http://www.moderntechno.de/index.php/meit/article/view/meit39-02-012
DOI: 10.30890/2567-5273.2025-39-02-012

CONCEPTUAL MODEL FOR DYNAMIC QUANTITATIVE CYBERSECURITY RISK ANALYSIS IN TELECOMMUNICATION DIGITAL ECOSYSTEMS

КОНЦЕПТУАЛЬНА МОДЕЛЬ ДИНАМІЧНОГО КІЛЬКІСНОГО АНАЛІЗУ РИЗИКІВ КІБЕРБЕЗПЕКИ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ ЦИФРОВИХ ЕКОСИСТЕМ

Reshetniak P.Y. / Решетняк П.Ю.
PhD Student / аспірант
ORCID ID: 0009-0005-1643-8239
National University of Life and Environmental Sciences of Ukraine,
Kyiv, Heroiv Oborony Str.15, 03041
Національний Університет Біоресурсів та Природокористування України,
Київ, вул. Героїв Оборони, 15, 03041

Анотація. *Стаття присвячена розробці концептуальної моделі динамічного кількісного аналізу ризиків кібербезпеки для телекомунікаційних цифрових екосистем. Мета розробки полягає у підвищенні точності оцінки ризиків та оперативності реагування на кіберзагрози в умовах мінливого ландшафту загроз і невизначеності стану активів. Метод базується на інтеграції онтологічних моделей, баєсових нейронних мереж (BNN) і методу Монте-Карло. Онтологічна модель формалізує знання про активи, сервіси та послуги, а BNN забезпечує ймовірнісне прогнозування компрометації з урахуванням невизначеності. Метод Монте-Карло застосовується для агрегації ймовірностей у ієрархіях сервісів та послуг. Результати включають розроблену концептуальну модель, яка реалізує безперервний аналіз ризиків у реальному часі, обчислення монетарного ризику та пріоритету відновлення для телекомунікаційних послуг, а також інтерактивну візуалізацію результатів. Показано, що концептуальна модель має потенціал уникнення недоліків традиційних підходів, таких як інертність і недостатнє врахування динамічних залежностей. Подальші напрямки досліджень охоплюють розширення онтологічної моделі, оптимізацію BNN та валідацію положень теоретичної моделі на прикладах телекомунікаційних послуг.*

Ключові слова: *Кібербезпека, телекомунікаційні екосистеми, динамічний аналіз ризиків, онтологічна модель, баєсові нейронні мережі, Монте-Карло симуляція.*

Вступ

Телекомунікаційна галузь як одна із складових критичної інфраструктури країни, все частіше стає об’єктом атак в кібернетичному просторі. Складні цифрові екосистеми, які об’єднують традиційну IT-інфраструктуру, телекомунікаційні мережі та хмарні сервіси, є основою для надання сучасних цифрових послуг. В той-же час, такі екосистеми фактично створюють широкий ландшафт для початкового доступу в складних ланцюгах кібератак. За даними звітів міжнародних організацій [1],[2], а також, звітів про нещодавні кібератаки

на телеком-компанії США та Європи [3],[4], саме телекомунікаційні мережі стають однією з найчастіших цілей масштабних і складних кібератак, серед яких DDoS-атаки, перехоплення трафіку, а також цільові атаки на критичні вузли телекомунікаційних мереж. Особливу небезпеку становлять так звані складні стійкі загрози (Advanced Persistent Threats, APT), ціллю яких є критичні елементи телекомунікаційної інфраструктури, а метою - тривала й непомітна присутність, що надає можливості перехоплення та витоку конфіденційних даних з можливістю подальшого знищення як самих інфраструктур, так й слідів присутності.

Постановка проблеми

Ефективне та своєчасне управління кіберризиками в складних гетерогенних середовищах компаній телекомунікаційної галузі є критично важливим завданням для убезпечення бізнес-процесів та захисту клієнтських даних, а також для прийняття обґрунтованих рішень щодо інвестицій та ефективного розподілу ресурсів на кіберзахист. Традиційні підходи та методики оцінки та управління кіберризиками, такі як ISO 31000, ISO 27005, як правило, орієнтовані на планово-періодичні оцінки ризиків (щоквартальні, щорічні, або при внесенні значних змін на рівні інфраструктур та мереж). Такі традиційні підходи мають низку недоліків та обмежень при застосуванні у гетерогенних динамічних середовищах, як-то:

1. Відсутність розуміння розмірів впливу на окремі телекомунікаційні послуги, що надаються кінцевим споживачам.

2. Інертність у реагуванні на швидко змінюваний ландшафт кіберзагроз, зокрема появу вразливостей нульового дня (zero-day) та нових векторів атак.

3. Неможливість виявлення та врахування подій у реальному часі, що знижує ефективність превентивних та коригувальних заходів.

4. Недостатнє відображення складних, багаторівневих та нелінійних взаємозв’язків між активами, сервісами, послугами, вразливостями та загрозами.

5. Зниження фактичного рівня захищеності в інтервалах між оцінками (так зване «вікно вразливості», коли ризики залишаються неврахованими та система

фактично перебуває в незахищеному стані).

6. Високий рівень невизначеності та неповноти даних про стан захищеності активів, обумовлений змінами (наприклад, у конфігураціях та архітектурах систем, мереж та інфраструктур).

Таким чином, практична проблема полягає у відсутності інтегрованого підходу до безперервного аналізу ризиків кібербезпеки в телекомунікаційних складних гетерогенних середовищах, який би враховував динамічні зміни як на рівні активів, так й на рівні загроз, дозволяв би враховувати невизначеності та неповну інформацію щодо стану та захищеності активів, та забезпечував оперативну і точну оцінку ризиків кібербезпеки у реальному часі, а також дозволяв би кількісно оцінювати ризики кібербезпеки не тільки на рівні окремих активів, а й на рівні телекомунікаційних послуг, що надаються кінцевим споживачам.

