УДК 621.039.586

В.Ф. Гречанінов, В.В. Бєгун
(Інститут проблем математичних машин і систем НАН України)

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ УПРАВЛІННЯ РИЗИКАМИ

Розглядаються сучасні проблемі регулювання безпеки в Україні. Описано сучасні стратегії управління безпекою на основі імітаційного імовірнісного структурно-логічного моделювання.

Ключові слова: безпека, ризик, аварія, потенційно небезпечний об'єкт, моніторинг безпеки, культура безпеки.

Вступ

Контроль техногенної безпеки – одна із основних функцій держави. Існують спеціально уповноважені центральні органи влади (ЦОВ), яким делегуються функції перевірок. Звісно, фінансування перевірок ЦОВ відбувається за бюджетні кошти, воно залежить від чисельності контролюючих інспекцій та алгоритмів контролю (моніторингу). Алгоритми моніторингу, своєю чергою, відповідають загальним принципам забезпечення безпеки – концепції або філософії безпеки.

Аналізуючи фактичний стан процесів контролю та регулювання техногенної безпеки в Україні, можна побачити відображення лише застарілих принципів, включаючи принцип планової економіки соціалістичної форми власності – "забезпечення 100% безпеки" (навіть у чинному законодавстві [1]. Більш передова філософія безпеки в Україні працює зараз тільки в ядерній галузі. Нові принципи: ризик-орієнтованого підходу, культури безпеки, операційного ризику впроваджуються насилу, що обертається втратами як для підприємства, так і для держави. На нашу думку, впровадження передових стратегій забезпечення безпеки гальмується перш за все складними методами контролю безпеки, закладеними у нових концепціях, адже потрібно визначати поточне кількісне (числове) значення ризику, до чого держава й суспільство не готові ні з наукової, ні з освітньої 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, як і задача визначення ризику ОПН за процедурами моніторингу ОПН. На сьогодні в Україні цю задачу розв'язують експертними методами на якісному рівні. Підготовка спеціалістів з безпеки, за рідкісними винятками, теж базується на досягненнях 70-х років минулого сторіччя, що суттєво гальмує впровадження й розвиток нових принципів регулювання безпеки оскільки бракує фахівців з відповідним рівнем освіти, тобто процес освіти та підготовки потребує радикального реформування. Всі ці три задачі пов'язані між собою, взаємозалежні і є предметом нашої роботи.

Процес регулювання безпеки містить багато складових з яких можна виділити такі важливі, 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 має відбуватися шляхом оцінки ступеня ризику від здійснення господарської діяльності. Таким чином,

ступінь ризику з 2008 року законодавчо стає загальною характеристикою рівня безпеки чи техногенної, чи промислової, чи пожежної, чи охорони праці або якості 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 [1], а саме: «ризик – кількісна міра небезпеки, що визначається функцією двох змінних – імовірності небажаної події й розміру збитку від неї». Для 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 множники в формулі (1) – випадкові величини, то й ризик R є випадковою величиною. З цього 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 [3] не передбачено моделювання процесів.

Ризик-орієнтований підхід як сучасна інформаційна технологія безпеки

На перших етапах розвитку безпеки основною стратегією забезпечення безпеки персоналу, населення та довкілля був контроль виробництва. З часом, у зв'язку зі складнощами виробничих процесів ці методи стали неефективними. З розвитком обчислювальної техніки й нових методів аналізу з'явилася нова стратегія – запобігання нещасним випадкам і аваріям. Уникнення ризиків (усунення загроз) стало можливим на основі глибокого системного попереднього аналізу виробництва і наступного моделювання. Ця філософія забезпечення 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 [4-6]. Принципи РОП не спростовують знань правил і інструкцій з безпеки, які панували на першому етапі.

Законом про об'єкти підвищеної небезпеки [1] передбачена кількісна оцінка ризиків відповідно до процедури декларування безпеки. Методикою визначення ризику [7] 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 [8]. Спираючись на знання, засновані на дослідженні ймовірнісної моделі виробництва, можна 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 [6, 8], що:

- з множини можливих небезпечних подій виділяються найбільш імовірні їх поєднання, небезпечні 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 дають змогу запобігати нещасним випадкам і надзвичайним ситуаціям, а в підсумку істотно, у десятки разів, знизити витрати на безпеку та рівні ризику.

