Бєгун В. В., к.т.н., науковий співробітник, т. 430-06-15, begunw@ukr.net.
Інститут Державного Управління у сфері Цивільного Захисту.

МОНІТОРИНГ БЕЗПЕКИ НА ОСНОВІ АНАЛІЗУ ІМОВІРНІСНИХ СТРУКТУРНО-ЛОГІЧНИХ МОДЕЛЕЙ ВИРОБНИЦТВА

Розглядаються процедури управління безпекою на основі ризик-орієнтованого підходу та задачі, які з цього виникають.

Ключові слова: безпека, ризик, моніторинг, мінімальні перерізи, управління безпекою

Існуючі методи контролю стану безпеки в галузях економіки України не відповідають сучасним вимогам суспільства, зокрема нещодавно прийнятому закону України “Про основні засади державного нагляду (контролю) у сфері господарської діяльності» [1], який набрав чинності з 2008 року. Чинні документи з контролю безпеки основані на застарілій концепції забезпечення 100% безпеки, що тягне за собою велику низку нормативних актів (пунктів правил) з безпеки та чисельну армію інспекторів для контролю їх виконання. Це “паперова” технологія моніторингу безпеки минулого сторіччя, яка в принципі суперечить ринковим методам саморегулювання, заважає розвитку ринкової економіки. Наслідком цього протиріччя й стало прийняття названого закону як засобу захисту підприємництва. Згідно з законом, організація державного нагляду повинна відбуватися з урахуванням оцінок ступеня ризику від здійснення господарської діяльності її суб’єктами. Таким чином, за законом, ступінь ризику стає загальною характеристикою рівня безпеки законодавчо: чи то техногенної, промислової, пожежної безпеки, безпеки праці, а також і якості продукції, що випускається підприємством.

Але у такий спосіб настає законодавче протиріччя з чинною нормативною базою, яке повинно бути вирішено найближчим часом. Для цього конче потрібне науково-методичне забезпечення робіт з контролю безпеки на основі європейських концепцій прийнятого ризику. Воно відсутнє, на мій погляд, з причин недостатньої обізнаності фахівців цієї галузі, в тому числі вчених, які не володіють (не навчалися) сучасним технологіям визначення ризиків на основі імовірнісних структурно - логічних моделей оцінки безпеки виробництв. Відповідні наукові напрями підготовки галузей знань з безпеки затверджені постановою Кабміну тільки наприкінці 2006 року [2], та недостатньо впроваджені в практику навчання. Галузеві стандарти вищої освіти затверджені тільки в цьому році [3]. Зрозуміло, що методичне і програмне забезпечення цих робіт також відсутнє, тобто, на мій погляд, потрібне негайне втручання (допомога) вчених і фахівців галузей високих (ядерних) технологій, де є напрацювання з аналізу безпеки великих систем (АЕС), або наукова допомога з навчання з Європи аналогічна тій, яка була надана фахівцям ядерної галузі в 90 роки минулого сторіччя.

Закон констатує як факт – теоретичною основою управління безпекою стає ризик-орієнтований підхід. Так Стаття 5 Закону, встановлює, що планові заходи зі здійснення державного нагляду (контролю) Інспекція визначає у віднесеній до його відання сфері критерії, за якими оцінюється *ступінь ризику* від здійснення господарської діяльності. Це сучасна норма розвинутих країн. Але дійсних оцінок ризику та заходів запобігання, розроблених на основі розрахунків ризику в Інспекції немає, також як і числових критеріїв, за якими здійснюється контроль. Відповідна постанова Кабінету Міністрів [4], хоча й повинна була визначати ці критерії, насправді є переглянутою інструкцією радянських часів, прив'язка до значень ризику умовна, ризик фактично не оцінюється. (Складно було в короткий час перейти на нові технології). Тобто, хоча закон й визначає ризик як новий предмет контролю безпеки, але не визначені методи та засоби контролю (ризиків). Таким чином перед науковцями галузі повстає нова задача. Рішення цієї задачі не тривіальне, воно означає перехід на нові технології регулювання безпеки на основі алгоритмів управління безпекою ризик-орієнтованого підходу (РОП), рис.1. Ось повний цикл управління безпекою підприємства в ринкових умовах господарювання на сучасному рівні [5-10].

