УДК 519.83

О.І. Лисенко, д-р.техн.наук., проф., І.В. Чеканова, канд.техн.наук., с.н.с, О.П. Кутовий канд.техн.наук.,с.н.с., В.А. Нікітін, канд.техн.наук.

СТРАТЕГІЇ УПРАВЛІННЯ РИЗИКАМИ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В УМОВАХ НЕВИЗНАЧЕНОСТІ

В матеріалах статті надається огляд найбільш поширених підходів щодо стратегій управління ризиками на об’єктах критичної інфраструктури. При виборі стратегії управління ризиками в умовах невизначеності пропонується використання різних критеріїв, які враховують цілісні установки, обмеження щодо умов його життєдіяльності та інших обставин. Надається аналіз критеріїв Вальда, Лапласа, Севіджа.

Ключові слова: стратегія управління ризиками, критична інфраструктура.

O. Lysenko, Doc. of Sc. (Eng.), I. Chekanova, Cand. of Sc. (Eng.), O. Kutovyi, Cand. of Sc. (Eng.),. V. Nikitin, Cand. of Sc. (Eng.)

RISK MANAGEMENT STRATEGIES ON CRITICAL INFRASTRUCTURE OBJECTS UNDER UNCERTAINTY

In article is an overview the most common approaches for risk management strategies on critical infrastructure objects. Choosing risk management strategies under uncertainty proposes to use different criteria, which take into account integral installation, restrictions on the conditions of his vital activity and other conditions. Wald’s, Laplace,Savage criteria analysis .

Keywords: risk management strategies, critical infrastructure.

До критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади [1]. Ці системи та об’єкти настільки важливі для держави, що їх недієздатність або знищення загрожують національній безпеці, економіці, здоров’ю або безпеці життєдіяльності населення.

Спроба ввести термін “критичний об’єкт національної інформаційної інфраструктури” були здійснена в Законі України від 16 січня 2014 року № 721-VII, що втратив чинність вже на початку лютого 2014 р. Раніше в проекті Закону України “Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України” (був зареєстрований під № 11125 від 31.08.2012 р., відкликаний 12.12.2012 р.) передбачалось внесення змін до Закону України “Про основи національної безпеки України”, і, зокрема, введення терміну “об’єкти критичної інформаційної інфраструктури” [2].

Введення терміну “критична інфраструктура” в законодавство України само по собі не може бути остаточною ціллю. Концепція критичної інфраструктури має стати підґрунтям дієвого механізму координації зусиль органів влади, спрямованих на недопущення втрати чи завдання невиправної шкоди найважливішим для життєдіяльності держави об’єктам, з урахуванням дії негативних факторів будь-якого походження, або техногенного, або природного, або соціально-політичного, або будь-якої комбінації з їх числа.

На сьогодні в державі досі відсутній загальний механізм управління захистом та безпекою об’єктів критичної інфраструктури, спостерігаються непоодинокі випадки дублювання функцій та ресурсів, відсутність спільних підходів та узгодженості дій стосовно проблем національного масштабу, а загрози таким об’єктам розглядаються в суто “відомчому” розрізі [2].

В умовах загострення небезпеки воєнного протистояння, виконання службово-бойових завдань з охорони ядерних об’єктів та об’єктів оборонно-промислового комплексу держави, як елементу критичної інфраструктури, є одним із головних напрямків стабілізації обороноздатності держави.

Під час існування об’єктів критичної інфраструктури існує ризик виникнення в певний момент часу подій, що загрожують нормальному функціонуванню економіки й органів управління, та здатні потенційно вплинути на обороноздатність держави.

Ризик як невід'ємний елемент економічного, політичного і соціального життя суспільства неминуче супроводжує всі напрями і сфери діяльності будь-якої організації, що функціонує в ринкових умовах.

Ризик є кількісною мірою безпеки, що дорівнює добутку ймовірності реалізації даної загрози, помноженій на ймовірність величини можливого збитку від неї [3,4].

Для підтримки обороноздатності держави в належному стані важливо не допустити виникнення подій здатних порушити нормальне функціонування об’єктів критичної інфраструктури – важливо мінімізувати загрозу, зменшити ризик її виникнення. Тому питання щодо управління ризиками на об’єктах критичної інфраструктури є актуальним.

Метою статті є аналіз стратегій управління ризиками на об’єктах критичної інфраструктури в умовах невизначеності.

