**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 ЗАЛЕЖНОСТІ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕНЬ ВІД СТАНУ ЗАХИЩЕНОСТІ ОБ'ЄКТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ, З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-КОГНІТИВНИХ ТЕХНОЛОГІЙ

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
Глухов Микита Олегович _____

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: Глухов Микита Олегович

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 залежності процесу прийняття рішень від стану захищеності об'єкту критичної інфраструктури, з використанням інформаційно-когнітивних технологій
затверджена наказом НУК від «14» 10 2025 р. № 1217-ч

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

1.Провести аналіз сучасних способів і методів визначення впливу основних факторів загроз на процес прийняття рішень при управлінні об'єктом критичної інфраструктури

2. Розробити математичну модель оцінювання впливу основних факторів загроз на процес прийняття рішень при управлінні об'єктом критичної інфраструктури.

3.Провести експерименти з оцінки впливу факторів вразливостей на процес прийняття рішень при управлінні об'єктом критичної інфраструктури.

4. Терміни виконання завдання:

термін видачі завдання: «01- 05» вересня 2025 р.

термін подання роботи: «18 » грудня 2025 р.

6. План-графік виконання кваліфікаційної роботи

| п/п | Заходи | Дата | | Готовність |
|---|---|---|---|---|
| | | Навч. тиждень | Контрольна дата | |
| 1. | Наукове стажування | 1 - 8 | 27.10.2025 | Звіт з наукового стажування |
| 2. | Організаційні збори | 9 | 29.10.2025 | Попередній варіант змісту КР |
| 3. | Рубіжний контроль | 10 | 05.11.2025 | Попередній варіант оглядових розділів, звіт з практика |
| 4. | Рубіжний контроль | 13 | 27-28.11.2025 | Доповідь на 13-ій Всеукраїнській науково-технічній конференції з міжнародною участю «СПІБТ–2025» |
| 5. | Рубіжний контроль | 14 | 3.12.2025 | 1. Попередній варіант повної КР<br>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.<br>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.<br>2. Зовнішня рецензія (окремо від КР). Резюме на КР.<br>3. Електронний варіант презентації.<br>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<br>2. Процедура захисту КР. |

Керівник професор, професор кафедри комп'ютерних технологій

д.т.н., інформаційної безпеки,_____ В.І. Передерій

та

Студент М.О. Глухов

# АНОТАЦІЯ

У магістерській кваліфікаційній роботі досліджувалася актуальна проблема вирішення задач дослідження залежності процесу прийняття рішень від стану захищеності об’єкту критичної інфраструктури, з використанням інформаційно-когнітивних технологій.

Проаналізовано основні особливості процесу прийняття рішень в управлінні об’єктом критичної інфраструктури. Встановлено, що даний процес має системний, багаторівневий і динамічний характер та формується під впливом комплексу технічних, організаційних, інформаційних і когнітивних факторів. Показано, що стан захищеності об’єкта виступає ключовим інтегральним показником, який визначає допустимі сценарії управління, рівень ризику та характер управлінських дій. Обґрунтовано необхідність урахування зворотних зв’язків між прийнятими рішеннями та подальшою зміною стану захищеності об’єкта критичної інфраструктури.

Здійснено аналіз сучасних методів та способів дослідження процесу прийняття рішень в управлінні об’єктом критичної інфраструктури. Проаналізовано імовірнісні, нечіткі, мультикритеріальні, імітаційні та гібридні методи, а також встановлено доцільність їх інтеграції в межах єдиного методологічного підходу.

Обґрунтовано застосування методів інформаційно-когнітивних технологій для оцінки залежності процесу прийняття рішень від стану захищеності об’єкта критичної інфраструктури. Розроблено інформаційно-когнітивну модель, яка дозволяє формалізувати вплив основних факторів загроз на стан захищеності та відобразити механізм трансформації інформації про цей стан у управлінські рішення.

Ключові слова: об’єкт критичної інфраструктури, інформаційно-когнітивні технології, процес прийняття рішень, стан захищеності, інформаційна безпека, кібербезпека, математичне моделювання.

## ABSTRACT

In the master's qualification work, an actual problem of solving research tasks related to the dependence of the decision-making process on the security state of a critical infrastructure object using information-cognitive technologies was investigated.

The main features of the decision-making process in the management of critical infrastructure objects were analyzed. It was established that this process has a systemic, multilevel, and dynamic nature and is formed under the influence of a complex of technical, organizational, informational, and cognitive factors. It was shown that the security state of the object acts as a key integral indicator that determines admissible management scenarios, the level of risk, and the nature of managerial actions. The necessity of considering feedback between the decisions made and subsequent changes in the security state of the critical infrastructure object was substantiated.

An analysis of modern methods and approaches to studying the decision-making process in the management of critical infrastructure objects was conductedProbabilistic, fuzzy, multicriteria, simulation, and hybrid methods were analyzed, and the expediency of their integration within a unified methodological framework was established.

The application of information-cognitive technology methods for assessing the dependence of the decision-making process on the security state of a critical infrastructure object was substantiated. An information-cognitive model was developed that allows formalizing the influence of the main threat factors on the security state and representing the mechanism of transforming information about this state into managerial decisions.


Keywords: critical infrastructure facility, information and cognitive technologies, decision-making process, state of security, information security, cyber security, mathematical modeling.

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ОКІІ – об’єкт критичної інформаційної інфраструктури; ПЗ – програмне забезпечення;

ОПР – Особа, що приймає рішення. DDoS – Distributed Denial of Service WEB – Всесвітня мережа.

ІБ – Інформаційна безпека. КБ – Кібербезпека.

IDS – Система виявлення вторгнень (Intrusion Detection System). IPS – Система запобігання вторгнень (Intrusion Prevention System).

SSL/TLS – Протоколи захисту з'єднання (Secure Sockets Layer / Transport Layer Security).

AES – Стандарт шифрування даних (Advanced Encryption Standard). RSA – Криптографічний алгоритм (Rivest–Shamir–Adleman).

HTTP/HTTPS – Протоколи передачі гіпертексту (Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure).

БМД – Байсовська мережа довіри

СППР – Система підтримки прийняття рішень

СС-система – Слабоструктурована система

ІКТ – інформаційно-когнітивні технології

# ЗМІСТ

# ВСТУП

Сучасні умови функціонування об’єктів критичної інфраструктури визначаються зростанням масштабів, інтенсивності та складності кіберзагроз, спрямованих на порушення сталості, безпечності та керованості технологічних процесів. Кіберпростір стає ключовим полем протиборства, а системи управління критичними інфраструктурними об’єктами — однією з головних мішеней для технічно складних і багатоступеневих атак, здатних спричинити серйозні економічні, екологічні та соціальні наслідки. За останні роки зросла кількість інцидентів, що прямо чи опосередковано впливають на процеси прийняття рішень в системах управління ОКІ, зумовлюючи необхідність глибокого наукового аналізу залежностей між станом їх кіберзахищеності та якістю управлінських рішень.

Процес прийняття рішень в управлінні об’єктами критичної інфраструктури є складною багатофакторною системою, на яку впливають технічні, організаційні, інформаційні та когнітивні чинники. Істотний вплив на цей процес мають саме кібернетичні загрози, оскільки вони можуть не лише порушувати функціонування технологічних систем та засобів зв’язку, а й спотворювати інформацію, знижувати рівень її достовірності, ускладнювати прогнозування подій та моделювання потенційних сценаріїв розвитку ситуацій. Це, у свою чергу, призводить до погіршення якості управлінських рішень, підвищення рівня ризику та зростання ймовірності виникнення критичних аварійних або кризових ситуацій.

Водночас в умовах високої невизначеності та швидкоплинності кіберзагроз актуальним стає застосування сучасних інформаційно-когнітивних технологій, здатних забезпечити інтегральний аналіз взаємодії факторів загроз, врахування когнітивних залежностей між ними, а також формування моделей, що дозволяють прогнозувати зміну стану захищеності ОКІ та його вплив на процес прийняття рішень. Когнітивне моделювання, інтелектуальний аналіз даних, методи побудови причинно-наслідкових графів, технології адаптивного

контролю та ситуаційного управління дають можливість отримати нові наукові результати щодо структури та динаміки залежностей між факторами кіберзахисту та якістю управлінських рішень.

***Актуальність теми**:* сучасні методи кіберзахисту, хоч і забезпечують достатній рівень безпеки окремих компонентів, недостатньо враховують їхній інтегрований вплив на процеси управління та прийняття рішень у системах критичної інфраструктури. Як показує аналіз інцидентів у сфері кібербезпеки, найбільшу небезпеку становлять саме комплексні атаки, що порушують когнітивну цілісність даних, спотворюють інформаційні потоки та зменшують рівень ситуаційної обізнаності операторів та автоматизованих систем. Через це виникає потреба у створенні методологічно нових моделей, здатних оцінювати не лише безпосередні ефекти атак, а й їхній побічний вплив на управлінські рішення. В зв'язку з цим, даний напрям дослідження є актуальним.

***Мета дослідження.*** Метою магістерської роботи є створення інформаційно-когнітивної моделі, що дозволяє оцінювати залежність процесу прийняття рішень в управлінні об'єктом критичної інфраструктури від його стану захищеності

***Завдання дослідження:***

- Визначити основні особливості процесу прийняття ріщень в управлінні об'єктом критичної інфраструктури.
- Провести аналіз сучасних методів та способів дослідження процесу прийняття рішень в управлінні об'єктом критичної інфраструктури.
- Застосувати методи інформаційно-когнітивних технологій оцінки залежності процесу прийняття рішень від стану захищеності об'єкту критичної інфраструктури.

***Об'єкт дослідження**:* процес прийняття рішень в системі управління об'єктом критичної інфраструктури.

***Предмет дослідження**:* Залежність процесу прийняття рішень від стану захищеності об'єкта критичної інфраструктури та її формалізація засобами інформаційно-когнітивного моделювання.

***Методи дослідження**:*

Системний аналіз, графо-аналітичні методи Байесовської мережі довіри, теорія експертних оцінок, інформаційно-когнітивні технології.

***Наукова новизна одержаних результатів**:* Розроблена модель оцінювання залежності процесу прийняття ріщень від стану захищеності ОКІ із застосуванням інформаційно-когнітивної технології.

***Очікуваний результат**:* Результати дослідження нададуть можливість вирішення задач з оцінки залежності процесу прийняття рішень від стану захищеності об’єкту критичної інфраструктури, з використанням інформаційно-когнітивних технологій.

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 та аналізу на реальних ОКІІ.

# 1. ОСНОВНІ ОСОБЛИВОСТІ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ОБ'ЄКТОМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 1.1 Роль і значення математичних методів та моделей в дослідженні процесу прийняття рішень при управлінні об'єктом критичної інфраструктури

Дослідження процесу прийняття рішень при управлінні об'єктами критичної інфраструктури потребує використання науково обґрунтованих інструментів аналізу, здатних адекватно відобразити складність, багатофакторність та динамічність таких систем. У цьому контексті математичні методи та моделі відіграють ключову роль, оскільки забезпечують формалізацію управлінських процесів, підвищують об'єктивність аналізу та створюють основу для розроблення ефективних механізмів підтримки прийняття рішень.

Насамперед математичні методи дозволяють представити об'єкт критичної інфраструктури як складну систему зі взаємопов'язаними елементами, що функціонують у умовах дії внутрішніх і зовнішніх загроз. Формалізація таких систем у вигляді математичних моделей дає змогу описати структурні та функціональні зв'язки між компонентами об'єкта, параметрами його стану та управлінськими впливами. Це забезпечує можливість переходу від інтуїтивного управління до системного аналізу, заснованого на кількісних показниках.

Важливе значення математичні методи мають у дослідженні залежності процесу прийняття рішень від стану захищеності об'єкта критичної інфраструктури. За допомогою моделей ризику, оптимізації та теорії систем можна кількісно оцінювати вплив загроз і вразливостей на функціонування об'єкта та визначати допустимі межі управлінських рішень. Це дозволяє обґрунтовувати вибір стратегій управління з урахуванням рівня безпеки та можливих наслідків реалізації негативних сценаріїв.

Особливу роль математичні методи відіграють у підтримці прийняття рішень в умовах невизначеності та неповноти інформації, що є характерними для управління об’єктами критичної інфраструктури. Застосування ймовірнісних моделей, методів статистичного аналізу, теорії нечітких множин та байєсівських підходів дозволяє враховувати стохастичний характер загроз і неточність вхідних даних. Це сприяє зниженню рівня суб’єктивності управлінських рішень і підвищенню їхньої стійкості до зміни умов функціонування об’єкта.

Суттєвим аспектом є використання математичних моделей для сценарного аналізу та прогнозування розвитку ситуацій. Імітаційне моделювання, динамічні та когнітивні моделі дають змогу досліджувати можливі варіанти розвитку подій залежно від різних управлінських впливів і рівня захищеності об’єкта. Такий підхід дозволяє оцінювати довгострокові наслідки рішень, своєчасно виявляти потенційні кризові стани та формувати превентивні заходи управління.

Не менш важливою є роль математичних методів у задачах оптимізації управлінських рішень. Методи лінійного та нелінійного програмування, багатокритеріальної оптимізації та теорії прийняття рішень дозволяють обирати найкращі альтернативи з урахуванням обмежених ресурсів, суперечливих цілей та вимог до рівня безпеки. У контексті управління об’єктами критичної інфраструктури це має особливе значення, оскільки дозволяє досягати балансу між ефективністю функціонування та забезпеченням належного рівня захищеності.

Крім того, математичні моделі забезпечують можливість аналізу зворотного зв’язку між прийнятими управлінськими рішеннями та зміною стану захищеності об’єкта. Дослідження таких динамічних залежностей дає змогу розглядати процес управління як безперервний цикл, у якому кожне рішення формує нові умови для подальших управлінських дій. Це створює підґрунтя для побудови адаптивних систем управління, здатних реагувати на зміну загрозового середовища в режимі реального часу.

Роль і значення математичних методів та моделей у дослідженні процесу прийняття рішень при управлінні об’єктом критичної інфраструктури полягають у забезпеченні наукової обґрунтованості, системності та прогнозованості управлінських рішень. Їх застосування сприяє підвищенню ефективності управління, зниженню ризиків та забезпеченню стійкого і безпечного функціонування критично важливих об’єктів у складних і невизначених умовах.

Математичні методи та моделі відіграють центральну роль у дослідженні процесів прийняття рішень на ОКІ, оскільки вони дозволяють:

- формалізувати складні багатофакторні процеси,
- виявляти приховані закономірності та залежності,
- моделювати динаміку об’єкта в умовах кібер- і фізичних загроз,
- прогнозувати наслідки управлінських дій,
- оцінювати ефективність різних стратегій управління.

Управління ОКІ має стохастичний характер через багатофакторність та невизначеність середовища. Тому математичне моделювання забезпечує:

- системний підхід до аналізу загроз;
- об'єктивність оцінювання ризиків;
- обґрунтованість рішень;
- оптимізацію розподілу ресурсів;
- можливість симуляційного прогнозування.

