УДК 351.862.1: 004.9

В.Ф. Гречанінов, канд. техн. наук., В.В. Бєгун, канд. техн. наук, В.П. Клименко, д-р. фіз.-мат. наук., професор, Яцюк О.П., канд. хім. наук.

АКТУАЛЬНІ ПРОБЛЕМИ МОДЕЛЮВАННЯ РИЗИКІВ І ЗАГРОЗ КРИТИЧНИХ ІНФРАСТРУКТУР

В цій статті розглядається реформування системи управління безпекою та актуальні проблеми моделювання ризиків і загроз критичних інфраструктур в Україні на основі ризик-орієнтованого підходу. Аналізується стан проблеми, визначені методи і алгоритм її рішення. Вперше пропонується рішення проблеми на основі створення інформаційної технології безпеки, розглянуті основні процеси, функції, математичні моделі та структура ІТБ.

Ключові слова: безпека, моделювання ризиків, інформаційні технології безпеки, критичні інфраструктури.

V. Grechaninov, Cand. of Sc. (Eng.), V. Begyun, , Cand. of Sc. (Eng.), V. Klymenko, Doc. of Sc. (Eng.), O. Yatsyuk, Cand. of Sc. (Chem.)

ACTUAL PROBLEMS OF RISKS AND THREATS MODELING OF CRITICAL INFRASTRUCTURE

Safety management system reforming and actual problems of risks and threats modeling of critical infrastructures in Ukraine based on risk-based approach are described in this article. Analyzes the state of the problem, defined methods and its solution algorithm. For the first time presented a problem solution based on informational security technology creation, basic processes, activities, mathematical models and structure of informational security technology are reviewed.

Keywords: safety, risks modeling, informational security technology, critical infrastructures.

Вступ. Проблеми захисту критичних інфраструктур (КІ) досліджуються з кінця минулого століття в усьому світі. Розпочиналися дослідження на пострадянському просторі на рівні Академії наук Росії академіком Махутовим Н.А., Петровим В.П., Ахметхановим Р.С. [1]. В Україні з 90-х років була прийнята низка постанов Кабінету Міністрів України щодо фізичного захисту КІ, зокрема: №615 від 10 серпня 1993 р.; №675-019 від 24.04.1999 р.; № 1170 від 28.07.2003, які передбачали тільки посилення охорони об'єктів. Досвід провідних країн світу з організації системи захисту критичної інфраструктури вивчався у Національному інституті стратегічних досліджень (НІСД) у 2012-2013 рр. Це було продовженням досліджень, розпочатих у 2008 році д.т.н. Дроздом І.П. у структурі тодішнього інституту РНБО [2]. Система управління безпекою потребує принципових реформ. З точки зору запобігання надзвичайних ситуацій (НС) існуюча структура системи попередження більш не є ефективна. Реформування управління ризиками з метою попередження виникнення НС техногенного походження на основі ризик орієнтованого підходу (РОП), потребує об'єднання зусиль фахівців системи Державної служби України з надзвичайних ситуацій (ДСНС), науковців інститутів НАН України, порад міжнародних експертів тощо.

Аналіз стану проблеми. У вересні 2014 року НІСД в рамках Програми професійної підготовки Офісу зв'язку НАТО в Україні провів першу міжнародну експертну нараду з питання розробки Зеленої книги [3], на якій було обговорено структуру майбутнього документа, створено робочу групу для написання тексту, узгоджено графік роботи тощо. 25 листопада 2014 р. у НІСД відбулася друга міжнародна експертна нарада з питання

розробки «Зеленої книги із захисту критичної інфраструктури в Україні». Участь у цій нараді взяли експерти з Франції, Центру передового досвіду НАТО, Польщі, Урядового центру безпеки США. Вони високо оцінили той факт, що в Україні розпочалася робота щодо захисту критичної інфраструктури. Тобто, можна констатувати, що з різних причин наукові заходи [4,5] (круглі столи, конференції) та дослідження на протязі 2008-2014 рр. пройшли з малою результативністю, і лише зараз визначено початок роботи. Для порівняння, у Росії достатня було трьох років від перших наукових публікацій до затверджених методик.

