УДК 004.02:004.04

В.В. БЄГУН[*], С.В. БЄГУН[*]

ОДИНИЦІ ВИМІРУ РИЗИКУ ЗА ТЕОРІЄЮ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ

[*]Інститут проблем математичних машин і систем НАН України, м. Київ, Україна

Анотація. *Останнім часом урядом прийнято достатньо велику кількість документів законодавчого рівня з напряму регулювання безпеки в усіх сферах діяльності відповідно до концепції ризик-орієнтованого підходу. Але при цьому спостерігається однобокість урядових рішень, яка проявляється перш за все у рекомендованих методах оцінки ризику, способах контролю (моніторингу) рівня ризику та пов'язаних з цим одиниць виміру ризику. Перевага віддається якісним методам оцінок ризику та інспекційним перевіркам об'єктів із використанням бальної шкали виміру ризику. З цього слідує небезпечна тенденція спрощеного підходу до важливого питання, гальмування впровадження сучасних ринкових методів управління, які базуються на кількісних оцінках ризику на основі моделювання, відповідного страхування ризику та декларування. Як свідчить досвід, тільки ці методи приводять до успіху самоврядування, зменшення державного тиску на бізнес та зближення з нормативним полем європейських країн. У статті аналізуються допущені системні помилки та пропонуються шляхи їх виправлення. Отже, стаття є дуже актуальною. Оскільки ІПММС постановою НАНУ визнано головною науковою організацією з наукового супроводу цієї важливої державної тематики, слід зробити відповідні роз'яснення. У статті обґрунтовано вибір одиниці виміру ризику на основі визначення відповідно до теорії розмірності та існуючої практики у небезпечних галузях виробництва, загальний алгоритм оцінки ризику на основі моделювання з можливістю оцінки людського чинника. Зроблена оцінка невизначеності за якісними та кількісними методами оцінок ризику, розглянуто алгоритм відбору подій, факторів та обставин, які потрібно враховувати в моделях оцінок ризику.*

Ключові слова: *безпека, ризик, небезпечна подія, шкала, невизначеність, моделювання безпеки.*

Аннотация. *В последнее время правительством принято достаточно большое количество документов законодательного уровня в направлении регулирования безопасности во всех сферах деятельности в соответствии с концепцией риск-ориентированного подхода. Но при этом наблюдается однобокость правительственных решений, которая проявляется в первую очередь в рекомендованных методах оценки риска, способах контроля (мониторинга) уровня риска и связанных с этим единиц измерения риска. Предпочтение отдается качественным методам оценок риска и инспекционным проверкам объектов с использованием балльной шкалы измерения риска. Из этого следует опасная тенденция упрощенного подхода к важному вопросу, торможение внедрения современных рыночных методов управления, которые основаны на количественных оценках риска на основе моделирования, соответствующего страхования риска и декларирования. Как свидетельствует опыт, только эти методы приводят к успеху самоуправления, уменьшению государственного давления на бизнес и сближению с нормативным полем европейских стран. В статье анализируются допущенные системные ошибки и предлагаются пути их исправления, поэтому статья является очень актуальной. Поскольку ИПММС постановлением НАНУ признан главной научной организацией по научному сопровождению этой важной государственной тематики, следует провести соответствующие разъяснения. В статье обоснован выбор единицы измерения риска на основе определения в соответствии с теорией размерности и существующей практики в опасных отраслях производства, общий алгоритм оценки риска на основе моделирования с возможностью оценки человеческого фактора. Проведена оценка неопределенности качественных и количественных методов оценок риска, рассмотрен алгоритм отбора событий, факторов и обстоятельств, которые необходимо учитывать в моделях оценок риска.*

Ключевые слова: *безопасность, риск, опасное событие, шкала, неопределенность, моделирование безопасности.*

Abstract. *Recently government has adopted quite a big amount of legislative documents directed on safety regulation in all spheres of activities according to risk oriented approach. However, at the same time, we could observe the one-sidedness of governmental decisions which become apparent first of all at the*

ISSN 1028-9763. Математичні машини і системи, 2019, № 1

recommended risk assessment methods, methods of control (monitoring) of risk level, and related to these units of risk measurement. The advantage is given to the qualitative methods of risk assessment and to the inspections of objects with risk estimations based on scoring approach using ordinal scales. The dangerous tendency of simplified approach to the solution of very complicated task appears as a consequence of these decisions which results in significant slowdown of implementation of the modern market methods of management based on quantitative risk assessment with modelling, appropriate risk insurance and declaration. As it is shown by the world experience only such quantitative methods lead to the success in self-government, in decreasing of governmental pressure on business and in harmonization of legislation with European countries. The analysis and the correction for the system errors that was made are proposed in this article, therefore this article is extremely relevant. Since the IMMSP of the NAS of Ukraine by the NAS of Ukraine decree is recognized as the main scientific institution for scientific support for this very important governmental theme, thus we must make appropriate clarification. The substantiation of the selection of the risk measurement unit based on the definition according to the theory of measurement scales and according to the existing practice at the dangerous branches of industry, general algorithm of risk assessment based on modelling with the possibility of human factor inclusion are given in the article. The estimation of the uncertainty of the qualitative and of the quantitative methods of risk assessment is performed in the article. The selection algorithm for the events, factors and circumstances that should be included in the models of risk assessments is considered.
Keywords: *safety, risk, dangerous event, scale, uncertainty, safety modelling.*

1. Вступ

Оскільки в Україні відбувається впровадження ризик-орієнтованого підходу (РОП) в управлінні безпекою, існує необхідність з'ясування одиниці виміру ризику. З цього приводу уваги заслуговують нещодавно прийняті нормативні документи [1, 2], де пропонується оцінювати безпеку балами за різними шкалами.

