УДК 004.822, 681.3, 519.81 https://doi.org/10.15407/pp2019.04.075

О.П. Ільїна, О.О. Слабоспицька

ПІДХІД ДО ПОБУДОВИ ТА ВИКОРИСТАННЯ МОДЕЛІ ПРЕДМЕТНОЇ ОБЛАСТІ РИЗИКІВ СТРАТЕГІЧНИХ РІШЕНЬ ОРГАНІЗАЦІЇ

Запропоновано концептуальну модель предметної області ризиків стратегічних рішень у системах організаційного управління (СОУ), яка є результатом операцій вибору, доповнення та інтерпретації, зумовлених специфікою відповідного об'єкту ризику, здійснених щодо елементів нормативного концептуального базису оперування з ризиками в інших сферах діяльності. Модель містить концепти: *Рішення*, *Наслідки для Рішення* і *для СОУ*, *Джерело*, *Фактор, Аспект* і *Подія ризику*, *Вразливість, Небезпечний вплив*, *Властивість, що зазнає впливу* та їх взаємозв'язки. На основі запропонованої моделі життєвого циклу стратегічного рішення та узагальнення відомих практик стратегічного управління розглянута система заходів менеджменту ризиків стратегічних рішень, поданих як дії щодо небезпечних впливів, загроз, уразливостей, об'єктів ризику та наслідків. Продемонстровано використання запропонованої концептуальної моделі при розробці методу оцінки ризиків, спричинених неоднозначністю знань, для рішень експертиз із представництвом різних ділових груп з використанням моделі «Дерево цінності». Метод ґрунтується на моделі, в якій формалізується множина факторів ризику, викликаного альтернативністю знань. Джерелами факторів є елементи постановки експертної проблеми. Види факторів є видами некогерентного співвідношення знань, вразливості пов'язані з характером дій експертів, небезпечні впливи спричиняються через використовувані системи експертних оцінок, що створюють події ризику в ході процесу життєвого циклу рішення. Кожен з аспектів ризику деталізується властивостями рішення, які є мішенями ризику внаслідок подій ризику. Метод надає оцінки ризику для висновку про задовільність експертизи та можливість вибору найменш ризикованої форми організації її процесу. Розвиток і використання запропонованої концептуальної моделі ризиків стратегічних рішень є перспективним для створення засобів підтримки процесів оборонного планування механізмами онтологічно базованого оперування досвідом щодо проблемних ситуацій та антикризових заходів.

Ключові слова: експертне прийняття рішень, стратегічне рішення, антикризова програма, менеджмент ризиків, концептуальний базис аналізу ризиків, ризик неоднозначності, дерево цінності, оборонне планування в умовах невизначеності.

Постановка та стан проблеми

Менеджмент сучасних систем організаційного управління (СОУ) має справу з множиною викликів, пов'язаних з новими умовами функціонування таких систем [1]. Серед них вирізняються:

– динамічність і значна непрогнозованість впливів зовнішнього середовища;

– ресурсна обмеженість можливостей, і, водночас, ситуативна поява непланованих шансів їх розширення (міжнародні проекти, міжгалузева кооперація тощо);

– множинність центрів відповідальності та компетентності об'єктного й функціонального профілю в структурі СОУ.

Окреме джерело викликів, критичне для створення засобів підтримки діяльності СОУ, складають такі властивості системи знань стосовно стану справ у предметній області (ПрО) цієї діяльності як неповнота, динамічність, розподіленість, слабка формалізованість та неоднозначність [2].

Характерним прикладом діяльності в системі зазначених викликів є сфера державної та міжнародної обороноздатності. Для її організацій сучасні умови створюють необхідність планування повсякденної спроможності до відповіді на максимально непередбачувані загрози, зумовивши відповідну побудову процесів управління на всіх рівнях (від стратегічного до тактичного). Для рішень стратегічного управління як факторів невизначеності виступають при цьому множинність потенційних та актуальних конфліктів і

слабка передбачуваність їх майбутньої поведінки. Водночас контексти прийняття рішень і критерії переваг для вибору варіантів дій формуються на основі знань з різних ПрО та інтенцій різних, а часто взаємопротирічних, систем інтересів. До цього додається необхідність інтегрованості окремих рішень до цілісної системи рішень СОУ, яка підлягає процедурам вирівнювання [3] та є формованою побічними впливами рішень у тій же мірі, як і цільовими.

До сучасних тенденцій належить зростання ролі рішень у моделях управління СОУ. Йдеться про концепцію організації, центрованої на рішеннях [1], і введення окремого ракурсу рішень до моделей бізнес-архітектур нарівні з ракурсом бізнес-процесів. Теорія та практика менеджменту декларують як максимальний внесок до втрати ефективності діяльності СОУ дефектів у системі прийняття рішень, насамперед повсякденних (через їх кількість і безпосередню участь у реалізації цілей) і стратегічних (через загрозу спрямування процесу діяльності в цілому).

За умов розглянутих рівня невизначеності та ціни помилки саме проблематика прийняття рішень у СОУ має бути центром розгортання менеджменту ризику [4]. Тому дещо парадоксальним видається факт відсутності розгляду рішення як самостійного об’єкта ризику в основних нормативних і методичних доробках цієї активно зростаючої галузі.

Наприклад, у сфері стратегічного оборонного планування НАТО використовується модель [5], де як об’єкт ризику розглядаються цілі, а процес планування служить потенційним джерелом ризику й розглядається інтегрально.

Водночас, з огляду на використовувані при цьому в діяльності НАТО моделі робастного прийняття рішень [6] і поєднання в портфелі рішень щодо створення спроможностей, антикризової протидії та превентивних впливів на небезпечні точки зовнішнього середовища [7], безпосереднє запровадження ризику рішень до сфери менеджменту ризиків може надати вагомий внесок до якості процесів планування. При цьому ризики рішень слід розглядати не тільки в зв’язку зі сприянням цілям СОУ, а й з іншими їх важливими властивостями [3], що мають вирішальне значення для процесу та наслідків їх виконання.

Використовуючи визначення ризику як «впливу невизначеності на цілі» [8] та сформувавши концептуальне середовище його конструктивного застосування до стратегічного рішення, можна створити підґрунтя для подальшої побудови інструментарію підтримки різних етапів процесу менеджменту ризику [4] рішень СОУ та онтологічної моделі для ведення й інтелектуального оперування щодо ретроспективи антикризових практик, як це успішно здійснюють в галузі кіберзахисту [9].

Метою роботи є побудова рамкової концептуальної моделі ПрО ризиків стратегічних рішень та її застосування до аналізу найбільш специфічного для такого об’єкта фактора ризику, пов’язаного з неоднозначністю залученого знання [2].

Для аналізу концептуальної бази розгляду ризиків різних типів, які є предметом опрацювання в основних сферах продуктивної діяльності, були використані інформативні джерела, що фіксують відповідний науковий доробок і кращі практики: індустріально апробовані міжнародні, національні й галузеві стандарти де-юре й де-факто і регламенти та публікації авторитетних фахових спільнот [10–29]. Отримані результати подані в табл. 1.

Наведені результати дозволяють стверджувати, що концептуальний базис розгляду ризиків, пов’язаних з різними об’єктами, має спільні закономірності, але й демонструє суттєві особливості, відповідні специфіці оперування ними в розглянутих сферах діяльності.

Отже, наявний досвід концептуалізації надає обґрунтування та передумови для побудови рамкової концептуальної моделі ПрО ризику стратегічних рішень.

