УДК 004.9

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

ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ ВИБОРУ ІНДИКАТОРІВ, ЗМІННИХ ТА ПОКАЗНИКІВ МОНІТОРИНГУ БЕЗПЕКИ

[*]Інститут проблем математичних машин і систем НАНУ, м. Київ, Україна
[**]Державна служба України з надзвичайних ситуацій, м. Київ, Україна

Анотація. *Розглянуті проблеми побудови систем моніторингу безпеки в Україні у зв'язку з появою нових урядових рішень щодо стратегій моніторингу на основі ризик-орієнтованого підходу. Обґрунтовується необхідність використання технології ситуаційних центрів та ймовірнісних моделей небезпечних процесів і систем для модулів аналізу та прогнозу.*
Ключові слова: *безпека, ризик-орієнтований підхід, моніторинг, інформаційні технології, моделі безпеки.*

Аннотация. *Рассмотрены проблемы построения системы мониторинга безопасности в Украине в связи с новым правительственным решением по стратегии мониторинга безопасности на основе риск-ориентированного подхода. Обосновывается необходимость использования технологии ситуационных центров и вероятностных моделей опасных процессов и систем для модулей анализа и прогнозирования.*
Ключевые слова: *безопасность, риск-ориентированный подход, мониторинг, информационные технологии, модели безопасности.*

Abstract. *The problems of construction of security monitoring systems in Ukraine taking into account new government decisions about monitoring strategies based on a risk-oriented approach are considered. The necessity of situational centers technology and probabilistic models of hazardous processes and systems for the modules of analysis and forecast usage is substantiated.*
Keywords: *safety, risk-oriented approach, monitoring, information technologies, models of security.*

1. Вступ

Нещодавно Кабінет Міністрів України (Кабмін) затвердив нову стратегію управління безпекою на основі ризик-орієнтованого підходу (РОП) [1] та низку постанов з управління ризиком у різних галузях і сферах безпеки. Крім того, на сайті Державної служби України з надзвичайних ситуацій (ДСНС) для громадського обговорення вже розміщено проект постанови Кабміну щодо затвердження регламенту з моніторингу безпеки на основі РОП [2]. Але, на жаль, в усіх цих документах є системні помилки, які не дозволять працювати методикам, що пропонуються у згаданих документах. Тобто, процеси євроінтеграції у сфері безпеки за такими методами неможливі навіть теоретично, тому дана стаття з теоретичних основ моніторингу актуальна. Наше прагнення у переході на європейські методи управління безпекою повинно матеріалізуватися завдяки розробленим за нашою участю та затвердженим розпорядженнями Кабміну № 37-р від 2014 р. і № 419-р від 2015 р. [3] і вже затвердженій стратегії 18.12.2017 [1]. Здавалося б, що все гаразд, але все залишається по-старому [4].

Перехід на Європейські стандарти та методи в управлінні безпекою, як свідчать прийняті урядові рішення, є нагальною потребою, але з чого почати? У статті [4] виділені наукові задачі загальної проблеми управління безпекою на сучасному рівні:

- перехід на інформаційні технології;
- задача мінімізації ризику;
- моделювання систем;
- моделювання можливих помилок людини;
- визначення прийнятних рівнів ризику по галузях виробництва,

• створення ПЗ з інтерактивними функціями на основі ГІС-технологій;
• інформаційне забезпечення служб з безпеки;
• зміна навчальних програм вищої освіти з безпеки.

Сказати, що це тільки суто наші задачі, було б неправильним, адже у більшості країн світу вони теж не розв'язані, хоча й подекуди існують системи моніторингу безпеки на основі ситуаційних центрів (СЦ) [5]. Проте існують навіть приватні підприємства, які створюють такі системи на замовлення [6]. Але задача не є суто інженерною, кожна з таких систем має свої відмінності. В Україні існують розбіжності навіть серед вчених і замовників СЦ. Це є однією з причин невиконання урядових рішень щодо їх будови.

2. Основна частина

2.1. Існуючі рішення

Розглянемо існуючі рішення, які відповідають кращій світовій практиці, описані в [5, 6] (рис. 1). Ситуаційний центр сьогодні є найважливішою технологічною основою ефективного управління. СЦ може бути представлений як організаційно-технічний комплекс, основу якого складають інформаційне та програмне забезпечення підтримки управлінських рішень на основі комплексного моніторингу факторів впливу на розвиток процесів, що відбуваються. Зауважимо, що ІПММС є автором ідеї та одним із перших користувачів нової технології [7, 8].