При цьому необхідність та важливість захисту КІ була очевидна, і відповідними постановами Кабміну України перелік об'єктів КІ двічі розширювався [6, 7]. Можна констатувати дефіцит чіткої координації робіт у всьому комплексі аспектів: політичному, науковому, юридичному, методичному та інформаційному. Мала бути класична схема за алгоритмом:

ЗАМОВЛЕННЯ (прозорий конкурс)→НАУКА (інститути НАНУ, галузеві наукові та науково-дослідні заклади, інші)→КОНЦЕПЦІЯ →ГРОМАДСЬКІ ОБГОВОРЕННЯ→ПЛАН ЗАХОДІВ→ЗАКОН (ПОСТАНОВА) →ВПРОВАДЖЕННЯ→НД (МЕТОДИКИ)→ДЕРЖАВНИЙ МОНІТОРИНГ. (1)

За цим алгоритмом проходять наукові розробки в усіх розвинених країнах, Росії тощо. Так, на всі кроки алгоритму у РФ достатньо було 3 роки. У 2004 році були перші наукові публікації [1,8], у 2005 – постанова [9], 2007 – методика [10], яка постійно удосконалювалася [11]. Вже у 2004 році з'явилися фундаментальні роботи під керівництвом академіка Махутова Н.А. [1], де були викладені не тільки основні визначення, а й повне наукове та методичне бачення, що відображено на рис.1.

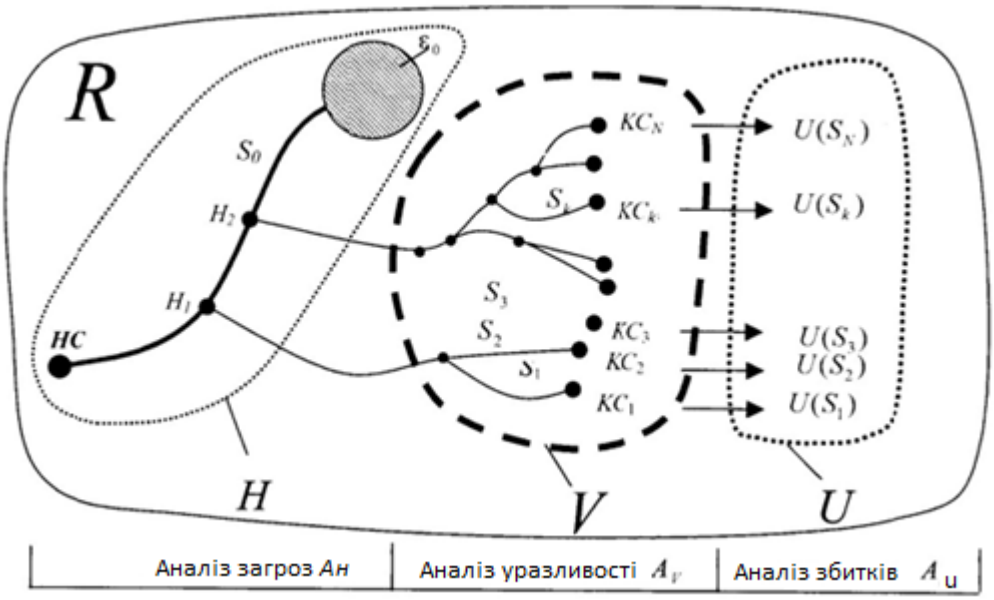

Рисунок 1 – структура аналізу ризику, загроз уразливості, збитків та захищеності КІ. $A_R = A_H$ U A_V U A_U. НС – початковий стан КІ; S_0 – сценарій вдалого виконання системою своїх функцій; KC_0 – заданий кінцевий стан КІ, ε_0 – околиця точки KC_0 в котрий кінцеві стани можливо рахувати неушкодженими; H_1, H_2 – вихідні події, S_i $(I = 1,2, \ldots. N)$ – сценарії відмови; KC_i $(I = 1,2, \ldots. N)$ – ушкоджені кінцеві стани КІ; $U(S_i)$ $(I = 1,2, \ldots. N)$ – збитки, що відповідають сценаріям S_i.

