

УДК 004.386:351.862.4

П.П. Кропотов¹, В.В. Бегун², В.Ф. Гречанінов¹¹ Державна служба України з надзвичайних ситуацій, Київ² Інститут проблем математичних машин і систем НАН України, Київ

СТВОРЕННЯ СУЧАСНОЇ СИСТЕМИ МОНІТОРИНГУ БЕЗПЕКИ – АКТУАЛЬНА ДЕРЖАВНА ТА НАУКОВА ЗАДАЧА

Розглянуто стан і проблеми системи моніторингу безпеки в Україні та її відмінності від систем розвинутих країн. Аналізуються функції в залежності від цілей, сам процес моніторингу розглядається як складова інформаційної технології безпеки. Запропоновано створення трирівневої системи моніторингу. Розглянуто будову критеріїв безпеки за принципами ризик-орієнтованого підходу, алгоритми аналізу інформації, концепцію нової системи та питання ведення бази даних і бази знань з питань безпеки.

Ключові слова: безпека, моніторинг, ризик, модель, інтерфейс, алгоритм.

Вступ

1. **Стан проблеми.** Сутність і призначення системи моніторингу безпеки та прогнозування (СМБ) полягають у спостереженні, контролі і передбаченні небезпечних процесів та явищ природи, техносфери, зовнішніх дестабілізуючих та інших факторів, які є джерелами надзвичайних ситуацій (НС), а також динаміки розвитку ситуацій, якщо НС сталася, визначення масштабів з метою вирішення завдань щодо мінімізації її поширення. Методичне керівництво і координація діяльності системи моніторингу і прогнозування НС на державному рівні має здійснюватися Державною службою України з надзвичайних ситуацій (ДСНС). Прогноз ризиків НС на території країни в цілому здійснює ДСНС у взаємодії з іншими центральними органами виконавчої влади. Разом з цим, на цей час моніторинг і прогнозування НС в Україні здійснюються на рівні регіональних, галузевих або інших самостійних підсистем, не об'єднаних у єдиний інформаційно-аналітичний комплекс. Загальнодержавну систему моніторингу джерел НС та їх прогнозування у державі не створено [1]. Сучасний стан розвитку суспільства показує зростаючу тенденцію впровадження технічних, інформаційних і програмних ресурсів як інструментальних механізмів підтримки інноваційного розвитку, що має бути відображено у СМБ, тощо.

У той же час кожен регіон України, ДСНС України та її територіальні органи мають достатню кількість технічних ресурсів: сучасні комп'ютери та мережі. Існує ситуаційний центр СБУ [2], що має системи відображення інформації на основі ГІС технологій, створене та відпрацьоване програмне забезпечення системи підтримки прийняття рішень (СППР) [2]. Всі ці елементи і є атрибутами сучасних систем моніторингу і прогнозування. Більш того, ще за часів початку формування Міністерства надзвичайних ситуацій України (МНС), була система моні-

торингу, яка функціонувала у межах єдиної державної системи цивільного захисту (ЄДСЦЗ). Але у зв'язку з загальними зовнішніми та внутрішніми причинами ця система знаходиться у неробочому стані. Тобто, проблема створення сучасної СМБ в Україні, на наш погляд, є в тому, щоб об'єднати існуючий науковий потенціал з проблем безпеки [2 – 4] на основі сучасної парадигми ризик-орієнтованого підходу (РОП) [5], визначитися з основними функціями і задачами СМБ саме з інформаційної точки зору.

2. **Відмінності від розвинутих країн, які мають бути усунуті.** На міжнародному рівні пріоритетні напрями дій у цій сфері відзначені Хіозькою рамковою програмою дій на 2005-2015 рр., яка спрямована на створення потенціалу протидії небезпекам природного походження та відповідним екологічним і техногенним ризикам. Цей документ прийнято на Всесвітній конференції зі зменшення небезпеки лих (відбулась 18-22 січня 2005 року в м. Кобе, префектура Хіого, Японія), він передбачає 5 пріоритетних напрямів діяльності у цій сфері:

забезпечення пріоритетності питань зниження ризику природних та техногенних небезпек у діяльності державних органів влади;

виявлення, оцінка та моніторинг факторів ризику виникнення лих та покращання раннього попередження;

широке використання знань, інновацій та навчання для створення безпечних умов і поліпшення системи реагування;

зниження основних факторів ризику виникнення надзвичайних ситуацій;

підвищення готовності сил реагування до дій в умовах лиха.

У більшості Європейських країн склалася досить розвинута й ефективна система органів, сил і засобів цивільної оборони (ЦО) або цивільного захисту (ЦЗ). Вона вирішує завдання забезпечення

захисту і виживання населення, економічного потенціалу та соціальної структури держави як у мирний час, під час різних лих, аварій і катастроф, так і в умовах воєнного стану. Звісно, має місце повна автоматизація процесів на основі сучасних комп'ютерних технологій [6].

Наближення вітчизняного законодавства у сфері техногенної та природної безпеки до вимог Європейського союзу (ЄС) передбачено, зокрема, і Угодою про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, на 2014-2017 рр. Одним із ключових проєктів ЄС у цій сфері стала програма із запобігання, готовності та реагування на катастрофи природного та техногенного характеру для країн Східного партнерства PPRD East, головним бенефіціаром якої в Україні є ДСНС України [6].

Основна частина

3. Визначення моніторингу в залежності від цілей. Діяльність з моніторингу і прогнозування НС є багатоплановою та багатофункціональною. Вона здійснюється багатьма організаціями (установами) з використанням різних методів і засобів. Так, наприклад, моніторинг і прогноз подій гідрометеорологічного характеру здійснюються ДСНС України, до компетенції якої належить реалізація державної політики у сфері гідрометеорологічної діяльності, та яка, крім того, веде моніторинг стану і забруднення атмосфери, води, ґрунту [1].