Аналіз останніх досліджень і публікацій.

Традиційні стандарти управління інформаційною безпекою (ISO/IEC 27005:2022, NIST SP 800-30/37/137 тощо) та методології кількісної оцінки ризиків (наприклад, FAIR) активно використовуються для ідентифікації та оцінки ризиків в організаціях телекомунікаційної галузі, але переважно розраховані на періодичне, статичне використання. Вони не завжди ефективно реагують на стрімкі зміни ландшафту загроз. При цьому актуальний ISO/IEC 27005 значно розвинувся з урахуванням «динамічної природи загроз та зростаючої складності IT-середовищ» [5], а модель FAIR пропонує кількісні оцінки ризику в монетарному вигляді. Водночас експерти зауважують, що традиційні «жорсткі» процеси оцінки ризиків не можуть самостійно підтримувати необхідний рівень захисту в умовах безперервних змін. Наприклад, NIST SP 800-137 підкреслює роль безперервного моніторингу ІБ (continuous monitoring) – «постійного усвідомлення стану безпеки, вразливостей і загроз» – як ключового елементу сучасного керування ризиком. У зв’язку з цим увага науковців зосереджується на понятті динамічної оцінки ризиків (DRA). DRA інтерпретується як «безперервний процес виявлення і оцінки ризиків до

функціонування організації в динамічному (майже реальному) часі». Cheimonidis і Rantos провели систематичний огляд на 50 DRA-моделях у кібербезпеці [6], класифікувавши їх за використаними методами аналізу. Вони констатують, що DRA-моделі мають допомагати в оперативному корегуванні заходів захисту у відповідь на актуальні загрози та можуть поєднувати різні джерела інформації з оточення (дані систем запобігання вторгнень, SIEM-систем, показники вразливостей тощо) для регулярного оновлення оцінок ризику. Згідно з висновками Cheimonidis та Rantos, більшість запропонованих DRA-моделей у кібербезпеці базується на методах штучного інтелекту та машинного навчання (зокрема, найчастіше застосовують баєсові мережі). При цьому значна увага приділяється системам критичної інфраструктури (ICS) – саме на них перевірено більшість моделей. Більшість розглянутих моделей є кількісними й оперують реальними даними довкілля: наприклад, вони використовують сигнали систем виявлення вторгнень (IDS) і інформацію про вразливості для обчислення ймовірностей атак та потенційних втрат. Так, Zhang et al. запропонували модель на основі нечітких ймовірностей в Баєсовій мережі для динамічної оцінки ризиків в промислових SCADA-системах [7], а Zhou et al. застосували поєднання Байєсових мереж і нечіткої ієрархічної обробки (FAHP) для моделювання суб'єктивних експертних знань і необхідних механізмів захисту [8]. Інші підходи включають графи атак, які відображають можливі шляхи проникнення (Debneath et al. застосували «байєсовий граф атак» для оцінки ризику в кластерах високопродуктивних обчислень [9]), марковські моделі для прогнозування змін і пріоритетів атак, а також різні методи нечіткої логіки (FAHP та ін.) для обробки невизначеності. Усі ці підходи поєднуються з аналізом поточної топології мережі й даними про наявні контрзаходи, що дозволяє підвищити точність оцінки ризиків.

Важливу роль у формуванні підходів до ризик-менеджменту відіграють міжнародні та галузеві ініціативи. Так, GSMA (асоціація мобільних операторів) розробляє стандарти безпеки мобільних мереж (наприклад, Mobile Threat Intelligence Framework – MoTIF) для класифікації загроз. ENISA у 2022–2023 рр.

представила Interoperable EU Risk Management Framework [10], що уніфікує кроки з оцінки ризиків і сприяє сумісності різних методологій у ЄС. В ITU-T існують рекомендації (наприклад, X.805, X.1205) щодо побудови архітектури безпеки та управління ризиками в телекомунікаціях. Також база знань MITRE ATT&CK надає загальнодоступний опис тактик і технік зловмисників, що широко використовується для побудови моделей загроз. Усі ці підходи підкреслюють необхідність безперервного моніторингу й оновлення оцінок ризику; зокрема, NIST SP 800-137 прямо визначає безперервний моніторинг як життєво важливий крок RMF.

В Україні також виконано низку досліджень у сфері динамічної оцінки ризиків. Наприклад, Палко та Мируценко (2024) наголошують на «обмеженості наявних стандартів і методологій в динамічних умовах сучасних PIC» і акцентують увагу на необхідності застосування гнучких адаптивних рішень [11]. Вони пропонують метрико-орієнтований підхід, що інтегрує нейромережеві моделі оцінки стану інфраструктури та метрики відповідності нормативним стандартам, створюючи масштабовану динамічну систему управління кіберризиками. Також, Палко (2025) відзначає, що традиційні статистичні методи малоефективні при обробці великих об’ємів гетерогенних даних і пропонує інтелектуальну модель на основі глибокої нейронної мережі для підвищення точності оцінки ризиків [12].