Як бачимо, на одній схемі визначено структуру критерію відношення об'єкта до класу КІ (рівень загроз, рівень уразливості, розмір можливого збитку), методологію і метод аналізу

ризику. Далі в тексті цієї статті наводиться математичний апарат аналізу критичності, заснований на ризик-орієнтованому підході, що в цілому відповідає кращій світовій практиці. Це підтверджує й цитата «Зеленої книги»: «Як вважають американські експерти, оцінка ризиків має складати основу політики із забезпечення національної безпеки, яка з фундаментальної точки зору являє собою процес управління ризиками». Крім того у Росії, як інтегральний показник захищеності $\boldsymbol{Z}$ вводиться індекс захищеності КІ, визначений як відношення законодавчо встановленого допустимого значення інтегрального ризику для об'єктів певної групи [$\boldsymbol{R}$] до поточного значення інтегрального ризику $\|R\|$:

$$Z = \frac{[R]}{\|R\|} \tag{2}$$

Як бачимо з рис.1, використана методологія ймовірнісного моделювання (ІАБ) та відповідне матричне представлення кінцевих станів [1]. Тобто задача вирішувалася в її природному за алгоритмом (1) комплексі та послідовності. Були навіть змінені структура і зміст освіти з безпеки: з 2003 року викладається дисципліна «Рискология». В Україні з прийняттям деяких законів європейського типу [12, 13] виникла необхідність розробки або зміни підзаконних актів, у тому числі постанови Кабміну про моніторинг: «Порядок функціонування системи моніторингу і прогнозування надзвичайних ситуацій». Але вона не затверджена до цього часу: причина – не має обґрунтування, наукової підтримки, не вказані засоби, структура, ресурси, процедури управління, реагування, оповіщення та ін. Присутня тільки формальна сторона – вимоги впровадження нового кодексу цивільного захисту [13]. Але оскільки реального переходу на концепцію РОП, незважаючи на вимоги нового законодавства не відбулося, неможливі розробка та впровадження нових методів і методик. Підтверджують цю думку і міжнародні експерти, тобто рішення проблеми безпеки КІ можливе тільки на основі ризик-орієнтованого підходу.

З метою скорочення терміну переводу запобігання НС та управління ризиками на основі РОП та сучасних інформаційних технологій (ІТ), пропонується наступний алгоритм паралельної роботи в зміні законодавства та створенні моделей ІТ (рис. 2):

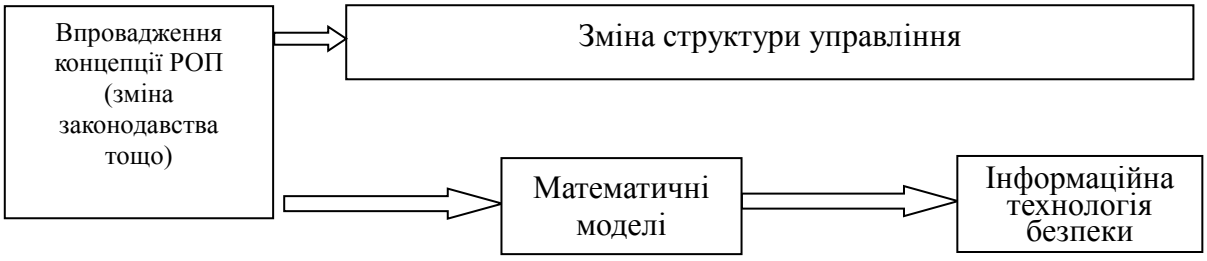

Рисунок 2 – Алгоритм впровадження РОП.

Авторами запропонована мінімально можлива структура [14] управління ризиком на основі РОП, представлена на рис.3. Подібні структури в тій чи інший формі існують в усіх розвинутих країнах. Як бачимо, присутність держави може бути мінімальною. Якщо менеджмент (в деяких випадках – власник) несе повну відповідальність за безпеку свого виробництва (об'єкта) перед третіми особами та державою, він буде більш мотивований у недопущенні аварій чи аварійних ситуацій. Окремо потрібно підкреслити, що як свідчить досвід [14], при досконалих математичних моделях, будуть знайдені підприємства (експерти), які зможуть достовірно визначити ризик його об'єкта та засоби його зниження.

Зовсім логічно й очевидно, що при належному рівні підготовки об'єкта й внутрішньому моніторингу наслідки аварійних процесів можуть бути істотно знижені, а в багатьох випадках попереджені. Тобто рівень безпеки відображає 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, у структурі існують тільки два елементи, що знаходяться на утриманні бюджету: органи державного нагляду за дотриманням чинного законодавства (суттєво зменшені) та державні органи ліцензування експертів. Ці органи існують і у старій структурі, але тут їх функції змінені й, відповідно, їх чисельність значно зменшується. Місцеві й державні органи влади контролюють тільки ступінь ризику.