Сейсмічні спостереження і прогноз землетрусів у країні здійснюються системою сейсмологічних спостережень і прогнозу землетрусів, до якої входять установи і системи спостереження Національної академії наук, Міноборони і Мінрегіону.

Особливістю системи моніторингу (контролю) безпеки в Україні є також наявність великої кількості потенційно небезпечних об'єктів (ПНО) та об'єктів підвищеної небезпеки (ОПН) [1]. Тобто, маємо $M = \{1, 2, \dots, m\}$ учасників процесу моніторингу, причому m залежить від рівня управління безпекою, та $\Phi = \{1, 2, \dots, \phi\}$ функцій (завдань) моніторингу для кожної підсистеми. Зауважимо, що деякі функції дублюються різними підсистемами. Іншими особливостями СМБ є фактична відсутність сучасного інформаційного забезпечення системи, а також політичні аспекти (нестабільність влади, високий рівень корупції). Головними невідповідностями методологій (стратегій) державного нагляду (контролю) вимогам сьогодення є принципово неправильна постановка завдання регулювання безпеки та практична відсутність економічного механізму саморегулювання.

Відповідно до Закону України «Про основні заходи державного нагляду» здійснення державного нагляду повинне відбуватися шляхом оцінок ступеня ризику від здійснення господарської діяльності.

Ризик – кількісна міра небезпеки, що визначається функцією двох змінних: імовірності небажаної події та розміру збитків від неї: $R = P \times U$. Завдання контролю (моніторингу) безпеки має бути представлено як алгоритм перевірки випадкової величини у реальному часі:

$$R(t) = P(t, x_i) \times U(P, Y_i), \quad (1)$$

де $P(t, x_i)$ – імовірність можливих небажаних подій (аварій); $U(P, Y_i)$ – можливі наслідки (збитки) від цих подій; x_i – групи показників (змінних індикаторів), які характеризують підприємство і обставини ймовірних небажаних подій (аварій).

Наслідки $U(P, Y_i)$ залежать від події, яка може трапитися та інших внутрішніх і зовнішніх факторів Y_i , зокрема, часу доби, пори року, погодних умов тощо. Тобто кінцевим результатом моніторингу має бути узагальнений розрахунковий параметр – ризик. Але ж в реальності цього немає, розрахунки та оцінки ризику не проводяться: немає ні методик, ні відповідного програмного забезпечення. Усі існуючі державні служби контролю безпеки проводять інспекції і оцінки безпеки на якісному рівні за трибальною шкалою: низький, середній, високий ризик. Інспекції не здатні ефективно виконувати свої функції через недостатні знання технологічних процесів і ризиків. Один і той же інспектор має перевіряти різні типи підприємств: металургійний комбінат, гірничо-збагачувальний комбінат, хімічний комбінат, АЗС, залізничний вокзал тощо.

4. Моніторинг як складова інформаційної технології безпеки (ІТБ). Моніторинг є однією зі складових елементів системи управління безпекою в ринкових умовах, що описано в [2, 4, 15]. Має бути як внутрішній моніторинг (моніторинг і контроль підприємства), так і моніторинг (контроль) зовнішній.

Внутрішній моніторинг (контроль) підприємства проводиться з метою перевірки дотримання вимог встановлених норм ризику для персоналу, населення та довкілля і має здійснюватися спеціалізованим підрозділом об'єкта. Під час його здійснення необхідно постійно контролювати (перевіряти) виробничі процеси та умови зберігання шкідливих і небезпечних речовин. Має також виконуватися функція повідомлення (оповіщення) про відхилення параметрів безпеки від допустимих норм. Якщо на об'єкті є N небезпечних речовин, умови зберігання контролюють $K1$ систем та L небезпечних процесів, які контролюють $K2$ систем. Складовою систем $K(K1, K2)$ є оператор системи оповіщення та запобігання поширенню НС.

Розглянемо, що має відноситися до параметрів безпеки (ПБ) – вектора допустимих значень вхідних параметрів $[X]$. Згідно з загальними уявленнями, це параметри, які підвищують ризик, але ризик є загальним параметром, що потребує розрахунку і залежить від параметрів виробництва $[Y]$. Якщо відомі допустимий ризик $[R]$, то на основі формул залежності (1) можна викреслити й граничні параметри безпе-

ки – **критерії безпеки** $[X_i] \in [X]$. Звичайно, потрібне рішення зворотної задачі, яка слідує з рівняння (1), а саме: на основі відомих допустимих значень ризику $[R]$ та постульованих наслідків $U = \text{const}$ з (1) отримуюмо рівняння відносно $[X_i]$, а саме:

$$[R] = P([X_i]) * U. \quad (2)$$

Потрібне чітке представлення критеріїв $[X_i]$ при створенні сучасної системи моніторингу. Оскільки законодавчо та нормативно прийнятий ризик $[R]$ не визначено, то, відповідно й ПБ не визначені, що робить неможливим рішення рівняння (2). Ця обставина дозволяє (примушує) створювати відомчі накази [7] про всякі заборони, які не завжди обґрунтовані, але на думку їх авторів зменшують ризик. Зв'язок з ризиком цих вимог не доведено, але заборона частіше створює проблеми у функціонуванні підприємств, що у підсумку може призводити до корупційних угод інспектора та господаря. В [8] теж є нечіткі визначення критеріїв безпеки, наведені критерії типу: «гарантування захисту життя та власності (ст.7)», або «створюється небезпека виникнення НС» або «відомості про надзвичайні ситуації, що прогножуються або виникли, з визначенням їх класифікації, меж поширення і наслідків, а також про способи та методи захисту від них». Такі критерії безпеки, які нечітко визначені не дозволяють створити автоматизовані СМБ. Під час внутрішнього моніторингу об'єкт проводить **самооцінку** процесів ідентифікації ризиків та виконання плану реагування на ризики, проводиться оцінка ефективності заходів для зниження ризиків та величини залишкового ризику і його прийнятність. Самооцінка безпеки, як показує досвід АЕС, є ефективною процедурою підтримки належного рівня безпеки і, на наш погляд, може бути успішно задіяна з належною методичною підтримкою й у сфері техногенної безпеки.