Таблиця 1. Показові підходи до менеджменту ризиків продуктивної діяльності

Об'єкт ризику	Трактування ризику	Опис підходу		
		Назва й джерело	Ціль управління	Спеціальні поняття
Сутність, що має цілі	Вплив невизначеності на цілі [8]	Менеджмент ризику [4]	Створення та захист цінності для причетних сторін	Опис, джерело, подія, власник ризику; небезпечний чинник; уразливість; правдоподібність; наслідок; принцип, структура, процес менеджменту ризику
Організація	Можливість відхилення фактично досягнутих цілей від очікуваних зацікавленими сторонами	Стандарт Комітету спонсорських організацій комісії Тредвея (COSO ERM – Integrated Framework) [10]	Забезпечення прийнятної ефективності організації й відстеження її стратегії за допомогою внутрішнього аудиту	Корпоративна система управління ризиками; 8-етапний процес управління; «куб COSO»: цілі (стратегічні, операційні, звітування, відповідності регламентам), етапи процесу, його організаційна структура
		Стандарт Федерації європейських асоціацій ризик-менеджменту (FERMA) [11]	Узгоджене управління ризиками на стратегічному, тактичному й оперативному рівні	Ті самі, що й у [8]; внутрішній і зовнішній звіт про ризики
		AS/NZS 4360:2004 [12]	Реалізація можливостей при управління шкідливими впливами	Сприятлива можливість; контекст (управління ризиками, внутрішній, зовнішній); подія ризику, її імовірність і наслідки; рівень ризику; прийняття ризику для додавання цінності
		Управління ризиками підприємства, кероване цінністю (VDERM), J. Celona [13]	Одночасне узгоджене створення та захист цінності для всіх причетних сторін	Можливість, драйвер цінності, ризиковий апетит, системний ризик, кореляція ризиків, теплова карта ризиків, техніка аналізу рішень
		Керівництво стратегічними ризиками, J.A. Torben [14]	Проактивне прийняття стратегічних ризиків при нейтралізації загроз для додаткової цінності	Стратегічний ризик; невизначеність; прийняття ризику; ризик стратегічного рішення; організація, що приймає стратегічні ризики
Проект	Можливість відхилення стану продуктів проекту від очікуваного	Настанови PMBoK (2017 р.) і практичного стандарту PMI [15]	Стале успішне завершення проектів	Можливість, імовірність події ризику, втрати й прибуток від неї, структура декомпозиції та реєстрризиків, рівень ризику
		Неперервне управління ризиками програмного проекту, C. Alberts [16]	Стале успішне завершення проектів і вдосконалення процесу розроблення	Таксономія ризиків, відповідний їй опитувальник, твердження про ризик, граф ризиків, матрична шкала для рівня ризику
		Методологія випереджального управління загрозами й можливостями (ATOM), D. Hillson [17]	Випереджальне перетворення загроз у можливості, доступне за наявних ресурсів	Можливість, загроза, структура декомпозиції ризиків за джерелом, об'єктом і наслідками, матрична шкала для рівня ризику
		Спрощений аналіз ризиків проекту, L. Virine [18]	Стале успішне завершення проектів	Ланцюг подій ризику, джерело ризику

Об'єкт ризику	Трактування ризику	Опис підходу		
		Назва й джерело	Ціль управління	Спеціальні поняття
Інформаційний актив	Можливість спотворення активу і/або невідповідності прав доступу до нього регламентованим	Стандартизоване управління ризиками [9, 19]	Забезпечення рівня інформаційної безпеки, прийнятного для причетних сторін	Загроза, небезпечний вплив, можливість, прояв загрози, вразливість, управлінський вплив, опрацювання ризику
		Аналіз факторів інформаційного ризику (FAIR), J. Freund, J. Jones [20]	Своєчасна нейтралізація загроз, доступна на наявних ресурсів	Онтологія ризиків, актив під ризиком, подія загрози, її частота, подія ризику, частота й обсяг втрат від неї, імовірність активізації загрози, вторинний ризик
		Загальна схема кібербезпеки NIST (NCF) [21]	Усунення ризиків із запобіганням або послабленням кібератак	Кібер-атака, загроза, вразливість, актив під ризиком, управлінський вплив, аудит активів і загроз
Інвестовані кошти	Можливість неотримання очікуваного прибутку від інвестиції і/або шкоди для інвестора	Регламенти III Базельского комітету з банківського нагляду (Basel III, 2011) [22]	Забезпечення мінімального регуляторного капіталу й виконання вимог регулятора	Операційний і кредитний ризик; Вартість під ризиком (VaR), середній збиток, ліквідний VaR, показники окупності за невизначеності (RORAC, RAROC, RARORAC) [22]
		Регламенти Європейської агенції зі страхування й фахових пенсій (Solvency II, 2016) [22]	Забезпечення мінімальної припустимої маржі й виконання вимог регулятора	Те ж саме; страхування й хеджування ризиків; стресове тестування варіантів фінансових операцій
Діловий процес організації	Можливість невідповідності процесу його призначенню в діяльності організації	Стандартизоване визначення оцінок ризику процесу за профілем його зрілості [23]	Обмежена оцінюванням ризику, необхідним для прийняття управлінських рішень	Коренева причина, свідчення й тип ризику (якості продукту, поточний і майбутній організаційний ризик), рівень спроможності процесу
		Стандартизоване управління ризиками в життєвому циклі систем і програмних засобів [24]	Забезпечення рівня ризику життєвого циклу, прийнятного для причетних сторін	Подія ризику, її імовірність і наслідки, профіль ризику проекту, категорія та критерії ризику, джерело, рівень, профіль і стан ризику
Інформаційна система	Можливість відмови системи	Вимірювання й управління ризиком відмови, S.A. Sherer [25]	Забезпечення рівня ризику відмови системи, прийнятного для зацікавлених сторін	Імовірність і збиток від відмови, витрати на забезпечення надійності системи та усунення дефектів після відмов
Інформаційна технологія	Можливість невідповідності технології потребам ділових процесів	Низхідне всебічне оцінювання ризиків, пов'язаних з елементами керування в інформаційній технології (GAIT), E. Hill [26],	Обмежена виявленням критичних функцій технології й управлінських впливів, які перешкоджають підтриманню технологією потреб ділових процесів	Ризик ділового процесу, ключовий управлінський вплив, автоматизований управлінський вплив, функція інформаційної технології, недолік функції або впливу, імовірність і наслідки недоліку
		Цілі керування інформаційними й пов'язаними технологіями (COBIT'2019) [27]	Досягнення цілей керованості (APO12 у [27]) та оптимізації (EDM03) ризиків, пов'язаних з інформа-	Профіль ризику, метрика досягнення цілей керованості й оптимізації ризиків, процес оцінювання управління ризиком

Об'єкт ризику	Трактування ризику	Опис підходу		
		Назва й джерело	Ціль управління	Спеціальні поняття
			ційними технологіями	
Стратегічна ціль в оборонному плануванні	Недосягнення стратегічної цілі	Стратегічне планування, ґрунтоване на ризиках (NATO RBFSP) [5]	Розроблення й стале виконання успішної програми управління ризиками стратегічних планів з передбаченням майбутніх невизначеностей та управлінням їх впливами	Внутрішній і зовнішній контекст планування, політика управління ризиком і комунікації щодо нього, ідентифікація, аналіз, оцінювання та опрацювання ризику, матриця RBFSP (зіставлення етапів управління ризиком за ISO 31000:2009 і діяльностей зі стратегічного планування НАТО
Цільова програма /ключовий процес у критичній галузі	Наявність шкідливих наслідків і сценаріїв, що призводять до їх появи	Прийняття рішень з усвідомленням ризиків (RIDM), D.M. Gerstein [28]	Консолідація різнорідних чинників ризику, наявних у програмах NASA, для вироблення управлінських рішень	Дворівнева класифікація ризиків (чинник ризику, його компонент), граничні умови, поріг, індикатор і стратегія опрацювання для компонента ризику, імовірність і наслідки події ризику
		Управління ризиками, проблемами й можливостями в оборонних програмах, F. Kendall [29]	Забезпечення на всіх етапах оборонної програми рівня ризику, прийнятного для причетних сторін	Небажана подія або умова, її імовірність, наслідки, влив, тяжкість, проблема, сприятлива можливість, категорія ризику, твердження про ризик

Концептуальна модель менеджменту ризиків стратегічних рішень

Визначення концептуального базису для подання й аналізу ризиків рішень має ґрунтуватися на вимогах повноти врахування:

– складу та співвідношень елементів моделі таких рішень;

– методів і задач, використовуваних кращими практиками їх прийняття;

– методів менеджменту ризику, перспективних для них як для елементів процесів планування в організаційних системах.

