УДК 004.9

В.В. БЄГУН*

ОГЛЯД СТАНУ ТА МОЖЛИВОСТЕЙ ВПРОВАДЖЕННЯ ІТ У СФЕРУ БЕЗПЕКИ

*Інститут проблем математичних машин і систем НАНУ, м. Київ, Україна

Анотація. *Проведено аналіз стану впровадження ІТ у сферу управління безпекою України. Визначено, що він не відповідає сучасним можливостям ІТ. Наведено короткий опис інформаційної технології безпеки. Визначено, що перехід на більш високий рівень інформатизації у цій сфері можливий разом зі зміною парадигми безпеки, що процеси інформатизації простіше здійснювати за галузями виробництва.*
Ключові слова: *безпека, ризик-орієнтований підхід, інформаційні технології, моделі безпеки.*

Аннотация. *Проведен анализ состояния внедрения ИТ в сферу управления безопасностью Украины. Определено, что оно не соответствует современным возможностям ИТ. Приведено краткое описание информационной технологии безопасности. Определено, что переход на более высокий уровень информатизации в этой сфере возможен вместе со сменой парадигмы безопасности, что процессы информатизации проще осуществлять по отраслям производства.*
Ключевые слова: *безопасность, риск-ориентированный подход, информационные технологии, модели безопасности.*

Abstract. *The analysis of the state of IT implementation in the safety management field of Ukraine is carried out. As a result of the analysis the current level of implementation is identified as not corresponding to the modern possibilities of IT. The short description of the Safety Management IT is given. The main conclusions are pointed out as: the transition to the next (higher) level of IT implementation in this field is possible with safety paradigm change; using the branch of industries principle is the simplest way to implement the IT in Safety Management.*
Keywords: *safety, risk-oriented approach, informational technologies, safety models.*

1. Вступ

Кількість аварій, надзвичайних ситуацій (НС) та пожеж в Україні за останні роки невпинно зростає. Обсяги матеріальних збитків вже перевищують один відсоток валового внутрішнього продукту (ВВП), не кажучи про людські втрати. Планові запобіжні заходи центральних органів виконавчої влади (ЦОВВ) не дають бажаного результату: єдина система цивільного захисту (успадкована від СРСР) надто застаріла. Контроль за станом потенційно небезпечних об’єктів (матеріальна база яких здебільшого деградує) неефективний, бо інспектори Державної служби України з надзвичайних ситуацій (ДСНС) недостатньо знаються на тонкощах технологічних процесів і відповідних ризиків. Отже, ситуація, що склалася, вимагає зміни системи управління безпекою, впровадження системи управління більш високого рівня – на основі ризик-орієнтованого підходу (РОП).

В ІПММС НАН України запропоновано таку нову інформаційну технологію управління безпекою (ІТБ) на основі нової концепції РОП, суть якої у попередженні аварій та НС на основі аналізу ризиків [1]. Запропоновано також здійснювати розв’язання задач з оцінювання ризиків аварій і НС у різних галузях виробництва за допомогою типових моделей і спеціальних програм, оснащених зрозумілим для звичайного користувача інтерфейсом [2]. Ця технологія відповідає сучасному тренду тотальної інформатизації суспільства, концепції розвитку системи електронних послуг в Україні, затвердженої Постановою Кабміну № 918-р від 16.11.2016 року, тощо. Але, на жаль, сфера безпеки життєдіяльності має суттєво нижчу інформаційну підтримку ніж, скажімо, торговельні мережі або банківська сфера, що відчуває кожна людина. Тобто пріоритет з інформатизації в Україні виявився не у сфері безпеки, а у сферах, які мають достатню фінансову підтримку.

ISSN 1028-9763. Математичні машини і системи, 2017, № 4

Мета роботи – дослідження проблеми інформатизації сфери безпеки в країні.

2. Аналіз стану впровадження ІТ у сферу управління безпекою України

ІТ сфери безпеки (ІТБ) розуміємо як сукупність інформаційних процесів, які забезпечують автоматизоване управління безпекою. ІТБ включає процеси збору інформації, аналіз ризиків за допомогою моделей безпеки, виводу інформації операторам та особам, що приймають рішення (ОПР). ІТБ використовує сукупність засобів і методів збору, обробки і передачі даних для отримання інформації нової якості про стан об'єктів підвищеної небезпеки (ОПН), небезпечних процесів або явищ. Структура ІТБ наведена на рис. 1, короткий опис у [2]. Вона базується на парадигмі РОП, є цифровою технологією та краще відповідає ринковій економіці, підтримує мінімальне втручання ЦОВВ у бізнес, забезпечує у цілому кращі показники безпеки для персоналу, населення й довкілля. Перехід на сучасну систему вимагає наш європейський вибір [3, 4] і чинне законодавство України.