До ключових математичних інструментів належать:

- теорія графів;
- когнітивне моделювання;
- системна динаміка;
- стохастичні процеси;
- теорія прийняття рішень;
- моделі ризиків та надійності;
- багатокритеріальні методи;

- модельно-орієнтовані методи прогнозування


Рисунок 1.1 – Узагальнена схема процесу прийняття рішень в управлінні ОКІ

Ця схема ілюструє багаторівневу структуру, у межах якої відбувається обробка даних, аналіз загроз, оцінка ризиків та вироблення управлінських рішень.

Роль математичних моделей у контексті кібер-фізичних загроз

Особливе значення математичні моделі мають у комплексному аналізі кібер-фізичних загроз, коли:

- кібератака змінює параметри технологічного процесу,
- фізичний вплив створює додаткові відмови,

- система має забезпечити керованість навіть у разі комбінованих атак.

Для цього застосовують:

- моделі стійкості кібер-фізичних систем,
- моделі когнітивної взаємодії факторів загроз,
- моделі прогнозування станів об’єкта,
- моделі оцінки достовірності інформації.

Використання таких моделей дозволяє оцінити зміни:

- швидкості прийняття рішень,
- точності та достовірності даних,
- надійності дій операторів,
- стійкості алгоритмів автоматичного управління.

## 1.2 Основні особливості застосування інформаційно-когнітивних технологій в дослідженні процесу прийняття рішень при управлінні об’єктом критичної інфраструктури.

Процес прийняття рішень при управлінні об’єктами критичної інфраструктури характеризується високим рівнем складності, багатофакторністю та динамічністю, що зумовлює необхідність застосування сучасних інформаційно-когнітивних технологій. Такі технології забезпечують можливість системного дослідження управлінських процесів у середовищі, де на функціонування об’єкта одночасно впливають технічні, організаційні, кібернетичні, фізичні та соціальні фактори, а також різноманітні загрози й ризики. Використання інформаційно-когнітивного підходу дозволяє формалізувати складні причинно-наслідкові зв’язки між елементами системи управління та представити їх у вигляді цілісної моделі, орієнтованої на підтримку прийняття рішень.

Важливою особливістю застосування інформаційно-когнітивних технологій у дослідженні процесу управління об’єктом критичної

інфраструктури є інтеграція формалізованих і неформалізованих знань. У практиці управління значну роль відіграють не лише кількісні показники та нормативно визначені параметри, але й експертні оцінки, професійний досвід та інтуїтивні судження фахівців. Інформаційно-когнітивні технології створюють умови для поєднання різнорідної інформації в єдиному інформаційному просторі, що підвищує повноту та обґрунтованість аналізу управлінських ситуацій.

Центральне місце в межах інформаційно-когнітивного підходу займає когнітивне моделювання, яке забезпечує формування узагальненого уявлення про структуру об’єкта критичної інфраструктури та механізми його функціонування. Когнітивні моделі дозволяють відобразити взаємозв’язки між загрозами, вразливостями, управлінськими впливами та показниками стану захищеності, що дає змогу досліджувати можливі сценарії розвитку подій і оцінювати наслідки прийнятих рішень. Завдяки цьому процес управління набуває прогнозного характеру, що є особливо важливим для запобігання кризовим та надзвичайним ситуаціям.

Застосування інформаційно-когнітивних технологій також є ефективним інструментом підтримки прийняття рішень в умовах невизначеності та неповноти інформації. У реальних умовах функціонування об’єктів критичної інфраструктури значна частина даних може бути неточною, запізнілою або суперечливою. Інформаційно-когнітивний підхід дозволяє враховувати такі особливості за рахунок використання методів нечіткого опису, сценарного аналізу та експертного моделювання, що знижує рівень суб’єктивності та підвищує стійкість управлінських рішень.

Важливою характеристикою інформаційно-когнітивних технологій є їхня орієнтація на сценарний аналіз і прогнозування. Формування альтернативних сценаріїв розвитку ситуації дає змогу оцінити ефективність різних управлінських стратегій, визначити потенційні наслідки впливу загроз та обрати оптимальні варіанти реагування. Це сприяє підвищенню готовності системи управління до дій у складних та швидкозмінних умовах

функціонування об’єкта критичної інфраструктури.

Крім того, застосування інформаційно-когнітивних технологій сприяє підвищенню адаптивності та стійкості системи управління. Когнітивні моделі дозволяють своєчасно виявляти критичні елементи та найбільш вразливі ланки об’єкта, вплив на які має вирішальне значення для забезпечення його безперервного функціонування. Це створює передумови для оперативного коригування управлінських рішень у відповідь на зміни внутрішнього або зовнішнього середовища.

Отже, інформаційно-когнітивні технології є ефективним інструментом дослідження процесу прийняття рішень при управлінні об’єктами критичної інфраструктури. Їх застосування забезпечує системність аналізу, підвищує обґрунтованість і прозорість управлінських рішень, а також сприяє підвищенню рівня безпеки, надійності та стійкості функціонування критично важливих об’єктів.

Інформаційно-когнітивні технології (ІКТ) дозволяють моделювати та аналізувати процес прийняття рішень в умовах складних, невизначених та багатофакторних загроз. Вони забезпечують:

- Інтеграцію даних із різних джерел (сенсорів, SCADA-систем, журналів подій, зовнішніх аналітичних ресурсів).
- Формалізацію когнітивних процесів людини та автоматизованих систем при прийнятті рішень.
- Виявлення причинно-наслідкових зв’язків між станом об’єкта, кібер- та фізичними загрозами і результатами управлінських дій.
- Прогнозування динаміки стану ОКІ під впливом комбінованих загроз.
- Оцінку ризиків і пріоритетність дій, що забезпечує стійкість і надійність системи управління.

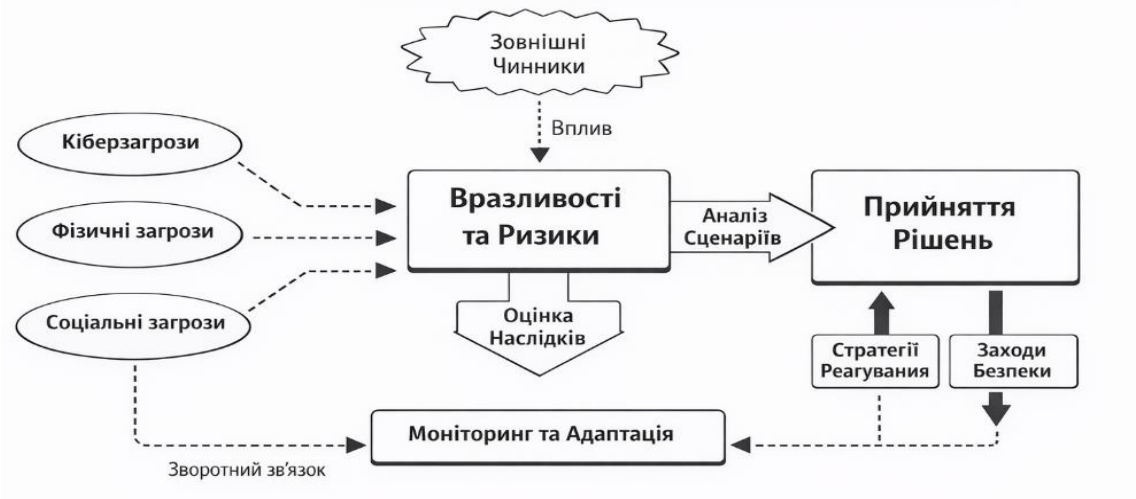


Рисунок 1.2. - Когнітивна модель впливу комплексних загроз на процес прийняття рішень

Особливості застосування ІКТ для комплексних загроз:

1) Інтеграція кібер- та фізичних загроз

ІКТ дозволяє враховувати одночасний вплив кібератак і фізичних факторів (наприклад, проникнення, руйнування інфраструктури, відключення електропостачання).

2) Динамічне моделювання сценаріїв

Створення моделей розвитку подій у часі, включаючи ескалацію гібридних атак, оцінку часу реакції та наслідків.

3) Ситуативний аналіз

Використання когнітивних карт для оцінки ситуаційної обізнаності операторів та автоматизованих систем управління.

4) Аналіз управлінських стратегій

ІКТ дозволяє моделювати різні варіанти дій у разі загроз і обирати оптимальні стратегії з урахуванням ресурсів, часу та потенційного ризику.

Переваги використання ІКТ

- Забезпечення системного та комплексного підходу до оцінки ризиків.
- Можливість врахування мультифакторних взаємозв’язків між кібер- і фізичними загрозами.

- Підвищення точності та достовірності оцінки стану об’єкта.
- Прогнозування динаміки розвитку кризових ситуацій.
- Підтримка прийняття рішень в умовах високої невизначеності та дефіциту часу.

## 1.3 Основні задачі дослідження залежності процесу прийняття рішень від стану захищеності об’єкту критичної інфраструктури.

Дослідження залежності процесу прийняття рішень від стану захищеності об’єкта критичної інфраструктури є складним науково-прикладним завданням, спрямованим на підвищення ефективності управління та забезпечення стійкого функціонування таких об’єктів в умовах дії комплексних загроз. Основною задачею такого дослідження є формування системного уявлення про взаємозв’язок між рівнем захищеності об’єкта та характеристиками управлінських рішень, що приймаються на різних рівнях управління.

Однією з ключових задач є ідентифікація та структуризація факторів, які визначають стан захищеності об’єкта критичної інфраструктури. Це передбачає аналіз сукупності технічних, організаційних, інформаційних, кібернетичних і фізичних складових безпеки, а також визначення їхнього впливу на можливості та обмеження процесу прийняття рішень. Розв’язання цієї задачі дозволяє встановити, які саме параметри стану захищеності є критичними для управління та потребують першочергового врахування.

Важливою задачею дослідження є встановлення причинно-наслідкових залежностей між рівнем захищеності об’єкта та вибором управлінських стратегій. Аналіз таких залежностей дає змогу визначити, яким чином зміна стану захищеності впливає на характер управлінських рішень, зокрема на їхню оперативність, жорсткість, ступінь ризикованості та спрямованість на запобігання або ліквідацію наслідків загроз. Це сприяє формуванню адаптивних механізмів управління, орієнтованих на поточний стан безпеки об’єкта.

Окрему увагу в межах дослідження приділяють задачі оцінювання впливу

загроз і вразливостей на процес прийняття рішень. Зокрема, необхідно визначити, як наявність або посилення певних загроз змінює пріоритети управління, обмежує доступні альтернативи та впливає на критерії вибору рішень. Розв’язання цієї задачі дозволяє підвищити обґрунтованість управлінських рішень у кризових та надзвичайних ситуаціях.

Суттєвою задачею є розроблення методів кількісної та якісної оцінки стану захищеності об’єкта критичної інфраструктури з точки зору підтримки прийняття рішень. Це передбачає визначення інтегральних показників захищеності, а також їх зв’язок із показниками ефективності управлінських рішень. Такий підхід створює можливість для порівняльного аналізу альтернативних управлінських сценаріїв та вибору найбільш доцільних рішень залежно від поточного рівня безпеки.

Не менш важливою задачею є дослідження процесу прийняття рішень в умовах невизначеності, що виникає внаслідок неповноти або нестабільності інформації про стан захищеності об’єкта. У цьому контексті особливого значення набуває аналіз того, яким чином рівень захищеності впливає на допустимий рівень ризику та на схильність осіб, що приймають рішення, до використання превентивних або реактивних стратегій управління.

Крім того, дослідження передбачає задачу аналізу зворотного впливу управлінських рішень на стан захищеності об’єкта критичної інфраструктури. Встановлення такого двостороннього зв’язку дозволяє розглядати процес управління як динамічну систему, у якій прийняті рішення безпосередньо формують майбутній рівень захищеності та визначають умови для подальших управлінських дій.

Отже, основні задачі дослідження залежності процесу прийняття рішень від стану захищеності об’єкта критичної інфраструктури спрямовані на виявлення та формалізацію ключових взаємозв’язків між безпековими характеристиками об’єкта та механізмами управління. Їх розв’язання створює наукове підґрунтя для розроблення ефективних систем підтримки прийняття рішень, здатних забезпечити підвищення рівня безпеки, надійності та стійкості.

Висновки розділу 1:

У результаті виконання розділу встановлено, що процес прийняття рішень при управлінні об’єктами критичної інфраструктури має складний, багатофакторний і динамічний характер та здійснюється в умовах невизначеності, обмеженого часу і підвищених вимог до надійності управління. Показано, що застосування математичних методів і моделей є необхідною умовою формалізації процесів управління, оцінювання ризиків і прогнозування наслідків управлінських рішень, а також забезпечує можливість кількісного аналізу впливу факторів загроз на стан захищеності об’єкта.

Обґрунтовано доцільність використання інформаційно-когнітивних технологій для дослідження процесу прийняття рішень, оскільки вони дозволяють інтегрувати формалізовані дані моніторингу із знаннями та експертними оцінками, враховувати причинно-наслідкові зв’язки, когнітивні особливості осіб, що приймають рішення, та динаміку змін загрозового середовища. Застосування когнітивних моделей створює передумови для підвищення обґрунтованості, адаптивності та своєчасності управлінських рішень в системах управління критичною інфраструктурою.

Визначено основні задачі дослідження залежності процесу прийняття рішень від стану захищеності об’єкта критичної інфраструктури, які полягають у формалізації показників захищеності, ідентифікації факторів загроз, встановленні причинно-наслідкових залежностей між рівнем захищеності та ефективністю управління, а також у розробленні моделей підтримки прийняття рішень в умовах невизначеності. Отримані результати створюють методологічну основу для подальшого аналізу сучасних методів дослідження та практичного застосування інформаційно-когнітивних технологій у системах управління об’єктами критичної інфраструктури.

# 2. АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА СПОСОБІВ ДОСЛІДЖЕННЯ ПРОЦЕСУ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ ОБ'ЄКТОМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

## 2.1 Аналіз сучасних способів і методів визначення впливу основних факторів загроз на процес прийняття рішень при управлінні об'єктом критичної інфраструктури.

Процес прийняття управлінських рішень у сфері функціонування об'єктів критичної інфраструктури (КІ) є складним багатофакторним явищем, що перебуває під безпосереднім впливом рівня їх захищеності. Стан захищеності визначає не лише допустимі межі управлінського впливу, але й структуру, часові параметри та ступінь обґрунтованості рішень, які приймаються в умовах підвищеної невизначеності та ризику. У зв'язку з цим сучасні наукові дослідження спрямовані на розроблення та вдосконалення методів аналізу залежності між рівнем захищеності об'єкта КІ та характеристиками процесу прийняття рішень.

Методологічною основою таких досліджень є системний підхід, відповідно до якого об'єкт критичної інфраструктури розглядається як складна соціально-технічна система з ієрархічною структурою, множинними внутрішніми та зовнішніми зв'язками, а також значною кількістю потенційних загроз. У межах цього підходу процес прийняття рішень трактується як динамічний процес трансформації інформації про стан захищеності в управлінські дії, спрямовані на збереження стійкості та безперервності функціонування об'єкта.

Одним із найбільш поширених сучасних методів дослідження такої залежності є імовірнісно-статистичне моделювання. Воно ґрунтується на формалізації загроз, вразливостей та наслідків у вигляді випадкових подій і дозволяє кількісно оцінювати вплив рівня захищеності на ймовірність прийняття того чи іншого управлінського рішення. У рамках цього підходу

ризик розглядається як функція ймовірності реалізації загрози та очікуваного збитку, що безпосередньо впливає на вибір альтернатив управління.