В діяльності сучасних організаційних систем важливе місце займає клас рішень, що можуть бути визначені як випереджальні антикризові. Саме вони відіграють роль стратегічних антикризових рішень та максимально відображують парадигму організаційного управління, пов'язану з факторами динамічності, невизначеності та інтегрованості, схарактеризованими в попередньому розділі. Ці рішення складають основу антикризових програм організацій, що набули особливої уваги в галузі кіберзахисту, а також становлять центральний елемент сучасних підходів до забезпечення обороноздатності держави [30]. Таким чином, побудова концептуального базису, достатнього для розгляду ризиків випереджальних антикризових рішень, може забезпечити достатність отриманого результату для організаційних рішень у цілому.

В табл. 2 надана характеристика моделі процесу життєвого циклу (ЖЦ) випереджальних антикризових рішень, яка відображає його найбільш визначальні риси та розвиває модель, використану в попередніх дослідженнях систем рішень організації [31].

Розгляд поданих характеристик процесу дозволяє дійти таких висновків.

1. Процес характеризується високим ступенем партисипативності, вимагаючи здійснення комунікації представників різних професійних точок зору на об'єкт планованого впливу та інтеграції суджень представників таких точок зору. Це створює ризик так званої неоднозначності (ambiguity) [2], зумовлений різницею в си-

стемах характеристик об'єктів та їх зв'язків, що відповідають досвіду професійної діяльності учасників процесу.

2. Повнота знань і даних стосовно ПрО рішення включно з повнотою представництва всіх професійних поглядів та інтересів є специфічним джерелом ризику.

3. Багато-вимірність впливів, які справляє рішення на діяльність СОУ, обумовлює багато-вимірність ризику, який має розглядатися в зв'язку з ним.

4. Множинність, різнотиповість і складність структури системи взаємозв'язків між елементами моделі різних етапів процесу, разом із комплексними впливами цих елементів на ризики, вимагають забезпечення засобів їх відображення в концептуальній моделі ризиків.

5. Високий рівень позатиповості та нестандартності випереджальних антикризових рішень разом із принциповою непередбачуваністю цілого спектру характеристик проблемних ситуацій призводить до потреби формування оцінок ризиків на ґрунті систем гіпотез щодо перебігу подій та з використанням відносного зіставлення ризиків варіантів замість стандартного використання ймовірностей настання й розмірів шкоди подій ризику для абсолютної оцінки ризику варіанта.

Таблиця 2. Принципові характеристики процесу ЖЦ випереджальних антикризових рішень

Етап	Виконувані дії	Учасники й джерела інформації	Результат
1. Аналіз пропроблемної ситуації	Виявлення й формалізація базового конфлікту Аналіз співіснуючих конфліктів Аналіз загрози впливу на цілі й цінності СОУ Побудова сценаріїв розвитку ситуації	ОПР (за сферами відповідальності) Експерти (за сферами компетентності) Базові сценарії	Модель конфлікту Сценарії граничних варіантів розвитку Оцінки впливу
2. Вибір цілі впливу на проблемну ситуацію	Вибір та обґрунтування ступеню впливу на базовий конфлікт Вибір мішеней впливу Аналіз наявних і доступних засобів	Фахівці: з актуальних загроз, з процесів планування, з забезпечуючої сфери, з зовнішніх зв'язків Носії інтересів, поставлених під загрозу Моделі оцінки загроз	Об'єкти, напрямки та рівні обраних впливів Принципові вимоги до забезпечення Вимоги до очікуваних результатів
3. Вироблення та первинний аналіз варіантів дій	Добір та інтеграція базових заходів для досягнення цілі Виявлення потенційних перешкод в досягненні цілі Побудова сценарного простору з урахуванням варіації факторів перешкод Аналіз стійкості запропонованих варіантів у сценарному просторі [6,7]	Фахівці в цільовій сфері «Червоні команди» [6,7] експертів Інформація щодо стану справ, засоби сценарного аналізу та критерії відсіву варіантів	Множина альтернативних варіантів з їх обґрунтуванням
4. Вибір варіанта	Формування та узгодження складу й структури моделі вибору Формування моделі та складу експертних груп Експертне оцінювання Інтеграція та узгодження експертних оцінок	Фахівці з обраних заходів Експерти з базових аспектів оцінки варіанта Стейкходери Рамкові моделі цінності	Обґрунтований варіант вибору
5. Підготовка до ви-	Планування заходів Розподіл відповідальностей і повноважень	Відповідні служби СОУ Діючі регламенти Наявні канали	План заходів Інструкції з виконання плану

Етап	Виконувані дії	Учасники й джерела інформації	Результат
конання	Розробка й планування системи допоміжних заходів Висунення вимог до документації, базових комунікацій і каналів інформування		заходів Склад і правила документообігу Інструкції з комунікацій
6.Аналіз результатів	Перевірка відповідності вимогам етапу 2 Аналіз виявленого рівня задовільності виконаного АВР для оперативної антикризової діяльності Анкетування учасників щодо вузьких місць процесів діяльності та пропозицій Корекція та актуалізація елементів моделі процесу	ОПР Аналітики з антикризового управління Учасники ділових процесів Стейкхолдери	Оцінка виконання Актуалізовані результати попередніх етапів Висновки стосовно змін в умовах і моделях випереджального антикризового управління.

Як концептуальний базис для розгляду організаційних рішень, що враховує зазначені особливості, може бути взята понятєва основа стандарту [8]. Введення додаткових концептів і взаємозв'язків, а також інтерпретація щодо ПрО стратегічних рішень здійснювалися з використанням підходів [5, 9]. Пропонована система концептів має структуру, показану на рисунку.

Концепти позначено як *E* з номерами, в той час як дуги *R* з номерами ідентифікують зв'язки між ними з такою семантикою:

*R*1 – «…має елемент, що виступає в якості…»;

*R*2 – «…породжує…»;

*R*3 – «…характеризує…»;

*R*4 – «…належить до … як елемент деталізації »;

*R*5 – «…змінює стан…»;

*R*6 – «…включає … до сфери впливу…», де знак … позначає концепт у початковій або кінцевій вершині дуги *R*.

*Об'єкт ризику E*3 – це організаційне рішення, що розглядається у вигляді п'яти-етапної структури його ЖЦ, охарактеризованої в табл. 1, та пов'язаних з