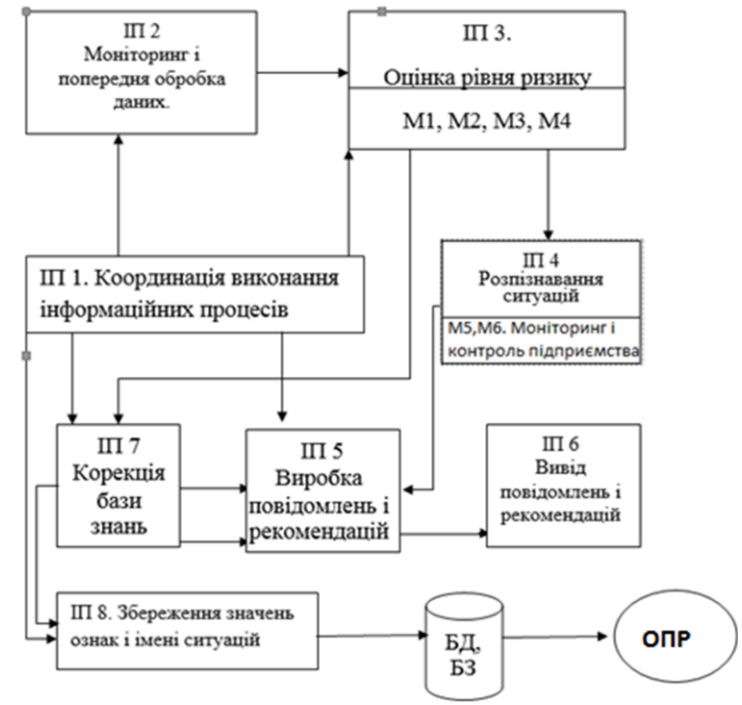

Рис. 1. Структура ІТБ (ІП1-ІП7 –інформаційні процеси, М1-М6-математичні моделі, ОПР – особа, що приймає рішення)

Впровадження парадигми РОП неможливе без використання ІТ, тому що при цьому вже обов'язкове моделювання процесів. Роль парадигми у забезпеченні безпеки представлена на рис. 2. Вона визначає усі процеси. Звичайно ідентифікують чотири парадигми: стовідсотковий контроль (інспекції) безпеки, ризик-орієнтований підхід, культура безпеки та операційний ризик [1]. Кожна парадигма визначає новий, більш високий стан в управлінні безпекою, з більшим аналізом, ширшим впровадженням ІТ. У зв'язку з цим при зміні парадигми неминучі зміни структури органів управління, а саме зменшення органів інспекцій та збільшення аналітиків. Це, у свою чергу, приводить до змін в освіті та інших змін у суспільстві. Тобто, стан системи управління залежить від парадигми та стадії розвитку управління (контролю) безпекою, що можливо представити як на рис. 3. Поняття «стадії безпеки» вводиться для уточнення стану системи управління безпекою. Як це відзначається в доповіді МАГАТЕ [8], у розвитку безпеки можна виділити три стадії, кожна стадія розвитку безпеки відповідає певній філософії безпеки. Вищою стадією розвитку безпеки, безумовно, є третя стадія, яку відносять до парадигм високої культури безпеки та операційного ризику. Визначення стадій розвитку безпеки на ОПН – це завдання аналітиків (контролю, інспек-

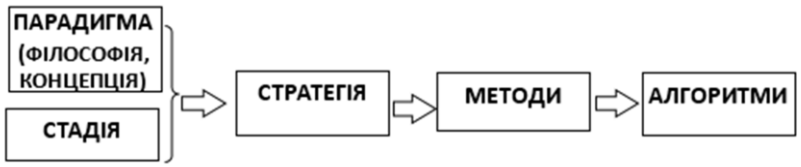

Рис. 2. Інформаційний зв'язок парадигми безпеки, стратегії забезпечення безпеки і методів управління

ції), які мають намір створювати моделі управління безпекою. Тільки парадигми вищого порядку потребують впровадження ІТ. Тобто, перехід на сучасні ІТ у сфері безпеки – ІТБ можливий, якщо відбудуться суттєві зміни у суспільстві, що обумовлені більш високою парадигмою. Парадигма РОП дозволяє провести повну інформатизацію процесів управління і контролю безпеки, може забезпечити їх прозорість та повну інформаційну підтримку ОПР [2]. Це твердження засновано на теорії моделювання процесів безпеки [2, 5–7, 13] та основній відмінності РОП – попередження аварій до їх виникнення на основі аналізу моделей процесів (рис. 1). Дійсно, якщо маємо модель процесу, то відомі її параметри та функціонал залежності ризику R від них:

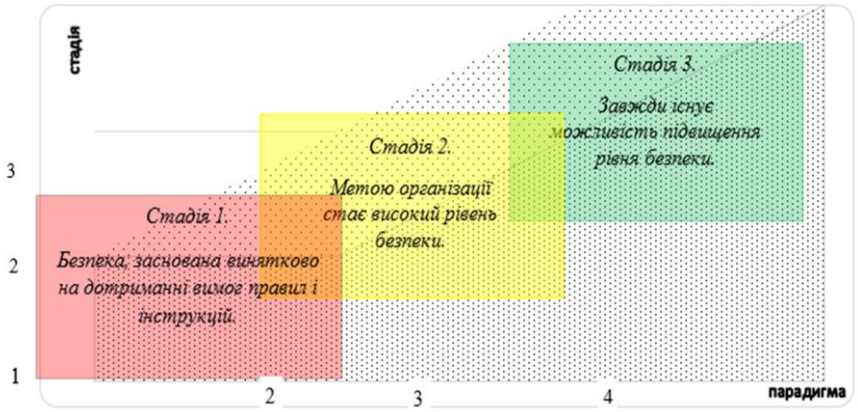

Рис. 3. Схема співвідношень парадигми та стадії розвитку культури безпеки

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

де $x1$ – змінна урахування всіх імовірних сценаріїв аварій для всіх режимів роботи;

$x2$ – змінна, що враховує всі можливі вихідні події, природного характеру тощо;

$x3$ – змінна урахування зношеності основного обладнання та статистики його відмов;

$x4$ – змінна урахування типів захисного обладнання та його стану;

$x5$ – змінна урахування навченості персоналу.

Види залежностей X1-X5 та спосіб їх отримання наведені у згаданих теоретичних працях. У такому випадку задача мінімізації ризику є суто математичною і може бути розв'язана відомими методами, що й дає змогу дати рекомендації ОПР щодо запобігання аварій та НС (рис. 1).

