

ФУНКЦІЇ УПРАВЛІННЯ І НАГЛЯДУ В РИЗИК-ОРІЄНТОВАНОМУ ПІДХОДІ ДО УПРАВЛІННЯ БЕЗПЕКОЮ

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

Анотація. У статті розглядаються сучасні проблеми регулювання безпеки в Україні. Описані функції управління й нагляду в управлінні безпекою в їх сучасному розумінні й ролі у процесах управління ризиками. Запропоновано нову стратегію і структуру державного нагляду на основі ризик-орієнтованого підходу. Оцінені ймовірності помилок контролю ризику за різними стратегіями державного контролю.

Ключові слова: безпека, ризик, потенційно небезпечний об'єкт, моніторинг безпеки, оцінка ризиків.

Аннотация. В статье рассматриваются современные проблемы регулирования безопасности в Украине. Описаны функции управления и надзора в управлении безопасностью в их современном понимании и роли в процессах управления рисками. Предложены новая стратегия и структура государственного надзора на основе риск-ориентированного подхода. Оценены вероятности ошибок контроля риска по разным стратегиям государственного контроля.

Ключевые слова: безопасность, риск, потенциально опасный объект, мониторинг безопасности, оценка рисков.

Abstract. The article deals with the modern problems of safety regulation in Ukraine. The functions of management and supervision of safety management in the modern sense and their role in the risk management process are described. A new strategy and structure of state supervision on the risk-based approach is suggested. The probabilities of risk control errors under different strategies of governmental regulation are estimated.

Keywords: safety, risk, potentially dangerous object, safety monitoring, risk assessment.

1. Вступ

Питання щодо функцій управління і нагляду техногенної безпеки залишається в Україні актуальним. Суть його формулюється просто: потрібно визначити міру втручання державних структур у діяльність потенційно небезпечних об'єктів (ПНО) на такому достатньому рівні, щоб уникнути небезпеки для персоналу, населення та довкілля, з одного боку, і при цьому, з іншого боку, не заважати працювати підприємству частими перевітками. Функції управління і нагляду мають бути й в середині організації (підприємства). За визначенням, функції управління і нагляду – це приведення в стан повного порядку управлінської діяльності в середині організації, планування, контроль і відстеження процесів, проблем, а також діяльність з підтримки цілей і стратегій організацій. Включає і функції з керування успішною діяльністю персоналу.

Функції управління і нагляду залежать від усіх організаційних факторів внутрішнього менеджменту, зовнішньої стратегії управління безпекою тощо.

2. Сучасна стратегія і структура управління безпекою

Сучасна стратегія й відповідна їй структура (рис. 1) в основі своїй мають єдиний метод управління безпекою, а саме: контроль виробництва різними державними інспекціями. Як стверджує бізнес [1], нині право на перевірку ПНО має майже сотня держструктур (76), більшість із них (44) має право зупинити роботу підприємства. Основна функція громадських рад з охорони праці й безпеки при держадміністраціях усіх рівнів – теж «перевірки стану безпеки». Вся ця армія державних інспекторів утримується, зрозуміло, за бюджетні

кошти, й бізнес теж втрачає великі кошти при перевірках (за оцінками Федерації роботодавців України більше 27 млрд грн). Але при цьому рівні ризику в усіх сферах життєдіяльності майже не зменшуються впродовж усього часу існування незалежної держави [2]. Цей факт свідчить про неефективність державних витрат, невідповідність стратегій державного контролю вимогам часу, принципово неправильну постановку задачі регулювання і контролю безпеки у сучасних умовах. Маємо протиріччя між заявленими цілями державних органів управління (запобігання небезпек) і фактичними діями з їх реалізації. Функцію «запобігання небезпек» можливо виконувати лише на основі сучасних інформаційних технологій управління ризиками та стратегії ризик-орієнтованого підходу (РОП).