Ще декілька слів про поняття *постульовані наслідки*: $U = \text{const}$. З досвіду відома більшість наслідків аварій: розгерметизація реакторної установки – це ризик опромінення; розгерметизація ємності хімічно небезпечної речовини – ризик отруєння; розлив нафтопродуктів – ризик пожеж і т.ін. На основі принципу «запобігання» небезпеки, очевидно, потрібно не допускати саме цих первинних (небезпечних) подій, які й уявляємо як *постульовані наслідки* U_i . Саме їх імовірність краще моделювати та розраховувати, а на основі цього моделювання визначати критерії безпеки $[X_i]$. Це виправдано, оскільки дозволяє реалізувати принцип «запобігання» ще на більш ранній стадії виникнення та розвитку аварії. Звісно, моделювання процесів та розрахунки ризику за умови, *якщо подія сталася*, теж необхідні. Такі оцінки дозволяють правильно прийняти рішення в умовах аварії.

Зовнішній моніторинг (контроль) у такому разі має проводитися виключно за параметрами (індикаторами), які важливі для безпеки регіону розташування ОПН, безпеки персоналу, населення та довкілля, а саме:

- чи планується управління ризиками,
- чи є кількісна оцінка (самооцінка) ризиків,
- чи задовольняються при цьому умови прийнятного ризику,
- чи реалізуються сплановані заходи зменшення ризику,
- чи виконуються основні вимоги законодавства.

Саме у такому значенні зовнішній моніторинг більше відповідає процесам державного нагляду (контролю). Оскільки ризик є комплексною та індивідуальною розрахунковою характеристикою об'єкта, то для кожного об'єкта мають бути розроблені заходи щодо зменшення ризику. Алгоритм розробки цих заходів є складовою моделі оцінок ризику [9]. Ці моделі саме і надають змогу визначити оптимальний (максимальний) проміжок часу між інспекціями T_m за умови неперевищення ризику для працюючого персоналу, населення та довкілля. При цьому слід врахувати ризики від усіх небезпек за тією ж умовою неперевищення допустимого рівня ризику:

$$\text{Max}(T_m) : R_a < [R_d], \quad (3)$$

де R_a – *поточне (оціночне) значення ризику*.

Коротко задачу оптимізації часу між інспекціями T_m перевірок об'єктів O_i з множини усіх об'єктів регіону L математично можна представити так [9]:

$$< O_i > O_i \in L; O_i : R_i = F(T_m); A \in L; R_a = \sum R_i; \quad (4)$$

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

В державному стандарті контролю якості води [11] визначення T_m залежить від кількості споживачів джерела води – можливих негативних наслідків – постраждалих, тобто значень ризику у неявному виді. Чим більша кількість потенційних споживачів (постраждалих – U_b), тобто більше значення ризику, тим частіше мають бути перевірки. У граничному випадку ($U_b > 500000$) – щоденно. Інтервал перевірок визначено директивним методом. На нашу думку, вимоги щодо його дотримання не виконують з причин дуже великих витрат на їх здійснення. Також не виконується й максимальний інтервал – 1 місяць для джерел, де мала кількість споживачів ($U_b < 12$) – сільський колодязь. З досвіду відомо, що в останньому випадку перевірки проводяться на вимогу або на прохання споживачів. Цей приклад корисний з погляду на можливість виконання вимог моніторингу: завищенні вимоги призводять до зворотного ефекту втрати контролю. Як приклад, пропонуємо розглянути СМБ, створену у ядерній галузі, де основні принципи СМБ, його програмно-технічного комплексу (ПТК) вже впроваджені. Ці принципи прописані також у чинній загальній нормативно-технічній документації (НТД) [4]. Основні з них:

уніфікація технічного та програмного забезпечення;

об'єднання інформаційних підсистем даних окремих напрямів моніторингу для комплексної оцінки інформації;

впровадження єдиних уніфікованих форм надання і збереження даних та інформації, створеної на їх основі;

відкритість інформаційних систем для широкого загалу користувачів.

Отже, ПТК має складатися з таких підсистем: збору даних, комунікаційного забезпечення, первинної обробки даних та аналітичної роботи з інформацією, картографічного відображення інформації, представлення інформації операторам та особам, що приймають рішення (ОПР), ведення та обслуговування баз даних (БД), системи оповіщення тощо. У такому виді СМБ дійсно стає основою запобігання НС [3], рис. 1.

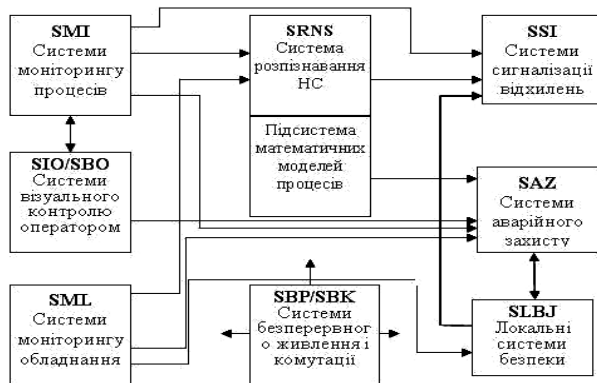


Рис. 1. Системи моніторингу у складі системи запобігання НС

Як бачимо, системи внутрішнього моніторингу (лівий стовпчик) є початком усіх процесів запобігання НС. Зрозуміло, що складність систем має бути залежною від рівня небезпечності об'єктів.

