УДК 621.039.586

В.В. БЄГУН[*], В.Ф. ГРЕЧАНІНОВ[*], В.П. КЛИМЕНКО[*]

ЩОДО ПИТАНЬ ПРО СУЧАСНІ МЕТОДИ РЕГУЛЮВАННЯ БЕЗПЕКИ

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

Анотація. *У статті розглядаються сучасні проблеми регулювання безпеки в Україні, аналізуються причини незадовільного стану безпеки в різних сферах. Описані сучасні стратегії управління безпекою на основі імітаційного ймовірнісного структурно-логічного моделювання.*
Ключові слова: *безпека, ризик, аварія, потенційно небезпечний об'єкт, моніторинг безпеки, культура безпеки.*

Аннотация. *В статье рассматриваются современные проблемы регулирования безопасности в Украине, анализируются причины неудовлетворительного состояния безопасности в различных сферах. Описаны современные стратегии управления безопасностью на основе имитационного вероятностного структурно-логического моделирования.*
Ключевые слова: *безопасность, риск, авария, потенциально опасный объект, мониторинг безопасности, культура безопасности.*

Abstract. *The problems of modern safety regulation in Ukraine are regarded, the causes of poor safety in various fields are analyzed. The current safety management strategy based on probabilistic simulation of structural and logical modeling is presented.*
Keywords: *safety, risk, accident, potentially dangerous object, safety monitoring, safety culture.*

1. Вступ

На території Україні розташовано більше 555 тис. підприємств, з них 46% приватної форми власності, 39% – колективної й тільки біля 15% – державної. Існують більше 20 тис. потенційно небезпечних об'єктів (ПНО), біля 8 тис. об'єктів підвищеної небезпеки (ОПН), 15 енергоблоків АЕС, розгалужена газотранспортна система, нафтопродуктопроводи та ін.

Безумовно, безпека людини (громадянина) є одним із основних параметрів життя, тому безпека взагалі та техногенна безпека, зокрема, контролюються державою. Методи та форми контролю, міра втручання та санкції при порушеннях залежать від держави, її устрою, форми власності тощо. В умовах минулої планової економіки та народної власності не тільки уповноважені контрольні органі, але й кожен громадянин мав право (й обов'язок) клопотатися про збереження соціалістичної власності.

В умовах капіталістичних відносин сьогодення все навпаки. Приватна власність є складовою приватного життя, зовнішнє втручання переслідується за законом. З іншого боку, норми техногенної безпеки все ж повинні виконуватися, але зовнішнє втручання з боку держави допускається тільки при порушенні безпеки персоналу, населення або довкілля. Власністю розпоряджається господар, і якщо немає порушень безпеки, навіть при незадовільному збереженні об'єкта, держава не має права на втручання. На жаль, не все це усвідомлено в нашому суспільстві, а законодавство суперечливе і має численні недосконалості. Ще заважають й застарілі звички фахівців з безпеки на їх безмежні права та високий рівень корупції в державі. З цих реалій і будуються відносини у сфері техногенної безпеки. Як повинно бути, які документи є обов'язковими, а які є пережитком минулого, потрібно з'ясувати найближчим часом на державному рівні.

2. Аналіз проблеми контролю безпеки

Аудит техногенної безпеки – одна із основних функцій Держави. Існують спеціально уповноважені центральні органи влади (ЦОВ), яким делегуються функції перевірок. Звісно,

ISSN 1028-9763. Математичні машини і системи, 2013, № 4

фінансування перевірок ЦОВ відбувається за бюджетні кошти, воно залежить від чисельності контролюючих інспекцій та алгоритмів контролю (моніторингу). Алгоритми моніторингу, у свою чергу, відповідають загальним принципам забезпечення безпеки – концепції або філософії безпеки.

Аналізуючи фактичний стан процесів контролю та регулювання техногенної безпеки в Україні, можна побачити відображення тільки самих старих принципів, включаючи принцип планової економіки соціалістичної форми власності – "забезпечення 100% безпеки" (навіть у чинному законодавстві [1]). Більш передова філософія безпеки в Україні працює поки тільки в ядерній галузі. Нові принципи: ризик-орієнтованого підходу, культури безпеки, операційного ризику впроваджуються на превелику силу, що обертається втратами як для підприємства, так і для держави. На нашу думку, впровадження передових методів забезпечення безпеки гальмується перш за все складними методами контролю безпеки за цими новими концепціями, адже потрібно визначати поточне кількісне (числове) значення ризику, до чого держава й суспільство не готові ні з наукової, ні з освітянської й виконавчої позицій. Тому розвиток і впровадження новітніх принципів моніторингу безпеки, оптимізація алгоритмів контролю й визначення кількісних значень ризику є дуже важливою й актуальною задачею для науки й суспільства.

Математична задача оптимізації державного моніторингу за критеріями мінімізації ризику для персоналу, населення та довкілля й мінімізації витрат державних коштів при цьому є новою, також, як і задача визначення ризику ОПН за процедурами моніторингу ОПН. На цей час в Україні рішення цієї задачі відбувається експертними методами на якісному рівні. Освіта з безпеки, за рідкісним винятком, теж продовжує теми 70-х років минулого сторіччя, що суттєво гальмує впровадження й розвиток нових принципів регулювання безпеки у зв’язку з недостатньою кількістю підготовлених фахівців, тобто вимагає радикального реформування. Всі ці три задачі пов’язані між собою, взаємозалежні і є предметом даної роботи.

У процесі регулювання безпеки можна виділити важливі складові, які аналізуються в роботі:

1. Базові принципи – філософія – у який спосіб (метод) управління більш ефективне.

2. Методична база, що ґрунтується на законах.

3. Визначення поточного стану безпеки – ризику для персоналу, населення та довкілля.