Схематично імовірнісно-статистичний підхід до аналізу процесу прийняття рішень можна подати таким чином: (рис. 2.1).


Рисунок 2.1 - Імовірнісно-статистичний підхід до аналізу процесу прийняття рішень

Водночас обмеженість статистичних даних та неможливість повної формалізації багатьох факторів захищеності зумовили активний розвиток методів нечіткої логіки та теорії нечітких множин. Ці методи дозволяють враховувати якісні характеристики стану захищеності, експертні оцінки та лінгвістичні змінні, що особливо важливо для стратегічного рівня управління об’єктами КІ. У таких моделях залежність між рівнем захищеності та управлінськими рішеннями встановлюється через систему нечітких правил, які

відображають причинно-наслідкові зв’язки між факторами загроз і реакціями системи управління.

Когнітивні моделі, зокрема нечіткі когнітивні карти, є логічним розвитком цього підходу. Вони дозволяють досліджувати не лише прямий, але й опосередкований вплив рівня захищеності на процес прийняття рішень, враховуючи зворотні зв’язки та ефекти накопичення. У таких моделях управлінські рішення розглядаються як результат взаємодії множини концептів, що характеризують технічний, організаційний та інформаційний стан об’єкта КІ.(рис. 2.2).


Рисунок 2.4 - Когнітивний підхід до аналізу процесу прийняття рішень

Важливе місце серед сучасних методів займають мультикритеріальні методи прийняття рішень. Вони застосовуються у випадках, коли стан захищеності об’єкта КІ оцінюється за сукупністю критеріїв, що часто є суперечливими. Такі методи дозволяють формалізувати компроміс між рівнем безпеки, економічною доцільністю, часом реагування та ресурсними обмеженнями. Залежність процесу прийняття рішень від стану захищеності в цьому випадку проявляється через зміну вагових коефіцієнтів критеріїв залежно від рівня загроз.

Для аналізу динаміки процесу прийняття рішень у часі широко використовуються методи імітаційного моделювання, зокрема системна динаміка та агентно-орієнтовані моделі. Системно-динамічні моделі дозволяють дослідити, як зміни стану захищеності об’єкта КІ впливають на затримки в прийнятті рішень, накопичення ризиків та ефективність управлінських дій. Агентно-орієнтовані моделі, у свою чергу, надають можливість врахувати поведінкові аспекти суб’єктів прийняття рішень, їхню адаптацію до змін рівня захищеності та реакцію на комплексні загрози. (рис.2.5).


Рисунок 2.5 - Імітаційний підхід

Окрему групу сучасних підходів становлять гібридні методи, які поєднують імовірнісні, нечіткі, когнітивні та імітаційні моделі в межах єдиної системи підтримки прийняття рішень. Такі методи дозволяють комплексно дослідити залежність управлінських рішень від стану захищеності об’єкта КІ, враховуючи як кількісні, так і якісні фактори, а також їхню динамічну взаємодію.

Загалом аналіз сучасних методів і способів дослідження залежності процесу прийняття рішень від стану захищеності об’єктів критичної інфраструктури свідчить про перехід від вузькоспеціалізованих моделей до інтегрованих методологічних підходів. Це зумовлено зростанням складності загрозового середовища та необхідністю прийняття обґрунтованих рішень у режимі обмеженого часу та інформації. Подальший розвиток цих методів пов’язується з удосконаленням гібридних моделей, підвищенням рівня формалізації експертних знань та розширенням можливостей систем підтримки прийняття рішень у сфері управління критичною інфраструктурою.

## 2.2 Аналіз сучасних способів і методів визначення впливу основних факторів загроз на процес прийняття рішень при управлінні об’єктом критичної інфраструктури.

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 забезпечення стійкості функціонування в умовах кібератак. Управління стійкістю функціонування об’єктів КІІ України ґрунтується на знаннях про стан об’єктів управління, стан середовища функціонування і впливи, які відбуваються. Невід’ємним елементом систем управління об’єктів КІІ є низка підсистем підтримки ухвалення рішень

Можливості таких систем безпосередньо залежать від здатності забезпечити особу, яка ухвалює рішення, якісно збалансованою інформацією,

що характеризує реальні і прогнозовані стани об’єктів критичної інфраструктури та запропонувати обґрунтований вибір траєкторії досягнення мети.

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» [18]. 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 (табл.2.1). 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 (рис. 2.6).


Рисунок 2.6 - Аналіз факторів загроз.

Таблиця 2.1 - Актуальні загрози критично-важливих об’єктів.

| Загроза | Пояснення |
|---|---|
| Несанкціоноване використання точок доступу для віддаленого обслуговування | Точки доступу для технічного обслуговування це спеціально створені зовнішні входи в мережу ІКТ, які часто недостатньо захищені |
| Мережеві атаки через офісні чи корпоративні мережі | Офісні ІТ зазвичай пов'язані з мережею декількома способами. У більшості випадків мережні з'єднання з офісів в 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), такі як системне програмне забезпечення, сервери додатків або бази даних, часто містять недоліки або вразливості, які можуть бути використані зловмисниками. Якщо такі стандартні компоненти також використовують у мережі ІКТ, ризик 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 загрозою для всіх 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 в 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 |

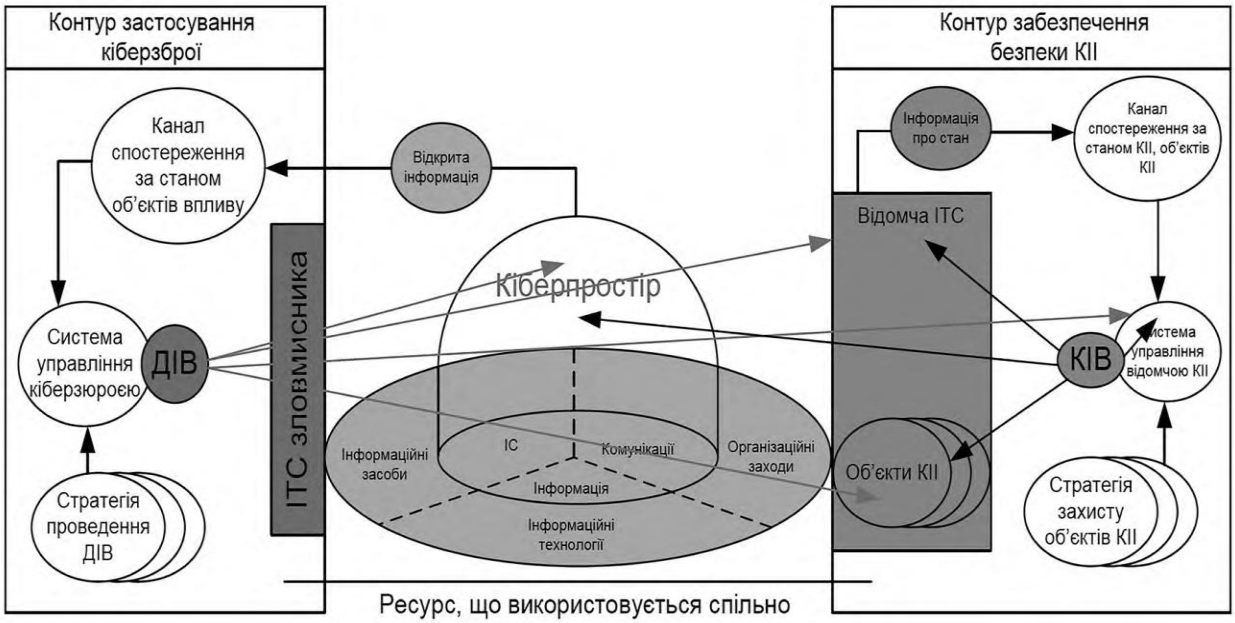


Рисунок 2.7 – Модель інформаційного протиборства в кіберпросторі

Аналіз відкритих джерел [19-22], присвячених забезпеченню безпеки КІ, надійності та стійкості функціонування об'єктів КІІ показав, що в них практично не розглянуті питання, пов'язані:

- з розробкою моделей і методів з побудови системи оцінки стану об'єктів КІІ;
- з розробкою науково-методичного апарата побудови автоматичної системи збору та приведення до єдиного вигляду інформації, що характеризує стан КІІ в умовах деструктивних інформаційних впливів;
- з розробкою моделей і методів адаптивного управління КІІ, що враховують поточний і прогнозований стан об'єктів КІІ.

Отже, існує необхідність у розробці підходів до побудови системи оцінки сталості функціонування КІІ. Під поняттям кіберживучості [23] розуміється здатність інформаційної системи виконувати свої функції в умовах, які виникають унаслідок протиборства щонайменше двох сторін, водночас відбувається спільне використання загального ресурсу, глобального інформаційного простору, управління якими має розглядатися як цілеспрямований вплив двох і більше підсистем управління (ри.2.7).

Тобто кіберстійкість багатоланкового об’єкта КІІ має розраховуватися як спільна *N*-мірна функція розподілу ймовірності збереження працездатності одночасно *N* ланок, які складають цей багатоланковий об’єкт КІІ.

Основою розрахунку кіберстійкості багатоланкових об’єктів КІІ є розрахунок показників кіберзахищеності і кіберживучості окремих ланок об’єкта КІІ. Тому, необхідно розробити методику розрахунку показників кіберзахищеності і кіберживучості об’єкта КІІ, причому визначальною властивістю з погляду можливості виконання об’єктом КІІ цільової функції буде кіберживучість, а кіберзахищеність буде складовою частиною функції.

Зважаючи на те, що властивості, які характеризують кіберживучість об’єкта КІІ – **Ω**, починають проявлятися тільки після того, як об’єкт зазнав впливу, то міра живучості має визначатися умовною імовірністю збереження працездатності, за умови, що система отримала локальне пошкодження.

Під показником кіберживучості одноланкового об’єкта КІІ, розуміється умовна ймовірність невиходу кінцевого стану об’єкта КІІ за межі заданої області безпечних станів SI простору безпечних станів S.

На сьогодні важливим фактором розвитку сучасного суспільства є забезпечення захищеності інформаційних систем, які є ключовими елементами будь-яких процесів незалежно від сфери людської діяльності. При цьому моделювання загроз безпеці, ступінь їх впливу на рівень безпеки займає провідне місце при проектуванні системи захисту інформаційного простору. Оскільки вирішення даної задачі безпосередньо пов’язане з людським фактором і характеризується високим ступенем невизначеності і складності формалізації, то доцільно звернути увагу на методи когнітивного моделювання. Дані методи базуються на використанні нечітких когнітивних карт (НКК) [1], яким властива простота, наочність, гнучкість, конструктивність, адаптація до невизначеності вхідних даних, використання знань і досвіду експертів предметної області.

Узагальнений алгоритм методики оцінки кіберстійкості КІІ наведено на рис. 2.8.

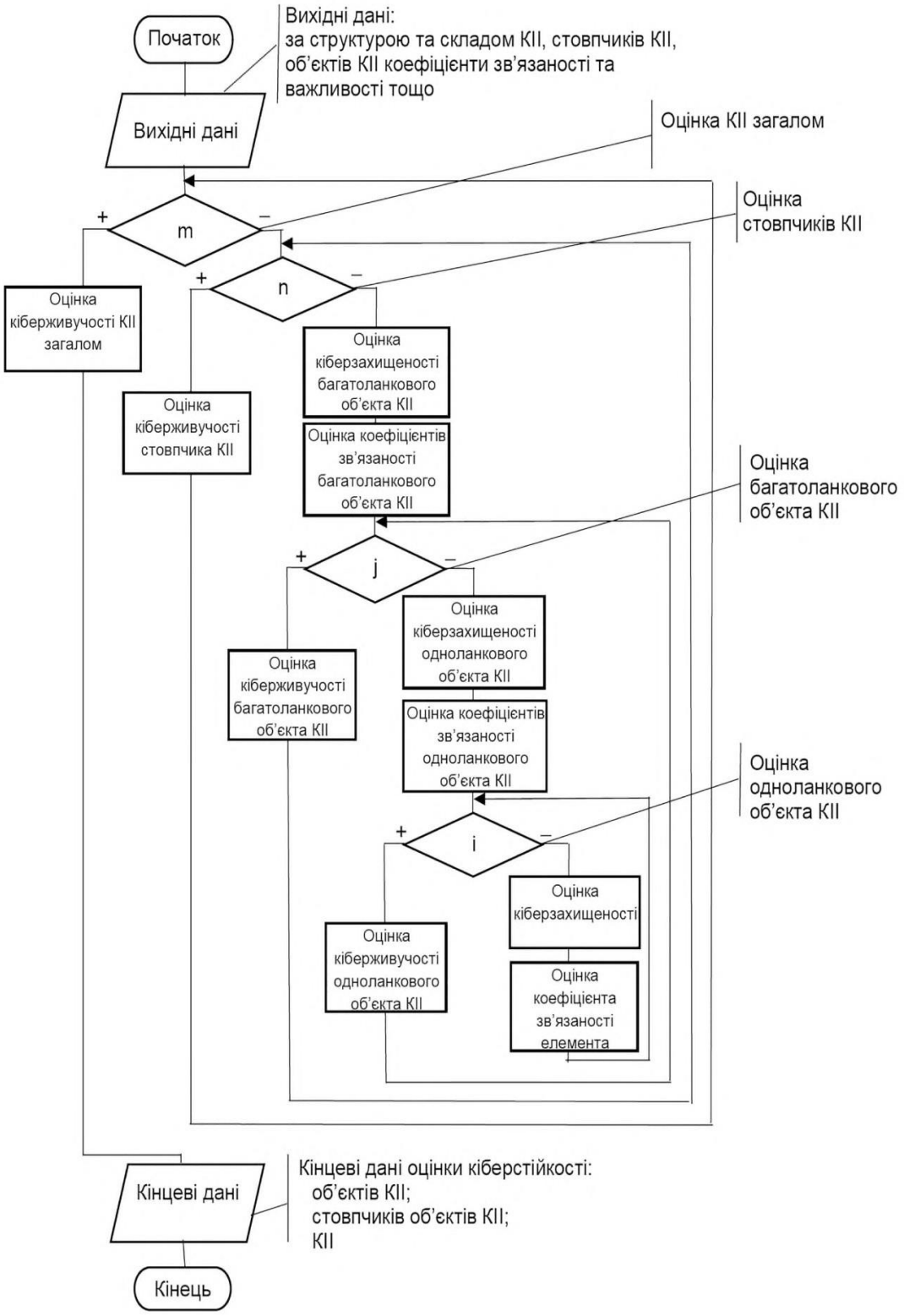


Рисунок 2.8 – Узагальнений алгоритм методики оцінки кіберстійкості КІІ.

Основою когнітивних технологій є когнітивна наука, що вивчає, як люди сприймають світ, як мислять, на що звертають увагу, як запам'ятовують інформацію тощо. Тому когнітивні технології спираються на засади нейронауки,

теорію синергетики (самоорганізації), комп’ютерні та інформаційні технології, математичне моделювання людської свідомості, інші наукові й практичні концепти, які раніше вважали складовими фундаментальної та прикладної природничої науки. [30,31].

Когнітивні технології - методи, засоби та прийоми, що забезпечують візуальне, гіпермедійне подання умов завдань та/або предметної галузі, яке допомагає знаходити або стратегію рішення (або саме рішення), або дозволяє оцінювати та порівнювати шляхи вирішення.