У працях вчених ІПММС [9–11] визначені можливі шляхи таких змін системи управління безпекою. Потрібне не тільки впровадження інформаційних технологій, але й зміна структури органів управління безпекою, причому зміни мають проходити одночасно, тому що проблема багатогранна, має, як мінімум, такі аспекти:

• Інформаційний (головний) – має бути впроваджена інформаційна технологія, що саме і визиває зміни системи управління.

• Політичний – має бути дерегуляція управління, перевага ринковим, економічним методам, а не інспекційним перевіркам.

• Науковий – мають бути розроблені нові методи, моделі, алгоритми, розрахункові програми (коди).

• Соціальний – зміни стосуються кожного громадянина, його безпеки та поведінки у процесах виробництва.

На жаль, жоден із наведених аспектів має на сьогодні небагато реальних можливостей реалізації. Зміни, які відбуваються, дуже повільні. Глобальна причина цього, на наш погляд, криється у нашій ментальності та пережитках минулої соціалістичної реальності. Дійсно, люди – чиновники, які знаходяться при владі, як пишуть усі ЗМІ, не дуже бажають втрачати важелі впливу на бізнес та переходити на прозорі ринкові методи. Добре відомо, що контроль безпеки підприємств, перевірки і є тим важелем впливу – це є корупція. Дуже багато рецептів боротися рекомендовано нам, утворено багато адміністративних структур,

узаконено навіть методологію визначення стану корупції [12], але досягнень мало. Модель, що пропонується в [12], створена системою, вона не може працювати у принципі, відображає тільки сам факт небажаної події, за яким неможливо визначити фактори та обставини, які на це впливають, а без повного розуміння проблему вирішити неможливо. З іншого боку, система не може перейти у принципово новий стан без зовнішніх впливів, не може змінити сама себе – це відома істина.

Що стосується наукового аспекту, то система теж знаходиться у режимі очікування. Повний перелік задач наведено у багатьох наукових працях, у тому числі нещодавніх [13]. У цих роботах розглядаються деякі важливі проблеми, але бачення ІТБ на рівні регіону та держави поки немає. У загальному виді, концептуально, проблема розглядалася навіть на рівні Президії НАНУ [1, 14] ще у 2015 році. Але ж, знову з загальних причин, відсутності фінансування тощо нових наукових робіт у цьому напрямі з'явилося дуже мало. Більш того, деякі публікації з цієї тематики зовсім далекі від реальності, не може бути навіть мови про практичну їх реалізацію. Велике значення для виконання наукових задач у цьому напрямі має освіта. Зараз дуже мало не тільки серед чиновників, але й серед людей з науковим ступенем таких, що знають математичні задачі адаптивного управління випадковими процесами, як того потребує ІТБ. Більшість вважають управління ризиком нісенітницею. Не вчили у минулому, та й зараз не навчають в українських ВНЗ методам управління ризиком. Один із керівників відділу ДСНС сказав з цього приводу: «Ми рятувальники або/чи пожежники. Нас вчили: горить – заливай, хтось тоне – витягуй. Запобігання НС у нашому розумінні – це виконання правил безпеки. Отже, ми й контролюємо, по можливості, виконання правил. Ваші методи (РОП) ми не розуміємо, нас не вчили моделювати та розраховувати ризики». На жаль, ситуація змінилася мало. Але щоб не заважати бізнесу, під впливом «вітрів свободи» з заходу, перевірки заборонили. Тобто, навіть цей дуже неефективний метод першої парадигми не діє, тому й не дивно, що зростає кількість аварій та НС. Як висновок, наукова частина проблеми залишається дуже великою [2, 15], хоча й існують рішення окремих задач. Але ж вона може бути успішно вирішена, запорукою чого є досвід ядерної галузі, де зміна парадигми відбулася на початку 2000 років [2]. Тільки системний підхід, комплексне рішення може принести успіх, причому для різних галузей виробництва повинні бути знайдені свої рішення. Рішення проблем безпеки по галузях виробництва – створення типових галузевих положень і програм управління ризиком вперше запропоновано в [16].

Повинні зрозуміти й довести це до усього нашого суспільства: немає іншого шляху до цивілізованого розвитку у сфері управління безпекою. Тому дуже потрібні як роботи з дослідження моделей небезпечних процесів і систем, так і адаптація вже відомих світових робіт у цьому напрямі до умов України. Наразі в Україні прийнято низку державних стандартів, аналогічних європейським. Один із них – ДСТУ IEC/ISO 31010:2013 «Керування ризиком. Методи загального оцінювання ризику» [17]. У ньому наведено майже два десятки методів (якісних і кількісних), за якими можна оцінювати ризики. Вибір методу та методології мають здійснити фахівці галузі під час розробки галузевих положень з управління ризиком. Ще один добре відомий серед фахівців з безпеки міждержавний стандарт – ГОСТ 12. 3.047.98 наводить велику кількість детерміністичних моделей аварійних процесів. Наприклад, моделювання процесу вибуху легкозаймистої рідини (ЛЗР) на відкритому просторі пропонується проводити за рівнянням:

$$\Delta p = p_0(0,8m_{пр}^{0,33} / r + 3m_{пр}^{0,66} / r^2 + 5m_{пр} / r^3), \qquad (2)$$

де p_0 – атмосферний тиск, кПа;

r – відстань від геометричного центру газопароповітряних хмар, м;

$m_{пр}$ – приведена маса газу або пари, кг.

На основі знань надлишкового тиску Δp за табл. 1 можливо визначити розмір імовірних руйнувань – збиток. За значенням збитку визначаємо ризик:

$$R = P \times U \,, \tag{3}$$

де P – імовірність негативної події (проливу), U – збиток.