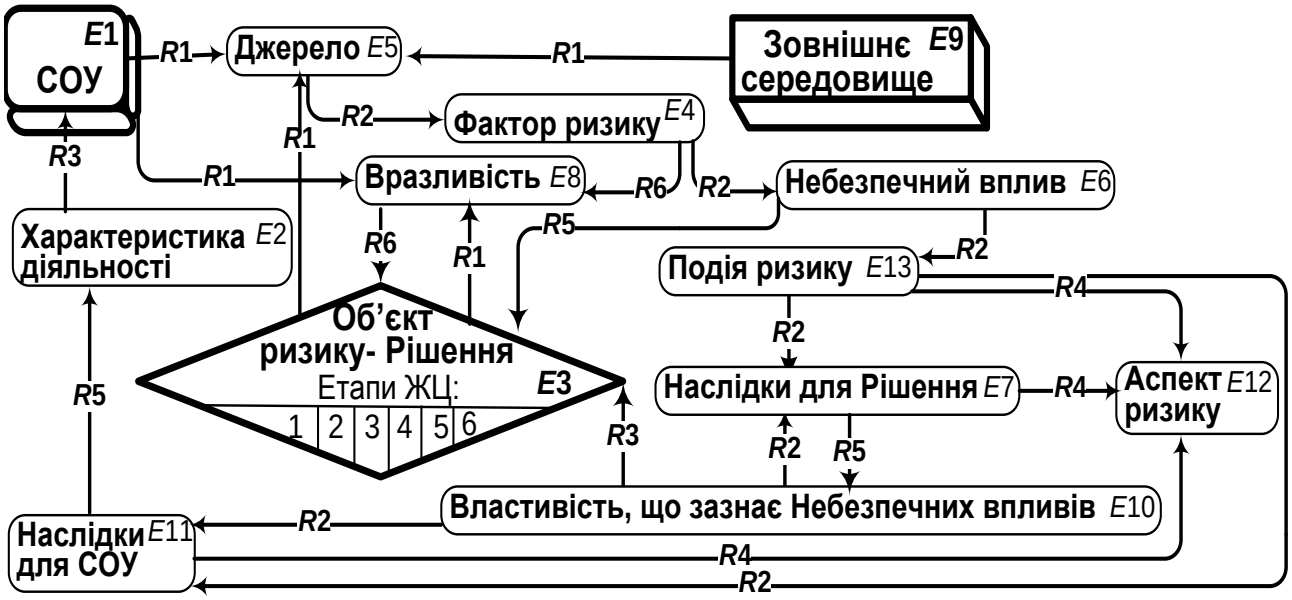

Рисунок. Структура концептуальної моделі ПрО ризиків стратегічних рішень

ним властивостей, що визначають його процесну якість і положення в системі рішень організації [32]. *Властивості* $E10$ становлять підмножину Властивостей рішення, зміна значень яких з наближенням до виділених критичних значень або з виходом за межі виділеної області прийнятності надає первинну характеризацію ризиків.

Безпосередніми маркерами ризиків слугують *Наслідки* $E7$ та $E11$ *Подій ризику* $E13$, рівень тяжкості (а також прийнятності та істотності) яких може бути оціненим на основі значень Властивостей $E10$ і Характеристик діяльності СОУ $E2$. У виродженому випадку $E7$ може співпадати з $E10$, а $E11$ – з $E2$.

Аспекти ризику $E12$ становлять базові функціональні та ціннісні виміри, за якими розглядається організаційне рішення як центральний елемент СОУ. Кожний з таких аспектів характеризується актуальними для нього елементами $E7$ та $E11$ як своїми складовими, а також подіями ризику $E13$, що спричиняють зміни їх значень.

Фактор ризику $E4$ становить властивість, притаманну об'єкту, який служить його *джерелом* $E5$ і належить до Зовнішнього середовища $E9$ (*зовнішній* фактор) або до елементів СОУ $E1$, безпосередньо пов'язаних із процесом ЖЦ рішення $E3$, чи до його характеристик, виступаючи в ролі *внутрішнього* фактору. Фактор характеризується значенням рівня його прояву, що визначає активізацію пов'язаного з ним *Небезпечного впливу* $E6$ при перевищенні критичного рівня. Характеризується також множиною *Вразливостей* $E8$, які уможливлюють та посилюють його вплив.

Небезпечний вплив $E6$ характеризується, крім породжуючого його фактору, множиною елементів рішення $E3$, на стан яких може впливати (зокрема, при наявності відповідних Уразливостей $E8$) і *Подіями ризику* $E13$, які змінюють стан Об'єкту ризику. Якщо Небезпечний вплив може бути пов'язаний із суб'єктами Зовнішнього середовища або СОУ, інтереси яких виступають у ролі Джерела $E5$ для відповідного Фактора ризику $E4$, він має тип *Загрози* та може додатково характеризуватися стадією свого розвитку. Обов'язковою характеристикою є *Рівень впливу*, що є суттєвим при оцінці Наслідків $E7$ та $E11$.

Подія ризику $E13$ визначається як зміна стану Об'єкту ризику $E3$, що спричиняє Наслідки $E7$ та $E11$. Рівень її значущості залежить від їх рівнів тяжкості. Подія ризику належить до сфери певного Аспекту ризику $E12$.

Крім розглянутих концептів, для побудови моделей менеджменту ризиків рішень зручно ввести комплексні концепти, що характеризують поточну ситуацію, яка має місце в ЖЦ окремого рішення.

Перший з них являє собою *Ситуацію небезпеки* з моделлю

$$SH = \{\langle E4^{*}_{i}, E5_{i}\rangle, SE8_{i}, \{E6_{ij}^{**}, j=1,...,N_i\}, i=1, ...,M\}, \quad (1)$$

а другий – Ситуацію ризику з моделлю

$$SR = \{E6_{ij}^{**}, SE10_{ij}, SE13_{ij}^{***}, \{E12_{ijk}^{***}, SE7_{ijk}^{***}, SE11_{ijk}^{***}, k=1,...,K_{ij}\}, j=1,...,N_i, i=1, ...,M\}, \quad (2)$$

де $E4^{*}_{i}$ – i-й актуалізованй фактор ризику з джерелом $E5_i$;

$SE8_i$ – множина наявних уразливостей, що сприяють впливу фактора $E4^{*}_{i}$;

$E6_{ij}^{**}$ – j-й небезпечний вплив, створюваний фактором $E4^{*}_{i}$;

N_i і M – кількості створюваних впливів та актуалізованих факторів;

$SE10_{ij}$ – множина властивостей рішення з критичними значеннями;

$SE13_{ij}^{***}$ – множина ініційованих подій ризику;

$E12_{ijk}^{***}$ – k-й актуальний аспект ризику;

$SE7_{ijk}^{***}$, $SE11_{ijk}^{***}$ – множини актуальних наслідків, що його репрезентують.

Далі продемонстровано приклади елементів, що здійснюють репрезентацію концептів $E4$, $E7$, $E12$.

В табл. 3 наведено основні аспекти ризику організаційних рішень і наслідки небезпечних впливів, пов'язані з ними, –

представлені у вигляді властивостей рішення, що складають відповідні мішені для таких впливів.

Таблиця 3. Мішені дії небезпечних впливів у складі аспектів ризику

Аспект ризику	Мішень дії небезпечного впливу
Результативність процесу вироблення (*AR*1)	Завершеність процесу (*TR*1.1) Збереження області застосування постановки (*TR*1.2) Якість (*TR*1.3) Своєчасність ухвалення (*TR*1.4) Вписуваність в систему процесу управління (*TR*1.5) Повторна використовуваність (*TR*1.6)
Здійснимість (*AR*2)	Забезпеченість ресурсом (*TR*2.1) Ефективність роботи команди виконавців (*TR*2.2) Задоволення нормативно-правових вимог (*TR*2.3) Своєчасність виконання (*TR*2.4) Здатність до адаптації щодо умов виконання (*TR*2.5)
Ефективність (*AR*3)	Прийнятність співвідношення вигоди/витрати (*TR*3.1) Конкурентоспроможність забезпечуваного ефекту (як послуги або продукції) (*TR*3.2) Скомпенсованість негативних впливів (*TR*3.3)
Прийнятність для стейкхолдерів (*AR*4)	Відповідність досягнутої вигоди очікуванням (*TR*4.1) Збереження балансу між інтересами різних стейкхолдерів (*TR*4.2) Забезпечення довір'я стейкхолдерів до дотримання їх інтересів (*TR*4.3)

В табл. 4 наведена рамкова структура груп факторів ризику з джерелами зі складу зовнішнього середовища, СОУ та системи знань, використовуваних на етапах процесу ЖЦ рішення.

Схарактеризовані основні фактори ризику, які створюють небезпеки для властивостей організаційного рішення, що є їх мішенями в аспектах *AR*1–*AR*4. Запропонована рамкова ієрархічна структура цих чинників орієнтована на можливість оцінки й моделювання подій і ризиків у зв'язку з індикаторами стану середовища та на вироблення й аналіз заходів менеджменту ризику.

