метод оцінки вправності	Складність виконання розрахунків
Матричний (формальний)	Універсальний для проведення оперативної оцінки системи захисту, потребує мінімальних обчислювальних потужностей	Не дає змоги проводити оцінку в умовах невизначеності, великої кількості показників оцінки

2.2. Особливості застосування імовірнісного методу Баєсових мереж довіри в дослідженні та оцінювані факторів впливу Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури.

Одним із найпотужніших математичних апаратів у теорії ймовірності за умов невизначеності є Ймовірнісні графо-аналітичні методи, якими вважаються Байєсові мережі, що дозволяють у логічний спосіб обчислювати ймовірності настання подій при різноманітних обставинах [19,20]. Переваги Байєсових мереж на практиці застосовуються такими відомими корпораціями, як Intel, Microsoft, NASA та ін. Зокрема, науковці NASA (Національного управління з аеронавтики і дослідження космічного простору (США)) використовують Байєсові мережі для забезпечення автономних можливостей обробки інформації для космічних апаратів, виявлення та ідентифікації будь-яких несправностей або несподіваних подій у системі, побудови розкладу виконання завдань для отримання максимальної вигоди, забезпечення проведення геологорозвідувальних робіт за допомогою роботів та ін. Науковці Microsoft серед іншого використовують апарат Байєсових мереж як засіб допомоги текстового редактора Microsoft Office Assistant. Серед різноманіття існуючих методів обчислення Байєсових мереж виділяють дві основні групи: точні та наближені методи. Необхідно відзначити однак, що незважаючи на усі переваги використання Байєсових мереж, їх обчислення для дуже складних систем являє собою NP-складну задачу, навіть за умови використання наближених методів розрахунку. Точні методи найчастіше використовуються для розв’язання підзадач, коли важливість має точність значення ймовірності настання події за умови обрання певної групи альтернатив. Наближені ж методи дозволяють з прийнятною похибкою обчислювати Байєсові мережі, що особливо важливо для розв’язання комплексних задач [21]. Детальну оцінку ефективності основних груп методів обчислення ймовірностей настання подій для Байєсових мереж з конкретними параметрами наведено на рисунку 2.1

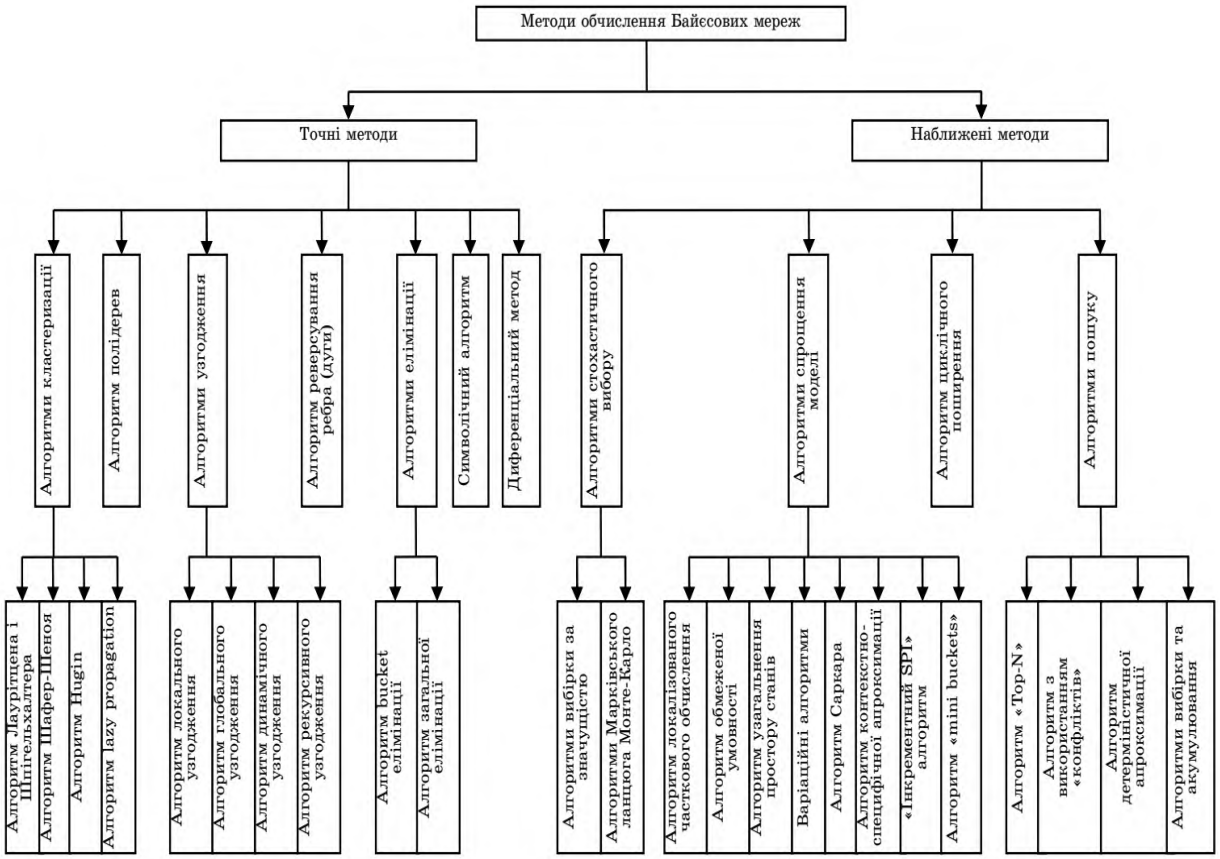

Рисунок 2.2 – Методи обчислення Байєсових мереж.

На сьогоднішній день не існує оптимально ефективного алгоритму для пошуку розв’язків рішень у Байєсових мережах, тому є потреба зниження складності обчислень у мережі. Одним із можливих варіантів зниження складності пошуку розв’язків рішень у Байєсових мережах пропонується використання переваг паралелізації під час перерахунку ймовірностей. Процес паралелізації полягає у поділі комплексної задачі на підзадачі, їх одночасному розв’язанні та формуванні результуючого розв’язку з розв’язків підзадач.

Застосування математичних апаратів за умов невизначеності вважають Байєсові мережі, які дозволяють у логічний спосіб обчислювати ймовірності настання подій при різноманітних обставинах.

Мережа Байєса (МБ) представляє собою пару <G,B>, де G – це направлений ациклічний граф, а P = {P(Xi | Pa(Xi)) | i = 1..n} – множина таблиць умовних ймовірностей вершин. P(Xi | Pa(Xi)) – це відповідно умовний

ймовірнісний розподіл вершини Xi залежно від інстанціювання її батьківських вершин – Pa(Xi). Коли вершина приймає значення одного зі своїх станів, то вона називається інстанційованою.

Сукупний ймовірнісний розподіл в МБ обчислюється за формулою:

$$P(X1, \dots, Xn) = \prod nP(Xi|Pa(Xi)). \quad (2.1)$$

Математично МБ – це модель для представлення існуючих і відсутніх імовірнісних залежностей. Зв'язок A → B є каузальним, якщо подія A є причиною події B, тобто якщо існує механізм, згідно з яким величина A приймає значення що впливає на B.

МБ називається причинною, якщо всі її зв'язки є причинні. Існує низка причин використання причинних моделей в штучному інтелекті:

- як правило, людина інтерпретує події з точки зору причини і наслідку, що спрощує розуміння користувачем причинно-наслідкових закономірностей;

- виявлення інваріантних причинно-наслідкових зв'язків у конкретній проблемі дозволяє передбачити наслідки випадкових подій і наслідки тих чи інших дій, тобто різних маніпуляцій або втручань;

- причинність і ймовірність тісно пов'язані між собою, так як причинність зазвичай передбачає існування імовірнісних відносин, що передають розуміння причинності; насправді необхідною умовою існування причинності є кореляція;

- аксіоматичні властивості МБ відповідають імовірнісним залежностям і випадкам їх відсутності, що виникають у причинній області;

- існують канонічні імовірнісні моделі, засновані на інтерпретації батьками вузла як причин або умов для цього вузла, а також на прийнятті незалежності причинно-наслідкових взаємодій; ці моделі зменшують кількість параметрів мережі, спрощують придбання знань і навіть сприяють зниженню обчислювальних витрат;

- причинні МБ підтримують деякі якісні аспекти рішень, які можуть бути визначені, щоб пояснити результати висновку; деякі з цих аспектів є у певних канонічних моделях.

2.2.1 Представлення мереж Байєса у вигляді графів.

Теорія графів часто використовується для моделювання процесів різної природи, а МБ також бувають представлені у вигляді графу.

Граф – це набір вершин (вузлів), з'єднаних дугами. Дуга між двома вершинами вказує на наявність відносини між ними, а спрямована дуга вказує напрямок цього зв'язку – від причини до наслідку. У байєсівській мережі всі дуги спрямовані, тобто це направлений граф.

Направлений граф – це пара G = <V, E>, де V = {X1, .., X n} – це множина вершин (змінні) і E = {(Xi, X j) | Xi, X j ∈V} – множина ребер графа.

Направлений граф є ациклічним, якщо він не містить спрямованих циклів, тобто для кожної вершини графа Xi немає спрямованого шляху, який починається і закінчується в Xi. Рисунок 2.3 а) показує приклад циклічного графу, рисунок 2.3 б) – ациклічного.

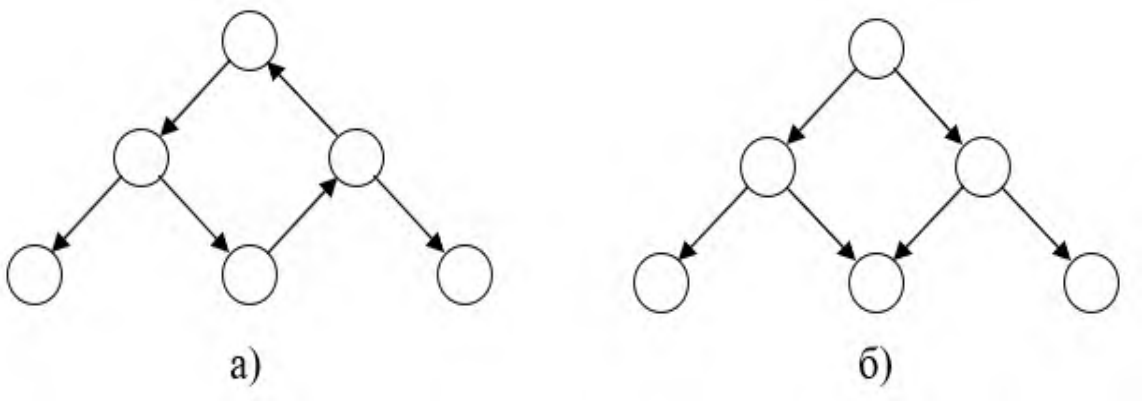

Рисунок 2.3 - Види графів: а) циклічний граф; б) ациклічний граф

На рисунку 2.4 в парі (Xi, X j)∈G, Xi є батьком вершини X j , а X j відповідно є нащадком Xi .

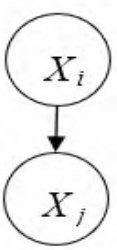

Рисунок 2.4 - Пара (Xi, X j)∈G

Вершина Xi називається коренем у направленому графі, якщо в неї не входять ребра, а вершина X j називається листком, якщо з неї не виходять ребра.

За типами структури графів МБ бувають деревами, однозв'язними мережами та багатозв'язними мережами.

Дерево – це направлений ациклічний граф, де кожна вершина може мати не більше одного батька (рис. 2.5).

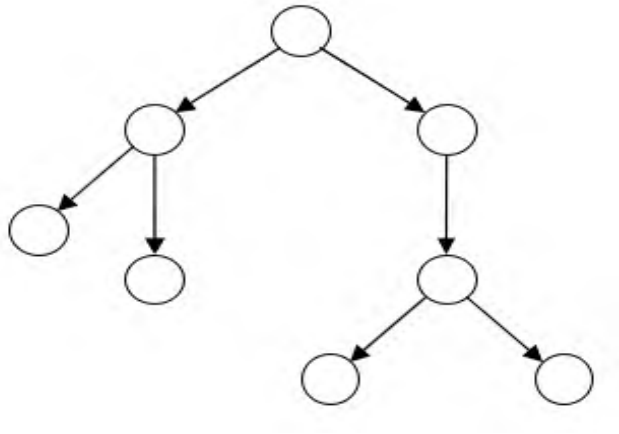

Рисунок 2.5 - Приклад дерева.

Однозв'язна мережа або полідерево – це направлений ациклічний граф, в якому кожна вершина може мати більше одного батька, але існує тільки один (ненаправлений) шлях між будь-якими двома вершинами (рис. 2.6).

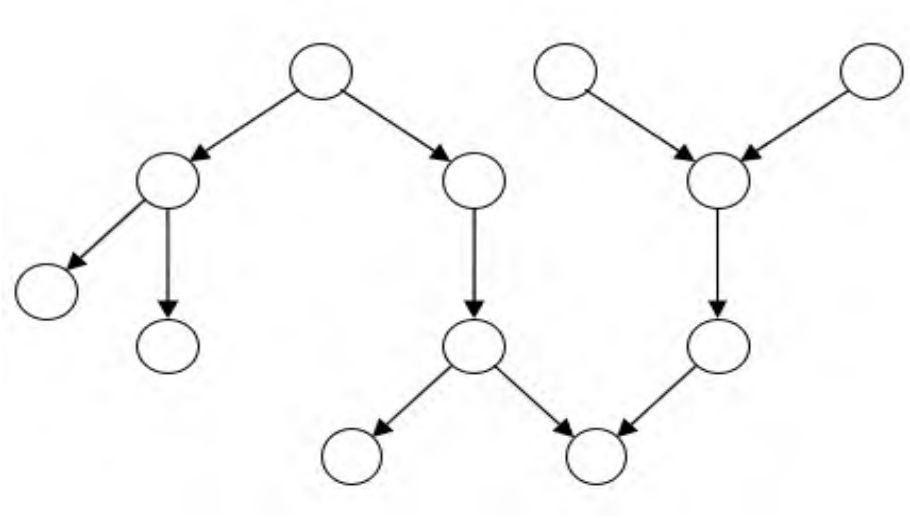

Рисунок 2.6 - Приклад полідерева.