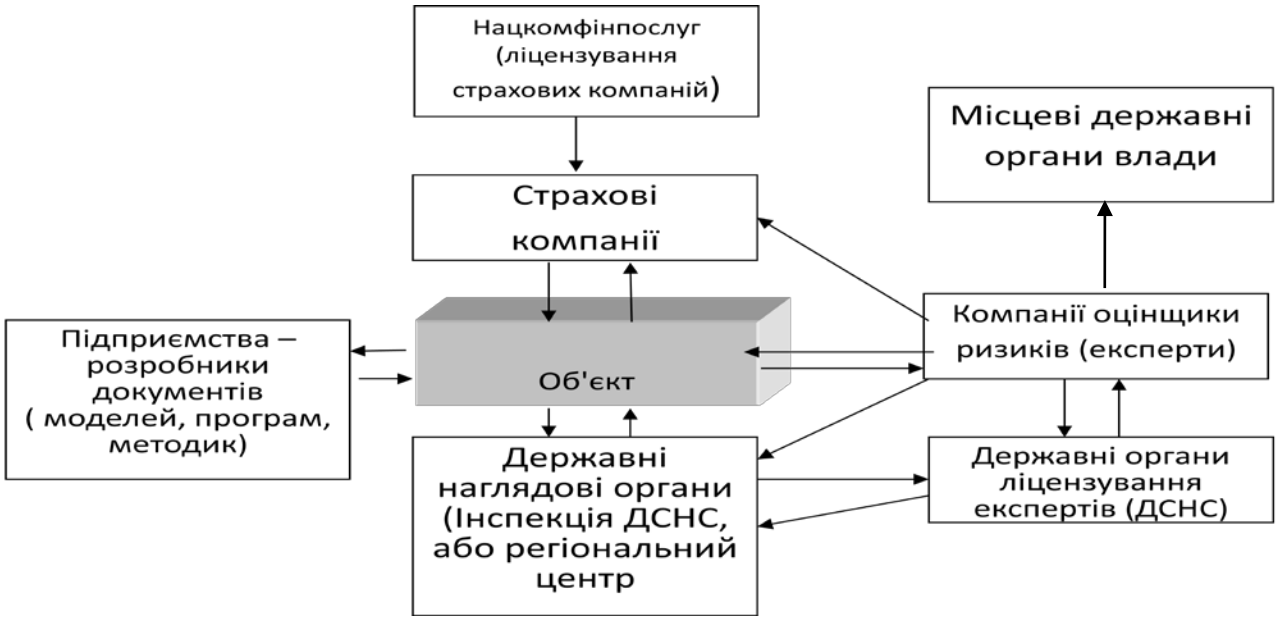

Рисунок 3 – Структура системи управління безпекою на основі ризик орієнтованого підходу.

Проблема безпеки КІ – багатогранна і має різні аспекти:

– політичний - має бути інша структура управління (дерегуляція);

– науковий - мають бути розроблені нові методи, моделі, алгоритми, розрахункові програми (коди);

– інформаційний - мають бути впроваджені інформаційні технології;

– соціальний - стосується кожного громадянина.

Отже, розглянемо політичні аспекти рішення проблеми за алгоритмом (1). Звичайно замовлення виникає, якщо є суспільна потреба або напрацювання науковців, що удосконалюють процеси чи впроваджується кращий світовий досвід. Замовником виступає або держава, або зацікавлені фірми.

Науковий аспект: вибір методології, критеріїв відношення, методик – повинен бути запропонований на основі аналізу існуючих розробок інших країн та власних досягнень наукової установи за напрямом основної діяльності (моделювання), звісно, на прозорих тендерних процедурах. Розробки програмного забезпечення мають бути невід'ємною частиною рішення проблеми та проводитися паралельно досвідченим колективом програмістів. Усі ці задачі необхідно вирішувати в їх взаємному зв'язку на основі концепції РОП. Загальний алгоритм управління ризиком наведено в багатьох працях [5,14], звісно він цілком підходить до управління безпекою КІ.