Таким чином, вітчизняні та зарубіжні дослідники активно експериментують з нейромережами, нечіткими методами та схемами інтеграції експертних оцінок для оцінки кіберризиків. Загалом, огляд останніх публікацій показує, що сучасні дослідження DRA поєднують AI/ML-підходи (зокрема Байєсові мережі), нечіткі моделі та глибоке навчання. При цьому визнано, що активна інтеграція актуальних даних про кіберзагрози (CTI) у моделі оцінки ризиків є перспективним напрямом. Зокрема, Cheimonidis та Rantos відзначають, що включення даних кіберрозвідки дозволить зробити DRA-системи не тільки реактивними, але й проактивними. Це, зі свого боку, вказує на необхідність подальших досліджень у розробці гнучких, самонавчальних моделей оцінки

ризику, здатних враховувати оновлену інформацію про нові вразливості та тактики атаки.

Мета статті

Метою статті є розробка концептуальної моделі динамічного кількісного аналізу ризиків кібербезпеки для організацій телекомунікаційної галузі. Запропонована модель має на меті підвищення точності оцінки ризиків, оперативності реагування на загрози та загальної кіберстійкості елементів гетерогенних динамічних середовищ.

Виклад основного матеріалу

Запропонована концептуальна модель складається з взаємопов'язаних компонентів, що реалізують повний цикл процесу аналізу ризиків кібербезпеки — від збору даних до візуалізації кількісних результатів. Модель орієнтована на формалізоване представлення сутностей, автоматизацію логічного виведення та прогнозування ризиків, що робить її придатною до масштабування та практичного впровадження в організаціях, що відносяться до критичної інфраструктури.

Структура концептуальної моделі, її компонент та взаємозв’язків (рис.1).

Ядром концептуальної моделі є **онтологічна модель активів, сервісів та послуг** — формалізоване представлення знань про інфраструктуру (активи, сервіси, послуги, відносини між ними, властивості, залежності тощо) та знань щодо загроз, вразливостей та ризиків.

Онтологічна модель формально представлена у вигляді кортежу:

$$O = \langle X, T, R, A, C, M \rangle \quad (1)$$

де:

X - множина концептів (класів), що репрезентують сутності телеком-інфраструктури та аспектів кібербезпеки: активи, сервіси, загрози, вразливості, контрзаходи тощо;

$T \subseteq X \times X$ - ієрархічні відношення між концептами типу “is-a”, які утворюють таксономію понять і забезпечують успадкування властивостей;

$R \subseteq X \times P \times X$ - множина семантичних відношень між концептами, де P -

множина предикатів (типів відношень), що визначають характер семантичного зв'язку між концептами (наприклад, "depends_on", "uses", "exposed_to" тощо);

A - множина атрибутів концептів, що містить їх кількісні та якісні характеристики, які використовуються в логічному виведенні, нечіткій оцінці та ймовірнісному прогнозуванні (наприклад, "CVSS_score", "criticality", "exposure_level", "business_impact", "patching_frequency", "data_sensitivity", "redundancy_level", "attack_type_probability" тощо);

C - множина формальних визначень концептів, що описує структуру їх атрибутів та допустимі значення властивостей, необхідні для валідації, логічного виведення та інтерпретації семантики об'єктів;

M - множина правил логічного й нечіткого виведення, які формалізують залежності між атрибутами концептів на основі правил детермінованої логіки ("IF-THEN") та правил з використанням нечітких термів та функцій приналежності, для автоматичної оцінки станів та рівня ризику активів.

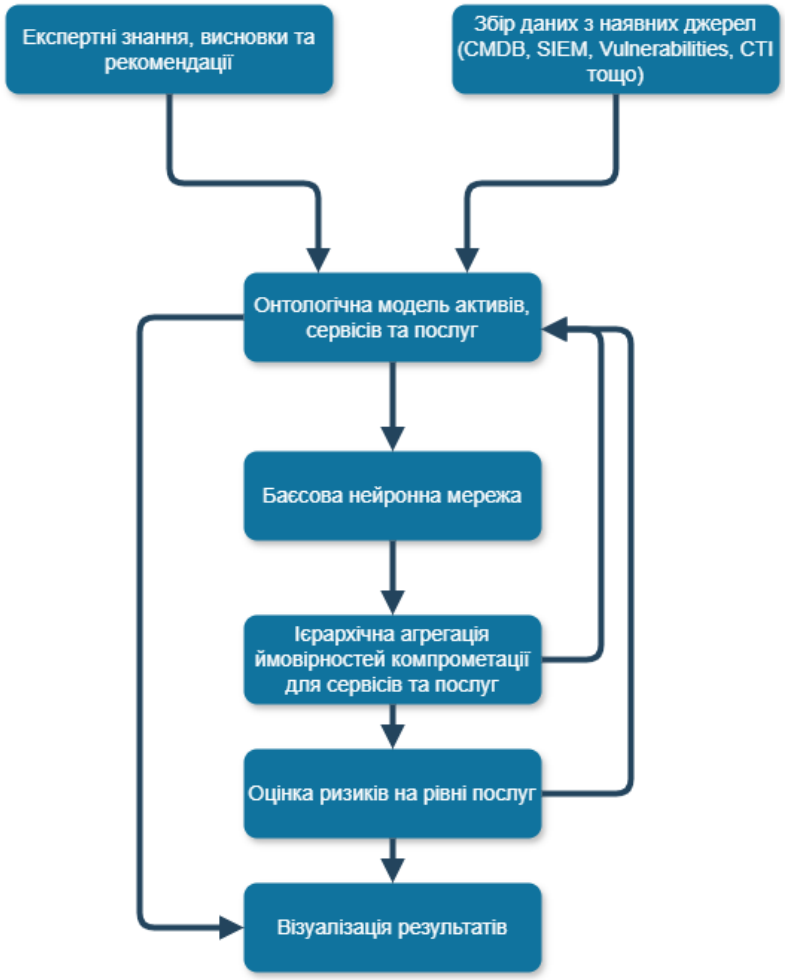

Рисунок 1 - Структура концептуальної моделі

Авторська розробка

Джерелами даних для онтологічної моделі активів, сервісів та послуг є як дані з наявних технічних систем (CMDB, SIEM, Vulnerability Scanners, Threat Intelligence (CTI) тощо), так і експертні знання, висновки та рекомендації (такі як критичність сервісів та послуг з точки зору бізнесу, ієрархія зв'язків між активами, сервісами та послугами, вимоги політик безпеки, тощо). Дані з наявних технічних систем (у структурованому та неструктуровані вигляді) обробляються ETL-процесами (Extract–Transform–Load), що:

1. забепечують автоматизоване вивантаженя даних із наявних технічних систем;

2. трансформують отримані дані (виконують семантичну нормалізацію атрибутів до онтологічної структури, встановлюють відношення між екземплярами концептів тощо);

3. завантажують перетворені дані у необхідному форматі до онтологічної БД.

Експертні знання інтегруються в онтологічну модель (вручну або за допомогою засобів автоматизації (наприклад, з використанням шаблонів та/або великих мовних моделей (LLM)) для:

1. формалізації лінгвістичних оцінок (наприклад, "високий рівень ризику", "частково захищено") у вигляді нечітких множин;

2. опису типових зв'язків та залежностей між об'єктами через предикати (наприклад, depends_on, exposed_to_threat);

3. введення нечітких і класичних правил логічного виведення у відповідну множину правил;

4. наповнення екземплярів концептів в онтологічній БД, включаючи допустимі значення атрибутів, категоризації та експертні граничні значення.

Таким чином, експертна інформація не просто додається як дані, а трансформується у правила логіки, семантичні відношення та структуровані визначення, що дозволяє моделі виводити нові знання, навіть за умов неповноти

технічних даних.

На основі даних в онтологічній моделі для кожного активу формується **вхідний вектор ознак** для подальшого розрахунку ймовірності компрометації активу за допомогою баєсових нейронних мереж (*BNN*):

$$x_i = [CVSS_i,\ PD_i,\ Exps_i, Topo_i, Anom_i, TI_i, Crit_i, Expl_i, Hist_i, Prot_i] \quad (2)$$

де:

$CVSS_i$ – оцінка критичності вразливості (у випадку наявності декількох вразливостей для активу обирається найвища);

PD_i – Patch Delay, проміжок часу між моментом, коли виправлення вразливості стало доступним та моментом застосування цього виправлення на рівні активу;

$Exps_i$ - рівень мережевої експозиції активу (загальнодоступний, доступний тільки всередині контрольованого периметру, додатково захищений внутрішній тощо);

$Topo_i$ - індикатор важливості активу у мережевій ієрархії;

$Anom_i$ - оцінка наявності поведінкових аномалій;

TI_i - індикатор активності загроз щодо активу або пов'язаних вразливостей;

$Crit_i$ - рівень бізнес-критичності активу;

$Expl_i$ – оцінка ймовірності експлуатації вразливості (з загальнодоступної бази EPSS);

$Hist_i$ – кількість зареєстрованих інцидентів по активу за визначений період часу;

$Prot_i$ – агрегований числовий індикатор, що відображає ефективність реалізованих механізмів безпеки для активу, і обчислюється як зважена сума нормалізованого вектору значень контролів безпеки, або через агрегацію за допомогою нечіткої функції належності та правил нечіткого виведення.

Баєсові нейронні мережі (BNN) у запропонованій концептуальній моделі використовуються для ймовірнісного прогнозування компрометації активів на основі багатовимірного вектору ознак, що сформовано на рівні онтологічної

моделі. На рівні концептуальної моделі, BNN за структурою не відрізняється від звичайної нейромережі - її архітектуру (кількість шарів, нейронів) доцільно проєктувати як типовий багатошаровий персептрон (*MLP*) [13]. З огляду на невелику кількість вхідних ознак (до 10), на наш погляд, достатньо двох прихованих шарів для того, щоб забезпечити баланс між точністю, обчислювальною ефективністю та здатністю оцінювати модельну невизначеність - особливо в умовах роботи *BNN* в режимі реального часу або періодичної пакетної обробки. Розмірність прихованих шарів (64 та 32) на етапі проектування концептуальної моделі вбачається як достатня для 10 ознак без перенавчання, при цьому не перевантажує обчислення (оптимально для inference < 1 секунда для батчів розмірністю до 1000 активів).

Для прихованих шарів доцільно використовувати сучасні функції активації на кшталт зрізаного лінійного вузла (*ReLU*) через її не сатуративний характер і здатність пом'якшувати проблему «зникаючого градієнта», що притаманно сигмоїдним чи тангенсовим функціям активації. У вихідному шарі, що продукує ймовірність компрометації, доцільно застосувати логістичну сигмоїду (σ), аби обмежити вихід діапазоном [0,1]. Це дозволить інтерпретувати вихід безпосередньо як ймовірність успішної компрометації.

Для зменшення епістемічної невизначеності BNN доцільно використати підхід Monte Carlo Dropout – випадкове відключення нейронів як під час навчання, так і при прогнозуванні. Оптимальний рівень dropout слід підібрати експериментально, але у якості відправної точки на наш погляд, доцільно обрати значення dropout = 0,2. Під час прогнозування BNN слід залишати в режимі тренування, щоб dropout був активним на кожному прогоні. Це перетворює одну мережу на стохастичний ансамбль моделей, який породжує розподіл результатів. Результуюча ймовірність компрометації оцінюється як середнє значення виходів за кілька прогонів (наприклад, 20), а невизначеність – через дисперсію або довірчий інтервал (наприклад, 95%).