Управлінська діяльність передбачає послідовність етапів науково-практичних досліджень, спрямованих на визначення достовірних та обґрунтованих характеристик ризику та виявлення ефективних заходів щодо його скорочення. Складові етапи визначення ризику представлені на рис. 1.

Оцінка ризику – це розрахунок розміру потенційно шкідливого впливу взаємодій та імовірність того, що він здійсниться зараз або у майбутньому.

Для того щоб оцінити рівень ризику, його необхідно виміряти. Щоб кількісно визначити ризик, необхідно знати всі можливі наслідки від проведення окремих дій і дати їм кількісну чи порівняльну інтерпретацію. Для кількісного оцінювання рівня ризику використовують ряд показників, таких як можливий результат, очікуване значення рівня ризику і відхилення від очікуваного значення. Вірогідність ризику (Р) є важкою для кількісного оцінювання величиною. Об'єктивний метод визначення можливості ризику заснований на розрахунку частоти настання події.

У випадках, коли неможливо визначити рівень ризику на основі об'єктивних даних, найчастіше використовують суб'єктивні оцінки. Суб'єктивна можливість є прогнозом результату події і може ґрунтуватися на аналізі частоти її настання.

До найвідоміших суб'єктивних методів оцінки ризику слід віднести експертні атрибутивні оцінки (інтуїтивне визначення допустимості ризику виходячи із накопиченого досвіду і підсвідомого аналізу небезпек), експертні оцінки чинників і критеріїв ризику, моделювань можливостей ризиків.

Як об'єктивна, так і суб'єктивна оцінки можливості ризику використовуються для визначення двох важливих критеріїв рівня ризику: середнього значення його рівня і мінливості ризику. Рівень ризику може постійно змінюватися, тому абсолютне значення можливості часто замінюється його очікуваним значенням. Очікуване значення, пов'язане з невизначеною ситуацією, є середньозваженим усіх можливих наслідків події, де можливість кожного результату використовується як частота або вага відповідного значення.