4. Підтримка належного рівня безпеки.

5. Контроль досягнутого поточного рівня.

6. Навчання виконавців.

7. Планування заходів зменшення рівня ризику для персоналу, населення та довкілля.

Це соціальні процеси, вони взаємозалежні й впливають на все суспільство, залежать від суспільної думки (свідомості), обстановки та ментальності нації.

Відповідно до Закону України [2] (ст. 5), здійснення державного нагляду повинне відбуватися шляхом оцінок ступеня ризику від здійснення господарської діяльності. Таким чином, ступінь ризику з 2008 року законодавчо стає загальною характеристикою рівня безпеки будь-то техногенна, промислова, пожежна безпека, охорона праці або якість продукції, що випускається підприємством. Цим продемонстроване бажання Держави увійти в Європейське співтовариство, її нормативно-правову базу зокрема. Причому, визначення ключового поняття "ризик" приводиться в цьому законі також у його європейському розумінні, на відміну від раніше прийнятого законодавства, у тому числі й Закону про об'єкти підвищеної небезпеки [3], а саме: «ризик – кількісна міра небезпеки, що визначається фун-

кцією двох змінних – імовірності небажаної події й розміру збитку від нього». Для цілей розрахунків вважають:

$$R = P \times U, \qquad (1)$$

де змінна P – це ймовірність аварії (небажаної події), а U – це розмір її наслідків (збиток). Оскільки обидва співмножники в формулі (1) випадкові величини, то й ризик R є випадковою величиною. З чого слідує, що завдання контролю (моніторингу) безпеки має бути представлено як алгоритм перевірки випадкової величини, що є багатовимірною функцією дійсних змінних. Але на сьогодні це не відповідає дійсності. Чинною інструкцією з перевірки стану безпеки [4] не передбачено моделювання процесів.

Для однозначного розуміння й постановки задачі наведемо стислий опис проблеми.

3. Опис об'єкта моделювання. Етапи розвитку безпеки

У світовій історії розвитку принципів забезпечення безпеки проглядаються чотири етапи [5]. Кожному етапу розвитку безпеки відповідає певна філософія безпеки та державного регулювання. Аналізуючи розвиток безпеки, на думку авторів, можна виділити такі філософії безпеки:

1. Забезпечення 100% безпеки.
2. Ризик-орієнтований підхід (РОП).
3. Культура безпеки – сучасна філософія безпеки АЕС.
4. Рентабельна безпека – філософія ринкових відносин.

Для кожної філософії безпеки розробляються свої, особливі алгоритми контролю й регулювання – стратегії забезпечення безпеки. Для можливості математичного моделювання процесів наведемо опис визначених стратегій та етапів розвитку безпеки.

3.1. Забезпечення 100% безпеки

Філософія забезпечення 100% безпеки зародилася з початком промислового розвитку – це безліч правил безпеки, які зобов'язані забезпечувати конструктори машин і, безумовно, виконувати оператори. Метод створення правил-заборон щодо безпеки після того, як нещасний випадок або аварія відбулися, привів до тієї великої безлічі правил відносно безпеки, які існують у вітчизняному законодавстві у виді «інструкцій», «зводів правил» та ін. Така політика існувала у свій час у більшості промислово розвинених країн. Існувала вимога забезпечити промислові машини захистом їхніх операторів від усіх небезпек, пов'язаних з роботою на цих машинах. Періодично виникаючі нещасні випадки або аварії ліквідувалися спеціальними численними загонами рятувальників, а при нормальних умовах дотримання встановлених правил контролювалися численною армією технічних інспекторів. Пізніше було доведено, що, коли всі небезпеки усунуті й контрольовані, то неможливо організувати процес виробництва взагалі. Підприємці вважали контроль безпеки урядовими (зовнішніми) структурами тягарем, що заважає виробництву. Ця філософія була визнана світовим суспільством неправильною, вона протирічила основним принципам ринкових відносин, тому розвинені країни відмовилися від таких принципів з середини 70-х років минулого століття. Але в умовах минулої планової економіки України у більшості процесів контролю все залишилося без змін до цього часу.

3.2. Ризик-орієнтований підхід (РОП)

З розвитком обчислювальної техніки й нових методів аналізу з'явилася нова філософія – попередження (запобігання) нещасних випадків і аварій. Це стало можливим на основі глибокого системного попереднього аналізу виробництва з метою визначення його ризиків (загроз) і способів їхнього попередження на основі моделювання. Ця філософія забезпе-

чення безпеки одержала ім'я ризик-орієнтований підхід (РОП, у сучасній літературі РІП – ризик-інформований підхід). Основні методи й принципи цього підходу описані в численних статтях та монографіях [6, 7]. Принципи РОП не спростовують знань правил і інструкцій з безпеки, які панували на першому етапі.

Законом про об'єкти підвищеної небезпеки [3] передбачена кількісна оцінка ризиків відповідно до процедури декларування безпеки. Методикою визначення ризику [8] є процедури моделювання для кількісної оцінки ризиків, визначення ймовірності виникнення аварій і впливу їхніх наслідків на діяльність об'єкта згідно з формулою (1). Це теоретично допомагає приймати оптимальні рішення відповідно до певних алгоритмів і уникати невизначеності у сенсі керування при цьому [9]. На основі знань, заснованих на дослідженні ймовірнісної моделі виробництва, можливо провести достовірні оцінки ризику. Побудова й дослідження таких моделей засновані на повних знаннях структури й процесів виробництва та теорії ризиків. Це, по суті, більш строге (упорядковане) виконання основних принципів (правил) безпеки (етап 1), тому що враховуються не тільки якісні принципи (порушення правил), але й їх кількісні (частотні, імовірнісні) характеристики. Дійсно, вся цінність імовірнісної моделі полягає в тому [7, 9], що:

• з множини можливих небезпечних подій виділяються найбільш імовірні небезпечні сполучення подій для цього виробництва;

• на підставі отриманих при побудові моделі якісних, логічних і частотних характеристик можливих подій виділяються найбільш важливі події.

