Журнал обчислювальної та прикладної математики **2022, № 2** Journal of Numerical & Applied Mathematics

УДК 004.02[004.9:614.8.084]

MSC 97U10

IMPLEMENTATION OF DIGITAL MANAGEMENT IN THE SECURITY FIELD

V. V. Begun

Institute of Mathematical Machines and Systems Problems of the Ukraine National Academy of Science, Kyiv, Ukraine, E-mail: begunw@ukr.net

ВПРОВАДЖЕННЯ ЦИФРОВОГО УПРАВЛІННЯ У СФЕРУ БЕЗПЕКИ

В. В. Бєгун

Інститут проблем математичних машин і систем НАН України, Київ, Україна, E-mail: begunw@ukr.net

Abstract. The implementation of information technologies in Ukraine in the field of security and the state of education in this direction were studied. A comparison of the degree of informatization in this field and education in this field with developed countries in the nuclear field is made. The problems and tasks of teaching the direction of digital management in the field of security and the main method of modeling dangerous systems and processes — probabilistic structural and logical models — are analyzed. Conclusions were made about the need for more widespread education in the applied field of security, formulation and solution of actual problems, creation of special software.
Keywords: applied problems, security, risk, information technologies, probabilistic modeling.

Анотація. Досліджено впровадження інформаційних технологій в Україні у сфері безпеки та стан освіти цього напряму. Зроблено порівняння ступеня інформатизації у цієї сфері та освіти у цій сфері з розвинутими країнами у ядерній галузі. Аналізуються проблеми та задачі навчання напряму цифрового управління у сфері безпеки та основний метод моделювання небезпечних систем та процесів — ймовірнісні структурно-логічні моделі. Зроблено висновки про необхідність більшого поширення навчання у прикладній сфері безпеки, постановці та рішенню актуальних задач, створення спеціального програмного забезпечення.
Ключові слова: прикладні задачі, безпека, ризик, інформаційні технології, ймовірнісне моделювання.

Вступ

Роботи І. І. Ляшка присвячені розв'язанню складних науково-практичних задач. Створення їм факультету кібернетики, постановка вивчення курсів прикладної математики та моделювання складних систем, як і все життя, скеровані на те щоб надати максимальну підтримку своєї державі у її науковому та цивілізаційному розвитку. На жаль, ці добрі справі не завжди знаходять сучасного продовження у важливих сферах життєдіяльності. Ми пишаймося тим, що випускники математичних та кібернетичних факультетів університетів України працюють в іноземних компаніях, багатьох університетах світу. Так, це свідчить про достатньо високий рівень навчального процесу, але фактично ми готуємо персонал для розвинутих та багатих країн, забуваючи про потреби нашої країни. Отже дуже важливі сфери життєдіяльності держави залишаються без наукової підтримки. Це, в першу чергу стосується сфери безпеки та військової сфері [2–4] . Можна навісти ступень інформатизації суспільства в Україні за спадом: банківська сфера, торгівля, освіта, ІТ індустрія, ядерна енергетика, авіаційний транспорт, комунальне господарство, сфера безпеки, військова сфера. Як бачимо інформатизація присутня там де є гроші. Але у сфері безпеки це призводить до корупції, у військової до необхідності просити допомоги у розвинутих країнах. (де працюють наші випускники). Як довело життя, потрібно різко змінювати (відновлювати) ситуацію. Отже розглянемо сферу безпеки.

Постановка задачі

Коротко про суть проблеми. В наукових працях дослідників країни, дисертаціях та дипломних роботах студентів та аспірантів дуже мало праць не тільки про рішення складних прикладних задач цього напряму, але навіть майже відсутні роботи з їх постановкою. Не впроваджені передові світові технології управління безпекою на основі ризик-орієнтованого підходу (РОП) та стандарти Євросоюзу цього напряму [2–4]. Державний нагляд за безпекою відбувається до цього часу по-старому, методами інспекційного надзору, як в радянські часи. Саме тому проблеми досліджень з безпеки полягають у необхідності створення нових моделей, методів, алгоритмів контролю та управління техногенною безпекою й аналізу можливості застосування існуючих із метою одночасного врахування багатьох факторів, у тому числі людського чинника та зовнішніх впливів, для отримання у зручний спосіб коректних результатів щодо абсолютної величини та невизначеності ризику від складних об'єктів, якими є потенційно небезпечні об'єкти (ПНО). Це суто задачі прикладної математики.