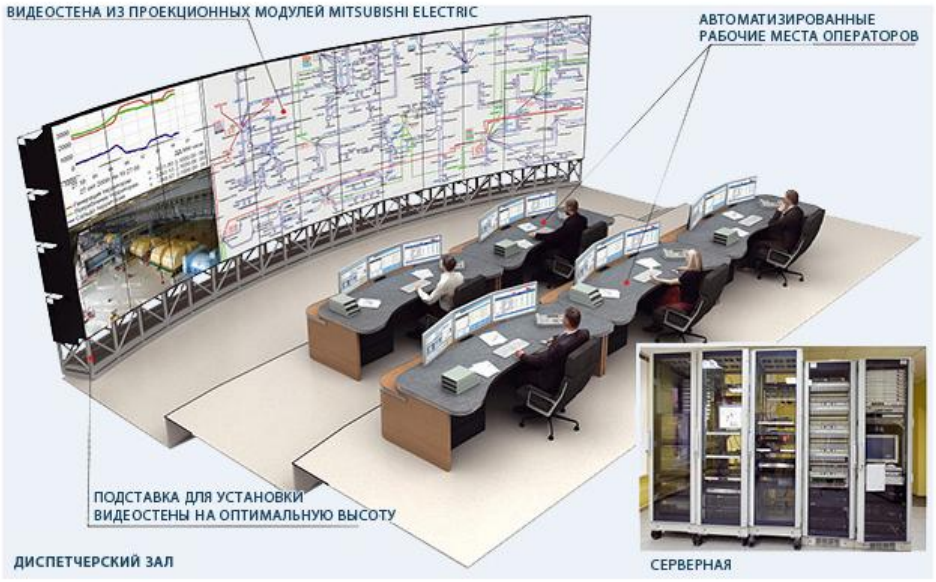

Рис. 1. Можливий вигляд ситуаційного центру

Система моніторингу процесів є першою системою, джерелом інформації СЦ. Процеси безпеки різноманітні, обширні та взаємозв'язані, тому СЦ з безпеки ієрархічні як за територіальними ознаками, так й за типами небезпек. Як йдеться у проекті регламенту про моніторинг [2] та у [9] у деякій мірі підсистеми моніторингу існують і у нашій державі, але не відповідають сучасності з таких причин: дані з небезпек розпорошені по різних відомствах, затверджений регламент моніторингу частіше не виконується з причин великого об'єму робіт (які не автоматизовані), і, головне, дані не аналізуються в комплексі, що не дає змоги робити прогнозування розвитку подій – головної задачі управління ризиком на основі парадигми РОП. Ця процедура, звичайно, у СЦ виконується на основі математичних моделей та спеціального програмного забезпечення (ПЗ) модулем аналізу і прогнозування, який є частиною програмно-апаратного комплексу.

Модуль аналізу і прогнозування СЦ (рис. 2) [6, 7] призначений для вирішення таких основних завдань:

• виявлення взаємозв'язків між різними явищами, формування факторних моделей за результатами аналізу;

• сценарна оцінка наслідків прийнятих управлінських рішень на основі розроблених моделей чинників;

• оцінка ризиків і ступеня впливу різних чинників на досліджувані процеси.

На основі цієї інформації формуються рекомендації особі, що приймає рішення (ОПР) щодо попередження негараздів, тобто запобігання НС. Алгоритм розробки таких рекомендацій теж описано у багатьох працях, наприклад, в [6, 7].

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Прибыль факт, млн. руб	2,83	2,91	2,84	2,81	2,98	3,05	3,05	3,11	3,07	3,38	3,41
Число клиентов	2227	2169,8	3112,6	3455,3	3298,1	3240,8	365	3526,3	3169,1	3211,8	3154,6
Число случайных покупателей	285,2	293,5	331,8	340,1	348,4	357	365	373	362	390	398
Количество магазинов в городах	20	20	20	20	21	21	21	21	21	22	22
Количество городов	5	5	6	6	6	6	6	6	6	6	6

Рис. 2. Приклад відображення прогнозної інформації

Програмно-апаратний комплекс повинен забезпечувати функціонування СЦ в таких основних режимах:

• стратегічне управління;

• моделювання і прогнозування;

• оперативне керування;

• кризове управління.

Інформаційний фонд СЦ (бази і банки даних, сховище даних) повинен містити повний набір даних по об'єктах управління, систему класифікації та кодування інформації. Необхідний доступ може реалізовуватися в режимах онлайн або оффлайн з урахуванням дотримання інформаційної безпеки. Звісно, варіанти ПЗ існують, але ж у кожному окремому випадку нові рішення будуть потрібні.

2.2. Системи моніторингу безпеки (СМБ) розвинутих країн

Лідерами серед розвинених країн є США та ЄС, в яких проводиться моніторинг небезпечних явищ, процесів, факторів із обов’язковим розміщенням засобів контролю на космічних платформах та передачею отриманої інформації на наземні центри моніторингу. Серед кращих зразків таких систем є Аварійна служба управління Європейського Союзу «Коперник» (Copernicus EMS), VS(США), Pachube (Японія) тощо. Існує низка міжнародних ініціатив, спрямованих на використання даних дистанційного зондування Землі для попередження та ліквідації надзвичайних ситуацій (НС) та екстреного реагування, до яких Україна вже почала долучатися. До них слід віднести Міжнародну «систему систем спостереження Землі» GEOSS (Global Earth Observation System of Systems), Міжнародну хартію

щодо космосу та великих катастроф, Партнерство з комплексної стратегії глобальних спостережень, Глобальний моніторинг в інтересах охорони навколишнього середовища та безпеки (GMES – Global Monitoring for Environmental Security), Програму попередження та зменшення наслідків стихійних лих Всесвітньої метеорологічної організації, Платформу ООН UN-SPI DER, Міжнародну ініціативу «Космос і великі катастрофи» (International Charter «Space and Major Disasters»). Такі системи надають можливість своєчасного прийняття рішень практично завжди. Своєчасна евакуація населення як попереджувальний захід цивільного захисту навіть у минулому 2017 р. дозволила запобігти значних людських втрат у цих країнах, хоча на це були витрачені значні кошти.

