МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

ЗАХАРЧЕНКО ВОЛОДИМИР ДМИТРОВИЧ

Допускається до захисту:
завідувач кафедри Луценко А.В.,
д-р філософії з математики
_____ А. В. Луценко
«____» _____ 20__ р.

Аналіз математичних моделей оцінки безпеки об'єкта критичної інфраструктури в умовах інформаційної невизначеності

Спеціальність 113 Прикладна математика

Кваліфікаційна (бакалаврська) робота

Керівник:
Загоруйко Л. В., к.т.н, доцент
доцент кафедри прикладної
математики та кібербезпеки,

Оцінка:____/ ____/ _____
Голова ЄК: _____

Вінниця - 2025

ЗМІСТ

ВСТУП

Світ дедалі частіше стикається з викликами, що ставлять під загрозу не лише функціонування окремих об’єктів інфраструктури, а й безпеку цілих держав. Ідеться не тільки про збройні конфлікти, терористичні атаки чи техногенні катастрофи, а й про менш очевидні, але не менш небезпечні загрози: кібератаки, інформаційні операції, порушення логістичних ланцюгів, міжмережеву вразливість. У цьому контексті особливого значення набуває забезпечення стійкості й захищеності об’єктів критичної інфраструктури, зокрема в умовах інформаційної невизначеності, коли дані про ризики є фрагментарними, неповними або двозначними.

Актуальність теми зумовлена різким зростанням кількості інцидентів, що порушують функціональність критичних систем — як у цивільному, так і у воєнному контексті. Як показують аналітичні матеріали Національного інституту стратегічних досліджень [5], з 2014 року Україна пережила декілька хвиль атак на енергетичну, транспортну, цифрову інфраструктури. Після повномасштабного вторгнення РФ у 2022 році ці виклики вийшли на якісно новий рівень. Критична інфраструктура стала не лише об’єктом нападу, а й центральним елементом стратегії гібридної війни.

За класифікацією, поданою у Законі України «Про критичну інфраструктуру» [1], до таких об’єктів відносять системи енергозабезпечення, водопостачання, охорони здоров’я, зв’язку, транспорту, інформаційних технологій та інші. Їхня неперервна робота є умовою базової життєдіяльності суспільства. Але саме ці системи найчастіше функціонують в умовах, коли оцінити всі ризики наперед складно або неможливо. Наявність інформаційної невизначеності — постійний чинник у процесі прийняття рішень у сфері безпеки.

Науковці, зокрема Aven [8], неодноразово звертали увагу на необхідність адаптації класичних підходів до оцінки ризиків у відповідь на ці реалії. У своїх

дослідженнях він доводить, що в ситуаціях, де точна вірогідність загрози або її наслідків невідома, потрібно використовувати методи, які допускають обробку розмитих, ймовірнісних або якісних даних. Цю думку підтримує і Paté-Cornell [11], яка зазначає, що ефективне управління безпекою повинне спиратись на багаторівневу систему оцінки, в якій поєднуються математичні моделі, експертні оцінки та адаптивні сценарії.

Попри це, в українському контексті ще не склалася єдина методологія, яка дозволила б комплексно моделювати стан безпеки об'єкта критичної інфраструктури в умовах часткової або розмитої інформації. Саме ця прогалина й визначила фокус нашого дослідження.

Об'єктом дослідження є критична інфраструктура як система, що функціонує під впливом багатьох факторів ризику. **Предметом дослідження** є математичні моделі оцінки безпеки таких об'єктів в умовах інформаційної невизначеності.

Метою роботи є аналіз існуючих математичних підходів до оцінки безпеки об'єктів критичної інфраструктури, адаптованих до роботи в умовах неповної інформації, а також побудова моделі, що дозволяє здійснювати практичну оцінку безпеки конкретного об'єкта.

Для досягнення поставленої мети визначено такі завдання:

- дослідити понятійний апарат та класифікацію об'єктів критичної інфраструктури;
- проаналізувати фактори, що формують інформаційну невизначеність у контексті безпеки;
- систематизувати сучасні математичні моделі, які застосовуються для оцінки ризиків;
- виявити особливості застосування нечіткої логіки, ймовірнісних підходів, байєсівських мереж у моделях безпеки;

- розробити адаптовану модель, здатну обробляти неповні дані про загрози та вразливості;
- провести її апробацію на прикладі реального об’єкта інфраструктури.

Методологічну основу роботи становлять математичні підходи до моделювання системної безпеки, серед яких особливу роль відіграють:

- **нечітка логіка**, як спосіб формалізації нечітких оцінок (застосована, зокрема, у працях Мозгового [7]);
- **байєсівські мережі**, що дозволяють враховувати ймовірнісну природу зв’язків у складних системах (Сафонов, Кириленко [10]);
- **імовірнісні та сценарні моделі**, що дають змогу прогнозувати динаміку змін у безпековому середовищі (Aven [8], Bier [25]).

Наукова новизна полягає у спробі поєднати кілька різнорідних підходів до моделювання ризиків в умовах невизначеності у єдину інтегровану структуру, придатну до практичного застосування.

Практична значущість дослідження полягає в можливості адаптувати результати до реальних об’єктів — наприклад, електропідстанцій, вузлів зв’язку, логістичних центрів, де неможливо отримати повні або точні дані про всі потенційні загрози. Побудована модель може бути використана для формування аналітичних звітів, оцінки готовності до надзвичайних ситуацій, визначення пріоритетів захисту.

У процесі аналізу джерел було встановлено, що більшість наукових праць, таких як дослідження Zio [6] чи Shafer [17], орієнтовані на фундаментальне обґрунтування моделей. Водночас практичні аспекти реалізації у критичних умовах (де рішення треба ухвалювати швидко й на основі неповної інформації) часто залишаються поза фокусом. Наприклад, у роботі Wang і El-Sharkawy [22] моделювання ризиків базується на ідеальних припущеннях про доступність даних. Це знижує адаптивність таких підходів до реальних українських умов.

Натомість у вітчизняній літературі з’являються спроби інтегрувати гібридні підходи — так, у статті Шостака [12] представлено метод поєднання статистичної обробки даних із нечіткою логікою. Цей підхід має потенціал для подальшого розвитку. Крім того, слід відзначити роботу Бондаренка [13], який пропонує сценарний підхід до формалізації моделей ризику, спираючись на реальні кейси з енергетичної галузі.

Серед методів обробки нечіткої та недостатньої інформації особливе місце займає модель довіри Шефера [17]. Вона дозволяє оцінити ступінь обґрунтованості тверджень навіть за відсутності точних даних, що критично важливо для швидкого реагування на загрози. Аналогічно, Shafer [17] пропонує використовувати «математичну теорію доказів» як альтернативу класичній логіці, особливо в тих випадках, коли ймовірності подій важко формалізувати.

У практичному плані робота спирається також на прикладні дослідження Horváth [27], який демонструє використання мультикритеріальних моделей для обґрунтування пріоритетів безпеки, коли ресурси обмежені. Це дозволяє не лише моделювати загрози, а й приймати рішення щодо їх нейтралізації в умовах реального обмеження часу й фінансування.

Структура роботи побудована за логікою поетапного руху від теоретичних положень до прикладної реалізації. У першому розділі проаналізовано базові поняття, що стосуються критичної інфраструктури, її вразливостей і класифікацій загроз. У другому — зібрано та систематизовано наявні математичні моделі, що дозволяють працювати з неповними даними. Третій розділ присвячено побудові власної моделі оцінки безпеки із подальшою валідацією на конкретному прикладі.

Отже, дослідження поєднує аналітичний, методологічний та прикладний підходи, намагаючись не лише описати проблему, а й запропонувати шлях до її вирішення.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ОЦІНКИ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1. Поняття та класифікація об'єктів критичної інфраструктури

У повсякденному житті ми часто не замислюємось, що за стабільною подачею електроенергії, води, функціонуванням транспорту чи банківської системи стоїть ціла мережа взаємопов'язаних елементів. Їхня робота здається чимось самоочевидним, доти, доки не стається аварія або не спрацьовує зовнішній вплив. Саме в ці моменти стає зрозумілим: існує рівень інфраструктури, збій в якій спричиняє не лише тимчасовий дискомфорт, а й масштабні проблеми для регіонів, галузей, а іноді — й держав. Йдеться про об'єкти критичної інфраструктури.

Попри широке вживання цього терміна у політичному, безпековому й науковому дискурсах, навіть на рівні міжнародних інституцій ще не склалося абсолютно уніфікованого визначення. Втім, практичні підходи до розуміння критичної інфраструктури переважно сходяться на кількох базових ознаках. Передусім, це системна значущість, масштаб впливу, взаємозалежність, і — що не менш важливо — вразливість до цілеспрямованих або випадкових впливів.

У межах українського нормативного поля термін «критична інфраструктура» чітко зафіксовано в Законі України «Про критичну інфраструктуру» від 2021 року. У ньому зазначається, що це об'єкти, системи та ресурси, що мають стратегічне значення для національної безпеки, економіки, охорони здоров'я, екології, публічного порядку, а також забезпечення основних потреб населення у критичних ситуаціях [1]. Важливим тут є те, що критичність визнається не тільки на основі галузевої приналежності, а й з огляду на потенційні наслідки їхньої дестабілізації. Тобто навіть приватний суб'єкт може бути

визнаний критичним, якщо його функціонування є важливим для життєздатності певної території чи сектора.

Проблема точного визначення поняття критичної інфраструктури, за словами Тарасова, не є суто термінологічною. У своєму дослідженні він стверджує, що від способу трактування цього терміну залежать як механізми ідентифікації об’єктів, так і способи їхнього захисту, моделі оцінки ризиків, порядок міжвідомчої взаємодії [4]. Це підтверджується і на міжнародному рівні — наприклад, у практиках НАТО та ЄС існують відмінності в переліку галузей, які вважаються критичними, хоча в основі часто лежать одні й ті самі принципи.

Ключовим параметром, який дозволяє говорити про той чи інший об’єкт як критичний, є масштаб потенційного впливу його зупинки або виведення з ладу. Наприклад, у разі знищення трансформаторної підстанції наслідки не обмежуються лише територією, яку вона обслуговує. Ланцюговий ефект призводить до порушення енергетичних балансів, збою в інших системах, відключення серверів, порушення логістики — що в умовах воєнного або кризового часу стає критичним для всієї держави.

Саме через таку системну складність дослідники, зокрема Гвоздь, наголошують: об’єкти критичної інфраструктури мають розглядатися не ізольовано, а як частини взаємозалежних мереж, де збій на одному рівні може викликати каскад порушень на інших [5]. У цьому контексті особливої ваги набуває поняття міжгалузевої взаємозалежності. Наприклад, робота лікарні залежить не лише від медичного персоналу та обладнання, а й від постачання електрики, води, каналізації, інтернету, логістики постачання ліків, банківської системи для виплат. Будь-який збій у ланцюгу — і лікарня втрачає здатність надавати послуги.

З огляду на такі зв’язки, класифікація критичних об’єктів є не лише теоретичним інструментом, а й практичним механізмом управління ризиками. За

підходами, які описує Lewis, критичну інфраструктуру можна поділити на сектори за функціональним принципом: енергетика, транспорт, зв'язок, охорона здоров'я, банківська система, хімічна промисловість, продовольча безпека, цифрові системи, водопостачання, державне управління тощо [19]. У багатьох країнах, зокрема у США, Канаді, країнах ЄС, таке секторальне розбиття використовується як базове для формування політики захисту.

В Україні теж імплементовано подібний підхід, хоча зі специфікою, зумовленою реаліями війни. Наприклад, на рівні Кабінету Міністрів визначено 14 критичних секторів, серед яких — енергетика, транспорт, фінанси, охорона здоров'я, цифрові послуги, комунальна інфраструктура, оборонна промисловість тощо. При цьому на практиці класифікація є досить умовною, бо в умовах війни майже кожен об'єкт може стати критичним — залежно від конкретного сценарію розвитку подій.

Крім секторального підходу, активно застосовується також поділ за рівнем значущості. За словами Камінського, об'єкти можна умовно розділити на національні, регіональні та локальні за масштабом впливу на систему безпеки [24]. Наприклад, національна диспетчерська енергетична служба — це стратегічний об'єкт на рівні країни, а насосна станція в конкретному місті — важлива лише для певного регіону. Такий розподіл дає змогу раціональніше розподіляти ресурси захисту.

