doi: 10.15407/visn2015.08.024

МОРОЗОВ
Анатолій Олексійович –
академік НАН України,
директор Інституту проблем математичних машин та систем НАН України

УДК 504.05

НАУКОВІ ОСНОВИ ВПРОВАДЖЕННЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В УПРАВЛІННІ ТЕХНОГЕННО-ЕКОЛОГІЧНОЮ БЕЗПЕКОЮ

За матеріалами наукової доповіді на засіданні Президії НАН України 17 червня 2015 року

Розглянуто актуальні питання управління безпекою на основі ризик-орієнтованого підходу, проаналізовано сучасний стан, визначено методи та алгоритми вирішення проблем. Запропоновано шляхи реформування системи управління безпекою в цілому, а також уперше запропоновано рішення на основі створення інформаційної технології безпеки. Обговорено основні процеси, функції, математичні моделі та структуру інформаційної технології безпеки.

***Ключові слова*:** безпека, ризик, модель, інформаційна технологія, алгоритм.

На сьогодні рівень ризику виникнення небезпечних ситуацій у всіх регіонах України залишається досить високим [1]. Причин для цього багато, але головною з них є застарілі методи управління безпекою, засновані винятково на інспекційних заходах. Негативний досвід великих техногенних аварій, що сталися за останні роки (наприклад, 2007 р. — катастрофа потяга з жовтим фосфором біля Ожидова; 2014 р. — залізнична аварія під Черкасами, внаслідок якої спалахнули цистерни з мазутом і ледь вдалося уникнути вибуху скрапленого газу; 2015 р. — масштабна пожежа на території нафтобази під Глевахою (рис. 1)), свідчить про об'єктивну необхідність удосконалення системи управління безпекою в Україні. Ситуація із забезпеченням безпеки викликає занепокоєння навіть у наших європейських партнерів, з 2008 р. в Україні працює місія ЄС за проектом Європейської комісії із запобігання, готовності та реагування на природні та техногенні катастрофи — PPRD. Щороку держава витрачає мільярди гривень на ліквідацію наслідків аварій, і незважаючи на те, що значні кошти витрачаються на державне інспектування, ці заходи є малоефективними.

Фахівці Інституту проблем математичних машин та систем (ІПММС) НАН України вперше в державі провели комплексні наукові дослідження з розроблення методології та реалізації сучасної системи управління техногенно-екологічною безпекою і отримали важливі результати [1—4]. Звісно, зовсім позбутися виникнення надзвичайних ситуацій неможливо (рис. 2), але правильний вибір стратегій управління безпекою дає можливість зменшити їх частоту та наслідки і в десятки разів знизити державні витрати на безпеку.

На жаль, кількість надзвичайних ситуацій в Україні не зменшується, а бюджетні витрати на подолання наслідків аварій постійно зростають (рис. 3). І хоча кількість загиблих і постраждалих залишається майже незмінною, ці величини на порядок перевищують відповідні показники для розвинених країн.

Отже, техногенний і промисловий стан України потребує переходу до регулювання безпеки на основі сучасної парадигми ризик-орієнтованого підходу, як це прийнято у більшості країн світу. Його основні принципи такі:

• рівень безпеки кожного громадянина, виробництва чи суспільства загалом має визначатися рівнем ризику;

• безпека — це прийнятний рівень ризику;

• ризик у кожному окремому випадку має враховувати всі джерела, фактори і обставини, що сприяють появі та розвитку небезпеки;

• ризик є добутком імовірностей небажаної події та її наслідків;

• усі заходи щодо запобігання небезпеці мають визначатися за допомогою розрахунків, узгоджених з досвідом фахівців.

Безпека є головною потребою кожної людини і основним чинником життєдіяльності суспільства. Належний стан безпеки в державі має підтримуватися відповідними законодавчими актами, обов'язковими для виконання. Проте в Україні це не так. Існують суттєві суперечності між вимогами законодавства і реальними процедурами регулювання безпеки.