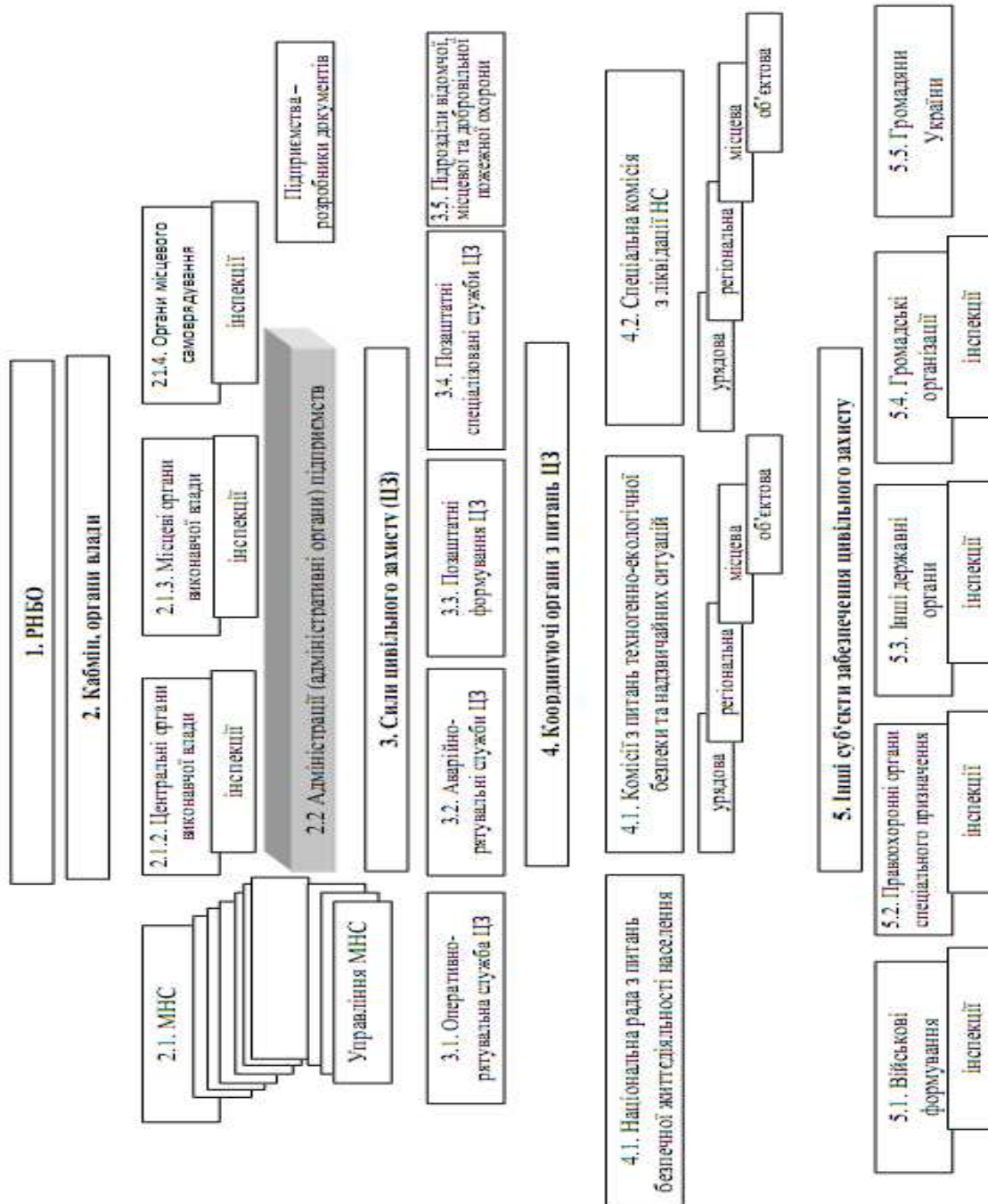


Рис. 1. Структура суб'єктів державного контролю безпеки

Сучасна структура суб'єктів цивільного захисту (ЦЗ), навіть у новому кодексі ЦЗ [3], відповідає початковій стадії розвитку безпеки. Вона розрахована (вибудована) з принципів загальнодержавної (соціалістичної) форми власності, яка панувала в недавньому минулому. Як бачимо з рис. 1, головною задачею всіх держструктур є інспекції, перевірки підприємств. У згаданому кодексі ЦЗ функція «запобігання» прописується як «моніторинг і контроль» «стану об'єкта», приватної власності в тому числі. Це і є тією оманю суспільства, на яку витрачаються народні кошти.

Маємо: всі суб'єкти державного контролю за безпекою утримуються за бюджетні кошти, але зобов'язані «наводити порядок» на приватному підприємстві. Це не відповідає принципам ринкового управління та існуючим міжнародним стандартам, а саме щодо власності – за безпеку повинен відповідати власник, а щодо методології, то головною повинна стати методологія запобігання небезпек на підприємстві. Це обов'язок власника. Усі процеси управління на підприємстві безпекою тощо мають здійснюватися за рахунок власника на добровільній основі, тому що за всі можливі наслідки він буде відповідати власними коштами – це перше й головне. По-друге, всім добре відомо, що стратегія «запобігання» дешевше стратегії «ліквідації» в десятки разів. Але наша сучасна реальність часто інша: прибуток отримує підприємство, а збитки, ліквідацію наслідків аварій, регреси сплачує держава. Отже, підприємця не цікавлять цінові стратегії управління безпекою, тому що цілі накопичення прибутку виконуються за рахунок бюджету та незахищеного персоналу.

За наведеною на рис. 1 структурою в принципі неможливо організувати державне управління безпекою на основі РОП – відсутні елементи системи, які можуть реалізувати нові алгоритми управління й контролю. Тобто усе сучасне управління відповідає першій, початковій стадії розвитку безпеки, де головними процедурами є інспекція та ліквідація наслідків аварій.

3. Структура органів управління ризиком у ринкових умовах

Мінімальна можлива структура органів управління ризиком представлена на рис. 2. Така структура в тій чи подібній формі існує в усіх розвинутих країнах. Як бачимо (рис. 2), присутність держави в управлінні безпекою може бути мінімальною. Якщо власник несе повну відповідальність за безпеку свого виробництва (ПНО або ОПН) за законом перед третіми особами, тоді він не допустить ні аварій, ні аварійних ситуацій. Такий власник дуже швидко знайде ті організації, які зможуть достовірно визначити ризик його підприємства та засоби його зниження. Тобто стратегії управління безпекою на основі РОП засновані на економічних методах.

