УДК 35.078.3

В.О. Собина, к.т.н., доцент, нач. каф., НУЦЗУ,
Л.В. Борисова, к.ю.н., доцент, викладач, НУЦЗУ

ПРОГНОЗ СТАНУ БЕЗПЕКИ ОБ'ЄКТУ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ З УРАХУВАННЯМ ДИНАМІКИ ЗМІНИ НЕБЕЗПЕЧНИХ ПОДІЙ У ЧАСІ

(представлено д-ром техн. наук Куценком Л.М.)

Пропонується адаптація раніше розроблених методичних апаратів аналізу ризиків внаслідок надзвичайних ситуацій для об'єктів обчислювальної техніки з урахуванням динаміки зміни небезпечних подій у часі. Показано, що ймовірність нештатних ситуацій зростає по експоненті, а стан безпеки ООТ по експоненті спадає, відповідно, заходи щодо зниження ризику доцільно приймати на найбільш несприятливих напрямках. При виборі засобів захисту інформації перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

Ключові слова: надзвичайна ситуація, об'єкт обчислювальної техніки, система прийняття рішень, стан безпеки.

Постановка проблеми. Одним з найбільш ефективних факторів зниження ризиків виникнення надзвичайних ситуацій техногенного характеру є створення і запровадження нових інформаційних технологій контролю за критичними параметрами технологічних процесів на об'єктах з небезпечною діяльністю на основі широкого використання автоматизованих і комп'ютерних засобів відповідно до Концепції створення єдиної державної системи запобігання і реагування на аварії, катастрофи та інші надзвичайні ситуації, затвердженої постановою Кабінету Міністрів України від 7 липня 1995 р. № 501. Вагомим кроком у цьому напрямку є розробка та впровадження в практичну діяльність Правил улаштування, експлуатації та технічного обслуговування систем раннього виявлення надзвичайних ситуацій та оповіщення людей у разі їх виникнення, затверджених наказом МНС від 15.05.2006 № 288, зареєстрованим в Мін'юсті 05.07.2006 за № 785/12659.

Кожний конкретний об'єкт є індивідуальним набором параметрів та інформаційних додаткових даних. Кожний параметр в інформаційній базі має:

– своє критичне значення, вище якого він переходить в передаварійну область;

– кожний з параметрів має і свій поріг аварійності;

– всі параметри інформаційної бази взаємозалежні, впливаючи один на одного тою чи іншою мірою.

Ступінь впливу параметрів один на одного досить різний і визначає швидкість наростання аварійного процесу. Відслідковуючи ситуацію з повним набором інформаційних даних на екрані монітора в режимі реального часу, важко передбачати розвиток ситуації через наступні причини:

– непередбачена кількість даних (приблизно від 10 до 500);

– велика кількість різнотипних об'єктів з різними технологічними процесами;

– однозначне існування гіпероб'єктів, що припускає особливий, індивідуальний підхід, деталізація інформації технологічних процесів, логічні залежності при зв'язках і впливі параметрів один на одного;

– знання технологічних процесів на досить серйозному рівні, що неможливо для диспетчера і тим більше для прийняття правильних управлінських рішень.

Аналіз останніх досліджень і публікацій показав, що необхідний ступінь інформованості досягається шляхом створення в найкоротший термін (0,5-3 доби) інформаційних систем різного класу й призначення (інформаційні, інформаційно-пошукові, інформаційно-керуючі), що функціонують на базі сучасних ПЕОМ, локальних мереж ПЕОМ, сучасних засобів зв'язку [1]. Така система повинна забезпечувати ідентифікацію та реєстрацію інформації про предметну галузь, що виникла, її зберігання, безперервне ведення й використання шляхом збору, агрегування, класифікації, переробки та видачі необхідної інформації в зручний для використання формі та з можливістю передачі її каналами зв'язку всім абонентам.

Особливе значення для нормального функціонування зазначених об'єктів має *забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах* [3]. Безпека – це комплексний критерій оцінки якості будь-якої сучасної системи, яка характеризує як динаміку системи, так і її технічне втілення.

Постановка завдання та його вирішення. Ризик можна оцінити тільки для об'єкту, та (або) системи, які підпадають під небезпеку. Тому ризик становить собою усвідомлену небезпеку (загрозу) настання в будь-якій системі негативної події з окресленими у часі та просторі наслідками або існування чи можливість ситуації при якій формуються передумови протидії реалізації задач і функції фірми і забезпеченню її безпеки. Показниками ризику можуть виступати соціальний, економічний, інші збитки та (або) змішаний збиток, повторюваність (імовірність) негативної події, яка становить собою показник небезпеки, комбінована характеристика збитку і повторюваності, тобто середні за одиницю часу втрати.

З урахуванням адаптації раніше розроблених методичних апаратів аналізу ризиків внаслідок надзвичайних ситуацій для об'єктів

обчислювальної техніки, показано, що при управлінні безпекою ООТ слід в оцінку ризику вводити весь спектр небезпек, можливих для досліджуваного ООТ при його роботі [3].