Таблиця 1. Наслідки вибухів

Ступінь ураження	Надлишковий тиск, кПа
Повне руйнування будівель	100
50% руйнування будівель	53
Середні пошкодження будівель	28
Помірні пошкодження будівель (пошкодження перегородок, рам, дверей та ін.)	12
Нижній поріг пошкодження людини хвилею тиску	5
Малі пошкодження (розбите засклення)	3

Рис. 4. Алгоритми оцінки ризику вибуху ЛЗР

Тобто, можна простежити алгоритм оцінки ризику за моделлю (2) (рис. 4).

Декілька слів стосовно першого кроку алгоритму. Якщо подія (розлив) вже відбулася, розрахунок потрібен рятувальникам. На етапі проектування об'єкта або декларування безпеки потрібна модель визначення ймовірності розгерметизації обладнання. Для цього необхідно моделювати рівень надійності, точніше, ймовірність відмов систем захисту як виробництва в цілому, так і конкретного обладнання (апріорну інформацію можна знайти у базах даних), а також рівень підготовки персоналу (для цього існують спеціальні методики). Далі слід визначити ризики для населення (техногенна безпека) і довкілля (екологія), тобто ризик визначається за умови моделювання в усіх сферах безпеки, якщо слідувати за алгоритмом рис. 4. Для цього створюється робоча група з кількох експертів, компетентних у сфері дослідження. До її складу повинні увійти представники галузі і самого підприємства, а також фахівець з ІТ з програмним забезпеченням та методикою розрахунків, який вміє моделювати ситуації (процеси та системи). До речі, він – єдиний «універсальний» фахівець і може працювати у складі групи будь-якої галузі. Вони аналізують процеси виробництва, ідентифікують ризики, потім за результатами аналізу та розрахунків разом розробляють рекомендації щодо запобігання небезпеки. Це досвід ядерної галузі.

За сучасними можливостями ІТ для користувача (споживачів інформації) необов'язкове знання методів моделювання та ПЗ, може бути створений виразний та зрозумілий інтерфейс (рис. 6).

Отже, стандарт ГОСТ 12.3.047.98 дає можливість достатньо просто моделювати проливи небезпечних речовин, вибухи й загоряння у приміщеннях та на відкритому просторі, знаходити зони ураження для персоналу і населення. На превеликий жаль, жоден із згаданих стандартів не знаходить застосування в офіційно затверджених методиках в Україні. Дуже обмежено й застосування ГОСТ (ДСТУ) 27.310-95 [20]. Хоча й існує низка нормативно затверджених методик визначення ризику небезпечних процесів (корупції [12], тощо), відносити до ІТ ці методики неможливо.

Інститути НАНУ здатні забезпечити моделювання усіх небезпечних процесів й усі процеси інформатизації сфери безпеки на сучасному світовому рівні [1, 14]. Але у сфері безпеки життєдіяльності, не зважаючи на наведене вище, фактично існуючу методику [18] та, навіть, Укази Президента України практичної реалізації інформаційної підтримки ОПР як для запобігання, так і під час ліквідації наслідків НС не існує. Причиною цього, крім небажання ДСНС переходити на нову парадигму [19], на наш погляд, є відсутність знань зв'язків існуючих моделей процесів управління безпекою, тобто, відсутність цілісного уявлення процесів.

Отже, створення комплексу моделей з безпеки галузі – необхідна умова створення ІТБ. Розглянемо деякі вимоги та особливості таких моделей. У першу чергу, має вирішуватися питання щодо типу моделей: якісна – кількісна, детерміністична – імовірнісна, імітаційна та ін. Питання далі: який метод має бути використано для моделювання, невизначеності методу та спосіб їх оцінок, точність та адекватність моделі. Стосовно моделювання процесів безпеки в Україні потрібно додатково висунути ще одну обов'язкову вимогу – компетентність автора щодо безпеки. Так, у світовій практиці ядерної галузі є вимоги до експерта (фахівця): вища спеціальна освіта, досвід роботи за напрямом і ліцензія або науковий ступінь. Але ж у більшості випадків інших галузей в Україні це ігнорується, що підтверджується наведеними прикладами некомпетентних методичних розробок. А це ще більша небезпека, ніж помилка фахівця чи, навіть, уся небезпека, що моделюється. Наслідком некомпетентної моделі є омана, що може призвести до катастрофи. До речі, катастрофа на ЧАЕС розпочалася з програми «випробувань», розробленою «науковцями» інституту з Донецька (Донтехенерго).

Другим важливим питанням щодо моделей з безпеки є вибір методології та методу. Як вже було сказано, часто при виборі методики рекомендують метод FMEA ((Failure Mode and Effects Analysis) або у перекладі «аналіз видів відмов та їх наслідків – АВВН» [20]), що не завжди правильно. Методика оцінки ризику корупції [12], яка базується на цій методології та офіційно затверджена ще у минулому році, але не використовується, на наш погляд, саме з цієї причини – недосконалості методу. Метод FMEA частіше використовується як метод попереднього (якісного) аналізу, щоб визначити ризики категорій «А» та «В» з метою їх подальшого аналізу іншим методом. Ще одним недоліком згаданої методики є невелика кількість градацій ризику – усього три діапазони, що навіть не відповідає стандарту [20]. Помилка вибору методології та спрощення методу призвело до унеможливлювання її практичного застосування і, як наслідок, потреби нової розробки. До речі, на наш погляд, кожна сучасна офіційна методика має бути представлена з програмним забезпеченням (ПЗ), чого немає у наведених прикладах. Неможливо зробити адекватні оцінки за цією методологією, дуже великі невизначеності отримуємо у підсумку, що зводить нанівець весь аналіз. Отже, при виборі типу моделі стосовно методу FMEA може бути така рекомендація: цього аналізу достатньо, якщо результатом є знехтуваний або малий ризик, інакше потрібен більш детальний аналіз.

