https://orcid.org/0000-0002-0045-8586

УДК 004.02[004.9:614.8.084]

В.В. БЄГУН[*]

РОЗВИТОК ПАРАДИГМИ РОП НА ОСНОВІ ТЕОРЕТИЧНИХ ДОСЛІДЖЕНЬ У СФЕРІ БЕЗПЕКИ

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

Анотація. *Розглянуто впровадження та розвиток парадигми ризик-орієнтованого підходу (РОП). Продемонстровано можливості методик РОП категоризувати загрози за ступенем небезпеки, що дозволяє застосовувати інформаційні технології (ІТ) та більш ефективно проводити оптимізаційні заходи. Простежено поступовий перехід на парадигму РОП з точки зору розвитку ІТ та як шлях до незалежного (неупередженого) аудиту важливих параметрів безпеки. Аналізуються можливості та обмеження існуючих методик, показана тенденція щодо переходу до адаптивного управління безпекою. Вказано на можливості скорочення витрат на побудову моделей визначення числових значень ризику за рахунок розробки ймовірнісних структурно-логічних моделей за типами небезпечних об'єктів та виробництв. Відмічено значний потенціал вітчизняних розробок у напрямі розвитку і впровадження ймовірнісно-фізичного підходу до оцінки довговічності та надійності з використанням імовірнісних моделей на основі DM- та DN-розподілів в умовах обмеженої інформації щодо відмов. Продемонстровано ефективність переходу в атомній енергетиці України з початку 2000-х років на сучасні методи аналізу безпеки, що базуються на парадигмі РОП, де завдяки оновленню процесів розробки, плануванню заходів безпеки та державного контролю збитки від аварійних зупинок зменшилися більш, ніж у 10 разів. У той же час відмічено відставання нашої країни у впровадженні парадигми РОП в інших галузях виробництва та життєдіяльності. Сформульовано пріоритетні проблеми та задачі щодо розвитку ІТ, які нині потребують вирішення у нашій країні та у світі, для прискорення впровадження РОП у широке коло галузей виробництва та сфер життєдіяльності.*

Ключові слова: *ризик, безпека, ризик-орієнтований підхід (РОП), небезпечний об'єкт, імовірнісна структурно-логічна модель, адаптивне управління, залишковий ресурс.*

Abstract. *The paper considers the introduction and development of the risk-based approach (RBA) paradigm. It describes the capabilities of RBA methods to categorize threats by their level of danger, which allows the use of information technologies and the implementation of more efficient optimization measures. A gradual transition to the RBA paradigm from the point of view of IT development and as a way to the independent (impartial) audit of the main safety parameters has been traced. The possibilities and limitations of the existing methods are analyzed, and the trend toward the transition to adaptive security management is shown in the paper. The possibilities of reducing the costs of building models for determining the numerical values of risk due to the development of probabilistic structural and logical models by types of dangerous objects and productions are demonstrated. The significant potential of domestic developments concerning the development and implementation of a probabilistic-physical approach to the assessment of durability and reliability using probabilistic models based on DM- and DN-distribution functions in conditions of insufficient information on failures is described in the article. The work demonstrates the effectiveness of the transition to the modern methods of safety analysis based on the RBA paradigm in Ukraine's nuclear energy sector since the early 2000s. In this sector, thanks to the updating of development processes, safety planning measures, and government control, the damages resulting from emergency shutdowns have decreased by more than 10 times. At the same time, it has been noted that our country is lagging behind in implementing the RBA paradigm in other areas of production and life. To accelerate the implementation of RBA in a wide range of industries and spheres of life, the priority problems and tasks related to the development of IT, which require solutions in our country and all over the world, have been formulated.*

Keywords: *risk, safety, risk-based approach (RBA), dangerous object, probabilistic structural and logical model, adaptive management, residual life.*

DOI: 10.34121/1028-9763-2023-2-55-68

1. Вступ

Завдяки успішному досвіду впровадження парадигми ризик-орієнтованого підходу у регулювання безпеки у провідних країнах світу, де окупність вкладень у безпеку на основі ризик-орієнтованого підходу складала від 1,29 до 2,89 на одиницю вкладених коштів [1], нині парадигма ризик-орієнтованого підходу впроваджується глобально по всьому світу у широке коло галузей та сфер життєдіяльності. При цьому впровадження інформаційних технологій є локомотивом розвитку ризик-орієнтованого підходу (РОП) завдяки можливості використовувати більш складні методи розрахунку, можливості накопичувати та використовувати у розрахунках ризиків значні за обсягом бази даних щодо відмов обладнання, помилок персоналу та нормального функціонування обладнання, включаючи часові ряди даних. Тому дослідження щодо проблем впровадження і розвитку інформаційних технологій, спрямованих на розвиток методів ризик-орієнтованого підходу, є актуальними і такими, що у результаті можуть мати значний позитивний ефект як на рівні окремих галузей, так і в цілому на рівні держави.

На жаль, в Україні спостерігається суттєве відставання, крім ядерної галузі, у впровадженні парадигми ризик-орієнтованого підходу для регулювання безпеки та у впровадженні інформаційних технологій у сферу регулювання безпеки.

Вперше визначення «ризик-орієнтований підхід» з'явилося у керівництві FATF [2]: «Ризик-орієнтований підхід передбачає адаптацію заходів реагування з боку наглядових органів таким чином, щоб вони максимально відповідали оціненим ризикам. Цей підхід дозволяє наглядовим органам виділяти порівняно обмежені ресурси для ефективного зниження виявлених ризиків ВГ/ФТ (відмивання грошей/фінансовий тероризм) відповідно до національних пріоритетів». Це визначення з фінансової сфери прийнято на початку 2000-х років у дуже важливих міжнародних стандартах із боротьби з міжнародним фінансовим бандитизмом – вкрай великою небезпекою всього людства. Саме це вже підкреслює значення РОП як явища.