Розглянемо динаміку зміни небезпечних подій у часі.

Якщо розуміти під безпекою ООТ відсутність непропустимого ризику враження обєкта при виникненні небезпечних подій, для оцінки вводиться функція $S(t)$. Сукупність характеристик небезпечних подій, «зважених» з ймовірностями їх виникнення визначимо як функцію ризику $H(t)$.

Для спрощення «потік» небезпечних подій будемо наближено вважати пуассонівським. Тоді для j-ї компоненти досліджуваного об'єкта можна записати

$$S_j(t) = \exp\left\{-t\sum_i^n \lambda_i \rho_{ij}\right\}; \tag{1}$$

$$H_j(t) = 1 - \exp\left\{-t\sum_{i=1}^n \lambda_i \rho_{ij}\right\}, \tag{2}$$

де λ_i – інтенсивність небезпечних подій *i*-го порядку; ρ_{ij} – ймовірність враження подією і-го виду j-ї компоненти досліджуваного об'єкта.

$$\lambda_i(t) = \frac{a_i(t)}{T}, \tag{3}$$

де $a_i(t)$ – математичне очікування числа подій і-го типу за період спостереження Т.

Наближено можна вважати, що

$$\rho_{ij} = \frac{n_{ij}}{n_i}, \tag{4}$$

де n_{ij} – число небезпечних подій *i*-го виду, які призвели до враження j-ї компоненти; n_i – загальне число небезпечних подій і-го виду; n – число джерел небезпеки для даного ООТ.

Тоді сумарні функції безпеки та ризику для всіх компонентів об'єкту будуть такими

$$S_\Sigma(t) = \prod_{j=1}^k S_j(t) = \exp\left\{-t\sum_{j=1}^k \Lambda_j\right\} \tag{5}$$

$$H_{\Sigma}(t)=\prod_{j=1}^{k}H_j(t)=1-\exp\left\{-t\sum_{j=1}^{k}\Lambda_j\right\}, \qquad (6)$$

де $S_j(t), H_j(t)$ – функції безпеки і ризику для j-го компоненту об'єкта;

$$\Lambda_j=\sum_{i=1}^{n}\lambda_i\rho_{ij}.$$

Проаналізуємо застосування на практиці наведених формул (1-6).

Для того ж об'єкта обчислювальної техніки (К = 2, п.6 прикладу 1) за результатами спостережень обчислені наступні інтенсивності небезпечних подій [3]:

I. виникнення проблеми із технікою $\rho_I(A)$ = 2,74 год$^{-1}$

II. перехоплення інформації або НСД через допоміжне обладнання $\rho_{II}(A)$ = 1,37 год$^{-1}$

III. ймовірність лихого задуму $\rho_{III}(A)$ = 0,8;

IV. ймовірність виникнення реальної техногенної або стихійної загрози ззовні $\rho_{IV}(A)$ = 0,5.

Тобто n = 10.

Протягом певного періоду спостережень мали місце:

50 подій I виду, з них 15 призвели до враження апаратури, 20 – до враження програмного забезпечення;

10 подій II виду, з них 3 призвели до враження апаратури, 5 – до враження програмного забезпечення;

5 подій III виду, з них 1 призвела до враження апаратури, 20 – до враження програмного забезпечення;

2 події IV виду, з них 1 призвела до враження апаратури, 1 – до враження програмного забезпечення.

Потрібно.

Визначити часткові та сумарні функції безпеки та ризику.

Для спрощення вважаємо, що:

1. інтенсивності відповідних подій вже обчислені за формулою (3);

2. повний умовний збиток дорівнює кількості всіх комплектів ООТ $Y(A)=10$;

3. усі події вважаємо незалежними одна від одної;

4. компонент вважається враженим, коли вражено хоча б один із компонентів ООТ або програмного забезпечення.

1. За формулою (4) обчислимо ймовірність враження компонент досліджуваного об'єкту:

– для апаратури

$$\rho_{I}^{HARD}=\frac{15}{50}=0,3;\ \rho_{II}^{HARD}=\frac{3}{10}=0,3;\ \rho_{III}^{HARD}=\frac{1}{5}=0,2;\ \ \rho_{IV}^{HARD}=\frac{1}{2}=0,5;$$

– для програмного забезпечення

$$\rho_{I}^{SOFT}=\frac{20}{50}=0,4;\rho_{II}^{SOFT}=\frac{2}{10}=0,2;\rho_{III}^{SOFT}=\frac{5}{5}=0;\rho_{IV}^{SOFT}=\frac{1}{2}=0,5.$$

Користуючись формулами (1) і (2) визначимо функції безпеки ризику для апаратури і програмного забезпечення по кожному із потоку подій:

– функції безпеки для апаратного забезпечення

$$S^{HARD}(t)=\exp\left\{-t\sum_{i=1}^{4}\lambda_i\rho_i^{HARD}\right\}=\exp\{-1,643t\}$$