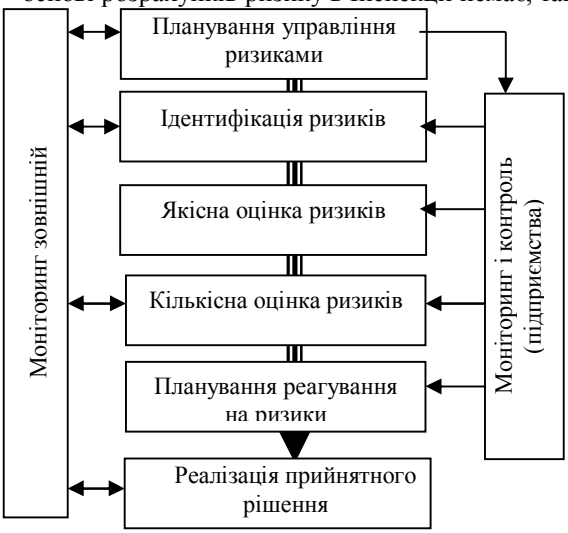

Рис.1. Алгоритм управління безпекою

Як бачимо, ключем стає поняття ризику. Більшість процедур управління пов'язана з оцінкою ризику. За визначенням, *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 імовірності їхньої реалізації до прийнятних значень.

Нажаль, більшість з наведеного на рис.1 не відображено в основних нормативних документах з контролю безпеки, що і є одною з причин непокращення безпеки, а навпаки – загострення ситуації.

У загальному випадку процес управління ризиками при здійсненні діяльності на об'єкті включає виконання шести процедур та постійний моніторинг і контроль. Короткий опис процедур.

Планування управління ризиками – це процес прийняття рішень з урахуванням попередньо проведених оцінок ризиків, що створює об'єкт

підвищеної небезпеки (застосування методології РОП для конкретної діяльності). Цей процес може містити в собі:

– Організацію в об'єкті спеціального підрозділу (групи управління ризиками), відповідального за оцінку і управління безпекою;
– Вибір та обґрунтування методики оцінки ризиків;
– Визначення джерел даних для ідентифікації ризику;
– Визначення інтервалу часу для аналізу ситуації.

Дуже важливим є визначення припустимих (прийнятних) рівнів ризику, які визначаються на основі чинного законодавства. На цьому етапі, звичайно, розробляється та оприлюднюється «Заява про політику підприємства в сфері безпеки»

Ідентифікація ризиків визначає ризики які можуть вплинути на діяльність, що розглядається. Характеристики цих ризиків повинні бути оформлені документально. Ідентифікація ризиків повинна проводитися регулярно протягом усієї діяльності об'єкта. Спеціалізований підрозділ повинен залучати до робіт по ідентифікації ризиків усіх учасників процесу: проектантів, експлуатаційників, фахівців інших підрозділів і незалежних експертів. Ідентифікація ризиків організовується як ітераційний процес. Перші розрахунки потенційного ризику виконують проектанти. У процесі діяльності об'єкту, з урахуванням досвіду експлуатації, уточнюються дані по надійності систем і устаткування, процедурам управління, помилкам персоналу і робиться перерахунок ризиків для об'єкту. Для формування об'єктивної оцінки в завершальній стадії процесу оцінки можуть брати участь незалежні експерти. Приклад ідентифікації ризиків, можна знайти в публікаціях [5-9].

Якісна оцінка ризиків – процедура спрощеної оцінки ризику за відносними шкалами, передує складним розрахункам. На цьому етапі необхідно визначитися з необхідністю проведення кількісних розрахунків. У випадку невеликого (знехтуваного, або цілком припустимого) ризику, кількісні розрахунки не виконуються. Якісна оцінка ризиків проводяться відповідно ГОСТ27.310-95 [7], це процес якісного аналізу результатів ідентифікації, а також визначення подій, що вносять найбільший внесок у загальний ризик і які потребують вживання заходів до їхнього зниження. Якісна оцінка визначає ступінь важливості ризику і складових його подій на основі досвіду з експлуатації. ГОСТ27.310-95 упорядковує процедуру якісній оцінки, завдяки чому зменшуються невизначеності оцінок. Доцільно створити банк даних ризиків усієї діяльності на об'єкті, заснований на систематизованих даних, у тому числі даних по впливу ризиків на персонал. На цьому етапі можливо визначення чинників найбільшого впливу, що створить передумови управління. На основі характеристик вагомості наслідків ризиків і якісних оцінок частоти відмов складається матриця «імовірність відмови – вагомість наслідків» для ранжування ризиків. Якщо за результатами якісній оцінки ризиків отримуємо високі *ранги відмов «*А» або «В» - потрібен обов'язковий поглиблений кількісний аналіз критичності, у

випадку низького рангу відмов «C» або «D» – можна обмежитися якісним аналізом [5]. Тобто зрозумівши роботу елементів і устаткування системи і об'єкту в цілому за допомогою ретельного аналізу, можливо без проведення числових розрахунків якісно визначити ризик, що утворює система.