Архітектура запропонованої BNN (рис.2).

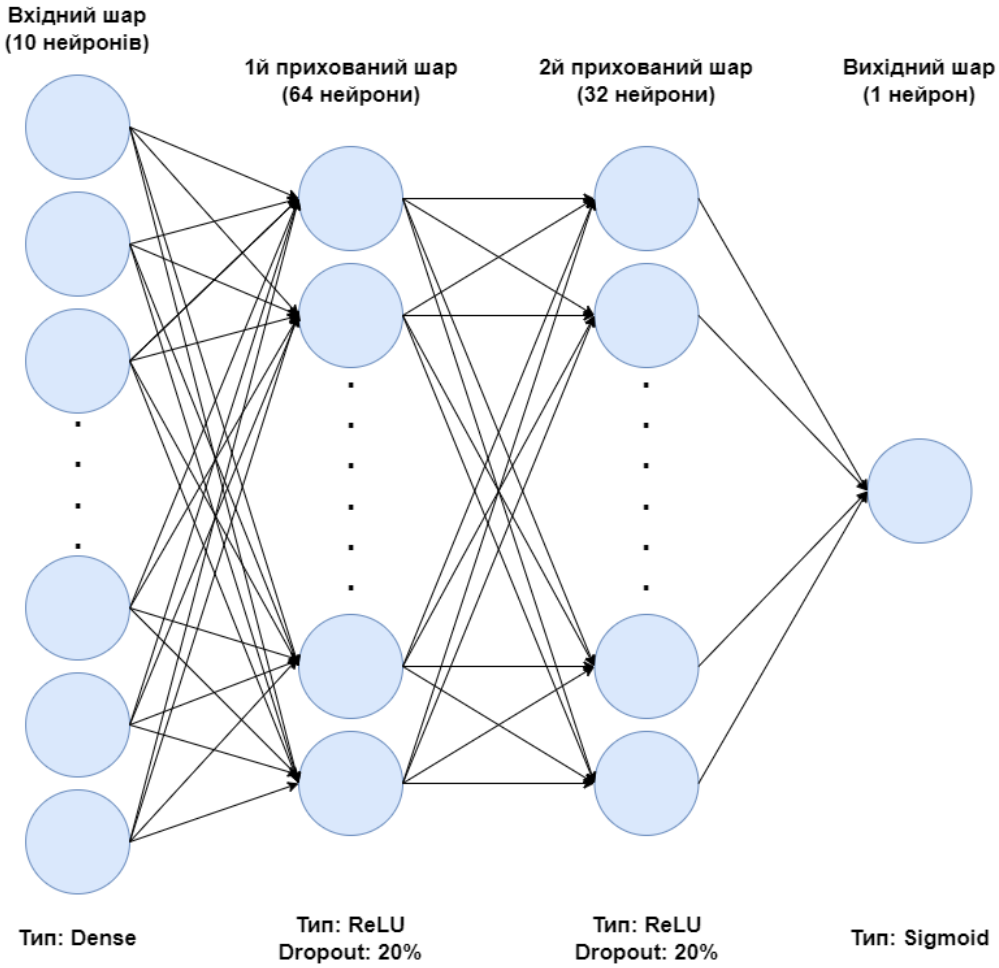

Рисунок 2 - Архітектура запропонованої BNN

Авторська розробка

Запропоновану BNN на рівні концептуального підходу вважається доцільним реалізувати згідно з наступним алгоритмом:

1. Формується вектор ознак $X_i = \{x_{i1}, x_{i2}, \ldots, x_{in}\}$, де x_{ij} – значення j-ї ознаки для кожного активу на основі даних з онтологічної моделі.

2. Параметри моделі (ваги) визначаються за допомогою апріорного нормального розподілу: $\Theta \sim N(\mu, \sigma^2)$, де $\mu = 0, \sigma^2 = 1$.

3. Навчання BNN виконується за допомогою алгоритму стохастичного градієнтного спуску (SGD). Регуляризація забезпечує відповідність параметрів моделі заданому апріорному розподілу $p(\Theta)$. Використовується метод Monte Carlo Dropout для оцінки невизначеності із значенням dropout = 0,2. В результаті навчання BNN моделі отримуємо апостеріорний розподіл параметрів $p(\Theta|X, Y)$, який використовується для отримання ансамблю передбачень на наступному

етапі.

4. На етапі прогнозування для кожного активу виконується N проходів моделі з активованим dropout (наприклад, $N = 20$): $\hat{Y}_i^{(j)} BNN(X_i, \Theta_j), j = 1, \dots, N$.

Отримані результати являють собою вибірку з апостеріорного розподілу ймовірностей компрометації активу,

5. В результаті, ймовірність компрометації активу визначається як середнє значення прогнозів:

$$P_{BNN}(i) = \frac{1}{N}\sum_{j=1}^{N} \hat{Y}_i^{(j)} \quad (3)$$

Невизначеність оцінюється через стандартне відхилення прогнозів:

$$\sigma_{BNN}(i) = \sqrt{\frac{1}{N-1}\sum_{j=1}^{N}\left(\hat{Y}_i^{(j)} P_{BNN}(i)\right)^2} \quad (4)$$

Довірчий інтервал визначається як:

$$CI_{BNN}(i) = P_{BNN}(i) \pm z\frac{\sigma_{BNN}(i)}{\sqrt{N}} \quad (5)$$

де $z = 1{,}96$, що відповідає 95%-му довірчому інтервалу для стандартного нормального розподілу $\mathcal{N}(0,1)$.