Відмітимо, що важливість для безпеки можливих (базисних) подій, за результатами моделювання, може відрізнятися в декілька порядків! Таким чином, філософія РОП дає додаткові знання, які дозволяють виконувати попередження нещасних випадків і надзвичайних ситуацій, а в підсумку істотно, у десятки разів, знизити витрати на безпеку та рівні ризику.

3.3. Культура безпеки

Принципи РОП діють і зараз у сфері регулювання безпеки в усіх розвинених країнах. Проте, подальший розвиток безпеки привів до філософії культури безпеки. Культура безпеки – сучасна філософія безпеки, заснована на вихованні мотивів "безпечного поводження (дій)" персоналу. Ця нова концепція забезпечення безпеки на основі принципів "Культури безпеки" зародилася на початку нового XXI сторіччя й впроваджена тільки для АЕС. Сутність культури безпеки полягає в досягненні того, щоб увага до безпеки приділялася організаціями і окремими особами. Формується загальний психологічний настрій на безпеку, що допускає самокритичність і самоперевірку, виключає благодушність і передбачає розвиток почуття персональної відповідальності й загального саморегулювання в питаннях безпеки.

За визначенням [10], культура безпеки – це такий набір характеристик, особливостей діяльності організацій і поводження окремих осіб, який встановлює, що проблемам безпеки, як тим, що володіють вищим пріоритетом, приділяється увага, обумовлена їхньою значимістю.

Уже з визначення ясно, що ця філософія вимагає ще більш глибоких знань безпеки виробництва, ніж попередні. Більше того, необхідно домагатися, щоб знання перейшли в переконання, які лягають в основу мотивації всіх дій персоналу небезпечного виробництва від простого виконавця до директора. Із психології безпеки [11] відомо, що домогтися такого поводження працівників – складне завдання. Шляхи його рішення проходять через професійний відбір, навчання й виховання, результативні діючі економічні стимули. Діяльність з розвитку культури безпеки здійснюється з метою безперервного підвищення безпеки шляхом удосконалювання управління та формування відношення персоналу до безпеки, що забезпечує правильне і безпечне виконання робіт, створення атмосфери відкрито-

сті та взаємоповаги [11]. Ця передова філософія безпеки рекомендована для впровадження в усіх небезпечних виробництвах.

3.4. Рентабельна безпека

На думку російських учених [12], стійкість роботи ОПН, АЕС у першу чергу у ринкових умовах необхідно розглядати ще у більш загальному виді, з урахуванням вартості заходів щодо безпеки й збитку від можливих загроз. Такий підхід відповідає філософії рентабельної безпеки й принципу ALARA і є найбільш загальним. Тобто АЕС й ОПН, що працюють у ринкових умовах, мають потребу в рентабельній безпеці, у проведенні економічно ефективних модернізацій усіх виробничих процесів. Це зовсім нова філософія безпеки. Потрібні системи й механізми керування, зв'язані з вартістю ризику й економічних вигід від зниження ризику. У цьому новому, навіть для атомної енергетики, напрямі починають працювати російські й закордонні фахівці [13]. На ОПН України ця філософія безпеки ще також не впроваджена.

4. Моніторинг – процедура управління безпекою. Опис процесу моніторингу

Моніторинг і контроль параметрів (підприємства) є обов'язковою процедурою регулювання безпеки для кожної філософії забезпечення безпеки. Вони проводяться з метою перевірки дотримання вимог встановлених норм безпеки (ризику) для персоналу, населення й навколишнього середовища. Види й процеси моніторингу і контролю залежать від прийнятої в державі концепції безпеки. Моніторинг, що здійснюється спеціалізованим підрозділом об'єкта, називають внутрішнім. Моніторинг, що здійснюється зовнішніми контролюючими органами це зовнішній моніторинг. Функції й ролі різних типів моніторингу залежать від філософії та стадії розвитку безпеки. На першій стадії розвитку безпеки ці типи процесів не взаємодіють, закриті один від одного. В умовах ринкового господарювання, приватної власності і при повній відповідальності керівника (хазяїна) виробництва за стан безпеки моніторинг також можливо поділити на два види:

- внутрішній – самоконтроль безпеки підприємства;
- зовнішній – контроль безпеки державними службами.

Цілі стають більш конкретні, внутрішній моніторинг організується підприємством для безаварійної роботи, тобто безпека й високі економічні показники не суперечать один одному. Усвідомлюється, що якісний внутрішній моніторинг можливий на основі кількісних оцінок (розрахунків) ризику. У першу чергу здійснюється контроль важливих для безпеки параметрів. Це контроль на основі попереднього системного аналізу, він оптимізується за допомогою цих розрахунків. Надлишковий контроль, також, як і його недолік, призводить до зниження ефективності виробництва, даремної витрати ресурсів.

Зовнішній моніторинг за стратегією РОП має бути тільки по параметрах, які важливі для безпеки регіону розташування ОПН. Держава повинна виконувати важливу функцію контролю безпеки без втручання у процеси виробництва на основі дозвільної системи регулювання безпеки та системи страхування ризиків. Частота державного контролю залежить від небезпеки процесів та виробництв – ступеня ризику, що створює підприємство для персоналу, населення та довкілля. Це є однією з головних переваг стратегії РОП у порівнянні з попередньою.