В багатозв’язних мережах між будь-якими двома вершинами може існувати декілька шляхів (рис. 2.7). Саме такі мережі зустрічаються найчастіше при вирішенні різноманітних задач.

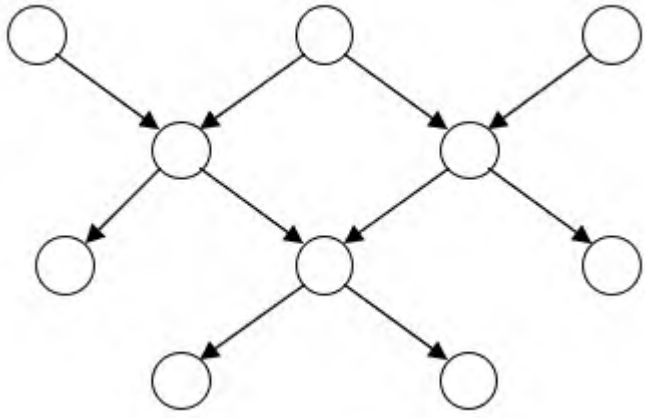

Рисунок 2.7 - Приклад багатозв’язної мережі

2.2.2 Типи мереж Байєса.

В залежності від типів станів вершин та властивостей самих вершин виділяють наступні типи мереж Байєса: дискретні; неперервні; гібридні; динамічні.

Дискретні мережі Байєса.

Дискретні МБ – це мережі, у яких змінні вузлів дискретні, тобто вони мають скінченну кількість станів.

Для опису ймовірнісного розподілу дискретної випадкової величини використовується таблиця – ряд розподілу. У Баєсівській мережі він записується у формі таблиць умовних ймовірностей.

На малюнку 2.8 наведено зразок дискретної мережі діагностування причини відсутності зображення на екрані монітору, де:

- S – стрибок напруги;
- M – пошкодження материнської плати комп’ютера;
- V – пошкодження відеоадаптера;
- I – немає зображення на екрані.

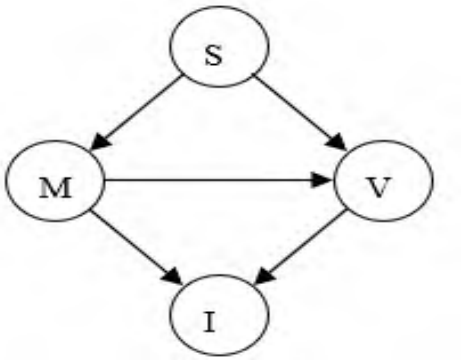

Рисунок 2.8 - Зразок дискретної МБ.

-

Вказаній структурі мережі відповідає наступний набір таблиць умовних імовірностей вузлів (табл. 2.2 – 2.5), де 1 означає позитивну відповідь, а 0 – негативну, тобто якщо M=0, це означає що материнська плата неушкоджена.

Таблиця 2.2 – Значення умовної ймовірності вузла S

Стан	Ймовірність
1	2
S=0	0,6
S=1	0,4

Таблиця 2.3 –Значення 2 ймовірності вузла M.

Батьки	Стани батьків	
1	2	3
S	S=0	S=1
Стан	Ймовірність	
M=0	0,6	0,4
M=1	0,4	0,6

Таблиця 2.4 – Значення умовної ймовірності вузла V.

Батьки	Стани батьків			
1	2	3	4	5
S	S=0	S=0	S=1	S=1
M	M=0	M=1	M=0	M=1
Стан	Ймовірність			
V=0	0,67	0,5	1	0,33
V=1	0,33	0,5	0	0,67

Таблиця 2.5 – Значення умовної ймовірності вузла I.

Батьки	Стани батьків			
1	2	3	4	5
M	M=0	M=0	M=1	M=1
V	V=0	V=1	V=0	V=1
Стан	Ймовірність			
I=0	1	0	0,5	0
I=1	0	1	0,5	1

Неперервні мережі Баєса.

Неперервні МБ – це мережі, у яких змінні вузлів є неперервними. У багатьох випадках події можуть приймати будь-який стан з прийнятого діапазону. Тобто змінна X є неперервною випадковою величиною, а набір її можливих станів є весь діапазон значень, який вона може приймати:

$$X = \{x : a \leq x \leq b\}.$$

Функція розподілу або щільність розподілу використовується для опису розподілу ймовірностей безперервної випадкової величини.

Нехай вузол X має декілька батьків – A ={A1,..,An}, тоді умовний розподіл випадкової величини задається такою формулою:

$$f(X|Ai) = N(\mu x \ + ki \ * \mu i; \sigma x), \tag{2.2}$$

де μx – математичне сподівання величини X; μi – математичне сподівання величини Ai;

ki – ваговий коефіцієнт, який відображає зв'язок між вузлом X та його батьком Ai; σx - стандартне відхилення величини X:

$$N(\mu_x + k_i * \mu_i; \sigma_x) = \frac{1}{\sigma_x\sqrt{2\pi}} * exp\left[-\frac{1}{2}\left(\frac{x-(\mu_x+k_i*\mu_i)}{\sigma_x}\right)^2\right]. \tag{2.3}$$

Зв'язок між змінною X та її батьками A ={A1,..,An} можна представити за допомогою лінійної регресійної моделі:

$$X \ = k1 \ * A1 \ + \cdots + kn \ * An + Qx, \tag{2.4}$$

де ki – регресійний коефіцієнт, який відображає зв'язок між змінними X та Ai ;

Qx – шумова компонента, що може бути записана у вигляді нормального розподілу з нульовим математичним сподіванням.

На рисунку 2.9 наведено зразок неперервної МБ з нормальним законом розподілу, де A1,..,An – батьки X ; B1,..,Bn – її нащадки; k1,..,kn – вагові коефіцієнти; QA1 ,..,QAn ,Qx,QB1 ,..,QBn – шумові коефіцієнти.

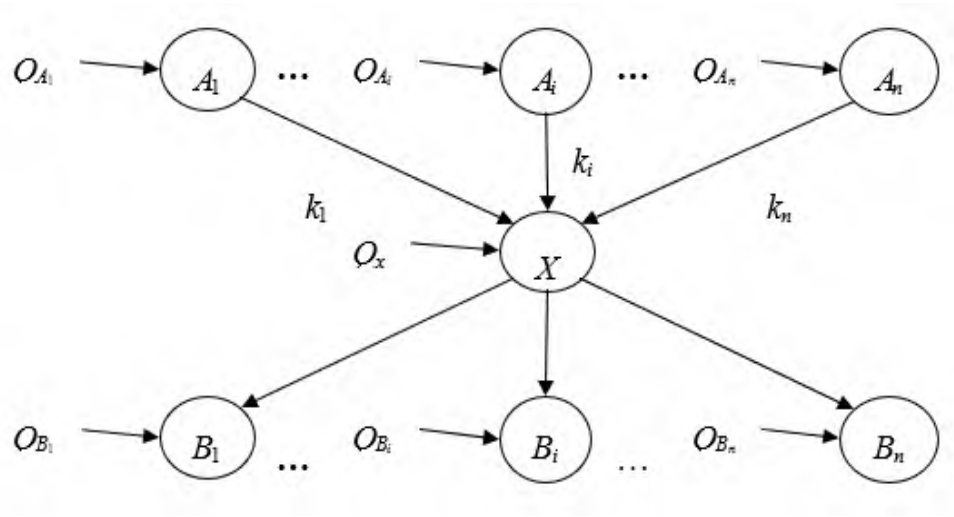

Рисунок 2.9 - Зразок неперервної МБ.

Гібридні мережі Баєса.

Гібридні МБ – це мережі, вузли яких містять як дискретні, так і неперервні змінні.

Використання дискретних і неперервних змінних в одній мережі вимагає деяких обмежень:

- дискретні вузли не можуть мати неперервних батьків;
- неперервні змінні мають нормальний закон розподілу, залежно від значень їх батьків;
- розподіл неперервної змінної X з дискретними батьками A і неперервними батьками B є нормальним.

Нехай дискретні випадкові величини A1,..,Ap та неперервні випадкові величини B1,...,Bm впливають на результуючу неперервну випадкову величину X, як показано на рисунку 2.10. Квадратні вузли мають дискретний розподіл, а круглі – неперервний.

Кожна з дискретних випадкових величин Aj (j =1,..., p) може приймати значення Aij (i =1,..,n j) з імовірностями Pij , для яких ∑Pij =1. Загальний вплив дискретних випадкових величин на X характеризується математичним сподіванням (μi1,..,μip) та стандартним відхиленням (σi1,..,σip).

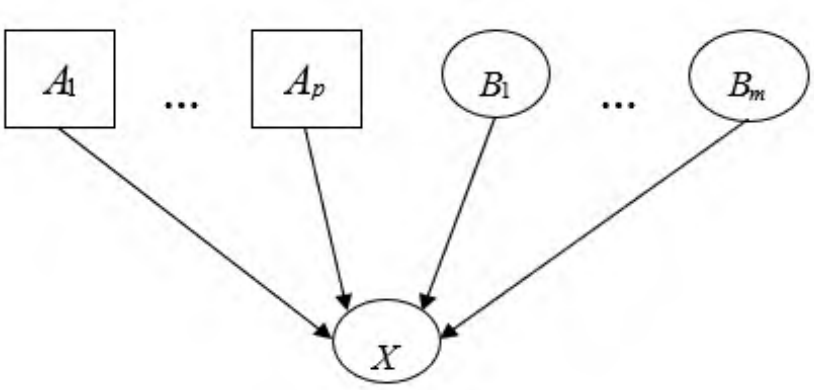

Рисунок 2.10 - Зразок гібридної МБ.

Загальний вплив неперервних величин та значень дискретних величин на кінцеву випадкову величину X позначається ваговими коефіцієнтами kl,i1,..,ip для l =1,..,m.

Тоді характеристики величини X можна обчислити за формулами:

$$\mu_x = \sum_{il=1}^{n_l} .. \sum_{ip=1}^{n_p} P_{1,il} * ... * P_{p,ip} * \left(\mu_{i1,...,ip} + \sum_{l=1}^{m} k_{l,i1,...,ip} * \mu_i\right), \quad (1.5)$$

$$\sigma_x = \sqrt{\sum_{i1}^{n_1} .. \sum_{ip}^{n_p} P_{1,i1} *..* P_{p,ip} * \left((\mu_{i1,..,ip} + \sum_{l=1}^{m} k_{l,i1,..,ip} * \mu_i)^2 + \sigma^2_{i1,..,ip} + \sum_{l=1}^{m} k^2_{l,i1,..,ip} * \sigma_l^2\right) * \mu^2.} \quad (1.6) \quad (2.5)$$

Динамічні мережі Баєса.

Динамічні МБ – це мережі, у яких значення вузлів змінюється з плином часу, тому вони використовуються для моделювання часових процесів. Динамічні Баєсівські мережі ще також називають «часовими», оскільки структура моделі залишається незмінною, хоча приховані вузли можуть бути додані для опису поточного стану процесу.

Найпростіший тип динамічної МБ – це прихована модель Маркова, в якій кожен шар має прихований дискретний вузол і спостережуваний дискретний або неперервний вузол (рис. 2.11).

Для визначення динамічної мережі необхідно вказати початковий розподіл P(X(t)), топологію всередині шару P(X(t + i) | X(t + i −1)) та між двома шарами - P(Y(t) | X(t).

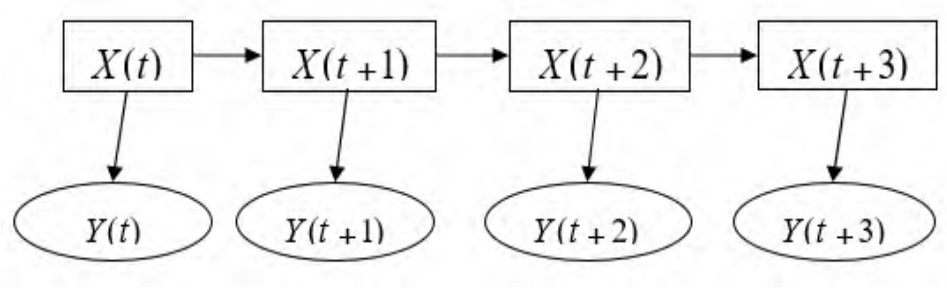

Рисунок 2.11 - Зразок динамічної мережі Баєса.

2.2.3 Визначення апріорних ймовірностей подій і формула Байєса.

Розглянемо приклад мережі на рис. 2.12, у якій ймовірність перебування вершини «e» у різних станах (e_k) залежить від станів (c_i, d_j) вершин «c» і «d» і визначається наступним виразом:

$$p(e_k) = \sum_i \sum_j p(e_k \mid c_i, d_j) \times p(c_i, d_j),$$

де $p(e_k \mid c_i, d_j)$ – ймовірність перебування в стані e_k в залежності від станів c_i, d_j. Оскільки події, що представлені вершинами «c» і «d» незалежні, то $p(e_k \mid c_i, d_j) = p(c_i) \cdot p(d_j)$.