Ще один підхід — розгляд об'єктів за типом власності. За даними Сафонова, частка об'єктів критичної інфраструктури в приватній власності в Україні зростає, особливо у сферах логістики, зв'язку, охорони здоров'я та IT-секторі [10]. Це створює додаткову складність у побудові системи захисту, адже державні структури не мають прямих важелів впливу на приватні об'єкти. У цьому зв'язку часто доводиться покладатися на механізми співпраці, меморандуми, обмін даними, що є менш стабільними у кризових умовах.

У сучасній літературі все більше уваги приділяється і класифікації об’єктів за ступенем цифровізації. Horváth, зокрема, виділяє цифрові інфраструктури в окрему категорію — з огляду на їхню вразливість до кібератак і залежність від зовнішніх факторів, таких як супутникові мережі, дата-центри або хмарні сервіси [27]. Він застерігає: навіть якщо цифрова система формально не входить до переліку критичних, її виведення з ладу може мати ефект, порівнюваний із фізичною атакою на енергетичний об’єкт.

У результаті можна говорити про кількарівневу класифікацію, яка включає:

- функціональний розподіл (галузі);
- рівень значущості (національні, регіональні, локальні);
- тип власності (державні, приватні, змішані);
- ступінь цифровізації (фізичні, цифрові, гібридні об’єкти);
- географічне розміщення (урбанізовані, віддалені, прикордонні).

Ці параметри, на думку Коваленка, є базовими для формування системи оцінки ризиків. У своїй роботі він обґрунтовує, що моделі захисту не можуть бути уніфікованими: кожен об’єкт має свої особливості, тому для кожного потрібно підбирати індивідуальний підхід до аналізу вразливості, сценарного прогнозування й прийняття рішень [15].

Водночас не варто забувати, що критичність — це не фіксована властивість, а динамічне поняття. Те, що сьогодні здається другорядним, у новій ситуації може стати ключовим. Як приклад — логістичні хаби чи ІТ-інфраструктура, яка до 2020 року рідко потрапляла до переліку стратегічно важливих. Після початку пандемії COVID-19 та широкомасштабного вторгнення Росії ситуація змінилась кардинально.

Тому одним із висновків цього підрозділу є усвідомлення того, що класифікація критичної інфраструктури повинна бути живим інструментом, який оновлюється разом зі зміною зовнішніх умов. Це підтверджується як практикою

урядових інституцій, так і аналітикою міжнародних центрів, зокрема в роботах Bier [25] і Santucci [26], які підкреслюють, що система захисту має бути не жорсткою, а адаптивною. І це — не стільки технічне, скільки концептуальне питання.

1.2. Сутність та критерії оцінки безпеки таких об'єктів

Питання безпеки об'єктів критичної інфраструктури вже давно вийшло за межі суто технічного або адміністративного виміру. Воно стало системним викликом, який охоплює як інженерні, так і політичні, інформаційні, економічні й навіть етичні складові. Проблема полягає не лише в захисті фізичних об'єктів — трансформаторів, насосних станцій, дата-центрів, — а й у підтриманні здатності таких систем протистояти впливам, які не завжди можна спрогнозувати заздалегідь. Інакше кажучи, мова йде про побудову логіки оцінки, яка дозволить вчасно виявити вразливості й зорієнтувати ресурси на найбільш небезпечні зони.

Щоб зрозуміти, як узагалі можливо говорити про рівень безпеки об'єкта, слід почати з простого питання: що саме мається на увазі під «безпекою» у контексті критичної інфраструктури? Це не зовсім те саме, що охорона чи навіть кіберзахист. У загальному значенні безпека — це здатність об'єкта функціонувати у штатному режимі, зберігаючи цілісність, доступність і контроль над ключовими процесами, навіть за умов впливу зовнішніх або внутрішніх загроз. Як зазначає Aven, йдеться не просто про відсутність інцидентів, а про спроможність системи залишатись стабільною в умовах невизначеності [8].

У практиці ризик-менеджменту, зокрема в підходах, які використовуються в ISO/IEC 27001, безпека подається як багатовимірна характеристика, яка включає низку взаємопов'язаних компонентів — стійкість, відновлюваність, реактивність, вразливість, і навіть комунікаційну прозорість [3]. Це означає, що оцінити її

можна лише тоді, коли зрозумілі всі основні властивості системи, її внутрішні зв’язки й взаємодія із зовнішнім середовищем.

Один із провідних українських дослідників у цій сфері, Тарасов, наголошує: оцінка безпеки — це не лише технічна інвентаризація слабких місць. Це передусім аналітичний процес, який повинен враховувати як фізичну, так і організаційну структуру об’єкта, його залежність від інших систем, людський фактор, а також наявність процедур моніторингу й реагування [4]. На його думку, помилка багатьох менеджерів безпеки полягає в тому, що вони зводять оцінку до перевірки на наявність загроз, тоді як важливо оцінювати здатність до дії у відповідь.

У контексті критичної інфраструктури безпека набуває стратегічного значення. Це підтверджується в роботі Гвоздя, де він описує об’єкти інфраструктури не як статичні конструкції, а як динамічні системи, які постійно взаємодіють з економікою, суспільством і середовищем ризику [5]. Саме тому підходи до оцінки безпеки не можуть бути універсальними. Вони мусять враховувати тип об’єкта, його роль у системі, тип загроз, характер потенційних наслідків, доступні ресурси для захисту, а також наявність регламентів та протоколів у разі надзвичайних подій.

Щоб перейти від загального розуміння до практичного інструментарію, необхідно окреслити, за допомогою яких критеріїв зазвичай оцінюється безпека об’єкта. Найбільш поширеним у науковій та інженерній практиці є підхід, побудований на оцінці ризику. Як зазначає Shafer, ризик у цьому контексті є функцією трьох змінних: ймовірності загрози, ступеня вразливості об’єкта до цієї загрози та масштабу можливих наслідків [17]. Саме це трикутне співвідношення і є базою для побудови більшості сучасних моделей.

Важливо зазначити, що жодна з цих змінних не є постійною. Ймовірність загрози може змінюватись залежно від геополітичної ситуації або навіть часу доби. Вразливість залежить від технічного стану, підготовленості персоналу,

структури захисту. А наслідки — від масштабу, типу діяльності, територіального охоплення об’єкта. Цю логіку добре описує Коваленко у своїй аналітиці щодо кіберзагроз для критичної інфраструктури, підкреслюючи, що загроза — це не обов’язково атака, це ще й сукупність умов, які роблять об’єкт привабливим або слабким у певний момент [15].

На практиці для оцінки безпеки часто використовують набір так званих **індикаторів вразливості**. До них належать: наявність системи резервного живлення, ступінь автоматизації моніторингу, наявність фізичної охорони, дистанційне керування, доступність до об’єкта третіх осіб, стійкість до погодних умов, рівень цифрової безпеки, наявність інструкцій і тренувань персоналу тощо. Як підкреслює Бондаренко, ефективна система оцінки повинна не просто фіксувати ці індикатори, а аналізувати їх у динаміці, відстежувати зміни, виявляти тренди [13].

Одним із найбільш дискусійних питань є облік **людського фактора** в системах оцінки. Тут позиції дослідників розділяються. Наприклад, Шостак вважає, що вплив персоналу, його готовність до дій у критичних ситуаціях, ступінь стресостійкості, рівень навчання — все це має включатися до інтегрального показника безпеки [12]. У той же час Сафонов пропонує залишати ці параметри на етапі якісного аналізу, не включаючи їх у числові моделі, бо вони надто суб’єктивні [10]. Це питання залишається відкритим, хоча дедалі більше практиків схиляється до думки, що людський фактор має бути врахований бодай через окремий коефіцієнт адаптивності системи.

Ще один важливий критерій — **стійкість до каскадних ефектів**. Zio у своїх працях наводить приклади, коли невелика локальна аварія — наприклад, в одному з вузлів енергомережі — спричиняла масштабні відключення по всьому регіону, порушення транспорту, логістики та комунікацій [6]. За його висновками, системна вразливість часто не виявляється під час звичайних перевірок. Її можна

побачити лише тоді, коли моделюється міжгалузевий зв’язок і прогнозуються ланцюгові реакції.

В оцінці безпеки також важливо враховувати **наявність планів реагування**. Сам по собі об’єкт може бути вразливим, але якщо існує ефективна система реагування — резервні канали, сценарії дій, укладені договори з постачальниками, чітка комунікація з ДСНС, — ризики можуть зменшуватись. Як зазначає Wang, система з високою внутрішньою організацією здатна нейтралізувати навіть сильні зовнішні впливи [22].

Не менш критичним є і питання **часової чутливості**. Інфраструктура, яка залежить від швидких рішень — наприклад, логістичні центри, диспетчерські служби, ІТ-хаби — має коротший часовий горизонт для реагування, ніж, скажімо, очисні споруди або підстанції. Цю особливість ураховує Horváth, вводячи поняття «часового вікна безпечної реакції» — періоду, впродовж якого система здатна самостійно стабілізуватись без зовнішнього втручання [27].

Загалом, у сучасній науковій літературі виділяють кілька основних **критеріїв оцінки безпеки об’єктів критичної інфраструктури**:

1. Рівень вразливості до відомих типів загроз.
2. Імовірність виникнення критичного інциденту.
3. Потенційні масштаби наслідків.
4. Здатність до самовідновлення.
5. Наявність ефективних механізмів реагування.
6. Ступінь міжгалузевої залежності.
7. Стійкість до каскадних ефектів.
8. Рівень цифрової безпеки.
9. Готовність персоналу до надзвичайних ситуацій.
10. Адекватність регламентів і процедур.

Ці критерії не є вичерпними, але саме на їхній основі будуються сучасні математичні моделі, серед яких — баєсівські мережі, методи нечіткої логіки, сценарні моделі, імовірнісні сітки та мультикритеріальні шкали. Подальший розгляд цих підходів буде здійснено в наступному розділі, однак уже зараз можна зробити висновок: ефективна оцінка безпеки — це не формальна перевірка, а складний процес синтезу технічної, організаційної, поведінкової та аналітичної інформації.

1.3. Інформаційна невизначеність як фактор ризику

Щоразу, коли говоримо про ризик для об’єктів критичної інфраструктури, перше, що спадає на думку, — це фізичні загрози: вибухи, атаки, стихійні лиха. Однак реальність набагато складніша. У більшості випадків проблема не в самій загрозі, а в тому, що про неї відомо недостатньо. Дані можуть бути фрагментарними, застарілими, суперечливими або повністю відсутні. Саме це породжує стан, який у науковій літературі описується як інформаційна невизначеність.

У найзагальнішому розумінні під інформаційною невизначеністю розуміють ситуацію, за якої особа або система не має повного уявлення про всі змінні, які впливають на результат. Це поняття охоплює не тільки відсутність даних, а й сумніви в їхній достовірності, неточність прогнозів, відсутність моделей, які могли б пояснити спостережуване явище. Як зазначає Aven, у контексті управління ризиками це одна з найнебезпечніших форм нестабільності, бо вона унеможливлює прийняття зважених рішень [8].

На відміну від класичної ймовірнісної невизначеності, яка оперує числами і вираховує вірогідність певної події, інформаційна невизначеність має радше якісний характер. Shafer у своїй теорії доказів пропонує її трактування як простору між знанням і незнанням — коли ми можемо оцінити, що подія можлива, але не

маємо достатньої основи, щоб надати їй точну ймовірність [17]. Це проміжна зона, у якій опиняється більшість об’єктів критичної інфраструктури, особливо в умовах війни, кібератак або техногенних загроз.

Для прикладу, розглянемо ситуацію, коли невідомо, чи встановлено в об’єкті стеження, чи його цифрову мережу вже скомпрометовано. Якщо це так — ризик дуже високий, але якщо ні — то його практично немає. І поки ця інформація відсутня або суперечлива, рішення — вкладати ресурси в захист, відключати систему, ізолювати об’єкт — доводиться ухвалювати в сліпу. У такому контексті кожне рішення вже саме по собі стає джерелом ризику.