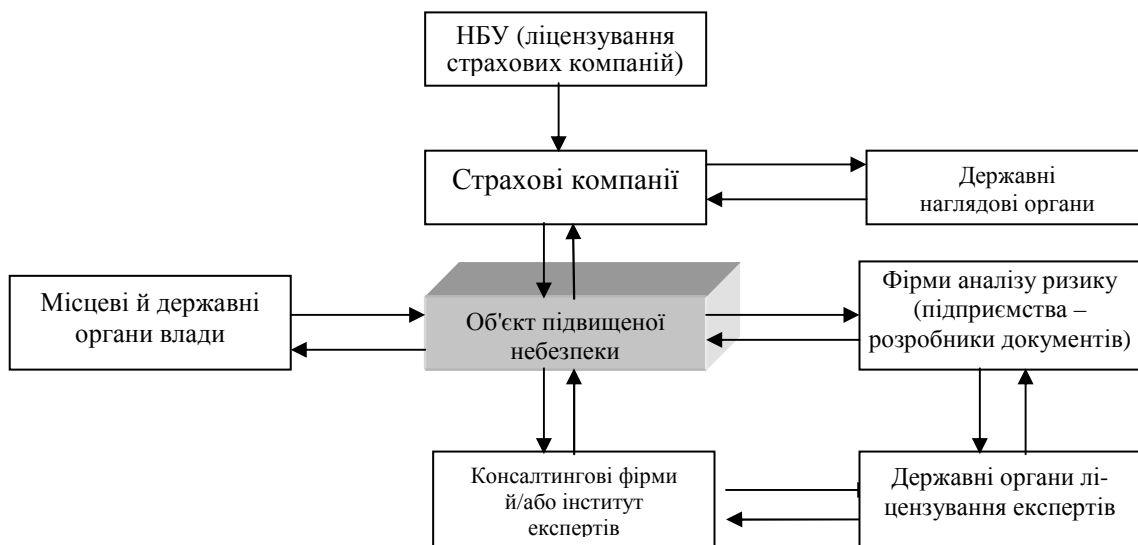


Рис. 2. Структура управління безпекою за умови відповідальності власника

Такий підхід призводить до значного зменшення державних витрат на безпеку й до підвищення ефективності управління. Управління безпекою стає однією із сфер загального менеджменту ПНО. Зовсім логічно й очевидно, що при належному рівні підготовки об'єкта та внутрішньому моніторингу наслідки аварійних процесів можуть бути істотно знижені, а в багатьох випадках попереджені. Тобто рівень безпеки визначає ступінь усвідомлення, передбачення, безперервної готовності до реагування. Це, у нашому випадку, стосується стаціонарних техногенних об'єктів підвищеної небезпеки й засобів транспортування небезпечних речовин.

Як бачимо (рис. 2), у структурі існують тільки два елементи, що знаходяться на утриманні бюджету: державні наглядові органи (суттєво зменшена кількість) та державні органи ліцензування експертів. Ці органи існують і у старій структурі, але тут їх функції й відповідно чисельність зменшуються в багато разів. Місцеві й державні органи влади контролюють лише ступінь ризику, який визначається спеціальними організаціями за кошти власника.

4. Загальний алгоритм управління ризиками підприємства на основі РОП

З інформаційної і математичної точки зору, керуючим впливом у стратегії РОП [4] є рішення про шляхи зниження ризику на основі аналізу ймовірнісної структурно-логічної моделі небезпечного підприємства та оцінок ризику. Оптимальний у сенсі мінімальних витрат алгоритм вибору рішення про зниження ризику наводиться на рис. 3.

Мету управління ризиком при здійсненні діяльності потенційно небезпечного об'єкта можна визначити як забезпечення безпеки персоналу, населення і навколишнього природного середовища шляхом встановлення і підтримки прийняттого рівня ризику при оптимальному використанні наявних ресурсів. Відповідно до законодавства України, «управління ризиками – це діяльність, пов'язана з ідентифікацією, аналізом ризиків і прийняттям рішень, спрямованих на мінімізацію негативних наслідків настання вихідних подій (явищ) і/чи зменшення ймовірності їхньої реалізації до прийнятних значень» [5].

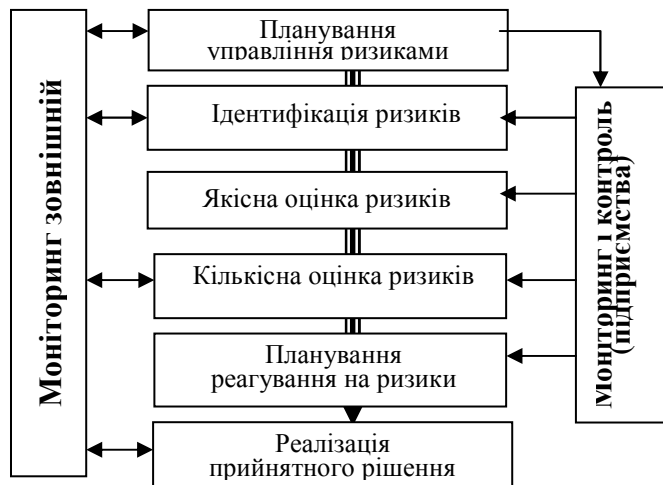


Рис. 3. Модель процесів управління ризиками

У загальному випадку процес управління ризиками при здійсненні діяльності на об'єкті включає виконання шести процедур та постійний моніторинг і контроль (рис. 3).

Планування управління ризиками – це процес прийняття рішень щодо застосування методології РОП для конкретної діяльності. Цей процес може містити в собі:

- створення спеціального підрозділу, відповідального за оцінку і управління ризиками;
- вибір методики оцінки ризиків;
- визначення джерел даних для ідентифікації ризику;

– визначення інтервалу часу для аналізу ситуації (аварії).

Дуже важливим є визначення припустимих (прийнятних) рівнів ризику, які визначаються на основі чинного законодавства.