Але як метод парадигму управління безпекою прийнято було вважати, що вона відбувалася значно пізніше, що не зовсім вірно. Першість була у сфері безпеки. Ще в дослідженнях імовірнісних моделей Бірнбаума, Расмуссена в 70-ті роки було запропоновано на основі моделювання визначати найбільш важливі загрози та аналізувати можливі міри захисту. Саме це і є основою ідеології РОП. Застосування РОП в економіці та фінансах, хоча зараз це більш поширено, йшло паралельно, а більш поширено було можливе при більшій доступності статистичних даних та значно більших загроз. У сфері безпеки, ще в роботі «WASH 1400» у 1975 році проф. Расмуссен розробив повну ймовірнісну модель найбільш небезпечної події – руйнування активної зони ядерного реактора (core destruction – CD) й модель розповсюдження радіоактивного забруднення у навколишнє середовище та модель впливу небезпечних чинників радіаційної аварії на людей та довкілля. Тобто, у цій роботі бачимо усі складові кроки щодо методу аналізу небезпек, які потім із часом стали основою системного аналізу та стандартизовані як імовірнісний аналіз безпеки (ІАБ). Було зроблено розрахунок імовірності небажаної події (НП) та її наслідків, тобто, фактично було розроблено алгоритм оцінки ризику [3–4]. Саме тому цей алгоритм увійшов у стандарти як у сферу економіки, так і у сферу безпеки, тоді ще без назви РОП. Суть ризик-орієнтованого підходу у будь-якій сфері полягає у зниженні ризиків: контроль у зонах підвищеного ризику зростає, а в безпечніших зонах знижується або відсутній. Це дозволяє вчасно вживати необхідних заходів там, де це необхідно, та значною мірою економити ресурси. Таким чином, ресурси розподіляються нерівномірно, залежно від ризику, причому це впливає як на частоту, так і на глибину перевірок [6]. Такі важливі результати та висновки були узагальнені в міжнародних стандартах.

Отже, *мета статті* полягає у проведенні аналізу впровадження РОП в управління безпекою небезпечних галузей виробництва України у порівнянні зі світовою практикою за аналогією з ядерною галуззю України та визначення шляхів подальшого розвитку сучасних неадміністративних методів управління безпекою, що є умовою інтеграції України в європейське суспільство.

2. Стандартизація аналізів безпеки

Сучасні стандарти ЄС з безпеки засновані на понятті «ризику» і вимагають оцінок ступеня ризику, що забезпечує прозорість та чіткість управління безпекою. Одним із перших, вже у 2001 році, в ЄС існував міжнародний стандарт (МОП-СУОП – 2001) [6], де було запропоновано новий алгоритм управління безпекою за принципом РОП, а саме, було рекомендовано дотримуватися такого порядку пріоритетності запобіжних і регулювальних заходів:

• усунення небезпеки/ризику;

• обмеження небезпеки/ризику шляхом використання технічних засобів колективного захисту або організаційних заходів;

• мінімізація небезпеки/ризику шляхом проєктування безпечних виробничих систем, що передбачають заходи адміністративного обмеження сумарного часу контакту зі шкідливими виробничими чинниками;

• там, де небезпеки/ризики не можуть бути обмежені засобами колективного захисту, роботодавець повинен безоплатно надати відповідні кошти для індивідуального захисту, в тому числі на придбання спецодягу, і вжити заходів стосовно гарантованого забезпечення їхнього використання й технічного обслуговування.

Цей новий алгоритм управління безпекою реалізується з того часу на базі інформаційних (комп'ютерних) технологій та представляється такими основними процедурами:

• визначення (розрахунок) ризику;

• визначення припустимих значень ризику;

• порівняння розрахункових і припустимих значень;

• прийняття рішень щодо запобігання аваріям (зменшення ризику).

Кожна з цих процедур може бути і була реалізована різними методами, вибір яких залежить від багатьох факторів, як то: ціна ризику в галузі, стадії розвитку безпеки, рівень компетенції з безпеки (освіти) фахівців, законодавча база тощо [6].

Отже, у наведеному формулюванні основного визначення мова тільки про нагляд, що важливо, але не є головною цінністю РОП. Більш важливе застосування цих алгоритмів для управління безпекою, що й було використано у сфері безпеки АЕС у першу чергу в усьому світі.

Наступним важливим кроком у напрямі стандартизації стали міжнародні стандарти ICO 31000 та ICO 31010 Risk management – Risk assessment techniques [7, 8]. Як глобальний висновок розвитку парадигми РОП у виданні стандарту 2019 року бачимо [8]: «Організації всіх типів і розмірів стикаються з внутрішніми та зовнішніми факторами та впливами, через які стає неможливо визначити, яким чином і коли вони досягнуть своїх цілей. Вплив невизначеності на цілі організації визначається як «ризик». Будь-яка діяльність організації пов'язана з ризиком. Організації управляють ризиком за допомогою його ідентифікації, аналізу та подальшого рішення, чи слід його обробити з метою задоволення критеріїв ризику. Протягом усього процесу організації здійснюють комунікації та консалтинг із заінтересованими сторонами, управляють та аналізують ризик і засоби управління, які модифікують ризик із метою забезпечення того, що подальша обробка ризику не буде потрібна». Тобто, на світовому рівні визнається схожість процесів управління ризиком для усіх організацій, констатуються певний алгоритм процесів та їх ефективність. Даний Міжнародний Стандарт описує цей систематичний і логічний процес у деталях, покроково, наведено 42 методи визначення ризику. Перше видання цього стандарту було у 2009 році, звісно, стан-

дарти діють в усіх країнах ЄС. В нашій країні вони не діють, тому потрібно звернути на це пильну увагу. Нагадую, що в ядерній енергетиці України принципи РОП впроваджені з початку 2000 років [9], хоча аналізи безпеки АЕС за цими алгоритмами були зроблені наприкінці 90-х років.

Як підтвердження важливості цього наведемо ще одну витримку з документів керівництва FATF [2]: «У рамках ефективної системи ризик-орієнтованого нагляду наглядовий орган виявляє, оцінює і розуміє ризики ВГ/ФТ, існуючі в секторі (секторах) і у суб'єктів, віднесених до його компетенції, і постійно знижує ці ризики ефективним чином. Це включає створення надійної системи оцінки ризиків, яка дозволяє виявляти, вимірювати, контролювати та здійснювати моніторинг ризиків ВГ/ФТ». Як бачимо, йдеться про створення надійної системи оцінки ризиків як обов'язкового елемента управління за принципами РОП. У фінансовому секторі використовуються економіко-математичні моделі прорахунку ризиків із точністю до десятих відсотка, але в інших областях часто достатньо розділити ризики на групи небезпеки, що ми й бачимо зараз у діяльності більшості контролюючих відомств.