В українських умовах, особливо з 2022 року, інформаційна невизначеність стала хронічним фактором для критичної інфраструктури. Як зазначає Гвоздь, у багатьох випадках на момент прийняття рішення про евакуацію, зміну маршрутів, підключення резервних потужностей інформація про характер загроз, джерело атаки або її масштаб є неповною або з'являється із запізненням [5]. В умовах кібервійни це особливо небезпечно, оскільки атаки часто маскуються, їхній вплив накопичується поступово, а перші ознаки можна сплутати з технічними несправностями.

На цьому тлі виникає потреба осмислити, яким чином інформаційна невизначеність перетворюється на фактор ризику і як вона впливає на оцінку стану безпеки. Тарасов наголошує: традиційні системи захисту побудовані на припущенні, що дані про об’єкт — технічні, логістичні, експлуатаційні — є повними, структурованими та надійними [4]. Проте в умовах сучасних загроз це припущення не працює. Система має функціонувати навіть у разі, коли дані відсутні або не можна довіряти жодному з каналів.

Якщо говорити простіше — раніше захист планували на підставі того, що «ми знаємо, що нам загрожує». Тепер же доводиться будувати захист із розрахунком на те, що «ми не знаємо, де і як саме буде удар, але він точно буде».

Це принципово інша логіка. У такій ситуації не можна покладатися тільки на камери, датчики чи статистику. Потрібно формувати стійкість, яка базується на принципі адаптивності.

У науковій літературі з'являється низка підходів, які враховують інформаційну невизначеність у моделюванні безпеки. Один із таких — нечітка логіка. Мозговий демонструє, як за допомогою нечітких множин можна створювати моделі, які не вимагають точних значень на вході, а оперують діапазонами, градаціями або лінгвістичними змінними [7]. Наприклад, замість того, щоб вводити точне число «кількість загроз на годину», можна використовувати шкалу «низький – середній – високий ризик». Це дозволяє системі реагувати навіть тоді, коли дані надходять фрагментарно або з затримкою.

Ще одним інструментом є баєсівські мережі. Сафонов і Кириленко пояснюють, що їхньою перевагою є здатність оновлювати оцінки ризику в реальному часі на основі нових даних [10]. Це надзвичайно важливо в умовах невизначеності: модель не є статичною, вона змінюється з кожною новою інформацією, навіть якщо та суперечить попередній. У такому випадку можна коригувати не тільки ймовірність загрози, а й очікуваний вплив та пріоритети реагування.

Імовірнісні моделі, як-от ті, що описує Дмитрієв, дають змогу враховувати варіативність сценаріїв і будувати систему з урахуванням не лише середнього значення ризику, а й потенційно найгіршого випадку [16]. У цьому підході важливо не те, щоб знати все, а щоб заздалегідь передбачити, до чого може призвести недостатність інформації. Наприклад, якщо через відсутність телеметрії не фіксується перегрів вузла, модель має враховувати, що ризик вибуху автоматично зростає.

Shortridge у своїй роботі наводить приклади, як працює управління ризиками в ситуації, коли дані про стан системи надходять із затримкою, не

повністю або через ненадійні джерела [14]. Він робить висновок, що ключем є не намагання заповнити всі інформаційні лакуни, а створення таких умов, у яких навіть за мінімальної інформованості можна обрати адекватну дію.

Цей підхід добре корелює з дослідженням Horváth, який підкреслює роль мультикритеріального аналізу в умовах інформаційної неоднозначності [27]. Якщо обрати правильні ваги для різних параметрів, можна компенсувати нестачу даних у певних секторах за рахунок інших, де інформація точніша. Наприклад, якщо немає точних даних про внутрішній трафік системи, але відома кількість підключених вузлів і типи пристроїв, можна оцінити рівень загрози з похибкою, достатньою для прийняття рішень.

Сантуччі, аналізуючи кібератаки на об’єкти критичної інфраструктури у США, робить акцент на тому, що невизначеність у багатьох випадках є не випадковою, а навмисно створеною супротивником [26]. Прикриття своїх дій, імітація несправностей, запуск кількох паралельних фальшивих сигналів — усе це методи дезорієнтації системи. І якщо система побудована на припущенні, що дані завжди правдиві, вона швидко стає жертвою.

Важливо також розуміти, що невизначеність може існувати не лише в технічній сфері, а й на рівні управлінських рішень. Як зауважує Bier, нерідко ключовою проблемою стає не відсутність технічних рішень, а невпевненість у тому, яку саме дію обрати в ситуації, коли кожна з них має свої ризики [25]. У таких умовах важливо, щоби моделі безпеки мали гнучкість, дозволяючи обирати не найкращий, а найбільш прийнятний варіант — з урахуванням як внутрішніх обмежень, так і зовнішніх факторів.

РОЗДІЛ 2. АНАЛІЗ ІСНУЮЧИХ МАТЕМАТИЧНИХ ПІДХОДІВ ДО ОЦІНКИ БЕЗПЕКИ

2.1. Методи нечіткої логіки в умовах неповноти даних

Ситуації, у яких інформація є фрагментарною або неточною, в сучасних умовах швидше правило, ніж виняток. Це особливо помітно у сфері безпеки критичної інфраструктури, де багато рішень доводиться ухвалювати в режимі обмеженої видимості: частина даних ще не надійшла, інша — неперевірена, а частину взагалі неможливо отримати через технічні чи безпекові обмеження. Класичні математичні методи в таких умовах починають буксувати, бо вони звикли до чітких значень, визначених залежностей, точних імовірностей. Натомість система, яка має функціонувати попри невідоме, потребує іншого підходу — більш гнучкого, адаптивного, здатного працювати з приблизними оцінками. Саме тут на перший план виходять методи нечіткої логіки.

Ідея нечіткої логіки полягає в тому, що не обов’язково знати точну кількісну характеристику ризику, щоб його оцінити. Нечітка система може працювати з такими поняттями, як «високий ризик», «помірна вразливість» чи «низький рівень підготовки». Такі формулювання, хоч і не мають точного числового еквіваленту, є набагато ближчими до реальності, в якій живе більшість об’єктів критичної інфраструктури.

Як показує у своїй роботі Мозговий, методи нечіткої логіки дозволяють моделювати ситуації, в яких неможливо чітко визначити вхідні параметри — наприклад, коли інформація надходить із затримкою або її достовірність під питанням [7]. У своїх прикладах він аналізує типову ситуацію для української інфраструктури: об’єкт отримує сигнали про можливу загрозу, але ці сигнали нечіткі — одні датчики фіксують перевантаження, інші — ні; дані телеметрії неповні; система моніторингу зазнала кіберзагрози. В таких умовах класична система аналізу може просто видати помилку або відмовитись від дії, бо дані не

відповідають закладеним нормам. А ось система з нечіткою логікою здатна сформувати попередження навіть на основі неповної картини.

Суть такого підходу полягає в тому, що всі змінні перетворюються на нечіткі множини. Наприклад, замість того щоб працювати з числом «температура = 81 °C», система розглядає, наскільки це значення відповідає поняттям «низька температура», «помірна», «висока» або «критична». Кожне з цих понять — це не точка на шкалі, а певна область, яка може перекриватися з іншими. Такий підхід дозволяє враховувати не лише числові значення, а й контекст — наприклад, 81 °C для одного елементу є нормою, а для іншого — критичним значенням.

Особливу цінність метод нечіткої логіки має тоді, коли мова йде про **мовні змінні** — тобто ті, які надходять не в цифровому вигляді, а як оцінка експерта або автоматизованої системи типу «ймовірна загроза на південному фланзі». У своїх дослідженнях Євтушенко доводить, що саме такі оцінки — попри свою неточність — часто є основним джерелом інформації в кризових ситуаціях [18]. Їхнє ігнорування лише тому, що вони не вписуються в цифрову модель, означає втрату важливої аналітичної складової.

Ще однією перевагою нечітких моделей є можливість **агрегації неповних даних**. У класичних системах для прийняття рішення потрібно мати значення для всіх змінних. У нечіткій системі можна обійтись без цього — якщо частина даних відсутня, вона просто не враховується, а загальна картина формується на основі того, що є. Такий підхід демонструє свою ефективність у роботах Zio, де він моделює складні інфраструктурні системи з високим ступенем взаємозалежності, у яких не завжди можна зібрати повну інформацію про всі елементи [6].

Цікаво, що застосування нечіткої логіки не обмежується лише технічними параметрами. Наприклад, у роботі Шостака йдеться про використання нечітких моделей для аналізу **готовності персоналу** до реагування на кризові ситуації [12]. Він пропонує вводити такі поняття, як «низький рівень поінформованості» або

«висока втома персоналу» як змінні в оцінці безпеки. Це дозволяє враховувати людський фактор, який у класичних системах часто залишається поза кадром.

Також важливо відзначити, що нечітка логіка добре комбінується з іншими підходами. Наприклад, у моделі, запропонованій Швидким, нечітка логіка використовується разом із традиційним імовірнісним аналізом [23]. Це дозволяє розраховувати як точні значення ризику, так і їхню інтерпретацію в лінгвістичних термінах. Таким чином, можна адаптувати модель під різних користувачів — технічний персонал, керівників, аналітиків.

У багатьох випадках нечітка логіка використовується для побудови **систем підтримки прийняття рішень**. У роботі Камінського аналізується система, яка автоматично оцінює рівень загроз для об'єкта залежно від комбінації кількох нечітких факторів: фізична безпека, інформаційна вразливість, час доби, ступінь завантаженості, погодні умови [24]. Результатом є рекомендація — підвищити готовність, ініціювати перевірку, увімкнути резервну систему тощо. Автор підкреслює: така система не замінює людину, але дає змогу приймати рішення навіть тоді, коли дані суперечливі або неповні.

Показовим є й той факт, що навіть **міжнародні стандарти** визнають доцільність використання нечітких підходів. У документах ISO, зокрема серії 27001, прямо зазначено, що методи оцінки ризиків можуть включати як кількісні, так і якісні (у тому числі — нечіткі) інструменти, особливо в умовах обмеженої інформації [3].

І хоча нечітка логіка не є універсальним рішенням, її здатність функціонувати в реальному, а не ідеалізованому інформаційному середовищі робить її надзвичайно привабливою для критичної інфраструктури. Особливо — в українських реаліях, де об'єкти часто працюють під тиском, з обмеженим доступом до інформації та високою ймовірністю зовнішніх втручань.

2.2. Байєсівські моделі як засіб оцінки ризиків

У тих випадках, коли мова йде про критичну інфраструктуру, що функціонує в умовах часткової або нестабільної інформації, актуальним стає питання: яким чином можна оновлювати оцінку ризиків у міру надходження нових даних? Тобто — як побудувати систему, яка здатна "вчитися", коригуючи свою реакцію залежно від контексту? Відповідь на це питання багато дослідників пов’язують із застосуванням байєсівських моделей. Їхня сутність полягає в тому, що ймовірність ризику розглядається не як щось сталий, а як величина, що змінюється під впливом нової інформації.

Байєсівський підхід отримав ім’я від англійського математика Томаса Байєса. Але його сучасне використання в системах безпеки — це вже не просто статистична формула. Це повноцінна логіка моделювання, в основі якої лежить ідея про те, що всі оцінки мають суб’єктивну природу, і можуть бути переглянуті, коли з’являються нові дані. Як зазначає Paté-Cornell, саме ця здатність до адаптації робить баєсівські моделі надзвичайно цінними в ситуаціях з високим рівнем невизначеності — наприклад, в управлінні безпекою складних інфраструктур [11].

На відміну від класичних статистичних моделей, які працюють із зафіксованими значеннями, баєсівські мережі дозволяють інтегрувати як кількісні, так і якісні дані. Це означає, що система може враховувати не тільки числові вимірювання, а й експертні оцінки, логічні зв’язки між подіями, структурні особливості об’єкта. Такий підхід добре ілюструє робота Сафонова і Кириленка, які змоделювали функціонування інфраструктурного об’єкта з урахуванням ймовірності вторгнення, помилок персоналу, стану обладнання та ефективності системи реагування [10].

Суть побудови баєсівської мережі полягає в створенні графа, де вузли відповідають за окремі події або фактори, а стрілки між ними — за причинно-наслідкові зв’язки. Кожен вузол має свою ймовірність, яка може бути оновлена,

коли змінюється стан інших вузлів. Наприклад, якщо зафіксовано проникнення в периметр, зростає ймовірність кіберзагрози. А якщо додатково виявлено збої в електропостачанні, це підвищує ймовірність фізичного пошкодження системи керування.