5. **Рівні моніторингу.** Як доведено у недавніх наукових дослідженнях [3, 10], СМБ має бути тривірневою, відповідно до системи управління. Отже, у зв'язку зі зміною системи управління безпекою [5], створення сучасної СМБ – це актуальна задача, яка не має достатньої наукової підтримки. Деякі пропозиції, навіть такі, що виходять від науковців, мають або загальний або футуристичний характер, не враховують реальні обставини та можливості держави. Найбільш реальна пропозиція СМБ [3] представлена на рис. 2, хоча вона була розроблена для моніторингу пожежної безпеки. На нашу думку, це вірно й для загальних параметрів безпеки, техногенної безпеки тощо. СМБ містить три рівні, які у структурі системи реалізовані у вигляді страт. Кожна страта об'єднує моделі об'єктів моніторингу певного рівня. На вхід мікрострати подається множина X показників стану безпеки об'єктів моніторингу, зокрема, характеристики причин (буде надійно працювати за умови об'єктивної (правдивої) інформації, що надходить). На вхід макрострати подається множина Y показників, які потрібні для управління цього рівня. На вхід метастрати подається множина Z показників впливовості факторів, що характеризуються показниками X . Елементами кожної страти є моделі, за допомогою яких множина вхідних показників відображається на множину вихідних показників цих страт. У такому виді СМБ дійсно стає основою запобігання НС [3],

рис. 1. Особа, яка приймає рішення (ОПР), має можливість завчасно приймати рішення на основі повної інформації про об'єкти, що спостерігаються.

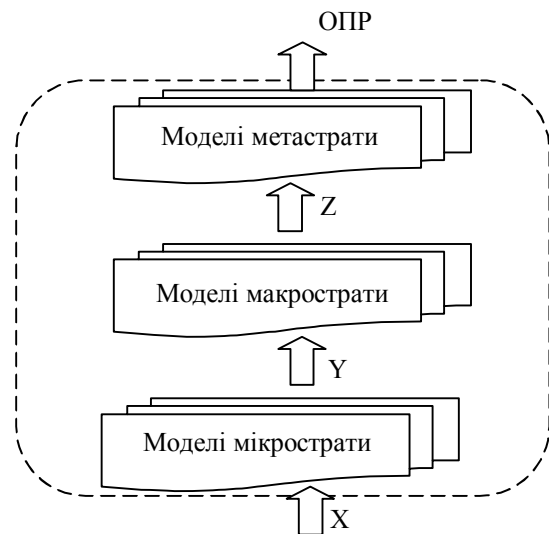


Рис. 2. Функціональна схема тривірневого перетворення інформації моніторингу

Майже за таким принципом, тільки в більш спрощеному (не автоматизованому) виді в державі уже діють деякі системи моніторингу. Так, у національній доповіді [1] описані державна система моніторингу довкілля (ДСМД) та національна система протиепідемічного нагляду, що діють на основі відповідних урядових рішень. Описані також результати аналізу стану довкілля, водних ресурсів, ґрунту, які перевірялися державною санітарно-епідеміологічною службою (СЕС). Оскільки останні системи (ДСМД і СЕС) відносяться до систем з повільно змінними процесами, результати роботи систем можуть використовуватися й для виконання функції «запобігання». Зрозуміло, що ці системи працюють у «ручному» режимі, але в Україні існують і автоматизовані системи. Це, в першу чергу, автоматизована система контролю радіаційної обстановки (АСКРО) навколо АЕС, хоча в підрозділах СЕС і є система радіологічного контролю [1]. Звісно, система АСКРО є найбільш інформаційно модернізованою, відповідає сучасним світовим вимогам до таких систем. Інформація про стан радіаційного забруднення в зоні АЕС контролюється автоматично у постійному режимі, проходить безперервну обробку та автоматично передається на більш високі рівні, аж до ОПР. З 2004 р. в Україні активно проводиться також робота по впровадженню на ПНО систем раннього виявлення (СРВ) НС, які повинні працювати в автоматичному режимі. Однак ця робота гальмується з причин, на наш погляд, недостатньої методичної і теоретичної підготовки. Як вже йшлося, функції моніторингу Φ залежать від типу об'єкта та вектора $[X_i]$ вхідних параметрів, число параметрів і має бути мінімальним, крім того, мають бути чітко визначені моделі відповідних страт: M_1 , M_2 , M_3 (рис. 2). Для кожного типу ПНО має бути визначений відповідно рис. 2 алгоритм перетворень інформації за схемою:

$$X \rightarrow M1 \rightarrow Y \rightarrow M2 \rightarrow Z \rightarrow M3 \rightarrow \text{ОПР}. \quad (5)$$

Мають бути визначені не тільки моделі $M1$, $M2$, $M3$, але й вектори інформації усіх рівнів, для чого потрібно визначитися з критеріями безпеки на кожному рівні.

6. **Критерій безпеки.** При оцінці рівня техногенної та природної безпеки держави необхідно враховувати багато критеріїв потенційної небезпеки територій, індивідуальний ризик смертності, критерій матеріального захисту від НС, кожен з яких, у свою чергу, враховує цілий ряд інших критеріїв. Наприклад у стандарті [11] якість води перевіряється майже сотнею параметрів (індикаторів). Але існують і комплексні параметри $Q(X)$, які є якоюсь комбінацією окремих індикаторів. Якщо будь-який індикатор X_i перевищує встановлені норми, вода вважається небезпечною для здоров'я або обмеженою для використання, тобто у загальному виді маємо такий критерій якості (безпеки):

$$Q(X) \leq [Q(X)], \quad X_i \leq [X_i], \quad (6)$$

де у правих частинах нерівностей мають бути допустимі рівні критеріїв безпеки на загальний параметр Q та окремі індикатори X_i . Зрозуміло, що кількість критеріїв має бути обмеженою. До речі, хоча в даному випадку мова йде про критерій якості, ми отожднюємо цей критерій з критерієм безпеки, що зрозуміло на інтуїтивному рівні: споживання неякісної води призводить або може призвести до небажаних проблем зі здоров'ям. Отже, порівнюючи рівняння (6) і (3), які тотожні, можна зробити висновок стосовно загальної будови критеріїв безпеки.

