

УДК 004.942

ДЕЯКІ ПИТАННЯ ЖИТТЄЗДАТНОСТІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ ТЕХНОГЕННОЮ БЕЗПЕКОЮ

О.О. Кряжич*, О.В. Коваленко**

*Інститут телекомунікацій і глобального інформаційного простору НАН України,

**Інститут ядерних досліджень НАН України

e-mail: economconsult@gmail.com

Згідно ст. 2 Кодексу цивільного захисту України, техногенна безпека – відсутність ризику виникнення аварій та/або катастроф на потенційно небезпечних об'єктах, а також у суб'єктів господарювання, що можуть створити реальну загрозу їх виникнення. Техногенна безпека характеризує стан захисту населення і територій від надзвичайних ситуацій техногенного характеру. Проведення антитерористичної операції в Луганській і Донецькій областях та підвищення ризику скоєння терористичних актів всією територією України виявили деяку проблематичність існуючих алгоритмів рятувальних дій служб цивільного захисту та систем підтримки прийняття рішень (СППР) з забезпечення техногенної безпеки та порятунку населення в умовах техногенних катастроф.

Проблема полягає в тому, що традиційно при виникненні будь-якої аварії чи катастрофи, за допомогою засобів обчислювальної техніки лише вирішуються оптимізаційні задачі визначення необхідних транспортних засобів, прокладання оптимальних маршрутів руху спецтранспорту до місця виникнення аварії, визначення необхідної кількості ресурсів, будуються графіки використання транспортних засобів, у разі масштабних аварій розробляються прогнози розповсюдження небезпеки, розраховуються економічні збитки та ін. При цьому головна увага приділяється дослідженню впливу людського чинника на виникнення надзвичайної ситуації чи аварії. Всі ці задачі розглядаються в межах якогось визначеного відрізка часу з встановленими умовами обмежень ресурсів та заданими параметрами розвитку ситуацій.

Україна має величезний комплекс підприємств, які пов'язані з виробництвом, переробкою та зберіганням сильнодіючих отруйних, вибухонебезпечних і вогненебезпечних речовин. Луганська і Донецька області являють собою зони з надзвичайно високим ступенем ризику техногенної небезпеки, як хімічної, так і радіаційної, бо кількість небезпечних підприємств на цих територіях перевищувала загальну кількість потенційно небезпечних та небезпечних об'єктів ряду розвинутих європейських країн. Відкрите військове протистояння на зазначених територіях перед службами порятунку поставило зовсім нові завдання – виникла потреба допомоги населенню через виникнення гуманітарної катастрофи в зонах конфлікту, яка обтяжується загрозою хімічного та/або радіаційного ураження за умов обмеження часу та ресурсів.

Можна навести ряд прикладів таких ситуацій. Так, Лисичанський нафтопереробний завод горів два дні після обстрілу з важкої артилерії, бо заводська пожежна частина була розграбована, а міські рятувальні команди хоч і прибули на місце катастрофи, не мали відповідної інформації та точного плану дій щодо роботи в умовах, що склалися. Така ж негативна інформація по Донецькому казенному хімічному заводу: постійні потрапляння снарядів та мін на територію заводу викликали вибухи та пожежі на складах небезпечних речовин, в Інтернеті та у пресі виникала інформація щодо загрози для розташованого поряд із заводом могильника радіаційних відходів, а обмеженість інформації та подія, що непередбачена жодними планами щодо ліквідації надзвичайних ситуацій, примушували рятувальників ліквідувати лише окремі осередки небезпеки. З м. Слов'янськ, яке в той час знаходилося під контролем сепаратистів, надходила інформація про пошкодження установки радону, що використовувалася для лікування хворих у санаторії «Ювілейний», та відповідні зміни радіаційного фону через цю подію.

Оперативно-мобільна група рятувальників вимушена була працювати з метою обстеження території в умовах постійних обстрілів. Перелік подібних ситуацій досить значний.

Метою даної роботи є аналіз можливостей щодо забезпечення життєздатності інформаційних технологій управління техногенною безпекою при їх адаптації до умов реального часу, що склався на момент застосування цих технологій.

Для реалізації поставленої мети вирішуються наступні завдання:

- обґрунтовується використання терміну «життєздатність»;
- розмежовується поняття життєздатності та живучості, як функції розвитку інформаційної технології у часі в залежності від змін ситуації та базових факторів, що визначають цю ситуацію;
- наводиться спрощена модель життєздатної інформаційної системи.

Слід зазначити, що питання живучості в інформаційних технологіях та складних інформаційно-обчислювальних системах досліджували Глушков В.М., Руденко Б.Н., Теслер Г.С., Черкесов Г.Н., життєздатності систем – Стафорд Бір.