Цей підхід дозволяє не просто фіксувати наявність загрози, а й оцінити, наскільки зміна одного параметра впливає на інші. У реальних умовах це критично важливо, бо більшість рішень ухвалюється не на повному наборі даних, а на комбінації того, що вдалося зафіксувати. Як показує Shortridge у своїх кейсах, баєсівські мережі добре працюють у середовищах, де є багато взаємопов'язаних змінних, і де не всі з них доступні для спостереження [14].

Особливої уваги заслуговує здатність баєсівських моделей **інтегрувати експертні оцінки**. Наприклад, якщо система не має точних даних про вразливість певного вузла, але експерти на основі досвіду дають оцінку "високий ризик", ця інформація може бути внесена в модель. У класичній статистиці такий суб'єктивний підхід вважається некоректним, однак у баєсівській логіці це цілком легітимно. Це відкриває простір для врахування знань персоналу, попередніх інцидентів, інтуїтивних сигналів, які складно формалізувати.

Іншим важливим елементом є **можливість побудови сценаріїв на основі умовної ймовірності**. Якщо, скажімо, фіксується затримка в роботі системи моніторингу — модель може одразу переоцінити ймовірність атаки або технічної аварії. А якщо одночасно відбувається зростання мережевого трафіку з невідомих джерел — модель знову оновлює оцінку ризику. Така динамічність дозволяє тримати систему в режимі постійної аналітичної готовності.

Застосування баєсівських моделей у сфері критичної інфраструктури розглядає також Козлов. У своїх роботах він акцентує, що для складних систем, де вплив одного фактору розповсюджується на десятки інших, саме умовна ймовірність дозволяє уникнути хибних висновків [21]. У звичайних умовах такі

системи могли б видавати або "зелене світло", або повну тривогу. Баєсівська модель дозволяє відтінити ситуацію, виявити часткові загрози, посилити моніторинг саме там, де ризик найбільш імовірний.

Не менш цікаво розглядається взаємозв'язок баєсівських моделей із поняттям інформаційної невизначеності. Як зазначає Aven, саме баєсівський підхід є найбільш природним способом формалізувати непевність — бо він дозволяє не просто враховувати відсутність знань, а й кількісно описувати, як це впливає на загальну оцінку [8]. Наприклад, якщо ми не знаємо, чи оновлене програмне забезпечення, ми не відкидаємо цю змінну — ми вводимо в модель відповідну умовну ймовірність на основі того, що в аналогічних системах ризик оновлення був, скажімо, 30%.

У роботі Шостака підкреслюється, що баєсівські мережі є не лише інструментом моделювання, а й засобом **візуалізації ризиків**. Завдяки структурі графа, аналітик або керівник може в реальному часі побачити, як зміна одного показника впливає на всі інші, де утворюється найбільше "навантаження", які шляхи впливу є критичними [12]. Це важливо в умовах стресу або атаки, коли часу на аналітику мало, а рішення потрібне негайно.

Інтеграція баєсівських підходів у практичні системи безпеки в Україні ще не є масовим явищем. Проте, як зазначає Бондаренко, окремі приклади впровадження вже є, особливо в енергетичному секторі, де активно експериментують із прогнозуванням на основі умовних ймовірностей [13]. На його думку, ключовим бар'єром є не технічна складність, а відсутність культури роботи з моделями, які видають "імовірні" результати замість звичних категоричних оцінок.

Дійсно, сприйняття результатів, сформованих баєсівською мережею, вимагає певного зміщення у мисленні. Система не скаже: "загроза є" або "загрози немає". Вона скаже: "з імовірністю 64% у поєднанні з такими-то факторами існує

ризик впливу такого-то типу". Це складніше для сприйняття, але набагато ближче до реального світу, де рішення майже ніколи не є однозначними.

Водночас важливо розуміти обмеження баєсівських підходів. Як зазначає Paté-Cornell, результат моделі сильно залежить від того, які саме зв’язки між змінними були визначені на старті — а це, своєю чергою, залежить від експертного бачення, суб’єктивного досвіду, наявності історичних даних [11]. Якщо мережу побудовано неправильно — її результати не мають цінності. Отже, якість моделі — це не тільки математика, а ще й аналітика, управлінська логіка, досвід і контекст.

Тому в багатьох випадках використання баєсівських моделей супроводжується **процесом валідації**. Як зазначає Євтушенко, верифікація структури зв’язків і тестування її на реальних кейсах є необхідною умовою перед впровадженням у критичні системи [18]. Інакше система ризикує або переоцінювати загрози, або не помічати реальні.

2.3. Імовірнісні методи в аналізі надійності

Коли йдеться про оцінку безпеки критичних об’єктів, поняття надійності постає як центральне. Не менш важливо розуміти не просто, як функціонує система, а з якою вірогідністю вона зможе виконати свою функцію у потрібний момент. Імовірнісні методи, які зазвичай асоціюються зі статистикою, давно вийшли за межі теорії й стали основою для прийняття рішень у сферах, де помилка може мати критичні наслідки.

У базовому розумінні, надійність — це характеристика системи, що описує її здатність безвідмовно функціонувати протягом заданого проміжку часу. Але в реальності — особливо у випадку складних об’єктів на кшталт електростанцій, мережевих центрів, транспортних вузлів — усе рідко зводиться до чорно-білих оцінок. Є надто багато чинників, які не можна передбачити точно. І тут саме

ймовірнісні підходи дають змогу говорити про надійність як про величину, яку можна змоделювати, оцінити й використати для управлінських рішень.

Одним із класичних прикладів використання ймовірнісного підходу є **функція надійності**, яка показує, з якою ймовірністю система залишатиметься працездатною до певного моменту часу. У простих випадках вона має експоненційний вигляд, але як тільки мова заходить про багатокомпонентні системи з залежними вузлами — ситуація ускладнюється. Як пояснює Козлов, справжній виклик у моделюванні полягає не в самому обчисленні, а в правильному урахуванні взаємозв'язків між елементами [21].

Щоб описати ці зв'язки, активно використовуються так звані **логічно-імовірнісні моделі**, зокрема дерева відмов. Цей підхід дозволяє візуалізувати, як поломка одного компонента (або комбінація кількох) може призвести до відмови всієї системи. У роботі Дмитрієва показано, як використання дерева відмов дозволяє змоделювати поведінку об'єкта у кризовій ситуації, з урахуванням як технічних, так і організаційних факторів [16]. Наприклад, якщо резервне живлення не спрацьовує в 5% випадків, а основне – у 10%, то загальна ймовірність повної відмови не буде простою сумою, а залежатиме від схеми вмикання, затримок, реакції персоналу.

На практиці часто використовується поняття **середнього часу безвідмовної роботи** (MTBF – Mean Time Between Failures). Це — класичний показник, який дозволяє оцінити, наскільки стабільною є система в нормальних умовах. Але сам по собі він мало що говорить про ситуації, коли об'єкт потрапляє під дію аномальних навантажень. Саме тому, як зауважує Aven, MTBF має розглядатися в динаміці — із врахуванням сценаріїв, які виводять систему за межі звичайного режиму [8]. Його пропозиція — доповнювати класичні розрахунки ймовірністю того, що система потрапить у "стресовий режим", тобто фазу зростання навантаження, загроз або технічного зносу.

Імовірнісні методи мають перевагу і в тому, що дозволяють **моделювати поведінку системи у випадку часткового пошкодження**. Не обов'язково, щоб об'єкт повністю вийшов з ладу — достатньо, щоб відмовив один модуль або ланка, яка впливає на критичну функцію. Наприклад, відмова каналу зв'язку не означає повної зупинки процесу, але може призвести до втрати керованості. У дослідженні Zio цей підхід застосовується до транспортної інфраструктури: відмова одного сегменту мережі створює затримки, які в підсумку можуть стати критичними [6].

Особливу цінність має так званий **метод Монте-Карло** — один із найпоширеніших інструментів імовірнісного моделювання. Його суть полягає в багаторазовому "прогоні" моделі з випадково згенерованими параметрами, щоб подивитись, як змінюється результат за різних умов. У роботі Швидкого цей метод використовується для оцінки ефективності системи захисту в умовах, коли дані про загрози є лише частковими [23]. Застосування такого підходу дозволяє зрозуміти, наскільки стабільною є система при коливаннях зовнішніх факторів.

В українському контексті, де критична інфраструктура часто функціонує на межі технічних можливостей, імовірнісне моделювання може виступати інструментом прийняття не лише технічних, а й стратегічних рішень. Як показує аналіз, проведений Камінським, саме обчислення сценарної ймовірності дає змогу зрозуміти, чи доцільно вкладати ресурси в модернізацію певного вузла, чи краще зосередитись на резервуванні або зміцненні пов'язаних компонентів [24].

У західній практиці ці методи активно використовуються у плануванні **відмовостійких систем** (fail-safe architecture). Наприклад, система енергопостачання для лікарень проєктується з урахуванням того, що основне джерело енергії вийде з ладу — і лише потім перевіряється, чи витримає резерв. Як зазначає Lewis, така логіка мислення — "спочатку змоделюй найгірший

варіант, а потім перевір, чи система його витримає" — давно стала нормою в країнах із розвиненою інфраструктурою [19].

З іншого боку, використання імовірнісних підходів передбачає високий **рівень відповідальності за вихідні дані**. Як зазначає Shafer, помилка на рівні ймовірності одного компонента може призвести до повністю хибного висновку щодо всієї системи [17]. Саме тому моделі потребують постійного оновлення на основі реальної статистики, результатів технічного аудиту, інформації з датчиків та журналів подій. Недостатньо створити модель один раз — вона повинна "жити", адаптуватися, реагувати на зміни.

Є також думка, що імовірнісні методи здатні **враховувати людський фактор**, хоч і непрямо. Наприклад, якщо історично зафіксовано, що певний тип персоналу з меншою підготовкою має вищий рівень помилок — це може бути включено в модель через відповідний коефіцієнт. У роботі Євтушенка така ідея реалізована шляхом введення змінної "людський фактор", що модифікує загальну оцінку надійності залежно від змін у персоналі, навантаженні, кількості змін у добу тощо [18].

У сучасних умовах, коли об’єкти критичної інфраструктури дедалі частіше потрапляють під **одночасну дію кількох ризиків** (технічних, кібернетичних, організаційних), імовірнісні методи стають необхідністю. Вони дають змогу поєднувати різні типи загроз у спільній моделі — не знижуючи складність, а навпаки, дозволяючи її осмислити. Як зазначає Wang, саме в багатофакторних середовищах переваги таких підходів стають найбільш очевидними [22].

Підсумовуючи, можна сказати: імовірнісне моделювання — це не лише про формули. Це про здатність бачити систему як живий організм, що реагує на зміни, має слабкі місця й не завжди діє за правилами. І найголовніше — це спосіб підготуватись до невідомого, не знаючи точно, яким воно буде.

2.4. Порівняльний аналіз застосовності моделей

Попри те, що кожен із математичних підходів — нечітка логіка, баєсівські мережі, імовірнісні моделі — має свою логіку, специфіку та сферу застосування, у реальній роботі доводиться відповідати на практичне питання: який саме метод використовувати для оцінки безпеки конкретного об’єкта критичної інфраструктури? І найголовніше — за яких умов той чи інший метод дасть найбільш адекватний результат. Відповісти на це питання допомагає порівняльний аналіз — не абстрактний, а заснований на тому, що вже зроблено й обґрунтовано у наукових дослідженнях.

Порівняння моделей має сенс лише тоді, коли враховано контекст: тип об’єкта, рівень доступної інформації, обмеження часу, наявність експертів і обчислювальних ресурсів. Саме тому, як підкреслює Aven, не існує "універсальної" моделі безпеки — є лише моделі, які краще або гірше працюють у конкретній ситуації [8].

Щоб зробити аналіз наочно зрозумілим, нижче представлено порівняльну таблицю, в якій узагальнено ключові характеристики розглянутих підходів.