Наприклад, відповідно до Закону України [5], здійснення державного нагляду має відбуватися через оцінювання *ступеня ризику*

Рис. 1. Пожежа на нафтобазі під Глевахою. 9—18 червня 2015 р.

Рис. 2. Пожежа на нафтосховищі у передмісті Лондона. 11—12 грудня 2005 р.

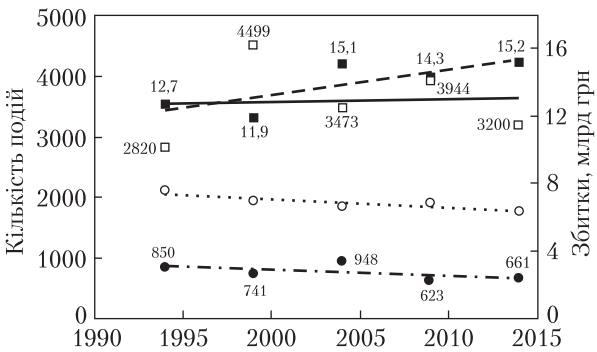

Рис. 3. Тренди безпеки: ○ — кількість надзвичайних ситуацій; ● — число загиблих; □ — кількість травмованих; ■ — матеріальні збитки

від здійснення господарської діяльності, тобто з 2008 р. ступінь ризику законодавчо стає загальною характеристикою рівня безпеки в усіх сферах безпеки: техногенної, промислової, пожежної, безпеки праці, а також якості продукції, яку випускають підприємства. Це демонструє бажання держави увійти в Європейське Співтовариство, зокрема в його нормативно-правову базу. Причому визначення ключового поняття «ризик» у цьому законі наведено у його європейському розумінні, на відміну від раніше прийнятого законодавства, у тому числі й закону про об'єкти підвищеної небезпеки, а саме: «*ризик — кількісна міра небезпеки, що визначається функцією двох змінних — імовірності небажаної події та розміру збитку від неї*». Для розрахунків приймають:

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

де R — ризик; P — імовірність аварії (небажаної події); U — розмір її наслідків (збитки). Оскільки змінні P та U — це складні випадкові функції багатьох змінних, то і R є випадковою величиною. Отже, завдання контролю (моніторингу) безпеки має бути представлене як *алгоритм перевірки випадкової величини*, яка є багатовимірною функцією дійсних змінних. На жаль, чинні сьогодні в Україні алгоритми контролю безпеки (ризику) ґрунтуються на застарілих нормах і прописані в підзаконних актах та наказах центральних органів влади, за якими рівень безпеки об'єкта при експертному оцінюванні стану обладнання, систем захисту чи виконання відомчих правил визначається людиною (інспектором). Це аж ніяк не відповідає новому законодавству, оскільки таке оцінювання здійснюється без урахування реальних кількісних оцінок безпеки.

Така ситуація гостро ставить проблему необхідності створення законодавчих актів, розроблення алгоритмів контролю (моніторингу) безпеки на основі кількісних методів. Тому фахівці Інституту ініціювали розроблення проектів розпоряджень Кабінету Міністрів України зі схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного і природного характеру [6] та про затвердження Плану заходів щодо реалізації цієї Концепції [7].

Актуальним завданням є також створення сучасного інформаційного забезпечення сфери безпеки. Можливості новітніх інформаційних технологій та відповідних процесів прийняття рішень на їх основі не впроваджено в нашій державі в жодній зі сфер безпеки, крім ядерної галузі, де це було зроблено завдяки виконанню міжнародних вимог.

Завдання державного регулювання безпеки тісно пов'язані з основними парадигмами (концепціями), етапами та принципами (стратегіями) забезпечення безпеки, які з розвитком технологій постійно змінюються. Аналізуючи історію розвитку безпеки у світі, можна виокремити чотири етапи, кожному з яких відповідає своя певна філософія, або парадигма безпеки і державного регулювання:

- забезпечення 100 %-ї безпеки;
- ризик-орієнтований підхід;
- культура безпеки — сучасна філософія безпеки АЕС;
- рентабельна безпека — філософія ринкових відносин.