Згідно з концепцією (парадигмою) РОП [3], рівень безпеки визначається ризиком (R). Але до цього часу у практичній діяльності існують невизначеності з цього питання, а саме: чим, якою мірою міряти ризик. На ці невизначеності вказують згадані нові НТД. За міжнародними стандартами, які нещодавно прийняті в Україні [4], та затвердженою у 2014 році концепцією [3], ризик вимірюється відношенням кількості можливих летальних випадків (ЛВ) (n) до кількості осіб у групі населення (N), для якої визначають ризик (R), причому $n \in N$, тобто за дуже простою формулою:

$$R = n / N . \qquad (1)$$

Для цілей порівняльних оцінок ризику МООЗ ще у минулому столітті затверджені такі рекомендовані допустимі граничні рівні: $R < 1*10^{-6}$ – малий, знехтуваний ризик, $R > 1*10^{-4}$ – великий, неприпустимий ризик.

Але чому саме ризик визначає рівень безпеки? Раніше в усіх документах з безпеки, в законах України в тому числі, безпеку визначали як СТАН захищеності людини, суспільства, довкілля. Але категорія «СТАН» може мати тільки якісні рівні для порівняння: задовільний – незадовільний, високий – низький та ін., а цього недостатньо для сучасного суспільства. Звісно, можливо створити якісні шкали для порівняння з додатковими ступенями якості, але в такому випадку необхідним є й словесний опис кожного ступеня порівняння. Для великої множини станів, різних за природою небезпек, отримуємо нерозв'язну задачу з реального визначення цього «стану». Ось чому при необхідності детального опису небезпек людство відмовилося від такого (якісного) визначення ще у другій половині минулого століття (початок 70-х). З'явилася необхідність більш детальної класифікації стану безпеки, яка відображає нескінченну множину ймовірних станів – кількісне, числове визначення. При цьому визначення безпеки як припустимого ризику надає можливість кількісних та прогнозних розрахункових значень небезпек. Дійсно, ризик як випадкова величина має значення від нуля до одиниці або від 0 до 100%, що тотожне. Нуль відображає відсутність

ризику, одиниця – достовірний, неминучий ризик. У діапазоні від 0 до 1 знаходиться нескінченна множина чисел, існує можливість їх натурального порівняння – ось перша (головна) причина переходу на нове визначення. Друга причина – можливість здійснення запобігання надзвичайним ситуаціям (НС) на основі попереднього аналізу, який включає визначення важливості подій у вигляді їх внеску в інтегральну величину ризику й оцінки ризику. А саме ці процедури й відображають саму суть РОП.

Так, управління безпекою у країнах-лідерах базується на використанні ризик-орієнтованого підходу (РОП) з економічними важелями впливу у вигляді відповідної системи страхування [5–8]. При цьому відбувається поступовий перехід на концепцію кумулятивного ризику [8].

Процес розробки, обґрунтування, оцінки й ухвалення рішення з використанням оцінок ризику повинний включати послідовні стадії, направлені на визначення відповідності матеріалів, що обґрунтовують, критеріям прийнятності і реалізація яких повинна забезпечувати вироблення обґрунтованого рішення.

Так, за найкращою світовою практикою оцінка ризиків проводиться ймовірнісними методами в такій послідовності [5–8]:

1. Попереднє планування та визначення мети.
2. Формулювання задачі розрахунку та збір необхідної інформації.
3. Аналіз впливу небезпечних факторів і оцінка відповідних ефектів.
4. Характеристика ризику, що передбачає як визначення величини ризику, так і аналіз невизначеності результатів.

При цьому у всіх згаданих документах впровадження РОП розглядається як фактор, що сприятиме покращенню конкурентоздатності виробництва через зменшення аварійності, зменшення страхових внесків та виплат.

2. Основна частина. Історична довідка з використання «бальних» методик

Спроба впровадження РОП в Україні на основі «бальних» методик не перша. Пропозиція виміру ризику у сфері безпеки на виробництві «балами», які нараховувалися за певною методикою [9], десять років тому була на основі існуючої ще за радянських часів. Методика була призначена для оцінки стану безпеки у сфері охорони праці (ОП) та техногенної безпеки інспекторами під час перевірок з метою управління безпекою. Експерти високого рівня сфери безпеки оцінили типові порушення на виробництві у балах за стобальною шкалою. За сумою балів виявлених інспектором порушень робилася загальна оцінка стану безпеки, яка ставала основою прийняття рішень для управління безпекою. Для порівняння результатів з міжнародним досвідом була сформована емпірична формула переводу балів до десяткового виду:

$$P = K_T \times K_б \times (M_{\max} - K_o + Sш_б + 0{,}1) \times 9 \cdot 10^{-7}, \qquad (2)$$

де K_T – коефіцієнт технічної небезпеки;

$K_б$ – коефіцієнт технічної небезпеки будівель та споруд;

K_o – коефіцієнт організаційної безпеки;

$M_{\max}$ – максимальний бал для оцінки ризику;

$Sш_б$ – сума штрафних балів, оцінених за шкалою штрафних балів.