2.3. Світові задачі моніторингу на найближчі роки

Оцінка ризику катастроф значною мірою базується на інформації щодо даних втрат від стихійних лих. На даний час у світі є різні методології збору даних відносно втрат від стихійних лих, а це створює труднощі щодо обробки агрегованих даних та оптимізації зусиль з профілактики на міжнародному рівні. Саме завдяки такій РОП-стратегії на світовому рівні, не зважаючи на збільшення катастроф, збитки, летальні наслідки знижуються [10] (рис. 3), хоча матеріальні втрати й зростають.

Рис. 3. Природні катастрофи у світі

У лютому 2017 року з метою універсалізації даних, які будуть надаватися країнами в рамках моніторингу виконання Сендайської рамкової програми дій зі зменшення небезпеки стихійних лих на період 2015–2030 рр. (далі – СРПД) Генеральною Асамблеєю ООН схвалено резолюцію A/71/644 щодо показників зменшення ризиків стихійних лих. Зокрема, згідно з сімома глобальними цілями СРПД [11], до 2030 року потрібно:

• добитися значного зниження світового рівня смертності внаслідок стихійних лих, щоб у період 2020-2030 років середня кількість таких смертей із розрахунку на 100 000 осіб була меншою, ніж у 2005–2015 роках;

• домогтися значного скорочення кількості постраждалих осіб у загальносвітовому масштабі, щоб у період 2020-2030 років середня кількість осіб, які постраждали від лих, з розрахунку на 100 000 осіб була меншою, ніж у 2005–2015 роках;

• скоротити прямі економічні втрати від стихійних лих по відношенню до світового валового внутрішнього продукту;

• значно зменшити шкоду, заподіяну стихійними лихами об'єктам критичної інфраструктури, та збитки у вигляді порушень роботи основних служб, включно з медичними установами і навчальними закладами, у тому числі за рахунок зміцнення їх потенціалу протидії;

• значно збільшити кількість країн із національними та місцевими стратегіями зі зменшення ризиків стихійних лих;

• посилити міжнародне співробітництво з країнами, що розвиваються, шляхом надання їм достатньої та безперервної підтримки у реалізації ухваленої на національному рівні політики у рамках виконання СРПД;

• істотно покращити ситуацію з наявністю систем раннього попередження, які охоплюють різні види загроз, інформації та оцінок ризиків стихійних лих, а також розширити доступ до них.

Отже, задачі, які відмічені на початку статті, корелюють з загальними задачами людства, проголошеними у Сендаї. Центральна, головна задача – це завчасне виявлення загрози збільшення ризиків. Відомо, що їх рішення можливе за рахунок постійно діючої системи моніторингу безпеки, яка містить підсистеми аналізу та прогнозування ризиків. Стосовно нашої держави маємо таку ситуацію. Питання здійснення моніторингу і прогнозування через створення та функціонування системи моніторингу і прогнозування відображені в Кодексі цивільного захисту України. Реалізацію комплексу зазначених питань покладено на єдину державну систему цивільного захисту й визначено в Положенні про її створення. Проте чіткого цілісного системного відображення реалізації завдань і заходів щодо моніторингу і прогнозування ризику виникнення НС в державі не створено. Тому існуючі територіальні і функціональні підсистеми єдиної державної системи цивільного захисту не забезпечують належного щоденного збирання, опрацювання, передавання та аналізування інформації про ймовірність виникнення НС техногенного та природного характеру, відпрацювання запобіжних заходів та пропозицій щодо їх проведення.

На даний час моніторинг і прогнозування НС в Україні здійснюються на рівні регіональних, галузевих або інших самостійних систем, не об'єднаних у єдиний інформаційно-аналітичний комплекс [9]. Такий стан справ призводить до зниження рівнів достовірності прогнозів щодо виникнення НС природного та техногенного характеру. Тому важливим залишається питання відпрацювання спільних методів збирання, оброблення та зберігання моніторингової інформації, що дозволить аналізувати та систематизувати ризики. Застосування технології СЦ є актуальною та нагальною потребою. Як доведено у попередній статті [4], навіть фінансові витрати на нові технології на сучасному рівні не такі й великі, значно менші щорічних збитків НС, які можна попередити. Але одним із негативних факторів є те, що ми не маємо своїх супутників. Інформація з космосу доступна з великим (до 3-х днів) запізненням, з чого слідує, що у такий спосіб можна відслідковувати тільки «повільні» небезпечні процесі, які у сфері управління безпекою у меншості.

Управлінням ООН із зменшення небезпеки катастроф створено онлайн-ресурс для збору даних щодо огляду стану готовності надання відомостей у зв’язку з оцінкою реалізації виконання СРПД. Починаючи з березня 2018 року, до системи онлайн-моніторингу СРПД необхідно надавати дані щодо кількості загиблих та кількості постраждалих осіб, які постраждали від стихійних лих, з розрахунку на 100 000 осіб; дані щодо прямих економічних втрат від стихійних лих по відношенню до світового валового внутрішнього продукту; дані щодо збитків, заподіяних катастрофами об'єктам критичної інфраструктури, та збитки основним службам, включно з медичними установами і навчальними закладами, у тому числі за рахунок зміцнення їх потенціалу протидії.