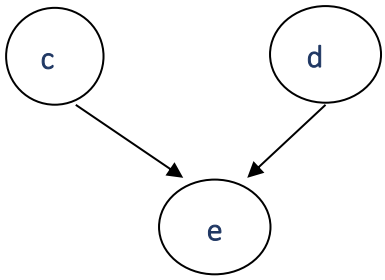

Рисунок 2.12 - Приклад найпростішої мережі довіри Байєса.

Розглянемо приклад складнішої мережі (рис. 2.13).

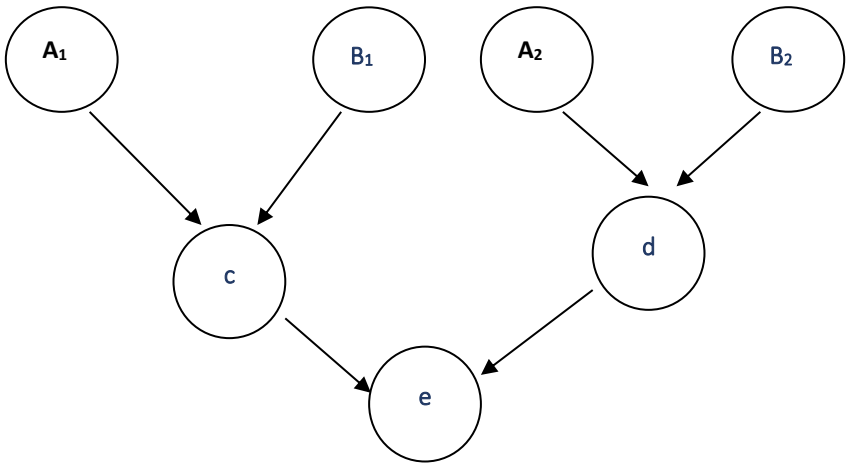

Рисунок 2.13 - Дворівнева мережа довіри Байєса.

Цей рисунок ілюструє умовну незалежність подій. Для оцінки вершин «c» і «d» використовують ті самі вирази, що й для обчислення ймовірності $p(e_k)$, тоді:

$$p(c_i) = \sum_m \sum_n p(c_i \mid A_{1m}, B_{1n}) \times p(A_{1m}) \times p(B_{1n}),$$

$$p(d_j) = \sum_m \sum_n p(d_j \mid A_{2m}, B_{2n}) \times p(A_{2m}) \times p(B_{2n}).$$

З цих виразів видно, що вершина «e» умовно не залежить від вершин A_1, A_2, B_1, B_2, оскільки немає стрілок, що безпосередньо поєднують ці вершини

Саме процес обчислення ймовірностей стає основою для формування рішень в умовах невизначеності на підставі МБ. Основу байєсівського підходу складає поняття умовної ймовірності. Вираз для умовної ймовірності $P(A|B) = x$ позначає, що при умові виникнення B (і усього іншого, що не має відношення до B), ймовірність виникнення A дорівнює x. Спільна ймовірність появи подій A і B визначається формулою повної ймовірності:

$$P(A,B) = P(A \mid B) \cdot P(B) = P(B|A) \cdot P(A). \qquad (2.6)$$

Це рівняння є *фундаментальним правилом* для обчислення ймовірностей і є основою для *теореми Байєса*:

$$P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}. \quad (2.7)$$

З формулою повної ймовірності тісно пов'язана формула Байєса. Якщо до експерименту ймовірності гіпотез були $P(H_1), P(H_2), ..., P(H_n)$, а в результаті експерименту з'явилась подія A, то із урахуванням цієї події «нові», тобто умовні ймовірності гіпотез, обчислюються за формулою Байєса:

$$P(H_k / A) = \frac{P(H_k)P(A/H_k)}{P(A)} (k = 1,2,...n), \quad (2.8)$$

$$\text{де } P(A) = \sum_{i=1}^{n} P(H_i)P(A/H_i).$$

Тоді умовна ймовірність $P(H_k / A)$ може знаходитись як відношення ваги дуги, що проходить через вершину, яка відповідає гіпотезі H_k, до ваги усього ймовірнісного графу.

2.3. Постановка задачі на дослідження впливу факторів Інформаційної та кібербезпеки на захищеність об'єкту критичної інфраструктури з використанням імовірнісного методу Баєсових мереж довіри.

Управління системою забезпечення захисту інформації критичної інфраструктури, як і у разі управління будь-якою соціально-технічною структурою, пов'язане зі значними складнощами, спричиненими неповнотою інформації, конфліктами інтересів та цілей, швидкими та численними змінами у різних галузях здійснення інформаційної боротьби за їхню потенційну безпеку.

Існуючі на сьогодні методики оцінки ефективності системи захисту не задовольняють належним чином критерії оцінки ефективності, не враховують адекватних і необхідних показників оцінки ризиків інформаційної безпеки, оцінок з точки зору ефективності загальної безпеки даних, вимоги, значення

фінансових витрат на створення системи захисту, IT-інфраструктури розподілених систем.

Тому алгоритми прийняття рішень на всіх рівнях ієрархії з управління захистом ОКІ, має відповідати сучасним математичним моделям щодо оптимізації ієрархічних структур. Зокрема, в умовах випадкових факторів впливу загроз або їх імітації, як показав аналіз, доцільно освоєння і застосування імовірнісно-статистичних методів моделювання та дослідження безпеки ОКІ.

Доцільність застосування імовірносно-статистичних методів для оцінки стану безпеки об'єктів ОКІ в умовах конкретизації ймовірності випадкових недружніх для них впливів (оцінюваних, наприклад, як імовірність правильного виявлення або як імовірність пропуску загрози), а їх (методів) конкретне використання може бути обрано після детального дослідження та аналізу щодо визначення стану безпеки ОКІ. Саме це є предметом дослідження у даній роботі. Таким чином має бути чітке формулювання завдання, що залежить від виду виникнення проблеми.

Виходячи з даного аналізу, для вирішення задачі дослідження та оцінки впливу факторів Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури, пропонується вирішення наступних завдань:

1. Провести аналіз сучасних методів та способів дослідження та оцінки факторів Інформаційної та кібербезпеки на об’єкті критичної інфраструктури.

2. Визначити особливості застосування імовірнісного методу Баєсових мереж довіри в дослідженні та оцінювані факторів впливу Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури.

3. Побудувати інформаційну модель впливу факторів інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури.

4. Визначити та провести оцінювання основних факторів впливу інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури.

5. Розробити інформаційно – логічну модель оцінки впливу факторів інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури із застосуванням імовірнісного методу Баєсових мереж довіри.

6. Виконати практичну реалізацію результатів дослідження захищеності об’єкту критичної інфраструктури із застосуванням імовірнісного методу Баєсових мереж довіри.

Висновки до другого розділу.

У даному розділі проведений аналіз та класифікація факторів Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури. Розглянуті вимоги, що пред’являються до застосування імовірносно-статистичних методів для оцінки стану безпеки об'єктів ОКІ в умовах конкретизації ймовірності випадкових недружніх для них впливів.

У розділі також визначені задачі на дослідження та оцінювання впливу факторів Інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури з використанням імовірнісного методу Баєсових мереж довіри.

РОЗДІЛ 3. ДОСЛІДЖЕННЯ ТА ОЦІНКА ФАКТОРІВ ВПЛИВУ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ НА ЗАХИЩЕНІСТЬ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ З ЗАСТОСУВАННЯМ ІМОВІРНІСНОГО МЕТОДУ БАЄСОВИХ МЕРЕЖ ДОВІРИ

3.1 Побудова інформаційної моделі впливу факторів інформаційної та кібербезпеки на захищеність об'єкту критичної інфраструктури.

Побудова інформаційної моделі впливу факторів інформаційної та кібербезпеки на захищеність об'єкту критичної інфраструктури — це структурований підхід для аналізу, який оцінює, як різні загрози кібератаки, вразливості, ризики, що впливають на стабільне функціонування об'єкта. Ця модель допомагає визначити слабкі місця, оцінити ризики та розробити ефективні заходи захисту для забезпечення конфіденційності, цілісності та доступності інформаційних систем, які є критично важливими для функціонування об'єкту критичної інфраструктури.

Для побудови інформаційної моделі необхідно наступне:

- Визначення об'єкта критичної інфраструктури:

ідентифікація об'єктів, порушення роботи яких може спричинити надзвичайні ситуації та негативно вплинути на екологічну, енергетичну, економічну чи іншу сферу.

- Ідентифікація факторів впливу:

аналіз потенційних загроз, до яких належать:

кіберзагрози: кібератаки, шкідливе програмне забезпечення, фішинг,

- Інформаційні загрози:

неповнота, невчасність, невірогідність інформації, негативний інформаційний вплив.

- Внутрішні ризики:

людський фактор, помилки персоналу, застаріле програмне забезпечення.

- Технічні вразливості:

недостатній захист обладнання, комунікаційних систем.

- Оцінка ризиків:

кількісна або якісна оцінка ймовірності реалізації загроз та можливих наслідків для об’єкта.

- Моделювання впливу:

побудова моделі, яка візуалізує зв'язок між факторами впливу, вразливостями об’єкта та його загальною захищеністю. Можна використовувати різні методи моделювання, наприклад, графічні моделі, статистичні методи, симуляції.

- Розробка заходів захисту:

на основі моделі розробляються та впроваджуються заходи для зменшення ризиків та підвищення захищеності, що включає:

- впровадження технічних засобів захисту інформації.
- розробка політик безпеки та процедур управління ризиками.
- навчання персоналу.
- встановлення резервних систем та процедур відновлення даних.

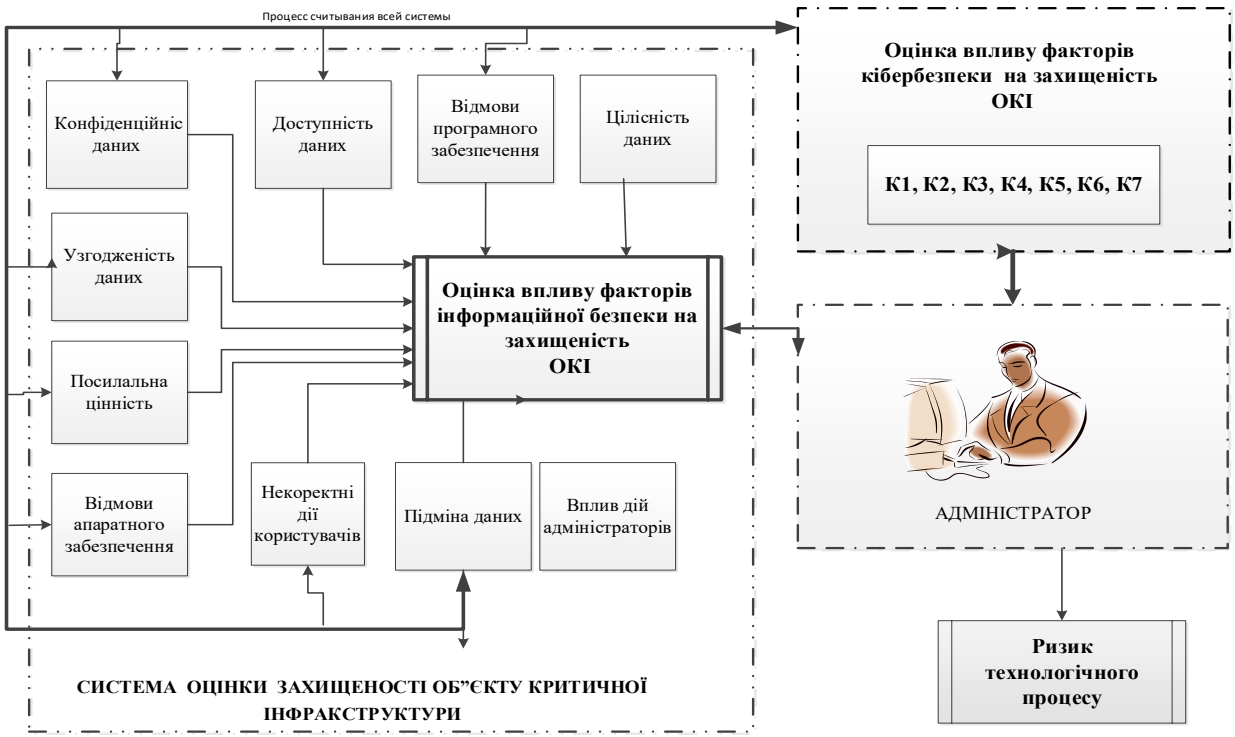

Рисунок 3.1 - Інформаційна модель впливу факторів інформаційної та кібербезпеки на захищеність об’єкту критичної інфраструктури.

У відповідності до запропонованої інформаційної моделі на рисунку 3.1, уся зібрана інформація контролюється і аналізується відповідними модулями системи моніторингу. Модуль входу користувача з правами Адміністратора - виконує аналіз стану привілейованості користувача. У кожного користувача призначені права доступу до різних видів ресурсів. Ці права дозволяють реалізувати повний контроль над можливостями клієнтів. Обмежуючи права доступу до певних компонентів можна досягти високого рівня безпеки, а також відсутності ризику в функціонуванні ОКІ.

Після завершення системою моніторингу сканування і контролю усіх секторів системи захисту, виконується оцінка ймовірностей поточного стану модулів контролю Інформаційної і кібербезпеки та стану ризику, які впливають на загальний стан безпеки об’єкту критичної інфраструктури. Якщо за результатами перевірки не виявлено загроз, то центральний модуль оцінює стан секторів системи як з повною ймовірністю захищеності.