«Бальна» одиниця виміру на той час не прижилася у суспільстві, незважаючи на наявність формули (2) та детальної методики нарахувань балів. «Бальна» одиниця виміру допускається й міжнародними стандартами для експертних оцінок ризику, але рекомендується це робити за вибором самих експертів. Очевидно, що «бальна» одиниця виміру, яка придатна в одній галузі, в інший галузі буде не зовсім точна тому, що бал буде мати іншу

ціну. Це й стало основною перешкодою для роботи у той час. Незважаючи на формулу (2), результати оцінок не зіставлялися. До інших недоліків таких «бальних» оцінок слід віднести:

• велика невизначеність, залежність від досвіду та знань процесів експертами;

• як наслідок великої невизначеності – неможливість чи складність розробки обґрунтованих заходів та засобів запобігання ризику;

• за кращою світовою практикою для об'єктів підвищеної небезпеки (ОПН) вже існували оцінки на основі моделювання з використанням імовірнісних методів (АЕС).

Ці та інші обставини і недоліки «бальних» методів саме й звели нанівець спробу впровадження парадигми РОП на початку 2000-х років. До речі, наведені висновки щодо недоліків «бальних» оцінок були пізніше повністю підтверджені міжнародною спільнотою фахівців з безпеки у вигляді міжнародного стандарту IEC/ISO 31010:2009, який чинний на території України з 2014 року – ДСТУ IEC/ISO 31010:2013 [4], про що в цій статті йдеться нижче.

Ситуація, що склалася зараз [1], майже повністю повторюється, тільки на більш загальному рівні: пропонується вимірювати ризик в усіх сферах безпеки балами з наступним переводом кількісної «бальної» оцінки у трирівневу якісну: великий, середній, малий ризик. При цьому скасовуються попередні урядові документи, які зв’язували числові на основі ймовірнісних методів оцінки та якісні оцінки ризику.

До речі, бальна методика у 2000-х також з’явилася при вже затвердженій на той час методиці оцінки ризику за міжнародними стандартами [10]. За методикою [10] було виконано достатньо робіт з оцінки ризиків підприємств нафтопереробної та енергетичної галузі. Як правило, ці роботи виконувалися науковими установами, оскільки дана методика була заснована на моделюванні процесів і систем об’єктів підвищеної небезпеки (ОПН).

Чому передові країни світу переходять на ризик-орієнтований підхід, заснований на ймовірнісних оцінках ризику [5–8]? Для відповіді наведемо деякі теоретичні відомості про шкали вимірювання.

3. Загальні відомості про шкали

При вимірюванні кожному об’єкту приписується певний елемент використовуваної математичної системи (зазвичай дійсні числа) [11]. Це означає, що ми можемо кількісно характеризувати те, в якій степені даний об’єкт спостереження (індивід, група, місто, організація, соціальна система) проявляє властивість, представлену через вимірювану змінну. Таким чином, процедура вимірювання припускає використання певної шкали вимірювань.

Шкала – це інструмент вимірювання, який є числовою системою, де властивості емпіричних об'єктів виражені у вигляді властивостей числового ряду. Розрізняють такі типи шкал.

Номінальні шкали використовуються тільки для якісної класифікації. Це означає, що такі змінні можуть бути виміряні тільки в термінах приналежності до певних істотно різних класів; при цьому неможливо визначити кількість у вигляді числової характеристики або упорядкувати ці класи. Наприклад, можна сказати, що два індивідууми розрізняються в термінах змінної А (наприклад, індивідууми належать до різних національностей). Типові приклади номінальних змінних: стать, національність, колір, місто і т.д.

Порядкові шкали дозволяють ранжирувати (упорядкувати) об’єкти, вказавши, які з них більшою чи меншою мірою мають якість, виражену даною змінною. Проте вони не дозволяють сказати «наскільки більше» або «наскільки менше». Типовий приклад порядкової змінної – це соціоекономічний статус сім’ї. Розуміється, що верхній середній рівень вище середнього рівня, проте сказати, що різниця між ними рівна, скажімо, 18%, не зможемо. Саме розташування шкал у такому порядку: номінальна, порядкова, інтервальна є хорошим прикладом порядкової шкали. Так само дана шкала вимірює рівень згоди з твер-

дженням, ступінь задоволеності.

Інтервальні шкали дозволяють не тільки упорядковувати об'єкти вимірювання, але і виразити через числові параметри і порівняти відмінності між ними. Дана шкала вимірює в інтервальних значеннях вік, дохід та ін.

Відносні шкали дуже схожі на інтервальні змінні. На додаток до всіх властивостей змінних, виміряних в інтервальній шкалі, їх характерною рисою є наявність певної точки – нуля. Таким чином, для цих змінних є обґрунтованими положення типу: *x* у два рази більше, ніж *y*. Типовими прикладами таких шкал є вимірювання часу або простору. Так само, шкала відносин вимірює стаж роботи, вік, дохід та ін.

4. Обґрунтування одиниці виміру ризику

Вибір шкали та одиниці вимірювання, а саме таке питання повстає зараз, має бути обґрунтованим, та, як зрозуміло з наведених визначень, залежить від змінної, яка вимірюється, і допустимої невизначеності при цьому.