Кількісна оцінка ризиків потрібна для визначення імовірності виникнення ризиків і впливу їхніх наслідків на діяльність, що допомагає приймати оптимальні рішення й уникати невизначеності (у змісті управління) при цьому. Кількісна оцінка ризиків передбачає виконання попередніх процесів - це завершальний етап задачі визначення ризиків, виконується за допомогою спеціальних програмних засобів, наприклад програми SAPHIR, рис. 2.

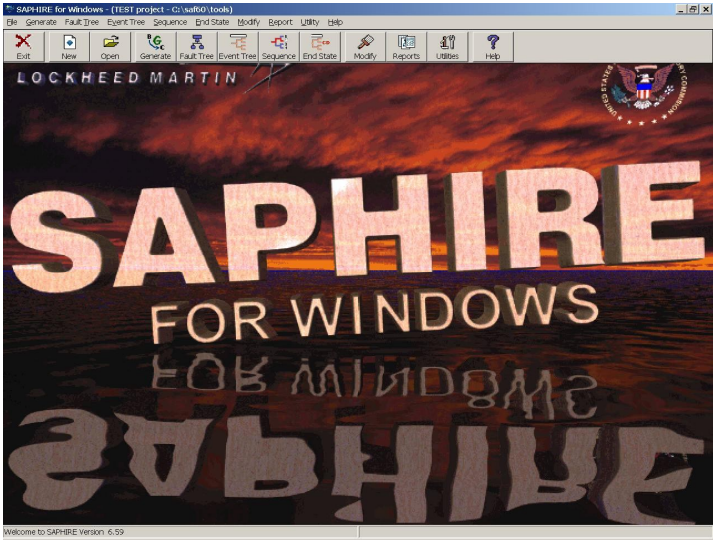

Рис.2. Головна сторінка програми SAPHIR

Результат розрахунків ризику (R) залежить від параметрів об’єкту, тобто ризик є функцією декількох комплексних змінних:

$$R = F(x1,x2,x3,x4,x5,x6), \quad (1)$$

де *X1* – змінна з урахування всіх імовірних сценаріїв аварій для всіх режимів роботи;

X2 – змінна з урахування всіх можливих вихідних подій, природного характеру тощо;

X3 – змінна з урахування зношеності основного обладнання та статистики його відмов;

X4 – змінна з урахування типів захисного обладнання та його стану;

X5 – змінна з урахування навченості персоналу;

X6 – змінна з урахування природно – кліматичних умов об’єкту.

Для проведення кількісних розрахунків створюється імовірнісна структурно-логічна модель об'єкту, яка складається з дерев подій (ДП) – сценаріїв можливих аварій, приклад зображено на рис. 3, та дерев відмов (ДВ) – моделей можливих відмов існуючих систем захисту, рис.4. Кількість дерев подій (сценаріїв) відповідає кількості вихідних подій, а дерева відмов відповідають функціям систем захисту. Детальний опис цієї методології можна знайти в роботах з аналізу безпеки АЕС, та в навчальних посібниках [5,11].

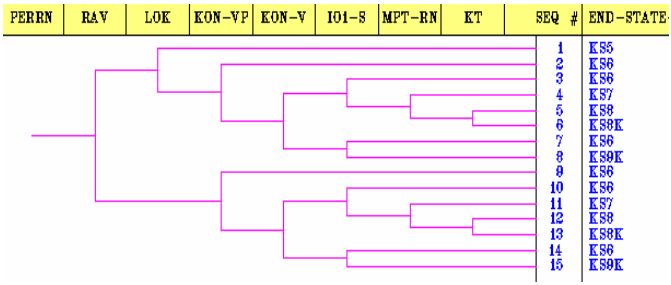

Рис. 3. Дерево подій ОПН «Нафтобаза», сценарій переповнення ємності при наливі

Важливий етап кількісного аналізу систем полягає в представленні умов невиконання функцій системи (її відмови) у вигляді так званої множини *мінімальних перерізів* – імовірного збігу подій, який призведе до відмови системи. Набір мінімальних перерізів системи однозначно визначений її деревом відмов, алгоритм вибору мінімальних перерізів складає найбільш важливу задачу розрахункового коду [8]. Кількість мінімальних перерізів залежить від кількості елементів системи та логіки дерева відмов – це всі сполучення подій за яких можливе виникнення аварії - може досягати для великих систем тисяч і навіть мільйонів комбінацій. За імовірність відмови системи приймається мінімальна апроксимація верхньої границі мінімальних перерізів, яка визначається за формулою:

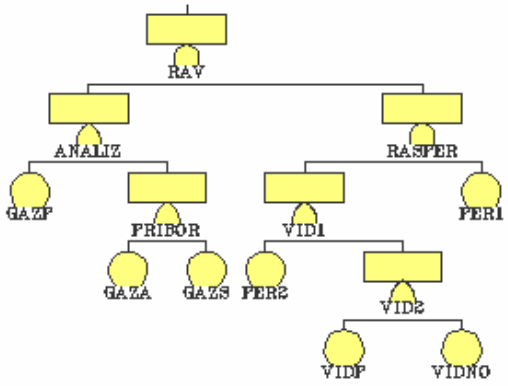

Рис. 4. Дерево відмов системи ідентифікації проливу

$$S=1-\Pi_i(1-C_i), \qquad (2)$$

де S - мінімальна верхня межа мінімальних перерізів для *неготовності* системи;

C_i - імовірність і-го мінімального перерізу;

m - число мінімальних перерізів.

Другим надзвичайно важливим результатом імовірнісного моделювання є таблиця значимості первинних (базисних) подій на імовірність виникнення відмови системи (небажаної події). Справді, якщо відомо, які події найбільше впливають на ризик, то задача управління зводиться до того, щоб зменшити вплив цих подій будь яким чином. Якщо це неможливо, або занадто дорого, то необхідно створювати спеціальні системи безпеки, призначенням яких є обмеження негативної дії небажаної події, або припинення небезпечного процесу на якомусь проміжному етапі. Кількісні дані по базисних подіях впливають на важливість самого мінімального перерізу – його відсотковий вклад в імовірність відмови системи.

За різними сценаріями виникнення й розвитку аварій за допомогою ДП моделюються можливі кінцеві стани. На рис. 3 їх 6 типів, з них повторюються: KS6 – 6 разів, KS7 – 2, KS8 – 2, KS8K – 2, KS9K – 2 рази, всього 15 варіантів реалізації. Відповідно до рис.3, імовірність кінцевого стану залежить від ймовірностей відмов систем захисту та визначається за простою формулою:

$$(P_{ks})_j = P_{вп} \times \Pi_l P_{lj}, \qquad (3)$$

де $j \in [1,15]$, $P_{вп}$ – імовірність вихідної події, P_{lj} імовірність відмові чи спрацювання системи l, $P_{l\,j} = P\ U\ (1\text{-}P)$де P – імовірність відмови системи l для кінцевого стану j, визначається за структурою ДП.

Оскільки відмова (P) системи залежить від надійності її елементів (параметрів $X_3 – X_5$ в формулі 1), то відповідно й імовірність кінцевого стану залежить від тих же ж параметрів підприємства. Тобто, приходимо до висновку, що за результатами імовірнісного моделювання можливо визначити залежність кінцевого стану системи за сценарієм можливої аварії від реального стану підприємства. Також, як і при моделюванні відмов систем безпеки за допомогою ДВ, для кінцевих станів генерується множина мінімальних перерізів. За імовірність кінцевого стану приймається мінімальна апроксимація верхньої границі мінімальних перерізів, яка визначається за формулою (2). Також, можливо визначити вплив – важливість відмов кожного елементу систем безпеки на значення імовірності кінцевого стану. Звідси витікають важливі висновки: 1) можливо планування заходів запобігання небажаних кінцевих станів на основі визначених залежностей, 2) під час моніторингу стану об’єкту небезпеки найбільшу увагу потрібно приділяти тим елементам систем, які мають найбільшу значимість відносно небажаного кінцевого стану за кількісними оцінками ризиків.

Планування реагування на ризики - це розробка методів і технологій зниження негативних наслідків ризиків. Якісне, науково обґрунтоване планування можливо за умови виконання всіх попередніх етапів процесу відповідно до рис. 1. Стратегія планування повинна відповідати типам ризиків, їх величині і значимості, наявності ресурсів і параметрів часу. У

найбільш небезпечних випадках, можливо, потрібно кілька варіантів реагування на ризики. Планування повинне здійснюватися у відповідності зі спеціальною методикою, що враховує специфіку об'єкту, чинні на ньому правила й інструкції.