У випадку присутності збоїв або загроз, відповідний модуль оцінює ймовірності ступеню захищеності секторів, після чого приймаються відповідні рішення щодо усунення загрози на ОКІ.

Результати оцінок ймовірності стану захищеності усіх модулів відправляються на центральний модуль адміністратора, де виконується контроль, оцінка та підтримка повної захищеності ОКІ.

Для підвищення інформаційної та кібернетичної безпеки розробляються різні інтелектуальні системи захисту інформації. Такі системи включають в себе використання різноманітних моделей і методів таких як: біометричні сканери або аналіз і запам'ятовування послідовності дій користувача, що зрештою згенерує спеціальні засоби захисту інформації.

3.2 Визначення та оцінка головних чинників впливу інформаційної та кібербезпеки на стан захисту об'єкта критичної інфраструктури.

Відповідно до Інформаційної моделі (рис.3.1), та нормативно-правової бази щодо захисту об'єктів критичної інфраструктури, найбільш впливовими

чинниками безпеки на ОКІ є чинники Інформаційної безпеки (І1 – І10) та чинники кібернетичної безпеки (К1 – К7),

Інформаційна безпека (Informational security) - це стан збереженості систем обробки і зберігання відомостей, яка контролюється та коригується модулем моніторингу інформаційної безпеки відповідних вузлів:

- І1 - незмінність відомостей;
- І2 - доступність відомостей;
- І3 - конфіденційність відомостей;
- І4 - узгодженість відомостей;
- І5 - посилальна цінність;
- І6 - збої апаратного забезпечення;
- І7 - збої програмного забезпечення;
- І8 - некоректні дії користувачів;
- І9 - вплив дій адміністраторів;
- І10 - енергетичні збої.

Кібербезпека (Cyber security) - це унеможливлення доступу хакерів до систем та інформації, що потенційно тягне за собою втрату конфіденційності та/або контролю. Контроль та коригування кібернетичної безпеки забезпечується модулем моніторингу кібернетичної безпеки відповідних вузлів:

- К1 - попередньої підстановки у запити відомостей і перевірка на SQL - ін'єкції;
- К6 - зовнішній тиск;
- К2 - перевірки системи на віруси;
- К3 - перевірки входу користувача з правами адміністратора;
- К4 - доступності відомостей та ресурсів;
- К5 - перевірки інформації на наявність підміни відомостей;
- К6 - захищеність відомостей;
- К7 - перевірки відомостей на незмінність (використовуючи хеш).

Для визначення і оцінки ступеня важливості найбільш дієвих зазначених чинників безпеки, в залежності від категорії критичності ОКІ, пропонується застосування методу експертних оцінок [22].

Метод експертних оцінок – це методологія, що використовується для збору та аналізу думок кваліфікованих фахівців з метою оцінки різноманітних явищ, процесів, проектів чи рішень.

Експертизу проводили експерти-фахівці, які мають досвід у розробці програмно–інструментальних засобів автоматичного тестування, і поскільки необхідно визначити тільки ранги чинників, то погодженість їх оцінок доцільно визначати за допомогою множинного коефіцієнта конкордації (K_0) запропонованого М. Кендаллом і Б. Смітом [22].

Для цього, експертам (m) пропонувалося присвоїти ранг (n) чинникам впливу наведених у таблицях 3.1. та 3.2.

Маючи набір оцінок необхідно підрахувати середній арифметичний ранг для кожного значення та перетворити його на підсумковий ранг. Чим менший середній ранг має (n), тим привабливішим він стає в застосуванні оцінюваної системи. Найменший середній ранг мають оцінки параметрів під номерами 1 та 9, тому вони займають першу послідовність у ранжованому ряді. Такі дії проводяться стосовно усіх оцінок, що в результаті формує загальний вигляд ранжованого ряду, наведений у таблиці 3.3

За наслідками досліджень наведених в таблицях 3.1 та 3.2, визначається погодженість експертів.

Для цього доцільно використати перевірку за допомогою критерія Фішера, *F*- критерія Фішера. Де через (X_{ij}) позначено ранг j -го фактору ($j = \overline{1,n}$) у ранжировці i -го експерта ($i = \overline{1,n}$). Для оцінки підготовленості експертів дотримуємось умови:

$$\sum_{j=1}^{n} X_{ij} = 0{,}5n(n+1) \qquad (3.1)$$

де: $\sum_{j=1}^{n} X_{ij}$- сума рангів у ранжирові j -го експерта.

Погодженість експертів при ранжирові груп інформації оцінювалася коефіцієнтом конкордації (згоди):

$$K_0 = \frac{12S}{m^2(n^2-n)-m\sum_{i-1}^{m} T_i} \quad (3.2)$$

де: $S = \sum_{j-1}^{n} di^2$ - сума квадратів відхилень сум рангів, отриманих усіма групами інформації, від середньо – арифметичного сум рангів

$$d_j = X_j - 0{,}5m(n+1) \quad (3.3)$$

де:d - відхилення суми рангів j-*го* виду від середнього значення сум рангів по всім видам;

$$T_j = \sum_{\mu=1}^{n}(t_{\mu i}{}^3 - t_{\mu i}) \quad (3.4)$$

де: $T_{\mu i}$-число повторень μ -го рангу в ранжировці і-*го* експерта.

При K_0 = 1 думка експертів вважається узгодженою повністю. При K_o*<1,* згідно з рекомендаціями для перевірки значимості погодженості визначаються значення статистики X^1 і X^2:

$$X_{\text{набл}}^{(1)} = K_0 m(n-1) \quad (3.5)$$

$$X_{\text{набл}}^{(2)} = \frac{(m-1)X^{(1)}}{m(n-1)-X^{(1)}} \quad (3.6)$$

Після чого необхідно визначити числа ступенів свободи (υ1) і (υ2) розподілу, для цього обчислюються значення величин;

$$\upsilon_1 = n-1\,,\, \upsilon_2 = \frac{L^2}{(m-1)\sum_{j=1}^{n} V_j^2} - (m-1) \quad (3.7)$$

де: $L = (m-1)\sum_{j=1}^{n} V_j$

$$V_j = \frac{1}{(m-1)\sum_{i=1}^{m}(X_{ij}-X_j^2)} \quad (3.8)$$

$$X_j = \frac{1}{m}\sum_{i=1}^{m} X_{ij}, \quad j = \overline{1,n} \quad (3.9)$$

По таблиці F – розподілу Фішера порівнюємо критичне значення $F_{кр.}$ при рівні значимості α =0.05 і числах ступеню свободи υ1 і υ2. Порівнюючи отримане значення $X_{набл}$ зі значеням $F_{кр.}$ робимо висновок, що думки експертів можна вважати погодженими.

Таблиця 3.1 – Результати експертного оцінювання факторів інформаційної безпеки (I)

m	**Експертні оцінки**									
	n – фактори впливу									
експерти	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**	**I9**	**I10**
E1	5	6	8	7	7	6	8	9	4	7
E2	8	9	9	10	7	9	8	10	6	8
E3	8	7	8	8	6	7	6	9	5	8
E4	4	6	5	5	8	9	10	2	9	7
E5	8	7	9	9	6	8	7	10	6	5
E6	9	8	9	6	5	7	8	9	8	10
E7	4	5	7	3	7	6	9	8	2	6
E8	6	8	7	6	6	7	8	9	6	10
E9	3	8	1	5	9	4	8	9	7	6
E10	4	8	10	9	7	8	9	8	6	5
$\sum_{j=1}^{m} x_{ij}$	*59*	*72*	*73*	*69*	*69*	*71*	*81*	*83*	*59*	*72*

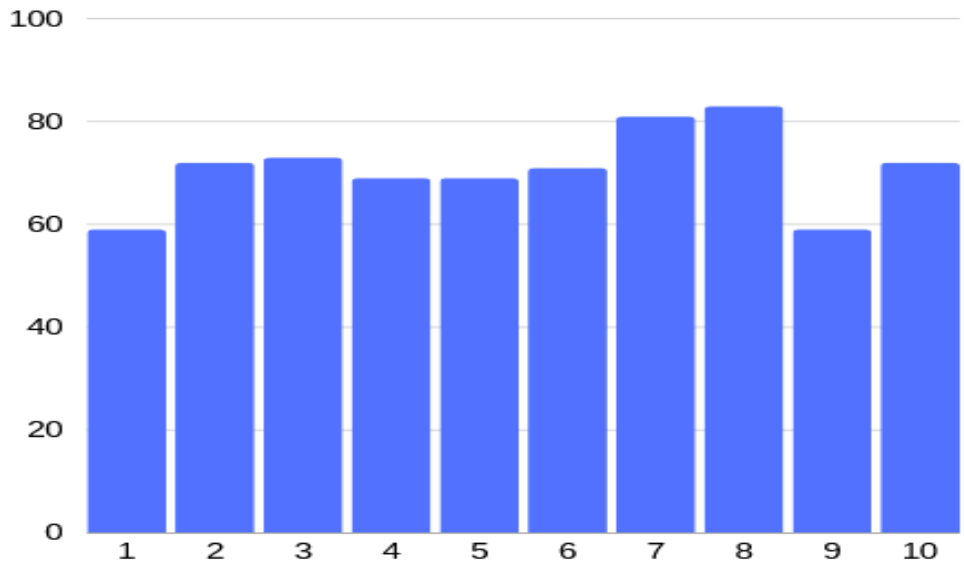

Рисунок 3.2 – Рангова гістограма розподілу важливості факторів інформаційної безпеки (І)

Таблиця 3.2- Результати експертного оцінювання факторів кібербезпеки (К)

m експерти	**Експертні оцінки**						
	n – фактори впливу						
	К1	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**
Е1	10	9	3	9	10	10	5
Е2	8	8	6	9	7	10	8
Е3	6	6	7	8	6	10	7
Е4	7	7	4	7	8	8	7
Е5	7	9	4	7	10	5	4
Е6	5	4	8	8	8	1	4
Е7	4	8	5	5	10	10	4
Е8	4	7	5	6	10	01	5
Е9	5	4	8	7	6	6	2
Е10	5	7	6	6	6	8	5
$\sum_{j=1}^{m} x_{ij}$	**61**	**69**	**56**	**72**	**81**	**78**	**51**

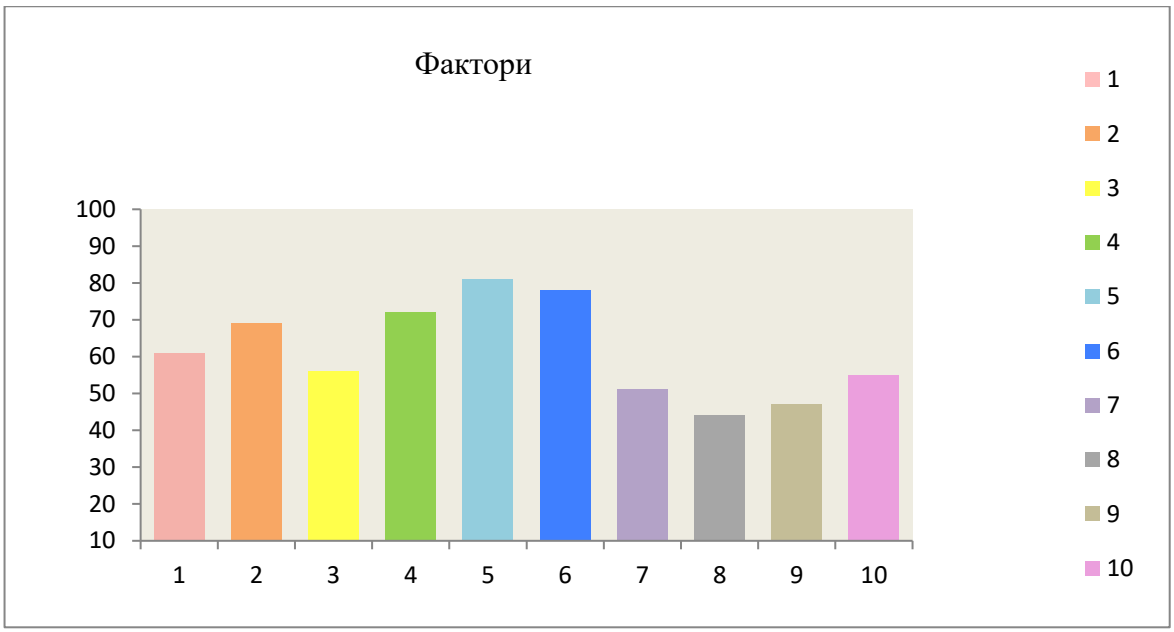

Рисунок 3.3 – Рангова діаграма розподілу важливості факторів впливу кібернетичної безпеки.

Задля перевірки злагоди отриманих ранжованих рядів проаналізуємо здобутий результат (табл.3.3) з застосуванням згаданого методу оцінки коефіцієнта конкордації.

Для обрахунку потрібно мати середню суму оцінок, яка у цьому випадку визначається за формулою 3.1:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} a_i\,, \tag{3.10}$$

де n – кількість кінцевих рангів;

a – значення кінцевого рангу чинника.

Маючи усі потрібні для розрахунку відомості отримаємо простий приклад наступного вигляду:

$$\bar{x} = \frac{700}{10} \rightarrow \bar{x} = 70$$

Отримавши результат зможемо побудувати таблицю (табл. 3.5), яка містить зміщення та квадрат середньої суми для суми кожної оцінки.