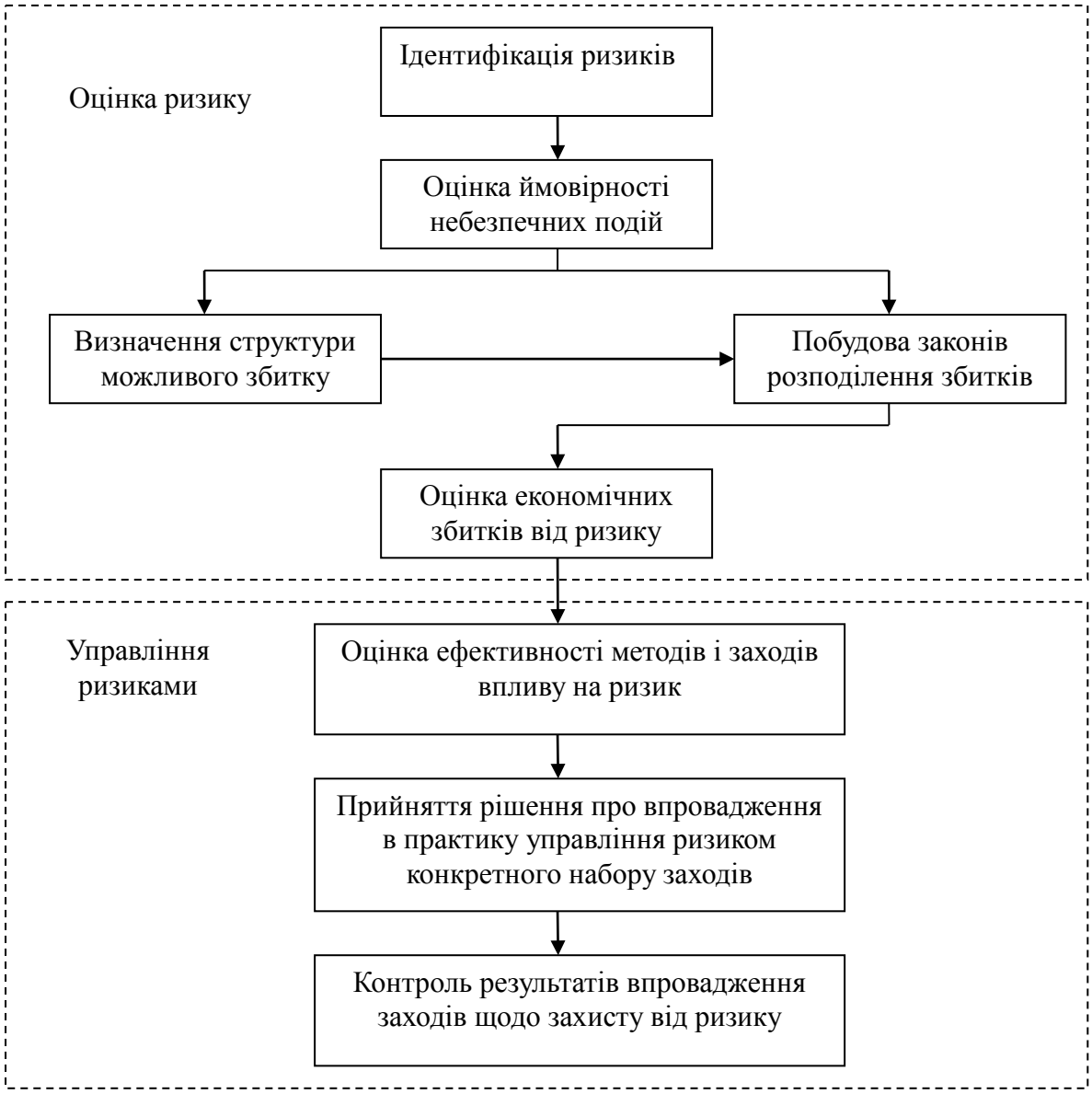

Рисунок 1.– Етапи визначення ризику

Загальна оцінка ризику розраховується за формулою [5]:

$$R = \sum_{i=1}^{n} B_i W_i \quad , \tag{1}$$

де R – рівень ризику;

B_i – ймовірність отримання збитку в розмірі W_i в результаті настання будь-якої небезпечної події (групи подій);

W_i – величина збитку, відображена у відповідних показниках;

n – загальна кількість можливих збитків, що можуть бути при настанні небезпечної події.

Кожний ризик описується визначеним числом чинників (не більше десятьох). Значення кожного з них ранжується за рівнем ризику (в міру наростання ризику), потім нормується. При цьому кожному чиннику на основі експертних висновків присвоюється своя

вага, що відбиває частку його впливу на загальний розмір рівня ризику. Чим ближчий рівень ризику до 1, тим ризик менший, чим ближчий він до n, тим він вищий.

Управління ризиками вимагає знань предметної діяльності, математичних методів оптимізації економічних завдань. Воно має бути орієнтоване не тільки на сьогодення, на розв'язання оперативних та тактичних завдань, а й створювати належну базу для ефективної діяльності у майбутньому.

Можливі три варіанти оцінки доцільності ризику:

При визнанні ризику абсолютно доцільним операція чи діяльність, якій він притаманний, проводиться за сценарієм, який фактично склався або проектувався. При цьому повинні проводитися звичайні (типові) заходи щодо контролю та фінансування ризику.

При визнанні ризику абсолютно недоцільним – діяльність, що пов'язана з цим ризиком, припиняється (проект проведення певної господарської операції відхиляється).

При неможливості остаточної оцінки доцільності ризику (сумнівна доцільність) переходять до наступного шостого етапу роботи щодо розробки стратегії управління ризиками – розробки заходів з контролю та фінансування ризику.

Практика управління ризиками охоплює різноманітні підходи до мінімізації наслідків ризику. В загальному вигляді вони поділяються на дві великі групи:

організаційні або методи контролю рівня ризику;

економічні або методи фінансування ризику.

Визначивши певний перелік заходів, проводять повторну оцінку доцільності ризику, визначаючи своє кінцеве ставлення до виду діяльності або операції, експертизи що проводиться.

При управлінні ризиком на державному рівні та наявності невизначеності в оцінках ризику в загальному випадку неможливо запропонувати однозначний підхід до визначення стратегії. При виборі стратегії управління ризиками в умовах невизначеності можуть бути використані різні критерії, які враховують цілісні установки, обмеження на умови його життєдіяльності та інші обставини. До числа таких критеріїв можна віднести: критерії Вальда, Лапласа, Севіджа та ін.