Цілком природно, що як нова парадигма РОП, заснована на моделюванні небезпечних систем та процесів, з'явилася з розвитком обчислювальної техніки, інформаційних технологій (ІТ) і нових методів аналізу, ІАБ тощо. Тільки з застосуванням ІТ стало можливим на основі глибокого системного (попереднього) аналізу виробництва визначення його ризиків (загроз) та способів запобігання. При цьому відбувається розгляд тисяч, іноді мільйонів способів реалізації ризику. Як вже йшлося, вперше роботи за цим алгоритмом виконані дослідниками із США у 1960–1970-ті роки у зв'язку з розвитком ІТ та цивільного авіабудування, атомної та хімічної промисловості [3, 4] і набули подальшого розвитку у багатьох роботах [10–15]. Важливо, що принципи РОП не заперечують знань правил та інструкцій із безпеки, які панували при застосуванні попередньої парадигми на основі принципу забезпечення 100 % безпеки. Ці інструкції та правила змінюються в результаті більш глибокого аналізу безпеки на основі РОП, переходу до принципу запобігання в результаті зміни контрольованих параметрів безпеки, що визначаються розрахунком, як результати моделювання. Тому суттєво змінюються також алгоритми контролю та управління безпекою [6]. РОП у контрольно-наглядовій діяльності передбачає зниження кількості державних перевірок у зонах, де ризик порушень менший. Таким чином, він знижує адміністративне навантаження на сумління підприємства.

Як концепція загального управління безпекою в ринкових умовах концепція РОП визначена світовим суспільством значно пізніше важливих досліджень у цьому напрямі. Основні сім принципів державного управління безпекою в ринкових умовах (РОП), викладені в Європейській директиві СЕВЕЗО [16] та концепції управління ризиками [17].

Це принципи: 1) прийнятності, 2) превентивності (запобігання), 3) мінімізації (АЛАРА), 4) повноти, 5) адресності (хто створює, той платить), 6) доцільного значення прийнятних рівнів, 7) інформування (декларування). Ці сім принципів у розвинутих країнах дійсно забезпечують належний рівень безпеки та відповідають новітнім концепціям безпеки і можливостям ІТ, завдяки чому управління переходить із наглядових (інспекційних) методів на економічні. Іншими словами, створюються умови, при яких вести бізнес із великими ризиками стає невигідно.

Доречно нагадати всі існуючі концепції управління, що важливо для створення розрахункових моделей.

Визначальна важливість для створення моделі визначення типу тієї або іншої концепції управління безпекою в тому, що концепція в залежності від початкової стадії розвитку безпеки задає об'єкту наступний алгоритм дій управління. На цей час світовим суспільством класифіковані такі парадигми (за послідовністю впровадження) [16]:

• забезпечення 100% безпеки (концепція нульового ризику) – це безліч правил безпеки, які зобов'язані забезпечувати конструктори машин й процесів і, безумовно, виконувати оператори, а спеціальні інспекції повинні це перевіряти – з 50-х років минулого століття;

• ризик-орієнтований підхід – попередження (запобігання) нещасних випадків і аварій на основі глибокого системного (попереднього) аналізу виробництва з метою визначення його ризиків (загроз) і способів їхнього попередження – з 70-х років минулого століття;

• культура безпеки – це такий набір характеристик і особливостей діяльності організацій і поведінки окремих осіб об'єкта, який встановлює, що проблемам безпеки, як таким, що мають найвищий пріоритет, приділяється увага, обумовлена їхньою значущістю, – з 90-х рр.;

• рентабельна безпека – стійкість роботи ОПН, АЕС, у першу чергу, у ринкових умовах розглядається в загальному виді, з урахуванням вартості заходів щодо безпеки й збитку від можливих загроз – з 2000-х.

До цього потрібно додати, що ідентифіковані три стадії розвитку адміністративного управління безпекою, які характеризуються відношенням ТОП менеджменту ОПН до питань безпеки [18]. Це потрібно враховувати при побудові моделі конкретного об'єкта, тому що не всі підприємства навіть однієї галузі мають однаковий ступінь розвитку безпеки. Як вже було сказано, моделювання за принципами РОП історично склалося на основі ймовірнісних моделей, на що є навіть відомі філософські обґрунтування та багато наукових праць.

Як розвиток імовірнісного моделювання та ІТ розроблена інформаційна технологія безпеки (ІТБ) [6], яка передбачає повну зміну функції управління безпекою в Україні, перехід на сучасні ринкові, економічні методи на заміну адміністративному – інспекційному нагляду. При цьому основою є ймовірнісне моделювання, але існують й інші методи. Розглянемо їх нижче.

3. Інші методи моделювання

Ризик є універсальною мірою рівня небезпеки, у наведених прикладах визначений методами ймовірнісного моделювання, але у рамках РОП можливе використання різних методів моделювання, кожен із яких має певні переваги та обмеження. Більшість методів (точніше 42) описані у згаданому міжнародному стандарті [8]. Для технічних систем переважно використовуються ймовірнісні методи. При цьому використання марковських аналізів можливе і є більш зручним для планування технічного обслуговування [6]. Але у той же час для моделювання ризиків від складних процесів виробництва, в яких важливу роль відіграє попередній стан системи (наприклад, стан активної зони ядерного реактора), використання марковських процесів можливе тільки для частин всієї системи (наприклад, системи захисту ядерної установки) і значно ускладнене для моделювання стану безпеки всієї системи. Тому при розробці методології ІТБ у більшості робіт було вирішено не використовувати марковські аналізи для моделювання ПНО у цілому. Марковські аналізи зручно використовувати на етапі планування коригуючих заходів для управління величиною ризику, як це було показано у [6].

Інший найбільш розповсюджений метод моделювання надійності складних систем – це використання мереж Петрі [6], але мережі Петрі мають певні проблеми при моделюванні динаміки подій та ситуацій множинних одночасних відмов і є менш зручні для розрахунку інтегральних показників ризику небажаних подій, тому при розробці методології ІТБ було вирішено у роботах з оцінок ризику їх не використовувати.