Таблиця 3.3 – Відхилення та квадрат середньої суми для кожної оцінки

Відхилення від середньої суми $\Delta = (\boldsymbol{x_j} - \overline{\boldsymbol{x}})$	Квадрат середньої суми $\boldsymbol{\Delta^2} = (\boldsymbol{x_j} - \overline{\boldsymbol{x}})^{\boldsymbol{2}}$
-12	144
1	1
2	4
-2	4
-2	4
0	0

Продовження таблиці 3.3

10	100
12	144
-12	144
1	1
$\sum = 537$	

На цьому етапі маємо усі необхідні дані для отримання коефіцієнту конкордації, що обчислюється за наступною формулою 3.2:

$$W = \frac{12 * S}{m^2(n^3 - n)} = \quad = \frac{12 * 537}{10^2(10^3 - 10)} = 0.596, \qquad (3.11)$$

де S – сума квадратів середньої суми;

n – кількість чинників;

m – кількість експертів.

Оскільки значення коефіцієнту W ≈ 0.596 є близьким до 1, це свідчить про злагоду експертних оцінок. Також, задля візуального представлення злагоди наведено гістограму (рис. 3.2), яка показує ступінь розбіжності в оцінках експертів.

3.3 Розробка інформаційно – логічної моделі оцінки впливу факторів інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури з застосуванням імовірнісного методу Баєсових мереж довіри.

Побудова Інформаційно-логічної моделі оцінки стану інформаційного та кіберзахисту ОКІ – представляє структуровану систему, яка використовує логічні зв'язки та інформаційні блоки для аналізу та оцінки рівня захищеності об'єктів кіберзахисту. Вона включає збір даних, їх обробку, аналіз ризиків, визначення вразливостей та розробку рекомендацій для підвищення безпеки.

У даному розділі розроблено Інформаційно – логічну модель, на якій показано формалізовані логічні зв'язки та інформаційні блоки для аналізу та оцінки рівня захищеності ОКІ (рис. 3.4).

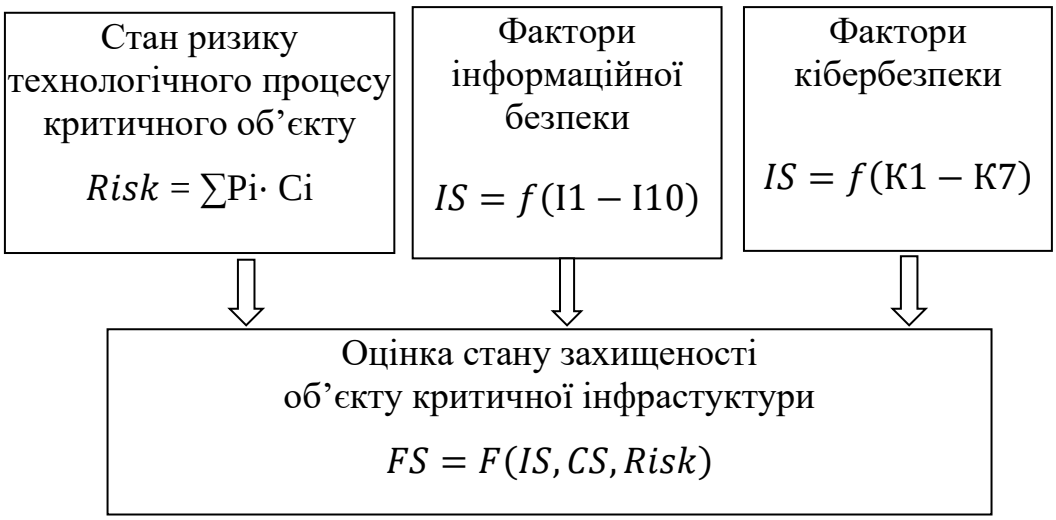

Рисунок 3.4 - Інформаційно – логічна модель оцінки стану інформаційного і кіберзахисту ОКІ.

Згідно з Інформаційно-логічною моделлю (рис.3.4), задля оцінки стану інформаційного та кіберзахисту ОКІ розроблено Баєсовську мережу довіри (БМД), спрощену будову якої наведено на рисунку 3.5.

На сьогодні один з найбільш слушних підходів, призначених для роботи з неповною, неточною та суперечливою інформацією, являє собою БМД, що ґрунтується на імовірнісному методі й спроможна у найбільшій мірі оперувати

відомостями, які надходять з обраних джерел для досягнення найвищого ефекту.

Баєсові мережі – це графові моделі імовірнісних та причинно-наслідкових взаємозв'язків між параметрами у статистичному інформаційному моделюванні. У Баєсових мережах, можуть злагоджено поєднуватися емпіричні частоти появи різних значень змінних, суб'єктивні оцінки «сподівань» та теоретичні уявлення про математичні вірогідності тих чи інших результатів з апріорною інформацією. Це створює важливу практичну перевагу і виокремлює Баєсові мережі з-поміж інших методик інформаційного моделювання [20].

Проте, шляхом опрацювання цієї проблеми в рамках поставленого завдання слугує глибший математичний та аналітичний підхід. Оскільки завдання, що розглядається, впроваджує нові інформаційні технології, що дає змогу застосувати імовірнісний математичний підхід у поєднанні з формуванням Баєсівської мережі довіри. Зіставлення цього набору обчислень дозволить значно підвищити рівень виконання поставленого завдання.

Баєсівська мережа довіри (БМД) є статистичним інструментом, що використовується для знаходження зв’язків поміж різними змінними та робить висновки про вірогідність подій, спираючись на ці зв'язки. Така мережа базується на теорії імовірностей та використовує у своїй основі правило Баєса для коригування вірогідностей у разі отримання нових розрахункових відомостей.

БМД являють собою графічні моделі подій та процесів, базовані на об’єднанні певних висновків теорії імовірностей та теорії графів. Баєсівська мережа (БМ) зображується парою <G, B>, де G – це спрямований ациклічний граф, який записується як набір залежностей і відповідає випадковим змінним, а B – представляє собою сукупність параметрів, що означують мережу. Компонента B містить у собі параметри $\Theta_{X^{(i)}|pa(X^i)} = P(X^{(i)}|pa(X^i))$ для кожного можливого значення $x^{(i)} \in X^{(i)}$ та $pa(X^{(i)}) \in Pa(X^{(i)})$, де

$Pa(X^{(i)})$ позначає набір батьків змінної $X^{(i)} \in G$, а кожна змінна $X^{(i)} \in G$ подається у вигляді вершини [21].

Визначення повної спільної ймовірності БМ розраховується за формулою (3.12):

$$P_B\left(X^{(1)}, X^{(2)}, \dots, X^{(N)}\right) = \prod_{i=1}^{n} P_B\left(X^{(i)} | P_A(X^{(i)})\right), \tag{3.12}$$

де A – множина станів середовища;

$N = (x_1, x_2, \dots, x_N)$ – вектор параметрів їх розподілів.

Розрахунок умовної вірогідності відбувається за наступним співвідношенням:

$$p(E|H_k) = \frac{p(E \cap H_k)}{p(H_k)}, \tag{3.13}$$

де E та H_k – співзв'язанні змінні мережі.

Умовна ймовірність визначає вірогідність настання події E , за умови того, що певна подія H_k відбулась. Вичерпна множина формується подіями що взаємовиключають одна одну за умови настання рівності:

$$\bigcup_{i=1}^{n} E_i = \Omega, \tag{3.14}$$

Якщо змінні між собою не мають спільних значень – вони не перетинаються. Теорія побудови БМ базується на припущенні, що події не перетинаються і є вичерпними, у такому випадку вірогідність події E визначаєтья за формулою (3.15) умовних ймовірностей:

$$p(E) = \sum_{i=1}^{n} p(E \cap H_i) \rightarrow \sum_{i=1}^{n} p(E|H_i) * p(H_i), \tag{3.15}$$

Саму ж формулу імовірності перетину двох подій *E* та *H* можна виразити, у наступному вигляді:

$$p(E \cap H_k) = p(E|H_k) * \ p(H_k) = \ p(H_k|E) * \ p(E), \qquad (3.16)$$

Дана формула (3.17) може бути трансформована наступним чином:

$$p(H_k|E) = \frac{p(E|H_{k)} * p(H_k)}{p(E)}, \qquad (3.17)$$

Беручи до уваги формули (3.13) та (3.18), процес обчислення події E можна представити у наступному вигляді:

$$p(H_k|E) = \frac{p(E|H_{k)} * p(H_k)}{\sum_{i=1}^{n} p(E|H_i) * p(H_i)}, \qquad (3.18)$$

Мережа Баєса, сформована на підставі формули (3.18), являє собою спрямований ациклічний граф, де кожен вузол є змінною, а кожна дуга – імовірнісна залежність, зумовлена кількісно використанням умовного розподілу вірогідностей для кожного вузла.

До складу мережі Баєса входять наступні складові:

− сукупність вузлів, що визначають елементи системи;

− сукупність спрямованих зв’язків між елементами системи [26].

У цій праці на підставі інформаційно-логічної моделі (рис. 3.4) для оцінки стану захищеності ОКІ побудована БМД, зображеною на рис.3.5. При формуванні її структури та таблиць умовних вірогідностей використовувались знання експертів.

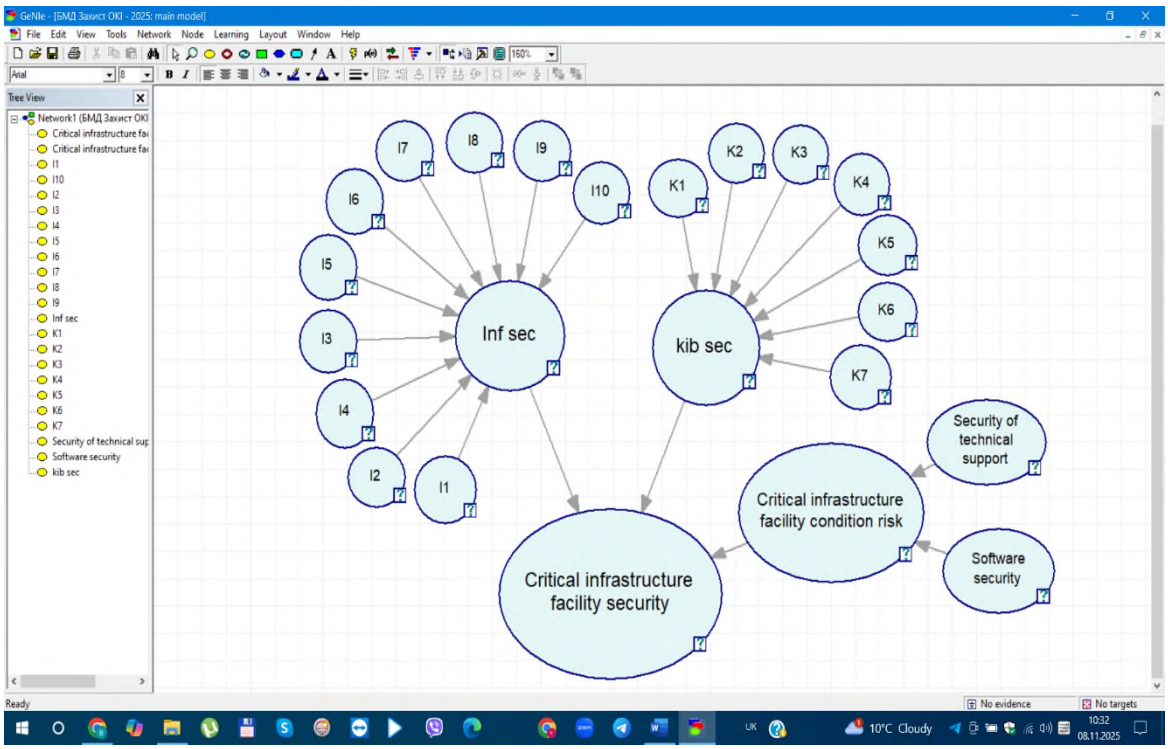

Рисунок 3.5 - Баєсовська мережа довіри оцінки впливу факторів інформаційної та кібербезпеки на стан захищеності об’єкту критичної інфраструктури.

Щоб описати вершини “Informational security” та “Cyber security”, було здійснено дослідження, де експертам-фахівцям запропонували провести оцінку умовних ймовірностей можливих станів чинників впливу на вказані вершини БМД, а саме:

Інформаційна безпека (Informational security) - це стан захисту, обробки та зберігання відомостей, який контролюється та надолужується відповідними програмами - сенсорами:

I 1 – цілісність даних;

I 2 – доступність даних;

I3 – конфіденційність даних;

I4 – узгодженість даних;

I 5 – посилальна цінність;

I6 - відмови апаратного забезпечення;

I7 - відмови програмного забезпечення ;

I8 – некоректні дії користувачів;

I9 - вплив дій адміністраторів;

I10-енергетичні відмови .

Кібербезпека (Cyber security) – це уникнення доступу зламників до систем та відомостей, що може спричинити втрату конфіденційності.

Нагляд та коригування кібернетичної безпеки забезпечується програмами – моніторингу:

К1 - попередньої підстановки у запиті даних та перевірка на SQL - ін'єкції;

К2 – перевірки системи на віруси;

К3 - перевірки входу користувача з правами адміністратора;

К4 – доступності даних та ресурсів;

К5 - перевірки інформації на наявність підміни даних;

К 6 - зо зовнішній вплив;

К7 - перевірки даних на цілісність (використовуючи хеш).

Результати експертних оцінок ймовірностей можливих станів факторів інформаційної (І) та кібербезпеки (К), наведені в таблицях 3.4 та 3.5.