Для кожної *парадигми* безпеки розробляють свої особливі *стратегії* забезпечення безпеки та відповідні *методи* і *алгоритми* регулювання й контролю. Крім того, відповідно до цілей організацій ідентифікують три стадії розвитку безпеки:

1. Безпеку засновано виняткова на дотриманні вимог правил і інструкцій.

2. Організація стає зацікавленою у створенні високого рівня безпеки.

3. Організація шукає можливості підвищення рівня безпеки.

Основними ознаками цих стадій є ставлення керівництва небезпечного об'єкта до питань безпеки, взаємодія з контролюючими органами та відносини між старшим персоналом і виконавцями. Розвиток відбувався поступово, від початкової стадії 1, де відносини суб'єктів безпеки були майже ворожими, до стадій 2 і 3, де питання безпеки стають головною і спільною справою. Парадигма безпеки залежно від стадії розвитку породжувала стратегії управління та стратегії контролю, які у свою чергу реалізовувалися в методах управління і контролю. Слід

зазначити, що філософії безпеки і стадії розвитку — це динамічні залежні ознаки, в кожному окремому випадку їх стан потребує уточнень.

Першій парадигмі в основному відповідала перша стадія розвитку безпеки. Від вибору парадигми залежать усі наступні інформаційні процеси і, відповідно, інформаційні потоки управління та контролю безпеки і, як результат, — загальний стан безпеки. Так, академік В.О. Лєгасов головною причиною аварії на ЧАЕС назвав саме неправильну тодішню філософію безпеки: *«Дело именно в философии безопасности. Если бы философия безопасности была бы правильной, то технические решения под эту вот философию конечно бы наши специалисты находили, потому что они грамотные специалисты, толковые люди, умеют считать и делать прочие вещи»*.

Філософія забезпечення 100%-ї безпеки зародилася з початком промислового розвитку. Це безліч правил безпеки, яких мають додержуватися конструктори машин і беззастережно виконувати оператори. Метод запровадження правил-заборон з безпеки, особливо після того, як стався нещасний випадок або аварія, зумовив появу у вітчизняному законодавстві величезної кількості інструкцій, регламентів, зведень правил і т.ін. Підприємці вважали контроль безпеки з боку урядових (зовнішніх) структур тягарем, який лише заважає виробничій діяльності, оскільки дотримання усіх правил, вимог та інструкцій потребує певних затрат і не завжди є обґрунтованим (рис. 4).

В Україні станом на 2014 р. існувало понад 100 різних документів, які регламентували обов'язкові до виконання вимоги тільки однієї Державної інспекції техногенної безпеки. Очевидно, що виконати всі вимоги неможливо. Крім того, така ситуація створює передумови для корупції. Цю філософію було визнано світовим співтовариством неправильною, такою, що суперечить основним принципам ринкових відносин і провокує втручання у внутрішні бізнес-процеси. Тому розвинені країни відмовилися від неї ще у середині 1970-х років, однак в Україні більшість принципів контролю залишилися без змін.