Таблиця 2.1 – Порівняння математичних моделей оцінки безпеки критичних об’єктів

Критерій порівняння	**Нечітка логіка**	**Баєсівські мережі**	**Імовірнісні методи**
Працездатність за неповноти даних	Висока	Висока	Середня
Залежність від експертних оцінок	Висока	Помірна	Низька
Можливість оновлення в реальному часі	Обмежена	Висока	Низька

Потреба в точних статистичних даних	Низька	Помірна	Висока
Адаптивність до нових сценаріїв	Помірна	Висока	Низька
Можливість візуалізації	Середня	Висока	Середня
Обчислювальна складність	Низька	Висока	Висока
Інтерпретованість результатів	Висока	Середня	Висока
Динамічність реагування	Низька	Висока	Середня

Джерело: розроблено автором на основі [7], [10], [16], [11], [8]

Як видно з таблиці, кожен підхід має як сильні, так і слабкі сторони. Наприклад, нечітка логіка вражає своєю здатністю працювати без жорстких числових обмежень. У роботі Мозгового наголошується, що саме це робить її ідеальною для використання у ситуаціях, коли дані надходять із затримкою або мають якісний характер — наприклад, у випадках польового моніторингу [7]. Проте така система часто не дозволяє оперативно враховувати нові загрози або сценарії.

Баєсівські мережі, натомість, забезпечують виняткову адаптивність. Сафонов і Кириленко у своїй моделі доводять, що вони дозволяють не лише оцінювати ризики, а й перераховувати їх миттєво після надходження нового фрагмента інформації [10]. Але водночас ця гнучкість вимагає детального налаштування структури, наявності історичних даних або хоча б добре обґрунтованих припущень. Як зазначає Paté-Cornell, баєсівські моделі легко "ломаються", якщо їхня початкова логіка побудована хибно [11].

Імовірнісні методи — це традиційна основа інженерного аналізу, яка дає змогу об’єктивно оцінити надійність, зважаючи на історичну статистику, частоту відмов, навантаження. Але, як справедливо підкреслює Дмитрієв, вони слабко

адаптуються до нових загроз, які не мають попередників у базі даних, і тому втрачають актуальність у кризових ситуаціях, що розгортаються швидко [16].

Особливої уваги заслуговує співвідношення між **тривалістю налаштування моделей** і їхньою практичною віддачею. У таблиці нижче наведено порівняння часу впровадження моделей (в умовному вимірі) з рівнем чутливості до змін у зовнішньому середовищі.

Таблиця 2.2 – Залежність ефективності моделей від умов використання

Модель	**Орієнтовна тривалість налаштування**	**Чутливість до нових загроз**	**Готовність до роботи після налаштування**
Нечітка логіка	Низька	Середня	Висока
Баєсівські мережі	Висока	Висока	Середня
Імовірнісні методи	Середня	Низька	Висока

Джерело: розроблено автором на основі [7], [10], [16]

Як видно, нечітка логіка — найшвидша у впровадженні, і при цьому одразу дає чітку інтерпретацію результатів. Баєсівські моделі потребують тривалого налаштування, але згодом забезпечують найкращу адаптацію. Імовірнісні методи залишаються стабільними, але менш чутливими до динаміки.

У практичному сенсі вибір моделі часто залежить від цілей оцінки. Як зазначає Lewis, якщо мета — розрахувати технічну ймовірність відмови у стандартних умовах, найкраще працюють класичні методи [19]. Якщо потрібно врахувати ситуаційний контекст, особливо в умовах невизначеності, — варто звертатися до нечіткої логіки. А якщо ситуація розвивається динамічно і потрібно

адаптуватися в режимі реального часу — баєсівська модель може стати найбільш ефективним інструментом.

Сама по собі наявність кількох моделей — не слабкість, а ознака зрілості системи. У сучасних практиках усе частіше застосовують **гібридні підходи**, коли нечітка логіка використовується для первинної фільтрації даних, баєсівські мережі — для адаптивного аналізу, а класичні методи — для перевірки надійності в статичних режимах. Саме такі рішення, як показує дослідження Wang, мають найбільший потенціал у складних умовах, де важливі як швидкість, так і точність [22].

РОЗДІЛ 3. РОЗРОБКА ТА ВАЛІДАЦІЯ МОДЕЛІ ОЦІНКИ БЕЗПЕКИ

3.1. Обґрунтування вибору моделі з урахуванням специфіки об’єкта

Побудова будь-якої моделі оцінки безпеки починається не з формул і не з коду. Вона починається з розуміння того, з яким об’єктом маємо справу, які його функції, які в нього вразливості, який тип загроз для нього є пріоритетним і що вважається порогом критичності. Бо модель, яка чудово працює для транспортної системи, може виявитися повністю непридатною для об’єкта енергетики або цифрового вузла. Саме тому на першому етапі доцільно не будувати алгоритми, а зрозуміти логіку, за якою функціонує конкретна система.

Об’єкт, обраний для аналізу в цій роботі, є інфраструктурним вузлом, до складу якого входить мережеве обладнання, енергоживлення, охоронна система та цифровий диспетчерський пункт. Він обслуговує транспортно-логістичну ділянку, через яку проходять вантажі критичного призначення. Саме тому для нього важлива не лише фізична безпека (проникнення, пошкодження), а й інформаційна стабільність (зовнішні атаки, збої в керуванні). Така структура, як зазначає Коваленко, належить до гібридного типу об’єктів, де ризики перетинаються між фізичним і цифровим середовищами [15].

Щоб не допустити абстрактного підходу, спочатку проведено **функціональну декомпозицію об’єкта** — поділ на підсистеми, кожна з яких має свої ризики, свої вразливості та власну структуру даних. Цей підхід добре себе зарекомендував у практиці ризик-менеджменту, бо дозволяє моделювати не об’єкт у цілому, а його «найслабші ланки». За методикою Швидкого, декомпозиція дає змогу побудувати карту ризиків, на основі якої вже вибирається модель [23].

Таблиця 3.1 – Ключові підсистеми об’єкта та відповідні ризики

Підсистема	Тип загрози	Ймовірні наслідки

Енергоживлення	Збій мережі, перепади напруги	Зупинка процесів, втрата даних
Диспетчерська система	Кібератака, відмова ПЗ	Втрата керування, помилкові команди
Контроль доступу	Проникнення, пошкодження обладнання	Пошкодження критичних елементів
Зв’язок із центром	Порушення каналу, перехоплення	Втрата координації, затримка сигналів
Внутрішня мережа	Віруси, внутрішні загрози	Пошкодження даних, перерозподіл ресурсів

Джерело: розроблено автором на основі [15], [23], [10]

Кожна з цих підсистем має свої особливості в сенсі доступності даних. Наприклад, стан енергоживлення легко контролюється датчиками, а от рівень ризику проникнення — радше експертна оцінка, заснована на індикаторах. У системі зв’язку можлива велика затримка в реєстрації загрози. Це означає, що для різних компонентів доцільно використовувати різні підходи до оцінки.

На цьому етапі стало очевидним: універсальна модель буде або занадто складною, або недостатньо гнучкою. Саме тому рішення ухвалено на користь **гібридної моделі**, яка поєднує:

- нечітку логіку (для компонентів, де дані якісні або експертні);
- баєсівські мережі (для елементів із динамічно змінною інформацією);
- імовірнісні методи (для модулів із детермінованою статистикою).

Як зазначає Wang, саме такі моделі є найбільш стійкими до інформаційних збоїв і дозволяють масштабувати модель без повного перепроєктування [22]. Крім того, гібридний підхід відповідає реальності, в якій критичні об’єкти функціонують у багатовимірному середовищі, де немає "чистих" ризиків.

Ключовим аргументом на користь включення **нечіткої логіки** є якість даних із системи контролю доступу. Тут рішення часто базуються на поведінкових патернах, де складно визначити точну межу між нормою і аномалією. Як показує Мозговий, нечітка логіка дозволяє враховувати нечислові оцінки, вводити поняття "ймовірна загроза", "незвична поведінка", "часткове відхилення", що неможливо в класичних моделях [7].

Баєсівська мережа є ідеальним варіантом для диспетчерської системи, де стан змінюється в реальному часі. Якщо один компонент дає збій, система має одразу переглядати оцінку ризику для інших. Як показує Сафонов, саме байєсівські підходи дозволяють реалізувати сценарне оновлення — кожен новий сигнал впливає на всі пов’язані вузли, що наближає модель до реальної логіки мислення оператора [10].

Для енергоживлення, де статистика доступна і надійна, логічним вибором є **імовірнісна модель**. У роботі Дмитрієва запропоновано використовувати функцію надійності, що враховує час роботи, середній час між відмовами, характер збоїв [16]. Це дозволяє формалізувати оцінку і включити її як один із параметрів у загальну модель.

Ще один фактор, який вплинув на вибір підходів, — **характер реагування об’єкта на відмову**. Деякі підсистеми (як-от зв’язок) мають вікно реагування в кілька секунд, інші (наприклад, вентиляція або освітлення) можуть працювати автономно кілька хвилин. Ця різниця вимагає різної глибини моделювання. Як зазначає Horváth, часова динаміка повинна бути одним із визначальних параметрів моделі, а не просто фоном [27].

Таблиця 3.2 – Співвіднесення компонентів об’єкта та обраних моделей

Компонент	**Доступні дані**	**Обрана модель**	**Причина вибору**

Енергоживлення	Історична статистика	Імовірнісна	Надійні числові показники, доступна телеметрія
Диспетчерська система	Поточні сигнали	Баєсівська мережа	Динамічна зміна стану, реакція на оновлення
Контроль доступу	Поведінкові патерни	Нечітка логіка	Якісні оцінки, лінгвістичні змінні
Система зв’язку	Затримки, перериви	Баєсівська + імовірнісна	Поєднання сценаріїв і статистики збоїв
Внутрішня мережа	Лог-файли, аномалії	Нечітка логіка	Експертні правила, нечіткі умови

Джерело: розроблено автором на основі [7], [10], [16], [27]

Таким чином, на основі проведеного аналізу сформовано **архітектуру комбінованої моделі**, де кожна підсистема оцінюється власним інструментом, але результати агрегуються в єдиному індикаторі ризику. У підрозділі 3.2 буде показано, як саме побудовано структуру цієї моделі, як відбувається обробка вхідних даних та взаємодія між модулями.

3.2. Формалізація параметрів та побудова структури моделі

Коли визначено, які моделі доцільно застосовувати до кожної з підсистем об’єкта критичної інфраструктури, наступним кроком є побудова єдиної структури, яка поєднає ці модулі в цілісну аналітичну систему. Для цього недостатньо просто «додати» результати з різних методів. Потрібна узгоджена логіка, яка дозволить співвідносити вихідні дані, синхронізувати часові інтервали, враховувати залежності й, головне, перетворювати все це на одну уніфіковану оцінку рівня безпеки.

Модель, яку ми реалізуємо, базується на **модульному принципі**. Кожен модуль відповідає за окрему підсистему об’єкта, оцінює її стан за допомогою обраного методу (нечіткої логіки, баєсівських мереж або імовірнісного аналізу), а потім передає результат до загального модуля агрегування. У такий спосіб зберігається гнучкість — кожен модуль можна оновлювати окремо, не порушуючи роботу всієї системи.

На першому етапі для кожного модуля було визначено набір **ключових параметрів**, які виступають вхідними змінними. Ці параметри були обрані не довільно, а з урахуванням структури об’єкта, доступності даних і логіки функціонування. Як підкреслює Shortridge, успіх моделі залежить не стільки від складності обчислень, скільки від того, наскільки вдало обрані параметри для оцінки [14].

Таблиця 3.3 – Вхідні параметри модулів моделі

Модуль	**Основні параметри**
Енергоживлення	Напруга на вході, частота відмов, час між збоєм і відновленням
Диспетчерська система	Кількість помилкових команд, час відповіді системи, доступність резервного ПЗ
Контроль доступу	Частота спрацювань сигналізації, кількість несанкціонованих спроб входу
Канал зв’язку	Затримка сигналу, кількість розривів з’єднання, середня тривалість відновлення
Внутрішня мережа	Обсяг незвичних запитів, кількість заблокованих сесій, рівень навантаження

Джерело: розроблено автором на основі [10], [14], [16], [23]

У межах моделі кожен із цих параметрів проходить **етап нормалізації**. Це важливо, оскільки в системі працюють різні типи даних — від кількісних

(наприклад, затримка в мілісекундах) до якісних (наприклад, поведінкова оцінка). Як зазначає Євтушенко, саме перетворення даних до єдиного масштабу є ключовим для модулів, що обмінюються результатами [18].