Одним із підходів до вирішення цих проблем є підхід, заснований на формалізації процесів на основі інформаційної технології. Він передбачає розробку структури нової сучасної інформаційної технології безпеки (ІТБ) з визначенням інформаційних процесів та функцій, розробку відповідних математичних моделей, методів адаптації загальних математичних моделей

до конкретних об'єктів, методів управління безпекою, критеріїв прийняття рішень та методів оцінки ефективності, розробку вимог до структури та наповнення відповідних бази даних (БД) та бази знань (БЗ), розробку вимог до програмного забезпечення, включаючи вимоги до інтерфейсу користувача [1].

Опис проблеми з боку освіти

До надзвичайних ситуацій та аварій на небезпечних виробництвах призводять колективні помилки, що є наслідками неготовності до роботи з небезпечними технологіями. Звісно для їх запобігання потрібне навчання. Але, це робилося (й робиться) у нас в недостатній мірі, за що й платимо дуже велику ціну, див. таблицю:

Показник готовності	**Україна**	**США**
Пуск перших блоків	1972 р	1960 р
Повний аналіз безпеки АЕС	ВАБ-1 - 2002-2005	1975 р (WASH-1400, Rasumussen's)
Підготовка спеціалістів АЕС	ОПІ - 1980 Кафедра АЕС «КПІ» -1986	1960
Методика аналізу помилок людини-оператора	(THERP) – застосовується з 2000 р	THERP – 1970, NUREG/CR-1278 -1982
Вивчення безпеки як предмета	КПІ - 1996	З 1980 р – все технічні ВНЗ

Як бачимо, середнє відставання від США навіть у найбільш сучасній галузі України — ядерній енергетиці складає біля 30 років. Тобто наші проблеми з безпеки — це проблеми освіти. Отже у США підготовку спеціалістів для ядерній галузі почали за 12 років до пуску першого атомного енергоблоку, у нас на 8 році після початку експлуатації та після аварії на ЧАЕС у 1986 році. Така ж ситуація і з впровадженням загальноєвропейських стандартів з управління безпекою. Мова в першу чергу про стандарти, що нормують якісні оцінки ризику (процедура FMEA — ДСТУ 27.310-95) та кількісні оцінки — IEC/ISO 31010:2009 — методи загального оцінювання ризику (ДСТУ-2013 р.) та інші. Незважаючи на їх існування державною мовою, вони не застосовуються з причин відсутності інформаційної підтримки, програмного забезпечення тощо [1, 7, 8].

Моделювання процесів управління в військовій сфері мало бути відповідати стандартам НАТО, наприклад, NATO STANDARD AAP-48, NATO System Life Cycle Processes. Цей стандарт вимагає оцінок ризиків різного походження на кожному етапі життєвого циклу, чого звісно не було й не має. Аналогічна ситуація була й з впровадженням сучасних систем управління на основі інформаційних технологій, вони теж відсутні з причин відсутності інформаційної підтримки та програмного забезпечення.

Огляд основних методів та принципів.

Головним, найбільш поширеним методом розв'язання цих задач є метод ймовірнісного аналізу безпеки (ІАБ) - probabilistic security analysis (PSA), що знайшов широке поширення у світі та застосування і в нашій державі для аналізу безпеки АЕС (за вимогами МАГАТЕ). Суть цього методу викладено в багатьох виданнях, та вивчається в Україні з 1996 року на кафедрах АЕС НТУУ "КПІ"та ОПІ. Але, відомо, що аналогічні курси в розвинутих країнах, США тощо, вивчаються в усіх ВНЗ технічного спрямування [9].

Отже, дуже коротко суть методу. Для моделювання небезпечних процесів на ПНО пропонується використовувати ймовірнісні структурно-логічні моделі (ЙСЛМ) з відповідним математичним апаратом. Модель представляється сукупністю дерев відмов (ДВ) та дерев подій (ДП), які являють собою слабкозв'язні зважені орієнтовані графи без циклів. Ваги ребер цих графів визначаються на основі величин ймовірності базисних (у випадку ДВ) подій чи ймовірності відмов систем безпеки (у випадку ДП). Вершини цих графів за допомогою розташованих у них логічних елементів та відповідних логічних операцій булевої алгебри на основі теорії ймовірностей, визначають внесок відповідних ребер у формулу розрахунку величини ймовірності кінцевого стану (КС) (у випадку ДП) чи у формулу розрахунку величини ймовірності відмови системи захисту (у випадку ДВ).

