https://doi.org/10.31891/2219-9365-2024-77-44
УДК 004.94

САКОВИЧ Богдан
Херсонський національний технічний університет
https://orcid.org/0000-0002-8863-0343
ЖАРІКОВА Марина
Херсонський національний технічний університет
https://orcid.org/0000-0001-6144-480X

ІМОВІРНІСНА ГРАФІЧНА МОДЕЛЬ ДЛЯ ОЦІНКИ РИЗИКІВ ПОШКОДЖЕННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ВІД РУЙНІВНИХ ПРОЦЕСІВ

У цій роботі запропоновано сучасний підхід до моделювання руйнівних процесів на основі байєсівських мереж для оцінки об'єктів критичної інфраструктури з множинними ризиками, з акцентом на руйнівні процеси, такі як бомбардування та кіберзагрози.Модель класифікує ризики на два рівні: низький і високий, і використовує ці класифікації для прогнозування потенційної шкоди інфраструктурі.

Ключові слова: модель, Баєсова мережа, об'єкти критичної інфраструктури, спрямований ациклічний граф, спрямована графічна модель, руйнівний процес, ризик, загроза.

SAKOVYCH Bohdan, ZHARIKOVA Maryna
Kherson National Technical University

PROBABILISTIC GRAPHICAL MODEL FOR ASSESSING THE RISKS OF DAMAGE TO CRITICAL INFRASTRUCTURE FACILITIES FROM DESTRUCTIVE PROCESSES

In this work, the process of modelling the destructive processes, risk of their emerging, and damage probability was described. The modelling displayed a method to assess the risk of damage to critical infrastructure facilities. The destructive processes were independent but may be simultaneous, which is crucial to take into account while modelling. This paper presents a novel Bayesian network approach for assessing multi-risk critical infrastructure, focusing on the risks posed by bombardment and cyber threats. The model classifies risks into two levels: low and high, and uses these classifications to predict potential infrastructure damage. The Bayesian network is constructed with four nodes representing bombardment (B), cyber-threats (C), and damage (D) to infrastructure (I). This study presents a comprehensive risk analysis model for crisis management, which covers pre-crisis, response, and post-crisis stages, evaluating risk distinctly in each. The model hypothesises that risk fluctuates based on multi-hazard processes and can be evaluated for each vulnerable object. Risk dimensions include the probability of threat, target attributes, and accessibility to threat-creating actors. A multi-hazard risk assessment is represented as a combination of these components, providing a dynamic risk rating for each entity. This aids in informed decision-making throughout the crisis management cycle and allows for a comprehensive understanding of the system's risk profile, taking into account the complex interplay of different risk factors. It provides a robust framework for risk assessment in complex systems and offers valuable insights for decision-makers in critical infrastructure protection, enabling them to make informed decisions about resource allocation, risk mitigation strategies, and emergency response planning.

Keywords: model, Bayesian network, critical infrastructure, directed acyclic graph, directed graphical model, destructive process, risk, threat.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

З моменту повномасштабного вторгнення російських військ в Україну численні будівлі, мости, залізниці, дамби та інші об'єкти критичної інфраструктури зазнали численних ризиків, пошкоджень і руйнувань, не кажучи вже про жахливі наслідки, такі як жертви, руйнування, невизначеність і біженці. Від самого початку вторгнення війська почали сіяти хаос і руйнування, посягаючи не лише на військові об'єкти, а й на житлові райони, торгові центри, заправки та об'єкти критичної інфраструктури [1]. Триваюча війна також загострює екологічні та природоохоронні проблеми, такі як глобальне потепління, засуха, численні лісові та степові пожежі, забруднення річок та озер, і навіть створює серйозну загрозу захворювань через антисанітарію та сміття, що призводить до жахливих наслідків. Більше того, існують не лише фізичні руйнівні процеси, а й «віртуальні». Так, чимало об'єктів критичної інфраструктури піддаються атакам хакерів і шахраїв, які прагнуть порушити цілісність системи та знеструмити цілі регіони і міста. Цифрові або кіберзагрози представляють собою тип, коли зловмисник поєднує два або більше способів вчинення кіберзлочину [2, 3].

Усі вищезазначені процеси становлять значну частину глобального масштабу. Як правило, вони зосереджені на підриві обороноздатності та цілісності країни. До слова, Європейський Союз розробляє визначені методи оцінки ризиків, щоб належним чином інформувати відповідні сили та представників про

ризики, що виникають у зв'язку з цими загрозами. Мета полягає в тому, щоб оцінити ступінь ризику різноманітних загроз і передати їх до систем раннього попередження і механізмів оцінки ризиків. Ці загрози можуть бути одночасними і різними, наприклад, бомбардування, кіберзагрози та обстріли (Рис.1).