Методи визначення ризику техногенної небезпеки

Цій проблемі присвячена велика кількість наукових праць [4-6,9-11], існують навіть міжнародні стандарти, де описані методи визначення ризику [12]. Сучасне українське законодавство [1, 2, 7], яке теж базується на ризик-орієнтованому підході, потребує 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 управління безпекою: 1) декларування безпеки й отримання ліцензії на 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 можна здійснити перегляд сценаріїв та визначити кількісні критерії. Кількісні розрахунки дають змогу 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. Ризик у кожному конкретному випадку залежить від параметрів безпеки підприємства: множини можливих вихідних подій, систем захисту та обладнання, ступеня підготовки персоналу тощо. З цього слідує, що й сили та засоби реагування залежать від цих параметрів. Тому завдання визначення ризику важливе не тільки для уникнення небезпеки, а й для регулювання розташування сил реагування. Отже, з математичної точки зору, це можна описати в такому вигляді: ризик R є функцією, як мінімум, таких 6 змінних:

$$R = F\left(x1,\ x2,\ x3,\ x4,\ x5,\ x6\right), \tag{2}$$

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 [8, 13]. 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 [8, 9, 13]. Така модель вперше розроблена дослідниками із США [14], там же розроблене спеціальне програмне забезпечення – комп'ютерний код «SAPHIR», який реалізує методологію на рівні числових результатів.

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 під час негативної 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: $\mathrm{Pr}_{ij}:\left(\vec{S},\vec{\Phi}\right)_{ij}\to\vec{P}_{ij}, j=1...J$, де $\vec{P}_{ij}=\left[P_{ij}^{разр},P_{ij}^{пор}\right]$ – вектор вірогідності руйнацій та уражень 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 за умови виконання прийнятих рішень, $\vec{E}_{kij}$ – вектор витрат, необхідних для реалізації рішень $\vec{S}_{kj}$.

Опис основних результатів моделювання

При численному рішенні систем описаних рівнянь отримуємо скінченні множини ймовірного збігу подій – мінімальних перерізів, які й 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 є найважливішою задачею розрахункового коду [8]. Кількість мінімальних перерізів залежить від кількості елементів системи та логіки дерева відмов – це всі збіги 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

$$\underset{i=1}{\overset{m}{S}}=1-П\left(1-C_i\right), \tag{3}$$

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 *m*

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

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

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 існування 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 що 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. 1–4 у вигляді 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. 1); кількість надзвичайних ситуацій – сфера цивільного захисту (за матеріалами національної доповіді МНС, рис. 2); пожежна безпека – кількість пожеж та збитки від пожеж (за матеріалами статистики пожежного нагляду, рис. 3); кількість порушень нормальної експлуатації на АЕС (за матеріалами щорічних звітів з безпеки, рис. 4).

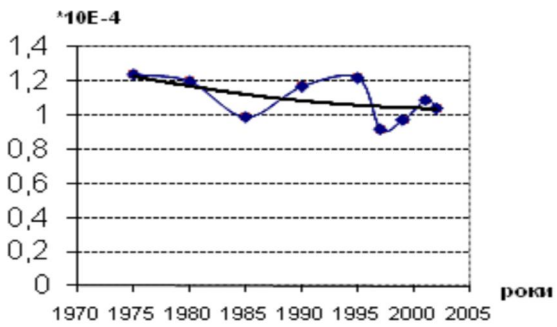

Рис. 1. *Ризик смертності на виробництві*

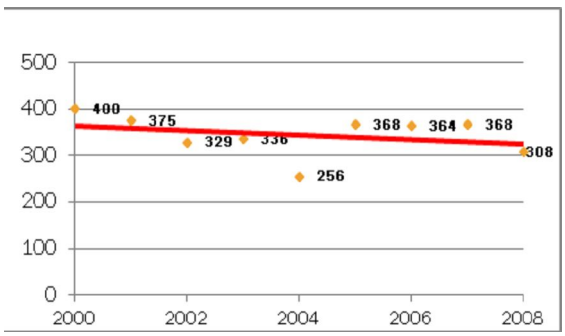

Рис. 2. *Кількість надзвичайних ситуацій*

Як бачимо з рис. 1, 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.

