

ОЦІНКА РИЗИКІВ НА ОСНОВІ АНАЛІЗУ ВРАЗЛИВОСТЕЙ ЗА СХЕМОЮ MAUT

А. В. Вусата^{1, а}, С. А. Смирнов¹, П. О. Наказной¹

¹Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
НН Фізико-технічний інститут

Анотація

Розглянуто підхід до знаходження кількісної оцінки ризику через формулу середніх втрат та запропоновано новий погляд на ризик на основі головного фактора їх утворення — вразливостей. Завдяки знайдений подібності ризику з багатокритеріальною теорією корисності (MAUT) встановлена необхідність перевірки вразливостей на їх залежність/незалежність. Перевірку розроблено для ймовірностей реалізацій вразливостей аналогічно до аксіом незалежності в MAUT. Таким чином на модельному прикладі була застосована створена перевірка незалежності та розроблені шляхи знаходження кількісної оцінки ризику у випадках сумісних залежних/незалежних вразливостей.

Ключові слова: ризик, кількісна оцінка ризику, аналогія, загроза, вразливість, багатокритеріальна теорія корисності, аналіз залежності/незалежності

Вступ

Ризик [1, с. 118] — величина прогнозованого збитку від реалізації загрози внаслідок прийняття рішення в умовах часткової невизначеності.

Не дивно, що головна задача при цьому — це управляти ризиками, тобто навчитися їх оптимізувати для конкретних ситуацій. Адже за останні десятиліття зросла чутливість населення навіть до рідко реалізованих подій, яким раніше взагалі не надавали значення.

Можливість такого явища, як управління ризиками, пов'язана з наявністю об'єктивної складової в тому, що ризик є вимірним і незалежним від сприйняття людини, а тому його можна ідентифікувати, оцінити та передбачити [2].

В загальному випадку, вдале управління полягає в тому, щоб на основі аналізу ризику прийняти ефективне рішення.

Аналіз ризику

В результаті аналізу для ЛПР формується цілісна картина ситуації та можливих ризиків, від якої буде залежати ефективність майбутніх рішень.

Ідентифікація — виявлення ризиків та причин їх виникнення для конкретної ситуації. Важливо ідентифікувати всі ризики для повноти картини.

Оцінювання ризику — знаходження кількісного показника фактичного рівня ризику і перевірка, чи не перевищує отримане значення допустимий ризик 1. Відповідно, оцінка включає визначення ймовірностей несприятливих подій та розподіл втрат.

$$R \leq R_d, \quad (1)$$

де R — знайдений ризик; R_d — допустимий ризик.

Прогноз ризику — оцінювання ризику в конкретні моменти часу в майбутньому, спираючись на попередні дані про минулі події.

1. Новий погляд на ризик

Управління ризиком неможливе без аналізу, а він полягає у знаходженні кількісної оцінки ризику.

Практика використання математичних моделей ризику показує, що краще розглядати ризик через три складові: загрозу, збитки від неї та ПР в умовах невизначеності, тобто як концепцію «ризик-загроза».

Відповідно, найефективніший та практично найпростіший спосіб подання ризику — через ймовірності реалізації цих загроз та втрати від них 2.

$$R = \sum_i p_i w_i, \quad (2)$$

де i - індекс загрози.

Будь-яка втрата утворюється від реалізації певної загрози, тому заглибимося більше у це поняття.

Загрози — це види небезпек для об'єкта ПР, які можуть призвести до негативних наслідків для ЛПР. Проте, не кожній загрозі піддається досліджувана ситуація, тому що загроза використовує вразливість (слабкість) системи.

Отже, саме вразливості породжують загрози, тому для визначення ризику необхідно розуміти типи загроз, які існують та знати вразливості системи:

$$\text{Загрози} + \text{Вразливості} + \text{Збитки} = \text{Ризик}$$

Розглянемо ризик через вразливості, як головний фактор його утворення в будь-якому середовищі. Такий вплив вразливостей на ризик можна зобразити схематично (рис. 1).