Детальний аналіз методу показників ризику

Як слідує із аналізу методів оцінки ризику у стандарті [4], для задач управління безпекою в їх сучасній інформаційній (цифровій) постановці «бальних» оцінок недостатньо. За класифікацією методів, запропонованою в [4], метод оцінок ризику шляхом попереднього нарахування балів [1] є Методом показників ризику [4]. У стандарті ДСТУ IEC/ISO 31010:2013 (IEC/ISO 31010:2009, IDT) [4] міжнародною спільнотою експертів у галузі безпеки чітко прописані переваги та недоліки методу показників ризику (дивись табл. А.1 та табл. А.2 у [4, с. 13–17] та п. В.28 [4, с. 65–66]), процитуємо їх:

– метод застосовний для задач ідентифікування ризику;

– метод завжди застосовний для аналізування наслідків ризику;

– метод завжди застосовний для аналізу ймовірнісних показників ризику;

– метод застосовний для аналізу рівня ризику;

– метод використовує напівкількісну міру ризику;

– метод призначений для ранжування та порівняння ризиків на якісному рівні;

– вихідні дані методу – низка чисел (комплексних індексів), які стосуються конкретного джерела та які можна порівняти з індексами, розробленими для інших джерел у межах тієї самої системи, або які можна змоделювати таким самим способом;

– характер і ступінь невизначеності методу – від низької до високої в залежності від обраних вхідних даних та обраного методу нарахування балів;

– перевага методу – індекси можуть бути придатним засобом ранжування різних ризиків;

– перевага методу – є можливість об'єднувати кілька чинників, що впливають на рівень ризику, в єдину «бальну» оцінку рівня ризику;

– обмеженість методу – якщо процес (модель) та їхні вхідні дані належно не підтверджені, результати можуть не мати сенсу;

– недолік методу – той факт, що вихідні дані є числовим значенням ризику, може бути неправильно витлумачено та використано, наприклад, під час подальшого аналізування витрат та вигод;

– недолік методу – у багатьох ситуаціях, коли застосовують індекси, немає базової моделі, яка дає змогу визначити, чи є окремі шкали чинників ризику лінійними, логарифмічними чи іншими, а також моделі для визначення того, як чинники треба поєднувати. У цих випадках упорядкування у своїй суті ненадійне і підтвердження його фактичних даних набуває особливої важливості.

Таким чином, підсумовуючи наведені у стандарті ДСТУ IEC/ISO 31010:2013 (IEC/ISO 31010:2009, IDT) [4] переваги та недоліки методу показників ризику, можна сфо-

рмулювати таке: метод показників ризику є дуже зручним методом для ранжування та порівняння ризиків у межах тієї самої системи (галузі) та обраної порядкової шкали на якісному рівні, але при порівнянні отриманих оцінок з оцінками ризиків, виконаними в рамках інших шкал, виникають складнощі, пов'язані з потребою перерахунку оцінок ризиків до єдиної шкали, що унеможливлює проведення прямих порівнянь і є дуже незручним. Через складність об'єднання сукупності оцінок ризиків та зважаючи на можливі суттєві невизначеності вихідних даних методу показників ризику, порядкові шкали більше не використовуються в сучасних методах оцінки ризику [4–8].

У той же час, імовірнісні методи з оцінкою абсолютної величини ризику (наприклад, з використанням комбінації методів аналізування дерев подій, загального оцінювання надійності людини (HRA) та байєсівського аналізування [4]) дозволяють легко порівнювати і об’єднувати різні оцінки ризику, мають низьку невизначеність із можливістю отримання й прямого порівняння кількісних вихідних даних, можуть бути напряму використані під час подальшого аналізування витрат та вигод [4]. Єдиним суттєвим недоліком таких методів є їх висока складність [4], що іноді є бар’єром для їх впровадження та використання. Але цей бар’єр у сучасному світі долається шляхом розроблення як інструментів для інспекторів стандартних методів та засобів, комп’ютерних програм тощо, де складність сучасних методів компенсується інтуїтивно зрозумілим інтерфейсом, детально описаним, простим набором вхідних даних і детальною інструкцією користувача, про що йдеться нижче.

Таким чином, у результаті існуючого у світі (суспільство, бізнес) запиту на надійні, компарабельні методи оцінки ризику з низькою невизначеністю [4–8], ймовірнісні методи оцінки ризику переважають у сучасних методах оцінки ризику. За визначенням [4, 12]: РИЗИК – імовірність виникнення негативних наслідків від провадження господарської діяльності та можливий розмір втрат від них, що вимірюється у кількісних та якісних показниках (цитовано із Закону України № 877-5). Для розрахунків, відповідно

$$R = P(X) * U , \tag{3}$$

де X – вектор вхідних параметрів, що впливають на ризик, $P(X)$ – ймовірність виникнення НП під впливом вхідних параметрів, а U – відповідні наслідки при цьому.

Отже, якщо керуватися принципами теорії розмірностей, то з формули (3) отримуємо, що ризик має вимірюватися тією ж одиницею, що й збиток (U), оскільки ймовірність $P(X)$ є безрозмірною величиною. Але, якщо збиток (U) визначається ймовірністю ЛВ або грошима, то й ризик маємо вимірювати ймовірністю ЛВ або грошима. Саме з цією обставиною є непорозуміння: з одного боку, це число менше одиниці $P(X) \in [0,1]$, а з другого, ми можемо сказати, що ризик коштує, наприклад, сто гривень. У дійсності протиріччя немає, просто маємо різні одиниці виміру. До речі, слід чітко розрізняти поняття «ймовірність ризику» і «ризик». Імовірність ризику – це ймовірність НП, без урахування наслідків, тобто $P \in [0,1]$ завжди менше одиниці, а ризик (R), відповідно до формули (3), добуток імовірності НП та наслідків НП. Тому, якщо мова йде про значення ризику у виді десяткового дробу (наприклад, $R = 7 \cdot 10^{-4}$), то для визначення ймовірності НП, відповідно до (3), потрібно виконати зворотну операцію, а саме: $P(X) = R / U$, де U – ймовірність летального випадку, якщо НП відбулася. Частіше наслідки U відомі фахівцям галузі, більш того, за чинним законодавством на кожному ОПН мають бути документи, що описують дії людини після виникнення будь-якої НП. Тому у кожній галузі існує ще й визначення ризику як імовірності найбільш небажаної події:

$$R = P_n(X) , \tag{4}$$

де X – вектор факторів та обставин виникнення НП.

