Приведена оцінка радіоактивної обстановки довкілля під час лісової пожежі шляхом чисельного моделювання виникнення і розвитку лісової пожежі, утворення радіоактивної «димової хмари» і викиду РПЗ із зони пожежі в атмосферне повітря дозволяють проводити прогнозні оцінки радіоекологічних наслідків, попереджувати і зменшувати дозові навантаження радіаційних регіонів, приймати управлінське рішення з ліквідації радіоекологічних наслідків.

Запропонована математична модель і алгоритми можуть бути використані для оперативного і довгострокового прогнозування радіаційного навантаження на населення та оцінки масштабів радіоактивного забруднення чистих територій.

СПИСОК ЛІТЕРАТУРИ

1. Азаров С.І. Дослідження находження ^{137}Cs в повітря при лісових пожежах в Чорнобильській зоні / Азаров С.І., Сидоренко В.Л., Руденко О.В., Пруський А.В. // Пожежна безпека: теорія і практика. – 2011. – Вип. 9. – С. 5–10.

УДК 519

В. О. Собина, кандидат технічних наук, Л. В. Борисова, кандидат юридичних наук, доцент, А. Б. Фещенко, кандидат технічних наук, доцент, Національний університет цивільного захисту України

БЕЗПЕКА ОБ'ЄКТУ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Інформація, інформаційний фонд за умов надзвичайної ситуації стає основним ресурсом ефективного прийняття рішень, спрямованих на ліквідацію надзвичайної ситуації. Інформація про можливість виникнення надзвичайної ситуації і тенденцій розвитку надходить до системи управління у ході вивчення оточуючого середовища, прогнозування та аналізу стану.

У системі управління надзвичайною ситуацією функціонує розширена інформаційна система, побудована на підставі наявних засобів масової інформації, обчислювальної техніки і системи подачі даних, яка відкрита для зовнішнього середовища, активно взаємодіє з групами та організаціями в межах і поза межами систем управління надзвичайною ситуацією. Мета цього управління – досягнення прийнятного рівня ризику.

Основними цілями використання обчислювальної техніки в системі управління надзвичайною ситуацією є забезпечення наявності ефективних інформаційних потоків, їх активного оперативного багатоаспектного

пошуку за заданими критеріями, збереження повноти та достовірності, захист від несанкціонованого доступу.

Інтенсивне зростання числа джерел небезпеки для об'єкту обчислювальної техніки (ООТ) та його компонентів, високі ймовірності їх реалізації та значні обсяги збитків призводять до необхідності пошуку ефективних засобів забезпечення безпеки цих об'єктів.

Найбільш уразливими об'єктами забезпечення інформаційної безпеки України в умовах надзвичайних ситуацій є система прийняття рішень з оперативних дій (реакцій), пов'язаних із розвитком таких ситуацій і ходом ліквідації їхніх наслідків, а також система збору та обробки інформації про можливе виникнення надзвичайних ситуацій.

Основою функціонування систем інформаційної підтримки прийняття колективних рішень (за міжнародною термінологією – brain storm – мозковий штурм) є застосування інтерактивної обчислювальної мережі та відповідних методів аналізу, що використовуються для отримання інформації та опрацюванні різних аспектів і шляхів вирішення поставленої проблеми. Широке використання ПЕОМ і розробка різного плану інформаційних систем підвищують ефективність прийняття групових рішень, алгоритмічні та програмні засоби яких є елементами моделювання деревовидних структур рішень аналізу ризику, прогнозування, містять засоби зв'язку та системи управлянні даними із загальним і індивідуальним доступом, стандартні засоби аналізу даних і управління інформацією. Особливе значення для нормального функціонування зазначених об'єктів має *забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах*.

До специфічних для даних умов напрямів забезпечення інформаційної безпеки належать:

– розробка ефективної системи моніторингу об'єктів підвищеної небезпеки, порушення функціонування яких може призвести до виникнення надзвичайних ситуацій, і прогнозування надзвичайних ситуацій;

– підвищення надійності систем обробки та передачі інформації, розробка спеціальних заходів із захисту інформаційних систем, які забезпечують керування екологічно небезпечними й економічно важливими виробництвами.

Поняття ризик та невизначеність широко використовуються в теорії гри та динамічному програмуванні. Ризик двомірна величина, що включає в себе як імовірність настання небажаної випадкової події (небезпеки), так і пов'язані з нею збитки та втрати. Ризик-орієнтований підхід можна визначити як аналіз ризику та застосування значення ризику виникнення негативної події, що може статися в навколишньому середовищі або на об'єкті техносфери, для застосування міри її небезпеки та використання цього значення як одного з критеріїв управляння.

Ризик – прогнозована векторна величина збитку, що може виникати в наслідок ухвалення рішень в умовах невизначеності та реалізації загрози. Він є кількісною мірою безпеки, що дорівнює добутку ймовірності реалізації даної загрози на ймовірність величини (величину) можливого збитку від неї.

Аналіз ризиків передбачає вивчення моделі загроз безпеці інформації, можливих наслідків від реалізації потенційних загроз (рівня заподіяної шкоди) і створення на основі результатів аналізу моделі захисту інформації в автоматизований системі.

Теорія безпеки є наукою про передбачення виникнення режимів функціонування системи, що загрожують її існуванню, і заходи щодо їхнього запобігання. Відповідно, розрізняють постановки задач дослідження внутрішньої й зовнішньої функцій безпеки: у першому випадку головна увага приділяється динаміці середовища в умовах впливу з боку системи, а в другому – поведінці системи щодо активного середовища.