Інформаційний: розглянемо інформаційні задачі (авторами пропонується сучасна інформаційна технологія управління ризиками КІ, описана нижче). Очевидно, ставити питання управління ризиками доречно тільки за умови можливості обробки великого потоку

інформації у реальному часі, тобто опираючись на сучасні інформаційні технології. Згідно з загальнотеоретичними знаннями [15] до структури інформаційної технології мають входити такі інформаційні процеси (рис. 4):

1. Інформаційний процес координації перетворень інформації (Information process coordinati) – IPC.
2. Інформаційні процеси попередньої обробки даних (Information processes data preprocessing) – IPPD.
3. Інформаційні процеси опосередкованих вимірювань (обчислень) параметрів процесів (Information processes measurement) - IPM.
4. Інформаційні процеси перетворень даних у признаки ситуацій (Information processes change data in situations signs) – IPDC.
5. Інформаційні процеси діагностики ситуацій (Information processes diagnostic situations) – IPDS.
6. Інформаційні процеси отримання рекомендацій оператору (Information processes of recommendations operator) – IPDR.
7. Інформаційні процеси модифікації правил розпізнавання (Information processes modifying the rules of recognition) – IPRM.
8. Інформаційні процеси формування історії моніторингу (Information monitoring processes of formation history) – IPFH.
9. Допоміжні інформаційні процеси (корекція БД і БЗ та ін.) (Supporting Information processes) – IPS.

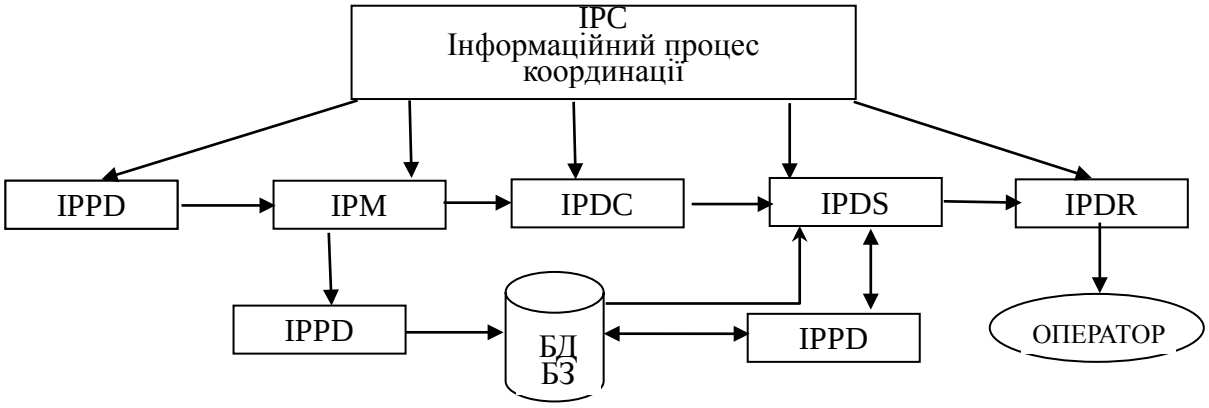

Рисунок 4 - Загальна схема зв’язків основних ІТ процесів.

Інформаційну технологію в її прикладному застосуванні щодо безпеки позначимо як ІТБ. Формування *структури комплексу інформаційних процесів* щодо безпеки є одним із важливих етапів моделі ІТБ. На основі загальнотеоретичних знань та власного досвіду авторами визначені такі інформаційні процеси ІТБ:

ІП 1. Координація виконання інформаційних процесів.

ІП 2. Моніторинг і попередня обробка даних.

ІП 3. Оцінка рівня ризику.

ІП 4. Розпізнавання ситуацій.

ІП 5. Вироблення повідомлень і рекомендацій.

ІП 6. Виведення повідомлень і рекомендацій.

ІП 7. Корекція бази знань (БЗ) і бази даних (БД).

ІП 8. Збереження значень ознак і імені ситуацій

Функціонування цих процесів у системі управління безпекою утворює сучасну інформаційну систему безпеки.

До основних функцій даної системи віднесемо такі функції за нормальних (ФН) і аварійних умов (ФА) роботи:

ФА 1. Вироблення рекомендацій оператору при аваріях.

ФН 2. Вироблення рекомендацій щодо заміни обладнання, яке підвищує значення ризику за нормальних умов експлуатації.

ФН 3. Вироблення рекомендацій щодо зниження ризику.

ФН 4. Визначення поточних значень ризику і рівня культури безпеки.

ФН 5. Вироблення рекомендацій щодо визначення періоду перевірок.

ФН 6. Вироблення рекомендацій щодо підготовки персоналу.