Отже, загальні та інформаційні вимоги до критеріїв повинні бути такими:

- чітко визначений зв'язок з безпекою;
- обґрунтовано ступінь достовірності і природності в якості індикатора безпеки;
- визначено вплив на загальний критерій безпеки (ризик) окремих індикаторів;
- знайдено залежність (функція) зведення окремих індикаторів до загального критерію.

Оскільки загальний критерій – ризик R стає параметром моніторингу, інформація про його визначення має бути в моделях перетворення (5) у виді функціональної залежності за формулою (1). Визначення поточного значення R на основі імовірнісного моделювання для складних систем описано у [9], отже це пряма задача. Для визначення критеріїв безпеки нижчого рангу потрібне рішення рівняння (2) відносно X_i , тобто розв'язування зворотної задачі, враховуючи наведені вимоги. Алгоритм цього рішення можливо навести для загального випадку лише у символічному виді. Розглянемо приклад параметрів безпеки АЗС. До параметрів безпеки відносимо параметри ідентифікації: загальну кількість нафтопродуктів X_1 , їх розташування у ємностях X_2 , умови зберігання X_3 , відстані до об'єктів турботи X_4 , навченість персоналу X_5 та ін. Усі індикатори X_i , у свою чергу, складаються з більш конкретних параметрів. Напри-

клад, якщо на АЗС є п'ять ємностей то ми повинні контролювати X_3 для кожної з п'яти ємностей. Крім того, само поняття «УМОВИ – X_3 » теж складне, воно містить декілька параметрів: підземне – наземне розташування (суттєво впливає на ризик R), тип ємностей (об'єм, матеріал та рік виготовлення, тип проекту та ін.), наявність запобіжних пристроїв та інші особливості, які добре відомі професіоналам галузі. Отже, неможливо контролювати усі умови та параметри X_i під час моніторингу. Очевидно, потрібно шукати параметри безпеки більш високого рівня навіть на рівні нижчої страти. Можна запропонувати, наприклад, концентрацію C_i парів нафтопродуктів у повітрі біля кожної ємності та на заправних майданчиках авто. Цей параметр C_i дійсно вказує на небезпеку виникнення вибуху чи пожежі при негерметичності обладнання чи розливу пального. Але якщо розлив відбувся, концентрація C_i наростає дуже швидко, часу на прийняття рішень, особливо літом, не вистачить. Тобто, якщо обрати параметром моніторингу безпеки швидко змінний параметр C_i , то потрібно бути робити і швидкодіючу систему автоматичного захисту, наприклад, систему пожежогасіння. З цього прикладу стає зрозумілим, що визначення критеріїв безпеки має відбуватися на основі моделювання ризику та підтверджуватися досвідом фахівців [9]. Очевидно, критерії безпеки з точки зору запобігання НС мають бути більше «попереджувальними», концентрувати увагу ОПР задовго до виникнення навіть розливів (подія U_1), тому що й причини розливів виникають з невиконання деяких вимог з безпеки X_k . Отже, якщо масив $[U]$ визначає можливі наслідки аварійних станів, що можуть статися, то саме моделювання події U_1 – проливу дасть відповідь про параметри безпеки X_i , що впливають на появу цієї події і, найбільш важливі з них за критерієм важливості (Бірінбаума чи Фусели-Весели) можуть бути обрані як критерії безпеки для СМБ. Як висновок, критерії безпеки мають визначатися розрахунком, який погоджується з досвідом.

Другий приклад раціонального визначення критерію безпеки також візьмемо з АЕС [12]. Мова про викиди радіоактивних речовин при роботі на потужності, які контролюються постійно так званою системою АСКРО та іншими системами безпеки.

Допустимий газоаерозольний викид Запорізької АЕС встановлено таким чином, щоб забезпечити неперевищення квоти ліміту дози (40 мкЗв/рік) для населення на межі санітарно-захисної зони за рахунок усіх шляхів формування дози з урахуванням місцевих метеорологічних параметрів. Величина допустимого викиду не залежить від кількості енергоблоків, які знаходяться в експлуатації. Величину допустимого викиду не буде перевищено, якщо виконуються обидві з таких нерівностей:

$$a - \sum_{i=1}^3 \frac{B_i}{PB_i} \leq 1; \quad b - \sum_{i=2}^{16} \frac{\bar{B}_i}{PB_i} \leq 1 \quad (7)$$

де B_i – фактичний добовий викид i -го радіонукліда (групи радіонуклідів, нормованої як один вид забру-

днення); \bar{B}_i – середній мза календарний місяць добовий викид i -го радіонукліда (групи радіонуклідів); PB_i – допустима границя (*предел – рос.*) викиду i -го радіонукліда (групи радіонуклідів).

Невиконання хоча б однієї з нерівностей (7) означає перевищення величини допустимого викиду.

Підсумовування у формулі (7а) здійснюється за трьома групами радіонуклідів: ДЖН – довгоживучі нукліди, ІРГ – інертні радіоактивні гази і радіойод (перші три рядки таблиці).