Рис. 1. Взаємозв'язок руйнівних процесів та їхніх наслідків

Вони вважаються руйнівними процесами, оскільки руйнують як критично важливу, так і цивільну інфраструктуру [4, 5, 6]. З цієї причини дуже важливо передбачати ризики та упереджувати майбутні загрози шляхом запобігання, пом'якшення наслідків та забезпечення готовності до них аж до етапу реагування на надзвичайні ситуації та створенні планів щодо відновлення об'єктів. Однак, коли існує ризик виникнення руйнівних процесів, це може призвести до численних взаємозв'язків останніх, які спричиняють та доповнюють одне одного, що називається ефектом доміно, або каскадним ефектом, і пояснюється різними вченими. Наступний розділ присвячений аналізу відповідних досліджень.

Аналіз досліджень та публікацій

Оцінкою та аналізом мультиризиків займаються багато вчених, і наші вітчизняні дослідники також виконали певні дослідження. Так, у статті [3] висвітлено проблему аналізу та управління ризиками, пов'язаними з множинними небезпеками. У цій роботі автори визначають деякі прогалини в існуючих дослідницьких проектах зі зниження ризику руйнівних процесів. Вони використали абсолютно новий підхід до аналізу ризиків, який розглядає всі компоненти ризиків з просторовою прив'язкою. Ризик представлений у вигляді наступних компонентів: характеристики небезпеки (небезпека, інтенсивність, площа, на яку впливає небезпека), характеристики вразливого об'єкта (місцезнаходження, вразливість і швидкість відновлення), а також просторово-часова загроза, що вимірюється часом, необхідним для того, щоб небезпека досягла об'єкта. Пропонується представити ризик небезпеки в динаміці як такий, що проходить наступні три стадії: потенційний ризик, ризик загрози та руйнування, відповідно. Індивідуальний ризик представляється у вигляді траєкторії в *n*-вимірному просторі його параметрів, а множинний ризик оцінюється за допомогою операції взяття максимуму. Запропонований підхід до аналізу ризиків дозволяє діагностувати ситуацію та приймати рішення протягом усього циклу управління ризиками, а також на стадії раннього попередження та реагування.

У дослідженні [4] представлено подієво-орієнтовану просторово-розподілену динамічну модель мультизагрозливого ризику для об'єктів критичної інфраструктури. Модель базується на трирівневій просторовій моделі, а також динамічних моделях соціально-економічної системи, вразливості та подієвій сценарній моделі небезпечного процесу, що ґрунтується на використанні кейс-підходу для накопичення та зберігання сценаріїв динаміки різних небезпек та мультинебезпек, їх комбінацій та ланцюжків. Кожен випадок може бути представлений як послідовність подій, занурених у певний контекст, де кожна подія може ініціювати сценарії, що описують динаміку мультинебезпеки. Автори стверджують, що ризик для певного об'єкта в певний момент часу є комбінацією стану об'єкта (i), загрози (ii), вразливості об'єкта (iii) та потенційної шкоди (iv).

У роботі [5] зазначається, що загрози для критичної інфраструктури можна розділити на три категорії: природні загрози (i), антропогенні (ii) та технічні (iii). Природні загрози, як правило, включають

погодні проблеми, а також геологічні небезпеки, такі як землетруси, цунамі, зсуви ґрунту та виверження вулканів. Вони можуть суттєво вплинути на ОКІ, особливо на транспортний сектор.

Автори роботи [13] оцінили множинні ризики глобальної портової інфраструктури на рівні активів у світлі численних небезпек, кількісно оцінивши ризики пошкодження фізичних активів і логістичних послуг (портовий ризик) та ризики для морських торговельних потоків (торговельний ризик). Дослідники виявили, що майже 86% усіх портів піддаються впливу більш ніж трьох небезпек. Таким чином, автори визначили кілька проблем, які перешкоджають розширенню детального аналізу ризиків до глобального масштабу. По-перше, порти можуть постраждати від кількох різних небезпек, які впливають на інфраструктуру та роботу порту, що ускладнює аналіз ризиків. Окрім впливу на самі портові активи (крани, термінали), порти вбудовані в локальні мережі критичної інфраструктури, такі як залізниця, дороги, а пошкодження електрики може зупинити роботу порту, навіть якщо сам порт не постраждав. Крім того, в роботі [14] автори провели дослідження, в якому інформація про небезпеку може сприяти ефективному реагуванню громадськості і, як наслідок, зменшенню травм і смертельних випадків шляхом складання рекомендацій щодо розробки дієвих і зрозумілих попереджувальних повідомлень про різні види небезпеки. Автори розробили різноманітні огляди та повідомлення про небезпеку, які були визначені під час п'яти віртуальних семінарів, проведених із експертами з різних галузей, а також опитування громадськості, щоб перевірити, чи підвищують наші розробки наміри людей діяти і чи допомагають їм правильно інтерпретувати подану інформацію. На противагу цьому, огляди небезпек із зазначенням часу та дій значно покращили розуміння людьми того, чи варто їм вживати негайних заходів. Більше того, додавання піктограми із зазначенням часу та дій до повідомлення про небезпеку значно підвищувало намір людей вжити заходів. Як у випадку з оглядами небезпеки, так і з повідомленнями, було виявлено, що намір людей діяти пропорційний серйозності та терміновості небезпеки, а також залежить від різних особистих факторів, таких як минулий досвід зіткнення з небезпекою. Отже, надання інформації на платформах, що відображають різні види небезпек, більш придатної для вжиття заходів, може спонукати громадськість до реагування і, в свою чергу, підвищити стійкість суспільства до катастроф. У роботі [15] пропонується трирівнева система оцінки мультиризиків, яка враховує можливі взаємодії між загрозами і ризиками. Перший рівень являє собою блок-схему, яка допомагає користувачам визначити, чи потрібен підхід, що враховує множинні загрози та ризики. Другий рівень - це напівкількісний підхід, який дозволяє визначити, чи потрібна більш детальна кількісна оцінка. Зрештою, третій рівень включає детальний кількісний аналіз множинних ризиків на основі баєсівських мереж.