Когнітивні технології – інформаційні технології, спеціально орієнтовані на розвиток інтелектуальних здібностей людини які розвивають уяву та асоціативне мислення людини.

Когнітивні технології "імітують" розумову діяльність людини. Вони, як правило, засновані на моделях з нечіткою логікою (fuzzy logic) і на нейронних мережах (neural networks). Цілі, переслідувані при створенні когнітивних систем, можуть бути представлені такими прикладами: отримання нових знань, прийняття рішень в складних ситуаціях і інтелектуальна обробка даних

На сьогодні в умовах складного динамічного середовища, що характеризується постійною невизначеністю та мінливістю політичних, економічних і соціальних чинників, основою успішного функціонування господарюючих суб'єктів є ухвалення адекватних управлінських рішень. Сучасні системи підтримки прийняття рішення є системами, максимально пристосованими до вирішення задач повсякденної управлінської діяльності і є інструментом, покликаним надати допомогу особам, що приймають рішення.

Зважаючи на ключову роль понять «знання» і «інтелект» у визначенні інтелектуальної діяльності, можна з’ясувати різницю між ними. Знання – це корисна інформація, накопичена індивідуумом, а інтелект – здатність індивідуума використовувати цю накопичену інформацію корисним (цілеспрямованим) чином. Більш широко інтелект можна розглядати як здатність особи, що приймає рішення, досягати певного рівня успіху при широкому різноманіттю цілей у великому діапазоні середовищ.

Інтелектуальними (когнітивними) функціями живого інтелекту є сприйняття, інтуїція, творчість, асоціація, індукція, силогізми (міркування, що

складається з трьох простих атрибутивних дій: двох засновків і одного висновку), впізнавання, прогнозування, планування, дедукція, класифікація, а також пошук і вибір, порівняння, ідентифікація, обчислення. Нині науковцями детально проаналізовано та формалізовано такі функції пошук, вибір, обчислення, зіставлення, дедукція.

Когнітивне управління базується на систематизованому управлінні процесами в результаті якого знання ідентифікуються, накопичуються, розподіляються та використовуються в організації для покращення її діяльності та підвищення конкурентоспроможності на ринку.

Когнітивне моделювання при дослідженні управління слабоструктурованими системами і ситуаціями є одним з нових напрямів в сучасній теорії підтримки і прийняття рішень.

Передумови до застосування когнітивного підходу до аналізу складних ситуацій, складності аналізу процесів та прийняття управлінських рішень у таких галузях як економіка, соціологія, екологія тощо обумовлені низкою особливостей, властивих цим областям, а саме:

- багатоаспектністю процесів, що відбуваються в них (економічних, соціальних тощо) і їх взаємопов'язаністю; в силу цього неможливо детальне дослідження окремих явищ - всі явища, що відбуваються в них, повинні розглядатися в сукупності;
- відсутністю достатньої кількісної інформації про динаміку процесів, що змушує переходити до якісного аналізу таких; мінливістю характеру процесів у часі тощо.

Досвід застосування різних моделей і методів на базі когнітивного підходу, показують доцільність розвитку даного підходу в управлінні технологічними об'єктами, комплексами, проектуванні системи захисту інформаційного простору, та в організації захисту об’єктів критичної інфраструктури.

## 2.3 Постановка задачі на дослідження залежності процесу прийняття рішень від стану захищеності об’єкту критичної інфраструктури, з використанням інформаційно-когнітивних технологій.

У сучасних умовах цифровізації та зростання ролі інформаційних ресурсів об’єкти критичної інфраструктури все частіше функціонують як складні автоматизовані інформаційно-керуючі системи. Їх надійне та безперервне функціонування безпосередньо залежить від ефективності систем технічного захисту інформації (ТЗІ), рівня автоматизації процесів обробки даних та здатності систем управління своєчасно приймати обґрунтовані рішення в умовах дії комплексних загроз.

Процес прийняття управлінських рішень у системах технічного захисту інформації здійснюється на основі результатів автоматизованої обробки даних про стан інформаційної безпеки, параметри функціонування технічних засобів, індикатори порушень, а також результати моніторингу інформаційних і технічних загроз. При цьому стан захищеності об’єкта критичної інфраструктури формується як інтегральна характеристика ефективності реалізованих технічних, програмних та організаційних заходів захисту інформації.

Проблемна ситуація полягає в тому, що існуючі автоматизовані системи підтримки прийняття рішень у сфері ТЗІ часто базуються на фрагментарних або детермінованих моделях, які недостатньо враховують когнітивні аспекти прийняття рішень, складні причинно-наслідкові зв’язки між факторами загроз, технічними вразливостями та станом захищеності інформації. Це призводить до зниження ефективності управлінських рішень, особливо в умовах комбінованих кібернетичних та фізичних загроз.

У зв’язку з цим задача дослідження полягає у створенні інформаційно-когнітивної моделі, що забезпечує формалізований опис впливу основних факторів загроз на стан технічного захисту інформації об’єкта критичної інфраструктури та дозволяє дослідити залежність процесу прийняття

управлінських рішень від результатів автоматизованої обробки інформації про цей стан.

У межах поставленої задачі об’єкт критичної інфраструктури розглядається як автоматизована інформаційна система, для якої формується вектор стану захищеності

$$S(t) = \{s_{conf}(t), s_{int}(t), s_{avail}(t), s_{tech}(t)\},$$

де $s_{conf}(t)$, $s_{int}(t)$, $s_{avail}(t)$— показники забезпечення конфіденційності, цілісності та доступності інформації, а $s_{tech}(t)$— узагальнений показник технічного стану засобів захисту інформації.

Процес прийняття рішень у системі управління ТЗІ визначається як функція автоматизованої та когнітивної обробки інформації:

$$D(t) = F(S(t), Z(t), M(t)),$$

де $Z(t)$— вектор факторів інформаційних і технічних загроз, а $M(t)$— інформаційно-когнітивна модель, що відображає правила, знання та причинно-наслідкові зв’язки між параметрами системи.

Таким чином, задача дослідження зводиться до аналізу та синтезу інформаційно-когнітивного механізму, який забезпечує автоматизовану підтримку прийняття управлінських рішень у системах технічного захисту інформації на основі оцінки стану захищеності об’єкта критичної інфраструктури.

*Задачі дослідження:*

1. Систематизація факторів загроз (кібер, фізичних, гібридних та внутрішніх) та визначення їх впливу на процес прийняття рішень.

2. Розробка когнітивної моделі, що відображає взаємозв’язки між станом захищеності, факторами загроз та управлінськими рішеннями.

3. Формалізація математичної моделі залежності результатів прийняття рішень від стану захищеності ОКІ.

4. Визначення ключових показників ефективності (ефективність, надійність, швидкість реакції).

5. Створення сценаріїв розвитку подій та симуляційних моделей для оцінки стійкості прийнятих рішень.

6. Розробка методики інтеграції експертних оцінок та даних систем моніторингу для підтримки прийняття рішень.

*Побудова когнітивної моделі*

Когнітивна модель включає:

1. **Вузли** — ключові фактори загроз, стан захищеності, параметри оператора та організаційні характеристики.

2. **Зв'язки** — причинно-наслідкові взаємозалежності, які можуть бути прямими або опосередкованими.

3. **Вагові коефіцієнти** — величини, що характеризують силу впливу одного вузла на інший.

4. **Механізм оновлення стану** — алгоритм оцінки зміни параметрів системи при виникненні загроз.

| Вузол | Тип | Параметри | Джерело даних |
|---|---|---|---|
| Кіберзагрози | Фактор | інтенсивність, тривалість, тип атаки | SCADA, IDS, журнали подій |
| Фізичні загрози | Фактор | масштаб, ймовірність, швидкість розвитку | Датчики, технічні системи, експертні оцінки |
| Гібридні сценарії | Фактор | комбінація кібер+фізичні загрози | Моделювання сценаріїв |
| Стан захищеності | Параметр | рівень резервування, надійність систем | Моніторинг, внутрішні системи |
| Когнітивні параметри | Параметр | обізнаність, навантаження, час реакції | Опитування операторів, симуляції |
| Внутрішні фактори | Параметр | організаційні процеси, ресурсні обмеження | Експертні оцінки, документи організації |

Висновки розділу 2:

У результаті виконання аналізу сучасних методів і способів дослідження процесу прийняття рішень при управлінні об’єктами критичної інфраструктури встановлено, що наявні підходи характеризуються різноманіттям математичних, імовірнісних, нечітких, імітаційних та експертних методів, які дозволяють оцінювати окремі аспекти стану захищеності та вплив загроз. Разом з тим, більшість існуючих методів орієнтована на аналіз окремих факторів і не забезпечує комплексного урахування динамічних змін загрозового середовища та когнітивних особливостей осіб, які приймають рішення.

Проведений аналіз сучасних способів і методів визначення впливу основних факторів загроз показав, що кібернетичні, фізичні та гібридні загрози мають нелінійний і взаємопов’язаний характер впливу на стан захищеності об’єктів критичної інфраструктури та ефективність управлінських рішень. Встановлено, що використання лише кількісних або лише якісних методів є недостатнім, а найбільш перспективним є інтегрований підхід, який поєднує аналіз ризиків, сценарне моделювання, експертні оцінки та когнітивні методи.

На основі узагальнення результатів аналізу сформульовано постановку задачі дослідження залежності процесу прийняття рішень від стану захищеності об’єкта критичної інфраструктури з використанням інформаційно-когнітивних технологій. Визначено необхідність розроблення моделей, які дозволяють формалізувати причинно-наслідкові зв’язки між факторами загроз, показниками захищеності та управлінськими рішеннями в умовах невизначеності. Отримані висновки обґрунтовують доцільність застосування інформаційно-когнітивного підходу як методологічної основи для подальшого дослідження та практичної реалізації систем підтримки прийняття рішень при управлінні об’єктами критичної інфраструктури.

# 3. МОДЕЛІ ТА АЛГОРИТМИ РОЗРОБКИ МЕТОДИКИ ОЦІНЮВАННЯ РІВНЯ ЗАХИЩЕНОСТІ ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ІЗ ЗАСТОСУВАННЯМ ІНФОРМАЦІЙНО-КОГНІТИВНИХ ТЕХНОЛОГІЙ

## 3.1 Розробка інформаційної моделі впливу основних факторів загроз на процес прийняття рішень при управлінні об'єктом критичної інфраструктури.

Процес прийняття рішень при управлінні об'єктом критичної інфраструктури формується під впливом множини взаємопов'язаних факторів загроз, що діють у складному, динамічному та невизначеному середовищі. Для формалізованого опису цього впливу доцільно застосувати інформаційну модель, яка забезпечує структуроване подання потоків даних, інформаційних перетворень та взаємозв'язків між загрозами, станом захищеності об'єкта та управлінськими рішеннями.

В основі інформаційної моделі лежить уявлення об'єкта критичної інфраструктури як соціально-технічної системи, у межах якої фактори загроз формують вхідний інформаційний потік, що трансформується в управлінські рішення через низку аналітичних і когнітивних процедур. При цьому інформаційна модель орієнтована не лише на фіксацію поточного стану, а й на підтримку прогнозування, сценарного аналізу та адаптивного управління.

Першим рівнем інформаційної моделі є рівень джерел загроз, який включає сукупність природних, техногенних, кібернетичних, соціальних та навмисних факторів. Ці фактори формують первинні дані у вигляді сигналів про потенційні небезпечні події, параметри середовища, індикатори відмов та аномалій функціонування. На цьому рівні інформація має різнорідний характер, відрізняється за повнотою, точністю та часовими характеристиками.

Другий рівень моделі становить рівень інформаційної інтерпретації загроз, у межах якого відбувається обробка первинних даних, їх нормалізація та

агрегація. Тут інформація про фактори загроз трансформується у показники ймовірності реалізації загроз, інтенсивності впливу та потенційних наслідків. На цьому етапі формується інформаційна база для оцінки стану захищеності об’єкта критичної інфраструктури.

Третій рівень - рівень оцінки стану захищеності, що є ключовим у запропонованій інформаційній моделі. Стан захищеності розглядається як інтегральна характеристика, яка відображає здатність об’єкта протидіяти визначеним загрозам з урахуванням наявних вразливостей, ресурсних обмежень та організаційних можливостей. Саме на цьому рівні формується узагальнене уявлення про допустимі та критичні режими функціонування об’єкта.

Четвертий рівень інформаційної моделі представлений рівнем аналітико-когнітивної обробки, де інформація про стан захищеності поєднується з цілями управління, нормативними обмеженнями та досвідом прийняття рішень. На цьому рівні реалізується аналіз альтернатив управлінських дій, оцінка ризиків, прогнозування розвитку ситуації та вибір допустимих стратегій реагування.

П’ятий рівень - рівень формування управлінських рішень, у межах якого результати аналітичної обробки трансформуються у конкретні управлінські дії. Рішення можуть мати оперативний, тактичний або стратегічний характер і безпосередньо впливають на зміну стану захищеності об’єкта, що замикає інформаційний цикл управління.

*Інформаційні потоки та зворотні зв’язки*

Характерною особливістю запропонованої інформаційної моделі (рис. 3.9) є наявність зворотних інформаційних зв’язків між рівнем прийняття рішень і рівнем факторів загроз. Реалізовані управлінські рішення змінюють параметри захищеності об’єкта, що, у свою чергу, впливає на чутливість системи до дії загроз та на характеристики нових вхідних даних. Таким чином, процес управління набуває адаптивного характеру, а прийняття рішень розглядається як безперервний інформаційний процес.

Інформаційна модель також передбачає можливість існування

невизначеності та неповноти інформації на кожному з рівнів. Це зумовлює необхідність використання ймовірнісних, нечітких та експертних механізмів обробки інформації, що дозволяє підвищити стійкість процесу прийняття рішень до помилок і неточностей вхідних даних.


Рисунок 3.9 - Інформаційна модель впливу факторів загроз на процес прийняття рішень

Розроблена інформаційна модель дозволяє формалізувати вплив основних факторів загроз на процес прийняття рішень при управлінні об’єктом критичної інфраструктури як багаторівневий інформаційний процес із наявністю зворотних зв’язків. Вона створює методологічну основу для побудови систем підтримки прийняття рішень, аналізу сценаріїв розвитку загроз та підвищення ефективності управління захищеністю критично важливих об’єктів.

Враховуючи результати наукових досліджень для оцінки і підтримки захисту інформації і кібербезпеки ОКІІ пропонується наступна інформаційна модель (рис.3.1).