У спеціальній літературі певної галузі виробництва це цілком розповсюджене та зрозуміле явище. Такі події іменують постульованими, за класифікацією ДСТУ [13], вони мають тяжкі або катастрофічні наслідки. Наприклад, у найбільш потенційно небезпечній галузі – атомній енергетиці, найбільш небезпечна подія – руйнування (плавлення) активної зони реакторної установки – Core Destruction (CD), для звичайної АЗС – це пожежа, для установки хлорування води – розгерметизація (розрив) ємності або комунікацій хлору. Наслідки цих подій, звичайно, відомі фахівцям галузі, і для визначення рівня ризику за формулою (3) потрібно тільки визначення ймовірності цієї (постульованої) події відповідно до виразу (4). Звісно, на практиці для визначення ймовірності постульованої події експертні судження вже стають малопридатними з причин великої розмірності вектора X. Математичне моделювання стає основним методом. Дійсно, оскільки наслідки відомі, для цілей запобігання не вистачає саме цієї величини – значення ймовірності НП та саме залежності її від складових вектора X (формула (3)).

Але визначення ризику за виразом (4) як імовірності постульованої події часто призводить до непорозумінь у громадськості, якщо фахівці-практики оперують такими результатами. Ситуація буде ще складнішою, якщо одиницею виміру стануть «бали», які нараховані експертами, хоча це принципово можливо, про що вже описано у вступі. При цьому важливо, що за міжнародними правилами за «бальною» методикою оцінка ступеня ризику має бути «аудитом безпеки», яку здійснює експертна компетентна організація [11]. Звісно, експерти можуть оцінити ризик у будь-яких одиницях та назвати заходи зменшення ризику (запобігання), але ж такий аудит коштує чимало. Аудит за визначенням передбачає участь декількох кваліфікованих експертів, тому невизначеності чи похибки зменшуються в декілька разів [11] у порівнянні з думкою одного, навіть компетентного експерта. Кількість експертів (k), яка необхідна, щоб отримати результат із заданою довірчою ймовірністю α та похибкою ε, розраховують за формулою (методика Райхмана і Азгольдова):

$$k = t_\alpha^{\,2} * S^2 / \varepsilon^2, \qquad (5)$$

де S – середнє квадратичне відхилення оцінки, а t_α – аргумент, значення якого беруть зі спеціальних таблиць.

При цьому варто враховувати, що за міжнародним визначенням експерт у сфері безпеки [14]: «Експерт (кваліфікований експерт) – фізична особа, яка на підставі атестації уповноваженим органом або професійним об'єднанням, ліцензії на професійну діяльність або академічну кваліфікацію й досвід належним чином визнана такою, що володіє експертними знаннями у відповідній сфері спеціалізації, наприклад, в області медичної фізики, радіаційного захисту, гігієни праці, пожежної безпеки, забезпечення якості або в будь-якій відповідній інженерно-технічній або пов'язаній із забезпеченням безпеки області». Тобто, по суті, інспектор ДСНС не може вважатися експертом за міжнародними нормами.

Як вихід з ситуації, на сучасному рівні розвитку інформаційних технологій (ІТ) досвідом «дорогих» експертів галузі можна скористатися тільки при побудові моделі процесів виникнення ризику. Тому саме світ й повернувся в бік РОП, заснованого на ймовірнісних методах, де для рішення складної задачі оцінки поточного стану безпеки необхідне й можливе математичне моделювання – модель, яку створюють висококваліфіковані експерти, користуються створеною складною моделлю інші користувачі, інспектори тощо. Тобто, складність створеної математичної моделі не помітна її користувачам за рахунок створення спеціальних розрахункових програм з інтуїтивно зрозумілого інтерфейсу з детальним описом потрібних вхідних даних та керівництвом щодо аналізу вихідних даних розрахунків.

Ефект дискретності бальної оцінки

Пропонований в [1] метод оцінки ризику шляхом нарахування балів залежно від виду об'єкта передбачає нарахування балів у діапазоні від 0 до 100 при відсутності проміжних значень (множина натуральних чисел). Тобто, не розрізняються рівні ризиків, які попадають у проміжні області між дискретними значеннями, наприклад, між 19 та 20 балами та ін. Крім того, максимальна можлива відмінність між нарахованими ризиками становить два порядки (10^2). Це є суттєвим недоліком при переході на систему страхування ризиків, як то передбачає найкраща міжнародна практика [5–8].

Таким чином, при переході на систему страхування (економічні важелі регулювання безпеки) в рамках документа [1] неможливо справедливо визначити розмір страхових внесків для об'єктів, відповідні ризики для яких відрізняються більше, ніж у 100 разів (наприклад, у 1000 разів), що є розповсюдженим випадком. При цьому в системі страхування, з боку власника потенційно небезпечного об'єкта (ПНО), йде боротьба за кожну копійку зменшення страхового внеску шляхом мінімізації ризиків та їх обґрунтування, а з боку страхової компанії – боротьба за точність визначення ризиків для зменшення ризиків втрат і для забезпечення власного прибутку.