Для зниження трудомісткості заповнення таблиць умовних ймовірностей цим вершин зручно призначити тип Noisy MAX [27]. Використання вершин типу Noisy MAX зручне ще й тому, що експертам значно простіше оцінювати вплив лише одного фактора на очікувану подію, ніж оцінювати спільну дію кількох факторів на неї.

Таблиця 3.4 - Результати експертного оцінювання умовних ймовірностей можливих станів факторів інформаційної безпеки (І).

Вершин	**I1**	**I2**	**I3**	**I4**	**I5**	**I6**	**I7**	**I8**	**I9**	**I10**
Стан										
високий	0,85–1	0,8 - 1	0,75 – 1	0,8 - 1	0,85-1	0,86 – 1	0,76-1	0,9-1	0,7-1	0,85-1
середній	0,4-0,84	0,36-0,79	0,46-0,74	0,46-0,79	0,55-0,84	0,55-0,85	0,41-0,75	0,1-0,9	0,3-0,7	0,1-0,8
низький	0,15-0,39	0,2 -0,35	0,25-0,45	0,15-0,45	0,25-0,54	0,3-0,54	0,25-0,4	0-0,1	0-0,3	0-0,15

Таблиця 3.5 - Результати експертного оцінювання умовних ймовірностей можливих станів факторів кібербезпеки (К).

Вершина	**К1**	**К2**	**К3**	**К4**	**К5**	**К6**	**К7**
Стан	Імовірність захищеності						
Висока	0,95-1	0,9 -1	0,85-1	0,95-1	0,9-1	0,8-1	0,9-1
Середня	0,4-0,95	0,4–0,9	0,4– ,85	0,4–0,9	0,4–0,9	0,4–0,8	0,4–0,9
Низька	0 - 0,4	0 - 0,4	0 - 0,4	0 - 0,4	0 - 0,4	0 - 0,4	0 - 0,4

Щоб описати вершину "Critical infrastructure facility security", було проведене дослідження, де експертам-фахівцям запропонували здійснити оцінку умовних ймовірностей можливих станів згаданої вершини БМД. Результати показані у таблиці 3.6.

Отже, вершина 'Critical infrastructure facility condition risk' набуває значення "occurs", якщо загроза порушення виробничого процесу ОКІ присутня, і "not occurs" у зворотному випадку.

Таблиця 3.6 - Умовні ймовірності вершини "Critical infrastructure facility security"

Батько	Risc		IS		CS	
Стан	occurs	notoccurs	noprotect	protect	noprotect	protect
nosufficient	0,2	0	0,25	0	0,35	0
sufficient	0.8	1	0,75	1	0,65	1

Розглянемо вершину “State of information security”**.**

На випадкову величину “State of information security” надають вплив наступні фактори: I1 – цілісність даних; I2 – доступність даних; I3 – конфіденційність даних; I4 – узгодженість даних; I5 – посилальна цінність; I6 - відмови апаратного забезпечення; I7 - відмови програмного забезпечення; I8 – некоректні дії користувачів; I9 - вплив дій адміністраторів; I10 - енергетичні відмови .

Виникає питання: яка ймовірність того, що випадкова величина “State of information security” приймає значення " negative "?

Для відповіді на це питання пропонується використовувати систему прогнозування значень ймовірностей, в основу якої покладено нечіткий логічний висновок за алгоритмом Мамдані з нечіткої бази знань [28-30], в якій значення вхідних та вихідний змінної задані нечіткими множинами. Враховуючи, що згідно з [25] найбільш значний вплив на стан інформаційної безпеки мають фактори: I1 - цілісність даних; I2 – доступність даних; I3 – конфіденційність даних; I4 – узгодженість даних; I5 – посилальна цінність; I6 - відмови апаратного забезпечення; I7 - відмови програмного забезпечення, експертами пропонується наступна нечітка база знань:

ПРАВИЛО 1: ЯКЩО u_1 *є "НЕ норма" І* u_2 *є " НЕ норма" ТО* v *є "висока"*

ПРАВИЛО 2: ЯКЩО u_2 *є "не норма" І* u_3 *є " не норма" І* u_5 *є "норма" ТО* v *є "висока"*

ПРАВИЛО 3: ЯКЩО u_3 *є "не норма" І* u_5 *є "норма" І* u_6 *є "норма" І* u_7 *є "не норма" ТО* v *є "висока"*

ПРАВИЛО 4: ЯКЩО u_4 *є "не норма" І* u_3 *є "норма" І* u_5 *є "не норма " І* u_7 *є "норма" ТО* v *є "середня"*

ПРАВИЛО 5: ЯКЩО u_1 *є "норма" І* u_3 *є "норма" І* u_4 *є "не норма" І* u_5 *є "не норма" І* u_6 *є "не норма" ТО* v *є "середня"*

ПРАВИЛО 6: ЯКЩО u_2 *є "норма" І* u_3 *є "норма" І* u_4 *є "* u_5*норма" І є "не норма" І* u_6 *є "норма" І* u_7 *є "не норма" ТО* v *є "середня"*

ПРАВИЛО 7: ЯКЩО u_6 *є "не норма" І* u_4 *є "* u_1*норма" І* u_2 *є "норма" І* u_3 *є "норма" І є "норма" І* u_7 *є "норма" ТО* v *є "низька"*

ПРАВИЛО 8: ЯКЩО u_1 *є "норма" І* u_2 *є "* u_3*норма" І* u_4 *є "норма" І* u_5 *є "норма" І є "норма" І* u_6 *є "норма" І* u_7 *є "норма" ТО* v *є "низька"*

Тут через u_i $(i = \overline{1,7})$ позначені лінгвістичні змінні:

u_1 є лінгвістична змінна " Цілісність даних " ;

u_2 є лінгвістична змінна " Доступність даних " ;

u_3 є лінгвістична змінна Конфіденційність даних ;

u_4 є лінгвістична змінна " Узгодженість даних " ;

u_5 є лінгвістична змінна "Посилальна цінність " ;

u_6 є лінгвістична змінна ″Відмови апаратного забезпечення ;

u_7 є лінгвістична змінна "Відмові програмного забезпечення " ;

а через v- лінгвістична змінна ймовірність того, що випадкова величина ″ State of information security ″ приймає значення "negative".

Для опису лінгвістичних змінних u_i $(i = \overline{1,7})$ будемо використовувати терм - безліч {"норма", "не норма" }, а для змінної v −терм - множина {" висока", "середня", "низька"}.

Функції приналежності $\mu_i(x_i)$ терма "норма" лінгвістичних змінних u_i $(i = \overline{1,7})$ задаються у вигляді двосторонньої гауссівської функції:

$$\mu_i(x_i) = gauss2mf(x_i, [\sigma_1^i, c_1^i, \sigma_2^i, c_2^i]) =$$

$$= \begin{cases} e^{-(x_i - c_1^i)^2 / 2(\sigma_1^i)^2}, & если\ 0 \le x_i \le c_1^i, \\ 1, & если\ c_1^i < x_i < c_2^i, \\ e^{-(x_i - c_2^i)^2 / 2(\sigma_2^i)^2}, & если\ c_2^i \le x_i \quad , \end{cases} \qquad (3.19)$$

Де: параметри $\sigma_1^i, \sigma_2^i > 0$; $c_1^i, c_2^i \ge 0$; $c_1^i \le c_2^i$; x_i - Елементи універсальної множини $X = [0;1]$, на якому визначені терми " норма ", " не норма ".

Врахування значень факторів інформаційної безпеки (I) (табл. 3.4) дозволяє визначити деякі із значень параметрів c_1^i, c_2^i, σ_1^i, σ_2^i $(i = \overline{1,7})$. Тоді функції приналежності $\mu_i(x_i)$ можна записати у вигляді:

$$\mu_1(x_1) = gauss2mf(x_1,[1,0,\sigma_2^1,0.3]), \quad x_1 \in [0,1];$$

$$\mu_2(x_2) = gauss2mf(x_2,[1,0,\sigma_2^2,0.25]), \quad x_2 \in [0,1];$$

$$\mu_3(x_3) = gauss2mf(x_3,[\sigma_1^3,0.8,1,1]), \quad x_3 \in [0,1];$$

$$\mu_4(x_4) = gauss2mf(x_4,[\sigma_1^4,0.75,1,1]), \quad x_4 \in [0,1]; \qquad (3.20)$$

$$\mu_5(x_5) = gauss2mf(x_5,[1,0,\sigma_2^5,0.2]), \quad x_5 \in [0,1];$$

$$\mu_6(x_6) = gauss2mf(x_6,[1,0,\sigma_2^6,0.15]), \quad x_6 \in [0,\ 1].$$

$$\mu_7(x_7) = gauss2mf(x_7,[\sigma_1^7,0.76,1,1]), \quad x_7 \in [0,\ 1].$$

Для визначення параметрів σ_1^i, σ_2^i функцій приналежності, які можуть приймати будь-які значення, тоді у формулах (3.20) надається значення 1.

Висловлювання " i-й фактор набуває значення "не норма"" протилежно висловлюванню "і-й фактор iнабуває значення "норма"". Тоді функції приналежності $\varphi_i(x_i)$ терма "не норма" лінгвістичних змінних u_i будуть мати вигляд:

$$\varphi_i(x_i) = 1 - \mu_i(x_i),\ (i = \overline{1,7}).$$

Для функцій приналежності термів "низька", "середня", "висока" лінгвістичної змінної v введемо позначення $\theta_i(y),\ (i = \overline{1,3})$ відповідно, де y - елементи універсальної множини $Y = \{0;1\}$, на якому визначені ці терми.

Функція $\theta_i(y)$ задається у вигляді симетричної функції Гауса:

$$\theta_i(y) = gaussfm(y,[\sigma_i, c_i]) = e^{-(y-c_i)^2/2\sigma_i^2}, \qquad (3.21)$$

де параметри $\sigma_i > 0;\ \ c_i \geq 0,\ (i = \overline{1,3})$.

Нижче наведено характерні графіки функцій приналежності. Графіки функцій $\mu_1(x_1), \varphi_1(x_1), \mu_2(x_2), \varphi_2(x_2), \mu_5(x_5), \varphi_5(x_5), \mu_6(x_6), \varphi_6(x_6)$ мають вигляд графіків на рис.3.6. Графіки функцій $\mu_1(x_1), \varphi_1(x_1), \mu_2(x_2), \varphi_2(x_2), \mu_5(x_5), \varphi_5(x_5)$ того ж виду як на рис.3.7.

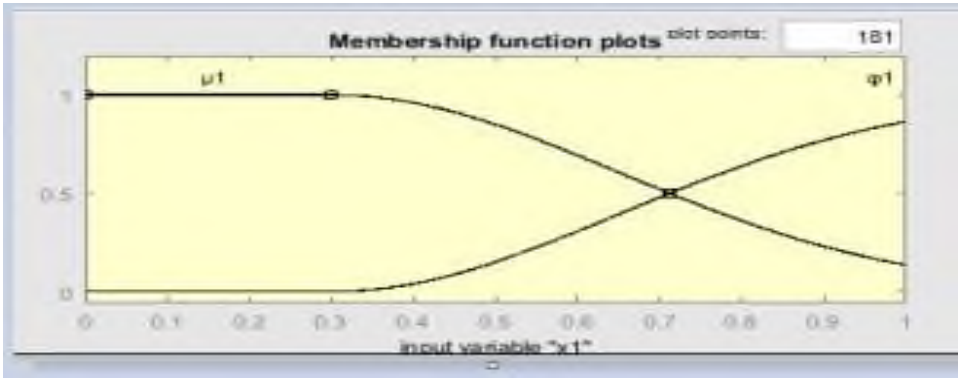

Рисунок 3.6 - Функції приналежності $\mu_1(x_1)$ та $\varphi_1(x_1)$

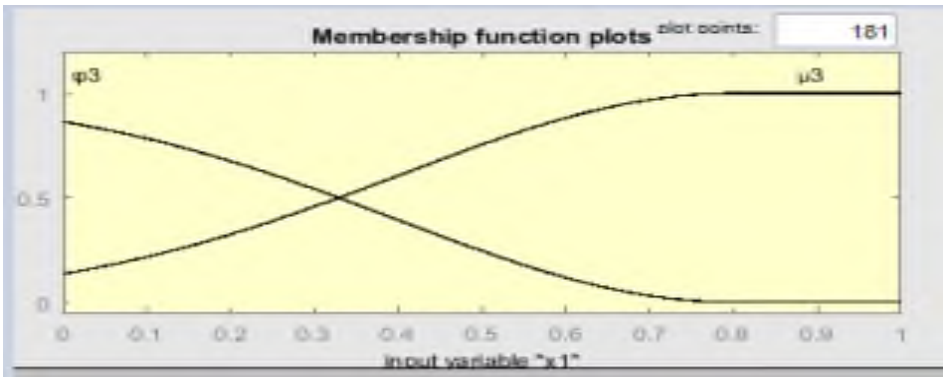

Рисунок 3.7 - Функції приналежності $\mu_3(x_3)$ та $\varphi_3(x_3)$

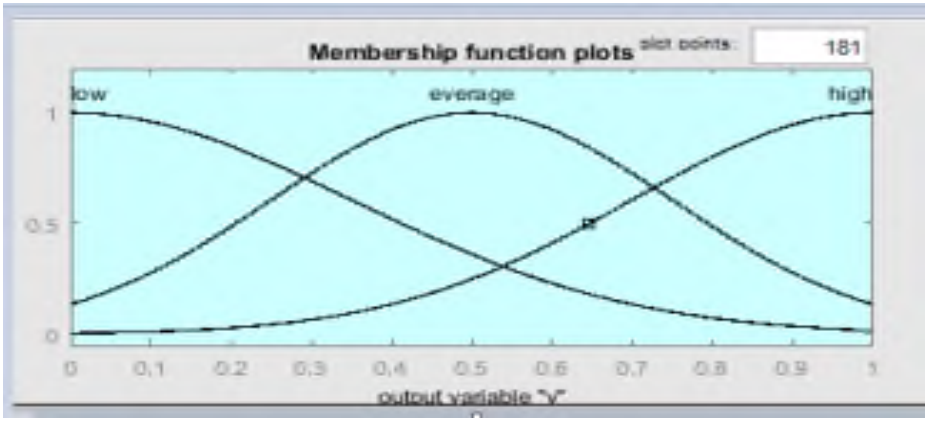

Рисунок 3.8 - Функції приналежності $\theta_i(y) \quad (i = \overline{1,3})$

Для налаштування нечіткої моделі **F**, тобто. визначення коефіцієнтів моделі $\sigma_2^1, \sigma_2^2, \sigma_2^5, \sigma_2^6, \sigma_1^3, \sigma_1^4, \sigma_1^7$; σ_j, c_j, $(j = \overline{1,3})$, потрібно [24], щоб значення середньоквадратичної нев'язки R було мінімальним:

$$R = \frac{1}{n}\sum_{k=1}^{n}(y_k - \mathbf{F}(P, E_k))^2 \to \min . \qquad (3.22)$$

Тут n - Обсяг вибірки експериментальних даних, що зв'язують входи $E = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$ з виходом y досліджуваної залежності:

$$(E_k, y_k),\ k = \overline{1,n},$$

де: $E_k = (x_{k,1}, x_{k,2}, x_{k,3}, x_{k,4}, x_{k,5}, x_{k,6}, x_{k,7})$ - вектор входів і y_k - вихід в k - парі.