На наступному етапі виконується **ієрархічна агрегація ймовірностей компрометації від рівня активів до рівня сервісів і далі до рівня послуг**, з урахуванням невизначеності, заданої через стандартне відхилення та довірчі інтервали. Ієрархія включає:

1. Активи (a_i): базові елементи інфраструктури, для яких розраховані ймовірність компрометації μ_i; $\mu_i = P_{BNN(i)}$, стандартне відхилення σ_i; $\sigma_i = \sigma_{BNN(i)}$ та довірчій інтервал.

2. Сервіси (s_j): одна чи більше інформаційних систем, що складаються з набору активів і мають категорію бізнес-критичності (наприклад, «Mission Critical», «Business Critical», «Operational», «Office Productivity») та надають певну внутрішню послугу (наприклад, транспортна мережа, AAA для FTTB, міжмережеві екрани тощо).

3. Послуги (o_k): кінцеві продукти для споживачів, що реалізуються одним

чи більше сервісами, і мають власну категорію бізнес-критичності, яка відображає пріоритет відновлення.

Для агрегації ймовірностей компрометації та врахування невизначеності на рівні сервісів та послуг запропоноване використання Монте-Карло симуляції з моделюванням ймовірностей компрометації активів через бета-розподіл. Бета-розподіл дозволить опосередковано врахувати довірчі інтервали активів, моделюючи повний розподіл ймовірностей на основі μ_i та σ_i. Бізнес-критичність сервісів використовується як зважений коефіцієнт у процесі агрегації на рівні послуг, що дозволяє врахувати їхню відносну важливість для функціонування послуги. Структура ієрархії та відношень між активами, сервісами та послугами отримуються з онтологічної моделі.

Ймовірність компрометації активу a_i моделюється як випадкова величина P_i, що підкоряється бета-розподілу: $P_i \sim B(\alpha_i, \beta_i)$, де параметри α_i та β_i визначаються на основі середньої ймовірності μ_i, та стандартного відхилення σ_i, отриманих з BNN:

$$\alpha_i = \mu_i \left(\frac{\mu_i(1-\mu_i)}{\sigma_i^2} - 1 \right) \quad (6)$$

$$\beta_i = (1-\mu_i) \left(\frac{\mu_i(1-\mu_i)}{\sigma_i^2} - 1 \right) \quad (7)$$

При цьому, використовується умова $\sigma_i^2 < \mu_i(1-\mu_i)$, для забезпечення додатних значень параметрів α_i та β_i. Бета-розподіл моделює повний розподіл ймовірностей, включаючи невизначеність, задану довірчим інтервалом $[\mu_i - 1{,}96 \cdot \sigma_i, \mu_i + 1{,}96 \cdot \sigma_i]$, який обчислюється аналітично на основі середньої ймовірності μ_i, та стандартного відхилення σ_i, отриманих з BNN, і відповідає 95% рівню довіри для нормального розподілу. Для подальших етапів (на рівні сервісів та послуг), де застосовуються Монте-Карло симуляції, використовується 95% довірчий інтервал ([2,5-й перцентиль, 97,5-й перцентиль] вибірок), що забезпечує емпіричну оцінку невизначеності з урахуванням складних агрегацій. При цьому, кількість ітерацій Монте-Карло симуляцій (T), що визначає точність статистичних оцінок, обирається залежно від необхідної точності з можливістю емпіричної перевірки стабільності результатів при збільшенні T.

Далі виконується **агрегація ймовірностей компрометації на рівні сервісів**. Ймовірність компрометації сервісу s_j визначається як ймовірність того, що хоча б один із його активів $a_j \in A_j$, (A_j – множина активів a_j з онтологічної моделі, що реалізують сервіс s_j) матиме ненульову ймовірність компрометації. За припущенням незалежності подій компрометації активів, ймовірність компрометації сервісу визначається як:

$$P_{s_j} = w_j\left(1 - \prod_{a_i}(1 - P_i)\right) \quad (8)$$

де: w_j - коефіцієнт бізнес-критичності сервісу s_j, що визначається методом експертних оцінок, та відображає привабливість сервісу для кібератак, та встановлюється на рівні онтологічної моделі. Значення w_j (таблиця 1):

Таблиця 1 - Відповідність значень w_j рівням бізнес-критичності сервісів

Рівень бізнес-критичності	**Значення w_j**
Mission Critical	1,0
Core IT	0,8
Business Critical	0,6
Business Operational	0,4
Office Productivity	0,2

Авторська розробка

Таким чином, на рівні концептуального підходу, алгоритм обчислення ймовірностей компрометації для сервісів з урахуванням невизначеності P_i виглядає наступним чином:

1. Для кожного активу a_i генеруються вибірки із заданою кількістю ітерацій T:

$$P_i^{(t)} \sim B(\alpha_i, \beta_i), t = 1,2, \dots, T \quad (9)$$

2. Для кожного сервісу s_j та кожної ітерації t обчислюється ймовірність компрометації:

$$P_{s_j}^{(t)} = w_j\left(1 - \prod_{a_i}\left(1 - P_i^{(t)}\right)\right) \quad (10)$$

3. Для кожного сервісу s_j обчислюється середнє значення ймовірності

компрометації $\hat{P}_{s_j}$ та стандартне відхилення $\hat{\sigma}_{s_j}$:

$$\hat{P}_{s_j} = \frac{1}{T}\sum_{t=1}^{T} P_{s_j}^{(t)} \quad (11)$$

$$\hat{\sigma}_{s_j} = \sqrt{\frac{1}{T-1}\sum_{t=1}^{T}\left(P_{s_j}^{(t)} - \hat{P}_{s_j}\right)^2} \quad (12)$$