Таблиця 4. Рамкова структура груп факторів ризику

Група факторів	Структура та склад групи
Фактори з джерелом у зовнішньому середовищі	Невизначеність проявів *F*1.*i*.1 Мінливість значень*F*1.*i*.1.1 Непоінформованість *F*1.*i*.1.2 Нестабільність впливів *F*1.*i*.2 Залежність від інших зовнішніх чинників *F*1.*i*.2.1 Залежність від внутрішніх параметрів організації *F*1.*i*.2.2 Залежність від стану об'єкту ризику *F*1.*i*.2.3 Керованість *F*1.*i*.3 Регістрованість *F*1.*i*.3.1 Компенсованість *F*1.*i*.3.2
Фактори з джерелом у внутрішній структурі й діяльності СОУ	Стан системи цілей*F*2.1 Невизначеність *F*2.1.1 Несинхронізованість *F*2.1.2 Ресурсна несумісність *F*2.1.3 Неінтегрованість *F*2.1.4 Ресурсний потенціал *F*2.2 Недостатність *F*2.2.1 Недоступність *F*2.2.2 Невигідність *F*2.2.3 Структура *F*2.3 Функціональна неадекватність *F*2.3.1 Неадаптивність *F*2.3.2 Надмірність і дубльованість *F*2.3.3 Технології *F*2.4 Механізми управління *F*2.5 Нерозподіленість і нефіксованість відповідальності *F*2.5.2 Некоординованість *F*2.5.3 Неінтегрованість цілей процесів *F*2.5.1 Неконтрольованість якості *F*2.5.4 Непідтриманість взаємодії *F*2.5.5 Неефективність зворотних зв'язків *F*2.5.6
Фактори з джерелом у системі використовуваного знання	Неформалізованість *F*3.1 Неалгоритмізованість *F*3.1.1 Невизначеність експертних ресурсів *F*3.1.2 Несистематизованість досвіду *F*3.1.3 Неповнота *F*3.2 Концептуальна *F*3.2.1 Інформаційна*F*3.2.2 В частині методологій застосування *F*3.2.3

В табл. 5 розглянуто можливості здійснення функцій менеджменту ризиків за рахунок заходів із впливу на об'єкти запропонованої концептуальної моделі.

Дії з менеджменту ризиків рішень СОУ, розглянуті в табл. 5, та способи їх реалізації гармонійно сполучені з моделлю Стратегічного планування, ґрунтованого на ризиках (SPRBF) [5]. Детальний розгляд наведених в табл. 5 способів реалізації необхідних впливів та виміру «Техніки» моделі SPRBF дозволяє виокремити множину технік, актуальних для таких впливів. Вона включає класи експертних методів, системно-аналітичних технік, схем планування та організаційного аналізу. Всі вони потребують, для свого використання в конкретній предметній області, аналізу тих зв'язків та властивостей, які використані в розглянутій концептуальній моделі та можуть поповнюватися надалі, при збереженні її когерентності.

В наступному розділі наведено приклад використання запропонованої концептуальної моделі для задач менеджменту ризиків, спричинених фактором неоднозначності використовуваних знань [2].

Таблиця 5. Цілі та заходи здійснення менеджменту ризиків рішень СОУ в середовищі концептуальної моделі

Тип об'єкту впливу	Здійснюваний цільовий вплив на об'єкт	Спосіб реалізації
Небезпечний вплив (загроза)	Безпосередня протидія	Перспективне створення засобів Використання штатних засобів Ситуативний пошук підходів у ретроспективі процесів прийняття рішень
	Зниження стадії розвитку загрози	Моніторинг з метою ранньої діагностики Випереджуючі дії Досягнення компромісу конфліктних інтересів Зміна балансу сил (залученням ресурсів, створенням кооперацій та ін.
	Послаблення чи нейтралізація джерела фактору ризику	Випереджувальний вплив на зовнішнє джерело за рахунок участі в процесах зовнішнього середовища Вплив на внутрішні процеси СОУ, актуальні для об'єкту – джерела фактору
Вразливість	Захист об'єкту – носія вразливості від актуальних негативних впливів	Використання штатних засобів Ситуативний пошук можливостей
	Заміщення об'єкту – носія в складі ділових процесів, які визначають критичні властивості рішення	Створення альтернативних об'єктів та маршрутів Використання штатних альтернатив
	Зміна сценаріїв та маршрутів функціонування об'єкту носія в ділових процесах виконання рішення	Створення сприятливих умов (ресурси, партнерська участь, додаткове інформування) Використання рамкових альтернатив Ситуативне використання прецедентів
Рішення (як об'єкт ризику)	Забезпечення повноти залучення знань у процесі прийняття рішення	Побудова ефективного розподіленого процесу (розподіл відповідальностей, регламентація взаємного інформування) Використання ретроспективної інформації та пошук аналогів Побудова та актуалізація сценарного простору, що визначає умови та

Тип об'єкту впливу	Здійснюваний цільовий вплив на об'єкт	Спосіб реалізації
		небезпечні впливи при виконанні рішення Створення профільних експерт них команд (поточного аналізу, багатоаспектної інтеграції, пошуку вузьких місць і перешкод та ін.)
	Забезпечення готовності до змін	Створення універсального та взаємосумісного набору можливостей Розробка рамкових антикризових програм Створення моделей багатокритеріального та робаст- ного до потенційних перешкод вибору варіантів дій Реалізація ітеративних та рефлексивних схем процесів прийняття рішень Ведення, актуалізація та наскрізне використання системи пріоритетів Аргументоване виведення висновків із отриманих результатів та їх конструктивне збереження
	Підтримка інтегрованості рішення	Ведення моделі та аналіз стану системи рішень СОУ Створення інтегральних контекстів для експертиз Реалізація багатокритеріальних та портфельних підходів
Наслідки ризику	Відвернення	Передбачення та моніторинг побічних наслідків рішень Вибір варіантів дії за принципом робастності до змін середовища Ресурсне забезпечення рішень, адекватне пріоритетності об'єктів їх впливу
	Протидія	Розробка і реалізація рамкових заходів Ситуативне використання можливостей СОУ Використання досвіду прецедентів Залучення зовнішніх можливостей
	Післякризова стабілізація	Планування та використання заходів та ресурсів для відновлення діяльності об'єктів та системи в цілому Модифікація моделей та сценаріїв діяльності на грунті винесених висновків

Оцінка ризиків, спричинених неоднозначністю, для рішень експертиз із представництвом різних ділових груп

Для рішень, розглянутих у перших розділах, характерна риса – це потреба в використанні розподілених та частково альтернативних знань відносно проблемної ситуації, а також властивостей та наслідків заходів з її розв'язання.

Запропонована раніше [32] методологія комплексної експертно-аналітичної підтримки формування та ведення систем рішень відповідних СОУ виводить на перший план у задачах менеджменту ризику підклас внутрішніх факторів альтернативності знань, джерелом яких є елементи розв'язуваної експертної проблеми. При цьому види факторів є видами некогерентного співвідношення знань, вразливості пов'язані з характером дій експертів, небезпечні впливи спричиняються через використовувані системи експертних оцінок, що створюють події ризику в ході процесу життєвого циклу рішення. Кожен з аспектів ризику деталізується властивостями рішення, які є мішенями ризику внаслідок подій ризику.

Запропонований метод оцінки відповідних ризиків, орієнтованої на такі проблеми їх менеджменту як моніторинг динаміки ризиків у системі рішень СОУ та вибір сприятливих методів реалізації процесу їх прийняття, демонструє можливості використання концептуальної моделі, описаної у попередньому розділі.

Будемо розглядати модель задачі прийняття рішення *TS*

$$TS = <PS, G, \{A\}, P, ST, NI, MP>, \quad (3)$$

де *PS* – проблемна ситуація, *G* – ціль дії щодо неї, *A* – альтернативний захід для реалізації *G*, *P* – доступний потенціал виконання, *ST* – поточний стан системи рішень організації [32], *NI* – можливі негативні

наслідки, *MP* – модель переваг [33] для оцінки перспективності альтернатив.

Кожний елемент *E* з (3) є структурою концептів *C*, що характеризуються своїми онтологічними визначеннями

$$Def\,(C) = \{X, R\}, \qquad (4)$$

де *X* – концепти, які визначають склад і властивості *C*; *R* – відношення, що пов'язують *C* і *X*.