Найбільш зручним методом моделювання ризику від таких складних об'єктів, якими є ПНО, у рамках розробки методології ІТБ є методи дерев відмов (ДВ) – Fault tree

analysis (FTA) та дерев подій (ДП) – Event tree analysis (ETA) [6, 8, 12], тому що у рамках такого підходу можливо побудувати ЙСЛМ для всіх стадій розвитку аварій, розрахувати відповідні величини ризиків і на основі цих знань і знань небезпечних сполучень (взаємозв'язків) подій (мінімальних перерізів – МП) у побудованих ЙСЛМ розробити заходи щодо запобігання небезпек з урахуванням значимості подій. Перевагою ЙСЛМ є й те, що їх легко модифікувати шляхом додавання нових базисних подій (БП) у міру накопичення знань про ПНО. Ще дуже важливо, що ймовірність відмови складної системи за методологією ЙСЛМ в РОП визначається з урахуванням імовірності можливої помилки людини-оператора. Вони (помилки) трактуються як випадкові події, мають у моделях всі кількісні характеристики випадкової величини, закон розподілу ймовірностей при цьому теж визначається [6, 12]. Отже, нагадаємо загальні процедури РОП.

4. Короткий опис РОП

Застосування РОП стосується різнобічних аспектів, як то: методичний, математичний (розрахунковий) та законодавчий. Це перш за все. Пояснюємо на прикладі успішної реалізації концепції в ядерній галузі України. Наведемо шлях до безпеки атомної енергетики України як приклад успішного розвитку концепції.

4.1. Шлях до безпеки атомної енергетики України

Отже, у 1994 р. відбулася ратифікація Конвенції з ядерної безпеки та інших міжнародних угод, за якими аналіз безпеки атомних блоків став обов'язковим. Далі були розробка й прийняття вітчизняного законодавства, відповідного світовому (Закон України про використання ядерної енергії – 1995 р.). Одночасно в 1994–2000 рр. розпочалося інтенсивне навчання персоналу в ядерній галузі в європейських країнах та США методам імовірнісного аналізу безпеки (ІАБ) як основному методу моделювання складних систем АЕС та володінню комп'ютерними програмами (кодами), які передавалися нашій країні безкоштовно. (До речі, кожна така програма коштувала біля мільйона доларів!) Завдяки цьому, у 1996–2000 рр. було проведено ймовірнісний аналіз безпеки (ІАБ) реакторних установок ВВЕР-440 (РАЕС), а в 2002 р. здійснена міжнародна експертиза розрахунків, що дозволило виконати розробку науково обґрунтованих заходів підвищення безпеки АЕС. І тільки після цього (1998 р.) відбулося визначення РОП як концепції управління безпекою. Потім з'явилася можливість переходу на нові принципи управління (культура безпеки), прийняття заяв АЕС про прихильність принципам безпеки (2004 р.), що відповідало на той час загальносвітовому рівню. Важливо, що з 1996 року розпочалося навчання студентів технічних університетів новим методам аналіза безпеки АЕС, були впроваджені нові навчальні дисципліни.

Як бачимо, існують (обов'язкові) умови й кроки переходу на нову концепцію:

а) відповідність законодавчих вимог світовим;

б) освітня діяльність – навчання персоналу;

в) існування програмного забезпечення (ПЗ);

г) наявність підготовлених аналітиків та разраховувачів.

Як підсумок, шлях до безпеки йде через прийняття європейського законодавства, а саме, у цьому випадку, визнання економічних на основі РОП, а не адміністративних методів управління безпекою. Зазначимо, що РОП є попередником більш високого ступеня безпеки – парадигми «Культура Безпеки» (КБ), яка не заперечує РОП, і вже впроваджена в галузі атомної енергетики України. Оскільки мета статті – впровадження РОП в управління безпекою усіх галузей, коротко повторимо основні положення РОП.

4.2. РОП – опис основних процедур

Основні процедури визначені в багатьох працях [6, 8–12]. У найбільш загальному виді це:

• визначення рівня ризику;

• визначення допустимих значень ризику;

• порівняння розрахункових та допустимих значень;

• розробка заходів щодо запобігання ризику;

• освіта та підготовка персоналу.

На цей час маємо безпеку як навчальний предмет, що представлялася такими дисциплінами: «Охорона праці», «Безпека життєдіяльності», «Цивільна безпека». Але це не відповідає кращій світовій практиці. Тому зміна освіти теж стає задачею впровадження РОП [6].

Відповідно до згаданих стандартів ISO більш детально процеси управління техногенним ризиком визначаються таким чином:

1. Планування управління ризиками.
2. Ідентифікація ризиків.
3. Якісна оцінка ризиків.
4. Кількісна оцінка ризиків.
5. Планування реагування на ризики.
6. Реалізація прийнятого рішення.
7. Моніторинг і контроль.

На цьому (останньому) кроці виділяють внутрішній та зовнішній моніторинг, останній має функції державного, але це суттєво відрізняється від інспекційного контролю попередньої парадигми. Дані процедури детально неодноразово описані в багатьох публікаціях, мають відповідні методичні розробки [6].

Важливо розуміти визначення основних понять щодо безпеки, які існують у світовій і деякі в українській законодавчій (нормативній) базі [7–8, 18–20]:

• БЕЗПЕКА – допустимий рівень ризику.

• РИЗИК – кількісна міра небезпеки, що визначається функцією двох змінних – імовірності небажаної події й розміру збитку від неї.

• ЙМОВІРНІСТЬ НЕБАЖАНОЙ ПОДІЇ – (математичне) числове визначення очікування події.

• ЗБИТОК – летальні випадки (відносні) або кошти.

• УПРАВЛІННЯ РИЗИКОМ – (ISO 31000-2009): процес управління ризиками - систематичне застосування політики менеджменту, процедур та практик щодо комунікації, консалтингу, встановлення контексту, а також ідентифікації, аналізу, оцінки, дослідження, моніторингу та аналізу ризику (стандарт ISO 73:2009, визначення 3.1).

• ДОПУСТИМИЙ РИЗИК – ризик, який не перевищує на території небезпечного об’єкта та/або за його межею гранично допустимого рівня.

• АНАЛІЗ РИЗИКУ – систематичне використання наявної інформації для ідентифікації небезпек та визначення ризику для однієї людини, населення, майна, соціальних та техногенних об’єктів і навколишнього середовища.

• ОЦІНКА РИЗИКУ – процес визначення ймовірності виникнення аварій чи надзвичайних ситуацій та відповідних йому збитків.