Термін «живучість» є широко відомим і застосовуваним розробниками обчислювальної техніки та інформаційних технологій ще з 60-х років минулого століття. У 80-і роки живучість технічних систем стала самостійною наукою з розвинутим понятійним апаратом. Так, у обчислювальних системах під терміном «живучість» розуміли відсутність втрат будь-якої задачі (функції) через відмову елементів [1]. З вдосконаленням засобів обчислення виникла необхідність забезпечення живучості програм та алгоритмів, у зв'язку з чим було запропоноване поняття гарантоздатності, як здатності системи або технології функціонувати правильно, достовірно і стабільно без огляду на існуючі зовнішні та внутрішні збурення [2]. Як один з елементів цього терміну, туди увійшло і поняття живучості. При цьому зазначається, що, наприклад, сучасна інформаційна система повинна мати властивості захисту і життєздатності, а це може забезпечити лише реалізація біологозоологічного підходу з представленням цієї системи, як кібернетичної [2].

Першу модель життєздатної системи, засновану на біологозоологічному підході запропонував в 70-і роки ХХ ст. англійський кібернетик Стаффорд Бір [3]. Теоретико-методологічні основи моделей Ст. Біра в подальшому були розвинуті його учнями відповідно до специфіки тих галузей, де вони працювали. Проте математичний апарат цих моделей і досі залишається мало розвинутим, хоча всі процеси, фактори впливу та трансформація інформації від входу до виходу з системи були описані Ст. Біром дуже ретельно. Сам Ст. Бір в деяких своїх роботах [3, 4] зазначав, що його труди призначені для практичного виконавця, тож не потребують над ускладнень та надмірного математичного апарату, що може стати на заваді у практичному застосуванні.

Проте будь-яку проблему, особливо пов'язану з побудовою життєздатної інформаційної технології, не можна вирішити без математичного означення та представлення у вигляді конкретних математичних моделей. Основи такого підходу закладені в багатьох роботах академіка В.М. Глушкова, зокрема, неодноразово підкреслюється, що основою програмування є математичне забезпечення [5] і до цього незмінно веде математизація знань [6].

Сучасні доробки вчених не оминають питань живучості інформаційних систем та інформаційних технологій. Велика увага приділяється пошуку стійких до перешкод (робастних) алгоритмів. Проте здебільшого ці дослідження живучості зводяться до вирішення детермінованих мережевих та комбінаторно-графових задач, де вивчаються різноманітні зв'язки без аналізу розвитку у часі [7], що, у підсумку, ускладнює породження необхідних алгоритмів для конкретного застосування та створення нових інформаційних технологій для СППР.

Життєздатну систему характеризує можливість адаптування до умов мінливого середовища [3]. Проте, на відміну від постулатів про життєздатну систему Ст. Біра, будь-яка система, створена людиною, має на меті не забезпечення самовиживання за будь-яку ціну, а виконання функцій, покладених на неї розробником. Спираючись на таку точку зору, життєздатність інформаційної технології управління техногенною безпекою буде представляти собою методи та засоби, що об'єднані в технологічний ланцюг для забезпечення збору, зберігання, обробки, виводу і розповсюдження інформації відповідно до умов зміни середовища для забезпечення виживання людини та живих організмів у разі виникнення небезпеки.

У практичному застосуванні це буде означати, що інформаційна технологія забезпечуватиме процедури обробки інформації щодо роботи деякої досліджуваної системи S на конкретний час t та прогнозування розвитку цієї системи на час Δt , тобто, на якусь найближчу перспективу.

Функціонування складної системи характеризується описом ситуацій, які показують стан системи, наприклад, $S_1, S_2, \dots, S_n$, де кожен стан S_n заданий конкретними показниками процесів функціонування системи (Y_n, X_n, U_n) , впливом зовнішнього середовища та факторів ризику Ξ_k :

$$S_n = \{(Y_n \in Y) \wedge (X_n \in X) \wedge (U_n \in U) \wedge (\Xi_n \in \Xi)\}, \quad (1)$$

де значення показника в момент часу $T_n \in T^\pm$ визначають, як відомо [8], відношення:

$$\begin{aligned} Y_s &= \hat{Y}[T_s]; X_s = \hat{X}[T_s]; U_s = \hat{U}[T_s]; \Xi_s = \hat{\Xi}[T_s]; \\ T_s &= \{t_s | t_s > t_{s-1}\}; T_s \in T^\pm; T^\pm = \{t | t^- \leq t \leq t^+\}; \\ Y &= (Y_i | i = \overline{1, m}); X = (X_j | j = \overline{1, n}); \\ U &= (U_q | q = \overline{1, Q}); \Xi = (\Xi_p | p = \overline{1, P}), \end{aligned} \quad (2)$$

де Y – множина зовнішніх параметрів Y_i , яка утримує всі показники якісного функціонування системи, у тому числі – безпечного функціонування; X – множина внутрішніх параметрів X_j , до складу якої входять конструктивні, технологічні та інші показники; U – множина керуючих параметрів U_q ; Ξ – множина параметрів зовнішнього впливу Ξ_p та факторів ризику з деякою вірогідністю P ; $\hat{Y}[T_s], \hat{X}[T_s], \hat{U}[T_s], \hat{\Xi}[T_s]$ – множина значень відповідних параметрів в час T_s ; $T^\pm$ – заданий або прогнозований період функціонування системи.