Також, дуже важливим є питання вибору типу методу моделювання: детерміністичний – ймовірнісний. Помилки цього типу можуть мати також фатальний наслідок, тому що дуже просто й непомітно губиться адекватність моделі. У згаданому ГОСТ 12.3.047, на основі світового досвіду зібрані найбільш адекватні моделі вибухонебезпечних процесів.

Усі моделі детерміністичні, легко перетворюються у відповідне ПЗ, адекватність перевірена світовим досвідом. До речі, для більшості моделей цього стандарту за прикладом рис. 6. ПЗ розроблено як для систем Windows, Linux, так й для Android. Скажімо, наслідки розливу цистерни небезпечної речовини є можливість вже зараз порахувати як на стаціонарних комп'ютерах, так і на смартфонах.

Коли більшість подій, що характеризують процес, мають стохастичну природу, прийнято проводити аналіз ризиків на основі ймовірнісної моделі. Ймовірнісні моделі та ймовірнісний аналіз безпеки (ІАБ) широко й порівняно давно використовуються у моделюванні безпеки складних систем, АЕС тощо [21]. Моделювання технічних систем, навіть таких складних систем, як АЕС, дещо простіше, ніж соціальних [22], оскільки порівняно легко прослідити вплив кожної події (відмови) на роботоздатність кожної підсистеми, в яку входять елементи, що моделюються. Ця обов'язкова процедура ймовірнісного моделювання звичайно виконується за допомогою згаданого методу FMEA. Процедура FMEA у цьому випадку – це якісний аналіз системи, що застосовується для визначення «впливових» подій, які обов'язково мають бути включені в імовірнісну модель, тобто у цьому випадку це попередній аналіз. Таким чином, питання вибору елементів системи для моделювання – наступний відповідальний крок моделювання систем безпеки. Використання методу FMEA – це один із способів розв'язку проблеми. У термінології ІАБ йдеться про базисні події (БП) – основу моделей ІАБ [21]. Вибір моделей саме БП – наступна задача ймовірнісного моделювання. Велике значення для ймовірнісних моделей має статистика, на основі якої створюються саме моделі БП, визначається їх елементарна статистика: математичне очікування, закон розподілу, дисперсія тощо. Для моделей безпеки технічних систем важливо враховувати світовий досвід, тобто використовувати байєсовські оцінки як апостеріорні.

Моделювання помилок людини – оператора (виконавця), помилок колективних дій, очевидно, теж необхідне для створення моделей з безпеки. За даними звітів з безпеки, до 80% причин усіх аварій та НС – це помилки людини. Для моделювання можливих помилок людини (людський чинник – ЛЧ) в імовірнісних моделях технічних систем звичайно використовується широко відома у техніці методологія THERP (Technique for Human Error Rate Prediction). Оскільки ця методологія призначена для технічних систем, то у роботах з моделювання інших систем роблять такі припущення: 1) імовірність базової помилки (Human Error Probability – HEP) фахівця високої кваліфікації (вища спеціальна освіта, достатній досвід) має порядок: $P = 1 \cdot 10^{-3}$ та 2) помилки досвідчених фахівців у різних сферах діяльності відбуваються за схожими сценаріями. Підсумкова ймовірність помилок залежить від інших факторів та обставин, як то: складність задачі, достатність часу, ергономіка робочого місця, рівень стресу та ін. [21]. Імовірність колективної помилки при роботі у бригаді також має моделюватися, що можливо за методологією THERP. Імовірності усіх подій, що враховуються у моделі, розраховуються на основі статистичних даних об'єкта, який моделюється, з урахуванням типу їх розподілу. Існують й інші методи моделювання ЛЧ, наприклад, на основі дерева рішень та ін. Вибір методу залежить від типу об'єкта та компетенції автора моделі. При цьому вітчизняної методики не існує, хоча і є вимога нормативних документів [18] обов'язковості моделювання ЛЧ. Вітчизняного ПЗ для моделювання складних систем імовірнісними методами теж не існує, як й ПЗ моделювання ЛЧ. Тобто, задач моделювання систем безпеки ще достатньо. З вищенаведеного зробимо висновок про складність моделювання безпеки та велику кількість невирішених науково-практичних проблем. Автором, як вихід, запропоновано створення типових моделей за галузями виробництва [23].

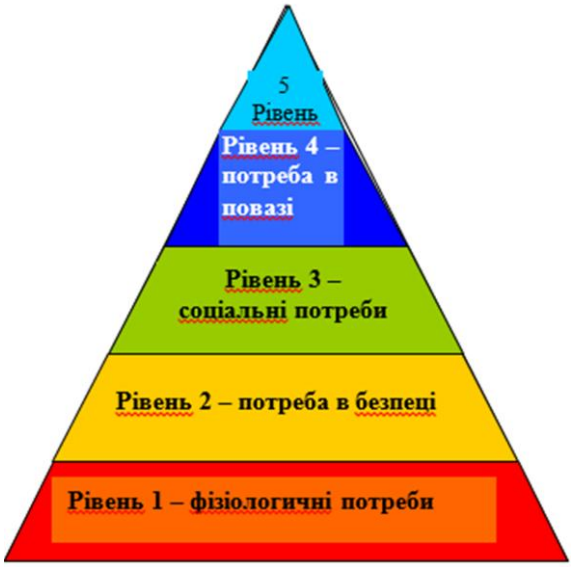

Рис. 5. Піраміда Маслоу – ієрархія потреб людини (Фізіологічні потреби знаходяться в основі піраміди, потреба в безпеці займає другі рівень, 3 рівень – соціальні потреби, 4 – потреба в повазі, 5 – духовні потреби. Рівні 1 та 2 – первинні, 3-5 –вторинні. В першу чергу повинні бути задоволені первинні рівні. При їх незадоволенні відпадає потреба в задоволенні вищих рівнів)