5. Процеси розвитку аварій – узагальнення для моделювання

Управління ризиками техногенного і природного характеру має бути з урахуванням можливих аварій та ймовірності їх проходження. На основі досвіду аналізу аварій та аварійних ситуацій [14] можна стверджувати, що процеси розвитку аварій, незважаючи на їх розмаїтість, мають однакові етапи та критичні точки або стадії (рис. 1). Дійсно, на рис. 1 відо-

бражено п’ять можливих стадій аварій: виникнення вихідних подій аварій (1), спрацювання або відмова захисних систем (бар’єрів) (2), аварійні дії персоналу (3), успішне припинення аварій або перехід аварій на рівень НС (4), ліквідування НС (5). Як бачимо, можливий аварійний ланцюг починається з виникнення вихідних подій та закінчується або успішним припиненням аварії персоналом, або діями рятувальних підрозділів у гіршому випадку. Кожна зі стадій уявляє собою множину дій або процесів, яка частіше відома заздалегідь на основі досвіду експлуатації. Так, наприклад, множина вихідних подій для АЕС – $\hat{J}$ у більшості досліджень обмежена числом порядку 10^2, причому для кожного $j \in \hat{J}$ відомі значення ймовірності P_j та функція розподілу ймовірності $P_j = F(x)$. Кожна з вихідних подій уявляє собою відмову обладнання або системи нормальної експлуатації, помилку персоналу чи зовнішні екстремальні умови. Друга множина подій $\hat{S}_n$ – спрацювання або відмова захисних систем (бар’єрів) – уявляє собою залежні від вихідної події сполучення двійкових функцій систем безпеки (захисних бар’єрів). Якщо маємо множину S_n систем безпеки, то для припинення аварій достатньо послідовне спрацьовування: $(S_n)_j = 0$. Множина аварійних дій персоналу M_A розглядається у відповідних аварійних інструкціях, але реальні дії персоналу під час аварії $A_j \in M_A$ не завжди відповідають інструкціям, тобто важливо враховувати ймовірність помилки людини (оператора). Дії рятувальних підрозділів $AP_j \in M_p$ – одна з п’яти ланок взаємопов’язаних подій (процесів), інакше кажучи, якщо спрацьовують системи безпеки при виникненні вихідних подій або персонал має достатні знання та навички, то й підрозділи МНС не потрібні. Тому сучасна теорія безпеки (й законодавство) рекомендує розглядати для кожного ризику всі можливі стадії виникнення та розвитку аварій в їх зв’язку, оскільки вони є одним ланцюгом [14] протидії перетворення вихідної події в масштабну аварію. Тривалість ланцюга залежить від кожної ланки і якщо, припустимо, ми вкладаємо великі кошти в кількість, навчання та технічні засоби (оснащення) рятувальних підрозділів, незважаючи на попередні умови виникнення та розвитку аварій, то тим самим ми не зможемо докорінно покращити рівень безпеки. В кращому випадку можемо мати менші чи більші наслідки (більше чи менше число загиблих та постраждалих).

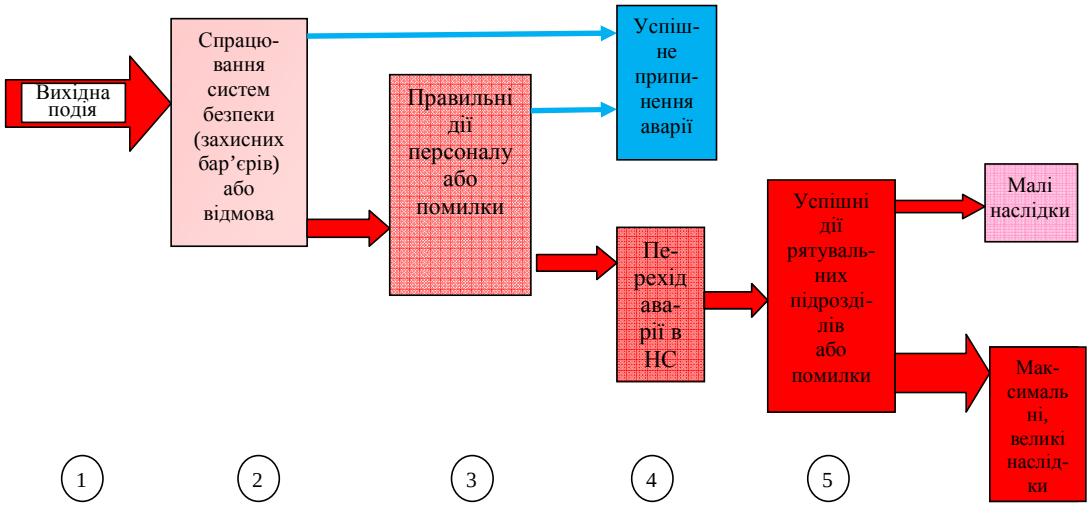

Рис. 1. Стадії виникнення та розвитку аварій

Як висновок, для цілей моделювання ризику важливо розглядати задачі управління безпекою в комплексі, як вони є на виробництві, без штучного розподілу їх за контролюючою організацією: ОП, МНС, ЦЗ, як то склалося історично на пострадянському просторі.

Дійсно, контроль порушень умов небезпечної праці робітником – це завдання ОП, але якщо в результаті може статися аварія, порушення стає об'єктом втручання рятувальних служб МНС, аварія великого масштабу може призвести до необхідності захисту населення – ЦЗ. Тобто маємо залежність для ризику аварій:

$$R_A = \hat{J} \bigcap S_n \bigcap M_A \bigcap M_P. \qquad (2)$$

З іншого боку, неприпустимий і зворотний сценарій – абсолютна надія тільки на запобіжні заходи та системи безпеки. Ймовірність виникнення аварій не може бути зменшена до нуля, також, як і неможливе виключення гірших сценаріїв на кожному етапі. Тобто маємо: задачу оптимального управління ризиком об'єкта потрібно розв'язувати в загальному виді [15], з урахуванням усіх (п'яти) процесів виникнення та розвитку можливих аварій. Очевидно, що процеси виникнення аварій цілком вкладаються в схему рис. 1 та формули 2 для усіх техногенних ризиків. Моделювання статистичної динаміки цього процесу можливе за допомогою ланцюгів Маркова лише в загальному виді. Для техногенних ризиків найбільш поширені ймовірнісні аналізи безпеки (ІАБ) на основі логічних імовірнісних структур процесів і виробництв – графів: дерев подій (ДП) та дерев відмов (ДВ) [7, 9].