Сукупність побудованих графічних структур у вигляді ДП та ДВ називаємо ймовірнісною структурно-логічною моделлю об'єкта. Кожна ймовірнісна модель цього типу описує певний ідеалізований досвід (чи спостереження).

Враховуючи значні витрати часу на побудову ЙСЛМ, потрібен критерій, за яким визначатиметься необхідність створення ЙСЛМ ПНО для проведення кількісних оцінок ризику. Таким критерієм є процедура якісного аналізу ризику АВВН (FMEA).

Мінімальні перерізи — це множини ймовірного збігу подій у ДВ, що призводить до небажаної події.

Ймовірність i-го мінімального перерізу (C_i) у ДВ розраховується за формулою

$$C_i = q_1 \cdot q_2 \cdot ... \cdot q_n,$$

де q_k — ймовірність k-ї базисної події (БП) в i-му мінімальному перерізі (МП). Для розрахунку ймовірності верхньої події у дереві відмов (S) можливо використовувати різні підходи у залежності від складності побудованого ДВ. Але у більшості випадків, коли ДВ містять лише AND та OR логічні елементи, розрахунок проводиться за оціночною формулою (верхня границя):

$$S = 1 - \prod_{i=1}^{m} (1 - C_i),$$

де m — кількість мінімальних перерізів у дереві відмов. Основні кроки алгоритму моделювання:

– Визначення вражаючих факторів небезпек та можливих кінцевих станів.
– Побудова імовірнісної моделі об'єкту — ДП, ДВ.
– Розрахунок імовірності небажаних подій. Генерація мінімальних перерізів (Min Cat).
– Аналіз значимості (важливості) (Ratio Importance).
– Аналіз чутливості (Sensitivity).
– Визначення подій що найбільш впливають на ризик.
– Розробка плану модернізацій чи покращення стану об'єкту.

Ефективність алгоритму демонструє Рис. 1, де зображено зміну основного розрахункового показника небезпеки АЕС — частоти плавлення активної зони (ЧПАЗ) завдяки заходам з безпеки, які розроблялися на основі проведення ІАБ для першого в Україні енергоблоку АЕС. Атомній блок став безпечніше майже на порядок! Достовірність розрахунків, їх експертизу проводять фахівці міжнародних компаній.

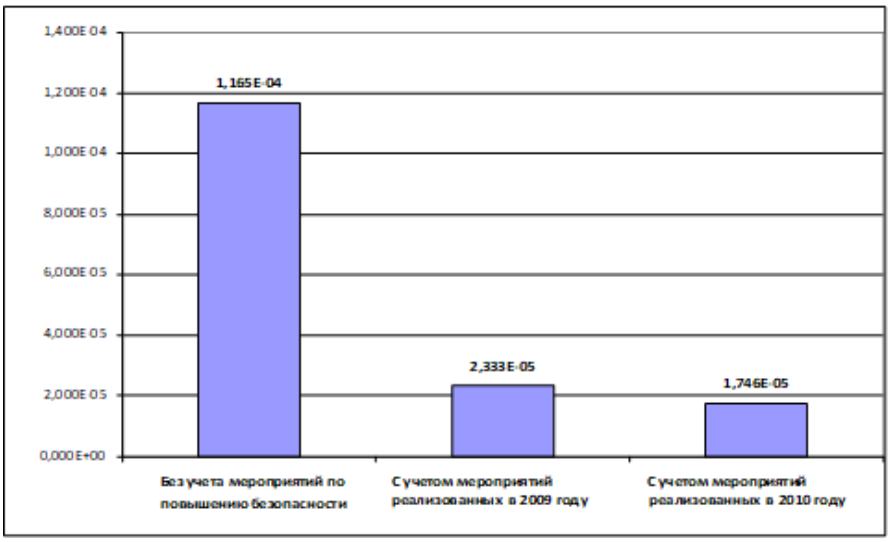

Рис. 1. Вплив на інтегральне значення ЧПАЗ заходів щодо підвищення безпеки для 1-го енергоблоку РАЕС.