Створення типової моделі дає можливість істотно спростити розрахунки ризиків для конкретних ОПН; здійснювати моніторинг поточного ризику об'єкта на основі такої моделі методом контроля поточних значень важливих параметрів. «Важливість» теж визначається з моделі за Фуселом-Веселі, Бірнбаумом чи коефіцієнтами зміни ризику. На основі типової моделі можлива розробка методики визначення ризику та відповідного ПЗ. Моделі повинні створювати провідні інститути НАН разом з фахівцями відповідних галузей виробництва.

Соціальний аспект впровадження ІТБ визначається впливом процесу зміни парадигми на життєдіяльність. Доречно згадати піраміду А. Маслоу (рис. 5) – безпека є фундаментальною потребою людини. За концепцією РОП, оцінка ризиків повинна бути для персоналу, населення та довкілля. Кожен працівник має бути поінформований щодо рівня небезпеки на своєму робочому місці, а господар зобов'язаний застрахувати життя та здоров'я працівника. Якщо має місце підвищений рівень ризику, це міжнародні вимоги. Але в Україні і досі не розроблено відповідних норм, тому й оцінюють ризики, здебільшого, за якісними шкалами.

А ризик-орієнтований підхід базується, передусім, на кількісних покажчиках. Причому, цифрові покажчики для визначення ступенів прийнятного ризику мусить сформулювати (визначити) держава. Наприклад, в європейських стандартах МООЗ чітко прописано: якщо ризик на якомусь підприємстві передбачає загибель п'яти осіб на 10 тисяч населення ($R > 5*10^{-4}$), він вважається неприпустимим. Підприємство отримує дозвіл на роботу лише тоді, коли мінімізує загрозу і сплатить солідний страховий внесок.

Але, оскільки припустимі рівні ризику в Україні не встановлені, то й наступні кроки впровадження РОП та ІТБ не можливі. В [16] пропонується на перших етапах впровадження ІТБ визначати прийнятні рівні по галузях виробництва з наступним їх зближенням, оскільки на сьогодні вони дуже різні, відрізняються на порядки. Це теж наукова задача, здебільше економічна та соціальна. Європейські норми для нас поки що недосяжні, але ж довго бути на низьких рівнях безпеки не можна.

Стосовно інформаційного аспекту впровадження РОП, крім наведеного, розглянемо інформаційне забезпечення служб з безпеки, ДСНС тощо. Стан цієї проблеми в Україні не відповідає сучасним вимогам та можливостям ІТ, адже він є вкрай застарілим. З найбільш прогресивних за європейською допомогою (PPRD) впроваджується атлас ризику [24]. У його сучасному стані інформація про усі регіони України представлена форматами doc, excel, pdf згідно з адміністративним розподілом. Можна отримати інформацію про усі підприємства, будівлі, дороги, річки, мости, населення, про все, крім ризику. Зрозуміло, це корисна інформація і на її основі можна створити ПЗ з інтерактивними функціями на основі ГІС-технологій. Це теж задача впровадження ІТБ. Ще в ЦОВВ існують БД про стан техногенної (аварії та НС) та пожежної безпеки. Ці БД також створені у форматі excel і ве-

дуться біля 20 років, тобто є достатня статистика з безпеки. Інформація представлена достатньо деталізовано, БД містять біля 40 полів: дати, місто, час, власник, короткий опис, збитки, причини та ін. Стосовно «причин» можуть бути неточності (невизначеності) з причин відсутності попереднього системного аналізу. БД мають статус обмеженого доступу, інформація з них може бути надана за запитом керівника або навіть за гроші, що також протирічить світовому досвіду. На сучасному рівні ця проблема може бути вирішена на основі технології «Blockchain», а це також задача впровадження ІТБ. БД та база знань мають бути реалізовані на архітектурі таблиць реляційної бази, збережених процедур для обчислень і звітності, наприклад, MS SQL-база та T-SQL-мова (PostgreSGL – http://www.postgresql.org/ about/news/1481/).

З практичної точки зору, існують пропозиції рятувальників щодо впровадження сучасних ІТ, але поки що у ДСНС немає на це потрібних ресурсів. Як першочергові об'єкти для інформатизації називають систему прийняття виклику, розподілу сил і засобів за викликом з відображенням на планшеті; відображати об'єкт, планування, під'їзди, гідранти і ін. засоби ліквідації тощо; оцінювати (розраховувати) необхідні ресурси; готувати план дій, картку гасіння пожежі; мати на пожежній машині відеокамеру з можливістю управління нею з пульта диспетчера.