Критерій Вальда використовується в тих умовах, коли вибирається стратегія управління виходячи з вимог отримання максимально можливого прибутку в гірших умовах. В цьому випадку кожній стратегії управління ризиками і можливій небезпечній події ставиться у співвідношення розмір очікуваного прибутку. Виграш у розмірі V_{ji} може бути визначений як різниця між отриманим доходом та понесеними витратами для обраної стратегії “j” в деяких умовах “i” [5] :

$$V_{ji} = D_{ji} - u(R, Z) \quad . \tag{2}$$

Стратегія управління ризиками згідно критерію Вальда визначається по величині показника Z, який відповідає значенню наступної умови:

$$V(Z) = \max_{j} \min_{i} V_{ji} \quad . \tag{3}$$

Критерій Лапласа використовується в тих умовах, коли не існує будь-якої переваги по відношенню до варіантів існуючих стратегій управління, та при їх виборі враховується лише величина зв’язаних з ними витрат. В цьому випадку стратегія управління може бути визначена по середньоваговому показнику витрат. Величина збитків управління, в даному випадку визначається наступним чином:

$$\bar{u}(\bar{R},\bar{Z}) = \int_{u_1}^{u_2} u(R,Z,t) f(t) dt \quad , \tag{4}$$

де $\bar{u}$ – середні витрати, обумовлені рівнем ризику $\bar{R}$ та затратами на його зменшення $\bar{Z}$;

$u(R,Z,t)$ – змінні витрати управління, які в загальному випадку залежать від рівня ризику R, витрат на його зниження зменшення Z та часу t;

u_1, u_2 – межі інтервалу існування витрат;

$f(t)$ – відома щільність розподілення (при рівномірному законі $f(t) = \frac{1}{u_2 - u_1}$).

Отримане за допомогою (4) значення середніх витрат $\bar{u}$ в загальному випадку визначає відповідну величину витрат $\bar{Z}$, та в свою чергу перелік необхідних заходів.

Критерій Севиджа використовується в тих умовах, коли потрібно вибрати стратегію захисту від дуже великих втрат. Така стратегія визначається з умов мінімізації максимальних для кожної небезпечної події втрат. В загальному випадку критерій Севіджа можна представити у наступному вигляді:

$$V(z) = \min_j \max_i u_{ji} \quad , \tag{5}$$

де u_{ji} – характеризують витрати при настанні небезпечних подій.

Визначення стратегій – це процес, у якому враховуються всі аспекти зовнішнього та внутрішнього функціонування.

Практика доводить, що розробка стратегій, як правило, завершується формуванням обґрунтованих планів, що мають складну внутрішню структуру.

Таким чином, запропоновані підходи щодо управління ризиками на об’єктах критичної інфраструктури в умовах невизначеності дозволяють: визначати оптимальну структуру витрат щодо управління ризиками на цих об’єктах; створювати базу даних експертних систем для підтримки осіб, які приймають рішення і виробляють нормативні документи.

Введення зазначених вище підходів щодо управління ризиками на об’єктах критичної інфраструктури дозволяють забезпечити якісне проведення досліджень з аналізу ризиків для таких об’єктів, визначити пріоритети та шляхи вирішення проблем щодо його зменшення.

Використання наведених підходів щодо управління ризиками на об’єктах критичної інфраструктури в умовах невизначеності надасть можливість особам, які приймають рішення своєчасно і якісно формувати науково-обґрунтовані підходи до розподілення ресурсів, які виділяються на захист об’єктів критичної інфраструктури.

СПИСОК ЛІТЕРАТУРИ

1. Бірюков Д. С. Стратегія захисту критичної інфраструктури в системі національної безпеки держави / Д. С. Бірюков, С. І. Кондратов // Стратегічні пріоритети. – 2012. – № 3(24). – С. 107–113.
2. Бірюков Д. С. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні / Д. С. Бірюков, С. І. Кондратов. – К.: НІСД, 2012. – 96 с.
3. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б.Качинський. – К.: Інститут проблем національної безпеки. – К., – 2003. – 472 с.

4. Качинський А.Б. Засади системного аналізу безпеки складних систем / А.Б Качинський, за заг. ред. академіка НАН України, д.т.н. В.П. Горбуліна. –К.: ДП НВЦ Евроатлантінформ, – 2006. –116 с.

5. Тихомиров Н.П. Методи аналізу и управления эколого-экономическими рисками: Учебн.пособие для вузов / Н.П. Тихомиров, І.М.Потравний, Т.М. Тихомирова [под ред. Н.П. Тихомирова]. – М.: ЮНИТИ-ДАНА, 2003. – 350 с.

❖ ❖ ❖