– функція ризику для апаратного забезпечення

$$H^{HARD}(t)=1-S^{HARD}(t)=1-\exp\left\{-t\sum\lambda_i\rho_i^{HARD}\right\}=1-\exp\{-1,643t\}$$

– функції безпеки для програмного забезпечення

$$S^{SOFT}(t)=\exp\left\{-t\sum_{i=1}^{4}\lambda_i\rho_i^{SOFT}\right\}=\exp\{-2,42t\}$$

– функція ризику для програмного забезпечення

$$H^{SOFT}(t)=1-S^{SOFT}(t)=1-\exp\left\{-t\sum_{i=1}^{4}\lambda_i\rho_i^{SOFT}\right\}=1-\exp\{-2,42t\}$$

1. Сумарні функції безпеки та ризику за формулами (4'), (5), (6)

$$S_{\Sigma}(t)=S^{HARD}(t)\cdot S^{SOFT}(t)=\exp\left\{-t\left(\sum_{i=1}^{4}\lambda_i\rho_i^{HARD}+\sum_{i=1}^{4}\lambda_i\rho_i^{SOFT}\right)\right\}=$$
$$=\exp\{-4,063t\}$$

$$H_{\Sigma}(t)=H^{HARD}(t)\cdot H^{SOFT}(t)=1-\exp\left\{-t\left(\sum_{i=1}^{4}\lambda_i\rho_i^{HARD}+\sum_{i=1}^{4}\lambda_i\rho_i^{SOFT}\right)\right\}=$$
$$=1-\exp\{-4,063t\}$$

Отже, *ймовірність нештатних ситуацій зростає по експоненті, а стан безпеки ООТ по експоненті спадає.*

При управлінні безпекою ООТ слід керуватися наступним:

– в оцінку ризику вводити весь спектр небезпек, можливих для досліджуваного ООТ при його роботі;

– заходи щодо зниження ризику приймаються на найбільш несприятливих напрямках (рис. 1) [3]. При виборі засобів захисту інформації перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

Висновки. Створення комплексної інформаційної технології у сфері програмно-цільового планування та управління повинно включати розробку, експериментальне і практичне відпрацювання методик синтезу єдиної інформаційної технології для вирішення задач планування та управління роботами із запобігання та ліквідації наслідків надзвичайних ситуацій.

Крім виконання інформаційних функцій у межах такої системи повинні бути передбачені можливості моделювання та прогнозування розвитку надзвичайних ситуацій при реалізації альтернативних стратегій управління ними, прогнозу потреби в ресурсах, що необхідні для ліквідації наслідків цих ресурсів.

ЛІТЕРАТУРА

1. Качинський А.Б. Засади системного аналізу безпеки складних систем / А.Б. Качинський. – К.: ДП НВЦ «Євроатлантикінформ», 2006. – 336 с.

2. Кузьмин И.П. Риск и безопасность с точки зрения системной динамики. Радиационная безопасность и защита АЭС / И.П. Кузьмин, С.В. Романов. – 1991. – Вып. 13. – С. 82-105.

3. Собина В.О. Агаліз та прогноз стану безпеки обєкту обчислювальної техніки в умовах надзвичайних ситуацій / В.О. Собина, Л.В. Борисова, О.В. Єлізаров // Проблеми надзвичайних ситуацій: зб. наук. пр. – Вип. 21. – Х.: НУЦЗУ, 2015. – С. 89-96. – Режим доступу: http://nuczu.edu.ua/sciencearchive/ProblemsOfEmergencies/vol21/Sobina.pdf.

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

5. Могилевский В.Д. Введение в теорию управления безопасностью систем (методика и примеры) / В.Д. Могилевский // Проблемы безопасности при чрезвычайных ситуациях. – 2001. – № 5. – С. 4-22.

6. Степанов Е.А. Информационная безопасность и защита информации: учеб. пособие / Е.А. Степанов, И.К. Корнеев. – М.: ИНФРА-М, 2001. – 304 с.

В.А. Собина, Л.В. Борисова

Анализ и прогноз безопасности объекта вычислительной техники в условиях чрезвычайных ситуаций

Предлагается адаптация ранее разработанных методических аппаратов анализа рисков вследствие чрезвычайных ситуаций для объектов вычислительной техники. При управлении безопасностью ОВТ нужно руководствоваться следующим: в оценку риска вводить весь спектр опасностей, возможных для исследуемого ОВТ при его работе; мероприятия по снижению риска принимаются на наиболее неблагоприятных направлениях.

Ключевые слова: объект вычислительной техники, состояние безопасности, анализ рисков.

V.A. Sobina, L.V. Borisova

Analysis and forecast of security computing facility in emergency situations

It is proposed to adapt previously developed methodical risk analysis devices due to emergency facilities computers. When managing OVT safety should be guided by the following: risk assessment to introduce the whole range of dangers possible for the test CET during its operation; risk reduction measures are taken in the most disadvantaged areas.

Keywords: object computing, security status, risk analysis.