Крім того, $\mathbf{F}(P, E_k)$ значення виходу нечіткої моделі при значенні входів, заданих E_k вектором ; $P = (\sigma_1^i, \sigma_2^i, \sigma_j, c_j)$ - вектор коефіцієнтів функцій приналежності термів вхідних і вихідний змінних нечіткої моделі. Облік знання експертів щодо впливу факторів інформаційної безпеки на стан Інформаційної безпеки об'єкту критичної інфраструктури дозволяє знайти за допомогою пакетів **Fuzzy Logic Toolbox** та **Optimization Toolbox** рішення завдання математичного програмування (24) і таким чином налаштувати нечітку модель.

3.4 Практична реалізація результатів дослідження захищеності об’єкту критичної інфраструктури з застосуванням імовірнісного методу Баєсових мереж довіри.

У цьому розділі для перевірки чинності результатів дослідження проведено експеримент оцінки міри захищеності об’єкта критичної інфраструктури із застосуванням імовірнісного методу Баєсових мереж

довіри. Нехай стан захищеності ОКІ на даний час оцінюється ймовірністю 90%. При першому експерименті проведемо оцінку захищеності ОКІ у випадках коли стани факторів Інформаційної безпеки: І1 - цілісність даних; І2 – доступність даних; І3 – конфіденційність даних, мають стан захищеності 90%, а стан захищеності вузлів: І4 – узгодженість даних, І5 – посилальна цінність; І6 - відмови апаратного забезпечення; І7 - відмови програмного забезпечення, перебувають у станах: ″низька захищеність″. Результати обчислень зображено на рисунку 3.9

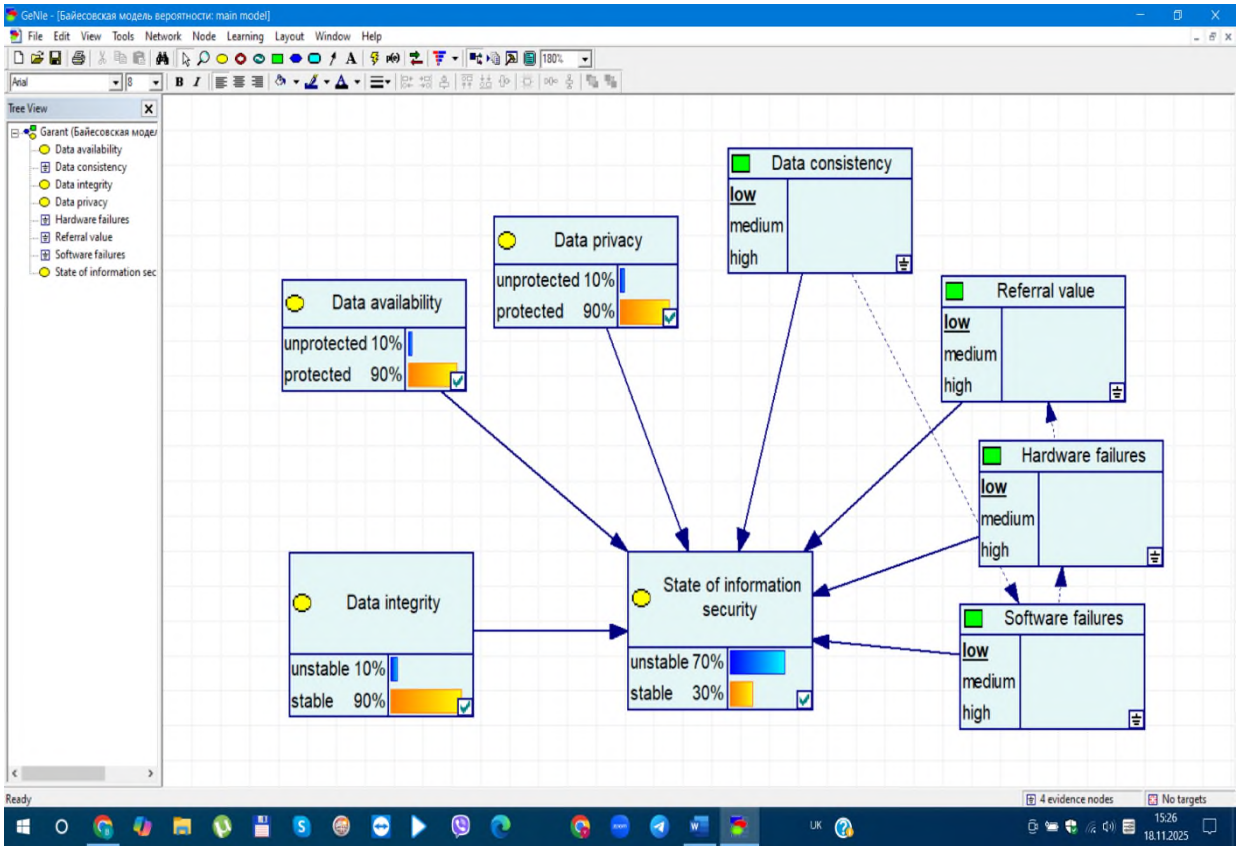

Рисунок 3.9 – Імовірність стану захищеності ОКІ при низькій захищеності вузлів І4, І5, І6, І7.

При другому експерименті стани захищеності Інформаційної безпеки: І1 - цілісність даних; І2 – доступність даних; І3 – конфіденційність даних, мають стан захищеності 90%, а стан захищеності вузлів: І4 – узгодженість даних, І5 – посилальна цінність; І6 - відмови апаратного забезпечення;

I7 - відмови програмного забезпечення, перебувають у станах: ″середня захищеність″. Результати обчислень зображено на рисунку 3.10.

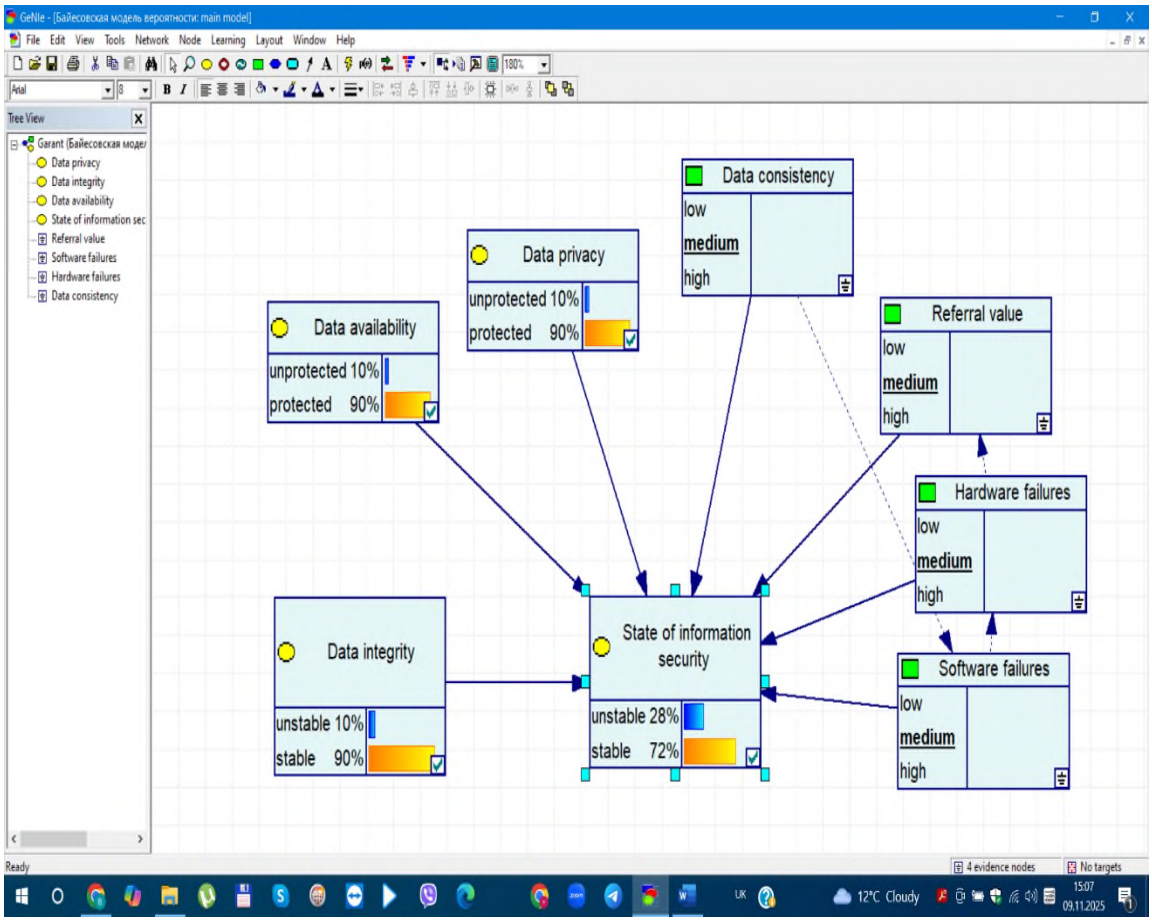

Рисунок 3.10 – Імовірність стану захищеності ОКІ при середній захищеності вузлів I4, I5, I6, I7.

При третьому експерименті стани захищеності Інформаційної безпеки: I1 - цілісність даних; I2 – доступність даних; I3 – конфіденційність даних, мають стан захищеності 90%, а стан захищеності вузлів: I4 – узгодженість даних, I5 – посилальна цінність; I6 - відмови апаратного забезпечення; I7 - відмови програмного забезпечення, перебувають у станах: ″висока захищеність″. Результати обчислень зображено на рисунку 3.11.

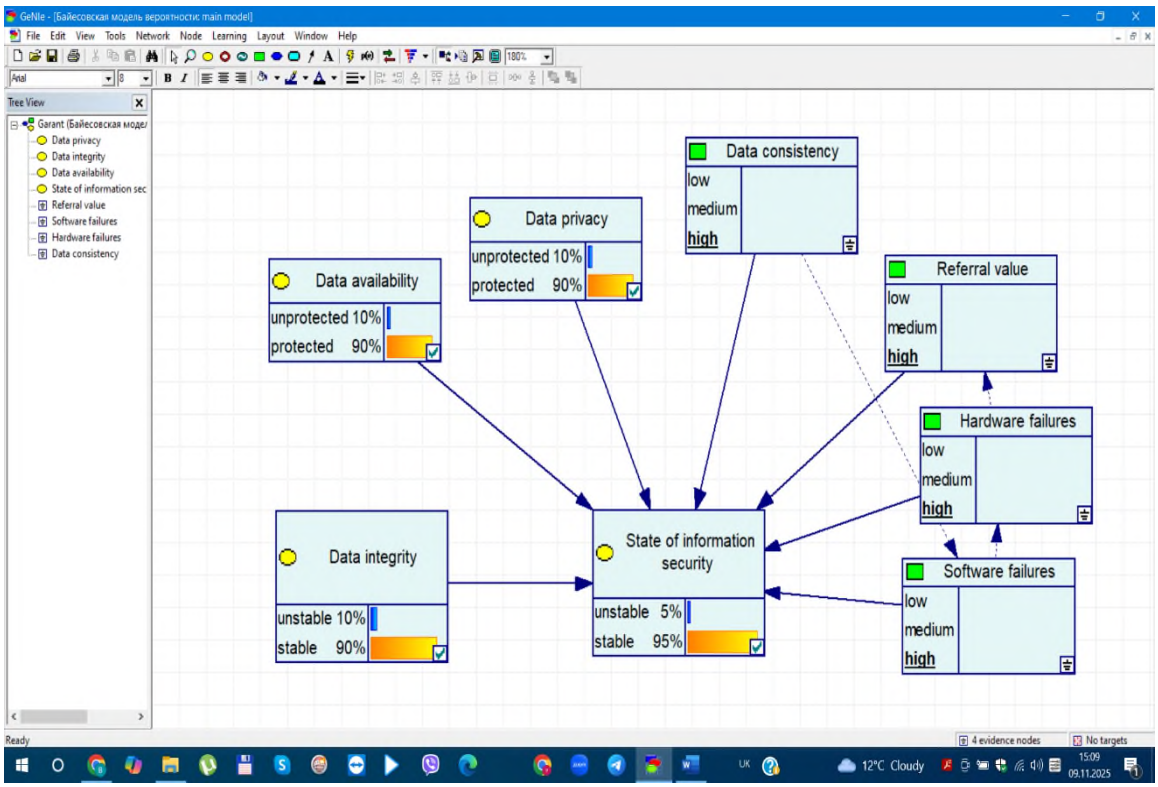

Рисунок 3.11 – Імовірність стану захищеності ОКІ при високій захищеності вузлів I4, I5, I6, I7.