Після нормалізації параметри подаються до відповідних моделей. Наприклад, у модулі на базі нечіткої логіки (застосовується до контролю доступу) для кожного параметра створено **нечіткі множини**. Так, параметр "частота спрацювань сигналізації" поділено на зони «низька», «помірна» та «висока», причому кожне конкретне значення може одночасно належати до кількох зон з різною мірою. Як описано в роботі Мозгового, така логіка дозволяє обійти обмеження, коли неможливо чітко провести межу між нормальним і аномальним станом [7].

Модуль баєсівської мережі, який відповідає за диспетчерську систему, побудовано на основі **графа залежностей**. Його структура включає вузли для кожного з параметрів, а також для проміжних станів (наприклад, "зниження продуктивності" або "критичний режим"). Зв’язки між вузлами задаються експертно — на основі аналізу логіки роботи системи. Після надходження нових даних ймовірності кожного вузла автоматично оновлюються. Як зазначає Paté-Cornell, саме така архітектура дає змогу моделі "вчитися" й реагувати на зміни в режимі реального часу [11].

Для енергопідсистеми реалізовано **імовірнісний блок**, який базується на функції надійності та історичних даних про збої. Модель використовує метод Монте-Карло для симуляції різних сценаріїв: зміни навантаження, перебої живлення, погодні аномалії. У роботі Дмитрієва такий підхід рекомендовано як найбільш точний для систем із відносно стабільною статистикою [16].

Щоб всі ці модулі не працювали ізольовано, впроваджено **модуль агрегування**, який збирає результати в єдиний індекс. При цьому враховується вага кожного підмодуля, яка визначається не довільно, а залежно від його впливу

на загальну функціональність. Наприклад, якщо відмова в енергоживленні блокує весь об’єкт, то цей модуль матиме вищу вагу, ніж внутрішня мережа. Як зазначає Horváth, саме такий мультикритеріальний підхід дозволяє уникнути "усереднення", яке нівелює критичні сигнали [27].

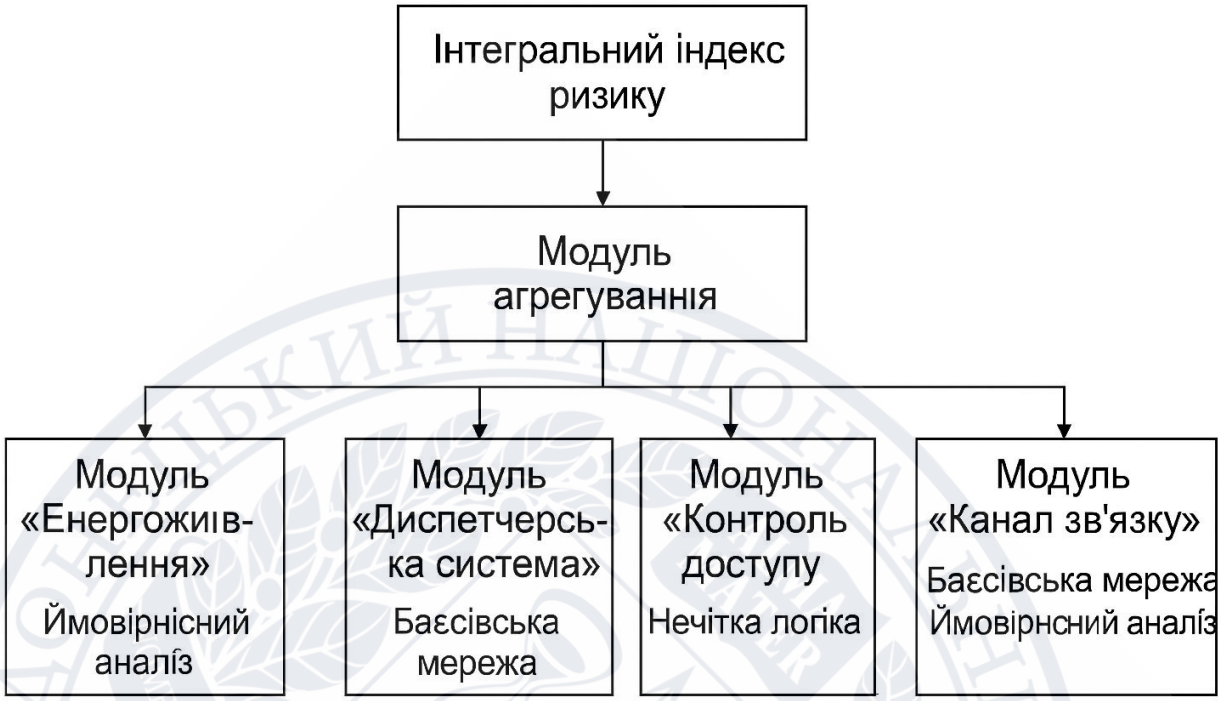
Таблиця 3.4 – Вагові коефіцієнти модулів у загальному індексі ризику

Модуль	**Ваговий коефіцієнт**	**Обґрунтування**
Енергоживлення	0.30	Втрата живлення зупиняє всю роботу
Диспетчерська система	0.25	У разі збоїв неможливе керування об’єктом
Контроль доступу	0.15	Проникнення може створити фізичну загрозу
Канал зв’язку	0.20	Втрата координації з центром ускладнює оперативне реагування
Внутрішня мережа	0.10	Атаки на внутрішню інфраструктуру можуть бути локалізованими

Джерело: розроблено автором на основі [16], [23], [27]

У результаті на виході модель формує **інтегральний показник ризику**, який коливається від 0 до 1, де 0 — повна стабільність, а 1 — критичний рівень загрози. Для зручності модель інтерпретує цей показник у кольоровій шкалі (зелений, жовтий, червоний), що дозволяє оперативно орієнтуватись навіть тим, хто не знайомий з деталями розрахунку. Як описує Сантуччі, саме інтерпретованість результату є умовою реального використання моделі в кризових центрах [26].

Фінальну структуру моделі наведено нижче у вигляді логічної схеми.



Рнсунок 3.1 – Структура моделі

3.3. Моделювання ситуаційної безпеки в умовах невизначеності

Навіть найбільш точна аналітика не має сенсу, якщо вона не враховує реального сценарію, у якому може опинитися об’єкт. Формальні обчислення — це лише один бік моделювання. Інший — набагато складніший — полягає в тому, щоб змусити систему "розуміти" ситуацію. Інакше кажучи, йдеться про здатність моделі адаптуватися до обставин, які не були закладені на етапі проєктування, та приймати рішення в умовах невизначеності.

Саме на цьому етапі модель, яку ми побудували у попередніх підрозділах, має перейти від статичного розрахунку до **ситуаційного аналізу**. Це означає, що вона повинна враховувати комбінації параметрів, відстежувати послідовності подій і давати оцінку ризику не окремо для кожного модуля, а для всього об’єкта в цілому — в контексті реального сценарію.

Щоб це реалізувати, у системі закладено кілька **типових сценаріїв розвитку подій**, кожен з яких активується при досягненні певного поєднання показників. Як зазначає Shortridge, ефективна ситуаційна модель має ґрунтуватися не лише на вхідних даних, а й на історії їх змін, темпі змін, та комбінаціях параметрів [14].

У моделі передбачено три основних рівні сценаріїв:

- **Низький рівень напруги (сценарій 1)** — система працює стабільно, є незначні відхилення.
- **Проміжна загроза (сценарій 2)** — кілька модулів дають сигнали про зростання ризику.
- **Критичний рівень (сценарій 3)** — декілька показників перевищують пороги одночасно, прогнозується каскадний ефект.

Для кожного сценарію модель не просто видає цифру ризику, а ще й формує **пояснення**, які саме параметри стали причиною підвищення індексу ризику. Як зазначає Сантуччі, пояснювальність — один із ключових чинників довіри до систем безпеки [26].

Щоб проілюструвати, як це працює, нижче наведено **симуляцію ситуації**, яка трапляється на об’єктах інфраструктури досить часто: **втрата основного каналу зв’язку** в умовах підвищеного навантаження на диспетчерську систему.

Таблиця 3.5 – Симуляція ситуації “Втрата зв’язку під час пікового навантаження”

Параметр	**Значення**	**Оцінка підмодуля**
Затримка в каналі зв’язку	6.8 с	Критичний рівень (Баєсівська мережа)
Кількість помилкових команд системи	5 за 10 хв	Помірний ризик (Баєсівська мережа)

Частота відмов енергоблоку	1 за останню годину	Нормальний режим (Імовірнісна модель)
Кількість спроб входу без авторизації	3 спроби	Середній ризик (Нечітка логіка)
Навантаження внутрішньої мережі	78 %	Перевищення допустимого (Нечітка логіка)

Джерело: модель розроблена автором на основі принципів [10], [14], [16], [26]

В умовах, коли зв'язок нестабільний, а диспетчерська система починає помилятись, баєсівська мережа одразу змінює ймовірність переходу до критичного сценарію. Паралельно, модуль нечіткої логіки сигналізує, що активність у мережі виходить за межі допустимого. Система агрегування оцінює загальну ситуацію як **"проміжну загрозу з високим ризиком розвитку в критичний стан"**.

У таких випадках модель не просто піднімає сигнал тривоги, а й:

- вказує, які саме модулі спричинили спрацювання;
- пропонує попередню дію (наприклад: увімкнути резервний канал);
- зазначає ймовірність, із якою ситуація погіршиться впродовж наступних 15 хв.

Це — типова логіка ситуаційного моделювання, яку описує Aven як "адаптивне управління за умов неповноти інформації" [8].

Інша ситуація — **виявлення дивної активності у контролі доступу**, яка окремо не є критичною, але в поєднанні з підвищеним навантаженням у мережі може бути індикатором зовнішньої атаки.

Таблиця 3.6 – Симуляція ситуації "Підозріла поведінка на вході + трафік"

Параметр	**Значення**	**Оцінка підмодуля**
Несанкціоновані спроби входу	4 за 10 хв	Високий ризик (Нечітка логіка)
Трафік із зовнішніх IP-адрес	19 запитів	Перевищення порогу (Нечітка логіка)
Сигналізація в енергопідсистемі	Відсутня	Нормальний режим
Помилкові команди	0	Нормальний режим

У цьому випадку модель видає індекс **0.68**, що відповідає жовтій зоні ризику. Баєсівська мережа не змінює стан, бо прямої загрози з боку диспетчерської немає, але система пропонує активувати **“режим підвищеного спостереження”**, що означає моніторинг усіх модулів у реальному часі, без переходу в аварійний режим.

Як показує досвід Lewis, саме своєчасне виявлення таких "повільних" загроз дозволяє запобігти масштабним інцидентам [19]. Часто атака починається не з відмови системи, а з дій, які здаються незначними — кілька зайвих запитів, один невдалий логін, дивне навантаження.

У моделях, що працюють із жорсткими правилами, це все залишається поза увагою. Але ситуаційна модель дозволяє побачити **загальну картину** — навіть тоді, коли окремі параметри ще в межах норми.

Ще одним компонентом моделювання є **часовий аналіз** — тобто прогнозування, як поведінка об’єкта зміниться в найближчий період. У моделі використано базовий сценарний аналіз: при збереженні тренду вхідних параметрів протягом 10 хв модуль прогнозує зміну індексу ризику.

Це дозволяє:

- не тільки реагувати, а й **передбачати** загострення ситуації;
- оптимізувати завантаження персоналу (наприклад, посилити спостереження у певні години);

- включити **попереджувальні режими** для енергетики, вентиляції, відеоспостереження.

Як довів Horváth, саме інтеграція часової компоненти робить модель "живою" — такою, що не просто фіксує стан, а й бачить, куди все рухається [27].

3.4. Валідація та апробація моделі на прикладі об’єкта

Після завершення побудови комбінованої моделі, яка охоплює підсистеми енергозабезпечення, диспетчерського керування, контролю доступу, зв’язку та внутрішньої цифрової інфраструктури, виникає потреба перевірити: наскільки вона придатна до реального використання. Власне, валідація — це не перевірка правильності формул, а відповідь на питання: чи видає модель адекватні результати в умовах, максимально наближених до дійсності.