Реалізація прийнятого рішення здійснюється як заключний етап всієї роботи з управління ризиками, на основі попереднього планування. Це можуть бути дії, які мають бути виконані негайно, або протягом якогось нетривалого терміну чи довгострокові заходи, що потребують значних матеріальних ресурсів. В деяких випадках реалізація прийнятого рішення контролюється державними наглядовими органами - інспекціями. У випадку, коли об'єкт створює загрозу, що перевищує прийняті рівні ризику, потрібно здійснювати заходи модернізації технологій або устаткування чи зовсім припиняти його діяльність.

Моніторинг і контроль (підприємства) параметрів проводяться з метою перевірки дотримання вимог встановлених норм ризику для персоналу, населення та довкілля. Моніторинг і контроль мають здійснюватися спеціалізованим підрозділом об'єкту. При цьому постійно контролюється процес ідентифікації ризиків, виконання плану реагування на ризики, оцінка ефективності заходів для зниження ризиків, величина залишкового ризику і його прийнятність. Відповідно до принципу №1 основополагаючих принципів безпеки [6] (сучасні міжнародні норми) головну відповідальність за забезпечення безпеки має нести особа або організація – об'єкт підвищеної небезпеки (ОПН), які відповідають за установку або діяльність, що пов'язана з ризиками. ОПН планує і організує (і сплачує) роботи з аналізу безпеки, захистом персоналу, населення та довкілля. Тому в ринкових умовах господарювання саме підприємство сильніше за інших учасників з контролю безпеки зацікавлене в зменшенні ризиків.

Таким чином, в умовах ринкового господарювання, приватної власності та повної відповідальності господаря виробництва за стан безпеки, моніторинг можливо поділити на два види:

– внутрішній – самоконтроль безпеки підприємством та
– зовнішній – контроль безпеки державними службами

Внутрішній моніторинг організується підприємством для організації безаварійної роботи, тобто безпека та високі економічні показники не суперечать один одному. Якісний внутрішній моніторинг можливій на основі кількісних розрахунків ризику. В першу чергу здійснюється контроль *важливих* для безпеки параметрів – це контроль на основі попереднього системного аналізу, він оптимізується за допомогою цих розрахунків. Надлишковій контроль, також як і його нестача призводить до зниження ефективності виробництва, марної трати ресурсів. Тому бережливий господар завжди оптимізує контроль параметрів виробництва та безпеки, які тісно пов'язані. Спосіб контролю параметрів, їх перелік та дискретність контролю в часі визначають спеціалісти за умов завчасного виявлення відмов

елементів з заданими довірчими інтервалами. Математичною основою цього може бути теорія діагностики або теорія масового обслуговування.

Зовнішній моніторинг має бути тільки по параметрах, які важливі для безпеки регіону розташування ОПН, безпеки персоналу, населення та довкілля, а саме: чи планується управління ризиками, чи є кількісна оцінка ризиків та чи задовольняються при цьому умови прийнятного ризику, чи реалізуються сплановані заходи зменшення ризику. Тобто, на сучасному перехідному етапі в сфері власності (господарювання), маємо протиріччя між застарілою системою моніторингу безпеки (стосується всіх контролюючих організацій) та сучасною теоретичною базою саморегулювання безпеки в ринкових умовах. З'ясувавши ці обставини, становиться зрозумілим чому зростає число підприємців, які незадоволені діями інспекцій, та чому, навіть, прем'єр міністр після зустрічі з підприємцями визначає негативну роль органів контролю безпеки.

Якісний контроль виконання діяльності з регулювання безпеки подає інформацію, що сприяє прийняттю ефективних рішень по запобіганню нових ризиків чи пом'якшення наслідків. Контроль може ініціювати вибір альтернативних стратегій, прийняття коректив, перепланування проекту для досягнення базового плану.

При організації управління ризиком, розробці пропозицій щодо прийняття управлінських рішень для забезпечення наочності, зручності проведення оперативних розрахунків ризику доцільно наносити на карти інформацію про зони ризику на об'єкті. Під зонами ризику розуміють приміщення й території, що обмежені ізолініями, яким відповідають визначені рівні ризику. Встановлення зон ризику має важливе практичне значення. Особливо велика роль цих зон при аналізі, оцінці обстановки й ухваленні рішення в аварійних умовах.