Ідентифікація ризиків – етап, на якому визначається, які ризики можуть вплинути на діяльність, що розглядається. Характеристики цих ризиків повинні бути оформлені документально. Ідентифікацію ризиків слід проводити з певною періодичністю впродовж усього терміну діяльності об'єкта. Спеціалізований підрозділ має залучати до робіт з іден-

тифікації ризиків усіх причетних до життєвого циклу об'єкта: проєктантів, експлуатаційників, фахівців інших підрозділів, незалежних експертів тощо. Ідентифікація ризиків організовується як ітераційний процес. Перші розрахунки потенційного ризику виконують проєктанти. У процесі діяльності об'єкта, з урахуванням досвіду експлуатації, уточнюються дані щодо надійності систем і устаткування, процедур управління, помилок персоналу і робиться перерахунок ризиків для об'єкта. Для формування об'єктивної оцінки в завершальній стадії процесу оцінки можуть брати участь незалежні експерти.

Якісна оцінка ризиків – це етап якісного аналізу результатів ідентифікації, а також визначення подій, що вносять найбільший внесок у загальний ризик і які потребують вживання заходів щодо їх зниження.

Якісна оцінка визначає рівень ризику і важливість складових його подій. Доцільно створити банк даних ризиків усієї діяльності на об'єкті, заснований на систематизованих даних, у тому числі даних щодо впливу ризиків на персонал. На цьому етапі можливе визначення чинників найбільшого впливу, що створює передумови управління.

Кількісна оцінка ризиків визначає ймовірність виникнення небажаних подій і вплив їх наслідків на людину, об'єкт та довкілля. Наявність такої інформації допомагає приймати оптимальні рішення й уникати невизначеності в управлінні. Кількісна оцінка ризиків передбачає виконання попередніх процедур і є завершальним етапом задачі визначення ризиків. Важлива складова цього етапу – оцінка надійності систем об'єкта, яка передбачає визначення умов невиконання функцій систем у вигляді так званої множини мінімальних перерізів [6]. Справді, якщо відомо, які події найбільше впливають на ризик, то задача управління зводиться до того, щоб зменшити негативний вплив цих подій у найбільш оптимальний спосіб. Якщо це неможливо, тоді необхідно створювати спеціальні системи безпеки, призначенням яких є обмеження негативної дії небажаної події або припинення небезпечного процесу на певному проміжному етапі.

Планування реагування на ризики – це розробка методів і технологій зниження негативних наслідків ризиків. Якісне науково обґрунтоване планування можливе за умови виконання всіх попередніх етапів процесу відповідно до рис. 3. Стратегія планування має відповідати типам ризиків, їх величині і значимості, наявності ресурсів і тимчасових параметрів. У найбільш небезпечних випадках можна передбачати кілька варіантів реагування на ризики. Планування має здійснюватися у відповідності із спеціальною методикою, що враховує специфіку об'єкта, чинні правила й інструкції.

Реалізація прийнятого рішення здійснюється як заключний етап усієї роботи з управління ризиками на основі попереднього планування. Це можуть бути дії, які повинні бути виконані негайно або впродовж певного нетривалого терміну, чи довгострокові заходи, що потребують значних ресурсів. У деяких випадках імовірних загроз для населення реалізація прийнятого рішення контролюється державними наглядовими органами. У випадку, коли об'єкт створює загрозу, що перевищує прийняті рівні ризику, потрібно здійснювати заходи модернізації технологій або устаткування чи зовсім припиняти діяльність цього об'єкта.

Моніторинг і контроль (внутрішній) важливих для безпеки параметрів проводяться з метою перевірки дотримання вимог встановлених норм. Моніторинг і контроль мають здійснюватися спеціалізованим підрозділом об'єкта. При цьому постійно контролюється процес ідентифікації ризиків, виконання плану реагування на ризики, оцінка ефективності заходів для зниження ризиків, величина залишкового ризику і його прийнятність.

Якісний контроль виконання діяльності надає інформацію, що сприяє прийняттю ефективних рішень із запобігання нових ризиків чи пом'якшення наслідків. Контроль може ініціювати вибір альтернативних стратегій, прийняття коректив, перепланування проєкту для досягнення базового плану.

Зовнішній (державний) моніторинг має бути тільки за параметрами, важливими для безпеки регіону розташування ОПН, безпеки персоналу, населення та довкілля, а саме: чи планується управління ризиками на підприємстві, чи є кількісна оцінка ризиків та чи задовольняються при цьому умови прийнятного ризику, чи реалізуються сплановані заходи зменшення ризику тощо.

5. Функції управління і нагляду в управлінні безпекою на основі оцінок ризиків

Функції управління і нагляду, згідно з описаною методологією РОП, стають головними з точки зору безпеки в управлінні підприємством. Відбувається передача цих функцій від держави власнику підприємства. Але на сучасному перехідному етапі у сфері власності (господарювання) маємо неврегульоване протиріччя між застарілою системою моніторингу безпеки (стосується всіх контролюючих організацій) та сучасною теоретичною базою саморегулювання безпеки в ринкових умовах [4]. Як тимчасове рішення пропонуємо для визначення параметрів зовнішнього контролю використовувати документи з безпеки ПНО, які розробляються відповідно до закону [5] власником: декларації з безпеки та плани ліквідації аварійних ситуацій і аварій (ПЛАСи). Саме в цих документах оцінені значення ризику підприємства та засоби його зниження. Періодичність зовнішніх перевірок має визначатися на основі визначених у документах рівнів ризику відповідно до закону [7] та світового досвіду діапазонів припустимого ризику [2]. Якщо розрахунком визначено незначний ризик – $R \leq 1 \cdot 10^{-6}$, перевірки державних інспекцій усіх рівнів можуть бути не частіше одного разу на 5 років. В умовах середнього ризику (міжнародні норми припустимого ризику – $1 \cdot 10^{-6} \leq R \leq 5 \cdot 10^{-5}$) перевірки можуть бути не частіше одного разу на 3 роки. Й тільки якщо результатом розрахунку є високий (терпимий) ризик – $5 \cdot 10^{-5} \leq R \leq 5 \cdot 10^{-4}$, перевірки можуть бути 1 раз на рік. У випадку неприпустимого ризику – $R \geq 5 \cdot 10^{-4}$ за міжнародними нормами діяльність не рекомендується, підприємцю пропонується розробляти програму зниження ризику.

