МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО"

НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

THEORETICAL AND APPLIED CYBERSECURITY

**Матеріали другої Всеукраїнської
науково-практичної конференції**

Випуск 2

Київ – 2024

Рекомендовано до друку Вченою радою
КПІ ім. Ігоря Сікорського
(протокол № 14 від 12 червня 2024 р.)

Theoretical and Applied Cybersecurity. Матеріали другої всеукраїнської науково-практичної конференції (TACS-2024). – Київ: Інжиніринг. – 190 с. ISBN 978-966-2344-98-1

До збірника увійшли матеріали доповідей, представлених на другій всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2024, 30 травня 2024 року, м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням кібернетичної безпеки критичних інфраструктур, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації. Наведені матеріали з актуальних проблем інформаційної та кібернетичної безпеки, можливості застосування штучного інтелекту, системного аналізу при забезпеченні підтримки прийняття рішень, комп'ютерному моделюванні процесів і систем, актуальні завдання забезпечення інформаційної та кібербезпеки.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

ISBN 978-966-2344-98-1

ВИЗНАЧЕННЯ КОЕФІЦІЄНТІВ ЛОГІКО-ЙМОВІРНІСНИХ МОДЕЛЕЙ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ ВІРТУАЛЬНИХ ЕКСПЕРТІВ

Д.В. Ланде, О.М. Новіков, Л.Б. Алексейчук

Національний технічний університет України
«Київський політехнічний інститут ім. Ігоря Сікорського»,
Київ, Україна
d.lande@kpi.ua

У роботі розглянуто питання моделювання загроз та аналіз ризиків для об'єктів критичної інфраструктури, зокрема, логіко-ймовірнісний метод для моделювання небезпечних станів і оцінки ризиків. Зроблено акцент на коректному визначенні ймовірностей переходів у мережах за допомогою генеративного штучного інтелекту. Запропоновано дві стратегії оцінки параметрів мережі: Output-алгоритм і Input-алгоритм, результати яких було порівняно за допомогою міри Фробеніуса, що підтвердило високу кореляцію отриманих матриць та їх узгодженість.
Ключові слова: логіко-ймовірнісна модель, критична інфраструктура, оцінка ризиків, штучний інтелект.

Вступ

Ефективним напрямком досліджень у сфері кібербезпеки є моделювання загроз та аналіз ризиків. Зокрема, задачі моделювання загроз, аналізу кібербезпеки та інші аспекти безпеки об’єктів критичної інфраструктури було розглянуто в роботах [1, 2] та інших.

Одним з напрямків вирішення задач моделювання загроз та аналізу ризиків об’єктів критичної інфраструктури є логіко-ймовірнісній метод, вперше запропонований англійським вченим Дж. Булем [3]. Логіко-ймовірнісний метод полягає у розробці моделі функції небезпечного стану із застосуванням операцій булевої алгебри з подальшим використанням теорії ймовірності. У роботах [4, 5] у якості об’єкту розвитку небажаної події

розглядалась система кіберзахисту інформаційно-комунікаційної системи, яка перебуває під впливом кібератак.

Важливим у питанням розробці та застосуванні логіко-ймовірнісних моделей є коректне та точне визначення їх коефіцієнтів. В роботах з теорії логіко-ймовірнісного моделювання це питання, частіше за все, залишається поза розглядом. Разом з цим, для визначення коефіцієнтів логіко-ймовірнісних моделей ІКС можна використовувати статистичні методи, методи, які враховують структуру мережі, методи машинного навчання і методи експертного оцінювання.

Статистичні методи базуються на спостереженні за мережевим трафіком протягом певного періоду часу. На основі історичних даних підраховуються частоти переходів між серверами, що дозволяє визначити коефіцієнти.

Методи, які враховують структуру мережі можуть дати уявлення про те, які сервери, ймовірно, будуть зв'язані між собою. Зокрема, метод Монте-Карло використовується для оцінки ймовірностей переходів шляхом випадкового генерування великої кількості можливих шляхів і аналізу результатів.