6. Методи визначення ризику техногенної небезпеки

Цій проблемі присвячена велика кількість наукових праць [7–9], існують навіть міжнародні стандарти, де описані методи визначення ризику [16]. Сучасне українське законодавство [2, 3, 8], яке теж базується на ризик-орієнтованому підході, вимагає перегляду й детального аналізу всіх можливих сценаріїв аварій та всіх можливих вихідних подій як цілісної системи забезпечення безпеки персоналу, населення та довкілля. Подібна потреба оцінки безпеки виникає у кожного суб'єкта діяльності небезпечних технологій у таких процесах: 1) декларування безпеки й отримання ліцензії на небезпечну діяльність; 2) оцінка рівня безпеки для страхування; 3) після виникнення випадкових небезпечних подій для оцінки рівня безпеки того, що відбулося; 4) під час контролю (інспекцій ЦОВ).

У рамках оцінок та аналізу ризику на основі ймовірнісних структурно-логічних моделей можливо здійснити перегляд сценаріїв та визначити кількісні критерії. Кількісні розрахунки дозволяють визначити ймовірності виникнення аварій, імовірності переходу аварії з однієї стадії в наступну, умови такого переходу, математичну значимість усіх випадкових подій, що дозволяє оптимальним чином робити розподіл коштів на запобігання аварій та ліквідацію наслідків. Оскільки ризик у кожному конкретному випадку залежить від параметрів безпеки підприємства $\left(\hat{J}, S_n, M_A\right)$, то з цього слідує, що й сили та засоби реагування залежать від цих параметрів. Тому завдання визначення ризику важливе не тільки для попередження небезпеки, а й для регулювання розташування сил реагування. З математичної точки зору, це можливо описати в такому виді: ризик R є функцією, як мінімум, таких 6 змінних:

$$R = F\left(x1,\ x2,\ x3,\ x4,\ x5,\ x6\right), \qquad (3)$$

де $x1$ – всі ймовірні сценарії аварій для всіх режимів роботи;
$x2$ – всі можливі вихідні події, природного характеру тощо;
$x3$ – зношеність основного обладнання та статистика його відмов;
$x4$ – типи захисного обладнання та його стан;
$x5$ – навченість персоналу;

$x6$ – наслідки з урахуванням природно-кліматичних умов.

Для проведення кількісних розрахунків створюється ймовірнісна структурно-логічна модель (ІСЛМ) об'єкта, яка складається з дерев подій (ДП) – сценаріїв можливих аварій та дерев відмов (ДВ) – моделей можливих відмов існуючих систем захисту [9, 17]. Кількість дерев подій (сценаріїв) відповідає кількості вихідних подій, а дерева відмов відповідають функціям систем захисту. Детальний опис цієї методології можна знайти в роботах з аналізу безпеки АЕС та в навчальних посібниках [7, 9, 17]. Така модель вперше розроблена дослідниками із США [18], там же розроблене спеціальне програмне забезпечення – комп'ютерний код «SAPHIR», який реалізує методологію на рівні числових результатів.

7. Математична постановка задачі моделювання управління ризиком

Формалізація задачі управління ризиком та математична модель можуть бути описані у такий спосіб. Функція ризику представляється як $R = \left\langle \vec{\theta}, \vec{P}, \vec{M} \right\rangle$, де $\vec{\theta}$ – вектор параметрів, які визначають сценарій розвитку аварії, $\vec{P} = \left[P_{тер}, P_{инд}, P_{соц} \right]^T$ – вектор вірогідності негативної події, $\vec{M} = \left[C_{раз}, N_{пор} \right]^T$ – вектор параметрів, що характеризують збиток та число вражених людей при негативній події (НП). Нехай небезпечна система складається з i підсистем, тоді для будь-якої i-ї підсистеми визначається ризик НП: $R_{ki} = \left\langle \vec{\theta}_k, \vec{P}_{ki}, \vec{M}_{ki} \right\rangle$. Передбачається, що відомі:

– детерміновані моделі фізичних процесів, які можуть виникати в i-й підсистемі при ВП: $f_{ij} : \vec{S}_{ij} \to \vec{\Phi}_{ij}$, $j = 1...J$ (набір елементарних подій), де $\vec{S}_{ij}$ – вектор параметрів, який визначає початковий стан i-ї підсистеми, $\vec{\Phi}_{ij}$ – вектор фазових змінних елементарних фізичних процесів, що можуть виникати в i-й підсистемі при ВП;

– статистична модель для оцінки вірогідності виникнення елементарних подій: $\text{Pr}_{ij} : \left(\vec{S}, \vec{\Phi} \right)_{ij} \to \vec{P}_{ij}$, $j = 1...J$, де $\vec{P}_{ij} = \left[P_{ij}^{разр}, P_{ij}^{пор} \right]$ – вектор вірогідності руйнацій та вражень людей.