У зв'язку з цим слід додатково зазначити, що потрібний у майбутньому відповідно до кращої міжнародної практики перехід на концепцію кумулятивного ризику [8] та аналіз невизначеності результатів [5–8] є значно утруднений у рамках оцінки ризику з використанням системи нарахування балів (метод показників ризику) [4, 8], як то пропонується в документі [1].

Стосовно теми статті зрозуміло, що одиницею виміру в такому випадку має бути (за формулою (3)) ймовірність НП помножена на наслідки, тобто результуюча розмірність або ЛВ, або грошовий еквівалент втрат.

Дійсно, основу концепції сучасної концепції РОП в питаннях управління безпекою складає порівняння поточного ризику з припустимим, а методологією ризик-орієнтованого підходу для оцінки безпеки складних систем служить імовірнісний аналіз безпеки (ІАБ), інші методи для аналізу ризику від складних систем застосовуються зрідка [4–8, 11].

Результати ІАБ можуть бути використані для визначення значимості різних чинників, що дають внесок у аварію або для висновку щодо ризиків, які створюють ОПН. В останньому випадку загально прийнято, щоб рішення про прийнятність ризику базувалися на таких трьох принципах:

• існують рівні ризику для окремих осіб чи суспільства в цілому у зв'язку з використанням технологій, які не слід допускати безвідносно до корисності цих технологій. Такі рівні часто називають межами прийнятності.

• Навіть при ризику менше зазначеного рівня безпека не може вважатися абсолютною і знання про те, як її поліпшити, ніколи не можна вважати повними. Відповідні дії включають постійне прагнення до зниження ризику за умови, що зусилля по досягненню цих поліпшень не є необґрунтовано високими.

• На рівнях, істотно більш низьких у порівнянні з межею прийнятності, ризик настільки низький, що його варто вважати знехтувано малим для того, щоб уникнути непотрібних витрат ресурсів, що відволікають увагу від істотних проблем безпеки, які можуть призвести до більшого ризику іншого типу. Такий відповідно низький рівень іноді називають мінімальною межею.

Реалізація цих принципів вимагає формулювання цілей безпеки, які базуються на відповідних визначеннях ризику, що забезпечують практичність порівняння реальних рівнів ризику з цілями, його значимість і наочність. Як приклад необхідності застосування розрахунків ІАБ, у [15] наводиться посилання на проект Чорнобильської станції до аварії в 1986 році. Цей проект допускав виникнення неконтрольованого перехідного процесу з руйнуванням усіх бар'єрів унаслідок неправильного функціонування однієї системи, а са-

ме системи управління реактивністю. Таким чином, якби ймовірнісні оцінки були зроблені, то розрахована ймовірність тяжких наслідків залежала б майже винятково від таких величин, як відмова з загальної причини системи управління чи людська помилка, тобто аварія в такому вигляді не могла б відбутися завдяки завчасно застосованим заходам. Необхідність запобігання аварій та мінімізації наслідків для навколишнього середовища є критерієм для визначення найкращих наявних технологій, якою є РОП. Як висновок, впровадження РОП на основі ймовірнісних методів має бути відповідним до світових норм і кращої світової практики й неможливе без моделювання небезпечних систем і процесів, а метод показників ризику має суттєві недоліки, що унеможливлюють його застосування.

5. Загальний алгоритм моделювання ризику

Математичне моделювання саме й потрібне для визначення діапазонів імовірностей НП за алгоритмом:

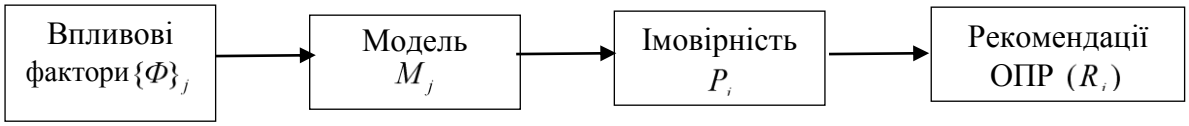

Рисунок 1 – Загальний алгоритм оцінки ризику

Звичайно впливові фактори $\{\Phi\}_j$ добре відомі фахівцям галузі, але стосовно моделей M_j, то вони в усіх наведених прикладах будуть різними. Для прикладу розглянемо наведені раніше об'єкти: АЕС; АЗС; установка хлорування води. Об'єктом моделювання у першому випадку (АЕС) будуть процеси відмов обладнання та спрацювання систем захисту [15], у другому (АЗС) – зовнішні фактори загорянь, у третьому – надійність системи комунікацій хлору та системи контролю цілісності. Додатково загальним фактором в усіх трьох випадках будуть можливі помилки персоналу (людський чинник (ЛЧ)) під час виникнення НП. Як доведено в багатьох наукових працях [11], у 80% НС дії персоналу є визначальними стосовно виникнення та розвитку НП. З чого можна зробити висновок, що моделювання можливих помилок персоналу є необхідною умовою парадигми РОП. Тому й у першій методиці оцінки ризику [10] була вимога моделювання ЛЧ за аналогією з оцінкою ризику від АЕС. Врахування можливих помилок можливе лише за умов їх ідентифікації, аналізу їх впливу на аварійні процеси [11, 15]. При цьому враховуються компетенції персоналу, знання, вміння, досвід роботи, вплив стресу та ін. Вже навіть аналіз (до моделювання) виявляє недоліки у підготовці, що можуть призвести до помилки. Таким чином, з'являється можливість намітити напрями підвищення кваліфікації персоналу, що, звісно, є елементом запобігання НС. Знову ж таки, моделі ЛЧ – Ψ_j можуть бути типовими для галузі, тому що вони (помилки), як правило, однієї природи. Звісно, ці моделі якимось чином мають бути включені в загальну модель: $\Psi_j \in M_j$. З цієї вимоги з'являється вимога вибору одиниці виміру ризику абсолютним числом, оскільки моделі Ψ_j існують у числовій формі [4]. Відомо, що такі моделі вже існують у кращій світовій практиці. Отже, якщо не враховувати ЛЧ, то похибка (невизначеність) оцінки буде дуже великою, що зводить нанівець спробу запобігання НС та парадигму РОП у цілому.