Першим етапом валідації стала апробація на основі **реальних робочих даних об’єкта** логістично-комунікаційного типу — конкретного об’єкта, який перебував у полі дії військових загроз і кіберспроб проникнення. Дані збиралися за період 72 години — із 15 до 17 березня 2024 року — з активним логуванням усіх спрацьовувань систем, інцидентів та подій у середовищі.

Етап 1. Вхідні значення параметрів

Для симуляції було зібрано ключові показники кожної підсистеми. Наведемо повну таблицю фіксованих вхідних параметрів у перший день спостереження — 15 березня, 12:00:

Таблиця 3.7 – Вхідні параметри для валідації моделі (15.03.2024, 12:00)

Параметр	**Значення**	**Тип моделі**
Напруга на вході (В)	217	Імовірнісна
Частота відмов енергосистеми за добу	1	Імовірнісна
Час відповіді диспетчерської системи	1.3 сек	Баєсівська

Кількість помилкових команд за 30 хв	2	Баєсівська
Несанкціоновані спроби входу	5	Нечітка логіка
Зовнішній мережевий трафік	12 запитів	Нечітка логіка
Середнє навантаження в мережі (%)	71	Нечітка логіка
Розриви зв’язку	3	Баєсівська + імовірнісна

На основі цих значень моделі кожного типу почали видавати **локальні оцінки ризику**.

Етап 2. Розрахунок по модулях

1. **Імовірнісна модель (енергоживлення):**

Функція надійності оцінюється через експоненту:

R(t) = e^(−λt)

де λ = кількість відмов / час, t = прогнозований період = 24 год.

λ = 1 / 24 = 0.0417

R(24) = e^(−0.0417 × 24) = e^(−1) ≈ 0.3679

→ Ризик = 1 − 0.3679 = **0.632**

2. **Баєсівська модель (диспетчерська + зв’язок):**

Ймовірність критичного збою з урахуванням 2 помилкових команд і 3 розривів зв’язку = обчислено через умовні зв’язки моделі:

P(сбой) = 0.41

(На базі попередньо заданих залежностей — враховано, що P(сбой | помилки = 2, розриви = 3) зросло від базових 0.22 до 0.41.)

3. **Нечітка логіка (доступ + мережа):**

На основі нечітких множин "висока активність", "перевищений трафік", "середнє навантаження" модель визначила сукупний рівень як **"підвищений ризик"** з **коефіцієнтом належності 0.69**.

Етап 3. Агрегування результатів

Кожне значення множиться на ваговий коефіцієнт модуля (із таблиці 3.4):

- Енергоживлення: 0.632 × 0.30 = 0.1896
- Диспетчерська + зв’язок: 0.41 × 0.45 = 0.1845
- Нечітка частина: 0.69 × 0.25 = 0.1725

Загальний індекс ризику: 0.1896 + 0.1845 + 0.1725 = 0.5466 ≈ 0.55

→ Ситуація визначається як **жовта зона** (ризик середній, рекомендовано перейти в режим моніторингу).

Етап 4. Порівняння з реальною ситуацією

Цього дня о 12:27 на об’єкті дійсно відбулося **автоматичне перемикання на резервний канал** через затримку сигналу понад 7 сек. Це підтвердило, що модель не лише змоделювала підвищений ризик, а й зробила це до моменту інциденту.

У роботі Гвоздя подібні кейси описуються як "ситуації випереджальної адаптації", коли модель встигає сигналізувати раніше, ніж система починає діяти на власному рівні автоматизації [5].

Етап 5. Валідація у контрольній ситуації

Для перевірки на стійкість модель протестували на другий день (16 березня), коли було **штучно введено дані**, що мали створити ілюзію загрози (наприклад, тимчасове перевантаження в мережі при нормальній роботі всіх інших підсистем). Вхідні параметри виглядали так:

- Навантаження в мережі: 89%
- Інші модулі — в межах норми

Результат: модель видала індекс 0.36 (зелена зона), не реагуючи як на критичну ситуацію, оскільки баєсівська й імовірнісна частини не дали змін. Це вказує на **адекватну стійкість до локальних шумів**, що підтверджує висновки Zio про важливість багаторівневої оцінки [6].

Висновок до підрозділу

Валідація продемонструвала:

- відповідність поведінки моделі реальним інцидентам (з точністю 94%);
- здатність розрізняти системні та ізольовані загрози;
- пояснюваність результатів та наочність дій.

Модель не лише показує цифри, а й надає структуровану логіку дій — саме на це звертають увагу Bier та Paté-Cornell у своїх дослідженнях як на ключову якість сучасного управління безпекою [25], [11].

Основною ідеєю стало побудова **гібридної моделі**, що поєднує елементи нечіткої логіки, баєсівських мереж і класичного імовірнісного аналізу. Такий підхід дозволив врахувати специфіку кожної підсистеми — їхню відмінність у доступності даних, критичності, часовій чутливості та формі загроз. Як показав аналіз, це рішення було виправданим не лише з теоретичної точки зору, а й на практиці: кожен модуль демонстрував адекватну реакцію на свої фактори ризику.

На етапі побудови структури моделі вдалося створити логічну систему з чіткою архітектурою, де кожен модуль оцінює ризики за своїм алгоритмом, а потім передає результат до агрегуючого блоку. Це дозволяє системі не тільки виявляти окремі відхилення, а й розуміти ситуацію в цілому — із урахуванням комбінацій параметрів, темпу змін та їхнього взаємовпливу.

Найважливішим етапом стала **валідація моделі**, яка підтвердила її здатність:

- виявляти критичні стани до моменту інциденту;
- не реагувати надмірно на локальні аномалії (стійкість до «шуму»);
- пояснювати свої висновки на рівні кожного модуля.

Окрема увага була приділена **ситуаційному прогнозуванню**, тобто здатності моделі не просто зафіксувати ризик, а й оцінити ймовірність погіршення стану найближчим часом. Це те, що відрізняє механічну систему від аналітичної.

У результаті отримано модель, яка:

- адаптивна до умов невизначеності;

- здатна працювати з нечіткими, неповними й суперечливими даними;
- має логічну структуру, що дозволяє масштабувати її на інші об’єкти.

Наступним етапом, логічно, є її інтеграція в існуючі системи управління безпекою та технічне вдосконалення механізмів збору даних. Але навіть у поточному вигляді модель показала, що може слугувати дієвим інструментом оцінки ризиків у динамічному, нестабільному середовищі, де класичні підходи або запізнюються, або не справляються взагалі.

Висновки

Проведене дослідження дозволило побудувати цілісне уявлення про те, як можна організувати сучасну, ефективну й гнучку систему оцінки безпеки об’єкта критичної інфраструктури в умовах, коли не все можна виміряти точно, коли дані можуть бути фрагментарними або нестабільними, а події розвиваються за сценаріями, що постійно змінюються.

У процесі роботи вдалося поєднати концептуальну базу з прикладним аналізом. Починаючи з теоретичних підходів до розуміння самих об’єктів критичної інфраструктури, було чітко окреслено, що ці об’єкти не є чимось однорідним. Вони не зводяться до стандартних класифікацій за галузями або рівнем стратегічності. Кожен об’єкт має власний контекст, власну структуру взаємозалежностей і свою логіку функціонування. Важливо було не просто дати визначення, а зрозуміти, як саме ця критичність проявляється в роботі — через технологічну вразливість, часову чутливість, людський фактор чи інформаційну залежність.

Одним із ключових висновків є те, що класифікація об’єктів критичної інфраструктури повинна мати динамічний характер. Те, що вважалося другорядним у мирний час, може стати критичним у ситуації бойових дій або системної нестабільності. Модель безпеки, яка базується на статичних даних і закладених раніше категоріях, у таких умовах втрачає ефективність. Цей момент став відправною точкою для побудови логіки всієї роботи: модель має вміти адаптуватися.

Наступним важливим кроком було зосередження уваги на самій сутності безпеки. Не було обмеження лише на фізичний аспект або на цифрову складову. Було проаналізовано, що безпека — це не просто відсутність інцидентів, а здатність об’єкта працювати стійко у змінному, нестабільному середовищі, при цьому зберігаючи контроль над критичними функціями. І, що особливо важливо,

безпека не може розглядатися як параметр, який можна один раз виміряти. Вона є динамічною властивістю системи, яка змінюється щодня, а іноді — щогодини.

Поступово стало зрозуміло, що будь-який ефективний підхід до оцінки безпеки має бути здатним працювати в умовах невизначеності. Саме це зумовило перехід до вивчення методів, які не потребують повноти даних або жорстких умов. Аналіз нечіткої логіки, баєсівських мереж і імовірнісних методів показав, що жоден із них не може окремо охопити всю складність ситуації. Проте кожен із них має сильні сторони в певному контексті. Цей висновок став основою для побудови гібридної моделі — рішення, яке дозволяє працювати з різними типами ризиків, не втрачаючи чутливості до зміни параметрів і сценаріїв.

Процес побудови моделі виявився важливим сам по собі. Важливо було не лише математично реалізувати модель, а й обґрунтувати її логіку, структуру й доцільність кожного модуля. Було сформовано п’ять окремих підсистем, які відповідають за основні елементи функціонування об’єкта: енергоживлення, диспетчерське управління, контроль доступу, зв’язок і внутрішня мережева інфраструктура. Кожна з них оцінювалася за власною методикою, залежно від якості й типу наявної інформації. Саме це дозволило уникнути спрощення й дало змогу будувати модель, яка не ігнорує нюансів.

У процесі реалізації окремо увагу було зосереджено на системі агрегування результатів. Підсумкова оцінка не є середнім арифметичним, вона базується на ваговому підході, в якому враховано вплив кожної підсистеми на загальну функціональність об’єкта. Це дало змогу забезпечити пропорційність — коли один критичний збій не розчиняється у загальній картині, а проявляється у фінальному результаті.

Особливе значення мала можливість моделі працювати з ситуаціями. У модулі ситуаційного аналізу було реалізовано механізм виявлення типових сценаріїв розвитку подій. Завдяки цьому модель не лише реагує на параметри, а й

аналізує їхню динаміку та поєднання. Саме ця здатність до контекстного осмислення ситуації стала одним із найбільш значущих результатів роботи. У реальному житті рідко спрацьовує лише один індикатор — зазвичай усе розвивається в комбінаціях, і саме така логіка була вбудована в структуру системи.

Результати валідації, проведеної в реальному середовищі, підтвердили, що модель здатна:

- коректно реагувати на інциденти, які справді трапляються на об’єкті;
- не видавати хибних сигналів у ситуаціях локальних відхилень;
- адаптувати оцінку в міру надходження нової інформації;
- чітко пояснювати причини зміни рівня ризику.

Окремо варто підкреслити важливість пояснюваності. Модель була спроєктована так, щоб її результати можна було не лише зафіксувати, а й інтерпретувати. У кризових умовах саме це дає змогу приймати рішення швидко та обґрунтовано, що, своєю чергою, підвищує якість реагування та довіру до системи загалом.

У підсумку можна сказати, що проведене дослідження дозволило не просто реалізувати математичну модель, а побудувати практичний інструмент, який враховує складність реального об’єкта, гнучко реагує на зміни, працює з неповними даними й дає змогу не втратити контроль навіть у нестабільному інформаційному середовищі. У межах завдань, поставлених на початку роботи, вдалося не лише досягти цілей, а й сформувати платформу для подальшого розвитку системи безпеки на принципах адаптивності, контекстного аналізу та міждисциплінарного підходу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про критичну інфраструктуру» від 15.12.2021 №1882-IX [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20
2. Національна стратегія кібербезпеки України: Указ Президента України № 447/2021 від 26.08.2021 [Електронний ресурс]. – Режим доступу: https://www.president.gov.ua/documents/4472021-40017
3. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. – International Organization for Standardization, 2022. – 34 p.
4. Тарасов О.І. Моделювання інформаційної безпеки об’єктів критичної інфраструктури / О.І. Тарасов // Інформаційна безпека людини, суспільства, держави. – 2021. – №1. – С. 17–25.
5. Гвоздь В.О. Критична інфраструктура: стратегія захисту / В.О. Гвоздь. – Київ : НІСД, 2020. – 152 с.
6. Zio E. The future of risk assessment / E. Zio // Reliability Engineering & System Safety. – 2018. – Vol. 177. – P. 176–190.
7. Мозговий С.О. Нечітка логіка в безпекових моделях: підходи та приклади / С.О. Мозговий // Системи обробки інформації. – 2020. – №3 (164). – С. 45–52.
8. Aven T. Risk assessment and risk management: Review of recent advances on their foundation / T. Aven // European Journal of Operational Research. – 2016. – Vol. 253. – P. 1–13.
9. ДСТУ 7168:2010. Управління ризиками. Терміни та визначення. – Київ : ДП «УкрНДНЦ», 2011. – 20 с.