Моделювання руйнівних процесів та оцінка ризиків

Існує низка методів, що відображають взаємодію та взаємозв'язок між небезпеками. Класифікація - це частина аналізу даних і розпізнавання образів, яка вимагає присвоєння класу описаним екземплярам за набором атрибутів і може бути реалізована різними способами, починаючи від дерев рішень, графів, списків, нейронних мереж, випадкових лісів і закінчуючи *k*-найближчими класифікаторами. Одним із найефективніших класифікаторів, у тому сенсі, що його прогностичні характеристики є конкурентоспроможними з найсучаснішими класифікаторами, є так званий «наївний баєсівський класифікатор», який навчається на основі навчальних даних, умовної ймовірності кожного атрибуту A_i з міткою класу C. Класифікація потім виконується шляхом застосування правила Баєса для обчислення ймовірності конкретного примірника C $A_1, \ldots, A_n$, а потім прогнозування класу з найвищою апостеріорною ймовірністю. Це обчислення стає можливим завдяки припущенню про сильну незалежність: всі атрибути Ai є безумовно незалежними за значенням класу C [7, 8].

Іншим баєсівським класифікатором є баєсівська мережа (БМ) або спрямована графічна модель (СГМ), що представляє собою спільний розподіл ймовірностей набору випадкових величин з можливими причинно-наслідковими зв'язками. Мережа складається з вузлів, що представляють випадкові величини, ребер між парами вузлів, що представляють причинно-наслідкові зв'язки, і умовного розподілу ймовірностей у кожному вузлі. Основною метою методу є моделювання апостеріорного умовного розподілу ймовірностей змінної після спостереження нових даних. Баєсівські мережі можуть бути побудовані або вручну зі знанням базової предметної області, або автоматично з великого набору даних за допомогою, наприклад, бібліотек Python.

Баєсівські мережі [16-19] широко використовуються для представлення причинно-наслідкових зв'язків між небезпеками. Це статистичні моделі (імовірнісні графічні моделі), які використовують теорему Баєса для обчислення умовної ймовірності, пов'язаної з настанням події. БМ можна використовувати в будь-якій сфері, де необхідно моделювати невизначену реальність за допомогою ймовірностей, наприклад, в управлінні ризиками, страхуванні, прогнозуванні, моделюванні різних систем тощо [7, 8]. Однією з них є моніторинг та оповіщення про небезпеки та загрози за допомогою камер або датчиків, де дані з різних джерел можуть бути інтегровані, щоб отримати інтерпретацію отриманих даних. Наприклад, об'єднати дані з різних датчиків, кутів і роздільної здатності, щоб визначити, що відбувається на сцені, або ж промислові

датчики можуть повідомляти про стан машини, і повна картина з'являється лише тоді, коли всі виміряні значення об'єднані. Часто проблеми об'єднання датчиків мають справу з різною часовою або просторовою роздільною здатністю і вирішують «проблему відповідності», тобто визначають, які події з одного датчика відповідають тим самим подіям, про які повідомляють інші датчики. БМ досить стійкі до пропущених даних, тому вони переплітають інформацію, що означає, що кожен датчик має нескінченний шанс надати правильне зображення, отже, об'єднання шансів усіх датчиків зазвичай збільшує ймовірність правильної інтерпретації.

Традиційна баєсівська мережа [16-19] складається з набору змінних, умовні залежності яких представлені спрямованим ациклічним графом (САГ), що записується у вигляді $G = [V, D]$, що супроводжується набором таблиць умовних ймовірностей (ТУІ). САГ - це тип орієнтованого графа без спрямованих циклів, де цикл - це набір спрямованих ребер, що починається з вершини $v \in V$, і якщо слідувати за стрілками в їхньому напрямку, то врешті-решт можна повернутися до початкової вершини.