Розглядається комплексна модель надзвичайної ситуації в небезпечній системі ОПН для аналізу та передбачення наслідків техногенних аварій, що включає:

– модель, засновану на баєсовському підході до оцінки вірогідності виникнення негативних подій в i-й підсистемі у формі «дерева відмов» – $\pi_k : \left(\left\{ \vec{P}_{ij} \right\}, \vec{\theta}_k \right) \to \vec{P}_{ki}$;

– імітаційну модель (дискретно-подієву структурно-логічну) розвитку аварії в формі «дерева подій» – $\mu_k : \left\{ \left(S, \Phi, \vec{P}_k \right)_i, \vec{\theta}_k \right\} \to \vec{M}_{ki}$, де $S_i = \left\{ \vec{S}_{ij} \right\}$, $\Phi_i = \left\{ \vec{\Phi}_{ij} \right\}$, $\vec{M}_k = \sum_i \vec{M}_{ki}$.

Тоді необхідно знайти набір сценаріїв з виконанням умови $\vec{M}_k > \vec{M}_p$, для яких розробляються рішення щодо зниження ризику – доведення до умови $\vec{M}_k < \vec{M}_p$, де $\vec{M}_p$ – вектор значень прийнятних наслідків. Функція рішень може бути представленою: $De = \left\langle \vec{S}_{kj}, \vec{P}^*_{kji}, \vec{E}_{kji} \right\rangle$, де $\vec{S}_{kj}$ – набір рішень щодо зниження техногенного ризику для k-го виробництва j-го об'єкта, $\vec{P}^*_{kij}$ – вектор вірогідності реалізації негативних наслідків при умові виконання прийнятих рішень, $\vec{E}_{kij}$ – вектор витрат, необхідних для реалізації рішень $\vec{S}_{kj}$.

8. Опис основних результатів моделювання

При численному рішенні систем описаних рівнянь отримуємо скінченні множини ймовірного збігу подій – мінімальних перерізів, якій призводять до відмови системи. Цей важливий етап кількісного аналізу систем полягає у представленні умов невиконання функцій системи (її відмови) у вигляді логічного добутку базисних подій, які входять у модель. Набір мінімальних перерізів системи однозначно визначений її деревом відмов. Алгоритм вибору мінімальних перерізів складає найбільш важливу задачу розрахункового коду [9]. Кількість мінімальних перерізів залежить від кількості елементів системи та логіки дерева відмов – це всі сполучення подій, за яких можливе виникнення аварії. Вони можуть досягати для великих систем тисяч і навіть мільйонів комбінацій. За ймовірність відмови системи приймається мінімальна апроксимація верхньої границі мінімальних перерізів, яка визначається за формулою

$$\overset{m}{\underset{i=1}{S}} = 1 - \Pi\left(1 - C_i\right), \tag{4}$$

де S – мінімальна верхня межа мінімальних перерізів для неготовності системи;

C_i – імовірність i-го мінімального перерізу;

m – число мінімальних перерізів.

Другим надзвичайно важливим результатом імовірнісного моделювання є таблиця значимості впливу первинних (базисних) подій на імовірність виникнення відмови системи (небажаної події). Справді, якщо відомо, які події найбільше впливають на ризик, то задача управління зводиться до того, щоб зменшити вплив цих подій будь-яким чином.

За різними сценаріями виникнення й розвитку аварій за допомогою ДП моделюються можливі кінцеві стани KS_i. Звичайно їх буває декілька n-типів, з них деякі (l) повторюються в різних m-варіантах реалізації. Ймовірність кінцевого стану залежить від імовірностей відмов систем захисту та визначається за простою формулою

$$\left(P_{ks}\right)_j = P_{вп} \times \prod_l P_l, \tag{5}$$

де $j \in [1, n]$, $P_{вп}$ – імовірність вихідної події, P_l – імовірність відмови чи спрацювання системи l,

$$P_l = P \bigcup \left(1 - P\right),$$

де P – імовірність відмови системи.

Оскільки відмова системи (P) залежить від надійності її елементів (параметрів $X_3 - X_5$ у формулі (2), то відповідно й імовірність кінцевого стану залежить від тих же параметрів підприємства. Тобто приходимо до висновку, що за результатами ймовірнісного моделювання можливо визначити залежність кінцевого стану системи за сценарієм можливої аварії від параметрів X_i реального стану підприємства. Також, як і при моделюванні відмов систем безпеки за допомогою ДВ, для кінцевих станів генерується множина мінімальних перерізів. За ймовірність кінцевого стану приймається мінімальна апроксимація верхньої границі мінімальних перерізів, яка визначається за формулою (3). Також можливо визначити вплив – важливість відмов кожного елемента систем безпеки на значення ймовірності кінцевого стану. Звідси витікають важливі висновки: 1) можливе планування заходів запобігання небажаних кінцевих станів на основі визначених залежностей, 2) під час моніторингу стану об’єкта небезпеки найбільшу увагу, з точки зору визначення реального стану безпеки, потрібно приділяти тим елементам систем, які мають найбільшу значимість відносно небажаного кінцевого стану за кількісними оцінками ймовірнісного мо-

делювання. Таким чином, доведено, що за допомогою ІАБ можливе визначення ризику від параметрів поточного стану об'єкта.