Таким чином, на основі кількісних розрахунків ризиків мають визначатися параметри внутрішнього і зовнішнього нагляду (моніторингу): перелік важливих для безпеки елементів системи (об'єкта) для контролю та частота контролю за умови прийнятних значень безпеки й ефективності виробництва. Така стратегія відповідає наведеним вище принципам РОП, світовому досвіду передових галузей і сфер безпеки, стає першим етапом дерегуляції. З часом мають бути розроблені більш докладні (ефективні) методики.

6. Якісні оцінки вигод переходу на нову концепцію

Економічні механізми регулювання безпеки дають можливість перекласти основний тягар функцій нагляду на саме власника ПНО, що, цілком природно, відповідає світовим принципам регулювання безпеки [8]. Управління безпекою стає частиною загального менеджменту підприємства. Ця функція має свої ресурси, які гармонійно входять у загальний бюджет. Актуальним стає перерозподіл відповідальності за безпеку, що відображається в посадових інструкціях усього персоналу. До речі, в концепції забезпечення 100% безпеки [4] державні інспектори оцінюють свою відповідальність як мінімум 50% на 50%, іноді навіть 90% на 10%. За концепцією РОП, має бути навпаки, а саме: інспекції – 10% на 90%, причому в цих 10% має бути більше співпраці, відношень спільної відповідальності, допомоги з боку інспектора відповідним службам підприємства.

Велике значення мають правильно організований облік, ведення державного кадастру прогнозованих і реальних збитків від надзвичайних ситуацій, публічна оцінка їх соціально-економічних наслідків – гласність. Така робота повинна проводитися спільно та у взаємодії з ЦОВ регіональними органами виконавчої влади. За таких умов на підвищення

ймовірності правильних дій персоналу має позитивне значення організаційного фактора «зовнішній вплив» [9].

За досвідом Росії [10] значна частина функцій управління і нагляду ЦОВ за новою концепцією перекладається на страхові компанії. Нормативна Умова страхування безпеки відповідно до ступеня ризику зобов'язує страхові компанії контролювати процеси безпеки. Оскільки мова йде про грошові активи, відповідальність їх моніторингу більша, ніж адміністративна відповідальність інспекторів. Помітну роль у рішенні завдань регулювання безпеки грає існуюча у країні система державних надзвичайних страхових фондів, що поєднує федеральний надзвичайний страховий фонд, страхові фонди суб'єктів Російської Федерації, органів місцевого самоврядування. Такі фонди акумулюють ресурси підприємств і організацій, вітчизняних і закордонних юридичних і фізичних осіб, у тому числі:

- плати у зв'язку з наслідками надзвичайних ситуацій;
- суми по позовах про відшкодування збитку й штрафів за правопорушення;
- кошти від реалізації зробленої на ПНО і конфіскованої продукції.

У країні здійснюється добровільне й обов'язкове державне страхування підприємств, установ і організацій, об'єктів їхньої власності й доходів, а також громадян, на випадок виникнення надзвичайних ситуацій природного або техногенного характеру. Кошти, що утворюються в результаті страхової діяльності, будуть використані на здійснення превентивних заходів і компенсацію збитку. Порядок страхування й перестраховування ризиків і використання засобів устанавлюється Урядом.

За умов нової концепції відроджується роль науки. Розробка й застосування зазначених та інших видів економічних механізмів у сполученні з можливостями, які впливають із вимог нової нормативно-правової системи, дозволяють ученим встановити й пропонувати до реалізації науково обґрунтовані комплексні програми забезпечення безпечного соціально-економічного розвитку об'єктів і територій. Тому результати наукових досліджень і системного аналізу небезпек у природно-техногенній сфері (ключове місце в соціально-економічному й політичному житті країни) впливають і будуть впливати на концептуальні підходи держави до проблем безпеки. Розробка й використання ймовірнісних моделей розвитку суспільства й основних виробничих процесів з урахуванням ризику виникнення природних і техногенних аварій і катастроф стає однією із головних умов забезпечення гарантованого рівня безпеки життєдіяльності й прийняттого ризику аварій і катастроф. При цьому враховуються не тільки радикальні й швидкі зміни, які прийнято вважати "винуватцями" виникнення аварій і катастроф, але й повільно наростаючі фактори, що загрожують у результаті якісного стрибка перейти в некеровану стадію з катастрофічно негативними наслідками для людини й природи.

7. Оцінки ймовірності помилок визначення ризику за різними стратегіями контролю

Стратегії контролю змінювалися разом з концепціями (філософією) безпеки [4]. Можливі такі стратегії контролю:

- Внутрішній контроль процесів на основі інструкцій у процесі виконання робіт та зовнішні часті інспекції – це перша стратегія контролю: \hat{S}_1 .

- Друга поширена сучасна стратегія: \hat{S}_2 – зовнішній (державний) контроль – експертні судження.

- Третя стратегія: \hat{S}_3 – контроль подій, що відбувається. Ця стратегія характерна для підприємств неперервного виробництва, енергетичної галузі тощо. Головна особливість цієї стратегії – висока надійність обладнання та 100% резервування обладнання й систем.