У БМ кожна вершина на орієнтованому графі відповідає випадковій величині, а кожне ребро означає статистичну залежність. Крім того, кожна вершина пов'язана з умовним розподілом ймовірностей відповідних випадкових величин, який залежить від її батьків у графі. Таким чином, якщо в графі G існує спрямоване ребро з вершини a до вершини b, то вершина a є батьком вершини b [16-19].

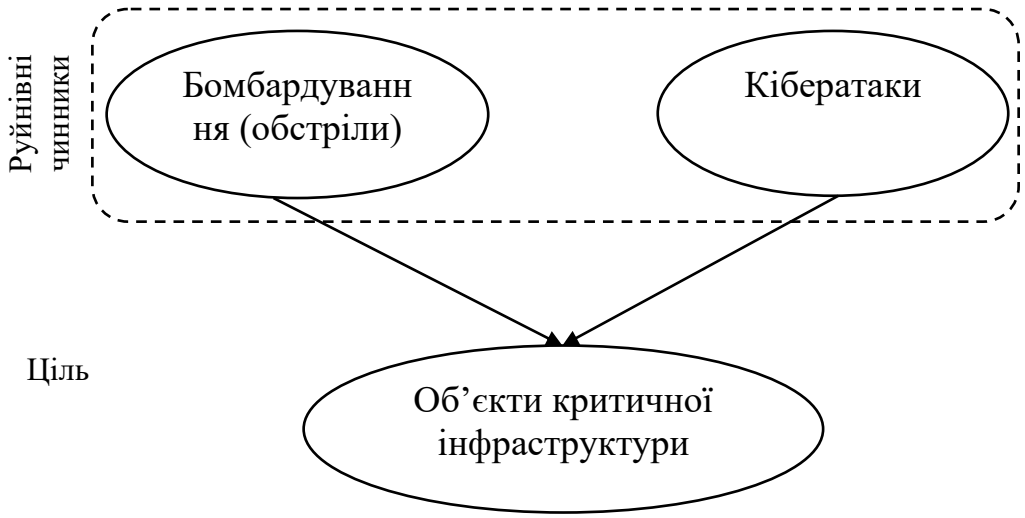

Рис. 2. Ймовірнісна модель із двома руйнівними процесами, що призводять до пошкодження об’єктів критичної інфраструктури

Два чинника в цьому прикладі вважаються незалежними, тобто між двома вершинами немає межі, але це припущення не є обов'язковим для загального випадку. Якщо в графі немає вузла, баєсівські мережі можуть відобразити стільки причинно-наслідкових зв'язків, скільки потрібно для точного опису реальної ситуації. Оскільки граф є ієрархічною структурою, використовуються такі терміни, як «батько», «нащадок» або просто конкретні вузли. Ймовірність випадкової величини графа залежить від його батьківських вершин:

$$P(A_1, \dots, A_x) = \prod_{i=1}^{x} P(A_i | Par(A_i))$$

Концепція БМ [16-19] побудована на теоремі Баєса [16, 17], яка допомагає виразити умовний розподіл ймовірності причини за даними спостережень за допомогою оберненої умовної ймовірності спостережуваних даних, наведених нижче. Теорема описує ймовірність гіпотези на основі певних спостережуваних даних у термінах попередньої ймовірності гіпотези та ймовірності даних, що підтверджують гіпотезу.

Наведена нижче модель відображає бомбардування (B), кібератаки (C), а також потенційну або вже завдану шкоду (D) об’єктам інфраструктури (I), в тому числі критично важливим об'єктам.

ISSN 2219-9365

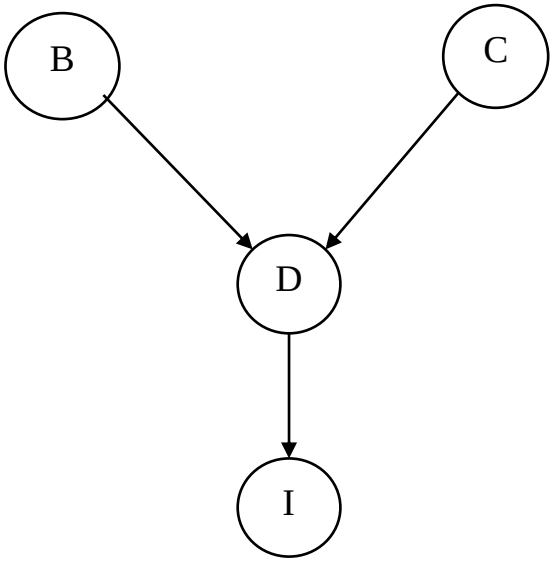

Рис. 3. Спрямована графічна модель для оцінки ризиків

Так, імовірнісний алгоритм для руйнівного процесу бомбардування (обстрілу) (B) побудований наступним чином:

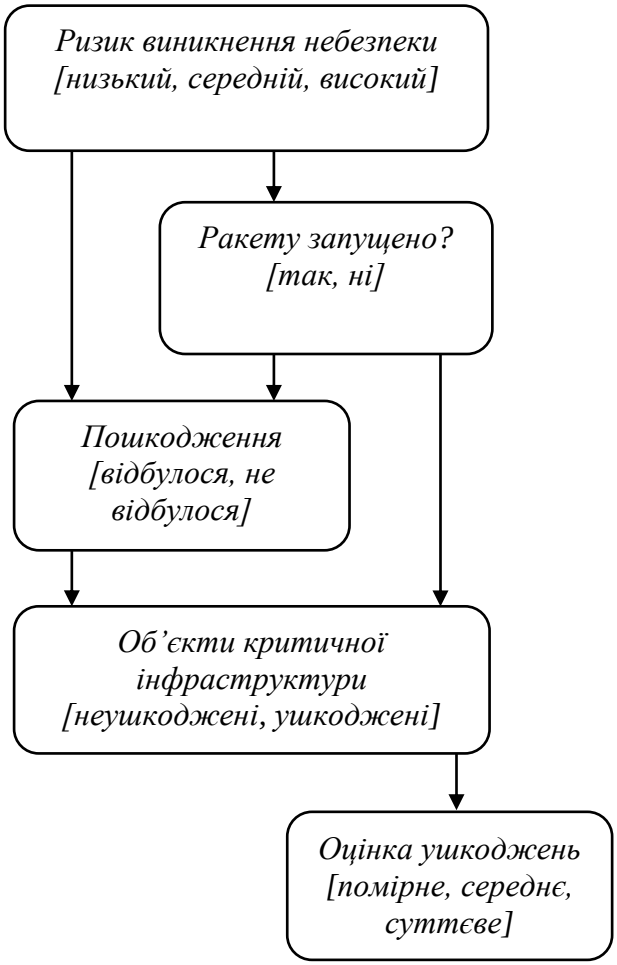

Рис. 4. Концепт мережі для процесу бомбардування

Змоделюємо це за допомогою баєсівської мережі (БМ). Припустимо, що ми маємо два рівні ризику: низький (0-0,5) і високий (0,5-1). Мета полягає у тому, щоб класифікувати ці ризики відповідно до їхньої інтенсивності, використовуючи метод класифікації. Створимо таблицю ймовірностей подій (див. Таблицю 1).

У цьому випадку можна застосувати теорему Баєса для моделювання ймовірності пошкодження інфраструктури (D) за умови виникнення повітряних бомбардувань (B) та кіберзагроз (C). Виразимо цю ймовірність як:

$$P(D|B,C) = \frac{P(B|D)P(C|D)P(D)}{P(B,C)}$$

де $P(D \mid B,C)$ - це апостеріорна ймовірність D для B і C, $P(D)$ - це попередня ймовірність D, $P(B \mid D)$ - це умовна ймовірність B для D, $P(C \mid D)$ - це умовна ймовірність C для D, і $P(B,C)$ - це спільна ймовірність B і C.

У БМ ми можемо представити ці ймовірності за допомогою таблиць умовних ймовірностей (ТУІ) і попередніх розподілів для змінних B, C і D. ТУІ визначають умовні ймовірності кожної змінної з урахуванням її батьків у мережі, тоді як останні представляють початкові ймовірності кожної змінної до того, як з'явилися будь-які дані.

Зокрема, баєсівська мережа для мультиризикового критичного порушення включає наступні компоненти:

змінна B представляє виникнення обстрілу, яка має попередній розподіл $P(B)$ = [0,6, 0,4] для низького та високого рівнів ризику;

змінна C представляє виникнення кіберзагроз, яка має попередній розподіл $P(C)$ = [0,7, 0,3] для низького та високого рівнів ризику;

змінна D відображає потенційну шкоду інфраструктурі, яка залежить як від B, так і від C.

Зокрема, ТУІ для D при заданих B і C визначає наступні ймовірності:

Таблиця 1

Таблиця умовних імовірностей

B	C	D	P(D|B,C)
Низький	Низький	Низький	0.9
Низький	Низький	Високий	0.1
Низький	Високий	Низький	0.5
Низький	Високий	Високий	0.5
Високий	Низький	Низький	0.1
Високий	Низький	Високий	0.9
Високий	Високий	Низький	0.2
Високий	Високий	Високий	0.8

Ця ТУІ визначає, що ймовірність пошкодження об’єктів інфраструктури залежить як від рівня бомбардувань, так і від кіберзагроз. Наприклад, якщо і B, і C низькі, то ймовірність того, що D буде низьким (low) становить 0,9, а ймовірність того, що D буде високим (high), - всього 0,1.