Підсумовування у формулі (7б) здійснюється за п'ятнадцятьма радіонуклідами (групам радіонуклідів), наведеними в окремій таблиці (від інертних радіоактивних газів (ІРГ), ізотопів металів – продуктів розпаду ядерного палива до ^3H (тритію); з підсумовування виключаються ДЖН. Структура критерію безпеки у виді нерівностей (7) використовується дуже часто, майже в усіх випадках впливу однотипних небезпечних факторів. До речі, за всі роки експлуатації ЗАЕС не було випадків перевищення допустимих викидів, звичайно, реальні викиди складають декілька відсотків допустимих викидів.

З наведених прикладів зробимо висновки, які характеризують критерії безпеки: КБ мають бути всебічно обґрунтовані та офіційно затверджені. КБ повинні періодично переглядатися з метою врахування новітніх досліджень та міжнародних рекомендацій. Завищені вимоги, або ще гірше, неправильна структура КБ може призвести до надмірних, необґрунтованих мір захисту (витрат підприємств), з другого боку занижені критерії безпеки призводять до професійних захворювань та ін.

Отже, локальні системи безпеки $K1$ і $K2$ повинні давати сигнал про відхилення індивідуальних параметрів небезпечних технологій $[X_i]$ та можливі зміни комплексного параметра. Системи $K1$ і $K2$ відповідно до сучасних уявлень відносяться до I рівня мікрострати, мають бути визначені ПБ, що передаються на верхні рівні.

7. **Алгоритм аналізу інформації.** Вже йшлося про моделі $M1$, $M2$, $M3$ перетворення інформації (5), саме в цих моделях і працюють алгоритми аналізу (перетворення) інформації. Основне завдання аналізу – розпізнавання аварійної ситуації, яка може призвести до НС. За результатом аналізу визначається ступінь наближення критерію безпеки до допустимого рівня (6). Мають бути задані заздалегідь діапазони наближення та їх ознаки до повідомлень. Звернемося до досвіду АЕС. Для параметрів, що контролюються напряму, наприклад, рівень теплоносія у парогенераторах $H_{\text{ПГ}}$ установлюється проектом (на основі модельних розрахунків) уставки попереджувальної (ПС) і аварійної сигналізації (АС): $H_{\text{ПГ}}(\text{ПС}) = H1$ та $H_{\text{ПГ}}(\text{АС}) = H2$, звідси $H1 > H2$. Тобто, якщо з деяких причин рівень теплоносія знижується (дуже небезпечна подія!), то спрацює попереджувальна сигналізація, оператор з'ясує причини події та приймає рішення щодо подальших дій (на АЕС впроваджені

автоматичні порадики, дають підказку, але оператор рішення приймає сам). Але якщо спрацює аварійна сигналізація, спрацює і автоматичний захист і АС, тобто в залежності від **важливості** критерію безпеки і його поточного значення алгоритм аналізу безпеки визначає **повідомлення про небезпеку**. На переконання авторів, зразком аналізу інформації та автоматизованого захисту є система моніторингу і запобігання НС в галузі атомної енергетики Франції. Це може бути прийнято за еталон при створенні єдиної системи моніторингу та прогнозування розвитку НС в державі, їх попередження завдяки управлінню ризиками.

8. Виведення повідомлень на різних рівнях.

Мета цього кроку моніторингу – своєчасне попередження при загрозах персоналу, ОПР тощо, а також проживаючого населення про можливу небезпеку. Мають бути варіанти в залежності від рівня управління та страти моніторингу. По-перше, не всі відхилення критеріїв безпеки ΔX_i мають проходити на більш високі рівні (страти). Так, у вищенаведеному прикладі про зниження рівня теплоносія в парогенераторі рішення приймає оператор, і населенню, та навіть керівництву АЕС, зовсім не потрібно про це знати. Але якщо при цьому спрацював аварійний захист з остановом реактора, маємо наслідки для АЕС – принаймні зменшення прибутку, та можливі наслідки для населення, якщо аварійна ситуація отримала подальшого розвитку.

Найбільш універсальним форматом виведення повідомлень у сучасному світі є кольорова гама: червоний, жовтий, зелений, білий колір відповідно до рівня загрози (ризик): високий, помірний, низький, знехтуваний ризик [13]. Це стосовно верхніх страт, на мікростраті оператору краще прямо вказувати відхилення критерію безпеки ΔX_i та надавати підказку про подальші дії. Зауважимо, що всі аварійні ситуації та дії з їх безпечного припинення мають бути проаналізовані у ПЛАСах та деклараціях з безпеки, тому у всіх випадках виведення повідомлень маємо суто інформаційну задачу, рішення якої залежить від софту об'єкта.

9. **Прогнозування стану об'єкта та можливого розвитку ситуацій – основна задача моніторингу безпеки НС.** Звичайно [1, 8], фахівці з безпеки ставлять функції моніторингу і прогнозування поряд, але це не зовсім так. Звернемося до прикладу збільшення рівня теплоносія в парогенераторах АЕС. Оператору важливо знати саме факт події, що відбулася та алгоритм своїх подальших дій. Але якщо подія розвивається до рівня НС, наприклад, великий пролив хімічно небезпечної речовини (ХНР), то у такому випадку потрібні моделі прогнозування розповсюдження небезпечних концентрацій ХНР в залежності від умов навколишнього середовища, погодних умов тощо. Тобто функції прогнозування важливі щодо прийняття рішень після того, як НС сталася. Для виконання цієї функції система повинна мати моделі розвитку НС та технічні засоби попередження населення [9].

Інша мова про моніторинг поточного стану безпеки в умовах НС. Тут більш доречно, на наш погляд, термінологія «розвідка ситуації», тому що у такому випадку ставиться мета дослідження уже зараженої території. Оскільки кількість небезпечних об'єктів дуже велика, забезпечення автоматизованого збору даних фактично з усієї території неможливе через великі затрати. Повинні бути декілька мобільних лабораторій у регіональних центрах, ця вимога фактично виконана, такі лабораторії вже існують.