ФН 7. Вироблення рекомендацій щодо страхування ризику.

Наведемо короткий опис названих функцій. *Функція* **ФА1** - вироблення рекомендацій оператору при аваріях за законодавством має бути в системах безпеки усіх небезпечних об'єктів. Тут, з впровадженням ІТБ, подається інформація з врахуванням усіх подій що відбуваються на об'єкті, якщо аварія уже сталася. Крім обов'язкових дій, прописаних у ПЛАСі, мають бути відображені, з врахуванням обставин, що склалися, рекомендації з ***оптимальних*** дій щодо приведення об'єкта у безпечний стан та дій необхідного захисту персоналу і населення з відображенням «поля» небезпек. З досвіду відомо, що найбільш великим інформаційним дефіцитом при аваріях є інформація про те, що відбувається. Оскільки ІТБ надає повну інформацію про процеси та події у реальному часі, має необхідні моделі для розрахунків, то виконати цю функцію не складає труднощів. Звісно, аналіз подій має бути з сценаріїв і моделей, що існують у ІТБ, тому при розробці моделей і сценаріїв аварій важливо враховувати наявний вітчизняний і світовий досвід експлуатації об'єктів свого класу небезпек.

Функція **ФН 2.** Вироблення рекомендацій щодо заміни обладнання, яке підвищує значення ризику за нормальних умов експлуатації. Функція нормальної експлуатації в ІТБ відслідковує рівень ризику та постійно порівнює його з допустимим. Ризик за будь-яких, навіть сприятливих умов, підвищується з різних обставин, наприклад, старіння обладнання. За наявності відповідної моделі ІТБ визначає обладнання систем безпеки, яке приблизило об'єкт до межі допустимого ризику та визначає також часові рамки для його заміни.

Функція **ФН 3**. Вироблення рекомендацій щодо зниження ризику. Ця функція є продовженням попередньої, на основі моделі визначає інші (усі) варіанти зниження ризику з урахуванням витрат на модернізацію системи. ІТБ переглядає усі варіанти та вибирає оптимальний або обраховує варіант оператора (за вимогою).

Функція **ФН 4**. Визначення поточних значень ризику й рівня культури безпеки. У режимі реального часу на основі існуючої перевіреної моделі розраховується значення ймовірностей розгерметизації небезпечних речовин, порушень небезпечних технологічних процесів та одночасних відмов захисних систем (бар'єрів). На основі знання обставин поточного часу (реального стану обладнання, погодних умов, яка зміна операторів працює та інші змінні обставини) оцінюється ризик для персоналу, населення та довкілля. Це основна функція ІТБ, саме за це і потрібне впровадження комп'ютерних технологій у сферу безпеки.

Функція **ФН 5.** Вироблення рекомендацій щодо визначення періоду перевірок. Визначається період зовнішнього моніторингу за умови мінімуму ризику для персоналу та довкілля. Виконання цієї функції відповідає потребам (зовнішнього) державного моніторингу.

Функція **ФН 6**. Вироблення рекомендацій щодо підготовки персоналу. Аналізуються безпосередні і кореневі причини аварій та аварійних ситуацій, що відбулися, з помилок персоналу тощо, та вносяться корективи навчальних програм персоналу.

Функція **ФН 7**. Вироблення рекомендацій щодо страхування ризику. Страхування – одне з основних елементів і умов регулювання ризику. В небезпечних галузях існують

механізми страхування, які можуть бути запущені в автоматизованому режимі. Це означає вироблення рекомендацій власнику і персоналу на оптимальних умовах.

Отже, для можливості виконання цих функцій авторами розроблені такі математичні моделі [14,16,17]:

М1. Типова модель галузі (алгоритм побудови та вимоги).
М2. Алгоритм адаптації для підприємства/КІ моделі галузі.
М3. Модель визначення важливих базисних подій (БП).
М4. Модель визначення параметрів моніторингу.
М5. Модель моніторингу.
М6. Модель визначення параметрів БП.
М7. Моделі оцінок ризику:
оцінка поточного значення ризику;
оцінка стану безпеки.
М8. Модель вироблення рекомендацій щодо зниження ризику.
М9. Модель урахування можливих помилок персоналу.
М10. Модель розрахунків ризику персоналу за робочими місцями.
М11. Модель розрахунків ризику для населення регіону розміщення об'єкту.
М12. Модель оцінок ризиків для сусідніх об'єктів.
М13. Модель визначення рівня культури безпеки.