На наступному кроці виконується **агрегація ймовірностей компрометації на рівні послуг.** Для цього використовується такий же алгоритм, як й на попередньому етапі, але без використання коефіцієнту бізнес-критичності, оскільки бізнес-критичність сервісів w_j вже врахована в P_{s_j}, а на рівні послуг бізнес-критичність впливає на оцінку наслідків, а не на ймовірність компрометації, тому її доцільно враховувати на етапі оцінки ризиків. Відповідно, для кожної послуги ймовірність компрометації визначається як:

$$P_{o_k}^{(t)} = 1 - \prod_{s_j \in S_k}\left(1 - P_{s_j}^{(t)}\right) \quad (13)$$

де: $P_{s_j}^{(t)}$ – вибірки з попереднього етапу, S_k – множина сервісів, що реалізують послугу o_k.

Для кожної послуги o_k обчислюється середнє значення ймовірності компрометації $\hat{P}_{o_k}$ та стандартне відхилення $\hat{\sigma}_{o_k}$:

$$\hat{P}_{o_k} = \frac{1}{T}\sum_{t=1}^{T} P_{o_k}^{(t)} \quad (14)$$

$$\hat{\sigma}_{s_j} = \sqrt{\frac{1}{T-1}\sum_{t=1}^{T}\left(P_{o_k}^{(t)} - \hat{P}_{o_k}\right)^2} \quad (15)$$

На останньому етапі виконується **оцінка ризику для послуги o_k** з урахуванням можливих порушень доступності послуги, а також конфіденційності та цілісності даних в контексті послуги, базуючись на загальній ймовірності компрометації $\hat{P}_{o_k}$. Для кожної послуги обчислюються два показники: кількісний (монетарний ризик) і якісний (пріоритет відновлення).

Розрахунок монетарного ризику виконується по формулі:

$$R_{o_k} = \hat{P}_{o_k} \times C \quad (16)$$

де C – значення максимально можливого збитку від компрометації послуги за певний період часу. При цьому:

- У випадку, якщо компрометація послуги впливає на її доступність для кінцевих абонентів, то значення C є прибутком від кожної послуги на певний період часу.
- У випадку, якщо компрометація послуги впливає на конфіденційність та/чи цілісність даних організації та її абонентів послуг, то значення C доцільно заздалегідь оцінювати на основі історичних даних, за допомогою сценарного аналізу та/або методом експертних оцінок.

Розрахунок пріоритету відновлення виконується по формулі:

$$PI_{o_k} = v_k \cdot \hat{P}_{o_k} \quad (17)$$

де v_k – коефіцієнт бізнес-критичності послуги (таблиця 2):

Таблиця 2 - Відповідність значень v_k рівням бізнес-критичності послуг

Рівень бізнес-критичності послуги	**Значення v_k**
Mission Critical	1,0
Core IT	0,8
Business Critical	0,6
Business Operational	0,4
Office Productivity	0,2

Авторська розробка

Відповідно до розрахованого значення пріоритету відновлення, можна побудувати шкалу пріоритезації для визначення подальших дій (таблиця 3):

Таблиця 3 - Приклад шкали пріоритезації дій

Рівень пріоритету	**Діапазон значень PI_{o_k}**	**Дії**
Критичний	$0{,}75 \leq PI_{o_k} \leq 1$	Негайна активізація Плану Відновлення для подій Критичного рівня.
Високий	$0{,}5 \leq PI_{o_k} < 0{,}75$	Негайний детальний аналіз подій та причин, активізація Плану Відновлення для подій Високого рівня.
Середній	$0{,}25 \leq PI_{o_k} < 0{,}5$	Запланований детальний аналіз подій та причин, активізація Плану Відновлення для подій Середнього рівня.
Низький	$0, < PI_{o_k} < 0{,}25$	Моніторинг стану та запланований аналіз подій, планування дій по відновленню.

Авторська розробка

На фінальному етапі результати оцінки ризиків, отримані на рівні послуг, а також дані з онтологічної моделі (ієрархії активів, сервісів, послуг, значень атрибутів і правил тощо) представляються у зрозумілій та інтерактивній візуальній формі з метою аналізу результатів та підтримки прийняття рішень. Модуль візуалізації також надає можливість внесення змін до онтологічної моделі шляхом редагування концептів та відношень між ними, редагування значень атрибутів та правил логічного виведення.

Висновки та подальші напрямки досліджень

У роботі розглянуто одну з можливих постановок задачі динамічного аналізу ризиків, що виникає в сучасних організаціях телекомунікаційної галузі. Розроблено концептуальну модель, яка описує процес динамічного кількісного аналізу ризиків кібербезпеки з урахуванням невизначеності та неповноти інформації про стан активів. З метою вдосконалення методів управління кіберризиками в умовах динамічного ландшафту складних загроз запропоновано інтегрований підхід, що забезпечує оперативну оцінку та прогнозування ймовірностей компрометації активів, сервісів і послуг. Особливості моделі включають використання онтологічних структур для інтеграції технічних і експертних знань, що дозволяє враховувати динаміку змін і забезпечувати комплексність аналізу. Запропоновано застосування баєсових нейронних мереж (BNN) для оцінки ймовірності компрометації активів із врахуванням модельної невизначеності, а також запропоновано використання методу Монте-Карло для агрегації ймовірностей компрометації на рівні сервісів та послуг. Додатково запропоновано використання засобів візуалізації, що підтримують прийняття рішень у реальному часі.