• Четверта стратегія: \hat{S}_4 – це стратегія контролю рівня культури безпеки. Вона відповідає III (вищій) стадії розвитку безпеки.

• П'ята стратегія: \hat{S}_5 – оцінки ризику ОПН (АЕС) на основі даних з надійності елементів систем об'єкта (розрахунки ймовірності НС) – стратегія РОП.

Алгоритм контролю на першій стадії розвитку безпеки. Алгоритм цього контролю прописаний у посадових інструкціях інспекторів усіх сфер контролю [11], де наведена також методика оцінки ефективності контролю. Схема алгоритму наведена на рис. 4. Оцінюємо ймовірність виявлення недоліків, важливих для безпеки, за цим алгоритмом. Як бачимо, результатом контролю можуть бути два варіанти: 1) ризик виявлено й усунуто за результатом к інспекції; 2) ризик не виявлено й він може створити певні проблеми, якщо це значимий ризик. Оскільки фактичний ризик R_x за цією стратегією взагалі не розраховується, оцінки мають експертний характер на якісному рівні (великий – середній – малий).

Ймовірність першого варіанта позначимо P_1 , другого P_2 ; ймовірність виявлення ризику інспекцією – P_6 ; ймовірність усунення ризику – P_y ; ймовірність того, що цей ризик значимий, – P_3 . Важливо знати ймовірність P_2 , так як вона залежить від усього ланцюга алгоритму. Якщо діяльність інспекцій ефективна, первинні ризики підприємства повинні зменшуватися.

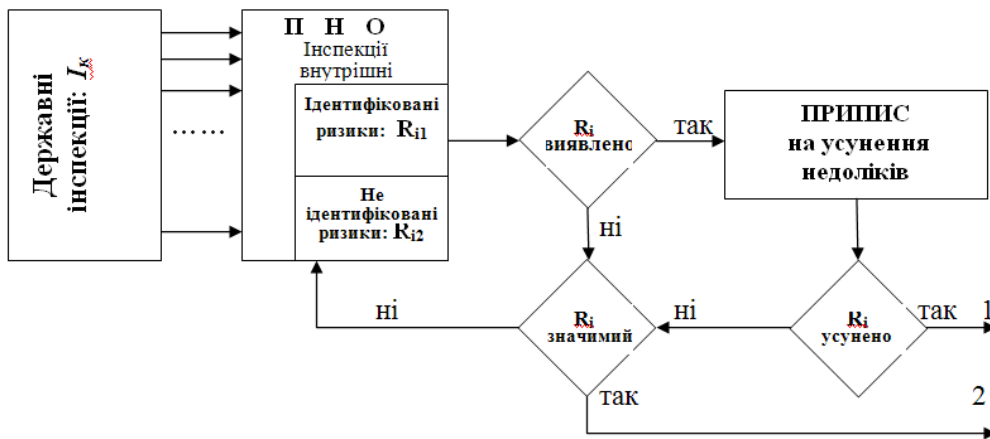


Рис. 4. Алгоритм процесів моніторингу за варіантом інспекцій

Очевидно:

$$P_1 = P_i P_{Ri} P_6 P_y, \quad (1)$$

де P_{Ri} – ймовірність ризику підприємства.

Ймовірність зменшеного ризику в цьому випадку:

$$\hat{P}_1 = P_{Ri} - P_i P_{Ri} P_6 P_y = P_{Ri} (1 - P_i P_6 P_y). \quad (2)$$

Варіант 2 можливий у двох випадках: якщо ризик не виявлено (2a) або не усунуто після припису (2b). Вважаючи події незалежними, маємо

$$P_2 = 1 - (1 - P_{2a})(1 - P_{2b}) = P_{2a} + P_{2b} - P_{2a} P_{2b}.$$

Оскільки $P_{2a} = P_i P_{Ri} P_6 (1 - P_y)$, $P_{2b} = P_i P_{Ri} (1 - P_6)$, отримуємо після спрощень:

$$P_2 = P_i P_{Ri} (1 - P_6 P_y - P_i P_{Ri} P_6 (1 - P_y)(1 - P_6)). \quad (3)$$

Із формул 2 і 3 бачимо, що ймовірність ризику після перевірки тим менше, чим успішнішими будуть дії виявлення й усунення ризиків, тобто ближче до одиниці будуть їх імовірності. У випадку рівності $(P_x, P_y) = 1$, отримуємо нульовий ризик. З досвіду [6] відомо, що $P_i \in (0,1;0,05)$, $P_{Ri} \in (1E-4;1E-6)$, звідки слідує, що $P_2 \in (1E-2; 1E-8)$ або, іншими словами, не перевищує 1%.

Як висновок, ефективність контролю за стратегією 1 дуже низка й не відповідає сучасності, чинним законам України тощо.

Зовнішній державний контроль – експертні судження стратегії \hat{S}_2

Ця чинна стратегія описана в [11]. Учасники процесу:

1. Особа, уповноважена за безпеку (відставний полковник), у складі підприємства.
2. Фірма-розробник документів з безпеки: повідомлення про ідентифікацію, ПЛАСу, (декларації) – це окреме підприємство (не має сертифікатів відповідності).
3. Інспектор МНС – капітан ЦЗ, який не має спеціальної освіти в галузі нових методик визначень ризику.
4. Посадовці МНС більш високого рангу мають право зупинити роботу, якщо складено припис про порушення безпеки.