Множина актуальних для *TS* точок зору {*VP*} відповідає діловим групам і стейкхолдерам організації і характеризується онтологічно множиною O (VP*)* своїх версій *Def*. Багатокритеріальна ієрархічна модель [33] *MP* із (3) включає, на першому рівні, систему ракурсів, що розкривають показник переваги варіанта рішення

$$AMP = <R, AC, F, AP>, \qquad (5)$$

де *R* – результативність для вирішення *PS*, *AC* – досяжність цілі *G*, *F* – здійсненність заходу, *AP* – прийнятність і можливість усунення наслідків.

Конструктивним для розв'язання задачі (3) є застосування, як формального подання *MP* з (3), додатково розвинутого апарату моделі Дерево цінності [33]. Він включає: механізми онтологічної аргументованості взаємозв'язків критеріїв, продукційні правила виведення рекомендацій з управління та спеціальні методи інтеграції і узагальнення оцінок [33].

Залучена до експертизи *VP* реалізує відображення свого фахового досвіду в оцінках, які надає для варіанта рішення, за допомогою оцінювання системи часткових критеріїв, що деталізують аспекти з (5):

$$CR\,(VP, R) = \psi_{VP}\,(G, PS),\ CR\,(VP, AC) = \psi_{VP}\,(G, A, ST),$$
$$CR\,(VP, F) = \psi_{VP}\,(A, P),\ CR\,(VP, AP) = \psi_{VP}(A, ST, NI), \qquad (6)$$

де *CR* – множина критеріїв, що представляють аспект; ψ – функція формування складу множини критеріїв та їх оцінок на підставі фахових знань про елементи (3).

Це визначає альтернативність експертного знання про елементи (5) при залученні множини *VP* до прийняття рішення (3).

Використання в постановці задачі для експертів єдиної моделі *MP* є поширеною практикою. Застосування вище охарактеризованого подання *MP* служить при цьому: забезпеченню підстав для інтеграції оцінок різних експертів; використанню проміжних рівнів ієрархії критеріїв для формування рекомендацій і класифікації альтернатив [33]; аналітичному використанню оцінок за межами даної експертизи і повторному використанню постановки задачі при оцінюванні рішень даного класу.

Проте відмінності між складом *MP* в (3) і результатами (6) призводять до можливості однієї з ризикованих форм *W* поведінки представників *VP* в експертизі:

– відмови від оцінювання критерію (W_1);

– оцінювання наданих критеріїв з викривленням професійних уявлень (W_2);

– оцінювання часткових критеріїв з «підгонкою» під оцінку інтегрального, яка відображає професійні пріоритети (в реальності зумовлені іншими аргументами) (W_3).

Такі форми поведінки експертів складають вразливості системи експертних оцінок, які роблять її чутливою до відмінностей інтерпретації елементів постановки задачі різними *VP*.

Розглянемо модель ризиків рішення, що приймається за таких умов. Вона має вигляд

$$MR=(\{AR_i, \{TR_{ij}, \{TRR_{ijk}(T, FC, SR)\}_{k=1,Kj}\}_{j=1,Ji}\}_{i=1,\ldots,4}, TT), \qquad (7)$$

де *AR* – аспект ризику рішення (див. табл. 3); *TR* – мішень ризику в межах аспекту (властивість рішення, порушення якої є одним із підаспектів ризику); *TRR* – небезпечний вплив, що викликає подію ризику, має тип *T* і продукується фактором ризику *FC* з джерелом *SR* (елемент (5)); J_i – число мішеней ризику в аспекті; K_j – число загроз, актуальних для мішені; *TT* – множина типів небезпечних впливів. Множина *TT* включає такі дефекти системи індивідуа-

льних експертних оцінок: T_1 – неповноту поданості в оцінці аспектів з (5); T_2 – невідповідність оцінки інтегрального критерію переваг фаховому досвіду; T_3 – невідповідність оцінки часткових критеріїв фаховому досвіду; T_4 – незіставність оцінок для процедур інтеграції й логічного виведення рекомендацій; T_5 – непереконливість для інших точок зору.

Ситуація небезпеки має модель

$$MSR=\langle TSR,CB,\{CST(V_i,V_j),FC,W(V_j)\}\rangle, \quad (8)$$

де TSR – тип джерела фактора ризику (R, AC, F, AP з (3)); CB – концептуальний базис небезпечного впливу (підмножина елементів з правої частини виразу (6) для TSR); $CST(V_i,V_j)$ – конфліктний елемент: концепт C, для якого

$$C\in E\,|\,(E\in CB)\wedge Def(C,V_i)\neq Def(C,V_j);$$

фактор ризику FC – одна з п'яти форм альтернативного співвідношення визначень C; $W(V_j)$ – форма поведінки представника точки зору V_j в ситуації при оцінюванні.

$$FC_1.\quad \exists X\,|\,X\in(O(VP_i),O(VP_j))\wedge$$
$$\wedge X\in Def(C,VP_i)\wedge X\notin Def(C,VP_j);$$

$$FC_2.\quad \exists X\,|\,X\in O(VP_i)\wedge X\notin O(VP_j)$$
$$\wedge X\in Def(C,VP_i)\wedge\neg\,\underline{UND}(X,\mathrm{VP}_i,VP_j),$$

де $\underline{UND}$ – відношення розуміння [32];

$$FC_3.\quad \exists X\,|\,(X\in O(VP_i)\wedge X\notin (O(VP_j))\wedge$$
$$\wedge X\in Def(C,VP_i)\wedge \underline{UND}(X,VP_i,VP_j)\wedge\neg\,\exists Z\,|$$
$$(Z\in VP_j)\wedge \underline{CONTR}\,(TR(X,VP_i,VP_j),Z), \quad (9)$$

де $\underline{CONTR}$ – відношення суперечності [32], $TR(X,VP_i,VP_j)$ – образ X в $O(VP_j)$;

$$FC_4.\quad \exists X\,|\,(X\in O(VP_i)\wedge X\notin (O(VP_j)\wedge$$
$$\wedge X\in Def(C,VP_i)\wedge \underline{UND}\,(X,\mathrm{VP}_i,VP_j)\wedge\exists Z\,|$$
$$(Z\in VP_i)\wedge \underline{CONTR}\,((TR\,(TR\,(X,VP_i,VP_j),$$
$$VP_j,VP_i)),Z);$$

$$FC_5.\ \exists X_1\,|\,(X_1\in O(VP_i),O(VP_j))\wedge X_1\in$$
$$\in Def(C,VP_i)\wedge\exists X_2\,|\,(X_2\in O(VP_i),(O(VP_j))\wedge$$
$$\wedge X_2\in Def\,(C,VP_j))\wedge \underline{CONTR}\,(X_1,X_2).$$

Кожен тип небезпечних впливів T визначено диз'юнкцією варіантів (FC, W).

$$T_1.\quad (FC_1,W_1)\vee(FC_2,W_3)\vee(FC_5,W_1);$$

$$T_2.\ (FC_1,W_2)\vee(FC_2,W_2)\vee(FC_4,W_2)\vee(FC_4,W_3)\vee$$
$$\vee(FC_5,W_2)\vee(FC_5,W_3); \quad (10)$$

$$T_3.\ (FC_1,W_3)\vee(FC_2,W_3)\vee(FC_4,W_2)\vee(FC_4,W_3)\vee$$
$$\vee(FC_5,W_2)\vee(FC_5,W_3)\vee(FC_3,W_2))\vee<FC_3,W_3);$$

$$T_4.\ (FC_4,W_2)\vee(FC_4,W_3)\vee(FC_5,W_2)\vee(FC_5,W_3);$$

$$T_5.\ (FC_2,W_2)\vee(FC_2,W_3)\vee(FC_4,W_2)\vee(FC_4,W_3)\vee$$
$$\vee(FC_5,W_2)\vee(FC_5,W_3).$$

Ґрунтуючись на моделі ризику (7), можна запропонувати оцінку його рівня для рішення, що приймається в постановці задачі (3), із залученням представників заданої множини $\{VP\}$, для яких є виявленою – апріорно або в рамках експертизи, онтологічна специфікація концептів постановки задачі.