Детальний опис названих моделей можна знайти у працях [14, 16, 17]. Схема ІТБ може бути представлена в наступному виді, рис. 5:

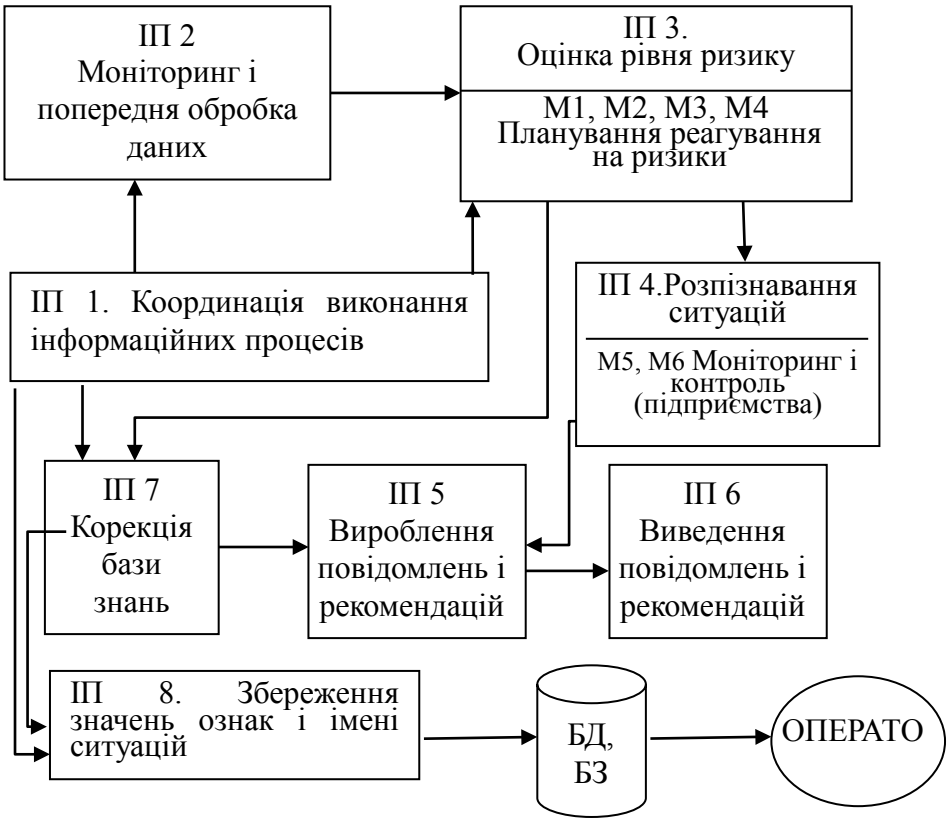

Рисунок 5 - Схема ІТ-процесів безпеки з позначенням моделей.

Більш детальні вимоги щодо інформаційних процесів і моделей ІТБ розглянуті у праці [16]. Пропонується додатково вирішити такі завдання:

– розробка критеріїв віднесення об'єктів критичної інфраструктури до різних категорій небезпеки;

категорування об'єктів критичної інфраструктури у відповідності з вказаними критеріями;

– ведення реєстрів об'єктів критичної інфраструктури з урахуванням їх категорії небезпеки;

– встановлення вимог до систем безпеки об'єктів критичної інформаційної інфраструктури з урахуванням їх категорії небезпеки;

– забезпечення взаємодії цих систем з державною системою виявлення, попередження і ліквідації наслідків комп'ютерних атак на інформаційні ресурси;

– здійснення оцінки захищеності критичної інформаційної інфраструктури України і її об'єктів;

– здійснення державного контролю в галузі безпеки критичної інфраструктури держави.

Таким чином, інформаційна технологія безпеки на основі РОП може бути застосована для рішення проблеми безпеки КІ з максимальним використанням інформаційних ресурсів та автоматизованої системи моніторингу. Це забезпечує управління на основі аналізу ризику та запобігання небезпек, з одночасною дерегуляцію державного нагляду. Можливе об'єднання баз даних з безпеки та прийняття рішень щодо безпеки на основі технологій ситуаційних центрів. В цілому, це, безумовно, приведе до суттєвого підвищення рівня безпеки та скорочення витрат.