^аanyavusata@gmail.com

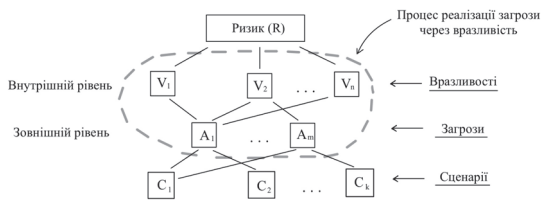


Рис. 1. Ієрархічне представлення ризику

У кожної системи (чи то людина, чи інформаційна система) на внутрішньому рівні є набір вразливостей $V_1, \dots, V_n$, які їй притаманні, а на зовнішньому – набір загроз $A_1, \dots, A_m$, які чекають нагоди, щоб використати слабкості системи. Окремо ці дві множини нічого не варті, лише разом вони утворюють процес реалізації загрози через вразливість (подія) та завдають втрат, а тому створюють ризик R . Звісно, існують різні сценарії ($C_i, i = 1, \dots, k$), коли ті самі події можуть реалізовуватися з іншою ймовірністю.

Але тепер постає питання, як саме задати оцінку ризику так, щоб виразити її через вразливості?

Розглянувши загальну формулу оцінки ризику 2, можна помітити певну схожість з багатокритеріальною теорією корисності через те, що і там, і там адитивна згортка.

2. MAUT

Багатокритеріальна теорія корисності — метод багатомірного аналізу інформації, який з теоретичної точки зору ідеальний, адже будується єдина математична теорія, яка дозволяє визначити конкретний вигляд загальної ФК в залежності від переваг ЛПР.

Особливість методу — аксіоматичне обґрунтування, яке стверджує, що при виконанні певних умов існує математичне доведення того, що результати є коректними, а тому придатними для подальшого використання. Тобто є набір аксіом, які має задовольняти функція корисності (ФК) ЛПР.

В MAUT ці аксіоми поділяються на дві групи [3]:

- Перша група — це аксіоми загального характеру (повноти, транзитивності та аксіома, яка заснована на припущенні, що функція корисності неперервна).
- Друга група умов — аксіоми незалежності між критеріями. Саме виконання цих аксіом дозволяє стверджувати, що критерії є незалежними:
 - 1) Незалежність за корисністю (незалежність критерію C_1 від критеріїв $C_2, \dots, C_N$).
 - 2) Незалежність за перевагою (незалежність пари критеріїв C_1, C_2 від критеріїв $C_3, \dots, C_N$).

Наслідок з аксіом

Р. Кіні [3] стверджував, що виконання аксіом незалежності за корисністю та за перевагою — достатня умова існування багатокритеріальної ФК (3, 4).

Якщо $\sum_{i=1}^n w_i = 1$, то маємо адитивну ФК 3

$$U(x) = \sum_{i=1}^n w_i U_i(x_i). \quad (3)$$

Адитивна функція дозволяє підсумувати вклади кожного з критеріїв в загальну корисність. Це найбільш вживана багатомірна ФК через свою простоту та активне використання на практиці.

Якщо $\sum_{i=1}^n w_i \neq 1$, то мультиплікативна ФК 4.

$$kU(x) + 1 = \prod_{i=1}^n [kw_i U_i(x_i) + 1]. \quad (4)$$

3. Аналогія

Представимо знайдену аналогію знаходження оцінки ризику зі знаходженням багатокритеріальної ФК в MAUT:

MAUT

$$U(x) = \sum_{i=1}^n U_i(x) w_i, \quad (5)$$

де i — критерій, x — альтернатива,

w_i — вага критерію,

U_i — однокритеріальна ФК альтернативи.

В результаті: $U(x)$ — ф-я корисності альтернативи по всім критеріям.

Ризик

$$R(c) = \sum_{i=1}^n p_i(c) w_i, \quad (6)$$

де i — вразливість, c — сценарій,

p_i — ймовірність реалізації вразливості в сценарії,

w_i — втрата від реалізації вразливості.

В результаті: $R(c)$ — загальний ризик сценарію по всім вразливостям.

В MAUT 5 головна ціль — побудувати загальну ФК для кожної альтернативи по всім критеріям, щоб отримати загальну картину корисностей альтернатив та обрати кращу з них.