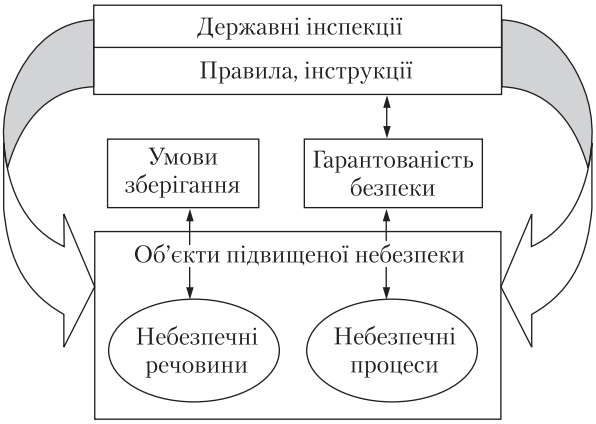

Рис. 4. Модель парадигми забезпечення 100%-ї безпеки

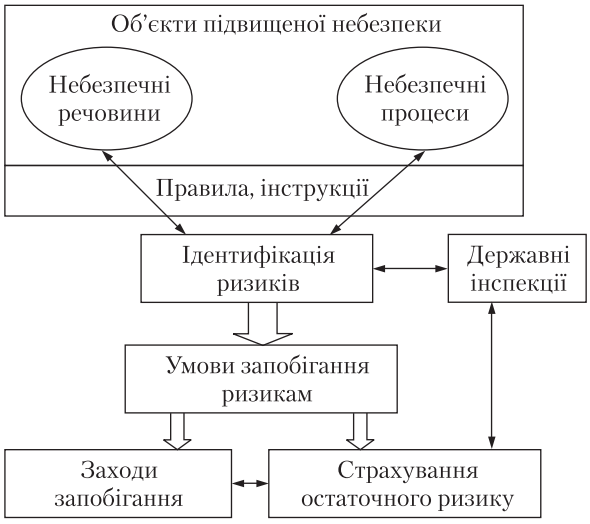

Рис. 5. Модель парадигми ризик-орієнтованого підходу

З розвитком обчислювальної техніки і нових методів аналізу з'явилася нова філософія — парадигма *запобігання* нещасним випадкам і аваріям. Це стало можливим завдяки глибокому системному (попередньому) аналізу виробництва з метою визначення для нього ризиків (загроз) і способів запобігання їм. Цю філософію називають ризик-орієнтованим (іноді — ризик-інформованим) підходом (РОП). Зрозуміло, що така філософія насамперед стала розвиватися в потенційно найнебезпечнішій ядерній галузі. Принципи РОП не спростовують знань, правил та інструкцій з безпеки, які

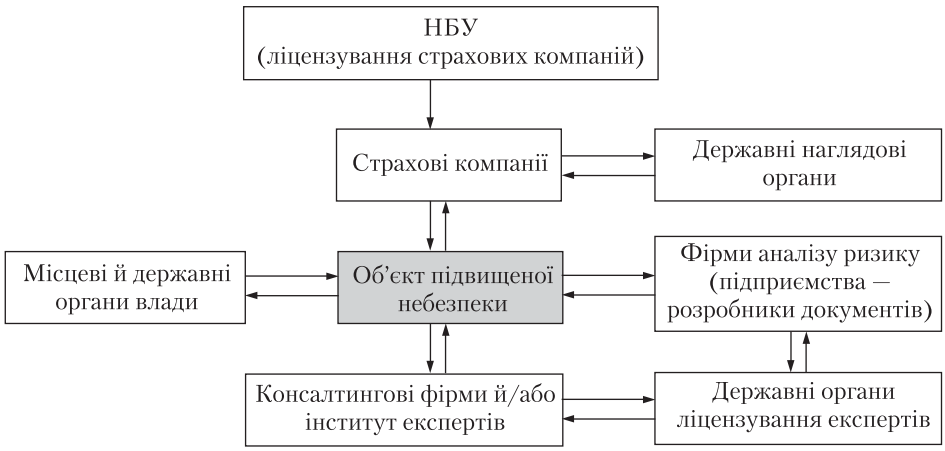

Рис. 6. Структура органів управління безпекою за стратегією РОП

панували на першому етапі, проте істотно змінюють алгоритми контролю (рис. 5).

Державні інспекції не контролюють на об'єктах небезпечні процеси та умови зберігання небезпечних речовин. За це повністю відповідає власник. Однак держава контролює повноту визначення ризиків, їх величини, страхування надлишкового ризику, заходи щодо запобігання аваріям. Доведено, що події, які передують аварії, навченість персоналу з їх припинення, технічний стан обладнання та систем безпеки об'єкта, заходи з ліквідації аварії тісно пов'язані між собою і стають одним єдиним ланцюгом. Саме цей ланцюг подій і моделюють за допомогою ймовірнісної моделі — сценарію розвитку аварії за ризик-орієнтованого підходу в управлінні безпекою.