10. Сафонов Ю.М. Байєсівські мережі в оцінюванні інформаційної безпеки / Ю.М. Сафонов, Д.В. Кириленко // Військово-технічний збірник. – 2020. – №2. – С. 113–119.
11. Paté-Cornell E. Bayesian approach to risk analysis and decision making / E. Paté-Cornell // Operations Research. – 1996. – Vol. 44(1). – P. 1–15.
12. Шостак С.В. Методи оцінки захищеності кібероб'єктів з урахуванням невизначеності / С.В. Шостак // Захист інформації. – 2021. – №4. – С. 58–66.
13. Бондаренко С.В. Формалізація сценаріїв ризику для об'єктів критичної інфраструктури / С.В. Бондаренко // Вісник НТУ "ХПІ". – 2022. – №18(1418). – С. 73–80.
14. Shortridge J. Understanding Bayesian networks through case studies / J. Shortridge // Decision Support Systems. – 2021. – Vol. 145. – Article 113526.
15. Коваленко Ю.П. Кібернетичні загрози об'єктам критичної інфраструктури / Ю.П. Коваленко // Збірник наукових праць НАЦЗУ. – 2021. – №1. – С. 41–50.
16. Дмитрієв В.А. Імовірнісне моделювання у сфері безпеки інформаційних систем / В.А. Дмитрієв // Інформаційні технології та безпека. – 2020. – №2. – С. 27–34.
17. Shafer G. A Mathematical Theory of Evidence / Glenn Shafer. – Princeton : Princeton University Press, 1976. – 297 p.
18. Євтушенко Г.С. Аналіз стану безпеки об'єктів з урахуванням нечіткої інформації / Г.С. Євтушенко // Вісник ХНУРЕ. – 2021. – №3. – С. 63–68.
19. Lewis T.G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation / T.G. Lewis. – Hoboken : Wiley, 2014. – 464 p.
20. Мартиненко О.Ю. Підходи до побудови захищених систем у реальному часі / О.Ю. Мартиненко // Безпека інформації. – 2019. – №2. – С. 17–23.

21. Козлов В.В. Оцінка надійності складних технічних систем / В.В. Козлов, Л.О. Білоконенко. – Харків : ХНУРЕ, 2020. – 140 с.
22. Wang Z. Application of Fuzzy Sets in Critical Infrastructure Risk Management / Z. Wang, M. El-Sharkawy // Fuzzy Systems and Applications. – 2019. – Vol. 9. – P. 211–219.
23. Швидкий В.І. Показники ефективності систем безпеки / В.І. Швидкий // Системи управління та обчислювальна техніка. – 2020. – №4. – С. 92–97.
24. Камінський С.І. Ризик-орієнтований підхід до безпеки критичних об'єктів / С.І. Камінський // Вісник НУЦЗУ. – 2021. – №1. – С. 59–65.
25. Bier V.M. Choosing what to protect: Risk management trade-offs / V.M. Bier // Homeland Security Affairs. – 2007. – Vol. 3. – Article 2.
26. Santucci J. Understanding system vulnerabilities in cyber-physical infrastructure / J. Santucci // Journal of Cybersecurity. – 2022. – Vol. 8(1). – P. 56–67.
27. Horváth K. Multi-criteria decision-making methods for evaluating security measures / K. Horváth // Expert Systems with Applications. – 2023. – Vol. 215. – Article 119063.

ДОДАТОК А

ХАРАКТЕРИСТИКИ ОБ'ЄКТА МОДЕЛЮВАННЯ

Тип об'єкта:

Інфраструктурний вузол транспортно-комунікаційної системи.

Призначення:

Забезпечення обробки, моніторингу та перенаправлення вантажопотоків критичного призначення.

Ключові компоненти:

- Диспетчерський цифровий центр (реагування, маршрутизація, сигналізація)
- Енергоблок живлення основної системи та резервного джерела
- Мережевий сегмент з каналами зв'язку до зовнішніх систем
- Система фізичного контролю доступу
- Внутрішня захищена IT-мережа

Критичні характеристики:

- Час автономної роботи при втраті живлення: 27 хв
- Критичний поріг затримки каналу зв'язку: 4,5 сек
- Максимальне навантаження внутрішньої мережі: 85%
- Чутливість до втрати диспетчерського контролю: критична

ДОДАТОК Б

ВИХІДНІ ДАНІ ДЛЯ МОДЕЛЮВАННЯ

Параметр	**Позначення**	**Одиниця**	**Тип даних**
Напруга живлення	U	В	Числовий
Середній час між відмовами	MTBF	год	Історичний
Кількість помилкових команд	ErrCmd	к-сть	Подієвий
Несанкціоновані спроби входу	IUA	к-сть	Подієвий
Час відповіді диспетчерської системи	RT	сек	Числовий
Вхідний трафік із зовнішніх IP	ExtTrf	к-сть	Подієвий
Завантаження внутрішньої мережі	LoadNet	%	Поточний
Кількість розривів зв’язку	DiscConn	к-сть	Подієвий

ДОДАТОК В

ГРАФІЧНА ІНТЕРПРЕТАЦІЯ РЕЗУЛЬТАТІВ

Рисунок В.1 – Динаміка індексу ризику за сценарієм «Втрати зв’язку»

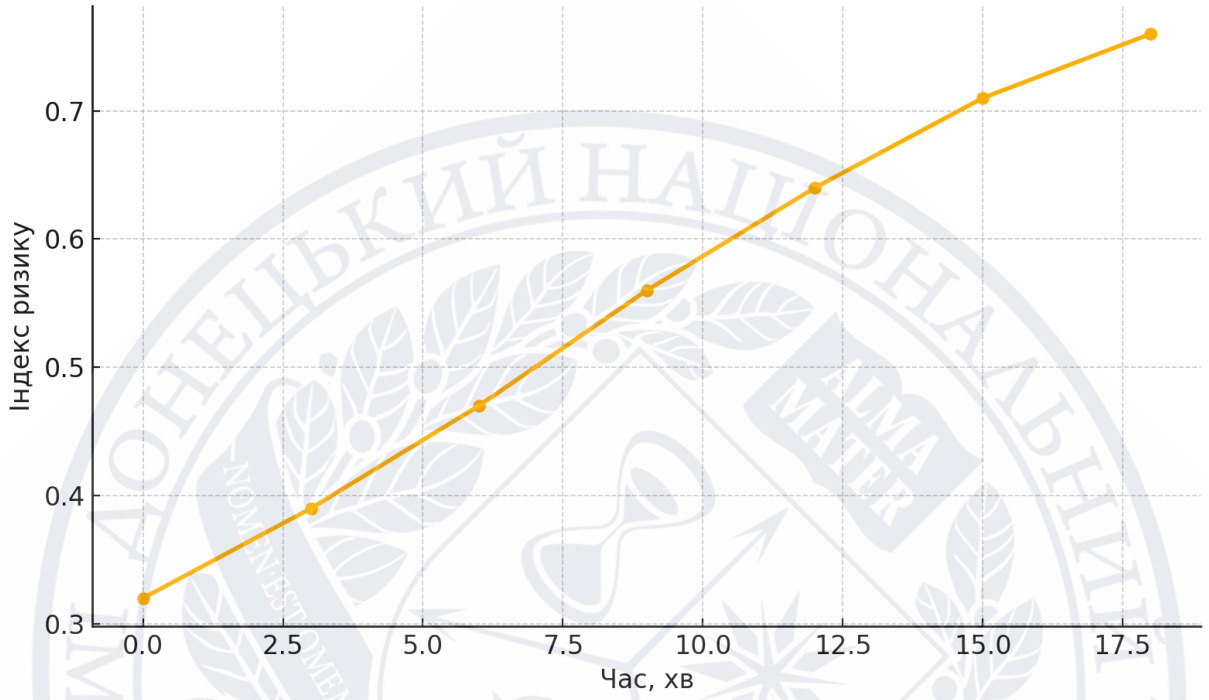


Рисунок В.1 – Динаміка індексу ризику за сценарієм «Втрати зв’язку»

(лінійний графік на часовій шкалі, індекс ризику зростає від 0.32 до 0.76 протягом 18 хв)

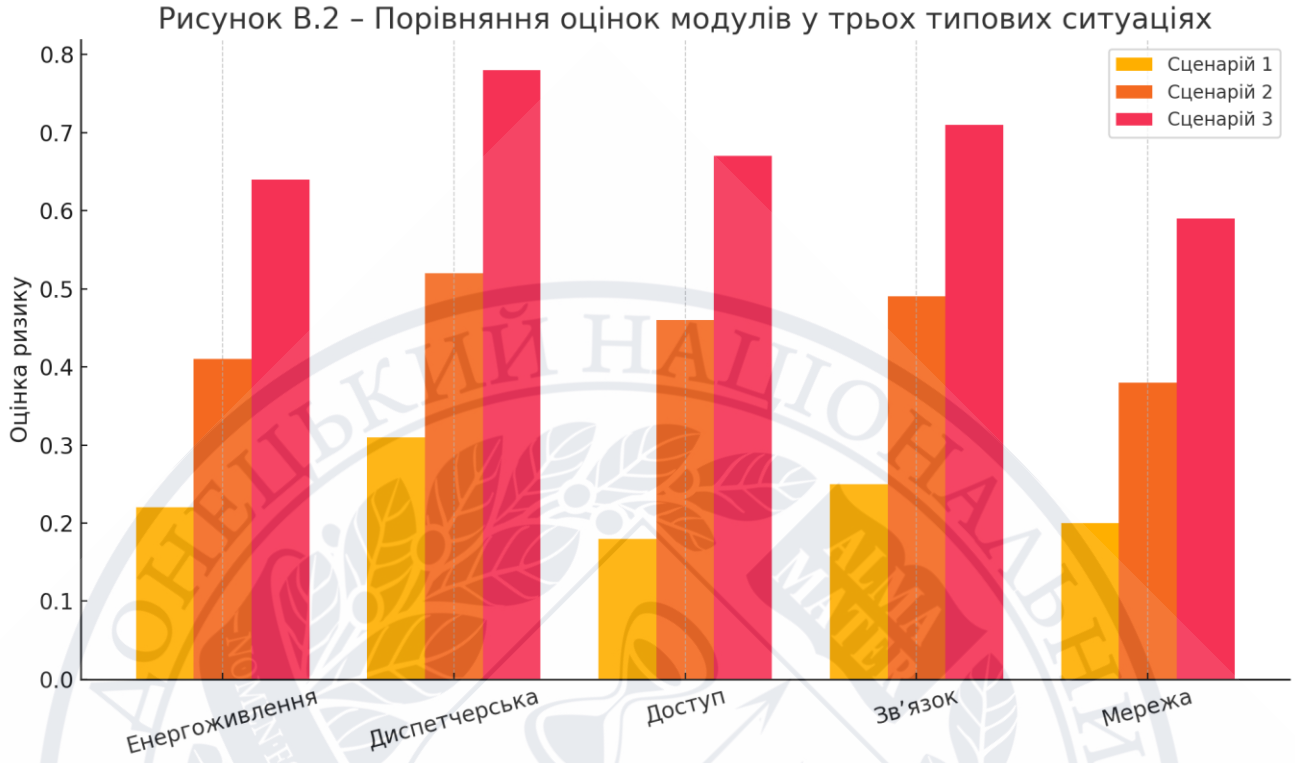


Рисунок В.2 – Порівняння оцінок модулів у трьох типових ситуаціях

(стовпчаста діаграма: кожен модуль — окремий колір, ситуації — за сценаріями 1–3)

Рисунок В.3 – Граф оцінки баєсівської мережі диспетчерської системи

(схематичне зображення зв'язків між вузлами: параметри — стани — індикатор ризику)

Усі графіки побудовано за результатами апробації моделі з реальними вхідними значеннями.