Також до 2019 року до системи моніторингу СРПД необхідно надавати інформацію щодо кількості країн з національними та місцевими стратегіями зі зменшення ризиків стихійних лих, інформацію щодо міжнародного співробітництва з країнами, наявність систем раннього попередження, які охоплюють різні види загроз, інформації та оцінок ризиків стихійних лих, а також розширити доступ до них.

2.4. Теоретичні основи моніторингу безпеки на основі ймовірнісного моделювання

Системи моніторингу безпеки (СМБ) є однією із складових підсистем автоматизованих систем управлення безпекою, які досліджуються в багатьох наукових працях [9, 12]. У проведених наукових дослідженнях доведено, що СМБ мають бути трьох рівнів: об’єктового – І-ий рівень, регіонального – ІІ-ий та державного – ІІІ-ій. Очевидно, що функції моніторингу Φ залежать від типу об’єкта та від вектора $[X_i]$ вхідних параметрів, які характеризують безпеку. Число параметрів i має бути мінімальним, але достатнім. Крім того, необхідно чітко визначити моделі перетворень інформації відповідних рівнів:

$M1, M2, M3$. Завдання моделей $M_j (i = 1,2,3)$ полягає в тому, щоб із множини інформації j-го рівня вибрати важливу інформацію I для передачі на наступний рівень для ОПР тощо. Тобто, для кожного типу об'єкта необхідно визначити алгоритм перетворень інформації за схемою:

$$X \to M1 \to Y \to M2 \to Z \to M3 \to I_{ОПР}. \quad (1)$$

Мають бути визначені не тільки моделі $M1, M2, M3$, але й вектори інформації (X, Y, Z) усіх рівнів. Ці вектори повинні містити критерії безпеки на кожному рівні, причому розмірність наступного має бути меншою, ніж попереднього. Інформація на кожному рівні має містити співвідношення параметрів моніторингу з допустимими значеннями критеріїв безпеки та рекомендації щодо рішення, як діяти оператору чи особі, що приймає рішення. У даній роботі проаналізовано саме формування критеріїв безпеки І-ого рівня з позиції ризик-орієнтованого підходу (РОП).

З позиції РОП – маємо можливість і необхідність виділення параметрів X_i, знання яких надає можливість визначити заходи попередження виникнення великого (неприпустимого) ризику. У сучасній практиці моніторингу в Україні ці параметри визначають експертними методами на основі досвіду. Проте, такі методи не завжди працюють об'єктивно та частіше мають великі невизначеності або навіть помилки. Прикладом такої системної помилки в Україні є спроба впровадження автоматизованих систем раннього виявлення (АСРВ) НС на автозаправках (АЗС) [13]. За діючою процедурою АСРВ на АЗС реагують на дим і вогонь та передають сигнал на підприємство розробника АСРВ, звідки тривожний сигнал передається в пожежну частину. Але ж для АЗС з десятками тон бензину критерії «дим та вогонь» не можна назвати раннім виявленням. Тобто, фактично основна функція за парадигмою РОП «запобігання виникнення НС» не виконується. З метою «запобігання» потрібно контролювати параметри X_i за результатами кількісних оцінок ризику відповідно до їх важливості та вірогідності настання подій, що можуть вплинути на можливість загоряння. Критерії безпеки мають бути більше «попереджувальними», концентрувати увагу ОПР задовго до виникнення, навіть розливів, пального, адже причини розливів виникають завдяки невиконанню деяких вимог з безпеки X_x. Під час здійснення моніторингу постійно контролюються виробничі процеси та умови зберігання шкідливих і небезпечних речовин. Необхідно також виконувати функцію повідомлення (оповіщення) про відхилення параметрів безпеки від допустимих норм. Припустимо, що на об'єкті є H небезпечних речовин. Умови їх зберігання контролюють $K1$ систем та $K2$ систем, які контролюють M небезпечних процесів. Складовою системи контролю $K(K1, K2)$ є також оператори АЗС. Розглянемо, що ж має відноситися до параметрів безпеки (ПБ) – вектора допустимих значень вхідних параметрів $[X]$. Згідно з загальними уявленнями, це параметри, які підвищують ризик. Але ризик є узагальненим параметром, який потребує розрахунку та залежить від деяких конкретних параметрів виробництва. Якщо відомий допустимий ризик $[R]$, то можна обчислити й граничні параметри безпеки – критерії безпеки $[X]$. На основі відомих допустимих значень ризику $[R]$ та постульованих наслідків $(U_i = const)$ отримуємо рівняння відносно $[X_i]$, а саме:

$$[R] = P([X_i]) \times U_i. \quad (2)$$

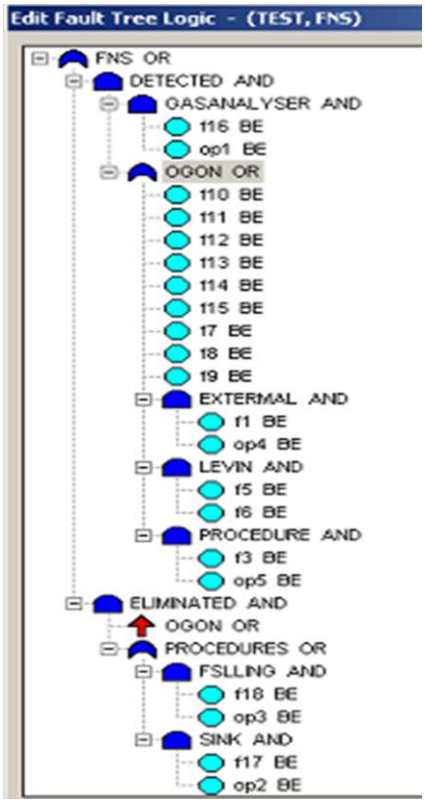

Рис. 4. Логічна модель НС загоряння АЗС (Позначення: BE – basic event – базисна подія)