Методи машинного навчання традиційно використовують для прогнозування трафіку в мережах, ймовірностей переходів на основі попередніх даних можуть застосовуватись нейронні мережі та LSTM. Ці методи можуть бути використані для прогнозування ймовірностей переходів на основі попередніх даних.

Методи експертного оцінювання можна використовувати для оцінки ймовірностей переходів у мережах серверів в умовах, коли доступні дані обмежені, неможливості врахувати трафік в реальній системі, коли історичні дані недостатні або не повністю відображають всі можливі стани і переходи в мережі, коли розглядаються системи з великою кількістю зв’язків різного рівня, де автоматичні методи можуть бути занадто складними. Серед відомих методів експертних оцінок можна назвати методи експертних опитувань, дельфійський метод, метод аналізу ієрархій, метод байєсовських мереж, тощо.

Мета дослідження. Метою роботи є представлення методології визначення ймовірностей переходів у мережах методів експертного опитування віртуальних експертів з використанням генеративного штучного інтелекту для визначення.

Опис методології. У цій роботі зупинимось саме на методі експертних опитувань, тобто залучення групи експертів для надання оцінок ймовірностей переходів на основі їхнього досвіду і знань. Для усереднення, досягнення консенсусу між експертами будемо застосовувати дельфійський підхід, в рамках якого група експертів незалежно оцінює ймовірності, а потім переглядає свої оцінки на основі узагальнених результатів. Будемо розглядати так званих «віртуальних експертів», які моделюються засобами генеративного штучного інтелекту [6].

Для оцінювання параметрів мережі пропонується застосування різних моделей генеративного штучного інтелекту, які реалізують «віртуальних експертів» [6]. На базі їх відповідей на спеціальні запити (промпти), що стосуються суті мережевих зв'язків, оцінюються ймовірності переходів за цими зв'язками.

Задача ставиться таким чином: нехай існує мережа з направленими зв'язками, вузли якої відповідають деяким серверам мережі. Відповідно до призначення вузлів і напрямків зв'язку необхідно надати експертні оцінки значень ймовірностей переходів.

Для оцінки цих ймовірностей і подальшого усереднення їх результатів можливо дві стратегії.

Перша стратегія полягає в оцінці зв'язків, що виходять із вузлів мережі. Для цього перебираються всі вузли мережі і запитуються ймовірності переходу від них по всім наявним вихідним зв'язкам. Такий підхід назвемо **Output**-алгоритмом.

Інший, протилежний підхід полягає у розгляданні всіх зв'язків, що входять в кожний вузол мережі і оцінювання ймовірностей входження за кожним із цих зв'язків. Такий підхід назвемо **Input**-алгоритмом.

Для розглянутих прикладів оцінюється міра взаємної близькості матриць зв'язків (*Output* та *Input*), що відповідають мережі, за Фробеніусом, показується що ця міра менше ніж близькість з випадковою матрицею, з матрицею суміжності.

Після отримання оцінок всіх ймовірностей за цими двома алгоритмами отримуються дві матриці, відповідні значення яких можна усереднити і надати як загальний результат експертної оцінки (у відповідності узгодженості цих матриць).

Для опису логічної структури інформаційно-комунікаційної системи використаємо орієнтований граф $G(V,E)$, де $v_i \in V$ - множина об'єктів/інформаційних ресурсів/сервісів системи, $E = (e_1,...,e_L)$, $e_k = (v_i, v_j)$ - наявність чи відсутність зав'язків між ними, $E \subseteq V \times V$ та $e_i \in E$.

Якщо на одному фізичному сервері розміщується декілька сервісів, що можуть бути об'єктами, джерелами загроз або через них можуть проходити сценарії атак, то будемо виділяти їх в окремі об'єкти - v_i. Отриманий граф $G(V,E)$ будемо представляти у вигляді матриці суміжності, яку називають матрицею доступності об'єктів. Граф буде орієнтованим тому що з деяких об'єктів можна ініціювати з'єднання тільки в односторонньому порядку.