10. **Ведення бази даних (БД) і бази знань (БЗ).** Інформація з НС має зберігатися та використовуватися на усіх рівнях управління у БД та БЗ. Але, відповідно до діючих в Україні відомчих наказів різних сфер безпеки, порушення технологічних процесів на потенційно небезпечних об'єктах (ПНО) взагалі не визначаються, а НС розслідуються недостатньо повно (без з'ясування кореневих причин). Частіше в існуючих БД усіх відомств коренева причина взагалі не вказана. Чинна методологія аналізу НС і НВ, а також їх причин, не відповідають нагальним потребам безпеки і міжнародним стандартам. Це також було доведено міжнародними експертами за програмою PPRD у 2013 році. Проаналізовано рівень автоматизованої підтримки в Україні процесів моніторингу та аналізу НС у різних сферах безпеки. З'ясовано, що в сучасних технологіях автоматизована підтримка обмежена задачами збирання та елементарної обробки первинної інформації, причому усі дані розташовані у відомчих БД, які не завжди узгоджуються між собою, не існує процедур перевірки їх відповідності. БД, що є у різних галузях, як правило, закриті не тільки від «широкого загалу користувачів», а й від інформаційних систем інших галузей. При цьому події, що кваліфікуються як НС, відображені у різних БД недостатньо, без висвітлення та аналізу корінних причин та з суттєвими помилками щодо їх класифікації [15]. Це робить наявну інформацію майже непридатною для управління безпекою в державі. Тому має бути визначено не тільки перелік параметрів БД, що передаються на різних рівнях, моделі розрахунків узагальнених параметрів безпеки, як того вимагає технологія РОП, але й хто і яким чином надає інформацію, за чий кошти саме створюються СМБ та її елементи, враховуючи умови приватної власності

Потрібно удосконалювати, змінювати чинні класифікатори НС та НВ і, відповідно, БД. Пропонуємо розробити нові методи аналізу причин НС та НВ на основі нових інформаційних технологій та існуючих БД, адже завжди потрібно з'ясовувати кореневі причини і розробляти дієві та ефективні заходи щодо запобігання повторного їх прояву за методикою ASSET. За основу нововведень можуть бути взяті аналогічні технології ядерної галузі, де світовий досвід впроваджено з середини 90-х років. Усі БД з НС та НВ, пожежної безпеки та інших відомств з безпеки потрібно об'єднати в одну національну БД з безпеки (НБДБ). На відміну від існуючих, НБДБ

повинна мати більш повну інформацію з НС і НВ, кореневі та безпосередні причини небажаних подій і коригуючі заходи на причини тощо. Ця оновлена НБДБ повинна відповідати кращій світовій практиці, мати достатнє інформаційне навантаження, задовольняти усі сфери безпеки та галузі виробництва.

11. **Концепція системи.** Як вже йшлося, у тому чи іншому виді СМБ існує у кожній галузі виробництва: існують методики визначення показників безпеки, регламенти перевірок, визначені (нормовані) припустимі рівні майже усіх небезпек. Але як вже було сказано, процеси моніторингу слабо інформатизовані, частіше проводяться у «ручному» режимі, загальний показник безпеки не визначається, не моделюються процеси виникнення небезпек. Це, у свою чергу, не дозволяє розробити заходів щодо запобігання ризиків на їх ранньому етапі виникнення. Проблема створення сучасної СМБ в Україні є в тому, щоб об'єднати існуюче наукове напрацювання на основі сучасної парадигми ризик-орієнтованого підходу (РОП) [5] та інформаційних технологій, *визначатися з основними функціями і задачами СМБ* в різних галузях і сферах безпеки саме з інформаційної точки зору. Це перше і головне, *розробка критеріїв безпеки* для окремого об'єкта і галузі в цілому – це друга важлива задача і етап створення СМБ. Пропонується напрацювання, що є в галузях, використати як цеглинки для створення сучасної СМБ, що дасть змогу пройти з прискоренням алгоритм її розробки – це третій основоположний принцип концепції. Перелік підсистем СМБ можна знайти в багатьох працях, але, як правило, вони обмежуються наведеними вище загальними принципами [4], які повторюються у різних сферах безпеки за галузевими принципами. Тому підсистеми СМБ мають бути типовими для об'єктів галузі відповідно рис. 1 за попереднє визначеними *критеріями безпеки* – це наступні принципи концепції. Не існує цілісної СМБ, яка могла б стати основою для прийняття рішень на державному, регіональному та об'єктовому рівнях. За раніше наведеними прикладами [4, 11, 12] має бути розроблений *регламент функціонування системи*, який буде відповідати чинному законодавству та сучасним ІТ. Такі принципи створення страти першого рівня. Наступні страти повинні створюватися на основі сучасних *ситуаційних центрів* та систем підтримки прийняття рішень (СППР) [2] на їх основі. Тут мають бути певний перелік математичних моделей, відповідне програмне забезпечення з сучасним доступним для розуміння інтерфейсом [16].

Висновки

В умовах економічної кризи та одночасного зростання рівня безпеки розбудова єдиної державної системи моніторингу та прогнозування можливих НС має визначатися як пріоритетний напрям фінансування державою через ДСНС.

Центральним постійно діючим органом управління має стати центр моніторингу та прогнозування

НС (ситуаційний центр ДСНС), утворення якого передбачено Загальнодержавною цільовою програмою захисту населення і територій від НС техногенного та природного характеру на 2013 – 2017 рр. [1], яке так і не розпочалося за браком коштів.

Система моніторингу безпеки європейського рівня, яку необхідно створити в Україні найближчим часом, має відповідати сучасним принципам інформаційного забезпечення системи державного рівня, бути єдиною для усіх сфер безпеки та об'єднувати існуючі інформаційні та технічні ресурси різних галузей. Розробка та впровадження такої системи – це складна задача професіоналів в галузі з інформаційних технологій та фахівців ДСНС.