Вплив невизначеності при оцінках ризику

Отже, з'ясовано, що моделі M_j можуть бути різного типу й мета їх – визначення ймовірності P(X) постульованої небажаної події (НП). Стосовно моделей вибору маємо велику міжнародну практику, яка сконцентрована у названих міжнародних стандартах. Але оскільки ми тільки розпочинаємо впровадження парадигми РОП, фахівці галузі, на наш пог-

ляд, розв'язання задачі повинні робити у тісній співпраці з науковцями. Тонкощів, що мають бути враховані, достатньо і головне – це невизначеності, які отримуємо у підсумку. Так, наприклад, процедура FMEA [13], яка на сьогодні пропонується як основна в нових проектах НТД [2], має невизначеності до двох порядків (сто разів!), що по суті є бар'єром доцільності використання. Тому в системах, де аварії мають великі та тяжкі наслідки, ця процедура рекомендована тільки як допоміжна [11, 15], а не залишкова модель. Значить, при виборі типу моделі потрібно з'ясовувати вимоги допустимої невизначеності результату. Для цього, у свою чергу, потрібно як мінімум: 1) з'ясувати невизначеності базисних подій (БП) шляхом первинного аналізу впливових факторів $\{\Phi\}_j$; 2) з'ясувати можливі (допустимі) відхилення результатів дослідження моделі.

Саме тому перший алгоритм із процедур моделювання – це аналіз можливих НП та подій, які вже відбувалися на об'єкті чи на подібних об'єктах [11], та відбір БП для моделі. Алгоритм, заснований на обробці статистичних даних, це елементарна статистика, реалізована багатьма математичними програмами, EXCEL, STATISTICA тощо. На основі статистичних гістограм визначаємо розподіл імовірності НП: математичне очікування БП, тип розподілу ймовірностей та дисперсію. Наприклад, для логнормального розподілу:

$$f(\lambda)=\frac{1}{\sqrt{2\cdot\pi}\cdot\sigma\cdot\lambda}\cdot\exp\left(-\frac{\left(\ln\left(\frac{\lambda}{\mu}\right)\right)^2}{\sigma^2}\right),\ \text{середнє значення}\ \bar{\lambda}=\mu\cdot\exp\left(-\frac{\sigma^2}{2}\right). \qquad (6)$$

Квантилі $\lambda_{0,05}=Q_{\log 0,05}$ та $\lambda_{0,95}=Q_{\log 0,95}$ розраховуються за такою формулою [16]:

$$Q_{\log 0,05}(\mu,\sigma)=\mu\cdot\exp(-\sigma\cdot Z_{0,95}-\sigma^2),\ \ Q_{\log 0,95}(\mu,\sigma)=\mu\cdot\exp(\sigma\cdot Z_{0,95}-\sigma^2), \qquad (7)$$

де $Z_{0,95}$ – 95% квантиль стандартного нормального розподілу ($Z_{0,95}$ =1,644854).

Маючи параметри $Q_{\log 0,05}$, $Q_{\log 0,95}$ та $\bar{\lambda}$ чи $\bar{p}$, як то, наприклад, дається у даних МАГАТЕ [17, 18], можливо розрахувати параметри для побудови відповідного логарифмічно-нормального розподілу (6) за такими формулами (формула (7)):

$$EF=\sqrt{\frac{Q_{\log\ 0,95}}{Q_{\log\ 0,05}}}\ ,\ \sigma=\frac{\ln(EF)}{Z_{0,95}},\ \mu=\bar{\lambda}\cdot\exp\left(\frac{\sigma^2}{2}\right). \qquad (8)$$

Логарифмічно-нормальний розподіл використовується як для побудови розподілів імовірності частоти відмов устаткування, так і для побудови розподілів імовірності частоти відмов устаткування на вимогу [11]. Найбільш ефективним використанням логарифмічно-нормального розподілу є ситуація, коли у дослідника завжди є доступ до всієї сукупності даних з точкових оцінок, що дає змогу кожного разу при отриманні нових даних просто перепідганяти параметри розподілу з урахуванням цих нових даних і використанням всієї сукупності точкових оцінок. Але використання логарифмічно-нормального розподілу є менш зручним при недоступності всієї сукупності даних із точкових оцінок при потребі вдосконалення поточного розподілу ймовірностей на основі нової додаткової інформації шляхом проведення байєсівських оцінок. Звісно, для іншого типу розподілів формули (6–8) будуть інші.

Визначення елементарної статистики та закону розподілу ймовірності випадкових БП є першою задачею моделювання небезпечних процесів в ІАБ, яка базується на статистиці НП підприємства (галузі) та даних з надійності обладнання систем захисту. Це окрема

процедура, яка зазвичай і відлякує фахівців-практиків, тому за міжнародним досвідом процедура оцінки ризику методом моделювання має здійснюватися фахівцями з інформатики, спільно з досвідченими фахівцями відповідної галузі.