Розрахунок імовірності виявлення ризику за стратегією \hat{S}_2 . Введемо додаткові позначення:

$R_{дон}$ – нормативний рівень ризику;

$R_{док}$ – рівень ризику, що визначено в документах з безпеки;

$R_{ф}$ – фактичний рівень ризику на ПНО;

R_i – рівень ризику, що констатує інспектор під час перевірки.

Звичайно, рівень ризику, задекларований підприємством, відповідає загальним вимогам $R_{док} < R_{дон}$. Але $R_{ф}$, скоріше за все, перевищує задеклароване значення. Це обумовлено умовами сьогодення в державі: відсутність верифікованих програм, сертифікованих фахівців, високий рівень корупції та ін. Оцінимо ймовірність виявлення ризику за таких умов за стратегією \hat{S}_2 .

Отже, як було визначено в [4], на поточне значення R_x впливає можлива відмова n – елементів об'єкта, k – зовнішніх факторів, i – обставин, разом N елементів моделі. В умовах, що визначено, фактори, обставини й елементи об'єкта, які суттєво впливають на ризик, не визначені (не визначена важливість для безпеки [6]), тобто інспектор може визначити їх випадково тільки на основі неповних знань об'єкта, процесів та технологій. Ймовірність правильного їх визначення інспектором дуже мала, інспектор не в змозі вивчити техпроцеси за час перевірки. Інспектор відповідає за безпеку лише в дисциплінарному полі, він не пов'язаний з процесами об'єкта. Таких об'єктів перевірки в нього декілька десятків чи навіть тисяч. У цих умовах мета дій інспектора – визначення декілька k_j зауважень. Він не має ні мотивів серйозної перевірки, ні програмних та інструментальних засобів. З досвіду відомо, що значення k_j обмежено невеликим числом $k_a < K$, $K \ll N$, причому деяка частина зауважень $k_{j1} \in k_j$ відповідає подіям, які взагалі не враховані в моделі, інші можуть мати невелику розрахункову важливість для безпеки. Для інспектора маємо комбінаторну задачу: потрібно визначити сполучення подій, яке найбільше впливає на ризик $R_{ф}$.

Припустимо, ймовірність сполучення l подій з максимальною важливістю (перший мінімальний переріз) – P_{\max} , причому $l < k_j$, $l \in N$. Ймовірність вибору інспектором саме цих подій буде $P_i = C_N^l$, для типового об'єкта $N \sim 100$, $l \sim 2-3$, $P_i \ll 1$, зневажлива мала величина.

Оскільки події незалежні, підсумкова ймовірність $P_R = P_{\max} \times P_i$ – це зневажлива мала величина другого порядку, тобто ймовірність виявлення ризику за стратегією \hat{S}_2 можна рахувати неможливою подією.

Розглянемо більш сприятливі умови: інспектор має оцінку ризику, що виконана компетентною організацією: $R_{\text{док}} \rightarrow R_{\phi}$. Тобто зробимо розрахунок імовірності помилкових суджень при безрозрахункових методах контролю при наявності повної ймовірнісної структурно-логічної моделі.

Оцінки ймовірності помилкових суджень можна виконати за методикою оцінки ймовірності помилки людини при виконанні розумових дій – THERP, яка широко використовується у процедурах ІАБ або її спрощеного варіанта методики ASP [6].

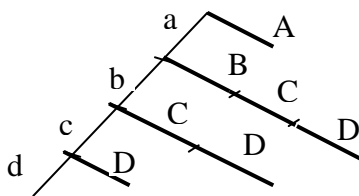
Коли в системі K існують декілька елементів H , які суттєво впливають на ризик, то, щоб перевірити їх стан або ймовірність відмови під час виконання основних функцій, потрібно виконати певний перелік робіт у заданій послідовності [11]. Безрозрахункові методи контролю основані на якісних оцінках інспектором подій та станів обладнання на основі затвердженої інструкції [11]. Отже, перевіряються $k \in \Omega$ елементів з повної множини N .

Якщо існує розрахункова ймовірнісна модель у декларації безпеки об'єкта (ІАБ-Р), інспектор може виявити хибний елемент з якоюсь імовірністю, що може бути легко розрахована за вказаними методиками. Операції (правильні дії, які потрібно виконати інспектору):

- a – з'ясувати перелік важливих елементів моделі;
- b – визначити реальний стан елемента (характеристики надійності);
- c – замінити в ІАБ-Р попередні значення на нові;
- d – провести розрахунок з використанням моделі.

Відповідно неправильні дії будуть:

- A – важливі елементи моделі не виявлені;
- B – реальний стан елемента не з'ясовано;
- C – не всі елементи замінені в ІАБ-Р (попередні значення) на нові;
- D – розрахунок проведено з суттєвими помилками.



$$P_A = 0,1; P_B = 0,2; P_C = 0,05; P_D = 0,01.$$

Аварійні послідовності:

$$\langle A, aBCD, abCD, abcD \rangle \rightarrow P_1, P_2, P_3, P_4.$$

$$P_1 = 0,1; P_2 = 9E-5; P_3 = 3,6E-5; P_4 = 0,00684.$$

Ймовірність помилки $P_{\Sigma} \approx 0,12$.

Рис. 5. Дерево помилок персоналу під час оцінок ризику

Дерево помилок представлене на рис. 5, розрахунок праворуч, імовірності помилкових дій визначені на основі експертних оцінок як середні значення.

Отже, в такому варіанті зовнішня перевірка має сенс, хоча сумарна помилка має відносно велике значення.