9. Оцінка ефективності управління безпекою

Інтеграція України в європейські структури неминуче призведе до зміни стратегії управління безпекою. Там прийнято стратегію упередження надзвичайних ситуацій (НС), а це знижує рівень небезпек, що значно дешевше для держави в цілому (7 – 30 разів). Природно, що науковці зобов'язані прискорювати цей процес. Ми маємо впроваджувати ринкові принципи й методи управління безпекою та відмовлятися від методів тоталітарного минулого – тотального контролю діяльності об'єктів підвищеної небезпеки (ОПН) майже сотнею державних структур. Це нонсенс, але факт, який ми отримали у спадщину від народної (соціалістичної) економіки, і більш ніж за 20 років панування начебто ринкових принципів господарювання так і не змогли, крім ядерної галузі, змінити свій світогляд щодо методів управління безпекою. Передові принципи ризик-орієнтованого підходу та культури безпеки успішно впроваджуються поки ще тільки в ядерній галузі. В інших сферах безпеки: охороні праці, техногенній безпеці, пожежній безпеці залишаються старі концепції управління. Авторами вироблені оцінки ефективності управління безпекою у різних сферах безпеки. Низьку ефективність управління безпекою в усіх сферах безпеки в порівнянні з безпекою АЕС ілюструють рис. 2–5 у виді трендів основних показників з безпеки. За критерії ефективності прийняті події, які вважаються головними показниками кожної сфери безпеки. За показники обрані інтегральні показники небезпек: ризик смертності на виробництві – сфера охорони праці (за матеріалами підручника з охорони праці, рис. 2); кількість надзвичайних ситуацій – сфера цивільного захисту (за матеріалами національної доповіді МНС, рис. 3); пожежна безпека – кількість пожеж та збитки від пожеж (за матеріалами статистики пожежного нагляду, рис. 4); кількість порушень нормальної експлуатації на АЕС (за матеріалами щорічних звітів з безпеки, рис. 5).

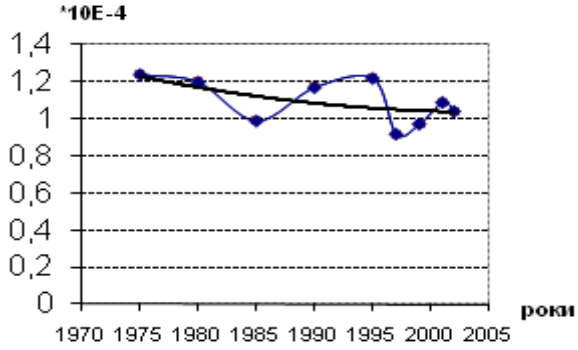

Рис. 2. Ризик смертності на виробництві

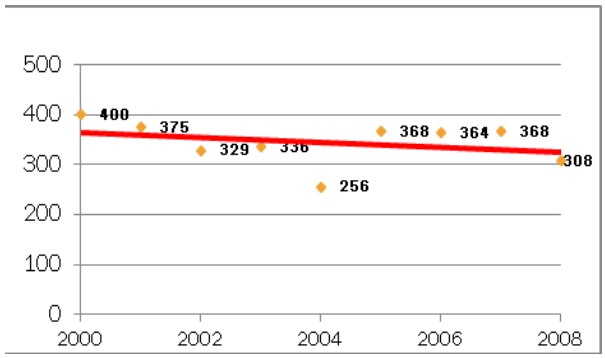

Рис. 3. Кількість надзвичайних ситуацій

Як бачимо з рис. 2, випадкова величина, а саме ймовірність летального випадку на виробництві, фактично не змінилася протягом 30 років, незважаючи на зміни декількох поколінь співробітників, обладнання та, навіть, державного устрою й форми власності. Тренд цієї випадкової величини лежить у дуже вузькому діапазоні [1E-4; 1,2E-4], відповідно математичне очікування $\mu = 1{,}093$, дисперсія вибірки $D = 0{,}014$, відповідно середнє квадратичне відхилення $\sigma = 0{,}1198$, коефіцієнт варіації $\beta = 0{,}1$, тобто маємо порівняльну стабільну величину.

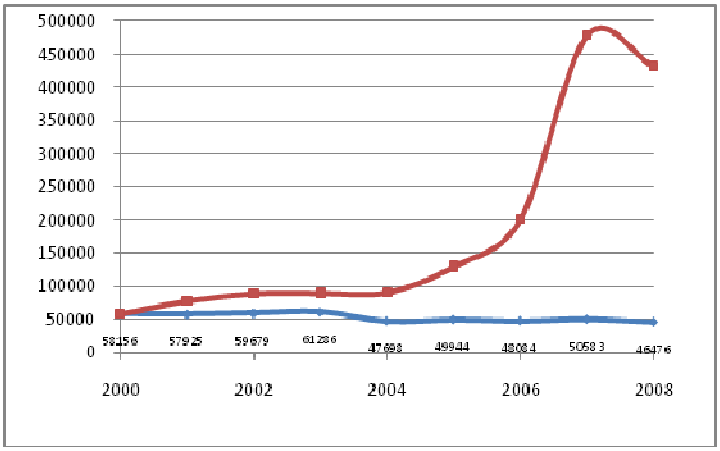

Рис. 4. Кількість пожеж та збитки від них

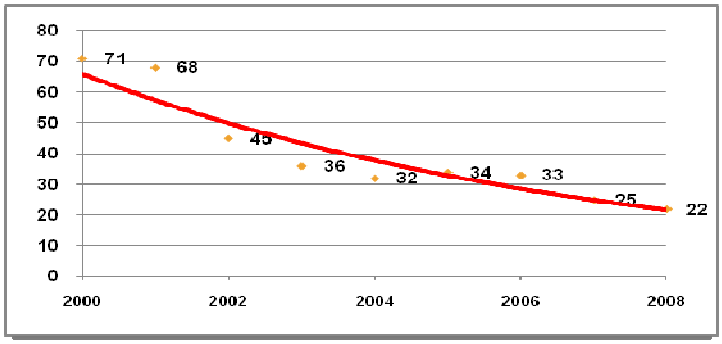

Рис. 5. Кількість порушень на АЕС України

Аналогічна поведінка й двох наступних випадкових величин: кількість надзвичайних ситуацій (рис. 3) та кількість пожеж (рис. 4). Стосовно пожеж, крім слабоспадаючого тренду кількості пожеж, маємо зростання майже в десять разів прямих збитків. Ці об'єктивні статистичні дані свідчать про низьку ефективність регулювання безпеки в цих сферах, неправильний вибір стратегії управління (перевага реагування на НС), відсутність системної роботи із запобігання надзвичайних ситуацій, застарілість основних принципів регулювання безпеки, їх невідповідність сучасним світовим нормам та інші недоліки в цих сферах діяльності.