Для отримання оцінок ризику, що використовуються для розв'язання прикладних задач у науці та техніці, використовують два показники:

– імовірність (частота) виникнення події, що призводить до небажаних наслідків;
– масштаб наслідків для заданої події.

Наприклад, дослідження проведені Executive Information Network стосуються ймовірності виникнення загроз безпеці інформації, а саме: 55% – нещасні випадки та помилки, 15% – недбалість; 10% – помста; 15% – пожежі; 3% – повені; 2% – землетруси.

Фірма Safeware проводила аналіз, у звіті якого вказано середню вартість і число збитків, ґрунтуючись на виділенні категорій ризиків. Крадіжки: середній збиток – 1125, кількість випадків – 136978, сума (млн.$) – 154,1; перепади напруги: середній збиток – 157, кількість випадків – 224403, сума (млн.$) – 35,2; нещасні випадки: середній збиток – 238, кількість випадків –93697, сума (млн.$) – 154,1; пожежі: середній збиток –1257, кількість випадків – 14001, сума (млн.$) – 17,6; блискавки: середній збиток – 195, кількість випадків – 748771, сума (млн.$) – 14,6; інші: середній збиток – 195, кількість випадків – 748771, сума (млн.$) – 14,6.

Приймемо раніше розроблені методичні апарати аналізу ризиків для обґрунтування рішень і дій посадових осіб за збереження всіх основних якостей інформації – конфіденційності, цілісності та доступності. Автор моделі оцінки ризику О.Л. Рогозін припускає, що за певний проміжок часу середній ризик, спричинений подією A, можна визначити за допомогою виразу

$$R(A) = P(A)Y(A), \qquad (1)$$

де $P(A)$ – частота події A, що має розмірність, обернену до часу;

$Y(A)$ – можливий одноразовий збиток, спричинений подією A, що має розмірність втрат.

Частота у формулі (1) чисельно дорівнює статистичній імовірності події A і виражається числом негативних подій за одиницю часу (відмов/міс., аварій/рік тощо). До неї можна застосувати основні теореми теорії ймовірності. Вважаємо, що ймовірність негативних подій – безрозмірна величина, тому згідно з формулою значення повинні мати розмірність збитків. Такий ризик є комбінованим або зведеним (до одиниці часу).

Статична ймовірність події A (ризик, що трапився під час події) дорівнює

$$P(A) = \frac{\nu(t)}{T},$$

де $\nu(t)$ – кількість проявів події A за час t, T – період спостереження.

Скористаємося показником ступеня уразливості $C_y(A)$ (або $R(A)$), який є відношенням уражених об'єктів (елементів) до їхньої загальної кількості (число загальних елементів – кількість елементів ООТ, які опинилися в зоні ураження), зафіксований для події певної інтенсивності:

Збиток у формулі (1) пов'язаний зі ступенем уразливості співвідношенням

$$Y(A) = C_y(A)Y_n(A),$$

де $Y_n(A)$ – умовний повний збиток унаслідок реалізації події A, який чисельно дорівнює кількості або вартості всіх елементів ООТ або кількості або вартості тих елементів ООТ, що опинилися в зоні ураження.

При розгляді частних ризиків, притаманних саме для певного типу елементів ООТ, які підпали під вплив небезпечної події, до формули (5) вводяться необхідні уточнення.

Очевидно, що *повний ризик як наслідок реалізації події А дорівнюватиме сумі ризиків цієї події для груп елементів ООТ кожного типу.*

Створення комплексної інформаційної технології у сфері програмно-цільового планування та управління включає:

- розв'язання завдань із захисту населення і територій від надзвичайних ситуацій неможливе без сучасної системи зв'язку, оповіщення та інформатизації ДСНС;
- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного

інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;

– розробку та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС.

СПИСОК ЛІТЕРАТУРИ

1. Антонюк А. О. Основи захисту інформації в автоматизованих системах : навч. посіб. / А. О. Антонюк. – К.: Академія, 2003. – 242 с.

2. Рагозин А.Л. Оценка и картографирование опасности и риска от природных и техноприродных процессов // Проблемы безопасности при чрезвычайных ситуациях. – 1993. – №4. – С. 16-41.

УДК 624.012

Д. О. Ступак, кандидат технічних наук, доцент,
В. А. Колле, М. П. Шаламай,
Черкаський інститут пожежної безпеки імені Героїв Чорнобиля
Національного університету цивільного захисту України

АПРОКСИМАЦІЯ ЛІНІЙ ІЗОТЕРМ ПАРАБОЛІЧНИМИ ЗАЛЕЖНОСТЯМИ В ПЕРЕРІЗІ ЗАЛІЗОБЕТОННОЇ БАЛКИ

Існують побудови температурних полів по перерізах залізобетонних балок [1-4], але вони виконані схематично і не містять точних даних температур, оскільки це здійснити експериментальним шляхом дуже важко. Тому для вирішення поставлених нами задач щодо розробки математичного апарату для інтерполяції температурних розподілів у перерізах залізобетонних ригелів і балок необхідно залучити температурні дані, отримані за теоретичним підходом розрахунковим методом.

Наші дослідження показали, що найбільш стійкий та надійний алгоритм, заснований на наближенні ліній ізотерм апроксимаційними залежностями [1-4].

При наближенні ізотерм параболічними кривими m-того порядку можна використовувати такий аналітичний вираз:

$$y(x) = y_0 + \frac{y_0}{x_0^m} \cdot x^m \qquad (1)$$

де x_0 і y_0 – координати точки перетину апроксимуючої кривої та осей координат;

m – показник ступеня еліптичної кривої, що наближає ізотерму.

Ступень m функціоналу (1) визначає порядок параболічної кривої, що встановлює її кривизну. Чим більше порядок, тим більша кривизна.