Для кожного з 20 елементів множини $GTRR$ можливих небезпечних впливів $TRR_{ij}(T_i,SR_j)$ оцінюється значущість EMT_{ij} з урахуванням всіх актуальних для нього конфліктних елементів CST_{ij} (див. (8)).

Нехай NVP – загальне число залучених точок зору, NT – число їх різних пар.

Значущість конфліктного елемента $CST_{ijr}(V_{L1},V_{L2})$, актуального для небезпечних впливів $TRR_{ij}(T_i,SR_j)$ у зв'язку з r-ю парою точок зору (V_{L1},V_{L2}), $r \le NT$, має вигляд

$$EMC_{ijr} = H \sum_{w\in Wa} P(w) / |W_a|, \quad (11)$$

де $P(w)$ – імовірність реакції у формі $w\in W_a$ на ситуацію, утворювану конфліктним елементом, з боку точки зору, що включає більш інформативне визначення CST; $H\in(0,1)$ – усереднений для V_{L1},V_{L2} рівень актуальності знань про концепт CST; W_a – множина форм реакції, актуальних для типу небезпечного впливу T_i (див. (10)).

Тоді значущість небезпечного впливу TRR_{ij} можна визначити як

$$E(TRR_{ij}) = \sum_{r=1}^{NT} \sum_{j=1}^{Nir} EMC_{ijr} / K_j \cdot NT,$$

де K_j – кількість концептів у визначенні SR_j з (6); Nir – число CST_{ijr}, актуальних для TRR_{ij}; NT – число пар точок зору.

Позначимо $ACT_S \in GTRR$ підмножину небезпечних впливів TRR_{ij}, актуальних для мішеней аспекту ризику AR_S (див. (7)). Тоді оцінку рівня ризику за цим аспектом, $RL_S \in (0,1)$, може визначити як

$$RL_S = \sum_{TRR_{ij} \in ACT_S} E(TRR_{ij}) / \left| ACT_S \right|.$$

На основі запропонованих оцінок ризику може визначатися рейтинг елементів системи рішень СОУ та задовільність окремого рішення в порівнянні з результатами кращих і гірших практик.

Число форм співвідношення (9) може бути розширено такою формою як вилученість концепту з визначень в одній або обох точках зору, з урахуванням рівня актуальності знань про нього (див. (11)). Пов'язавши цю форму з типами небезпечних впливів в рамках умов (10), можна використати запропонований підхід для вибору процедур управління ризиками рішень, пов'язаних з альтернативністю знань (вилучення суперечностей з постановки задачі, включення компромісної версії моделі цінності, звуження кола точок зору, що залучаються тощо).

Висновки

На ґрунті аналізу світового досвіду побудови концептуального базису менеджмента ризику в різних сферах діяльності була створена рамкова концептуальна модель предметної області ризиків для стратегічних рішень, які характеризуються запропонованою моделлю життєвого циклу, в сучасних системах організаційного управління.

Розглянуто основні аспекти ризику та властивості процесу життєвого циклу рішення – мішені дії небезпечних впливів у складі кожного з аспектів. Схарактеризовано основні групи факторів ризику.

Запропоновано подання цілей і заходів менеджменту ризиків як цільових впливів, що здійснюються для об'єкту концептуальної моделі, за допомогою засобів, характерних для сучасного антикризового управління та стратегічного планування за умов високого ступеню невизначеності (з залученням моделей робастного оборонного планування).

Показано використання запропонованої концептуальної моделі для аналізу й оцінки ризиків рішення, спричинених дією фактора неоднозначності розподілених знань при використанні прийнятої для стратегічних рішень експертної процедури оцінювання за Деревом цінності.

Планується подальше використання та розвиток результатів для створення моделей і засобів онтологічної підтримки ведення й використання знань стосовно проблемних ситуацій і добору антикризових заходів, базованому на ризиках рішень оборонного планування.

Література

1. Blenko M.W., Mankins M., Rogers P. The Decision-Driven Organization. Harvard Business Review. 2010. Is. 6. [Electronic resourse]. Mode of access: https://hbr.org/2010/06/the-decision-driven-organization.
2. Renn O. Coping with complexity, uncertainty and ambiguity. The risk governance approach. NSF-DFG Joint Risk Meeting, Washington, D.C., Oct. 3-5, 2012. 33 p.
3. Pisano G.P. Creating an R&D Strategy. 2012. [Electronic resourse]. Mode of access: http:www.hbs.edu/facultyPublication%20Files//12-095_fb1bdf97-e0ec-4a82-b7c0-42279dd4d00e.pdf.
4. ISO 31000:2018 Risk management – Guidelines. 16 p.
5. Analysis Support Guide for Risk-Based Strategic Planning. Technical Report STO-TR-SAS-093-Part-I – 2018, STO/NATO. 156 p.
6. Lempert R.J., Warren D., Henry R. et al. Defense Resource Planning Under Uncertainty. An Application of Robust Decision Making to

Munitions Mix Planning. RAND Corporation, 2016. 109 p.
7. Johnson S., Libicki M., Treverton G.F. New challenges, new tools for defense decisionmaking. MR-1576, RAND Corporation, 2003. 408 p.
8. ISO Guide 73:2009 Risk management Vocabulary. 15p.
9. ISO 27000:2018 Information technology – Security techniques. Information security management systems. Overview and vocabulary. 34 p.
10. Enterprise Risk Management – Integrating with Strategy and Performance. Executive Summary. COSO, 2017. 16 p. [Electronic resourse]. Mode of access: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.
11. FERMA Risk Management standard – FERMA, 2002. 16 p. [Electronic resourse]. Mode of access: // http://www.ferma.eu/.
12. Australia/New Zealand AS/NZS 4360:2004 Risk management /Standards Australia. 65 p.
13. Celona J., Hall E., Driver J. Value-Driven ERM: Making ERM an Engine for Simultaneous Value Creation and Value Protection. *J. of healthcare risk management: the journal of the American Society for Healthcare Risk Management*. 2011. N 30(4). P. 15–33.
14. Torben J.A., Garvey M., Roggi O. Managing Risk and Opportunity. The Governance of Strategic Risk-Taking. Oxford University Press, 2014. 204 p.
15. Practice Standard for Project Risk Management. *Project Mnagement Institute*, Inc., 2009. 128 p.
16. Alberts C., Dorofee A., Marino L. Executive Overview of SEI MOSAIC: Managing for Success Using a Risk-Based Approach. Technical Note CMU/SEI-2007-TN-008, 2007. 33 p.
17. Hillson D.A., Simon P.W. Practical project risk management: The ATOM Methodology (2nd ed.). Vienna, US: Management Concepts, 2012. 410 p.
18. Virine L., Trumper M. Project Risk Analysis Made Ridiculously Simple. World Scientific Publishing Co. Pte. Ltd., 2017. 283 p.
19. ISO 27005:2018 Information technology – Security techniques – Information security risk management. 56 p. [Electronic resourse]. Mode of access: https://www.iso.org/standard/75281.html.
20. Freund J., Jones J. Measuring and Managing Information Risk. A FAIR Approach. Elsevier, 2015. 391 p.
21. Офіційний сайт NIST CyberSecurity Framework. [Electronic resourse]. Mode of accesshttps://www.nist.gov/cyberframework.
22. Grouhy M., Galai D., Mark R. The Essentials od Risk Management. McGraw-Hill Education, 2014. 669 p.
23. ISO/IEC PDTR 33015.3:2019 Information technology – Process assessment – Guide to process risk determination. 41 p.
24. ISO/IEC 16085:2006 Systems and software engineering – Life cycle processes – Risk management. 34 p.
25. Sherer S.A., Alter S. Information Systems Risks and Risks Factors, are they Mostly about Information Systems? Communications of AIS 2004. Vol. 14. N 1. P. 29–64.
26. GAIT for IT General Control Deficiency Assessment. The Institute of Internal Auditors. [Electronic resourse]. Mode of access: https://www.iiacolombia.com/resource/guias/GAIT_GeneralControl.pdf. 25 p.
27. COBIT'2019 Framework. Governance and Management Objectives – ISACA, 2018. 302 p.
28. Gerstein D.M. et al. Developing a Risk Assessment Methodology for the National Aeronautic and Space Administration. RAND Corporation, 2016. 113 p.
29. Kendall F. Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. Washington, DC 20301-3030, 2017. 96 p. [Electronic resourse]. Mode of access: https://www.acq.osd.mil/se/docs/2017-rio.pdf.
30. NATO Standard AJP-5. Allied Joint Doctrine for the Planning of Operations. Ed. A V.2. NATO Standardization Office, 2019. 134 p.
31. Ильина Е.П., Синицын И.П. Модели и методы поддержки аналитического сопровождения поля решений организации. *Проблеми програмування*. 2017. № 3. С. 93–107.
32. Ильина Е.П. Методы и модели использования экспертно-аналитического знания для поддержки принятия решений в организации. Часть 1. *Модели знания о решениях. Проблеми програмування.* 2016. № 1. С. 89–101.
33. Ильина Е.П., Слабоспицкая О.А., Синицын И.П., Яблокова Т.Л. Автоматизированная поддержка принятия решений по управлению программами фундаментальных научных исследований с использованием экспертной методологии. Киев / Препринт. 2011. 94 с.