Можна подати ризик аналогічно, але через вразливості. Тобто ціль 6 — дізнатися загальний ризик для сценарію по всім можливим вразливостям, як суму часткових ризиків по кожній вразливості.

Проте, напрошується питання: чому не перевіряється незалежність вразливостей (як перевіряють незалежність критеріїв в MAUT), а одразу застосовується формула (та сама адитивна згортка)?

Вразливості можуть бути як залежними, так і незалежними, але на практиці всі оминають цей факт. У випадку залежних вразливостей окрім того, що немає математичного підтвердження коректності використання адитивної згортки, в результаті ще можна отримати невірні дані про кількісну оцінку, а тому на цей результат не можна спиратися. Адже таке недбале ставлення може призвести до катастроф соціального, техногенного чи природного походження.

Вихід з цієї ситуації пропонуємо наступний: перенести аналіз на основі аксіом з MAUT на незалежність вразливостей.

4. Незалежність вразливостей

Розділимо аналіз ризику на два етапи – якісний і кількісний [2]. Кількісний аналіз – кінцевий етап (визначення оцінки), а якісний – початковий етап (знаходження загроз, з'ясування вразливостей).

До якісного аналізу слід додати дослідження вразливостей на їх незалежність між собою тим шляхом, який використовується в МАУТ, тобто через перевірку виконання аксіом незалежності на вразливостях.

Перенесення аксіом

Нехай $A_1, A_2, \dots, A_n$ – вразливості, $n \geq 3$; $a_1, a_2, \dots, a_n$ – оцінки вразливостей (втрати).

1) Незалежність за корисністю

Аналогія: незалежність 1-го критерію від інших $\rightarrow$ незалежність 1-ї вразливості від інших.

З одного боку має виконуватися 7

$$P(A_i | A_1, \dots, A_{i-1}, A_{i+1}, \dots, A_n) = P(A_i^* | A_1 = a_1, \dots, A_n = a_n) = P(A_i^*), \quad (7)$$

де $A_1, \dots, A_n$ – вразливості, які реалізувалися, A_i^* – вразливість, яка ще не реалізувалася.

З іншого боку 8 (за ф-ю умовної ймовірності)

$$P(A_i^* | A_1, \dots, A_n) = \frac{P(A_i^* \cap \bigcap_{j=1, j \neq i}^n A_j)}{P(\bigcap_{j=1, j \neq i}^n A_j)}. \quad (8)$$

З 7 і 8 слідує вираз 9:

$$P(A_i^*) = \frac{P(A_i^* \cap \bigcap_{j=1, j \neq i}^n A_j)}{P(\bigcap_{j=1, j \neq i}^n A_j)}. \quad (9)$$

9 можливе лише, коли виконується 10

$$P(A_i^* \cap \bigcap_{j=1, j \neq i}^n A_j) = P(A_i^*) P(\bigcap_{j=1, j \neq i}^n A_j). \quad (10)$$

$\Rightarrow$ вразливості незалежні за корисністю, якщо $\forall c, \forall i = 1, \dots, n$ виконується співвідношення 10.

2) Незалежність за перевагою

Аналогія: незалежність 2-ох критеріїв від інших $\rightarrow$ незалежність 2-ох вразливостей від інших.

$\Rightarrow$ вразливості незалежні за перевагою, якщо $\forall c, \forall i = 1, \dots, n$ виконується співвідношення 11

$$P(A_{i_1}^* \cap A_{i_2}^* \cap \bigcap_{j=1, j \neq i_1, j \neq i_2}^n A_j) = P(A_{i_1}^* \cap A_{i_2}^*) P(\bigcap_{j=1, j \neq i_1, j \neq i_2}^n A_j). \quad (11)$$

Варто зауважити, що залежність вразливостей може провокувати залежність втрат від їх реалізацій.

5. Оцінки ризику в залежності від розвитку подій

Якщо вразливості несумісні, то оцінка ризику залишається 6.

В реальних ситуаціях майже завжди реалізації вразливостей сумісні. Якщо це так, то необхідно перевіряти їх залежність/незалежність відповідно до розділу 4.