• УПРАВЛІННЯ РИЗИКАМИ – процес прийняття рішень та здійснення заходів, спрямованих на забезпечення мінімально можливого ризику.

• ЛЮДСЬКИЙ ЧИННИК (ЛЧ) – це причини ризику, пов’язані з помилками людини.

Опис наведених вище основних процесів визначення ризику є у всіх сферах застосування РОП. Предметом аналізу у сфері безпеки стають всі небезпечні процеси та системи, наприклад, для АЕС, як найбільш складного об’єкта:

• всі об’єкти майданчика АЕС на всіх режимах роботи;

• всі можливі вихідні події аварій (обставини);
• надійність обладнання;
• процедури експлуатації та ремонтів;
• дії персоналу – людський фактор (ЛЧ).

Важливим є те, що врахування можливих помилок персоналу під час аналізу ризику у світовій практиці є обов'язковим, але у вітчизняних нормативних документах немає затвердженої методики цього напряму, тобто за офіційно діючими процедурами немає можливості оцінити ризик за світовими нормами в Україні.

Як основний результати наведених вище процедурних рішень аналізу й оцінки ризику отримуємо алгоритм розробки рекомендацій щодо зниження ризику [6, 9, 12], а саме:

• Визначення вражаючих факторів небезпек та можливих кінцевих станів.
• Побудова ймовірнісної моделі об'єкта – ДП, ДВ.
• Розрахунок імовірності небажаних подій. Генерація мінімальних перерізів (Min Cat).
• Аналіз значимості (важливості) (Ratio Importance).
• Аналіз чутливості (Sensitivity).
• Визначення подій, які найбільш впливають на ризик.
• Розробка плану модернізацій чи покращення стану об'єкта.

Це велика та кропітка робота. Наприклад, звіт з імовірнісного аналізу безпеки одного блока АЕС складає біля двох десятків томів, але виконана робота приносить значний економічний ефект, і, відповідно, покращуються показники безпеки, що взаємопов'язано. Так, основним показником безпеки АЕС за нормальних умов експлуатації є кількість аварійних зупинок блока на потужності. Звісно, захисні системи безпеки (СБ) включають аварійну зупинку реактора, якщо виявляється загроза неконтрольованого (непроєктного), тобто, небезпечного режиму. Зупинка роботи призводить до скорочення енерговиробітки, тобто, збитку, а він складає в середньому 1 млн доларів за добу відключення. На цьому прикладі легко зрозуміти зв'язок прибутку та безпеки (рис. 1). Скорочується кількість небезпечних ситуацій – зменшення ризику, зменшується збиток, зростає прибуток у десятки разів. Тобто, витрати на аналіз безпеки повертаються багатократно.

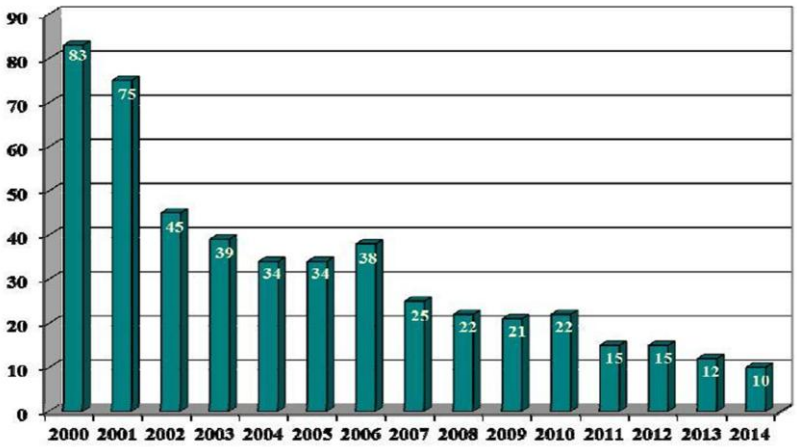

Рисунок 1 – Зменшення порушень на АЕС України із впровадженням нових концепцій управління

Після підтвердження ефективності РОП для АЕС у світі розпочалося активне впровадження концепції РОП і в інші небезпечні галузі виробництва. Звісно, задачі регулювання (управління) безпеки завжди були й будуть актуальними, тому що безпека є базовою потребою людини. На жаль, в Україні в інших, крім атомної енергетики, галузях це відбувається надто повільно.

Отже, в рамках впровадження РОП в інші небезпечні галузі України основні процеси й задачі, за аналогією з атомною галуззю, були сформульовані таким чином [6]:

• Розробка методик моделювання небезпечних систем.
• Оптимізація обслуговування складних систем із точки зору теорії надійності.

• Моделювання впливу людського чинника на надійність та безпеку.

• Створення (об'єднання) та ведення баз даних (БД) та баз знань (БЗ) з безпеки.

• Визначення критеріїв моніторингу безпеки на основі розрахункової моделі.

• Визначення шляхів розповсюдження небезпечних речовин у навколишньому середовищі.

• Розвиток теорії і практики управління ліквідацією НС з електронними радниками оператору.

• Розрахунок страхових внесків у залежності від рівня ризику об'єкта.

• Аналіз інформаційних потоків із безпеки у напівавтоматичному режимі.

Окремо потрібно висвітлити процедуру (моделювання) врахування можливих помилок персоналу під час моделювання небезпечних процесів – ЛЧ. Саме цією процедурою відрізняється застосування РОП у сфері безпеки та інших сферах застосування парадигми, фінансової тощо. Великі дослідження у цьому напрямі зроблені у США (корпорація Локхід (Lockheed) [10–13], але, на жаль, вітчизняних розробок у цьому напрямі майже немає. Наведемо основні тези цього розділу РОП.

4.3. Моделювання впливу людського чинника

Отже, в наведених згаданих прикладах моделей ІАБ (для АЕС) дії (помилки) оператора можуть враховуватися в таких варіантах [12]:

• як типи різних помилок під час виконання аварійних дій;

• помилки, що не призвели до відмов;

• помилки, що призвели до відмов;

• дії, що приводять до відмов;

• як успішні і аварійні послідовності;

• як дії по відновленню оператором функцій систем, що відмовили (RA);

• при аналізі взаємозалежності і взаємного впливу окремих подій (THERP).

Для аналізу помилок оператора світовим суспільством розроблено і впроваджено у практику ряд методик. Найбільш поширені такі методики аналізу і обліку людського чинника розроблені у США [12]:

• THERP – Визначення значущості помилок людини в техніці – Technique for Human Error Rate Prediction.