Рішення рівняння (2) дає можливість визначити для кожного фактора його допустимі значення $[X_i]$ за умови неперевищення допустимого ризику. Отже, критерії безпеки мають бути визначені на основі моделювання ризику та підтверджуватися досвідом фахівців [9]. Тому, якщо масив $[U]$ визначає можливі наслідки k аварійних станів, що можуть статися, то саме моделювання події $[U_1]$ – проливу палива – дасть відповідь про параметри безпеки X_i, що впливають на появу цієї події. Найбільш важливі з них, за критеріями важливості (Бірнбаума, чи Фуселі-Весели), можуть бути обрані як критерії безпеки для СМБ.

З метою перевірки наведених положень побудовано ймовірнісну структурно-логічну модель НС на АЗС – займання проливу пального на АЗС, яка має сучасні системи захисту [14], за допомогою коду SAPHIRE (рис. 4). В моделі враховано 18 факторів F_i ($i \in$ [1, 18]), та 4 можливі помилки персоналу ($OP_к$) ($k \in$ [1, 4]), що можливі при виявленні проливу та відмовах елементів систем безпеки. За результатом моделювання отримано значення ймовірності НС: P = 8.18E-5 (на основі середньо статистичних імовірностей базисних подій) та логічну функцію ймовірності НС:

$$P = \Phi(F_i \vee OP_k). \qquad (3)$$

Ця функція відтворюється сполученням подій (мінімальних перерізів (МП) – min cat) M_c, які призводять до виникнення НС. Саме вона є джерелом інформації про критерії безпеки та вибору запобіжних заходів попередження НС [15]. Усього утворюється 36 МП, але ж імовірність першого й останнього відрізняються на вісім порядків (табл. 1). Тобто, до 3-го порядку малості функція може бути записана тільки як сума 14 МП (14 членів у формулі):

$$P = F1 \cdot F18 \cdot OP4 + F10 \cdot F18 \cdot OP3 + F18 \cdot F9 \cdot OP3 + \ldots + F17 \cdot F9 \cdot OP2 + \varepsilon. \qquad (4)$$

Вона може бути використана як імітаційна модель виникнення НС для вибору факторів F_i як управляючих впливів, що найбільш оптимальні. До другого порядку малості, згідно з табл. 1, тільки 11 з 18 факторів мають якийсь вплив, з чого слідує висновок, що кількість подій, які потрібно контролювати навіть на першому рівні, значно скорочується за результатами моделювання. Отже, на основі (3, 4) можна будувати залежності ймовірності виникнення НС від кожного фактора та їх сполучень імітацією змін фактора у діапазоні припустимих (можливих) значень (рис. 5). Як бачимо, найбільш впливові фактори (перший мінімальний переріз) змінюють імовірність виникнення НС у різній мірі від 1 до 4 порядків. Отже, логічно обрати за критерій безпеки для внутрішнього моніторингу саме ці фактори як найбільш впливові, а за результатами імітаційного моделювання помилок персоналу визначати найбільш впливовий напрям при підготовці (тренінгу) персоналу.