З цією метою потрібно найближчим часом підготувати для подання на розгляд Верховної Ради доповнення до Кодексу ЦЗ щодо створення СМБ та направити до Кабінету Міністрів України доповнення до ПКМ №11 від 09.01.2014. В цих доповненнях конкретизувати організаційну структуру, склад критеріїв безпеки, склад та порядок функціонування механізмів усіх ланок СМБ у системі ДСНС, вимоги завдання і відповідальність усіх суб'єктів діяльності СМБ.

Список літератури

1. Стан техногенної та природної безпеки в Україні в 2015 році. Звіт МНС та НАН. [Електрон./ресурс]. – Режим доступу: http://www.mns.gov.ua/content/national_lecture.html.
2. Ситуаційні центри. Теорія і практика. НАН України. – ІПММС. – К., 2009. – 347 с.
3. Гречанинов В.Ф. Інформаційні технології аналізу стану техногенної безпеки та планування протидії надзвичайним ситуаціям: автореф. дис. на здобуття наукового ступеня кандидата техн. наук: 05.13.06 / В.Ф. Гречанинов. – К., 2014. – 22 с.
4. РД 211.0.8.107-05 Методичні рекомендації з питань створення систем моніторингу довкілля регіонального рівня, затверджені наказом Міністерства охорони навколишнього природного середовища України від 16.12.2005 N 467.
5. Про схвалення «Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та при-

родного характеру» // Розпорядження КМ України від 22 січня 2014 р. № 37-р. – К., 2014.

6. Программа предотвращения, готовности и реагирования на техногенные и природные катастрофы, финансируемая ЕС в Восточном регионе ENPI (PPRD-East). Политика оценки рисков / угроз для восточного региона (ENPI). – Брюссель, 2012. – 72 с.

7. Інструкція щодо вимог пожежної безпеки під час проектування автозаправних станцій. Затверджено Наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи 06.12.2005 N 376.

8. Кодекс цивільного захисту України. Законодавство України [Електронний ресурс]. – Режим доступу до ресурсу: <http://zakon1.rada.gov.ua/laws/show/5403-17>.

9. Бегун В.В. Решение задачи определения текущего уровня риска (мониторинга) с применением алгоритмов МГУА / В.В. Бегун, В.В. Литвинов Моделирование-2012. ИПМЕ им. Г.Е. Пухова. – К., 2012. – С. 92-97.

10. Голуб С.В. Методология створення автоматизованих систем багаторівневого соціоекологічного моніторингу: автореф. дис. на здобуття наук. ступеня д-ра техн. наук: 05.13.06 / С.В. Голуб. – К., 2008. – 35 с.

11. ДСанПіНом 2.2.4-171-10 «Гігієнічні вимоги до води питної, призначеної для споживання людиною».

12. Регламент радиационного контроля при эксплуатации объектов ОП Запорожская АЭС. – 00.РБ.ХҚ.Р.2.01.А. – 2010 – 267 с.

13. СТП 0.41.066-2006. Системы оценки уровня эксплуатационной безопасности и технического состояния АЭС с ВВЭР. ГП НАЭК «Энергоатом». – К., 2006.

14. Воробієнко П.П. Системи оповіщення цивільного захисту: навчальний посібник / П.П. Воробієнко, С.І. Белюсов. – Одеса: ОНАС ім. О.С. Попова, 2012. – 76 с.

15. Гречанинов В.Ф. Функції управління і нагляду в ризик-орієнтованому підході до управління безпекою / В.Ф. Гречанинов, В.В. Бегун // Математичні машини і системи. – К.: ІПММС, 2014. – №1. – С. 159-170.

16. Актуальні проблеми моделювання ризиків і загроз критичних інфраструктур / В.Ф. Гречанинов, В.В. Бегун, В.П. Клименко, О.П. Яцук // Науковий вісник Укр.НДІПБ. – 2015. – №1(31). – С. 125-134.

Надійшла до редколегії 3.09.2015

Рецензент: д-р фіз.-мат. наук, проф. В.П. Клименко, Інститут проблем математичних машин та систем НАН України, Київ.

СОЗДАНИЕ СОВРЕМЕННОЙ СИСТЕМЫ МОНИТОРИНГА БЕЗОПАСНОСТИ – АКТУАЛЬНАЯ ГОСУДАРСТВЕННАЯ И НАУЧНАЯ ЗАДАЧА

П.П. Кропотов, В.В. Бегун, В.Ф. Гречанинов

Рассмотрены состояние и проблемы системы мониторинга безопасности в Украине, ее отличия от систем развитых стран. Анализируются функции в зависимости от целей, сам процесс мониторинга рассматривается как составляющая информационной безопасности. Предложено создание трехуровневой системы мониторинга. Рассмотрены строение критериев безопасности на принципах рискориентированного подхода, алгоритмы анализа информации, концепция новой системы, вопросы ведения базы данных и базы знаний по вопросам безопасности.

Ключевые слова: безопасность, мониторинг, риск, модель, интерфейс, алгоритм.

DEVELOPMENT OF MODERN SYSTEM FOR SECURITY MONITORING IS URGENT STATE TASK

P.P. Kropotov, V.V. Begun, V.F. Grechaninov

The article considers the state of the security monitoring (SM) system, its problems, and differences of SM system in Ukraine from SM systems in developed countries. The functions of the SM system are analysed in dependence of the aims, while the monitoring process itself is considered as a part of information security technology. The creation of three-tier SM system is proposed. The structure of security criteria is considered basing on the principles of risk-oriented approach and on the analysis of algorithms. The concept of the new SM system is considered together with practical questions regarding the maintenance of database and knowledge base on the security issues.

Keywords: security, monitoring, risk, model, interface, algorithm.