Типи аварій або надзвичайних ситуацій відповідно до масштабів впливу класифікують за 4 рівнями: об'єктовий, місцевий, регіональний, державний.

Законодавчо у нашій країні не встановлено числові значення прийнятого ризику. Світові товариства ВООЗ і МООП рекомендують такі рівні: незначний ризик — $R \le 1 \cdot 10^{-6}$; припустимий ризик — $1 \cdot 10^{-6} \le R \le 5 \cdot 10^{-5}$; високий (терпимий) ризик — $5 \cdot 10^{-5} \le R \le 5 \cdot 10^{-4}$; неприпустимий ризик — $R \ge 5 \cdot 10^{-4}$. Отже, сьогодні необхідне розроблення всіх атрибутів нової концепції: методик визначення рівнів ризиків на основі сучасних наукових досягнень, відповідних моделей, алгоритмів і програмного забезпечення.

Прийняття такої філософії безпеки потребує реформування державних наглядових органів, широкого впровадження інформаційних процесів, змінення навчальних програм тощо. Процеси реформування наглядових органів мають відбуватися одночасно з процесами впровадження нової концепції. Тільки завдяки фаховому моделюванню на основі наукових підходів можна визначити реальні ризики небезпеки того чи іншого об'єкта, що дасть змогу завчасно приймати рішення і здійснювати заходи щодо зменшення цих ризиків.

За результатами моделювання розробляють алгоритм управління ризиком, який включає виконання шести процедур, а також постійний моніторинг і контроль. Процедури алгоритму управління ризиком:

1. Планування управління ризиками — процес прийняття рішень щодо застосування методології РОП для конкретного виду діяльності.

2. Ідентифікація ризиків — визначення того, які ризики можуть вплинути на певний вид діяльності.

3. Якісна оцінка ризиків — процес якісного аналізу результатів ідентифікації, а також визначення подій, які роблять найбільший внесок у загальний ризик і потребують вживання заходів щодо його зниження.

4. Кількісна оцінка ризиків — визначення ймовірності виникнення ризиків і впливу їх наслідків на певний вид діяльності; це допомагає приймати оптимальні рішення й уникати невизначеності в процесі управління.

5. Планування реагування на ризики — розроблення методів і технологій зниження негативних наслідків ризиків.

6. Реалізація прийнятого рішення — заключний етап усієї роботи з управління ризиками на основі попереднього планування.

Моніторинг і контроль параметрів безпеки проводять з метою перевірки дотримання вимог встановлених норм. З огляду на комплексні та індивідуальні характеристики ризиків об'єктів, для кожного з них на основі алгоритму управління ризиком потрібно розробити заходи зменшення ризику та визначити оптимальний (максимальний) проміжок часу між інспекціями T_m за умови врахування ризиків від усіх небезпек та неперевищення допустимого ризику:

$$\text{Max}\,(T_m): R_a < [R_d]. \qquad (2)$$

Мінімальну можливу структуру управління ризиком наведено на рис. 6. Така структура відповідає парадигмі, не нижчій за РОП, і стадіям 2 або 3 і в такій самій чи дуже подібній формі існує в усіх розвинених країнах. Як бачимо, присутність держави може бути зведена до мінімуму. Логічно й очевидно, що за належного рівня підготовки об'єкта і наявності внутрішнього моніторингу наслідки аварійних процесів можна істотно зменшити, а в багатьох випадках і запобігти розвитку аварійних ситуацій. Отже, рівень безпеки відображує ступінь усвідомлення, передбачення, безперервної готовності до реагування. Це стосується як стаціонарних техногенних об'єктів підвищеної небезпеки, так і засобів транспортування небезпечних речовин.

Як бачимо, у структурі є тільки два елементи, що перебувають на бюджетному утриманні: органи державного нагляду за дотриманням чинного законодавства та державні органи ліцензування експертів. Ці органи були і в старій структурі, але в новій їхні функції змінилися. Державні та місцеві органи влади контролюють лише ступінь ризику. Оскільки R_a є розрахунковою і випадковою величиною (2), стає зрозумілим, що необхідно впроваджувати інформаційні технології. В ІПММС НАН України було розроблено інформаційну технологію безпеки, структуру якої зображено на рис. 7. Ця інформаційна технологія дозволяє оператору приймати рішення як для вироблення заходів з попередження неприйнятних рівнів ризику, так і після того, як аварія вже сталася.