Будь-яка складна система у своєму функціонуванні досягає деякого інтервалу невпевненості. Заданий інтервал – інтервал реального часу, основні параметри якого нам відомі. Прогнозований період – інтервал невпевненості, параметри якого можуть бути невідомі зовсім, або сумнівні. Враховуючи це, життєздатність системи можна представити як функцію часу (та інформації, що входить), тобто, представити життєздатність як задачу моделювання вірогідності розвитку ситуації в часі.

Вирішуючи часткові задачі обробки кожного з видів інформації $J_k(S, t)$, $k = 1, \dots, r$ на проміжку часу $[t_1, t_2]$, інформацію, що обробляється, можна представити у наступному вигляді:

$$J'(S, t) = \|i(S_l, t)\|_{l=1}^p, \quad (3)$$

де $i(S_l, t)$ – інформація, що отримана від джерела інформації S_l , $l = 1, \dots, p$.

Приймаємо, що джерело поставляє інформацію безперервно. У цьому випадку можна вважати, що система S життєздатна в момент часу t , за умови, що всі джерела інформації S_l , $l = 1, \dots, p$ надають інформацію, що знаходиться в деякій області O_l . У

випадку наявності хоча б одного джерела інформації S_l' , інформація від якого виходить за межі припустимої області, можна казати про загрозу життєздатності системи.

Аналізуючи такий підхід у тривимірній системі координат, можна зазначити наступне: нехай припустима область змін показників джерела інформації S_l представлена сферою O_l з центром у деякій точці M_l . Приймаємо, що радіус цієї сфери дорівнює R_l . Якщо в деякий момент часу t' інформація, яка надається джерелом S_l , буде відповідати центру інформаційної сфери O_l , то вірогідність P_l життєздатності системи S згідно джерела інформації S_l буде оцінена, як 1. Наближення інформаційних даних до межі інформаційної області O_l буде означати зменшення вірогідності життєздатності системи S . На самій межі припустимої області цю вірогідність приймаємо за 0. Час t_l^0 , за який $P(S_l, t) = 0$ назвемо критичним за джерелом S_l . Якщо взяти до уваги всю сукупність джерел інформації про роботу системи S , то:

$$t_{кр} = \min(t_1^0, t_2^0, \dots, t_p^0). \quad (4)$$

На основі запису (4) можна визначити вірогідність настання критичного стану системи S :

$$P(S, t) = \min(P_1(S, t), P_2(S, t), \dots, P_p(S, t)). \quad (5)$$

Вираз (5) підтверджує формулу (3) і дозволяє представити співвідношення (1) як спрощену модель життєздатної інформаційної системи:

$$S_n = \{((Yn \in Y) \wedge (Xn \in X) \wedge (Un \in U) \wedge (\exists n \in \Xi)) \cap (Tn + \Delta T \in T)\}, \quad (6)$$

як можливості задовільно виконувати всі закладені в систему функції у будь-якій точці часового інтервалу до досягнення критичного стану системи.

Висновки

У підсумку слід зазначити, що найбільш природнім засобом звуження невизначеності часового інтервалу є поділ його на декілька частин з наступним обчисленням значень цільової функції у вузлах сітки. У даному випадку пропонується розбивати часовий інтервал за методом «золотого перетину», тобто, обробляти та представляти для прийняття рішень значну частину інформації про поточний стан подій та інформацію з найбільш вірогідним прогнозом розвитку ситуації (у співвідношенні 0,618 : 0,382), що дозволить в сукупності отримати вірогідність забезпечення життєздатності інформаційної системи (для реалізації мети щодо забезпечення техногенної безпеки) згідно джерела інформації близькою до 1.

Список літератури

1. Руденко Б.Н., Ушаков И.Н. Надежность систем энергетики. - М.: Наука, 1986. – 52 с.
2. Теслер Г.С. Концепция построения гарантоспособных вычислительных систем / Г.С. Теслер // Математичні машини і системи. – 2006. – №1. – С. 134-145.
3. Бир Ст. Мозг фирмы / Бир Ст. – М.: Либроком, 2009. – 416 с.
4. Бир Ст. Кибернетика и управление производством / Бир Ст.; пер. с англ. В. Я. Алтаева. – М.: Наука, 1963. – 276 с.
5. Глушков В.М., Барабанов А.А., Калинин Л.А., Михновский С.Д., Рабинович З.Л. Вычислительные машины с развитыми системами интерпретации. – К.: Наукова думка, 1970. – 262 с.
6. Глушков В.М. Кибернетика. Вопросы теории и практики. – М.: Наука, 1986. – 488с.
7. Громов Ю.Ю. Синтез и анализ живучести сетевых систем : монография / Ю.Ю. Громов, В.О. Драчев, К.А. Набатов, О.Г. Иванова. – М. : «Издательство Машиностроение-1», 2007. – 152 с.
8. Згуровський М.З. Системний аналіз. Проблеми, методологія застосування / М.З. Згуровський, Н.Д. Панкратова. – К.: «Наукова думка», 2011. – 728с.