Розглянемо модельний приклад (автомобіль) та два можливі сценарії розвитку негативних подій. Перший сценарій C_1 – потраплення автомобіля у яму, другий C_2 – зіткнення з іншим автомобілем. Такі приклади продемонструють і той факт, що ймовірності настання одних і тих самих вразливостей однієї системи можуть відрізнятися при різних сценаріях.

Представлені вразливості системи у таблиці 1).

Табл. 1. Розподіл втрат для вразливостей

Вразливість	Втрати
A_1 —може зірватися передній бампер	2000 грн.
A_2 —може розбитися переднє скло	1500 грн.
A_3 —може подряпатися диск на колесі	700 грн.
A_4 —може відвалитися глушник	300 грн.

З певного пункту технічного обслуговування були взяті статистичні дані (табл. 2) про кількість реалізацій різних наборів вразливостей автомобіля в результаті вказаних вище сценаріїв.

Табл. 2. Статистичні дані про реалізації вразливостей для C_1 та C_2

Вразливості	Реалізації C_1	Реалізації C_2
A_1	1200	3000
A_2	600	2800
A_3	3000	900
A_4	2500	750
$A_1 \cap A_2$	250	900
$A_1 \cap A_3$	600	400
$A_1 \cap A_4$	400	300
$A_2 \cap A_3$	300	490
$A_2 \cap A_4$	200	200
$A_3 \cap A_4$	480	260
$A_1 \cap A_2 \cap A_3$	48	300
$A_1 \cap A_2 \cap A_4$	40	150
$A_1 \cap A_3 \cap A_4$	200	70
$A_2 \cap A_3 \cap A_4$	100	90
$A_1 \cap A_2 \cap A_3 \cap A_4$	30	65

Перевірка незалежності:

Для C_1 (табл. 2):

1) Незалежність за корисністю

$$P(A_1 \cap A_2 \cap A_3 \cap A_4) = P(A_1)P(A_2 \cap A_3 \cap A_4) = P(A_2)P(A_1 \cap A_3 \cap A_4) = P(A_3)P(A_1 \cap A_2 \cap A_4) = P(A_4)P(A_1 \cap A_2 \cap A_3) \quad (12)$$

$$\frac{30}{4000} = \frac{1200}{4000} \cdot \frac{100}{4000} = \frac{600}{4000} \cdot \frac{200}{4000} = \frac{3000}{4000} \cdot \frac{40}{4000} = \frac{2500}{4000} \cdot \frac{48}{4000}$$

=> рівність виконується.

2) Незалежність за перевагою

$$P(A_1 \cap A_2 \cap A_3 \cap A_4) = P(A_1 \cap A_2) \cdot P(A_3 \cap A_4) = P(A_2 \cap A_3)P(A_1 \cap A_4) = P(A_2 \cap A_4)P(A_1 \cap A_3) \quad (13)$$

$$\frac{30}{4000} = \frac{250}{4000} \cdot \frac{480}{4000} = \frac{300}{4000} \cdot \frac{400}{4000} = \frac{200}{4000} \cdot \frac{600}{4000}$$

=> рівність виконується.

У сценарії C_1 вразливості виявилися сумісними і незалежними, як за ймовірностями, так і за втратами. Знаходити оцінку ризику за адитивною згортокою не можна. Модифікуємо її під наш випадок (доповнимо загальними втратами від сумісних подій) 14.

$$R(c) = \sum_{i=1}^n p_i(c)w_i + \sum_{i,j=1}^n p_i(c)p_j(c)(w_i + w_j) + \dots + \prod_{i=1}^n p_i \sum_{i=1}^n w_i, \quad i \neq j. \quad (14)$$

Для C_2 (табл. 2):

1) Незалежність за корисністю

$$\frac{65}{4000} \neq \frac{3000}{4000} \cdot \frac{90}{4000} \neq \frac{2800}{4000} \cdot \frac{70}{4000} \neq \frac{900}{4000} \cdot \frac{150}{4000} \neq \frac{750}{4000} \cdot \frac{300}{4000}$$

=> рівність не виконується.