Моніторинг та контроль безпеки є одною зі складових процесу управління безпекою. В нових умовах господарювання, підвищеної відповідальності суб'єктів господарювання потрібні й нові, більш ефективні методи організації цього процесу. Тільки аналіз імовірнісної структурно-логічної моделі ОПН з виділенням мінімальних перерізів систем безпеки та оцінка важливості подій на основі імовірнісних критеріїв важливості, надає можливість завчасного визначення імовірного критичного збігу обставин та розробці на цій основі заходів запобігання ризику. Тому для дійсного контролю ризику об'єкту в сучасних умовах потрібен комп'ютер (ноутбук) з заздалегідь розробленою моделлю виробництва та поточні значення імовірності впливових (важливих розрахункових) подій, які інспектор вносить в модель. Ці поточні значення залежать від вище зазначених факторів виробництва (1), для інспектора має існувати чітка методика їх визначення. Програма визначить ступінь ризику, порівняє його з припустимим та запропонує оптимальні заходи зі зменшення ризику.

Відповідно до принципів ризик-орієнтованих підходів у діяльності по регулюванню безпеки будь-який контроль має розглядатися як складова процедур ризик – менеджменту:

– організація ризик – менеджменту;
– інформаційної підтримки ризик – менеджменту;
– стратегії контролю (розрахунку) ризику;
– стратегії страхового захисту.

Тільки за такою сучасною організацією моніторингу можливо досягнення цілей промислової та екологічної безпеки, забезпечення раціонального використання обмежених людських, матеріальних і фінансових ресурсів та економічне стимулювання розробки і впровадження безпечних, ресурсозберігаючих технологій. Але такі нові методики моніторингу на Україні відсутні, задача науковців постає в тому, щоб вони з'явилися найближчим часом.

Висновки. Потрібна докорінна зміна технологій управління безпекою, в тому числі й процедур моніторингу безпеки, на основі ризик-орієнтованих підходів, та відповідних розрахунків ризику. На основі кількісних розрахунків ризиків мають визначатися параметри внутрішнього і зовнішнього моніторингу: перелік елементів системи (об'єкту) для контролю та частота контролю за умови прийнятних значень безпеки та ефективності виробництва.

1. *Закон України* "Про основні засади державного нагляду (контролю) у сфері господарської діяльності». 5.04.2007, N 877-V.
2. *Постанова КМУ* від 13 грудня 2006 р. N 1719 «Про перелік напрямів, за якими здійснюється підготовка фахівців у вищих навчальних закладах за освітньо-кваліфікаційним рівнем бакалавра».
3. *ГСВУ* з безпеки
4. *Постанова КМУ* від 14 листопада 2007 р. N 1324 «Про затвердження Порядку розподілу суб'єктів господарювання за ступенем ризику їх господарської діяльності для безпеки життя і здоров'я населення, навколишнього природного середовища щодо пожежної безпеки».
5. *В.В.Бєгун, І.М.Науменко.* Безпека життєдіяльності (забезпечення соціальної, техногенної та природної безпеки). Навчальний посібник. – К.: "Фенікс", 2004. - 328 с.
6. Основополагающие принципы безопасности (основы безопасности). Серия норм МАГАТЭ по безопасности, № SF-1. МАГАТЭ, Вена, 2007 г, 34 с.
7. *Директива Ради* 96/82/ЕС від 9 грудня 1996 р. стосовно контролю небезпеки від великомасштабних аварій, що включають небезпечні речовини. Офіційний журнал L 010 , 14/01/1997 стор. 0013 – 00
8. *Белов. П.Г.* Теоретические основы менеджмента техногенного риска. Автореферат диссертации. М., 2007.
9. Концепція управління ризиками надзвичайних ситуацій техногенного і природного характеру. Проект. http://www.mns.gov.ua/освіта та наука;
10. *Н.А.Махутов.* Научно – методические подходы и разработка мероприятий по обеспечению защищенности критически важных для национальной безопасности

объектов инфраструктуры от угроз техногенного и природного характера. Ж. Проблемы безопасности и чрезвычайные ситуации. ВИНИТИ, М. 2004, №1

11. Вероятностный анализ безопасности атомных станций / *Бегун В.В., Горбунов О.В., Каденко И.Н.* и др. К.: Випол, 2000 г., 558 с.