References

1. Blenko M.W. The Decision-Driven Organization – M.W.Blenko, M.Mankins, P.Rogers / Harvard Business Review. – 2010. – Is. 6. [Electronic resourse]. Mode of access: https://hbr.org/2010/06/the-decision-driven-organization.
2. Renn O. Coping with complexity, uncertainty and ambiguity. The risk governance approach / O.Renn – NSF-DFG Joint Risk Meeting, Washington, D.C., Oct. 3-5, 2012. – 33 p.
3. Pisano G.P. Creating an R&D Strategy / G.P. Pisano – 2012. [Electronic resourse]. Mode of access: http:www.hbs.edu/facultyPublication %20Files// 12-095_fb1bdf97-e0ec-4a82-b7c0-42279dd4d00e.pdf.
4. ISO 31000:2018 Risk management – Guidelines. – 16p.
5. Analysis Support Guide for Risk-Based Strategic Planning. / Technical Report STO-TR-SAS-093-Part-I – 2018, STO/NATO. – 156 p.
6. Lempert R.J. Defense Resource Planning Under Uncertainty. An Application of Robust Decision Making to Munitions Mix Planning / R.J. Lempert, D.Warren, R.Henry et al. – RAND Corporation, 2016. – 109 p.
7. Johnson S. New challenges, new tools for defense decisionmaking / S.Johnson, M.Libicki, G.F. Treverton – MR-1576, RAND Corporation, 2003. – 408 p.
8. ISO Guide 73:2009 Risk management Vocabulary. – 15p.
9. ISO 27000:2018 Information technology – Security techniques – Information security management systems — Overview and vocabulary – 34 p.
10. Enterprise Risk Management – Integrating with Strategy and Performance. Executive Summary. – COSO, 2017. – 16 p. [Electronic resourse]. Mode of access: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.
11. FERMA Risk Management standard – FERMA, 2002. – 16 p. [Electronic resourse]. Mode of access: // http://www.ferma.eu/.
12. Australia/New Zealand AS/NZS 4360:2004 Risk management /Standards Australia.– 65 p.
13. Celona J. Value-Driven ERM: Making ERM an Engine for Simultaneous Value Creation and Value Protection / J.Celona, E.Hall, J.Driver // J. of healthcare risk management: the journal of the American Society for Healthcare Risk Management – 2011 – N 30(4) – P.15-33.
14. Torben J.A. Managing Risk and Opportunity. The Governance of Strategic Risk-Taking / J.A. Torben M.Garvey, O.Roggi – Oxford University Press, 2014. – 204 p.
15. Practice Standard for Project Risk Management / Project Mnagement Institute, Inc., 2009. – 128 p.
16. Alberts C. Executive Overview of SEI MOSAIC: Managing for Success Using a Risk-Based Approach / C.Alberts, A. Dorofee, L.Marino – Technical Note CMU/SEI-2007-TN-008, 2007. – 33 p.
17. Hillson D.A. Practical project risk management: The ATOM Methodology (2nd ed.) / D.A.Hillson, P.W.Simon – Vienna, US: Management Concepts, 2012 – 410 p.
18. Virine L. Project Risk Analysis Made Ridiculously Simple / L.Virine, M.Trumper – World Scientific Publishing Co. Pte. Ltd., 2017. – 283 p.
19. ISO 27005:2018 Information technology – Security techniques – Information security risk management.. – 56 p. [Electronic resourse]. Mode of access: https://www.iso.org/standard/75281.html.
20. Freund J. Measuring and Managing Information Risk. A FAIR Approach / J.Freund, J. Jones – Elsevier, 2015. – 391 p.
21. Офіційний сайт NIST CyberSecurity Framework. [Electronic resourse]. Mode of accesshttps://www.nist.gov/cyberframework.
22. Grouhy M. The Essentials od Risk Management / M.Grouhy, D.Galai, R.Mark – McGraw-Hill Education, 2014. – 669 p.
23. ISO/IEC PDTR 33015.3:2019 Information technology – Process assessment – Guide to process risk determination. – 41 p.
24. ISO/IEC 16085:2006 Systems and software engineering – Life cycle processes – Risk management. – 34 p..
25. Sherer S.A. Information Systems Risks and Risks Factors, are they Mostly about Information Systems? / S.A.Sherer, S.Alter // Communications of AIS 2004. – V.14. – N 1. – P. 29-64.
26. GAIT for IT General Control Deficiency Assessment / The Institute of Internal Auditors. [Electronic resourse]. Mode of access: https://www.iiacolombia.com/resource/guias/GAIT_GeneralControl.pdf. – 25 p.
27. COBIT’2019 Framework. Governance and Management Objectives – ISACA, 2018. – 302 p.
28. Gerstein D.M. et al. Developing a Risk Assessment Methodology for the National Aeronautic and Space Administration /

D.M.Gerstein et al. – RAND Corporation, 2016. – 113 p.
29. Kendall F. Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs /F.Kendall – Washington, DC 20301-3030, 2017. – 96 p. [Electronic resourse]. Mode of access: https://www.acq.osd.mil/se/docs/2017-rio.pdf.
30. NATO Standard AJP-5. Allied Joint Doctrine for the Planning of Operations. Ed. A V.2 / NATO Standardization Office, 2019. – 134 p.
31. Ilina E.P. Models and methods for automated analytic support of the organization decisions field/ E.P.Ilina, I.P.Sinitsyn / Problems in Programming – 2017. – N 3 – P. 93-107.
32. Ilina E.P. Methods and models of the expert analytic knowledge using for the decision support in organization. Part 1. Decisions models / E.P.Ilina // Problems in Programming. – 2016. – N 1. – P. 89–101.
33. Ilyina E. Program Management of Fundamental Scientific Research Decision Making Au-tomated Support with Expert Methodology. / E.Ilyina, O.Slabospitskaya, I.Sinitsyn, T.Yablokova. – Draft of Software Systems Institute of NAS of Ukraine, 2011. – Kiev, 2011. – 94 p.

Одержано 31.10.2019

Про авторів:

Ільїна Олена Павлівна,
кандидат фізико-математичних наук,
старший науковий співробітник,
провідний науковий співробітник.
Кількість наукових публікацій в українських виданнях – більше 60,
http://orcid.org/0000-0002-1528-366X,

Слабоспицька Ольга Олександрівна,
кандидат фізико-математичних наук,
старший науковий співробітник,
старший науковий співробітник.
Кількість наукових публікацій в українських виданнях – більше 50.
Кількість наукових публікацій в зарубіжних виданнях – 7,
http://orcid.org/0000-0001-6556-0947.

Місце роботи авторів:

Інститут програмних систем
НАН України,
03187, Київ-187,
проспект Академіка Глушкова, 40.
Тел.: +38(044) 526 4286.
E-mail: olsips2017@gmail.com