Стосовно другої процедури (з'ясування можливих відхилень результатів дослідження (моделі)) мають визначитися фахівці галузі: бажано зменшення невизначеності (дисперсії), але це може призвести до суттєвого ускладнення моделі [11]. Тому невизначеності БП потрібно «прогнати» через (проект) модель, наприклад, методом Монте-Карло для оцінки невизначеності кінцевого результату та порівняння з допустимим для прийняття рішень ОПР.

6. Висновки

1. Метод показників ризику з використанням бальної оцінки має суттєві недоліки і є застарілим для впровадження сучасної інформаційної технології аналізу безпеки на основі РОП.
2. Застосування ймовірнісних методів моделювання відкриває шлях до впровадження ІТ у сфері безпеки.
3. На основі ймовірнісного (числового) моделювання та відповідно до числової одиниці виміру ризику можливі більш повна інформаційна підтримка всіх процесів управління безпекою, розробка заходів запобігання. Зокрема, заходи та засоби запобігання ризику обґрунтовуються розрахунком на основі аналізу важливості подій та чутливості ризику до їх змін.
4. Числові одиниці та моделі надають можливість ураховувати ЛЧ, відповідний рівень підготовки персоналу та шляхи його покращення.
5. Невизначеності за умов числового моделювання розраховуються і не залежать від інспектора (користувача розробленої математичної моделі). При цьому складність створеної математичної моделі не помітна її користувачам за рахунок створення інтуїтивно зрозумілого інтерфейсу з детальним описом потрібних вхідних даних та керівництвом щодо аналізу вихідних даних розрахунків.
6. За числовими одиницями виміру ризику може бути математично обґрунтована та оптимізована періодичність інспекційних перевірок за критерієм мінімуму ризику для персоналу, населення та довкілля.

СПИСОК ДЖЕРЕЛ

1. Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності та визначається періодичність здійснення планових заходів державного нагляду (контролю) у сфері техногенної та пожежної безпеки Державною службою з надзвичайних ситуацій: Постанова Кабінету Міністрів України від 05.09.2018 р. № 715. URL: http://zakon.rada.gov.ua/laws/show/715-2018-%D0%BF.
2. Методологія оцінювання корупційних ризиків у діяльності органів влади. Затверджено Рішення Національного агентства з питань запобігання корупції 02.12.2016 р. № 126. Зареєстровано в Міністерстві юстиції України 28 грудня 2016 р. за № 1718/29848.
3. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру: Розпорядження Кабінету Міністрів України від 22.01.2014 р. № 37-р. URL: http://zakon.rada.gov.ua/laws/show/37-2014-%D1%80.
4. ДСТУ IEC/ISO 31010:2013. Керування ризиком. Методи загального оцінювання ризику. Національний стандарт України (IEC/ISO 31010:2009, IDT). Київ: Мінекономрозвитку України, 2015. 73 с.
5. Strategic Research Action Plans 2016-2019. URL: https://www.epa.gov/research/strategic-research-action-plans-2016-2019.
6. Working Together. FY 2018-2022 U.S. EPA Strategic Plan. Washington: U.S. EPA, 2018. 56 p. URL: https://www.epa.gov/sites/production/files/2018-08/documents/fy-2018-2022-epa-strategic-plan-print.pdf.

7. Guidance: PRP Performance of Risk Assessments in RI/FS. URL: https://www.epa.gov/enforcement/guidance-prp-performance-risk-assessments-rifs.
8. Framework for Cumulative Risk Assessment. EPA/630/P-02/001F. Washington: U.S. EPA, 2003. 129 p.
9. Рекомендації щодо розробки системи управління охороною праці підприємства (з урахуванням вимог міжнародного стандарту OHSAS 18001-99 «Система менеджменту охорони здоров'я та безпеки персоналу»). Звіт з НДР, наук. керівн. Г.Г. Лесенко. Київ: ННДІОП, 2004. 132 с.
10. Методика визначення ризиків та їх прийнятних рівнів для декларування об'єктів підвищеної небезпеки. Нормативне виробничо-практичне видання. Держнаглядохоронпраці. К.: Основа, 2003. 191 с.
11. Бегун В.В., Горбунов О.В., Каденко И.Н. Вероятностный анализ безопасности атомных станций. К.: Випол, 2000. 558 с.
12. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України від 05.04.2007 р. № 877-V. URL: http://zakon.rada.gov.ua/laws/show/877-16.
13. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.
14. Глоссарий МАГАТЭ по вопросам безопасности. Терминология, используемая в области ядерной безопасности и радиационной защиты. Издание 2007 года. Международное агентство по атомной энергии. Вена, 2008. 303 с.
15. Серия изданий по безопасности МАГАТЭ, №75 – INSAG–6. Вероятностный анализ безопасности. Вена: МАГАТЭ. 1994.
16. Корн Г., Корн Т. Справочник по математике (для научных работников и инженеров). М.: Издательство «Наука», 1974. 832 с.
17. Component Reliability Data for Use in Probabilistic Safety Assessment. IAEA-TECDOC-478. Vienna: International Atomic Energy Agency, 1988. 298 p.
18. Survey of Ranges of Component Reliability Data for Use in Probabilistic Safety Assessment. IAEA-TECDOC-508. Vienna: International Atomic Energy Agency, 1989. 182 p.

Стаття надійшла до редакції 10.01.2019