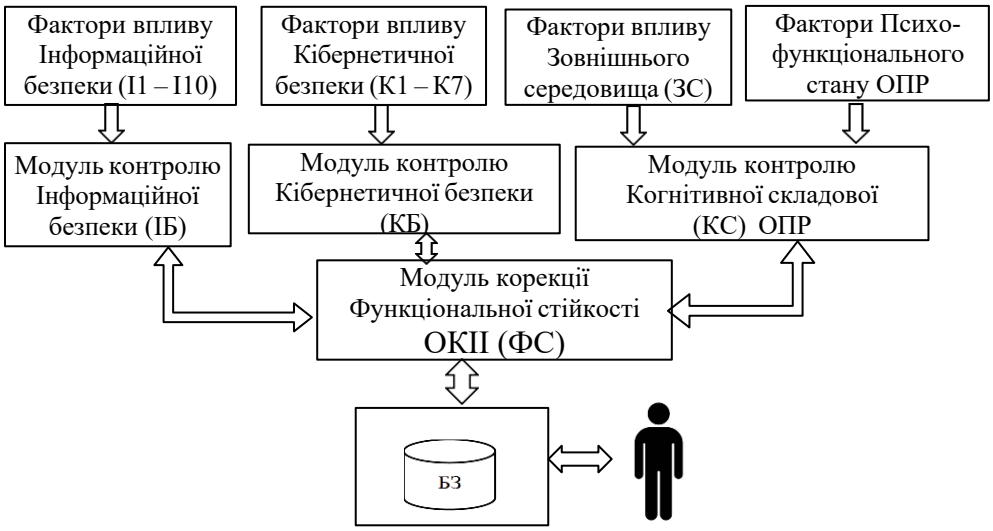


Рисунок 3.1 - Інформаційна модель оцінки та корекції оперативного стану захисту інформації і кібербезпеки ОКІІ.

У відповідності до Інформаційної моделі, та результатів наукових досліджень, найбільш впливовими факторами безпеки на ОКІІ є фактори Інформаційної безпеки (І1 – І10), фактори Кібернетичної безпеки (К1 – К7), фактори впливу Зовнішнього середовища (ЗС), фактори Психо-функціонального стану та Когнітивної складової ОПР.

*Інформаційна безпека (Informational security)* - це стан захищеності систем обробки і зберігання даних, яка контролюється та корегується модулем моніторингу (ММ) інформаційної безпеки відповідних вузлів: І1 - цілісність даних; І2 - доступність даних; І3 - конфіденційність даних; І4 - узгодженість

даних; І5 - посилальна цінність; І6 - відмови апаратного забезпечення; І7 - відмови програмного забезпечення; І8 - некоректні дії користувачів; І9 - вплив дій адміністраторів; І10 - енергетичні відмови.

*Кібернетична безпека* (*Cyber security)* - це запобігання доступу хакерів до систем та інформації, що потенційно призводить до втрати конфіденційності та/або контролю. Контроль та корегування кібернетичної безпеки забезпечується модулем моніторингу (ММ) кібернетичної безпеки відповідних вузлів: К1 - попередньої підстановки в запити даних і перевірка на SQL - ін'єкції; К6 - зовнішній вплив; К2 - перевірки системи на віруси; К3 - перевірки входу користувача з правами адміністратора; К4 - доступності даних і ресурсів; К5 - перевірки інформації на присутність підміни даних; К6 - захищеність даних К7 - перевірки даних на цілісність (використовуючи хеш).

Для визначення і оцінки ступеню важливості найбільш впливових факторів безпеки на ОКІІ пропонується застосування методу експертних оцінок [45].

Експертизу проводили експерти-фахівці, які мають досвід у розробці програмно–інструментальних засобів автоматичного тестування, і по скільки необхідно визначити тільки ранги факторів, то погодженість їх оцінок доцільно визначати за допомогою множинного коефіцієнта конкордації $K_0$ запропонованого М. Кендаллом і Б. Смітом [45].

Для цього, експертам ($m$) пропонувалося привласнити ранг (n) факторам впливу наведених в таблицях 3.1. та 3.2.

По результатам 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 ($\overline{j = 1, n}$ ) у ранжировці $i$ -го експерта ($\overline{i = 1, n}$ ). 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 К*0* = 1 думка експертів вважається узгодженою повністю. При К*о <1*, згідно з рекомендаціями для перевірки значимості погодженості визначаються значення статистики Х1 і Х2:

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

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

Після чого необхідно визначити числа ступенів свободи (υ1) і (υ2) розподілу, для чого 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 (І)

| **m експерти** | **Експертні оцінки** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | **n – фактори впливу** | | | | | | | | | |
| | **І1** | **І2** | **І3** | **І4** | **І5** | **І6** | **І7** | **І8** | **І9** | **І10** |
| **Е1** | 7 | 6 | 5 | 8 | 5 | 5 | 6 | 3 | 3 | 4 |
| **Е2** | 10 | 9 | 7 | 6 | 7 | 8 | 5 | 1 | 3 | 2 |
| **Е3** | 8 | 9 | 9 | 10 | 10 | 10 | 9 | 1 | 7 | 2 |
| **Е4** | 8 | 7 | 8 | 9 | 7 | 9 | 7 | 3 | 4 | 3 |
| **Е5** | 10 | 10 | 8 | 8 | 8 | 7 | 6 | 2 | 4 | 3 |
| **Е6** | 9 | 6 | 7 | 10 | 6 | 9 | 8 | 3 | 5 | 5 |
| **Е7** | 7 | 8 | 9 | 8 | 9 | 10 | 7 | 2 | 3 | 4 |
| **Е8** | 8 | 10 | 7 | 9 | 8 | 7 | 5 | 1 | 6 | 2 |
| **Е9** | 8 | 8 | 8 | 7 | 7 | 8 | 6 | 4 | 4 | 3 |
| **Е10** | 10 | 8 | 9 | 10 | 9 | 9 | 7 | 2 | 7 | 4 |
| $\sum_{j=1}^{m} x_{ij}$ | **85** | **81** | **77** | **85** | **76** | **82** | **66** | **22** | **46** | **32** |

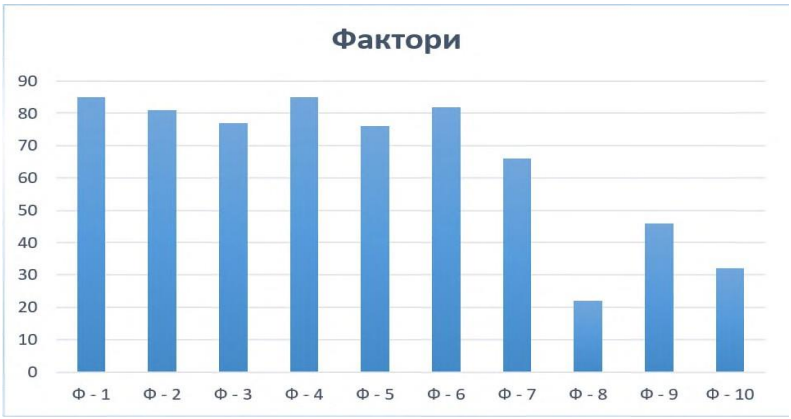


Рисунок 3.2 – Рангова діаграма розподілу важливості факторів впливу інформаційної безпеки.

Таблиця 3.2- Результати експертного оцінювання (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** |

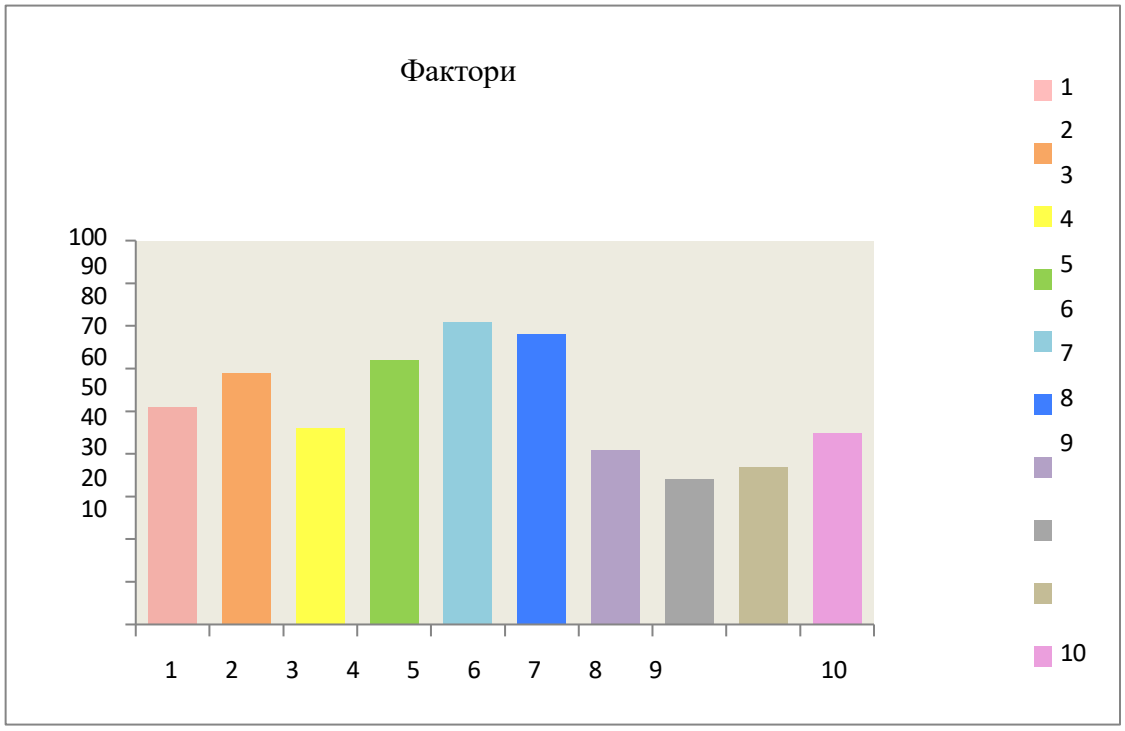


Рисунок 3.3 – Рангова діаграма розподілу важливості факторів впливу кібернетичної безпеки.

## 3.2 Оцінка впливу основних факторів загроз на процес прийняття рішень при управлінні об’єктом критичної інфраструктури.

Функція прийняття рішень формується та набуває завершеного вигляду у специфічних психічних утвореннях, зокрема у структурі індивідуальних якостей особистості, які визначають індивідуально-стильові особливості процесу вибору. У зв’язку з цим ефективне управління психічними процесами осіб, що приймають рішення (ОПР), є неможливим без урахування та оцінювання сукупності їх індивідуальних характеристик.

Визначення функціональних станів ОПР доцільно здійснювати не на основі окремих показників фізіологічних або психологічних функцій, а з урахуванням характеру їх взаємодії та взаємовпливу в процесі професійної діяльності. Функціональний стан формується як результат інтеграції низки взаємопов’язаних параметрів, що відображають як внутрішні, так і зовнішні умови функціонування людини в системі управління.

Функціональні стани ОПР зумовлюються сукупністю специфічних властивостей особистості, серед яких важливе місце займають індивідуальні особливості темпераменту, що проявляються у динамічних характеристиках перебігу психічних процесів та відображають силу, рухливість і врівноваженість нервової системи. Вагоме значення має також рівень мотивації до аналітичної діяльності та прагнення до підвищення професійної майстерності. Окрему роль відіграє здатність до короткочасного інтенсивного напруження в умовах стресових ситуацій, а також емоційна стійкість, зокрема емоційно-моторна та емоційно-сенсорна. До важливих характеристик належать швидкість переключення, стійкість і обсяг уваги, швидкість та точність складних рухових реакцій, координація рухів, здатність до формування й трансформації рухових стереотипів, а також наполегливість і рішучість у поєднанні з ініціативністю та самокритичністю.

На діяльність ОПР впливає комплекс внутрішніх і зовнішніх факторів, до яких належать гігієнічні та антропометричні умови, когнітивні характеристики,

психофізіологічні та фізіологічні фактори, а також властивості інформаційної моделі. Ступінь впливу зазначених факторів є неоднаковим і визначається їх інтенсивністю, тривалістю дії та часовими характеристиками.

Аналіз факторів, що впливають на когнітивний стан ОПР, базується на результатах досліджень у галузі ергономіки та інженерної психології, проведених протягом останніх десятиліть. У цих роботах виокремлено низку чинників, які визначають особливості процесів прийняття рішень людиною в системах підтримки прийняття рішень. Особливу увагу приділено тим факторам, які здатні динамічно та випадково змінюватися безпосередньо в процесі діяльності. Такі зміни, як правило, неможливо передбачити на етапі проєктування систем, що зумовлює необхідність розроблення засобів і методів контролю їх впливу на ефективність діяльності ОПР.

До факторів, що можуть істотно змінюватися в процесі роботи, належать функціональний стан ОПР, який характеризується сукупністю психофізіологічних і когнітивних параметрів, а також умови навколишнього середовища, в яких здійснюється професійна діяльність. Зміна стану ОПР може відбуватися як під впливом зовнішніх чинників, так і внаслідок дії внутрішніх процесів, пов’язаних із когнітивною діяльністю. Водночас умови навколишнього середовища можуть містити шкідливі або несприятливі фактори, що призводять до погіршення якості діяльності ОПР.

Таким чином, динамічні фактори, які впливають на результативність діяльності ОПР, доцільно поділяти на дві основні групи: фактори, зумовлені станом самого ОПР, зокрема психофізіологічні та когнітивні, і зовнішні фактори, пов’язані з умовами навколишнього середовища.

З аналізу літературних джерел випливає, що до складу когнітивного функціонального стану належать такі характеристики, як напруженість діяльності, рівень стомлення, мотивація, концентрація уваги, інформаційна пропускна здатність та монотонність виконуваних операцій. Поточний функціональний стан ОПР визначається сукупним впливом зазначених факторів.

Напруженість діяльності поділяється на емоційну та операційну, при цьому її рівень відображається у змінах фізіологічних показників людини. Для оцінювання цих змін розроблено нормативні значення, які дозволяють виділити оптимальний, допустимий і неприпустимий рівні напруженості. Оскільки напруженість не може бути безпосередньо виміряна одним числовим показником, для її формалізації застосовується порядкова шкала.

Окрім реєстрації фізіологічних параметрів, при оцінюванні напруженості аналізується ступінь відхилення умов праці від нормативних. Для цього використовуються такі показники, як коефіцієнт завантаженості, період зайнятості та швидкість доступу до інформації. Інтенсивність вхідного інформаційного потоку має відповідати інформаційній пропускній здатності ОПР, яка залежить від організації роботи та функціонального стану, зокрема від рівня стомлення.

Динаміка розвитку стомлення визначається витратами фізичних зусиль, напруженістю уваги, темпом роботи, робочою позою, монотонністю діяльності, температурними умовами та іншими факторами. Кожному з них відповідають умовні показники, які виражаються у відсотках часу, необхідного для відновлення працездатності. За сумісного впливу декількох факторів їх оцінки можуть підсумовуватися як арифметично, так і геометрично.

Фактори зовнішнього середовища, що впливають на працездатність ОПР, поділяються на фізичні та хімічні. Їх дія може спричиняти небажані функціональні зміни в організмі людини та, як наслідок, призводити до зниження якості діяльності. Характер впливу таких факторів визначається інтенсивністю та тривалістю їх дії.

Спільною рисою розглянутих факторів є нелінійний характер їх сумарного впливу, оскільки результат одночасної дії кількох чинників, як правило, перевищує просту суму ефектів від кожного з них окремо. Для факторів навколишнього середовища встановлено нормативи, які передбачають чотири рівні впливу на людину: комфортний, відносно дискомфортний, екстремальний та надекстремальний. Зазначені рівні можуть бути використані

при побудові формалізованих моделей впливу факторів на якість діяльності ОПР.

Серед усього комплексу чинників особливу увагу слід приділяти психофізіологічним факторам, таким як стомлення, емоційна напруга та мотивація, оскільки вони характеризуються залежністю від зовнішніх умов, неможливістю їх опису одним числовим показником, відсутністю прямого вимірювання та складною часовою динамікою, що визначається початковим станом ОПР.