Показано, що запропонований підхід дає змогу реалізувати стратегію проактивного управління кіберризиками, враховуючи як поточний стан активів, так і еволюцію загроз.

Практична цінність моделі полягає в її здатності до безперервного аналізу в режимі реальному часі, що є критично важливим для телекомунікаційних екосистем. Наукова новизна роботи полягає в інтеграції онтологічних моделей

представлення знань, BNN і методу Монте-Карло, що реалізують підхід до динамічного кількісного аналізу ризиків кібербезпеки.

Подальші напрямки досліджень передбачають:

1. Дослідження методів виявлення нових і прихованих знань в онтологічній моделі: аналіз можливостей застосування алгоритмів логічного виведення, графового аналізу та машинного навчання для виявлення неявних залежностей і вразливостей у телекомунікаційних екосистемах, що сприятиме підвищенню точності оцінки ризиків.

2. Оптимізація багатошарової архітектури баєсових нейронних мереж (BNN): дослідження впливу глибини архітектури та методів регуляризації на ефективність навчання BNN, зокрема задачі мінімізації проблеми зворотнього поширення помилки, для забезпечення стабільності прогнозування ймовірностей компрометації активів.

3. Практичну валідацію концептуальної моделі на прикладах реальних телекомунікаційних послуг.

Література:

1. EY Top-10 Risks in Telecommunications: Evolving sector considerations for 2025. URL: https://www.ey.com/content/dam/ey-unified-site/ey-com/fr-fr/insights/telecommunications/documents/ey-gl-top-10-risks-in-telecommunications-01-2025.pdf (дата звернення: 20.05.2025).

2. ENISA Cybersecurity of Critical Sectors: Telecom Sector and Digital Infrastructure. URL: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/telecom-sector-and-digital-infrastructure (дата звернення: 20.05.2025).

3. 2024 United States telecommunications hack. URL: https://en.wikipedia.org/wiki/2024_United_States_telecommunications_hack (дата звернення: 20.05.2025).

4. Orange Hack Reveals Telecom Cybersecurity Flaws. URL: https://cybermagazine.com/cyber-security/orange-breach-exposes-critical-telecom-security-gaps (дата звернення: 20.05.2025).

5. Understanding ISO 27005: A Guide to Risk Management in Cybersecurity. URL: https://isecjobs.com/insights/iso-27005-explained/#:~:text=controls,and%20methodologies%20in%20Risk%20management (дата звернення: 20.05.2025).

6. Cheimonidis, P., & Rantos, K. (2023). Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review. Future Internet, 15(10), 324. https://doi.org/10.3390/fi15100324.

7. Zhang, Q.; Zhou, C.; Xiong, N.; Qin, Y.; Li, X.; Huang, S. Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems. IEEE Trans. Syst. Man Cybern. Syst. 2016, 46, 1429–1444.

8. Zhou, B.; Sun, B.; Zang, T.; Cai, Y.; Wu, J.; Luo, H. Security Risk Assessment Approach for Distribution Network Cyber Physical Systems Considering Cyber Attack Vulnerabilities. Entropy 2022, 25, 47.

9. Debnath, J.K.; Xie, D. CVSS-based Vulnerability and Risk Assessment for High Performance Computing Networks. In Proceedings of the 2022 IEEE International Systems Conference (SysCon), Montreal, QC, Canada, 25–28 April 2022; pp. 1–8.

10. ENISA Interoperable EU Risk Management Framework. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report-Interoperable%20EU%20Risk%20Management%20Framework_Updated.pdf (дата звернення: 20.05.2025).

11. Палко, Д., & Мирутенко, Л. (2024). МЕТОД КОМПЛЕКСНОЇ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 487–502. https://doi.org/10.28925/2663-4023.2024.26.731

12. Палко, Д. (2025). ІНТЕЛЕКТУАЛЬНІ МОДЕЛІ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В РОЗПОДІЛЕНИХ СИСТЕМАХ НА ОСНОВІ НЕЙРОМЕРЕЖЕВОГО ПІДХОДУ. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(27), 429–448. https://doi.org/10.28925/2663-4023.2025.27.764

13. Talpini, J., Sartori, F. & Savi, M. Enhancing trustworthiness in ML-based network intrusion detection with uncertainty quantification. J Reliable Intell Environ 10, 501–520 (2024). https://doi.org/10.1007/s40860-024-00238-8.

Abstract. *This article is dedicated to the development of a conceptual model for dynamic quantitative cybersecurity risk analysis in telecommunication digital ecosystems. The goal of the proposed model is to enhance the accuracy of risk assessment and the responsiveness to cyber threats in the context of a rapidly evolving threat landscape and asset state uncertainty. The method is based on the integration of ontological models, Bayesian Neural Networks (BNNs), and the Monte Carlo method. The ontological model formalizes knowledge about assets, services, and offerings, while the BNN enables probabilistic forecasting of compromise considering uncertainty. The Monte Carlo method is applied to aggregate probabilities across hierarchical layers of services and offerings. The results include the developed conceptual model that implements continuous real-time risk analysis, monetary risk calculation, and recovery prioritization for telecommunication services, as well as interactive result visualization. It is demonstrated that the conceptual model has the potential to overcome limitations of traditional approaches, such as inertia and insufficient consideration of dynamic interdependencies. Future research directions include the expansion of the ontological model, optimization of the BNN, and validation of the theoretical framework using telecommunication service case studies.*

Keywords: *Cybersecurity, telecommunication ecosystems, dynamic risk analysis, ontological model, Bayesian Neural Networks, Monte Carlo simulation.*

Науковий керівник: д.т.н., проф. Семко В.В.

Стаття відправлена: 30.05.2025 р.