• HCR – Надійність людини як функція його здібностей – Human Cognitive Reliability.

• SLIM – Метод індексів імовірності успіху – Succes Likelihood Index Method.

• DNE – Прямі числові оцінки – думки (експертні оцінки) – Direct Numerical estimation.

• MAPPS – Метод моделювання дій (помилок) при техобслуговуванні – Maintenance Personnel Performance Simulation.

Опис та засоби застосування методик можна знайти у роботах [10, 12], але як було зазначено, всі названі методики, розроблені у США, спираються на ментальний досвід тієї країни, який суттєво відрізняється від українського. На тепер, в атомній галузі та інших ці розрахунки проводяться на основі THERP або на основі експертних оцінок. Тобто, на наш погляд, потрібна розробка вітчизняної методики для подальшого розвитку концепції РОП у державі.

5. Обґрунтування вибору типу методології та моделей безпеки

Більшість методів моделювання безпеки небезпечних об'єктів в ЄС засновано на експертних оцінках, які мають нормативну та методологічну підтримку [6–8]. Але ці методи майже не використовуються в Україні із причин різного розуміння поняття «експерт», про що

вже йшлося, а саме: відсутній нормативний механізм атестації експертів галузі, відповідно, і механізм відповідальності експерта за результати, якщо може статися великий ризик всупереч прогнозу. Більш того, у нашій країні частіше експертами є особи за посадою, а не за компетенцією, адже існують випадки займання посади не за правилами цивілізованого суспільства.

Отже, оскільки експерт зацікавлений у тому, щоб був позитивний висновок для замовника, йому за це платять кошти, логічно слідує від нього позитивна якісна оцінка: «середній» або «маленький» (низький) ризик. Існує й інша думка щодо більшого поширення експертних методів. Це те, що вони більш доступні, не потребують, на перший погляд, занадто високої компетенції модельєра та дорогого ПЗ. Частіше достатньо базової вищої освіти та належного досвіду роботи за спеціальністю, але, як сказано вище, для роботи цих методів в Україні потрібні законодавчі зміни. Тому основою моделей, що ми пропонуємо для розвитку РОП в Україні, є математичні (ймовірнісні) методи, які є більш принциповими та неупередженими, ніж експертні. Так, можливо кількісне (ймовірнісне) моделювання стримує його складність, не вистачає фахівців, тому хибно спрацьовує принцип «розумної достатності». Недостатній аналіз причин НС, що відбулися, призводить до неможливості їх більш детального моделювання і, відповідно, запобігання повторів НС [12].

Автори вважають суттєвим розвитком РОП запропоновані раніше «типові ймовірнісно-структурні моделі» [6]. Великі складнощі ймовірнісного моделювання в тому, що весь об'єм робіт (розрахунки) практично може виконати тільки спеціаліст-математик, але вони вирішуються в нашій країні за рахунок «типових моделей» галузі та спеціальних цифрових серверів із безпеки [6, 19]. Тому саме ця ідея, на наш погляд, є важливим кроком розвитку РОП в Україні й не тільки. Моделювання на основі ЙСЛМ, очевидно, дешевше навіть за експертне, за умови існування попереднє розробленої моделі та існуючого ПЗ у хмарних сервісах [20].

Хоча складнощі ймовірнісного моделювання доведено, але не зважаючи на це, більшість дослідників безпеки складних систем обирають саме такі моделі.

Ось, на нашу думку, основні переваги ЙСЛМ [6].

• Існує апробована світова практика використання моделей цього типу у ядерній галузі.

• Імовірнісні моделі дають достатньо інформації для побудови алгоритму управління: $u_i = u_i(x_i, P_i)$.

• Існує можливість забезпечити достатній рівень деталізації моделі, і, що дуже важливо, можна простежити вплив будь-якого елемента складної системи на ризик.

• Необхідність створення моделі об'єкта (кількісних оцінок ризику) визначається за алгоритмом РОП за процедурою якісного аналізу ризику – АВВН (FMEA).

При цьому [6]:

• якщо у матриці «ймовірність-наслідки» $[P,U]$ $\breve{R}$ $(S_{ij}) \in [A]$, ЙСЛМ потрібна (A, B, C, D – відповідні ранги матриці);

• якщо у матриці $[P,U]$ $\breve{R}$ $(S_{ij}) \in [C,D]$ – кількісний аналіз не потрібен.

До переваг ЙСЛМ потрібно віднести й можливість побудови моделі об'єкта будь-якої складності та можливість легкої зміни (уточнення) моделі. Професійні коди типу SAPFHIRE надають усе для цієї можливості. Дійсно, якщо існує складна система – об'єкт $O(B_j)$, який складається з N елементів (B_j) різної природи, що відображені в ЙСЛМ множиною Ŏ та базисними подіями X_{ij}, ймовірності $P(X_{ij})$ яких визначені, а в результаті моделювання визначений ризик R, маємо можливість навести адаптивний алгоритм управління безпекою на основі ЙСЛМ (визначення подій, що найбільше впливають на ризик) [6]:

1. Вибрати найбільш важливі події на площині важливості: $X_{ij} \in [A]$.

2. Перевірити чутливість та відібрати найбільш чутливі: $X_{ij}^{'}$ ={max Sensitivity Xij}.

3. Обрати події за умови: $P(X_{ij}^{''}) < P(X_{ij}^{'})$.

4. $\breve{O} \to O(B_j)$ (B_j елементи, які найбільше впливають на ризик).

5. Перевірити затрати і ресурси заміни $B_j : Q(X_{ij}^{''}) \to \min Q : dR < 0$.

6. Перевірити інші варіанти зменшення R, Q.

Управління $u_{i+1} = u_i(X_{ij}^{''}, P_i)$, обране у такий спосіб призводить до мінімального ризику з мінімальною витратою коштів на безпеку. Цей алгоритм покладено в основу розробки плану модернізацій чи покращення стану безпеки об'єкта (ОПН, АЕС) на основі ЙСЛМ і, як бачимо, на основі позитивного досвіду ядерної галузі (рис. 1), що приводить до дуже хороших результатів.