Використовуючи теорему Баєса, обчислимо апостеріорну ймовірність D, враховуючи конкретні значення B і C, на основі попередніх ймовірностей та умовних ймовірностей, зазначених у ТУІ. Наприклад, якщо видно, що і B, і C мають високий ризик виникнення, то є сенс обчислити апостеріорну ймовірність того, що D має становить низький ризик наступним чином:

$$P(D = Low \mid B = High, C = High) = P(D = Low)P(B = High \mid D = Low)P(C = High \mid D = Low))/(P(B = High, C = High)$$

На основі заданої моделі баєсівської мережі можна визначити спільний розподіл ймовірностей:

$$P(B,C,D) = P(B) * P(C) * P(D \mid B,C)$$

У наведеному вище виразі $P(B)$ і $P(C)$ - це граничні ймовірності вузлів B і C, а $P(D \mid B,C)$ - це умовна ймовірність D при заданих B і C. Тепер представимо це за допомогою таблиці ймовірностей (матриці ймовірностей). Припустимо, що кожна вершина може набувати лише двох значень: 0 або 1, що, відповідно, означає відсутність або наявність кожної події:

$$P(B = 0) = 0.6, P(C = 0) = 0.8$$
$$P(D = 0 \mid B = 0, C = 0) = 0.9, P(D = 1 \mid B = 0, C = 0) = 0.1$$
$$P(D = 0 \mid B = 0, C = 1) = 0.3, P(D = 1 \mid B = 0, C = 1) = 0.7$$

$$P(D = 0 \mid B = 1, C = 0) = 0.2, P(D = 1 \mid B = 1, C = 0) = 0.8$$
$$P(D = 0 \mid B = 1, C = 1) = 0.01, P(D = 1 \mid B = 1, C = 1) = 0.99$$

Ця матриця дає повне уявлення про спільні ймовірності всіх можливих комбінацій B, C і D. Вона дозволяє розрахувати апостеріорну ймовірність завдання ушкодження D за будь-яких конкретних значень B і C.

Наступним кроком виступає оцінка ризиків. Комплексний підхід до оцінки ризиків охоплює всі три основні етапи антикризового управління, а саме докризовий етап, етап реагування та посткризовий етап. На кожному етапі ризик оцінюється по-різному, в результаті чого виділяється потенційний ризик (на докризовому етапі), активний ризик (на етапі реагування) та залишковий ризик (післякризовий етап). Така диференціація дозволяє ухвалювати більш обґрунтовані рішення щодо вжиття тих чи інших заходів протягом усіх етапів антикризового управління уповноваженим на це особам.

Ключовими атрибутами ризику в контексті цього дослідження є його динамічність та розподіл у просторі. Ми припускаємо, що ризик у кожній просторовій точці коливається залежно від впливу множинних руйнівних процесів. Окрім того, ми також припускаємо, що ризик може бути оцінений для кожної територіальної зони або кожного вразливого об'єкта, що формує його просторову прив'язку.

У фокусі аналізу ризику в поданій моделі - оцінка ймовірності ушкоджень через залучення цільового об'єкта (в даному випадку - об'єктів критичної інфраструктури). Ризик виникає унаслідок взаємодії численних загроз і цільових об'єктів, на які впливає загроза. У цьому контексті ризик має декілька вимірів:

- Ймовірність реалізації загрози, яка залежить від того, чи має суб'єкт конкретну ціль, і потенціал загрози, який залежить від наявності інструментів, що використовуються суб'єктом (якщо це можливо);
- Атрибути цілі, такі як вразливість об'єкта, потенційне ушкодження та швидкість відновлення;
- Доступність об'єкта для суб'єктів, що спричиняють загрозу.

З цього випливає, що оцінка ризиків, пов'язаних із множинними загрозами, може бути представлена як комбінація наступних компонентів:

- Оцінка ймовірності виникнення загрози (P_T);
- Оцінка потенціалу загрози (E_T);
- Доступність об'єкта для суб'єкта (A_O);
- Вразливість об'єкта (V_O);
- Швидкість відновлення об'єкта (S_R^O).

Наприклад, якісна оцінка ризику для цілі в будь-який момент часу t буде точкою або областю в n-вимірному просторі якісних значень компонентів мультиризику:

$$R(t) = \left(P_T, E_T, A_O, D_O, V_O, S_R^O\right).$$

Ця оцінка є динамічною і може бути присвоєна кожному вразливому об'єкту та територіальній одиниці.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Представлено імовірнісну графічну модель для оцінки ризиків пошкодження об'єктів критичної інфраструктури від руйнівних процесів. Сучасний метод оцінки ризиків є корисним для моделювання сценарію множинних ризиків пошкодження інфраструктури внаслідок руйнівних процесів і дозволяє врахувати попередні знання як щодо ризиків, так і їхніх взаємозалежностей, а також внести ясність щодо ушкодження, що може бути завдане. Це, в свою чергу, може допомогти у розробці стратегій зменшення ризиків та розподілу ресурсів для захисту об’єктів критичної інфраструктури. Модель на основі мережі Баєса забезпечує базову основу для моделювання руйнівних процесів і ризиків від них. Подальша робота охоплюватиме вдосконалення моделі, вивчення додаткових методів класифікації, оцінку підходів до попередньої обробки даних, а також можливе включення моделі в програмну складову.