Зовсім протилежну ситуацію можна спостерігати в атомній галузі, де впроваджені сучасні міжнародні принципи регулювання безпеки та діяльність якої проходить під пильним міжнародним контролем. За показник безпеки обрано кількість порушень (навіть не аварій, а порушень-відхилень від нормальних умов експлуатації) за той же період (рис. 5). За період незалежності відбулося скорочення числа порушень на АЕС майже в десять разів (!), а за порівняльний період – в 4 рази. Лінія тренду на цій діаграмі має експоненціальний характер.

10. Висновки

Потрібні корінні зміни технологій управління безпекою, у тому числі й процедур моніторингу безпеки, на основі ризик-орієнтованих підходів і відповідних розрахунків ризику. На основі кількісних розрахунків ризиків повинні визначатися параметри внутрішнього й зовнішнього моніторингу. Можливість невиконання цілей безпеки також є ризик. Але якщо його прийняти й урахувати, то безсумнівні такі вигоди від впровадження системи управління ризиками ОПН (АЕС) на цій науковій базі:

– система виявляє «вузькі місця» у технологічних процесах;

– формує стимули вдосконалювання процесів шляхом мінімізації ризику, оптимізації чисельності персоналу і його зарплати;

– поліпшує фінансові результати підприємства за рахунок зменшення втрат;

– підвищує експлуатаційну стійкість ОПН (АЕС) за рахунок підвищення якості технологічних процесів і контролю ризиків;

– забезпечує умови оптимізації програм модернізації й ремонту устаткування і в кінцевому підсумку забезпечує розвиток складних технічних систем.

Ситуацію з регулювання безпеки у сфері цивільного захисту потрібно змінювати докорінно. Стратегія управління безпекою має відповідати новому державному устрою та приватній формі власності.

СПИСОК ЛІТЕРАТУРИ

1. Комарницький В.М. Правове регулювання відносин щодо надзвичайних ситуацій в Україні: автореф. дис. / В.М. Комарницький. – К., 2002. – С. 19.
2. Закон України “Про основні засади державного нагляду (контролю) у сфері господарської діяльності». – 5.04.2007. – N 877-V.
3. Закон України «Про об'єкти підвищеної небезпеки». – N 2245-III. – 18.01.2001.
4. Інструкція з організації роботи органів державного нагляду у сфері цивільного захисту та техногенної безпеки, затверджено наказом МНС від 12.01.2010. – N 1.
5. Бєгун В.В. Моніторинг безпеки на основі аналізу ймовірнісних структурно-логічних моделей виробництва / В.В. Бєгун // Моделювання та інформаційні технології. – К.: ІПМЕ ім. Г.Є. Пухова, 2009. – Вип. 52. – С. 17 – 26.
6. Ковалевич О.М. К вопросу об определении "степени риска" / О.М. Ковалевич // Вестник Госатомнадзора России. – 2004. – № 1. – С. 73 – 80.
7. Белов П.Г. Теоретические основы менеджмента техногенного риска: автор. дис. / П.Г. Белов. – М., 2007. – С. 33.
8. Методика визначення ризиків та їх прийнятних рівнів для декларування об’єктів підвищеної небезпеки. Нормативне виробничо-практичне видання. Держнаглядохоронпраці. – К.: Основа, 2003. – 191 с.
9. Вероятностный анализ безопасности атомных станций / В.В. Бегун, О.В. Горбунов, И.Н. Каденко [и др.]. – К.: Випол, 2000. – 558 с.
10. Культура безопасности. Серия изданий по безопасности. № 75-INSAG-4. Международная консультативная группа по ядерной безопасности. – Вена: МАГАТЭ, 1991.
11. Шойгу Ю.С. Подпроект «Формирование системы инновационного образования в МГУ имени М. В. Ломоносова в области психологии» [Электронный ресурс] / Ю.С. Шойгу. – Режим доступа: http://www.psy.msu.ru/science/innovation/index.html.
12. Сазыкин Б.В. Управление рисками: концепция повышения эксплуатационной устойчивости и развития / Б.В. Сазыкин, А.Г. Краев. – М.: PROATOM, МИФИ, 2008. – Режим доступа: http://www.proatom.ru/modules.php?name=Stories_Archive&sa=show_month&year=2008&month=11&month_l=Ноября.
13. Амелина М.А. Примерка Международных стандартов ядерного страхования [Электронный ресурс] / М.А. Амелина, Л.А. Саченко. – Режим доступа: http://www.atombroker/ru/docs.
14. Бегун В.В. «Избыточные» силы и средства при ликвидации последствий чрезвычайных ситуаций: актуальная проблема. ІПМЕ НАН України / В.В. Бегун, С.В. Бегун, Ю.Н. Скалецкий // Моделювання та інформаційні технології. – 2009. – Вип. 53. – С. 37 – 48.
15. Управление рисками организаций. Интегрированная модель. Комитет спонсорских организаций Комиссии Тредвея (COSO). – 2004. – Сентябрь. – Режим доступа: http://www.ispl.ru/Analiz_razvitiya_IT_v_korporatsii_na_osnove_COSO_ERM_5.html.
16. ГОСТ Р 51901.1-2002 (МЭК 60300-3-9:1995) Менеджмент риска. Анализ риска технологических систем.
17. Хенли Э.Дж. Надежность технических систем и оценка риска / Э.Дж. Хенли, Х. Кумамото; пер. с англ. В.С. Сыромятникова. – М.: Машиностроение, 1984. – 356 с.
18. US NRC. Reactor Safety Study (WASH-1400) Main Report. – 1975. – 210 с.

Стаття надійшла до редакції 16.10.2013