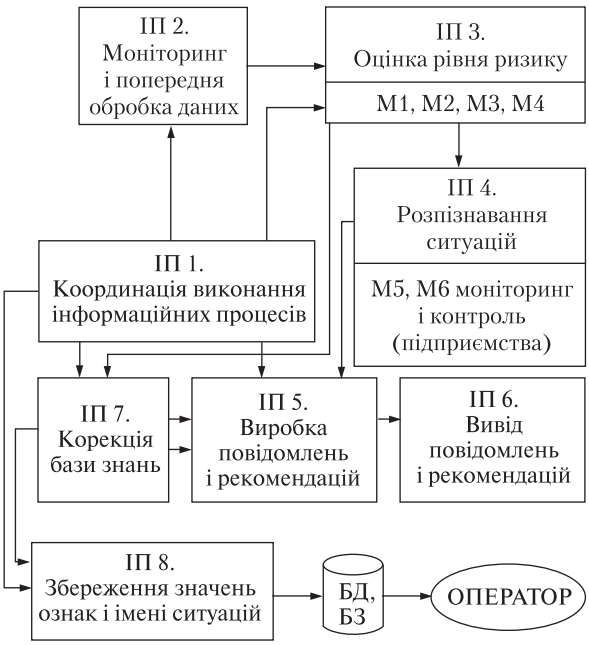

Рис. 7. Структура інформаційної технології безпеки

Основні моделі інформаційних процесів мають бути такі:

- моделі проблемних ситуацій у сфері безпеки;
- модель «еталона» безпеки, у вигляді показників безпеки, значень ризику тощо;
- набір математичних методів і моделей для розрахунків параметрів процесу, які неможливо виміряти або визначити безпосередньо;
- набір методів і моделей для розв'язання задач моніторингу процесу, зокрема для визначення поточного стану безпеки (розпізнавання ситуацій);
- модель пошуку рішень щодо корекції процесів;

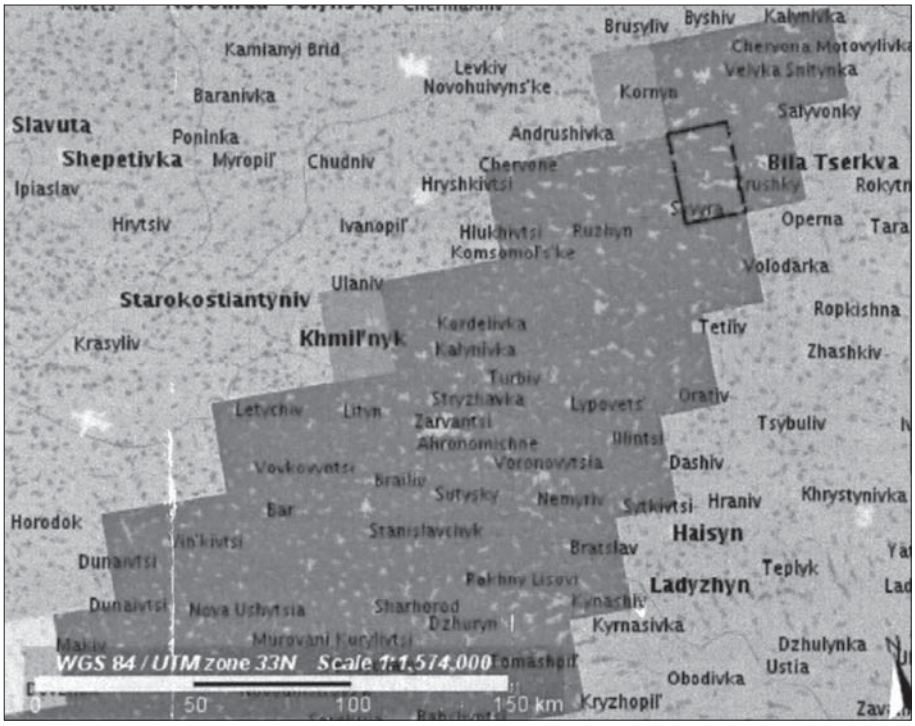

Рис. 8. Моделювання за допомогою системи РОДОС поширення викидів продуктів горіння під час пожежі на території нафтобази у смт Глеваха (станом на 10.06.2015)