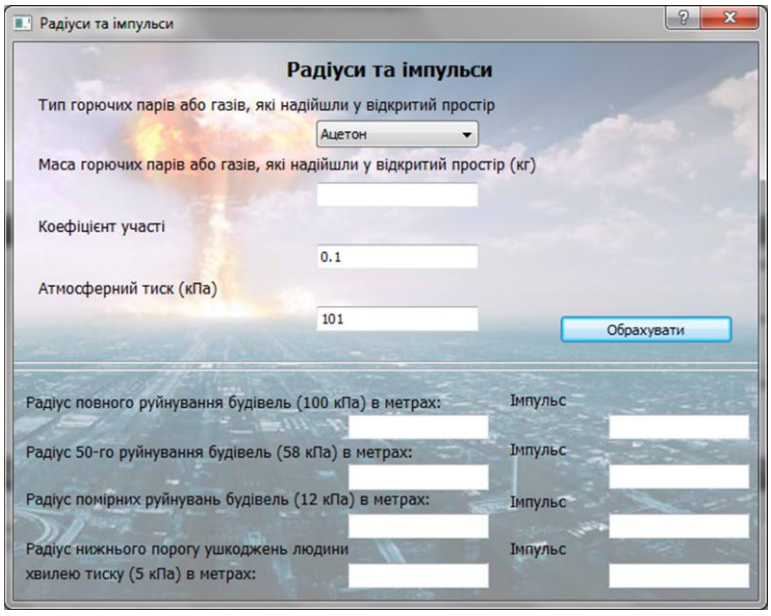

Рис. 6. Сторінка розрахунків радіусів руйнувань при вибухах на відкритому просторі горючих парів або газів

Важливим питанням є постановка вимог до програмного забезпечення. Коротко їх можна сформулювати так: сучасні мови програмування (Java або C#), інтуїтивно зрозумілий інтерфейс, лаконічний дизайн, рішення завдань у реальному часі, ГІС-технології. Приклад інтерфейсу програм розрахунків за рівнянням (3) наведено на рис. 6. Вхідні дані: тип ЛЗР, її кількість та погодні умови, вихідні: радіуси зон ураження та руйнівні імпульси.

Апаратна реалізація ІТБ на сучасному стані також може бути значно простіша, ніж наші нещодавні уявлення про АСУ ТП чи АСУ. Сенсори, необхідні для визначення рівня небезпеки на підприємстві, які збирають інформацію щодо різних параметрів фізичного середовища на підприємстві, стали значно простіше, дешевше та більш універсальні. Прикладом таких пристроїв може бути мінікомп'ютер Raspberry PI для обчислень і зв'язку з центральним сервером і мікроконтролер Arduino для взаємодії з сенсорами (існує великий перелік сенсорів для цього мікроконтролера http://arduino.ua/ru/hardware/) (рис. 7).

Як обчислювальний блок підійде будь-який мінікомп'ютер, можливо, модульний, здатний виконувати прості скріптові програми, мати стабільне з'єднання з сенсорами і інтернетом як за допомогою кабельного, так і бездротового з'єднання.

Бажано також, щоб вартість такої техніки була не надмірно великою, адже для забезпечення безпеки та релевантності таких наборів (обчислювальний блок, сенсори, з'єднання з інтернет) має бути мінімум два в різних частинах зони підвищеної небезпеки підприємства.

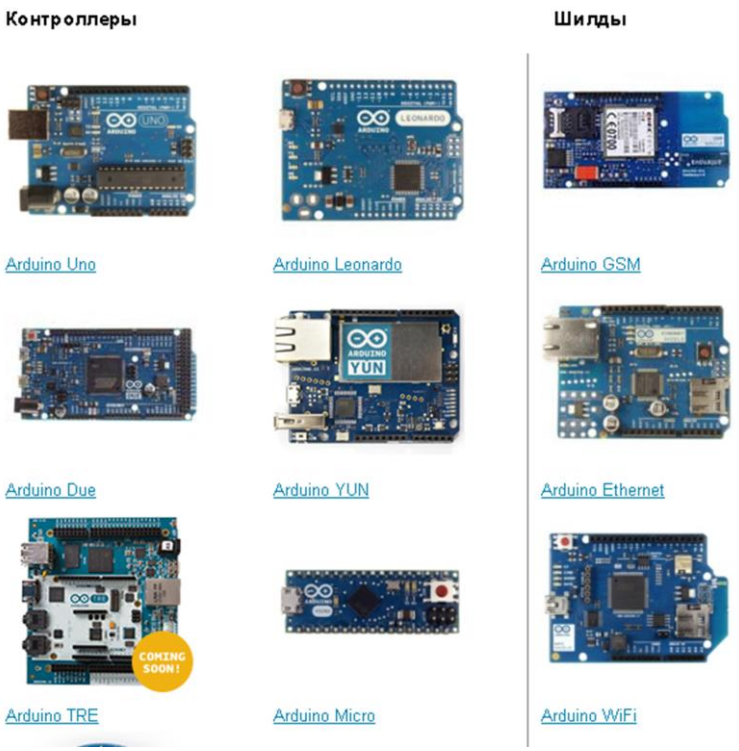

Рис. 7. Пристрої системи Arduino

Звичайно, питання програмування під Arduino вимагає більш детального дослідження, можливе залучення досвідчених фахівців, але в мережі Інтернет є багато довідників та інструкцій. В цілому Arduino вважається найпростішим мікроконтролером для початківців, при цьому його функціональність майже не обмежена. Для зв'язку з центральним сервером досить мінімального мережевого обладнання та доступу в мережу. Для резервного доступу можна використовувати 3G модем будь-якого українського оператора зв'язку. У такому варіанті приблизний кошторис на одне підприємство близько 150 доларів, що спростовує міфи про занадто велику вартість впровадження ІТ.