У задачах прийняття рішень якість діяльності ОПР доцільно оцінювати за двома основними показниками: тривалістю вироблення рішення та його адекватністю. Перший показник може бути об’єктивно зафіксований як інтервал часу між надходженням інформації та реалізацією керуючих дій. Оцінювання адекватності рішення має суб’єктивний характер і здійснюється шляхом аналізу відповідності прийнятих дій стану керованого процесу. У зв’язку з цим доцільним є оцінювання можливості прийняття адекватного рішення з урахуванням доступної інформації, впливу зовнішніх факторів та когнітивних характеристик ОПР.

Властивості факторів, що впливають на діяльність ОПР, узагальнено в таблиці 3.1. Її аналіз дозволяє зробити висновок, що параметри зовнішнього середовища можуть бути представлені у вигляді векторних функцій дійсної змінної, що створює передумови для побудови числових моделей на основі функціональних залежностей і диференціальних операторів. Водночас параметри стану ОПР є нечисловими величинами, які не можуть бути описані одним або кількома числовими показниками, що обмежує можливість використання класичних методів математичного моделювання.

Зв’язки між параметрами зовнішнього середовища, характеристиками стану ОПР та показниками якості його діяльності потребують формалізації з використанням математичного апарату, здатного поєднувати числові й нечислові змінні. При цьому значення параметрів стану ОПР не підлягають безпосередньому вимірюванню, що зумовлює наявність невизначеності при їх

визначенні за когнітивними показниками. Адекватність прийнятих рішень також має нечисловий характер і додатково містить невизначеність, обумовлену психофізіологічним станом ОПР.

Аналіз наукових джерел свідчить про існування тісного взаємозв’язку між факторами навколишнього середовища та когнітивним станом ОПР, який, у свою чергу, впливає на адекватність його дій. Водночас ефективність діяльності визначається не лише зовнішніми умовами, а й здатністю організму протидіяти негативному впливу середовища, що залежить від рівня когнітивної складової та напруженості нервової системи.

Крім того, суттєвий вплив на діяльність ОПР мають початкові значення психофізіологічних характеристик, зокрема рівень стомлення та концентрації уваги. Зовнішні впливи можуть змінювати ці характеристики як у напрямі покращення, так і у бік погіршення. Різноманіття взаємозв’язків між параметрами стану ОПР, зовнішніми чинниками та показниками якості діяльності значно ускладнює задачу побудови адекватної математичної моделі впливу зовнішніх і психофункціональних характеристик.

По даним з літературних джерел, для дослідження СППР знайшли широке застосування математичні методи: теорія інформації, теорія масового обслуговування, теорія автоматичного керування, теорія автоматів, теорія статистичних рішень. Але жодна із цих теорій не дозволяє комплексно розв'язати питання створення моделей діяльності, що встановлюють зв'язок між вхідними впливами, станом ОПР і результатами його діяльності. У першу чергу, це зумовлено складністю величин, що визначають стан ОПР, та нелінійним характером взаємозв'язків між факторами, і продуктивністю його роботи

Таблиця 3.1. Властивості факторів, що впливають на діяльність ОПР.

| Позн | Фактор | Вектор або скаляр | Числова нечислова | Вимірність | Оптимальне значення |
|---|---|---|---|---|---|
| | ***Психо-функціональні фактори*** | | | | |
| Ез | Емоційне збудження | С | Ч | П | Так |
| Ен | Емоційну напруженість | В | Ч | П | Min |
| Сн | Стрес як стан підвищеної емоційної напруженості | В | Ч | П | Min |
| Нпг | Низька психологічна готовність до діяльності | С | Ч | П | Так |
| Нпм | Низька професійна майстерність | С | Ч | П | Так |
| Фвт | Фізична або психологічна втома | В | Ч | П | Min |
| Нд | Незвичайні умови діяльності. | С | Ч | П | Так |
| | ***Когнітивні фактори стану*** | | | | |
| Кс | Стомленість | Н | Ч | К | Min |
| Кн | Напруженість | Н | Ч | К | Так |
| Кінф | Інформаційна пропускна здатність | | Ч | К | Так |
| Ктр | Тривалість реакції | | Ч | П | Min |

## 3.3 Розробка та дослідження математичної моделі оцінки залежності процесу прийняття рішень від стану захищеності об'єкту критичної інфраструктури, з використанням інформаційно-когнітивних технологій.

Згідно Інформаційно – логічної моделі (рис.3.4) для оцінки та корекції стану інформаційного і кібернетичного захисту ОКІ розроблена Байєсовська мережа довіри (БМД), спрощена структура якої наведена на рисунку 3.12.

На сьогоднішній день однією з найбільш відповідних моделей, призначених для роботи з неповною, неточною і суперечливою інформацією, є

БМД, яка заснована на ймовірнісному підході і здатна у максимальному ступені використовувати інформацію, що надходить з виділених джерел для досягнення максимального ефекту.

Баєсові мережі - це графові моделі імовірнісних і причинно-наслідкових зв'язків між змінними в статистичному інформаційному моделюванні. У Баєсових мережах, можуть органічно поєднуватися емпіричні частоти, появи різних значень змінних, суб'єктивні оцінки «очікувань» і теоретичні уявлення про математичні ймовірності тих чи інших наслідків з апріорної інформації. Це являється важливою практичною перевагою і відрізняє Баєсові мережі від інших методик інформаційного моделювання [46].

Повна загальна ймовірність БМД обчислюється по формулі:

$$P_B(X^{(1)},...,X^{(N)}) = \prod_{i=1}^{N} P_B(X^{(i)} \mid P_A(X^{(i)})) \qquad (3.10)$$

де: А – безліч станів середовища; $N = (x_1,...,x_N)$ - вектор параметрів їх розподілів.

Умовна ймовірність події визначається співвідношенням:

$$p(E \mid H_k) = \frac{p(E \cap H_k)}{p(H_k)}, \qquad (3.11)$$

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

Взаємовиключні події формують вичерпну безліч, якщо

$$\bigcup_{i=1}^{n} E_i = \Omega. \qquad (3.12)$$

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

імовірностей:

$$p(E) = \sum_{i=1}^{n} p(E \cap H_i) = \sum_{i=1}^{n} p(E \mid H_i) \cdot p(H_i). \qquad (3.13)$$

Використовуючи формулу (2.50), імовірність перетинання подій $E$ і $H$ можна виразити в такий спосіб:

$$p(E \cap H_k) = p(E \mid H_k) \cdot p(H_k) = p(H_k \mid E) \cdot p(E),$$

звідки одержуємо:

$$p(H_k \mid E) = \frac{p(E \mid H_k) \cdot p(H_k)}{p(E)}. \qquad (3.14)$$

З урахуванням формули (2.51) і (2.53) можна представити так:

$$p(H_k \mid E) = \frac{p(E \mid H_k) \cdot p(H_k)}{\sum_{i=1}^{n} p(E \mid H_i) \cdot p(H_i)}. \qquad (3.15)$$

У математичній частині взаємозв'язку ймовірностей різних типів інформації представляється у формі графа. Повноцінна модель графа системи показана на рисунку 3.12.

При побудові структури БМД та таблиць умовних ймовірностей використовувалися експериментальні дані та знання експертів.

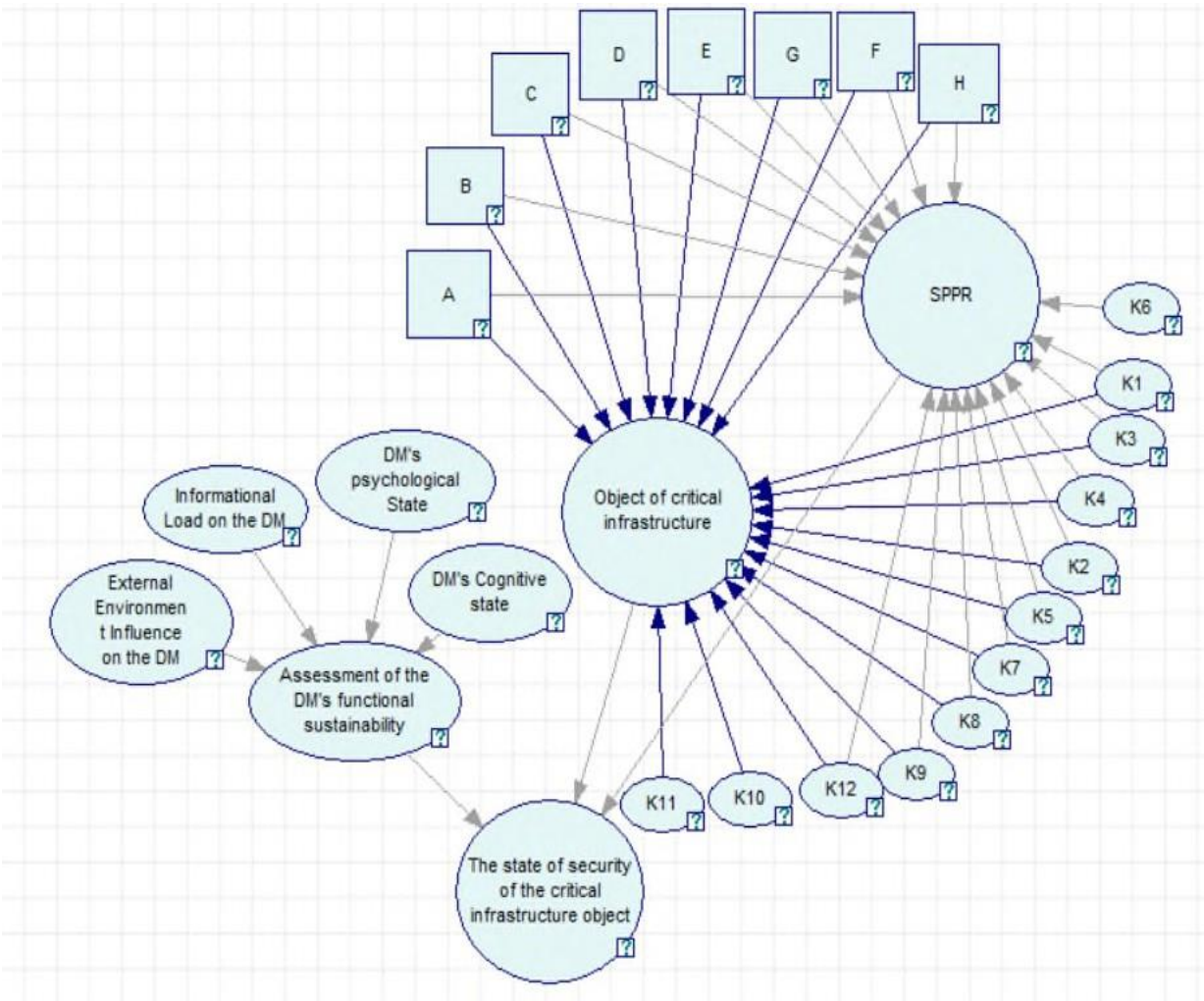


Рисунок 3.12 - Повноцінна модель БМД.

Вершини A,B,C,D,E,G,F,H,K2,K3,K1,K6,K8,K11,K10,K9,K7,K12,K5,K4 є вершинами типу ″decision″, відповідають однойменним модулям моніторингу ФС і модулям контролю ФС і можуть приймати три стани: ″висока захищенність″, ″середня захищенність″, ″низька захищенність″ [47].

Далі будемо позначати ці стани **вз**, **сз**, **нз** відповідно, а вершини (змінні) A,B,C,D,E,G,F,H,K2,K3,K1,K6,K8,K11,K10,K9,K7,K12,K5,K4 будемо позначати через $M_i$ $(i = \overline{1,20})$ відповідно.

Дані вершини (модулі) є комплексом основних показників ФС системи і представлені модулями моніторингу: модуль A - модуль попередньої підстановки в запити даних і перевірки на SQL - ін'єкції; модуль B - модуль перевірки системи на віруси; модуль C - модуль перевірки входу користувача з правами адміністратора; модуль D - модуль моніторингу апаратних збоїв;

модуль E - модуль моніторингу доступності даних і ресурсів; модуль F - модуль некоректності роботи користувачів; модуль G - модуль перевірки даних на цілісність (використовуючи хеш); модуль H - модуль моніторингу оцінки функціональної стабільності користувачів; модулями контролю: модуль K1- цілісність даних; модуль K2 - доступність даних; модуль K3 - конфіденційність даних; модуль K4 - узгодженість даних; модуль K5 - посилальна цінність; модуль K6 - зовнішній вплив; модуль K7 - відмови апаратного забезпечення; модуль K8

- відмови програмного забезпечення; модуль K9 - вплив дій користувачів; модуль K10 - вплив дій адміністраторів; модуль K11- захищеність даних; модуль K12 - енергетичні відмови.

Модулі виконують сканування, закріплених за ними секторів. При цьому ймовірність *P* безпеки модуля *M* оцінюється по формулі:

$$P_i = \frac{L_i}{N_i}, \qquad (3.16)$$

де: $L_i$ - кількість нормально функціонуючих секторів; $N_i$ - загальна кількість секторів, перевірених модулем $M_i$

По обчислених ймовірностях можна визначити стан вершин A,B,C,D,E,G,F,H,K2,K3,K1,K6,K8,K11,K10,K9,K7,K12,K5,K4 БСД за допомогою таблиці умовних ймовірностей можливих станів модулів моніторингу і контролю захищеності ОКІІ.

Для цього експертам-фахівцям, працюючим у розподілених організаційно-технічних системах критичного застосування, було запропоновано провести комплексну оцінку по ступеню важливості можливих ймовірностей стану данних модулів. Результати експертного оцінювання наведено в таблицях 3.3, 3.4.

Таблиця 3.3 -Таблиця умовних ймовірностей можливих станів модулів захищеності (I).

| **Вершина** | **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** |
|---|---|---|---|---|---|---|---|---|
| **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 | 0,95-1 |
| Середня | 0,4-0,95 | 0,4-0,9 | 0,4- 0,85 | 0,45- 0,95 | 0,4- 0,9 | 0,4- 0,8 | 0,4- 0,9 | 0,4-0,95 |
| Низька | 0 - 0,4 | 0 - 0,4 | 0 - 0,4 | 0 - 0,45 | 0 - 0,4 | 0 - 0,4 | 0 - 0,4 | 0 - 0,4 |

Таблиця 3.4 -Таблиця умовних імовірностей можливих станів модулів захищеності (K)

| **Вершина** | **K1** | **K2** | **K3** | **K4** | **K5** | **K6** | **K7** | **K8** | **K9** | **K10** | **K11** | **K12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Стан** | **Імовірність захищеності** | | | | | | | | | | | |
| Висока | 0,85-1 | 0,9--1 | 0,85-1 | 0,8-1 | 0,95-1 | 0,9-1 | 0,9-1 | 0,9-1 | 0,7-1 | 0,85-1 | 0,9-1 | 0,9-1 |
| Середня | 0,15-0,85 | 0,1-0,9 | 0,15-0,8 | 0,2-0,8 | 0,1-0,9 | 0,1-0,9 | 0,1-0,9 | 0,1-0,9 | 0,3-0,7 | 0,1-0,8 | 0,1-0,9 | 0,1-0,9 |
| Низька | 0-0,15 | 0-0,1 | 0-0,15 | 0-0,2 | 0-0,05 | 0-0,1 | 0-0,1 | 0-0,1 | 0-0,3 | 0-0,15 | 0-0,1 | 0-0,1 |

Вважаємо, що вершини мережі ″SOTO″, ″ARSPPR″, ″assessment of the DM's functional stability″ і ″ FUNCTIONAL STABILITY of the SYSTEM″ – бінарні, тобто мають два стани. Змінні ″SOTO″и ″ARSPPR″ можуть приймати значення: ″захищено″ і ″незахищено″, а змінні ″assessment of the DM's functional stability″ і ″ FUNCTIONAL STABILITY of the SYSTEM″ можуть приймати значення ″стабільна″ і ″нестабільна″. Оскільки розглянуті вершини мають велику кількість батьківських зв'язків, то для заповнення таблиць умовних ймовірностей знадобилася б величезна кількість табличних значень. Для зниження трудомісткості заповнення таблиць умовних ймовірностей цим вершинам зручно назначити тип Noisy MAX. Використання вершин типу Noisy MAX зручно ще й тому, що експертам значно простіше оцінювати вплив тільки одного фактора на очікувану подію, чим робити оцінку спільного впливу декількох факторів на нього [48].