Логіко-ймовірніснісну модель такої системи було запропоновано:

$$J(A) = P(G, A, O, P),$$

Де $J(A)$ - критерій ймовірності успішності сценарію атаки,

$G(V,E)$ - відома та фіксована топологія мережі,

$V = \{v_1,...,v_N\}$ – множина об'єктів/ресурсів/сервісів у ІКС,

$A = \{a_1,...,a_K\} \subset V$ - множина джерел загроз,

$O = \{o_1,...,o_M\} \subset V$ - множина критичних об'єктів для атак,

$P = \{P_1, \ldots, P_N\}$ - ймовірності захоплення об'єктів ІКС.

Саме для оцінки значень пропонується підхід оцінки перехідних ймовірностей за допомогою множини віртуальних експертів».

Розглянемо мережу з вузлами (Рис. 1):

Firewall - S1, Mail Server - S2, Web Server - S3, AWP Administrator – S4, AWP Clients - S5, Application Server - S6, DB Server – S7.

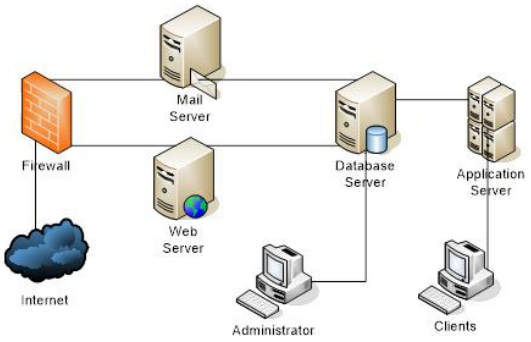

Рисунок 1 – Приклад мережі [5]

Ці вузли зв'язані між собою спрямованим зв'язками, яким відповідає матриця суміжності, елементами якої можуть бути 0 і 1 (Таблиця 1).

Таблиця 1 - комунікації (Links)

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	1	1	0	0	0	0
Mail Server (S2)	1	0	0	0	0	0	1
Web Server (S3)	1	0	0	0	0	0	1
AWP Administrator (S4)	1	1	1	0	1	1	1
AWP Clients (S5)	0	0	0	0	0	1	0
Application Server (S6)	0	0	0	0	1	0	1
DB Server (S7)	0	0	0	0	0	1	0

При застосуванні методології «віртуальних експертів» здійснюється звернення до сервісів генеративного штучного інтелекту ChatGPT https://chat.openai.com/, Gemini (https://gemini.google.com/), Groq (https://groq.com/). Надалі для оцінки значень параметрів системи багатократно надаються запити (промпти), які після цього усереднюються.

Оцінка параметрів на основі алгоритму Output

Послідовно для всіх вузлів мережі, з яких виходять зв'язки, виконуються промпти, результати виконання яких усереднюються:

Промпт 1 (p12=P(S1->S2), p13=P(S1->S3)):

Нехай відбулось проникнення у корпоративну мережу через фейрвол, зловмисники хочуть досягти сервера баз даних. Кількісно оцініть умовну ймовірність того, що вони пройшли від фейрволу до поштового сервера – p12, до веб-сервера – p13. Надайте експертні чисельні значення умовних ймовірностей p12, p13.

Аналогічним чином формуються промпти 2 – 5.