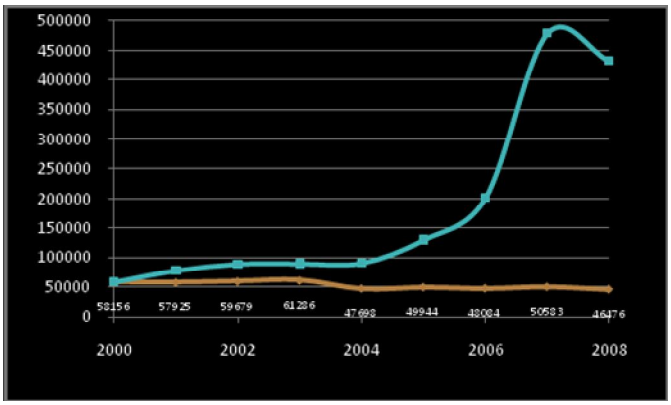

Рис. 3. *Кількість пожеж та збитки від них*

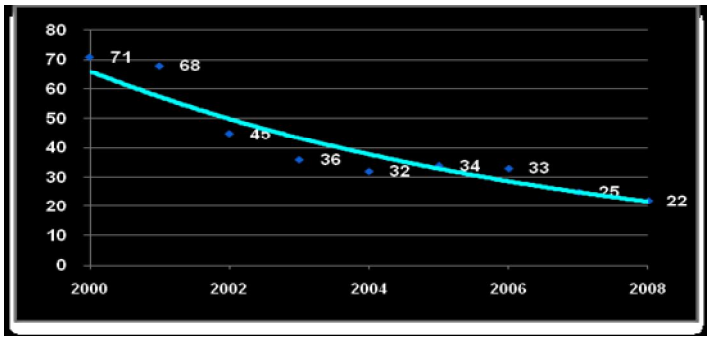

Рис. 4. *Кількість порушень на АЕС України*

Аналогічна поведінка й двох наступних випадкових величин: кількість надзвичайних ситуацій (рис. 2) та кількість пожеж (рис. 3). 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 надзвичайним ситуаціям, 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. 4). 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.

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 інформаційних технологій 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 завдяки зменшенню втрат;
- підвищує експлуатаційну стійкість ОПН (АЕС) шляхом 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 і технологія управління безпекою мають відповідати новому державному устрою та сучасному комп'ютеризованому суспільству.

Список літератури:

1. Закон України «Про об'єкти підвищеної небезпеки». – N 2245-III. – 18.01.2001.

2. Закон України "Про основні засади державного нагляду (контролю) у сфері господарської діяльності». – 5.04.2007. – N 877-V.

3. Інструкція з організації роботи органів державного нагляду у сфері цивільного захисту та техногенної безпеки, затверджено наказом МНС від 12.01.2010. – N 1.

4. 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.

5. Ковалевич О.М. К вопросу об определении "степени риска" / О.М. Ковалевич // Вестник Госатомнадзора России. – 2004. – № 1. – С 73-80.

6. Белов П.Г. Теоретические основы менеджмента техногенного риска: автор. дис. / П.Г. Белов. – М., 2007. – С. 33.

7. Методика визначення ризиків та їх прийнятних рівнів для декларування об'єктів підвищеної небезпеки. Нормативне виробничо-практичне видання. Держнаглядохоронпраці. – К.: Основа, 2003. – 191 с.

8. Вероятностный анализ безопасности атомных станций / В.В. Бегун, О.В. Горбунов, И.Н. Каденко [и др.]. – К.: Випол, 2000. – 558 с.

9. Амелина М.А. Примерка Международных стандартов ядерного страхования [Электронный ресурс] / М.А. Амелина, Л.А. Саченко. – Режим доступа: http://www.atombroker/ru/docs.

10. 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.

11. 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*

12. ГОСТ Р 51901.1-2002 (МЭК 60300-3-9:1995) Менеджмент риска. Анализ риска технологических систем.

13. 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.

14. US NRC. Reactor Safety Study (WASH-1400) Main Report. – 1975. – 210 С.

В.Ф. Гречанинов, В.В. Бегун

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ УПРАВЛЕНИЯ РИСКАМИ

Рассматриваются современные проблемы регулирования безопасности в Украине. Описаны современные стратегии управления безопасностью на основе имитационного вероятностного структурно-логического моделирования.

Ключевые слова: безопасность, риск, авария, потенциально опасный объект, мониторинг безопасности, культура безопасности.

V. Hrechaninov, V. Begun

INFORMATION TECHNOLOGY RISK MANAGEMENT

The article deals with the problem of modern safety regulation in Ukraine. 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.

❖ ❖ ❖