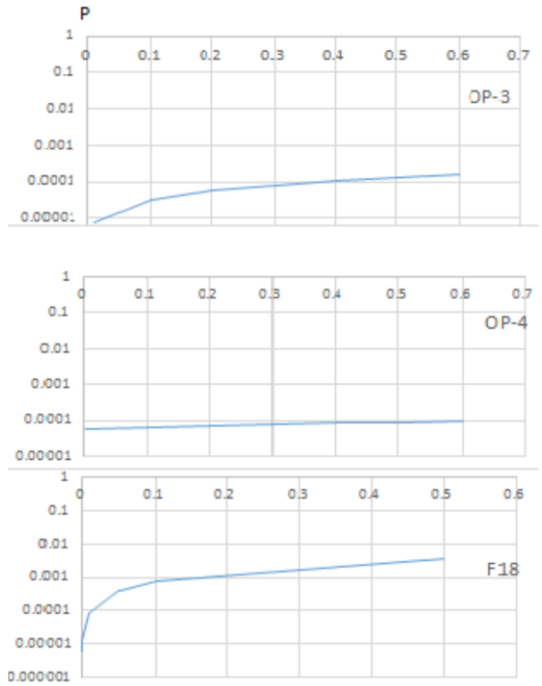

Рис. 5. Залежності ймовірності НС від впливових факторів

Як бачимо (рис. 5), найбільший вплив на ймовірність виникнення НС має фактор F18. Він змінює ймовірність виникнення НС майже на 4 порядки, з чого слідує, що саме можливість його проявлення має контролюватися найбільш ретельно. У таблиці значимості він також посідає перше місце (табл. 2). Звісно, потрібно вивчити умови його виникнення та засоби попередження, тренувати персонал щодо аварійних дій мінімізації його шкідливого впливу. Функції, що показані на рис. 5, відображають чутливість ризику [15]. Саме за їх допомогою можливо здійснити найкраще управління ризиком. Підсумовуючи, можна сказати, що ймовірнісне моделювання складних систем та процесів надає можливість проведення ретельного аналізу процесів виникнення небезпеки та на його основі здійснювати не тільки прогнозування зміни ризику, але й обирати фактори найбільшого впливу для зменшення ризику до прийнятих значень. Але, як вже неодноразово було сказано [4, 9], такі моделі можуть будувати фахівці, що пройшли спеціальну підготовку. Тому вони повинні бути створені заздалегідь для їх практичного використання у модулі аналізу й прогнозування СЦ. Оператор ОПР повинен мати можливість зміни значень факторів, вхідних даних тощо.

2.5. Інші моделі для модуля аналізу і прогнозування

Звісно, не тільки ймовірнісний метод аналізу (ІАБ) безпеки можливий для застосування у СЦ. Наприклад, у банківській сфері для аналізу ризиків широко використовується методологія ключових індикаторів ризику (КІР) (рис. 6), заснована на вагових коефіцієнтах факторів різної природи [16, 17]. Ця методологія моделювання теж можлива й для інших галузей і сфер безпеки, але ж вона тільки здається простішою. Її впровадження потребує висококваліфікованих експертів, до того ж у сфері безпеки значно більше факторів впливу, ніж у фінансовій, що створює додаткові труднощі.

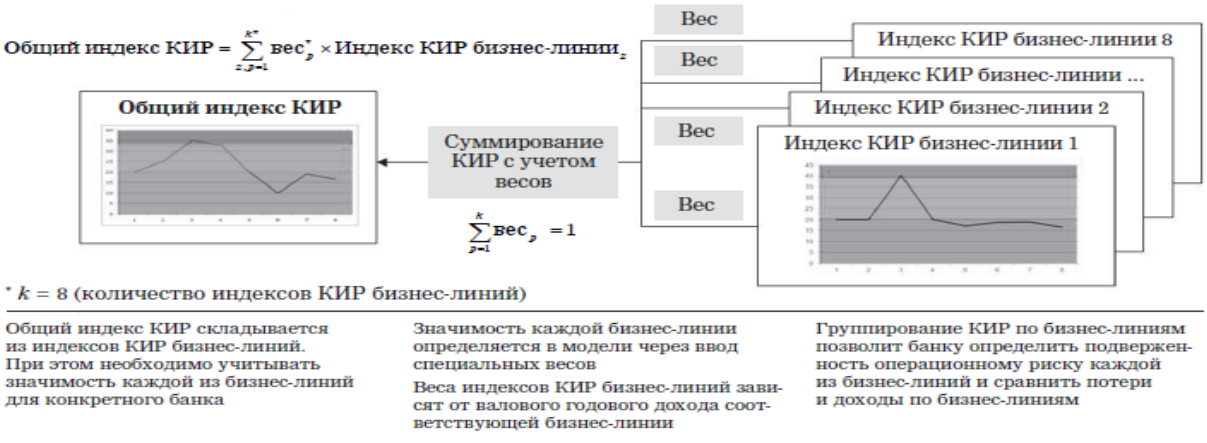

Рис. 6. Методологія ключових індикаторів ризику

Таблиця 1. Мінімальні перерізи логічної функції FNS

Cut No.	% Total	% Cut Set	Frequency	Cut Sets
1	31.2	31.2	2.400E-004	F1, F18, OP3, OP4
2	50.7	19.5	1.500E-004	F10, F18, OP3
3	70.2	19.5	1.500E-004	F18, F9, OP3
4	85.8	15.6	1.200E-004	F18, F7, OP3
5	89.7	3.9	3.000E-005	F15, F18, OP3
6	92.2	2.5	1.950E-005	F18, F3, OP3, OP5
7	94.2	2.0	1.500E-005	F12, F18, OP3
8	96.1	2.0	1.500E-005	F14, F18, OP3
9	97.6	1.5	1.167E-005	F18, F8, OP3
10	99.0	1.4	1.080E-005	F13, F18, OP3
11	99.4	0.4	2.625E-006	F11, F18, OP3
12	99.6	0.2	1.600E-006	F1, F17, OP2, OP4
13	99.7	0.1	1.000E-006	F10, F17, OP2
14	99.9	0.1	1.000E-006	F17, F9, OP2
15	100.0	0.1	8.000E-007	F17, F7, OP2
16	100.0	0.0	2.000E-007	F15, F17, OP2
17	100.0	0.0	1.300E-007	F17, F3, OP2, OP5
18	100.0	0.0	1.000E-007	F12, F17, OP2
19	100.0	0.0	1.000E-007	F14, F17, OP2
20	100.0	0.0	8.000E-008	F1, F16, OP1, OP4
21	100.0	0.0	7.780E-008	F17, F8, OP2
22	100.0	0.0	7.200E-008	F13, F17, OP2
23	100.0	0.0	5.000E-008	F10, F16, OP1
24	100.0	0.0	5.000E-008	F16, F9, OP1
25	100.0	0.0	4.000E-008	F16, F7, OP1
26	100.0	0.0	1.750E-008	F11, F17, OP2
27	100.0	0.0	1.000E-008	F15, F16, OP1
28	100.0	0.0	6.500E-009	F16, F3, OP1, OP5
29	100.0	0.0	5.000E-009	F12, F16, OP1
30	100.0	0.0	5.000E-009	F14, F16, OP1
31	100.0	0.0	4.800E-009	F18, F5, F6, OP3
32	100.0	0.0	3.890E-009	F16, F8, OP1
33	100.0	0.0	3.600E-009	F13, F16, OP1
34	100.0	0.0	8.750E-010	F11, F16, OP1
35	100.0	0.0	3.200E-011	F17, F5, F6, OP2
36	100.0	0.0	1.600E-012	F16, F5, F6, OP1