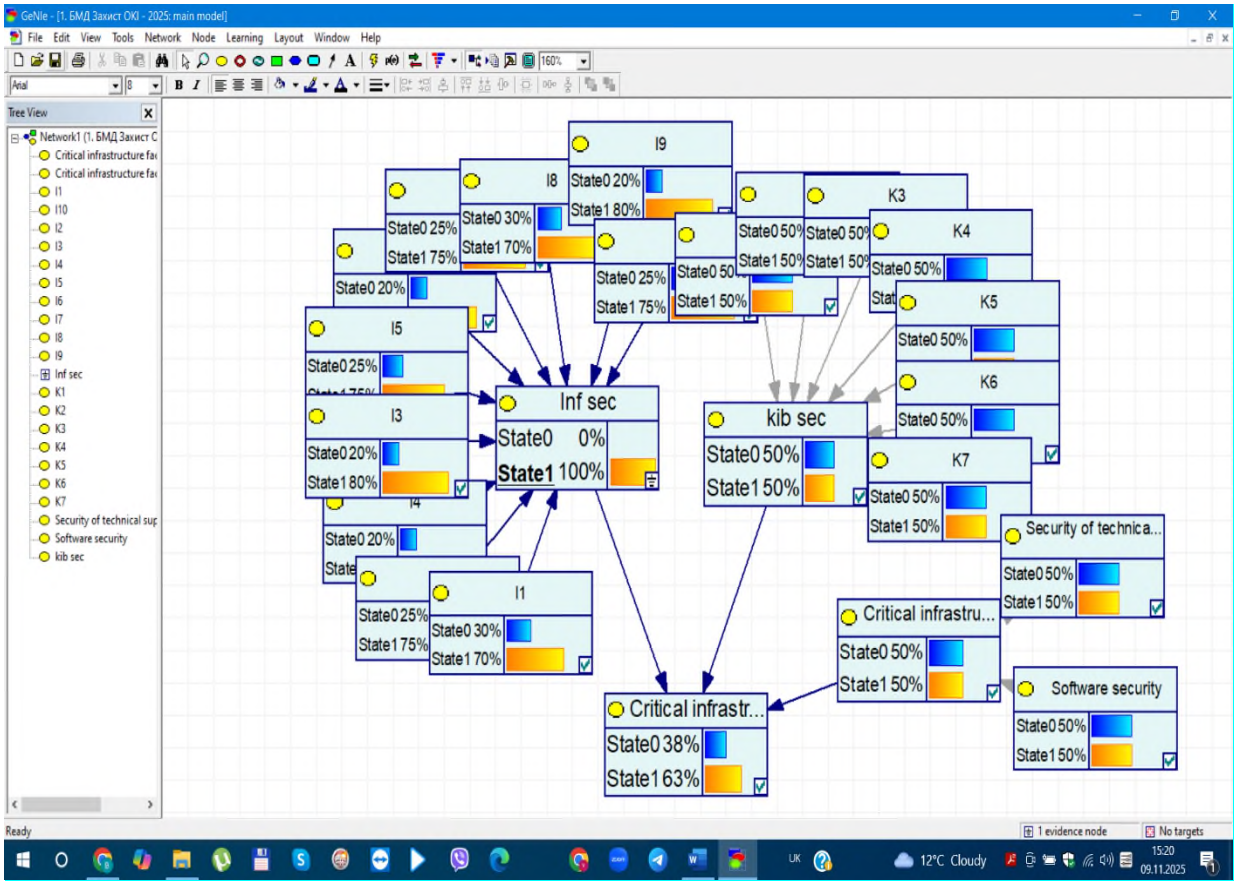

Рисунок 3.12 – Загальна ймовірність стану захищеності ОКІ при різних станах впливових факторах.

Якщо вузли I4, I5, I6, I7 знаходяться в стані "низька захищеність", і "середня захищеність" то ймовірність того, що система знаходиться в стані "стабільна" дорівнює 30% і 72% відповідно (рис.3.9, 3.10).

У відповідності до нормативних джерел для ОКІ 2,3,4 категорії критичності значення ймовірності стану захищеності менше 90% є не прийнятним. Оскільки ці значення менше 90%, то ОКІ вважати захищеним не можна. У цих випадках необхідно усунути небезпеку, на яку вказують результати сканування секторів модулів контролю та моніторингу: зараження системи вірусами; неузгодженість даних; недостатня посилальна цінність; енергетичні відмови, доступності даних та ресурсів, перевірки інформації на наявність підміни даних, зовнішній вплив.

Якщо вузли I4, I5, I6, I7 знаходяться в стані "висока захищеність", то ймовірність того, що система знаходиться в стані "стабільна" дорівнює 95% (рис.3.11). Отже, ОКІ вважається захищеним.

Висновки до третього розділу.

У даному розділі для визначення рівня захищеності об’єкта критичної інфраструктури від факторів Інформаційної та кібербезпеки розроблено інформаційну та інформаційно – логічну моделі. Для оцінювання стану безпеки використано імовірнісний метод та побудована Баєсовська мережа довіри.

Для прогнозування рівня безпекового стану критичного об’єкту побудована нечітка База знань з застосуванням знань експертів та теорії нечітких множин та проведено ряд експериментів що підтвердили ефективність даного методу.

ВИСНОВКИ

У магістерській роботі досліджувалась нагальна проблема залежності захищеності об'єкта критичної інфраструктури від чинників, що мають високий ступінь невизначеності, складність суворого формалізування та є суб'єктивними.

У роботі досліджені проблемні питання оцінювання стану захисту об'єктів критичної інфраструктури, проведено аналіз та окреслено головні чинники загроз, які впливають на стійкість об'єктів. Здійснено детальний аналіз сучасних підходів і методів оцінки та підтримання захищеності об'єктів критичної інфраструктури.

Для визначення рівня захищеності об’єкта критичної інфраструктури від факторів Інформаційної та кібербезпеки розроблено інформаційну та інформаційно – логічну моделі для оцінювання стану безпеки з використанням імовірнісного методу Баєсовських мереж довіри. Для прогнозування рівня безпекового стану критичного об’єкту побудована нечітка База знань з застосуванням знань експертів та теорії нечітких множин. В процесі дослідження залежності захищеності об’єкту критичної інфраструктури від впливу факторів Інформаційної та кібербезпеки використовувались системний аналіз, графо-аналітичні методи Байесовської мережі довіри та теорія експертних оцінок.

Застосування сукупності теоретичних і практичних засад розробки та досліджень надасть змогу вирішення завдань з оцінювання захищеності об’єкту критичної інфраструктури, залежно від чинників, що мають високий ступінь невизначеності, складність суворого формалізування та є суб'єктивними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон «Про критичну інфраструктуру» від 16.11.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/1882-20

2. Закон України Про національну безпеку України Форма доступу - https://zakon.rada.gov.ua/laws/show/2469-VIII

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України; Стратегія від 26.08.2021 Форма доступу - https://www.president.gov.ua/documents/4472021-40013

4. Закон України "Про основи національної безпеки України" 19 червня 2003 року № 964-IV. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text

5. Закон України "Про основні засади забезпечення кібербезпеки України" 5 жовтня 2017 року № 2163- VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

6. Указ Президента України. Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року "Про Стратегію забезпечення державної безпеки". 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#Text

7. Гордієнко С.Г., Доронін І.М. (2024). Інформаційно-правові аспекти захисту критичної інфраструктури України. Інформація і Право. № 3(50). С. 115-123. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311678.

8. Суходоля О. (2023). Стійкість критичної інфраструктури ЄС: посилення політики та координації. НІСД, 9 с. URL: https://niss.gov.ua/sites/default/files/2023-02/az_eu-cip-coordinated_24022023.pdf

9. Cyber defence. (30 Jul. 2024). NATO. URL: https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en

10. Гончар С. Аналіз факторів впливу на стан кібербезпеки інформаційної системи об’єкту критичної інфраструктури / Гончар С., Леоненко Г. //

Information Technology and Security. – 2016. – Vol. 4, Iss. 2 (7). – Pp. 262-268. – Bibliogr.: 5 ref.

11. Шевченко, С., Жданова, Ю., Спасітєлєва , С., Мазур, Н., Складанний , П., & Негоденко, В. (2024). Математичні методи в кібербезпеці: кластерний аналіз та його застосування в інформаційній та кібернетичній безпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(23), 258–273. https://doi.org/10.28925/2663-4023.2024.23.258273

12. Яременко О.І., Страхніцький Я.І. (2022). Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. Публічне управління та митне адміністрування. № 1. С. 76-82. URL: http://customs-admin.umsf.in.ua/archive/2022/1/13.

13. Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crisis Management, Vol. 15. No. 1. Pp. 50-59. DOI: https://doi.org/10.1111/j.1468-5973.2007.00504.x

14. Guidotti, R., Chmielewski, H., Unnikrishnan, V., Gardoni, P., McAllister, T., & van de Lindt, J. (2016). Modeling the resilience of critical infrastructure: the role of network dependencies. Sustainable and Resilient Infrastructure, Vol. 1. No. 3–4. Pp. 153–168. DOI: https://doi.org/10.1080/23789689.2016.1254999

15. Sellevåg, Stig Rune. (2022). "Abstraction-decomposition space for critical infrastructure systems: A framework for infrastructure planning and resilience policies." Security and Defence Quarterly, Vol. 39. No. 3. Pp. 6-20. DOI: https://doi.org/10.35467/sdq.

16. Ленков, С.В. Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів / С.В. Лєнков, В.М. Джулій, А.М. Берназ, І.В. Муляр, І.В. Пампуха // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2023. – Вип. №78. – С. 123-134

17. Бурячок, В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко – К.: ДУТ, 2015р. – 288 с

18. Технічний GDPR: 5 цікавих аспектів - URL: https://legalitgroup.com/tehnichnij-gdpr-5-tsikavih-aspektiv/

19. Jouffe L. New search strategies for learning Bayesian networks / Jouffe L. and Munteanu P. // Proc. of tenth international symposium on applied stochastic models and data analysis (ASMDA 2001). – Compiegne (France). 12 – 15 June 2001. – Vol. 2. – P. 591-596

20. Баєсова мережа - URL:https://www.wikidata.ukua.nina.az/%D0%91%D0%B0%D1%94%D1%81%D0%BE%D0%B2%D0%B0_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C.html

21. Баєсова мережа - URL:https://www.wikiwand.com/uk/%D0%91%D0%B0%D1%94%D1%81%D0%BE%D0%B2%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0

22. Коефіцієнт кореляції рангу Кендала - URL:

https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%B5%D1%84%D1%96%D1%86%D1%96%D1%94%D0%BD%D1%82_%D0%BA%D0%BE%D1%80%D0%B5%D0%BB%D1%8F%D1%86%D1%96%D1%97_%D1%80%D0%B0%D0%BD%D0%B3%D1%83_%D0%9A%D0%B5%D0%BD%D0%B4%D0%B0%81D0%BB%D0%B0

23. Суходоля О.М., Харазішвілі Ю.М., Бобро Д.Г., Сменковський А.Ю., Рябцев Г.Л., Завгородня С.П. (2020). Енергетична безпека України: методологія системного аналізу та стратегічного планування. 178 с. URL: https://niss.gov.ua/sites/default/files/2020-12/sukhodolia_energy_security_sayt-1.pdf

24. Концептуальна модель - URL:https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C

25. Логічна модель даних -

URL:https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%B3%D1%96%D1%87%D0%BD%D0%B0_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85

26. Murphy K. A brief introduction to graphical models and Bayesian networks / Technical report 2001-5-10, departament of computer science, University of British Columbia, Canada, May 2001. - 19 p.

27. Perederyi V., Borchik Eu., Ohnieva O. Information Technology for Decision Making Support and Monitoring in Man-Machine Systems for Managing Complex Technical Objects of Critical Application, Advances in Intelligent Systems and Computing, 2021, Vol. 1246, pp. 448–466. DOI: 10.1007/978-3/

28. Perederyi V., Borchik Eu., Lytvynenko V., Ohnieva O. Information Technology for Performance Assessment of Complex Multilevel Systems in Managing Technogenic Objects.CEUR Workshop Proceedings, 2020, Vol. 2805, pp. 175-188.

29. Perederyi V., Borchik, Eu., Wójcik W., Ohnieva O. Assessment and Information Security Provision of the Decision Support Process in Technogenic Object Management Systems. CEUR Workshop Proceedings, 2021, Vol. 3101, pp. 322–334.

30. Evaluation of the influence of environmental factors and cognitive parameters on the decision-making process in human-machine systems of critical application / [V. I. Perederyi, E. Y. Borchik, V. V. Zosimov, O. S. Bulgakova,] // Radio Electronics, Computer Science, Control. - 2024. - № 1 – P. 77-84. DOI 10.15588/1607-3274-2024-1-7.