6. Адаптивне управління

Наступний крок розвитку РОП – розуміння поняття можливості управління безпекою (ризиком) як управління випадковими процесами з адаптацією. Звісно, управління частково спостережуваними випадковими процесами відоме давно, але в роботах [6, 14] доведено, що це поняття може бути поширено на більш загальні процеси та знайдені математичні оператори для саме цього управління безпекою.

Тобто, доведено, що теоретичною основою управління ризиком може бути адаптивне управління, короткий опис якого наведено нижче [6].

«Нехай x – керований імовірнісний процес з характеристикою інформації: $P \in \ddot{Y}$. Тоді (x_i, P_i) утворюють точку в певному просторі, $u_i \in U$ – управління, $z_i \in U$ – збурення – випадкові величини з імовірнісним розподілом: $dG(x_i, P_i, u_i, z_i)$.

Отже, маємо:

$$x_i = T_1(x_i, P_i, u_i, z_i), \tag{1}$$

$$P_{i+1} = T_2(x_i, P_i, u_i, z_i). \tag{2}$$

Також маємо управління:

$$u_i = u_i(x_i, P_i). \tag{3}$$

Послідовність перетворень $\{T_1, T_2\}_i$, $i = 0, 1, 2, \ldots$ *дає процес управління з адаптацією*

Характеристика управління

• Управління (3) має властивість адаптації в тому сенсі, що воно залежить від всієї доступної в момент i інформації P_i про процес. Для того, щоб інформація про процес із часом накопичувалася, необхідно спеціально обирати T_2 таким чином, щоб опис процесу P_{i+1} був більш повним, ніж P_i.

• Якщо зі станом x_{i+1} зв'язати показник якості управління $W(x_{i+1})$, то за рахунок більшої інформованості управління внаслідок адаптації цей показник може покращуватися.

• При цьому послідовність перетворень $\{T_1, T_2\}_i$, $i = 0, 1, 2, \ldots$ дає процес управління з адаптацією.

Для організації адаптивного управління ризиком (побудова операторів перетворень $\{T_1, T_2\}_i$) у дослідженні [6] пропонується використовувати ймовірнісні структурно-логічні

моделі (ЙСЛМ). Імовірнісні моделі дають достатньо інформації для побудови алгоритму управління: $U = \{u_i\}$, $u_i = u_i(x_i, z_i)$, наприклад, відсортовані за критерієм значущості МП. Саме названі властивості-можливості ЙСЛМ надають змогу створити набір операторів $\{T_1, T_2\}$ – адаптивний алгоритм управління безпекою на основі ЙСЛМ. Головним є визначення подій, які найбільше впливають на ризик, тобто елементів ЙСЛМ, що мають максимальну значущість та чутливість. У такому разі послідовність перетворень $\{T_1, T_2\}_i$, $i = 0, 1, 2, \ldots$ дає процес управління з адаптацією, що може постійно знижувати ризик із оптимальними витратами коштів.

7. Розробка методик визначення залишкового ресурсу як етап розвитку РОП

Ще в середині 90-х років у нашому інституті були розроблені стандарти визначення залишкового ресурсу тепломеханічного обладнання [20, 21], на основі яких розроблені відповідні методики. Відомо, що переважними процесами руйнування, які призводять до відмов тепломеханічного обладнання, є незворотні деградаційні процеси типу об'ємна та контактна втома, механічне зношування, корозія та старіння. На підставі рекомендацій стандартів ДСТУ 3004 та ДСТУ 3433 як теоретичну модель відмов тепломеханічного обладнання приймають дифузійний монотонний розподіл (*DM*-розподіл).
Функція розподілу (модель відмов) має вигляд

$$F(t) = DM(t, \mu) = \Phi\left(\frac{t-\mu}{\sqrt{ut}}\right),$$

де μ, n – параметри розподілу, t – час.

Ці основні характеристики DM-розподілу визначаються за статистикою відмов та відновлення за результатами підконтрольної експлуатації: математичне очікування середнього напрацювання на відмову, математичне очікування потоку відмов, математичне очікування потоку відновлень. Як результат визначають математичне очікування залишкового ресурсу:

$$\pi(\tau) = \frac{\left[\mu\left(1+\frac{\nu^2}{2}\right)-\tau\right]\Phi\left(\frac{\mu-\tau}{\nu\sqrt{\mu\tau}}\right)+\frac{\mu\nu^2}{2}\exp\left(\frac{2}{\nu^2}\right)\Phi\left(-\frac{\mu+\tau}{\nu\sqrt{\mu\tau}}\right)+\frac{\nu\sqrt{\mu\tau}}{\sqrt{2\pi}}\exp\left[-\frac{(\tau-\mu)^2}{2\nu^2\mu\tau}\right]}{\Phi\left(\frac{\mu-\tau}{\nu\sqrt{\mu\tau}}\right)}.$$

Роботи у цьому напрямі, виконані останнім часом [23–26] із прогнозування зносу контактного проводу залізничних шляхів та трубопроводів АЕС, показують майже абсолютний збіг результатів розрахунків за цим методом із практичними замірами зносу. Точніша оцінка надійності експлуатованих систем дозволяє забезпечити заданий рівень надійності, приймати ефективніші рішення про терміни подальшої експлуатації і вжиття заходів щодо забезпечення експлуатаційної надійності. Оскільки визначається ймовірність відмови на заданому інтервалі часу, маємо можливість розрахувати ризик, тому цей напрям правомочно також віднести до методології РОП.

8. Висновки

1. Парадигма РОП в управлінні безпекою є найбільш ефективною й допускає оптимізацію управління безпекою в ринковому розвитку господарства суто економічними методами за умов прийнятного ризику. Тому впровадження міжнародних стандартів із безпеки має бу-