Таблиця 2. Важливість події НС «Займання пального»

IMPORTANCE MEASURES REPORT
(Sorted by Fussell-Vesely Importance)

Event Name	Num. of Occ.	Probability of Failure	Fussell-Vesely Importance
F18	12	1.000E-001	9.930E-001
OP3	12	3.000E-001	9.930E-001
OP4	3	4.000E-001	3.138E-001
F1	3	2.000E-002	3.138E-001
F10	3	5.000E-003	1.961E-001
F9	3	5.000E-003	1.961E-001
F7	3	4.000E-003	1.569E-001
F15	3	1.000E-003	3.922E-002
OP5	3	5.000E-001	2.549E-002
F3	3	1.300E-003	2.549E-002
F12	3	5.000E-004	1.961E-002
F14	3	5.000E-004	1.961E-002
F8	3	3.890E-004	1.526E-002
F13	3	3.600E-004	1.412E-002
OP2	12	2.000E-001	6.617E-003
F17	12	1.000E-003	6.617E-003
F11	3	8.750E-005	3.432E-003
OP1	12	1.000E-001	3.309E-004
F16	12	1.000E-004	3.309E-004
F5	3	4.000E-004	6.275E-006
F6	3	4.000E-004	6.275E-006

Методологія імітаційного моделювання теж надає можливість управління стохастичними процесами [18], теж існує ПЗ для реалізації методології. Звісно, моделі небезпечних процесів та систем також мають бути створені заздалегідь. Але ж, як і у методології ІАБ, кінцевий продукт, саме ПЗ, може мати вигляд «чорної скриньки» з доступом ОПР тільки до масивів вхідних та вихідних параметрів.

3. Параметри моніторингу вищих рівнів

Таким чином, ми дійшли до висновку, що фактори моніторингу I рівня $[X]$ мають бути науково обґрунтовані шляхом моделювання небезпечних процесів і систем. Факторі моніторингу (вхідні параметри) II рівня – $[Y]$ – це більш загальні параметри, причому існують фактори $[Q] \in [Y]$, які не потрібно моніторити на I (об'єктовому) рівні: стан повітря, якість питної води, ймовірність паводку, ймовірність землетрусу та ін. Тобто, якщо в регіоні існує k небезпечних процесів та m небезпечних об'єктів, з яких за даними моніторингу I рівня отримуємо дані про узагальнений територіальний ризик:

$$R = \sum_k R_k + \sum_m R_m + \delta,\ R < [R], \tag{5}$$

де δ – загальна погрішність моделювання, [R] – допустимі нормативні значення ризику.

Вектор параметрів моніторингу II (регіонального) рівня можна представити як

$$Y = R + Q. \tag{6}$$

Обробка інформації вектора Y потребує моделювання взаємного впливу ризиків різного походження. Як приклад такого впливу можна привести нещодавню повінь у США,

яка призвела до вибухів на хімічному заводі [19], або роль цунамі в аварії на АЕС Фукусіма.

Вибір факторів моніторингу ІІІ рівня – $[Z]$ можна здійснювати з узагальнення ризику на рівні регіонів (ІІ рівень) на основі обробки вихідних даних (5) та (6) та вимог обрахування й представлення даних за установленим форматом за Сендайськими вимогами. Очевидно, що поставлені задачі моніторингу легко можуть бути вирішені за технологією СЦ. Звісно, загальні фактори Z мають бути відомі на І та ІІ рівнях, більше того, інформаційна технологія СЦ дозволяє зробити наскрізний перегляд факторів ризику з вищого рівня і завжди мати інформацію про ризики вищого рангу на об'єктовому рівні. Створювання системи моніторингу в іншому варіанті суперечить світовому досвіду, не може бути корисним для безпеки держави [9, 12].