Оцінимо ймовірність помилки (пропуску ризику) за стратегією РОП (рис. 2). По суті ця процедура повинна називатися *аудитом безпеки*. Учасниками процесу регулювання (аудиту) безпеки є лише відповідальні особи:

- об'єкт підвищеної небезпеки – суб'єкт підрозділу внутрішнього моніторингу;
- фірми аналізу ризику (підприємства – розробники документів);
- консалтингові фірми й/або інститут експертів;
- державні органи ліцензування експертів.

Завдання персоналу об'єкта підвищеної небезпеки полягає в тому, щоб не помилитися у виборі фірми аналізу ризику – відібрати компетентну у своїй галузі фірму. Для оцінки цієї помилки попередньо оцінимо існування таких фірм взагалі. За статистикою розвинутих країн імовірність тривалого існування на ринку послуг такої фірми дорівнює $(1 - P_k)$, де $P_k = 0,001$, (ймовірність відмивання грошей). Оскільки фірм десятки, ймовірність помилки зменшується і становить рівень четвертого порядку. Оскільки існує кримінальна відповідальність за законом, скоріше фірма знайде компетентного підрядника – $P_{\Pi} \leq 95\%$, помилки розрахунків фірми дуже малі, бо працюють професіонали високої кваліфікації, рівень імовірності помилки ($P \sim 1E-3$), тобто загальна ймовірність помилки, має мале значення – рівень знехтуваного ризику.

8. Висновки

Аудит техногенної безпеки майже повністю виявляє усі ризики, надає можливість обґрунтованого страхування, впровадження нових інформаційних технологій управління безпекою, що створює умови зменшення ризику. Потрібно розробляти оптимальні або хоча б адекватні стратегії державного контролю та доводити їх до суспільства відповідним навчанням фахівців у закладах освіти. Функції управління і нагляду в управлінні безпекою повинні відповідати державному устрою та формі власності. Сучасна стратегія державного нагляду в Україні залишилася від загальнонародної (соціалістичної) форми власності: контроль виробництва частими державними інспекціями. Такий контроль в умовах, що склалися, майже не впливає на рівень ризику. Функції управління і нагляду в управлінні безпекою повинні перейти до компетенції господаря небезпечного об'єкта й виконуватися за його кошти спеціальними підприємствами. Така форма нагляду відповідає новій стратегії – це аудит техногенної безпеки, який виконується за рахунок власника.

Що стосується оптимізації частоти контролю, то при нинішніх законодавчо встановлених методах оцінки безпеки на якісному рівні задача не має рішення взагалі. З цього можна зробити дуже прості висновки: 1) некеровані процеси не можуть призвести до поліпшення ситуації; 2) наука й освіта з безпеки мають великий борг перед суспільством (народом) за невизначеність стратегій управління безпекою та недоведення сучасних норм, правил, алгоритмів до суспільства.

Наведене визначення й опис функцій управління і нагляду повинні бути покладені в основу галузевих методик внутрішнього моніторингу безпеки та державного нагляду в ринкових умовах господарювання. Це узагальнений світовий досвід, який ми маємо впроваджувати в державі. Тільки за цих умов можливе рішення завдання більш високого порядку, а саме дерегуляції безпеки на основі ринкових принципів саморегулювання.

СПИСОК ЛІТЕРАТУРИ

1. Федерація роботодавців в Україні. 17.04.2013, 07:32 388 0. [Електронний ресурс]. – Режим доступу: <http://ua.fru.org.ua>.
2. Бегун В.В. Щодо питань про сучасні методи регулювання безпеки / В.В. Бегун, В.Ф. Гречанінов, В.П. Клименко // Математичні машини і системи. – 2013. – № 4. – С. 135 – 146.
3. Кодекс цивільного захисту України. Законодавство України [Електронний ресурс]. – Режим доступу: <http://zakon1.rada.gov.ua/laws/show/5403-17>.
4. Бегун В.В. Моніторинг безпеки на основі аналізу ймовірнісних структурно-логічних моделей виробництва / В.В. Бегун // Моделювання та інформаційні технології. – К.: ПІМЕ ім. Г.Є. Пухова, 2009. – Вип. 52. – С. 17 – 26.
5. Закон України від 18.01.2001 № 2245-III «Про об'єкти підвищеної небезпеки». Законодавство України [Електронний ресурс]. – Режим доступу: <http://zakon3.rada.gov.ua/laws/show/2245-14>.
6. Вероятностный анализ безопасности атомных станций / В.В. Бегун, О.В. Горбунов, И.Н. Каденко [и др.]. – К.: Випол, 2000. – 558 с.
7. Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності». – 5.04.2007. – N 877-V.
8. Концептуальний підхід до управління ризиками надзвичайних ситуацій техногенного і природного характеру / Г.А. Хміль, Є.П. Буравльов [та ін.] // Екологія і ресурси: зб. наук. праць ПНБ РНБО. – Київ, 2007. – Спецвипуск. – С. 112.
9. Культура безпеки на ядерних об'єктах України: навч. посібник / В.В. Бегун, С.В. Бегун, С.В. Широков [та ін.]. – К.: НТУУ «КПІ», 2009. – 363 с.
10. Модели и механизмы управления безопасностью [Электронный ресурс] / В.Н. Бурков, Е.В. Грацианский, С.И. Дзюбко [и др.]. – Москва, 2001. – С. 140. – Режим доступа: http://www.mtas.ru/search/search_results.php?publication_id=1350.
11. Наказ МНС України «Про затвердження Тимчасової інструкції з перевірки і оцінки стану техногенної безпеки потенційно небезпечних об'єктів господарювання». – 1999. – № 39. – 05.02.

Стаття надійшла до редакції 24.01.2014