ти головною задачею в Україні. Концепція РОП разом із цифровізацією суспільства мають бути затверджені законодавчо, як в Європі.
2. Запропоновані типові ЙСЛМ забезпечують повноту і адекватність моделювання об'єктів і систем на основі парадигми РОП. Це чи не єдиний швидкий шлях наближення до вимог Євросоюзу щодо управління безпекою за економічними критеріями. Позитивний приклад атомної енергетики підтверджує можливість переходу на світові стандарти управління безпекою в нашій країні.
3. Запропонована інформаційна технологія безпеки на основі ЙСЛМ забезпечує заміну застарілих державних адміністративних структур нагляду на сучасні технології управління на основі комп'ютерних технологій та ринкових механізмів страхування ризику. Це приведе до скорочення управлінських структур, зменшення втручання у бізнес та зменшення витрат бюджетних коштів.
4. Типові ЙСЛМ як основа сучасної ІТБ та методи оцінки залишкового ресурсу на основі ймовірнісно-фізічних методів є кроком у розвитку парадигми РОП, що надає можливості розпочинати роботи у напрямі підвищення безпеки в сучасних умовах розвитку ІТ, господарських відносин та права в Україні.
5. Потрібна розробка вітчизняних галузевих методик для подальшого розвитку концепції РОП в нашій державі, розробка типових ЙСЛМ за галузями виробництва та відповідного програмного забезпечення.
6. Потрібно створювати цифрові сервіси для визначення ризику ОПН та КВІ відповідно до інших цифрових сервісів, що вже існують у країні.
7. Освіта з безпеки має відповідати світовому рівню з вивченням курсів сучасних методів аналізу та оцінки ризиків різної природи.

СПИСОК ДЖЕРЕЛ

1. Health and Safety at Work: new EU Strategic Framework 2014–2020 – frequently asked questions. MEMO/14/400. Brussels: European Commission, 2014. 5 p.
2. FATF Recommendations (Financial Action Task Force). URL: https://www-fatf--gafi-org.translate.goog/en/home.html?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc.
3. Rasmussen N.C. Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400 (NUREG 75/014). Washington: U.S. Nuclear Regulatory Commission, 1975. 198 p.
4. Vesely W.E., Goldberg F.F., Roberts N.H., Haasl D.F. Fault Tree Handbook. NUREG-0492. Washington: U.S. Nuclear Regulatory Commission, 1981. 209 p.
5. РОП у сфері безпеки. URL: https://fireman.club/inseklodepia/risk-orientirovannyiy-podhod/.
6. Бєгун В.В. Методологічні основи інформаційної технології управління безпекою на основі ризик-орієнтованого підходу: дис. … д-ра техн. наук: 05.13.06. Київ, 2020. 553 с.
7. Международный стандарт ISO 31000. Риск Менеджмент – Принципы и руководства. ISO 31000:2009.
8. Risk management – Risk assessment techniques. International Standard IEC 31010:2019, IEC, Geneva, 2019.
9. Громов Г.В., Дыбач А.М., Севбо А.Е., Гашев М.Х., Бойчук В.С. Применение риск-информированных подходов в инспекционной деятельности. *Ядерна та радіаційна безпека*. 2010. № 3 (47). С. 9–15.
10. Blakman H.S. Human Reliability Assessment Training Course. Idaho: INL, 1995. 121 p.
11. Bickel J.H., Kelly D.L., Leahy T.J. Fundamentals of Probabilistic Risk Assessment (PRA). Idaho: INL, 1995. 305 p.
12. Бегун В.В., Горбунов О.В., Каденко И.Н., Письменный Е.Н., Зенюк А.Ю., Литвинский Л.Л. Вероятностный анализ безопасности атомных станций: учебн. пособ. Киев: НТТУ КПИ, 2000. 568 с.
13. Handbook of Parameter Estimation for Probabilistic Risk Assessment. NUREG/CR-6823 SAND2003-3348P. Washington: U.S. Nuclear Regulatory Commission, 2003. 294 p.

14. Методика визначення ризиків та їх прийнятних рівнів для декларування об’єктів підвищеної небезпеки. Нормативне виробничо-практичне видання. Держнаглядохоронпраці. К.: Основа, 2003. 191 с.
15. Бєгун В.В. Загальні питання стохастичного моделювання небезпек виробництв. *Моделювання та інформаційні технології*: зб. наук. праць ІПМЕ ім. Г.Є. Пухова НАН України. К., 2008. Вип. 45. С. 198–203.
16. Директива Ради 96/82/ЕС від 9 грудня 1996 р. стосовно контролю небезпеки від великомасштабних аварій, що включають небезпечні речовини. *Офіційний журнал L 010*. 1997. 14.01. С. 0013–00.
17. Хміль Г.А., Буравльов Є.П., Гетьман В.В., Бєгун В.В. Концептуальний підхід до управління ризиками надзвичайних ситуацій техногенного і природного характеру. *Екологія і ресурси*: зб. наук. праць ІПНБ РНБО. К., 2007. С. 53–63.
18. Серия изданий по безопасности МАГАТЭ, №75 - INSAG-3. Основные принципы безопасности атомных электростанций. Вена: МАГАТЭ, 1989. URL: https://www.iaea.org/sites/default/files/31104784445_ru.pdf.
19. Кодекс цивільного захисту України. Законодавство України. URL: http://zakon1.rada.gov.ua/laws/show/5403-17.
20. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України від 05.04.2007. N 877-V. URL: https://zakon.rada.gov.ua/laws/show/877-16#Text.
21. Бєгун В.В., Волошин О.Ф., Бєгун С.В. Оптимізація контролю безпеки торговельно-розважальних комплексів на основі аналізу моделей визначення ризику. *Інформаційні технології та комп’ютерне моделювання*: матеріали міжнар. наук.-практ. конф. (м. Івано-Франківськ, 15–16 грудня 2022 р.). Івано-Франківськ: п. Голіней О.М., 2022. С. 4–6.
22. ДСТУ 3004-95. Надійність техніки. Методи оцінки показників надійності за експериментальними даними. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=51308.
23. ДСТУ 3433-96. Надійність техніки. Моделі відмов. Основні положення. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=93624.
24. Стрельников П.В. Оценивание надежности оборудования управляющих систем и машин в условиях малой статистики или отсутствия отказов. *УСиМ*, 2013. N 6. С. 49–52.
25. Федухин А.В. К вопросу о прогнозировании остаточного ресурса изделий электронной техники. *Математичні машини і системи*. 2020. № 1. С. 149–156.
26. Федухин А.В., Муха Ар.А. Оценка остаточного ресурса высоковольтных быстродействующих выключателей тяговой электросети железных дорог. *Молодий вчений*. 2022. № 1 (101). С. 120–123.
27. Федухін О.В., Муха Ар.А. Оцінка залишкового ресурсу контактного проводу електрофікованих залізничних доріг. *Математичні машини і системи*. 2022. № 2. С. 91–101.

Стаття надійшла до редакції 11.05.2023