4. Висновки

1. Критерії безпеки для автоматизованих систем моніторингу безпеки потрібно обирати за результатами ймовірнісного та/або імітаційного моделювання. Для практичної реалізації цього необхідна розробка, у першу чергу, відповідних галузевих керівництв з управління ризиком.
2. Система моніторингу безпеки, яка створюється, має бути заснована на нових технологіях ситуаційних центрів, має бути впроваджена разом з інформатизацією роботи рятувальних підрозділів та структурними організаційними змінами системи управління безпекою.
3. До функціонування системи моніторингу на сучасному рівні повинні бути пред'явлені такі вимоги:

• здійснювати безперервний збір інформації про розвиток небезпечних природних явищ і техногенних процесів із різних джерел на всій території України в одному місці;

• своєчасно виявляти негативні процеси у техносфері, небезпечні природні явища, інші чинники, що є джерелами виникнення небезпечних подій та НС;

• прогнозувати ризики виникнення та розвитку небезпечних подій та НС і розробляти перелік необхідних запобіжних заходів для конкретних регіонів та районів країни;

• готувати оптимальні й обґрунтовані управлінські рішення щодо запобігання виникненню небезпечних подій та НС, їх ліквідації;

• зменшити кількість жертв та обсяг втрат матеріальних цінностей внаслідок НС за допомогою достовірного прогнозування, своєчасного попередження і реагування на них;

• створити єдину інформаційну базу даних про небезпечні території і об'єкти, на яких за певних умов можуть виникнути небезпечні події та НС;

• здійснити постійну інформаційно-аналітичну підтримку з питань цивільного захисту діяльності центральних і місцевих органів виконавчої влади, органів місцевого самоврядування.

СПИСОК ДЖЕРЕЛ

1. Про затвердження Стратегії реформування системи державного нагляду (контролю), схваленої розпорядженням Кабміну 18.12.2017 р.
2. Регламент функціонування системи моніторингу і прогнозування ризику виникнення надзвичайних ситуацій. Проект [Електронний ресурс]. – Режим доступу: http://www.mns.gov.ua/content/national_lecture.html.
3. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру. Розпорядження Кабінету Міністрів України від 22.01.2014 № 37-р [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/37-2014-%D1%80.
4. Бєгун В.В. Огляд стану та можливостей впровадження ІТ у сферу безпеки [Електронний ресурс] / В.В. Бєгун // Математичні машини і системи. – 2017. – № 4. – С. 67 – 77. – Режим доступу: http://www.immsp.kiev.ua/publications/articles/2017/2017_4/04_2017_Begun.pdf.

5. Ситуационные центры [Електронний ресурс]. – Режим доступу: https://www.polymedia.ru/sistemnaya-integratsiya/analiticheskaya-platforma-visiology/.
6. Аналитическая платформа Visiology [Електронний ресурс]. – Режим доступу: https://www.polymedia.ru/sistemnaya-integratsiya/analiticheskaya-platforma-visiology/.
7. Морозов А.О. Інформаційно-аналітичні технології підтримки прийняття рішень на основі регіонального соціально-економічного моніторингу / А.О. Морозов, В.Л. Косолапов. – К.: Наукова думка, 2002. – 347 с.
8. Інформація про організацію (ІПММС) [Електронний ресурс]. – Режим доступу: http://www.immsp.kiev.ua/history/.
9. Кропотов П.П. Створення сучасної системи моніторингу безпеки – актуальна державна та наукова задача / П.П. Кропотов, В.В. Бєгун, В.Ф. Гречанінов // Системи обробки інформації. – Харків: ХУПС, 2015. – Вип. 11 (136). – С. 199 – 206.
10. Количество связанных с погодой катастроф неумолимо растет, но число их жертв уменьшается, пишет британский журнал The Economist [Електронный ресурс]. – Режим доступа: https://www.economist.com/blogs/graphicdetail/2017/08/daily-chart-19.
11. Сендайская рамочная программа по снижению риска бедствий на 2015–2030 годы [Электронный ресурс]. – Режим доступа: http://www.unisdr.org/we/inform/publications/54970.
12. Голуб С.В. Методологія створення автоматизованих систем багаторівневого соціоекологічного моніторингу: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: 05.13.06 / С.В. Голуб. – Київ, 2008. – 35 с.
13. ДБН В.2.5-76:2014. Автоматизовані системи раннього виявлення загрози виникнення надзвичайних ситуацій та оповіщення населення. – Київ: Мінрегіон України, 2014. – 46 с.
14. Системи захисту АЗС [Электронный ресурс]. – Режим доступу: https://www.forter.com.ua/news-and-articles/systemu_bezopasnosti_azs/
15. Вероятностный анализ безопасности атомных станций: учебн. пособ. / В.В. Бегун, О.В. Горбунов, И.Н. Каденко [и др.]. – Киев: НТТУ КПИ, 2000. – 568 с.
16. Сизикова В. Методика разработки системы индексов ключевых индикаторов риска / В. Сизикова, В. Гаврилина, В. Битюцкий // Риск-менеджмент в кредитной организации. – 2016. – № 4 (24). – С. 54 – 69.
17. Operational Risk Sound Practice Guideline «Key Risk Indicators». The Institute of Operational Risk. – Copyright, 2010, – С. 41 [Електронний ресурс]. – Режим доступу: www.ior-institute.org/public/IORKRIGuidanceNov2010.pdf.
18. Томашевський В.М. Моделювання систем / Томашевський В.М. – К.: Видавнича група BHV, 2005. – 352 с.
19. У Каліфорнії жертвами зсувів стали 13 людей [Електронний ресурс]. – Режим доступу: https://www.rbc.ua/ukr/news/kalifornii-zhertvami-opolzney-stali-13-chelovek-1515545833.html.

Стаття надійшла до редакції 07.02.2018