В результаті отримання результатів виконання промптів від систем штучного інтелекту отримані параметри мережі, якій відповідає така таблиця умовних ймовірностей (матриця Output):

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	0.4	0.5	0	0	0	0
Mail Server S2)	0.28	0	0	0	0	0	0.78
Web Server (S3)	0.27	0	0	0	0	0	0.75
AWP Administrator (S4)	0.55	0.55	0.55	0	0.55	0.23	0.65
AWP Clients (S5)	0	0	0	0	0	1	0
Application Server (S6)	0	0	0	0	0.29	0	0.66
DB Server (S7)	0	0	0	0	0	1	0

Оцінка параметрів на основі алгоритму Input:

Послідовно для всіх вузлів мережі, у які входять зв'язки, виконуються промпти, результати виконання яких усереднюються:

Промпт 1 (p21=P(S2->S1), p31=P(S3->S1),

p41=P(S4->S1)):

Нехай відбулось проникнення у корпоративну мережу, зловмисники хочуть досягти сервера баз даних. Відомо, що йде звернення до фейрволу із внутрішнього сегменту. Кількісно оцініть умовну ймовірність того, звернення до фейрволу йде від поштового сервера (p21), від веб-сервера (p31), від сервера адміністратора (p41). Надайте експертні чисельні значення умовних ймовірностей p21, p31, p41.

Аналогічним чином формуються промпти 2 – 6.

Таблиця умовних ймовірностей (Input):

	S1	S2	S3	S4	S5	S6	S7
Firewall (S1)	0	0.34	0.3	0	0	0	0
Mail Server (S2)	0.28	0	0	0	0	0	0.25
Web Server (S3)	0.38	0	0	0	0	0	0.3
AWP Administrator (S4)	0.4	0.36	0.35	0	0.44	0.35	0.65
AWP Clients (S5)	0	0	0	0	0	0.4	0
Application Server (S6)	0	0	0	0	0.59	0	0.5
DB Server (S7)	0	0	0	0	0	0.38	0

Оцінка близькості отриманих матриць

Оцінка міри близькості дозволяє нам побачити, наскільки отримані матриці корельовано між собою, і наскільки вони відрізняються від випадкової матриці і матриці комунікацій. Для проведення розрахунків отримані матриці нормуються (їх значення будуть варіюватись від 0 до 1) шляхом ділення всіх елементів на найбільший. У

даному випадку застосовується норма Фробеніуса $\|\cdot\|_F$, що дорівнює кореню квадратному із суми квадратів різниць всіх елементів відповідних матриць:

$$\|A, B\|_F = \sqrt{\sum_{i,j}(a_{ij} - b_{ij})^2}.$$

В процесі попарного порівняння застосовувались такі матриці:

Output – таблиця умовних ймовірностей, отримана за алгоритмом Output;

Input – таблиця умовних ймовірностей, отримана за алгоритмом Input;

Links – таблиця комунікацій;

Random – випадкова матриця.

У результаті розрахунків (Таблиця 2) виявилося, що матриці Output та Input зв'язані між собою сильніше всього, що свідчить про їх узгодженість, тобто коректності застосування методу.

Таблиця 2 – результати взаємного порівняння матриць.

Матриця 1	Матриця 2	Норма Фробеніуса, різниці матриць
Output	*Input*	0,167
Output	*Links*	0,248
Intput	*Links*	0,286
$\frac{Output + Input}{2}$	*Links*	0,211
Output	*Random*	0,407
Input	*Random*	0,520

Наведена таблиця, отримана у результаті нормування відповідних матриць і розрахунку міри Фробеніуса, свідчить щодо високої кореляції отриманих матриць Output та Input, а також можливості використання їх середніх значень, які дають результати найбільш корельовано з вихідною комунікаційною матрицею.

Висновки

Логіко-ймовірнісний метод є ефективним інструментом для моделювання загроз і аналізу ризиків, що дозволяє створювати моделі, які враховують ймовірності розвитку небажаних подій внаслідок зовнішніх впливів. Проте коректне визначення коефіцієнтів для таких моделей залишалось проблемним питанням.

Запропонований підхід із залученням множини віртуальних експертів, створених засобами генеративного штучного інтелекту, показав свою ефективність. Віртуальні експерти дозволяють оперативно та надійно оцінити ймовірності переходів у мережах навіть за відсутності повних історичних даних.