3. Висновки

1. Стан впровадження ІТ у сферу безпеки є дуже низьким, не відповідає сучасним можливостям ІТ та потребам суспільства.
2. Існуюча інформація з безпеки у ЦОВВ є достатньою для впровадження ІТБ, вона може бути успішно використана на основі світового досвіду, досвіду ядерної енергетики та описаних розробок для створення відповідних методик управління ризиком.
3. Перехід на більш високий рівень інформатизації можливий разом зі зміною парадигми безпеки, що має відбутися як умова входження України в Євросоюз.
4. Процеси інформатизації простіше здійснювати за галузями виробництва на основі створення типових моделей та визначення галузевих інформаційних критеріїв безпеки, припустимих рівнів ризику тощо.
5. Зміна програм освіти з безпеки – необхідна умова при наступних змінах парадигми та впровадження ІТБ.
6. Потрібна зміна чинного законодавства, законодавче поле має бути таким, щоб власник усіма своїми активами відповідав за безпеку об’єкта і персоналу, тоді не держава, а саме власник активно впроваджуватиме РОП.
7. Потрібно скористатися світовим досвідом та досвідом ядерної галузі України, впроваджувати у практику управління світові стандарти та скористатися європейською допомогою на дерегуляцію на користь впровадження ІТБ в Україні.

СПИСОК ЛІТЕРАТУРИ

1. Морозов А.О. Наукові основи впровадження ризик-орієнтованого підходу в управлінні техногенно-екологічною безпекою / А.О. Морозов // Вісник НАН України. – 2015. – № 8. – С. 24 – 32.
2. Бєгун В.В. Впровадження інформаційних технологій у сферу безпеки / В.В. Бєгун // Науково-технічна інформація. – 2016. – № 1. – С. 40 – 46.
3. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру. Розпорядження Кабінету Міністрів України від 22.01.2014 № 37-р [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/37-2014-%D1%80.

4. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/984_011.
5. Белов П.Г. Теоретические основы менеджмента техногенного риска: автореф. дис. на соискание научн. степени докт. техн. наук: спец. 05.26.03 «Пожарная и промышленная безопасность» / П.Г. Белов. – М., 2007. – 33 с.
6. 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.
7. Бєгун В.В. Розробка методів управління техногенною безпекою міста на основі імовірнісних структурно-логічних моделей небезпек виробництв: автореф. дис... канд. техн. наук: 21.06.01 / Бєгун В.В.; Нац. акад. наук України, Ін-т пробл. моделювання в енергетиці ім. Г.Є. Пухова. – К., 2007. – 20 с.
8. Развитие культуры безопасности в ядерной деятельности: доклады по безопасности. – Вена: МАГАТЭ, 2000. – № 11. – 24 с.
9. Бєгун В.В. Щодо питань про сучасні методи регулювання безпеки / В.В. Бєгун, В.Ф. Гречанінов, В.П. Клименко // Математичні машини і системи. – 2013. – № 4. – С. 135 – 146.
10. Морозов А.О. Інформаційно-аналітичні технології підтримки прийняття рішень на основі регіонального соціально-економічного моніторингу / А.О. Морозов, В.Л. Косолапов. – К.: Наукова думка, 2002. – 347 с.
11. Морозов А.О. Управління безпекою в епоху інформаційного суспільства / А.О. Морозов, В.Ф. Гречанінов, В.В. Бєгун // Вісник НАН України. – 2015. – № 10. – С. 34 – 41.
12. Методологія оцінювання корупційних ризиків у діяльності органів влади. Затв. рішення Національного агентства з питань запобігання корупції 02.12.2016 р., № 126; зареєстр. у Міністерстві юстиції України 28.12.2016 р., № 1718/29848.
13. Лифар В.О. Моделі, методи та інформаційні технології оцінки техногенного ризику об'єктів підвищеної небезпеки: дис. … д-ра техн. наук. – Миколаїв, 2017. – С. 21
14. Постанова НАН України «Впровадження ризик-орієнтованого підходу в управління безпекою» від 17.06.2015.
15. Кропотов П.П. Створення сучасної системи моніторингу безпеки – актуальна державна та наукова задача / П.П. Кропотов, В.В. Бєгун, В.Ф. Гречанінов // Системи обробки інформації. – 2015. – Вип. 11 (136). – С. 199 – 206.
16. Галузеве керівництво з розробки та реалізації політики управління ризиками / В.В. Бєгун, В.Ф. Гречанінов, В.П. Клименко [та ін.] // Пожежна та техногенна безпека. – 2016. – № 6. – С. 32 – 33.
17. ИСО/МЭК 31010:2009 (ISO/IEC 31010:2009). Управление рисками: методики оценки потенциальных рисков (Risk management – Risk assessment techniques).
18. Методика визначення ризиків та їх прийнятних рівнів для декларування об'єктів підвищеної небезпеки. Нормативне виробничо-практичне видання. Держнаглядохоронпраці. – К.: Основа, 2003. – 191 с.
19. Бєгун В. Основне призначення РОП – підтримувати ризики небезпечного об'єкта на прийнятному рівні / В. Бєгун // Пожежна і техногенна безпека. – 2017. – № 3. – С. 19 – 21.
20. ГОСТ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.
21. Вероятностный анализ безопасности атомных станций / В.В. Бегун, О.В. Горбунов, И.Н. Каденко [и др.]. – К.: Випол, 2000. – 558 с.
22. Концепція освіти з безпеки / В.О. Кудін, В.В. Бегун, В.Ф. Гречанінов [та ін.] // Теорія і практика управління соціальними системами: філософія, психологія, педагогіка, соціологія. – 2015. – № 3. – С. 33 – 44.
23. Бєгун В.В. Метод решения проблемы расчета техногенных рисков / В.В. Бегун, С.А. Вахнин // Управляющие системы и машины. – 2014. – № 3. – С. 3 – 9.
24. PPRD East 2 в Україні [Електронний ресурс]. – Режим доступу: http://pprdeast2.eu/en/strany-partnery/ukraine/.

Стаття надійшла до редакції 23.11.2017