Література

1. HYPR. What is a hybrid attack [Електронний ресурс] / HYPR. – 2022. – Режим доступу до ресурсу: https://hypr.com/security-encyclopedia/hybrid-attack.
2. Joint Framework on countering hybrid threats a European Union response [Електронний ресурс] / European Commission. – 2018. – Режим доступу до ресурсу: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016JC0018.
3. Spatially-Distributed Multi-Hazard Risk Analysis [Електронний ресурс] / M. Zharikova, G. Barbeito, M. S. Nistor, S. W. Pickl. – 2021. – Режим доступу до ресурсу: https://ceur-ws.org/Vol-3101/Paper6.pdf.

4. Event-Based Spatially Distributed Multi-Risk Analysis / M. V. Zharikova, V. G. Sherstjuk // Conf. Comput. Sci. Inf. Technol. – Springer, Cham, 2020. – DOI: 10.1109/CSIT49958.2020.9321990.

5. Modeling Hybrid Attacks and Operations to Assess the Threats in Early Warning Systems / V. Sherstjuk та ін. // 12th Int. Conf. Adv. Comput. Inf. Technol. (ACIT). – Ruzomberok, Slovakia, 2022. – С. 39-44. – DOI: 10.1109/ACIT54803.2022.9913106.

6. An event-triggered approach to security control for networked systems using a hybrid attack model / J. Liu та ін. // Int. J. Robust Nonlinear Control. – 2021. – Т. 31, № 12. – С. 5796-5812. – DOI: 10.1002/rnc.5570.

7. Strategic Compass [Електронний ресурс] / Council of the European Union. – 2022. – Режим доступу до ресурсу: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

8. The Landscape of Hybrid Threats: A Conceptual Model (Public Version) / P. Cullen та ін. – Publ. Off. Eur. Union, 2021. – EUR 30585 EN. – ISBN 978-92-76-29819-9. – DOI: 10.2760/44985.

9. A Hybrid Model for Information Security Risk Assessment / S. Haji, Q. Tan, R. Soler Costa // Int. J. Adv. Trends Comput. Sci. Eng. – 2019. – Т 8, № 1. – С. 100–106. – DOI: 10.30534/ijatcse/2019/1981.12019.

10. Hybrid Risk Assessment Model based on Bayesian Networks / F. Aguessy та ін. // Proc. 11th Int. Workshop Secur. (IWSEC 2016). – Tokyo, Japan, 2016. – С. 21–40. – DOI: 10.1007/978-3-319-44524-3_2.

11. The Role of Context for Crisis Management Cycle / F. Aligne, J. Mattioli // Supporting Real Time Decision-Making (Annals of Information Systems 13) / F. Burstein та ін. (Eds.). – Springer, New York, 2010. – С. 113-132. – DOI: 10.1007/978-1-4419-7406-8_6.

12. Common threats and vulnerabilities of critical infrastructures / R. J. Robles та ін. // Int. J. Control Autom. – 2008. – Т. 1, № 1. – С. 17-22.

13. Multi-Hazard Risk to Global Port Infrastructure and Resulting Trade and Logistics Losses / J. Verschuur та ін. // Commun. Earth Environ. – 2023. – Т. 4, № 5. – DOI: 10.1038/s43247-022-00656-7.

14. Actionable and understandable? Evidence-based recommendations for the design of (multi-) hazard warning messages / I.Dallo, M. Stauffacher, M. Marti // Int. J. Disaster Risk Reduct. – 2022. – Т 74. – С. 102917. – DOI: 10.1016/j.ijdrr.2022.102917.

15. A three-level framework for multi-risk assessment / Z. Liu та ін. // Georisk: Assess. Manag. Risk Eng. Syst. Geohazards. – 2015. – Т. 9, № 2. – С. 59-74. – DOI: 10.1080/17499518.2015.1041989.

16. Introduction to Artificial Intelligence with Python (CSCI E-80) [Електронний ресурс] / Harvard Extension School. – 2020. – Режим доступу до ресурсу: https://cs50.harvard.edu/extension/ai/2020/fall/notes/2/.

17. Bayesian networks / M. Horný // Boston Univ. Sch. Public Health. – 2014. – Т. 17, № 5.

18. Метод оцінки ризику при відмові двигуна на повітряному судні в польоті на основі мережі Байєса / Колесник А.В., Смеляков С.В., Бердник П.Г., Колодяжний О.І. // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2020. – № 2(64). – С. 53-60. – DOI: https://doi.org/10.30748/zhups.2020.64.08.

19. Bayesian Networks [Електронний ресурс] / N. Ruozzi. – Erik Jonsson School of Engineering & Computer Science at the University of Texas at Dallas. – Режим доступу до ресурсу: https://personal.utdallas.edu/~nrr150130/gmbook/bayes.html.