Для опису зашумленних вершин ″SOTO″, ″ARSPPR″ і ″FUNCTIONAL STABILITY of the SYSTEM″ експертам-фахівцям було запропоновано провести оцінку по ступеню важливості умовних ймовірностей можливих станів

зазначених вершин. Результати представлені в таблицях 3.5, 3.6.

Таблиця 3.5 - Опис вузла ″SOTO″

| **Батько** | **A** | | | **B** | | |
|---|---|---|---|---|---|---|
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,7 | 0,15 | 0 | 0,65 | 0,1 | 0 |
| Захищене | 0,3 | 0,85 | 1 | 0,35 | 0,9 | 1 |
| **Батько** | **C** | | | **D** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,8 | 0,1 | 0 | 0,6 | 0,05 | 0 |
| Захищене | 0,2 | 0,9 | 1 | 0,4 | 0,9 | 1 |
| **Батько** | **E** | | | **F** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,7 | 0,05 | 0 | 0,75 | 0,15 | 0 |
| Захищене | 0,3 | 0,95 | 1 | 0,25 | 0,85 | 1 |
| **Батько** | **G** | | | **H** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,85 | 0,1 | 0 | 0,8 | 0,2 | 0 |
| Захищене | 0,15 | 0,9 | 1 | 0,2 | 0,8 | 1 |
| **Батько** | **K1** | | | **K2** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,6 | 0,1 | 0 | 0,75 | 0,1 | 0 |
| Захищене | 0,4 | 0,95 | 1 | 0,25 | 0,9 | 1 |
| **Батько** | **K3** | | | **K6** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,8 | 0,1 | 0 | 0,55 | 0,05 | 0 |
| Захищене | 0,2 | 0,9 | 1 | 0,45 | 0,95 | 1 |
| **Батько** | **K8** | | | **K11** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,6 | 0,1 | 0 | 0,7 | 0,15 | 0 |
| Захищене | 0,4 | 0,9 | 1 | 0,3 | 0,85 | 1 |

Таблиця 3.6 - Опис вузла ″ARSPPR″

| **Батько** | **A** | | | **B** | | |
|---|---|---|---|---|---|---|
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,7 | 0,05 | 0 | 0,55 | 0,1 | 0 |
| Захищене | 0,3 | 0,95 | 1 | 0,45 | 0,9 | 1 |
| **Батько** | **C** | | | **D** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,8 | 0,2 | 0 | 0,65 | 0,1 | 0 |
| Захищене | 0,2 | 0,8 | 1 | 0,35 | 0,9 | 1 |
| **Батько** | **E** | | | **F** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,7 | 0,1 | 0 | 0,6 | 0,05 | 0 |
| Захищене | 0,3 | 0,9 | 1 | 0,4 | 0,95 | 1 |
| **Батько** | **G** | | | **H** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,55 | 0,1 | 0 | 0,7 | 0,15 | 0 |
| Захищене | 0,45 | 0,9 | 1 | 0,3 | 0,85 | 1 |
| **Батько** | **K1** | | | **K2** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,4 | 0,05 | 0 | 0,5 | 0,1 | 0 |
| Захищене | 0,6 | 0,95 | 1 | 0,5 | 0,9 | 1 |
| **Батько** | **K3** | | | **K6** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,7 | 0,2 | 0 | 0,6 | 0,1 | 0 |
| Захищене | 0,3 | 0,8 | 1 | 0,4 | 0,9 | 1 |
| **Батько** | **K8** | | | **K11** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,55 | 0,1 | 0 | 0,6 | 0,1 | 0 |
| Захищене | 0,45 | 0,9 | 1 | 0,4 | 0,9 | 1 |
| **Батько** | **K10** | | | **K9** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,45 | 0,15 | 0 | 0,7 | 0,15 | 0 |
| Захищене | 0,55 | 0,85 | 1 | 0,3 | 0,85 | 1 |
| **Батько** | **K7** | | | | | |
| **Стан** | **нз** | **сз** | **вз** | | | |
| Незахищене | 0,65 | 0,05 | 0 | | | |
| Захищене | 0,35 | 0,95 | 1 | | | |

Таблиця 3.7 - Опис вузла ″FUNCTIONAL STABILITY of the SYSTEM″

| **Батько** | **К7** | | | **К12** | | |
|---|---|---|---|---|---|---|
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,25 | 0,07 | 0 | 0,2 | 0,05 | 0 |
| Захищене | 0,75 | 0,93 | 1 | 0,8 | 0,95 | 1 |
| **Батько** | **К5** | | | **К4** | | |
| **Стан** | **нз** | **сз** | **вз** | **нз** | **сз** | **вз** |
| Незахищене | 0,25 | 0,05 | 0 | 0,3 | 0,1 | 0 |
| Захищене | 0,75 | 0,95 | 1 | 0,7 | 0,9 | 1 |
| **Батько** | **SOTO** | | | **ARSPPR** | | |
| **Стан** | незахищене | | захищене | незахищене | | захищене |
| Нестабільна | 0,15 | | 0 | 0,13 | | 0 |
| Стабільна | 0,85 | | 1 | 0,87 | | 1 |
| **Батько** | **Assessment of the DM's functional stability** | | | | | |
| **Стан** | нестабільна | | | стабільна | | |
| Нестабільна | 0,2 | | | 0 | | |
| Стабільна | 0,8 | | | 1 | | |

Оскільки вершинам ″SOTO″ і ″ARSPPR″ був призначений тип Noisy MAX, то тим самим було зроблене допущення про те, що стан вершини $M_j$ впливає на ймовірності станів вершин ″SOTO″ і ″ARSPPR″ незалежно від того в якому стані перебувають вершини $M_i$ ($i = \overline{1,20},\ i \neq j$,) Тому ймовірності $P_{\text{SOTO}}$ й $P_{\text{ARSPPR}}$ того, що вершини ″SOTO″ і ″ARSPPR″ перебувають у стані ″захищено″ можна обчислити по формулах:

$$P_{\text{SOTO}} = \prod_{i=1}^{14} P(\text{SOTO} \mid M_i), \tag{3.17}$$

$$P_{\text{ARSPPR}} = \prod_{i=1}^{17} P(\text{ARSPPR} \mid M_i) \tag{3.18}$$

де: $P(\text{SOTO} \mid M_i)$ і $P(\text{ARSPPR} \mid M_i)$ – ймовірності того, що вершини ″SOTO″ і ″ARSPPR″ перебувають у стані ″захищено″ за умови, що вузол $M_i$ перебуває в одному зі станів: ″висока захищенність″, ″середня захищенність″, ″низька захищенність″.

У людино-машинних системах критичного застосування найбільш нестабільним звіном є ОПР, на кожному ієрархічному рівні керування ОКІІ, що вимагає окремого розгляду оцінки ФС ОПР при функціонуванні ОКІІ в реальному часі. Модуль оцінки ФС ОПР представлений вершиною мережі ″assessment of the Dm's functional stability″.

На функціональну стійкість ОПР, в основному, впливають 4 фактора [48]: зовнішнє середовище, інформаційне навантаження, його психологічний і когнітивний стан. Це відображено на Байесовській мережі тим, що вершина ″assessment of the DM's functional stability″ має 4 батьківських вершини: ″ External Environment Influence on the DM″, ″ Informational Load on the DM″, ″ DM's psychological State ″, ″ DM's Cognitive state ″. На рисунку 3.12 ці вершини позначені як EE, I L, PS, CS відповідно. Будемо вважати, що змінні мережі EE, I L, PS, CS – бінарні і можуть приймати значення: ″positive″ і ″negative″.

Експертами-фахівцями на ОКІІ була проведена оцінка, по ступеню важливості, умовних ймовірностей можливих станів вузла типу ″noisy MAX″ ″assessment of the DM's functional stability″. Результати представлені в таблиці 3.8.

Таблиця 3.8 - Опис вузла ″assessment of the Dm's functional stability″

| Батько | Informational Load on the DM | | External Environment Influence on the DM | | Інші причини |
|---|---|---|---|---|---|
| Стан | negative | positive | negative | positive | |
| unstable | 0,67 | 0,0 | 0,85 | 0,0 | 0,01 |
| stable | 0,33 | 1,0 | 0,15 | 1,0 | 0,99 |
| батько | DM's Cognitive state | | DM's psychological State | | інші |
| стан | negative | positive | negative | positive | причини |
| unstable | 0,62 | 0,0 | 0,73 | 0,0 | 0,01 |
| stable | 0,38 | 1,0 | 0,27 | 1,0 | 0,99 |

Застосуємо типи вузлів ″ Chance - General ″ для родительських вузлів EE, I L, PS, CS.

Спосіб оцінки ймовірностей станів вершин EE і I L докладно викладений у роботі [49]. Нижче коротко дана суть цього підходу.

Розглянемо вузол EE. На випадкову величину ″external Environment Influence on the DM″ впливають наступні фактори: інтенсивність виробничого шуму IN;

інтенсивність і частота вібрацій IV; освітленість робочого місця E; температура T; рівень електромагнітного впливу f; перепади атмосферного тиску $\Delta P/\Delta t$. Існують нормативні значення цих факторів, при яких вплив факторів зовнішнього середовища вважається позитивним ( комфортним) для ОПР.

Чим значніше відрізняються значення зовнішніх факторів і когнітивних складових від нормативних, тим ймовірніше, що їхній вплив на ОПР буде негативним. Для прогнозування ймовірностей впливу значень даних факторів, в основу покладений нечіткий логічний вивод по алгоритму Мамдані по нечіткій базі знань, у якій значення вхідної і вихідної змінної задані нечіткими множинами. Для настроювання нечіткої моделі F вирішується завдання математичного програмування про мінімізацію значення середньоквадратичній неув'язки, що виникає через різницю між експериментальними результатами та результатами, обчисленими по алгоритму Мамдані. Аналогічно вирішується завдання на базі експериментальних даних і знань експертів у середовищі **Fuzzy Logic Toolbox** і **Optimization Toolbox**, як при впливі навколишніх факторів середовища на ОПР так і його когнітивній складовій.

На рисунках 3.13-3.15 представлені результати розрахунку ймовірності стану захищеності ОКІІ, при низькій, середній і високій захищеності.

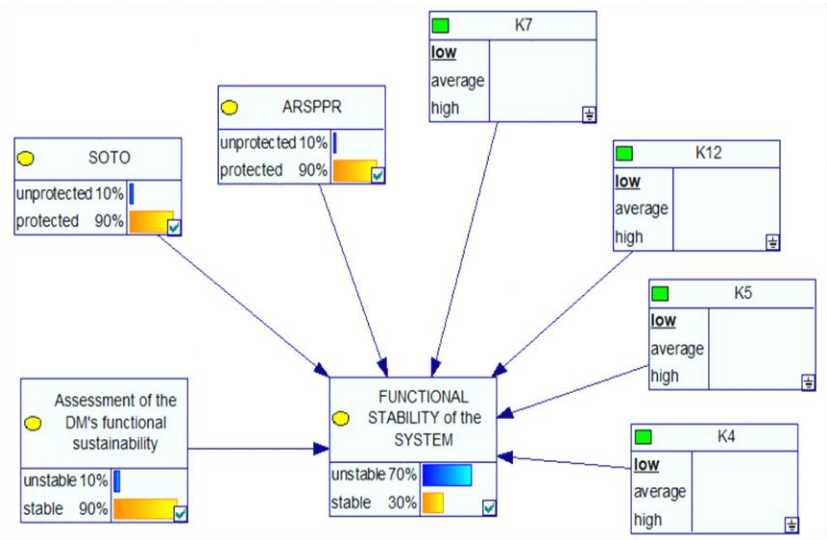


Рисунок 3.13 – Результати розрахунку ймовірності стану захищеності ОКІІ по описаному алгоритму, при низькій захищеності K4,K5,K7.

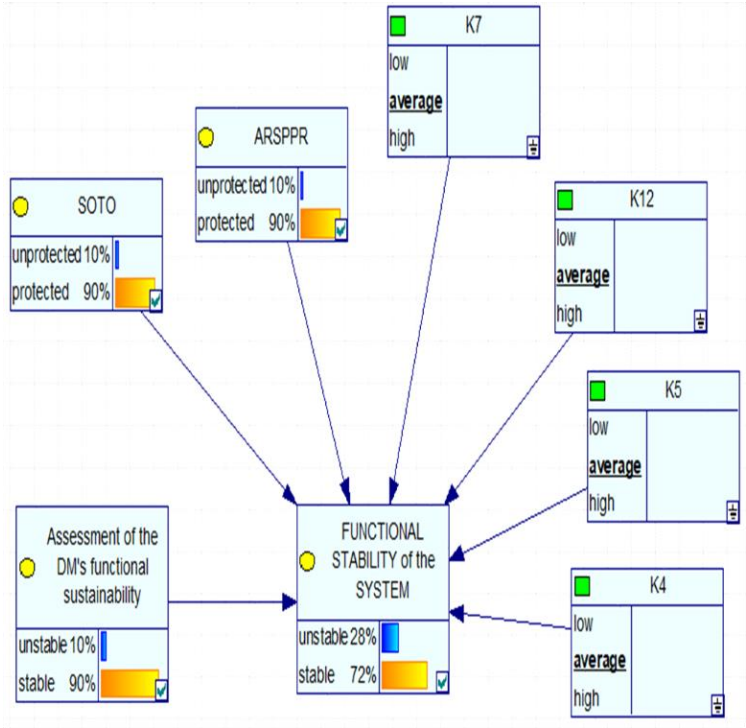


Рисунок 3.14 – Результати розрахунку ймовірності стану захищеності ОКІІ по описаному алгоритму, при середній захищеності К4,К5,К7, К12.