• модель перетворення первинних даних у значення ознак небезпечної ситуації;

• модель структури системи підтримки прийняття рішень (СППР).

Звісно, має бути розроблено відповідне програмне забезпечення. Наприклад, в ІПММС НАН України створено моделі та програми, які вже впроваджені в європейську систему прогнозу та підтримки аварійного реагування при радіаційних аваріях (система РОДОС). Ця система працює в центрах аварійного реагування багатьох європейських країн і зараз за підтримки ЄС впроваджується в Україні. Систему адаптовано для зон впливу українських АЕС. На сьогодні її вже встановлено в кризовому центрі Держатомрегулювання, завершується впровадження цієї системи у Гідрометцентрі та НАЕК «Енергоатом».

Як приклад можливо нетрадиційного використання цієї системи ми зробили моделювання поширення продуктів горіння внаслідок пожежі на нафтобазі під Васильковом станом на 10 червня 2015 р. На рис. 8 наведено дані розрахунку концентрацій шкідливих викидів продуктів горіння нафтобази з урахуванням поточного стану атмосферних процесів.

На жаль, в Україні немає систем, які б могли моделювати різні техногенні процеси з оцінкою їх ризику. І досі ще не введено в промислову експлуатацію Національний ситуаційний центр, розроблений нами для РНБО України. У цьому Центрі є база даних потенційно небезпечних об'єктів, і якби він працював, можна було б моделювати й прогнозувати розвиток подій і наслідки аварії на нафтобазі під Васильковом, так, як ми це робили за допомогою системи РОДОС. У розвинених країнах світу керівники держави не виїздять на місця аварій, бо це не дає нічого, крім відволікання ліквідаторів від їхньої роботи. Урядовці зазвичай знаходяться у ситуаційному центрі, де й керують процесом ліквідації аварії. У нас же все не так.

Отже, підсумовуючи все сказане, слід зазначити, що для реалізації в нашій державі нових принципів управління безпекою на основі РОП першочерговими завданнями є розроблення:

• рекомендацій щодо структури центральних органів влади з безпеки;

• моделей інформаційних технологій безпеки для різних небезпек і галузей виробництва;

• галузевих баз даних та баз знань, національної бази даних;

• методик та інструкцій з контролю процесів;

• положень з розслідування надзвичайних ситуацій та призначення корегуючих заходів;

• змін законодавства та нормативних документів з безпеки;

• моделі актуарних розрахунків;

• вітчизняного програмного забезпечення;

• змін освітніх програм з безпеки.

Довгострокові завдання впровадження РОП та підвищення рівня безпеки мають бути такими:

• принциповий перехід на вищі рівні і парадигми безпеки;

• формування змін ідеології суспільства щодо ставлення до безпеки;

• забезпечення контролю інтегральних рівнів безпеки життєдіяльності громадян;

• інтеграція в міжнародні системи моніторингу безпеки.

Отже, наукові основи впровадження ризик-орієнтованого підходу в управлінні техногенно-екологічною безпекою, з огляду на їх значущість як для кожного підприємства, так і для держави в цілому, повинні стати найвищим пріоритетом у суспільстві. Зважаючи на міжгалузевий характер цієї проблеми, необхідність у використанні знань з різних напрямів науки, на нашу думку, доцільно було б сформувати відповідну Раду з ризик-орієнтованого підходу в управлінні безпекою на чолі з НАН України, яка б відповідала за наукову підтримку діяльності у цій сфері.