References

1. HYPR. What is a hybrid attack [Electronic resource] / HYPR. – 2022. – Access mode: https://hypr.com/security-encyclopedia/hybrid-attack.

2. Joint Framework on countering hybrid threats a European Union response [Electronic resource] / European Commission. – 2018. – Access mode: https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52016JC0018.

3. Spatially-Distributed Multi-Hazard Risk Analysis [Electronic resource] / M. Zharikova, G. Barbeito, M. S. Nistor, S. W. Pickl. – 2021. – Access mode: https://ceur-ws.org/Vol-3101/Paper6.pdf.

4. Event-Based Spatially Distributed Multi-Risk Analysis / M. V. Zharikova, V. G. Sherstjuk // Conf. Comput. Sci. Inf. Technol. – Springer, Cham, 2020. – DOI: 10.1109/CSIT49958.2020.9321990.

5. Modeling Hybrid Attacks and Operations to Assess the Threats in Early Warning Systems / V. Sherstjuk et al. // 12th Int. Conf. Adv. Comput. Inf. Technol. (ACIT). – Ruzomberok, Slovakia, 2022. – P. 39-44. – DOI: 10.1109/ACIT54803.2022.9913106.

6. An event-triggered approach to security control for networked systems using a hybrid attack model / J. Liu et al. // Int. J. Robust Nonlinear Control. – 2021. – Volume 31, № 12. – P. 5796-5812. – DOI: 10.1002/rnc.5570.

7. Strategic Compass [Electronic resource] / Council of the European Union. – 2022. – Access mode: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf.

8. The Landscape of Hybrid Threats: A Conceptual Model (Public Version) / P. Cullen et al. – Publ. Off. Eur. Union, 2021. – EUR 30585 EN. – ISBN 978-92-76-29819-9. – DOI: 10.2760/44985.

9. A Hybrid Model for Information Security Risk Assessment / S. Haji, Q. Tan, R. Soler Costa // Int. J. Adv. Trends Comput. Sci. Eng. – 2019. – Volume 8, № 1. – P. 100–106. – DOI: 10.30534/ijatcse/2019/1981.12019.

10. Hybrid Risk Assessment Model based on Bayesian Networks / F. Aguessy et al. // Proc. 11th Int. Workshop Secur. (IWSEC 2016). – Tokyo, Japan, 2016. – P. 21–40. – DOI: 10.1007/978-3-319-44524-3_2.

11. The Role of Context for Crisis Management Cycle / F. Aligne, J. Mattioli // Supporting Real Time Decision-Making (Annals of Information Systems 13) / F. Burstein et al. (Eds.). – Springer, New York, 2010. – P. 113-132. – DOI: 10.1007/978-1-4419-7406-8_6.

12. Common threats and vulnerabilities of critical infrastructures / R. J. Robles et al. // Int. J. Control Autom. – 2008. – Volume 1, № 1. – P. 17-22.

13. Multi-Hazard Risk to Global Port Infrastructure and Resulting Trade and Logistics Losses / J. Verschuur et al. // Commun. Earth Environ. – 2023. – Volume 4, № 5. – DOI: 10.1038/s43247-022-00656-7.

14. Actionable and understandable? Evidence-based recommendations for the design of (multi-) hazard warning messages / I.Dallo, M. Stauffacher, M. Marti // Int. J. Disaster Risk Reduct. – 2022. – Volume 74. – P. 102917. – DOI: 10.1016/j.ijdrr.2022.102917.

15. A three-level framework for multi-risk assessment / Z. Liu et al. // Georisk: Assess. Manag. Risk Eng. Syst. Geohazards. – 2015. – Volume 9, № 2. – P. 59-74. – DOI: 10.1080/17499518.2015.1041989.

16. Introduction to Artificial Intelligence with Python (CSCI E-80) [Electronic resource] / Harvard Extension School. – 2020. – Access mode: https://cs50.harvard.edu/extension/ai/2020/fall/notes/2/.

17. Bayesian networks / M. Horný // Boston Univ. Sch. Public Health. – 2014. – Volume 17, № 5.

18. Kolesnyk, A., Smelyakov, S., Berdnyk, P., & Kolodyazhnyy, O. (2020). Metod otsinky ryzyku pry vidmovi dvyhuna na povitryanomu sudni v pol′oti na osnovi merezhi Bayyesa. Zbirnyk naukovykh prats′ Kharkivs′koho natsional′noho universytetu Povitryanykh Syl. – 2020. – № 2(64). – P. 53-60. – DOI: 10.30748/zhups.2020.64.08.

19. Bayesian Networks [Electronic resource] / N. Ruozzi. – Erik Jonsson School of Engineering & Computer Science at the University of Texas at Dallas. – Access mode: https://personal.utdallas.edu/~nrr150130/gmbook/bayes.html