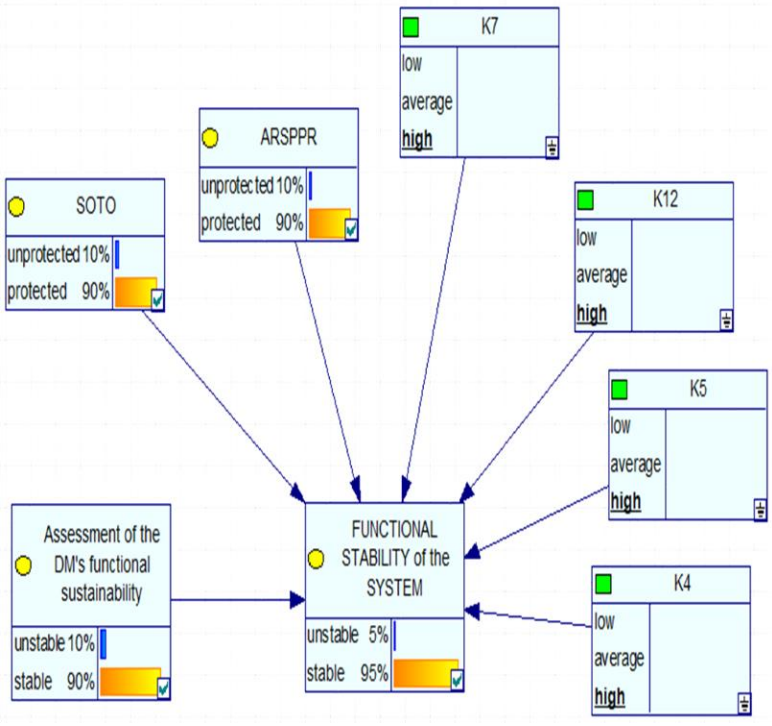


Рисунок 3.15 – Результати розрахунку ймовірності стану захищеності ОКІІ по описаному алгоритму, при високій захищеності К4,К5,К7,К12

Висновки розділу 3:

У результаті виконання розділу обґрунтовано доцільність застосування інформаційно-когнітивних технологій для дослідження залежності процесу прийняття рішень від стану захищеності об’єктів критичної інфраструктури в умовах комплексних і динамічних загроз. Розроблена інформаційна модель впливу основних факторів загроз дозволяє структуровано подати взаємозв’язки між кібернетичними, фізичними та гібридними загрозами, параметрами стану захищеності об’єкта та управлінськими рішеннями, що створює основу для системного аналізу процесів управління.

Проведена оцінка впливу основних факторів загроз показала, що їх дія має нелінійний і взаємопов’язаний характер, а зміна інтенсивності окремих загроз може призводити до суттєвих коливань стану захищеності та ефективності прийнятих рішень. Застосування когнітивних підходів і експертних оцінок дало змогу врахувати невизначеність, якісні характеристики загроз та когнітивні особливості осіб, які приймають рішення, що підвищує обґрунтованість результатів оцінювання.

Розроблена та досліджена математична модель оцінки залежності процесу прийняття рішень від стану захищеності об’єкта критичної інфраструктури забезпечує формалізований опис взаємодії факторів загроз, когнітивних параметрів і управлінських альтернатив. Модель поєднує числові та нечислові параметри, що дозволяє застосовувати її в умовах неповної та нечіткої інформації, а також використовувати як основу для побудови систем підтримки прийняття рішень. Отримані результати підтверджують ефективність інформаційно-когнітивного підходу та можливість його практичного застосування для підвищення рівня захищеності і надійності функціонування об’єктів критичної інфраструктури.

# ВИСНОВКИ

У магістерській кваліфікаційній роботі виконано комплексне дослідження залежності процесу прийняття управлінських рішень від стану захищеності об’єкта критичної інфраструктури з використанням інформаційно-когнітивних технологій. Актуальність теми зумовлена зростанням складності та інтенсивності загроз, що впливають на функціонування критично важливих об’єктів, а також необхідністю підвищення обґрунтованості управлінських рішень в умовах невизначеності, дефіциту часу та інформації.

Проаналізовано основні особливості процесу прийняття рішень в управлінні об’єктом критичної інфраструктури. Встановлено, що даний процес має системний, багаторівневий і динамічний характер та формується під впливом комплексу технічних, організаційних, інформаційних і когнітивних факторів. Показано, що стан захищеності об’єкта виступає ключовим інтегральним показником, який визначає допустимі сценарії управління, рівень ризику та характер управлінських дій. Обґрунтовано необхідність урахування зворотних зв’язків між прийнятими рішеннями та подальшою зміною стану захищеності об’єкта критичної інфраструктури.

Здійснено аналіз сучасних методів та способів дослідження процесу прийняття рішень в управлінні об’єктом критичної інфраструктури. Визначено, що традиційні детерміновані та суто імовірнісні підходи мають обмежені можливості щодо відображення складних причинно-наслідкових зв’язків і когнітивних аспектів управління. Проаналізовано імовірнісні, нечіткі, мультикритеріальні, імітаційні та гібридні методи, а також встановлено доцільність їх інтеграції в межах єдиного методологічного підходу. Зроблено висновок, що найбільш перспективними є методи, здатні поєднувати формалізовані дані з експертними знаннями та враховувати динаміку стану захищеності об’єкта.

Обґрунтовано застосування методів інформаційно-когнітивних технологій для оцінки залежності процесу прийняття рішень від стану

захищеності об’єкта критичної інфраструктури. Розроблено інформаційно-когнітивну модель, яка дозволяє формалізувати вплив основних факторів загроз на стан захищеності та відобразити механізм трансформації інформації про цей стан у управлінські рішення. Запропонований підхід забезпечує можливість врахування невизначеності, неповноти інформації та когнітивних особливостей суб’єктів управління, а також створює основу для побудови автоматизованих систем підтримки прийняття рішень.

У результаті виконання роботи досягнуто поставленої мети та вирішено основні завдання дослідження. Практична цінність отриманих результатів полягає в можливості використання запропонованої інформаційно-когнітивної моделі для підвищення ефективності управління захищеністю об’єктів критичної інфраструктури, зокрема в системах технічного захисту інформації та автоматизованої обробки даних. Запропоновані підходи можуть бути використані при розробленні та вдосконаленні систем моніторингу, аналізу загроз і підтримки прийняття рішень.

# СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Доктрина інформаційної безпеки України від 25 лютого 2017 року №47/2017.

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

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

4. 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

5. Закон України Про основні засади забезпечення КБ Форма доступу - https://zakon.rada.gov.ua/laws/show/2163-19

6. Закон України «Про інформацію» Редакція від 16.07.2020 Форма доступу - https://zakon.rada.gov.ua/laws/show/2657-12

7. Закон України «Про захист інформації в інформаційно телекомунікаційних системах» Редакція від 04.07.2020 Форма доступу - https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

8. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» Редакція від 10.02.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

9. Закон України «Про захист персональних даних» Редакція від 15.12.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/2297-17 10. Закон України «Про державну таємницю» Редакція від 24.11.2021 Форма доступу - https://zakon.rada.gov.ua/laws/show/3855-12

10. Thor Olavsrud. 4 information security threats that will dominate 2017. CIO (December 29, 2016) [Online tool]. – Available at : https:// cio.com/article/ 3153706/security/4-information-security-threats-thatwill-dominate-2017.html.

11. Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions / L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi,

A. Dejamkhooy, R. Bayindir, M. Iranpour // 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, Odisha, July 29–31, 2020, Keonjhar, Odisha, India. P. 1–8.

12. Тарасенко Ю.С., Соляннiков В.Г., Калюжний О.Е. Концептуально гносеологічні аспекти інформаційної безпеки (захищеності) з позицій соціальної інженерії, DOI: УДК 621.396.96 ISSN 2521-6643 Системи та технології № 2 (60) 2020 с.39-50

13. Тарасенко Ю.С., Соляннiков В.Г., Бруй І.І. Кібербезпека: інформаційні аспекти захисту від технологій впливу, Міжнародна науковопрактична інтернет-конференція «Інноваційні рішення в економіці, бізнесі, суспільних комунікаціях та міжнародних відносинах» (16 квітня 2021, Дніпро). – Дніпро: Університет митної справи та фінансів, 2021. с.424-426

14. Kaspersky Security Network. Развитие информационных угроз во втором квартале 2021 года. Отчеты о вредоносном ПО. Мобильная статистика. Целевые атаки. 12 авг 2021. https://securelist

15. Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions / L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi,

A. Dejamkhooy, R. Bayindir, M. Iranpour // 2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE), Keonjhar, Odisha, July 29–31, 2020, Keonjhar, Odisha, India. P. 1–8.

16. Прокопович–Ткаченко Д.І., Стелюк Б.Б., Соляннiков В.Г., Підходи до авторизації та автентифікації безпроводового доступу комунікаційних систем // Матеріали міжнародної науково–практичної конференції “Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення”. – ТНЕУ, Тернопіль, 2019 (43), С. 93–95.

17. Северина, С. В. Інформаційна безпека та методи захисту інформації / С. В. Северина // Вісник Запорізького національного університету. Економічні науки. – 2016. – № 1. – С. 155–161.

18. Гончар С.Ф. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури / Мохор В.В., Дибач О.М. // Ядерна та радіаційна безпека. – 2019. – №2(82). – С.57-61.

19. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об’єктів критичної інфраструктури. Монографія. К.:«Альфа Реклама», 2019.176с.

20. Мохор В. В., Гончар С. Ф., Дибач О. М. Методи оцінки сумарного ризику кібербезпеки об’єктів критичної інфраструктури. Ядерна та радіаційна безпека, 2019. № 2(82). С. 4-8. doi: 10.32918/nrs.2019.2(82).01.

21. Ерохин В. В., Погонышева Д. А., Степченко И. Г. Безопасность информационных систем: учебное пособие. М.: «Флинта», 2016. 184 с.

22. Чио К., Фримэн Д. Машинное обучение и безопасность. Пер. с анг. А.В. Снастина. М.: ДМК Пресс, 2020. 388 с.

23. Hentea M. Improving security for SCADA control systems. Interdisciplinary Journal of Information, Knowledge, and Management. 2008. Vol. 3, P. 73-86. doi: 10.28945/91.

24. Izadi M., Hosseinian S. H., Dehghan S., Fakharian A., Amjady N. A critical review on definitions, indices, and uncertainty characterization in resiliency-oriented operation of power systems. International Transactions on Electrical Energy Systems. 2021. V. 31(1). doi: 10.1002/2050-7038.12680.

25. Krings A., Oman P. A simple GSPN for modeling common mode failures in critical infrastructures. Proceedings of the 36th Annual Hawaii International Conference on System Sciences, 2003. Big Island, HI, USA, 2003, HICSS 2003, P. 10-19. doi: 10.1109/HICSS.2003.1174908.

26. Kosko B. Fuzzy Cognitive Maps // International Journal of Man-Machine Studies. – 1986. – Vol. 24(1). – P. 65–75.

27. Е. А. Зюзикова, "Использование нечеткой гибридной модели для анализа рисков информационной безопасности", Научный журнал «Студенческий», № 11 (31), с. 5-7, 2018.

28. Information Security Risk Analysis SWOT. / Shevchenko H. and an. Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine. P. 309 – 317. http://ceur-ws.org/Vol-2923/paper34.pdf

29. О. В. Салієва,та Ю. Є. Яремчук, "Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі", Реєстрація, зберігання і обробка даних, т. 21, № 4, с. 28-39, 2019.

30. О. В. Салієва, та Ю. Є. Яремчук, "Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання", Безпека інформації, № 1, с. 42- 49, 2020.

31. О. В. Салієва, та Ю. Є. Яремчук, "Когнітивна модель для дослідження рівня захищеності об'єкта критичної інфраструктури", Безпека інформації, т. 26, № 2, с. 64-73, 2020.

32. Національний інститут стандартів та технологій (NIST) США. URL: https://www.nist.gov/ cyberframework / cybersecurity-framework (дата звернення: 10.02.2023).

33. Європейське агентства з кібербезпеки (ENISA). URL: https: // www.enisa.europa.eu/topics/cybersecurity-act/cybersecurity-certification (дата звернення: 15.02.2023).

34. Міжнародна організація зі стандартизації (ISO). URL:https://www.nist.gov/cyberframework/cybersecurity - framework (дата звернення: 10.02.2023).

35. NIST Cybersecurity Framework, NIST. URL: https://www.nist.gov/cyberframework (дата звернення: 11.02.2023).

36. Introduction to the Cybersecurity Capability Maturity Model (C2M2), NIST. URL: https://www. nist. gov/services-resources/software/cybersecurity-evaluation-tool-cset (дата звернення: 11.03. 2023).

37. Cybersecurity Evaluation Tool, CSET.URL: https://www.nist.gov/cyberframework/cybersecurity framework (дата звернення: 10.02.2023).

38. Cybersecurity of AI and Standardisation. URL https:// www. enisa. europa.eu /publications /cybersecurity-of-ai-and-standardisation (дата звернення: 22.02.2023).

39. Embedded Sim Ecosystem, Security RisksandMeasures. URL: https: //www.enisa.europa. eu/ publications/embedded-sim-ecosystem-securityrisks-and-measures (дата звернення: 11.03.2023).

40. Saliieva O., Yaremchuk Yu. Determining the level of security of the information security system based on cognitive modeling // Ukrainian Scientific Journal of Information Security, 2020, vol. 26, issue 1, pp. 42-49.

41. Про основні засади забезпечення кібербезпеки України, Закон України № 2163-VIII (2021) (Україна). https://zakon.rada.gov.ua/laws/show/2163-19#Text

42. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України", Указ Президента України № 96/2016 (2021) (Україна). https://zakon.rada.gov.ua/laws/show/96/2016#Text

43. Terje Aven. Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*. 2016. V. 253. № 1. P. 1–13.

44. Jain P., Pasman H. J., Waldram S., Pistikopoulos E. N., Mannan M. S. Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management. *Journal of Loss Prevention in the Process Industries*. 2018. V. 53. P. 61–73.

45. Сазонов А.Е. Применение общесудовых экспертных систем контроля безопасности для снижения влияния человеческого фактора на аварийность судов / А.Е. Сазонов, А.В. Козлов. Рос. мор. Регистр судоходства. Научно техн. сб. вып. 24. – СПб, 2001.

46. 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.

47. Perederiy V., Borchik E. Information technology for determination, assessment and correction of functional sustainability of the human-operator for the

relevant decision-making in human-machine critical application systems. Theoretical and practical aspects of the development of modern science: the experience of countries of Europe and prospects for Ukraine: monograph. Riga, Latvia: “Baltija Publishing”, 2019. – Pp. 490-509.

48. Viktor Perederyi, Eugene Borchik, Oksana Ohnieva Information Technology of Control and Support for Functional Sustainability of Distributed Man-Machine Systems of Critical Application (2019) Lecture Notes in Computational Intelligence and Decision Making.Proceedings of the XV International Scientific Conference “Intellectual Systems of Decision Making and Problems of Computational Intelligence” (ISDMCI'2019), Ukraine, May 21–25, 2019. Pages 461-477 https://link.springer.com/chapter/10.1007/978-3-030-26474-1_33 (https://doi.org/10.1007/978-3-030-26474-1_33)]

49. Viktor Perederyi, Eugene Borchik, Oksana Ohnieva Information Technology of Control and Support for Functional Sustainability of Distributed Man-Machine Systems of Critical Application (2019). Advances in Intelligent Systems and Computing, 2020, 1020, pp. 461–477https://link.springer.com/chapter/10.1007/978-3-030-26474-1_33 (https://doi.org/10.1007/978-3-030-26474-1_33).