REFERENCES

1. Grechaninov V.F. *Information technologies for analysis of technology safety and planning of countering actions to emergency situations*. Ph.D. (Tech.) thesis. Kyiv, 2014. [in Ukrainian].
   [Гречанінов В.Ф. *Інформаційні технології аналізу стану техногенної безпеки та планування протидії надзвичайним ситуаціям*: автореф. дис. ... канд. техн. наук. Київ, 2014].
2. Begun V.V., Grechaninov V.F. In: Proc. Int. Conf. *The concept of critical infrastructure protection: state, problems and prospects of its implementation in Ukraine*. [in Ukrainian]. http://www.niss.gov.ua/articles/1527/.
   [Бєгун В.В., Гречанінов В.Ф. Проблеми регулювання техногенної безпеки в Україні. В кн.: *Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні*: зб. матер. Міжнар. наук.-практ. конф. (7—8 лист. 2013 р., Київ). К.: НІСД, 2013. С. 69—81].
3. Grechaninov V.F., Begun V.V. *Matematychni mashyny i systemy (Mathematical Machines and Systems)*. 2014. (1): 159. [in Ukrainian].
   [Гречанінов В.Ф., Бєгун В.В. Функції управління і нагляду в ризик-орієнтованому підході до управління безпекою. *Математичні машини і системи*. 2014. № 1. С. 159—170].
4. *Situational centers. Theory and practice*. (Kyiv: Intertekhnodruk, 2009). [in Ukrainian].
   [Ситуаційні центри. Теорія і практика. К.: Інтертехнодрук, 2009].
5. http://zakon4.rada.gov.ua/laws/show/877-v.
   [Закон України. *Про основні засади державного нагляду (контролю) у сфері господарської діяльності*. 05.04.2007. № 877-V].
6. http://zakon4.rada.gov.ua/laws/show/37-2014-%D1%80.
   [Розпорядження Кабінету Міністрів України. *Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру*. 23.01.2014. № 37-р].
7. http://www.kmu.gov.ua/control/uk/cardnpd?docid=248135163.
   [Розпорядження Кабінету Міністрів України. *Про затвердження Плану заходів щодо реалізації Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру на 2015—2020 роки*. 25.03.2015. № 419-р].

А.А. Морозов

Институт проблем математических машин и систем НАН Украины
пр. Академика Глушкова, 42, Киев, 03680, Украина

НАУЧНЫЕ ОСНОВЫ ВНЕДРЕНИЯ РИСК-ОРИЕНТИРОВАННОГО ПОДХОДА В УПРАВЛЕНИИ ТЕХНОГЕННО-ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТЬЮ

По материалам научного доклада на заседании Президиума НАН Украины 17 июня 2015 года

Рассмотрены актуальные проблемы управления безопасностью на основе риск-ориентированного подхода. Проанализировано нынешнее состояние проблемы, определены методы и алгоритм ее решения. Предлагаются пути реформирования системы управления безопасностью в целом, а также впервые предложено решение проблемы на основе создания информационной технологии безопасности. Рассмотрены основные процессы, функции, математические модели и структура информационной технологии безопасности.

***Ключевые слова*:** безопасность, риск, модель, информационная технология, алгоритм.

A.O. Morozov

Institute of Mathematical Machines and Systems Problems
of National Academy of Sciences of Ukraine
42 Glushkov Ave., Kyiv, 03680, Ukraine

SCIENTIFIC PRINCIPLES OF RISK-ORIENTED APPROACH IMPLEMENTATION TO TECHNOGENIC AND ECOLOGICAL SAFETY MANAGEMENT

According to the materials of scientific report at the meeting of the Presidium of NAS of Ukraine June 17, 2015

Actual problems of safety management on the basis of risk-oriented approach are discussed. The state of the problem is analyzed; the methods and algorithms of solving it are defined. The general reform of the safety management system is proposed. The new solution of this problem on the basis of the information technology of safety creation is proposed; the basic processes, functions, mathematical models and the structure of information technology of safety are considered.

***Keywords*:** safety, risk, model, information technology, algorithm.