Відповідно, незалежність за перевагою теж не буде виконуватися. А тому у сценарії C_2 вразливості виявилися сумісними і залежними (тільки за ймовірностями). Модифікуємо формулу для знаходження кількісної оцінки ризику і під цей випадок 15.

$$R(c) = \sum_{i=1}^n p_i(c)w_i + \sum_{i,j=1, i \neq j}^n p_{ij}(c)(w_i + w_j) + p_{i,\dots,n}(c)(w_i + \dots + w_n). \quad (15)$$

Як було зауважено раніше, ймовірнісна залежність реалізації вразливостей в деяких випадках може проковувати залежність втрат і тоді буде присутня експертна оцінка спільних втрат замість їх суми ??.

$$R(c) = \sum_{i=1}^n p_i(c)w_i + \sum_{i,j=1, i \neq j}^n p_{ij}(c)(w_{ij}) + p_{i,\dots,n}(c)(w_{i\dots n}), \quad w_{ij} \neq w_i + w_j. \quad (16)$$

У випадку сумісних подій у нас усюди модифікована мультиплікативна форма, що підтверджує подібність з MAUT.

Для подальшого знаходження оцінки ризику необхідно з'ясувати ймовірності реалізацій вразливостей, як їх частоту ($P = N/n$, N - загальна кількість спостережень, n - кількість реалізацій подій). Для цього з допомогою формули включень-виключень знайдемо унікальні перетини реалізацій вразливостей (які не включають інші перетини) (табл. 3).

Загальна кількість спостережень:

$$C_1: \sum A_i = 3884; \sum \bigcap_i A_i = 5428.$$

$$C_2: \sum A_i = 3920; \sum \bigcap_i A_i = 5445.$$

Кінцевий етап — знаходження оцінок ризику по модифікованим формулам та порівняння результатів з оцінками по адитивній формулі (табл. 4).

Табл. 3. Унікальні реалізації вразливостей в C_1 і C_2

Вразливості	n	
	C_1	C_2
A_1	208	1855
A_2	8	1685
A_3	1938	145
A_4	1730	235
$A_1 \cap A_2$	192	515
$A_1 \cap A_3$	382	95
$A_1 \cap A_4$	190	145
$A_2 \cap A_3$	182	165
$A_2 \cap A_4$	90	25
$A_3 \cap A_4$	210	165
$A_1 \cap A_2 \cap A_3$	18	235
$A_1 \cap A_2 \cap A_4$	10	85
$A_1 \cap A_3 \cap A_4$	170	5
$A_2 \cap A_3 \cap A_4$	70	25
$A_1 \cap A_2 \cap A_3 \cap A_4$	30	65

Табл. 4. Порівняння кількісних оцінок ризиків для C_1 та C_2

	адитивн.	сумісн.+незал.	сумісн.+зал.
C_1	593,1	619,1	-
C_2	1635,1	-	1976,58

Врахувавши сумісність і можливу залежність реалізацій вразливостей, отримали більш точні, а головне коректні результати представлення ризику.

Висновки

Аналіз отриманих кількісних оцінок ризиків для різних способів їх розрахунку (адитивної форми та модифікованих мультиплікативних форм) вказує на важливість врахування сумісності вразливостей та необхідність перевірки їх на залежність/незалежність. Адже це відіграє важливу роль у коректності отриманих оцінок ризику для подальшого їх застосування.

Запропонований підхід до оцінки ризиків на основі аналізу вразливостей – новий погляд на побудову оцінок ризику, а тому новий інструмент аналізу безпеки. Проте, є сенс досліджувати й інші шляхи оцінки ризику при сумісних вразливостях (наприклад, через нечіткі та неадитивні міри).

Перелік використаних джерел

1. Качинський А. Б. Безпека складних систем / під ред. члена-кореспондента НАН України Довгого С. О. — К. : Юстон, 2017. — 498 с.
2. Вишняков Я. Д., Радаев Н. Н. Общая теория рисков. — 2 изд. — М. : Академия, 2008. — 368 с.
3. Кини Р. Л., Райфа Х. Принятие решений при многих критериях: предпочтения и замещения. — 1981. — 557 с.