Отже, коротко наведемо етапи управління ризиком, які мають бути забезпечені інформаційною технологією безпеки (ІТБ):

– планування управління ризиками,
– ідентифікація ризиків,
– якісна оцінка ризиків,
– кількісна оцінка ризиків,
– планування реагування на ризики,
– реалізація прийнятого рішення,
– мониторинг і контроль: внутрішній та зовнішній.

В якості прикінцевих положень потрібно сказати, на основі власного досвіду, що існують методичні розробки цього напряму навчання, та позитивна практика виконання курсових та дипломних робіт [7–9].

Висновки

Навчання управлінню ризиками надзвичайних ситуацій техногенного та природного характеру має розглядатись як невід'ємна частина державної політики національної безпеки та соціально-економічного розвитку держави, однією з найважливіших функцій всіх органів виконавчої влади та суб'єктів господарювання всіх форм власності, має здійснюватись на основі зазначених вище принципів, акумулюючи кращі досягнення людства в усіх галузях виробництва.

Ризик-орієнтований підхід як сучасна методологія управління безпекою в розвинених країнах, значно (в 7–50 раз) зменшує витрати державного бюджету на ліквідацію наслідків надзвичайних ситуацій за рахунок їх попередження, запобігання. Існують апробовані світові технології процесів управління ризиком на рівні міжнародних стандартів, які потрібно застосовувати в нашій країні, не тільки в ядерній галузі. Сучасні інформаційні технології та наявність новітніх комп'ютерів дозволяють зробити процес регулювання безпеки в Україні сучасним та менш затратним. Для цього потрібне якісне всебічне навчання.

Студенти здатні опанувати курс протягом 1-2 семестрів на рівні компетенції достатньої для створення програмного забезпечення і, хоча цей факт не утримує їх від бажання заробляти більше грошей в іноземній компанії, у такій спосіб можна продемонструвати владі та потенційним споживачам рішення задач безпеки на сучасному інформаційному рівні. Це, в свою чергу, наблизить державу до перемоги на інформаційному та антикорупційному фронті.

Потрібне приділяти більше уваги прикладним задачам математики та інформатизації сфері безпеки, переглянути навчальні та робочі програми вищих навчальних закладів усіх рівнів акредитації, поширити тематику курсових та дипломних робіт на важливі сфері життєдіяльності суспільства.

Література

1. Бєгун В. В Методологічні основи інформаційної технології управління безпекою на основі ризик-орієнтованого підходу: дис. доктора технічних наук: 05.13.06 / Бєгун Василь Васильович. Київ, 2020. 553 с.
2. Бегун В. В. Впровадження інформаційних технологій у сферу безпеки. *Науково-технічна інформація.* 2016. № 1. С. 39–45.
3. Морозов А. О., Гречанінов В. Ф., Бєгун В. В. Управління безпекою в епоху інформаційного суспільства. *Вісник НАН України.* 2015. № 10. С. 34–41.
4. ДСТУ 27.310-95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения.

5. ГОСТ 12.1.004-91 Система стандартов безопасности труда (ССБТ). Пожарная безопасность. Общие требования (с Изменением N 1). URL: http://docs.cntd.ru/document/gost-12-1-004-91-ssbt
6. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on an EU Strategic Framework on Health and Safety at Work 2014-2020. COM(2014) 332 final. Brussels: European Commission, 2014. 15 p.
7. Кудін В. О., Бєгун В. В., Гречанінов В. Ф., Яцюк О. П. Концепція освіти з безпеки. *Теорія і практика управління соціальними системами.* 2015. № 3. С. 33–44.
8. Бєгун В. В., Гречанінов В. Ф. Науковці розробили нову концепцію освіти з безпеки. Концепція освіти з безпеки. Вища освіта. Інформаційно-аналітичний портал про вищу освіту в Україні та за кордоном. URL: http://vnz.org.ua/statti/7502-naukovtsi-rozrobyly-novu-kontseptsiju-osvity-z-bezpeky (дата звернення: 16.03.2015).
9. Хенли Э. Дж., Кумамото Х. Надежность технических систем и оценка риска. М.: Машиностроение, 1984. 528 с.

Надійшла: 12.09.2022 / Прийнята: 30.09.2022