Два алгоритми оцінки ймовірностей переходів – Output та Input – показали узгодженість результатів, що підтверджує коректність методу. Попарне порівняння матриць, отриманих за цими алгоритмами, з матрицею комунікацій та випадковою матрицею виявило високий рівень їх подібності, що свідчить про надійність запропонованого підходу.

Таким чином, запропоновані методи експертного оцінювання за участі віртуальних експертів відкривають нові можливості для оперативного аналізу ризиків.

Перелік використаних джерел

1. Dinesh Kumar Saini. Cyber Defense: Mathematical Modeling and Simulation. International Journal of Applied Physics and Mathematics, Vol. 2, No. 5, September 2012, pp. 312-315. DOI: http://dx.doi.org/10.7763/IJAPM.2012.V2.121

2. Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, Sithamparanathan Kandeepan A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. Engineering Science and Technology, an International Journal, Vol. 31, July 2022, 15 p. DOI: http://dx.doi.org/10.1016/j.jestch.2021.09.011

3. Boole George. An investigation of the laws of thought, on which founded the mathematical theories of logic and

probabilities. London, 1854. - 343 p. Режим доступу: https://www.gutenberg.org/ebooks/15114

4. L. Alekseichuk, O. Novikov, A. Rodionov, D. Yakobchuk Cyber Security Logical and Probabilistic Model of a Critical Infrastructure Facility in the Electric Energy Industry // Theoretical And Applied Cybersecurity - Vol.5 No. 1, 2023, pp. 61-66. DOI: https://doi.org/10.20535/tacs.2664-29132023.1.287365L

5. L. Alekseichuk, O. Novikov, A. Rodionov, D.Yakobchuk The Best Scenario of Cyber Attack Selecting on the Information and Communication System Based on the Logical and Probabilistic Method // Theoretical And Applied Cybersecurity. - Vol.5 No. 2, 2023, pp. 81-88. DOI: https://doi.org/10.20535/tacs.2664-29132023.2.288973

6. Dmytro Lande, Leonard Strashnoy. GPT Semantic Networking: A Dream of the Semantic Web - The Time is Now. - Kyiv: Engineering, 2023. - 168 p. ISBN 978-966-2344-94-3

ЗМІСТ

Терещенко А.М., Задірака В.К.
Метод реалізації вентиля тоффолі на основі вентиля марголуса на чотирьох і більше кубітах…….. 3
Ланде Д.В., Новіков О.М., Алексейчук Л.Б.
Визначення коефіцієнтів логіко-ймовірнісних моделей кібербезпеки з використанням віртуальних експертів……. 10
Даник Ю.Г., Шестаков В.І.
Особливості трансформації державної політики у сфері кібербезпеки в умовах війни…….. 20
Пучков О.О., Субач І.Ю., Рибак О.О.
Технологія ідентифікації політичної спрямованості джерел інформації на базі машинного навчання…… 25
Паршин О.Ю., Яковлєв С.В.
Диференціальна атака на шифр idea на основі властивостей його ключового суматора…….. 28
Драгунцов Р.І., Зубок В.Ю.
Особливості атак з використанням соціального графу та підходи до захисту…… 32
Смирнов С. А., Лугінін Б.А.
Оптимальне розподілення ресурсів захисту при багатопозиційних кібератаках…… 36
Васалатій А.Ю., Бичок В.В., Циганкова О.В., Хмельницький М.О.
Застосування SAT-розв'язувачів для пошуку n-ок Шура… 40
Mykola Ilin, Oleksandr Rybak, Iryna Stopochkina
Estimating the probability of attacks on key objects of the supply chain of critical infrastructure objects…… 46
Гуменюк О.О., Комар А.В., Свобода І.М., Ланде Д.В.
Виведення та аналіз наративів у інформаційних потоках за допомогою штучного інтелекту…… 50
Свобода І.М.
Формування стратегій кібербезпеки за допомогою методу аналізу ієрархій та штучного інтелекту…… 54
Палагін В.В., Івченко О.В.
Аналіз шкідливого трафіку на канальному рівні…….. 58