Висновки: Використання представлених в рамках цієї роботи алгоритмів впровадження ризик - орієнтованого підходу з урахуванням кращого світового досвіду та нових інформаційних технологій, дозволить обґрунтовано підійти до питання забезпечення безпеки об’єктів критичної інфраструктури з одночасним реформування органів державного нагляду.

Рішення має бути комплексним: від методології, моделі до програм моніторингу. Відповідно до світової практики мають бути використані концепція ризик-орієнтованих підходів, методологія ймовірнісного аналізу безпеки та відповідне програмне забезпечення.

СПИСОК ЛІТЕРАТУРИ

1. Махутов Н.А. Научно-методические подходы и разработка мероприятий по обеспечению защищенности критически важных для национальной безопасности объектов инфраструктуры от угроз техногенного и природного характера / Н.А. Махутов // Проблемы безопасности и чрезвычайные ситуации. – 2004. – № 1. – С. 41 - 49.
2. Дрозд І.П. До проблеми убезпечення техногенних об’єктів України / В.П. Горбулін, В.В. Гетьман, І.П. Дрозд // Екологія довкілля та безпека життєдіяльності. - 2008. №5, С.5 – 9.
3. Зелена книга з питань захисту критичної інфраструктури в Україні. – К.: - НІСД, 2014. С.- 35. Режим електронного доступу: http://www.niss.gov.ua/.
4. "Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні". Аналітична записка НІСД - 2012. Режим електронного доступу: http://www.niss.gov.ua/articles/1477/ .
5. Бєгун В.В. Проблеми регулювання техногенної безпеки в Україні / В.В. Бєгун, В.Ф. Гречанінов // Концепція захисту критичної інфраструктури: стан, проблеми та перспективи її впровадження в Україні: зб. матеріалів Міжнар. наук.-практ. конф. (м. Київ – м. Вишгород, 7–8 листопада 2013 р.). – К.: НІСД, 2013. – С. 77 – 88.
6. Перелік особливо небезпечних підприємств, припинення діяльності яких потребує проведення спеціальних заходів щодо запобігання заподіянню шкоди життю та здоров'ю

громадян, майну, спорудам, навколишньому природному середовищу / Затв. Постановою Кабінету Міністрів України від 06.05.2000 №765.

7. Постанова Кабінету Міністрів України від 23.12.2004 № 1734 «Про затвердження переліку підприємств, які мають стратегічне значення для економіки та безпеки держави».
8. Махутов Н.А. Обеспечение защищенности критически важных объектов на основе снижения их уязвимости / Н.А. Махутов, В.П. Петров, Д.О. Резников, В.И. Куксова // Проблемы безопасности и чрезвычайные ситуации. – 2009. – № 2. – С. 50 - 69.
9. Постановление Совета Безопасности России 08.11.2005 «Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий».
10. «Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры» (утв. ФСТЭК России 18.05.2007).
11. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (2012 до 2020) (Утверждены Президентом Российской Федерации Д.Медведевым 3 февраля 2012 г., № 803).
12. Закон України "Про основні засади державного нагляду (контролю) у сфері господарської діяльності». – N 877-V. – 5.04.2007 р.
13. Кодекс цивільного захисту України. Законодавство України [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/5403-17.
14. Функції управління і нагляду в ризик-орієнтованому підході до управління безпекою/ В.Ф. Гречанінов, В.В. Бєгун. // Математичні машини і системи. – К.: ІПММС, 2014. – №1. – С. 159-170.
15. Левыкин В.М., Шевченко И.В.. Метод построения информационной технологии диагностики состояния сложного технологического процесса // Управляющие системы и машины. – К.: МНУЦ ИТ, 2014. - №3. – с. 33-38.
16. Бегун В.В. Мониторинг риска объектов повышенной опасности на основе предварительного моделирования / В.В. Бегун // Зб. наук. праць "Моделювання та інформаційні технології" міжнар. наукового семінару «Моделювання-2010». – К.: ІПМЕ ім. Г.Є. Пухова, 2010. – Т.1. – С. 152 – 163.
17. Гречанінов В.Ф. Інформаційні технології аналізу стану техногенної безпеки та планування протидії надзвичайним ситуаціям: автореф. дис. на здобуття наук. ступеня кандидата техн. наук: 05.13.06 / В.Ф. Гречанінов. – Київ, 2015. – 22 с.

❖ ❖ ❖