УДК 35.078.3

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

АНАЛІЗ ТА ПРОГНОЗ СТАНУ БЕЗПЕКИ ОБ'ЄКТУ ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

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

Пропонується адаптація раніше розроблених методичних апаратів аналізу ризиків внаслідок надзвичайних ситуацій для об'єктів обчислювальної техніки. Показано, що при управлінні безпекою ООТ слід керуватися наступним: в оцінку ризику вводити весь спектр небезпек, можливих для досліджуваного ООТ при його роботі.

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

Постановка проблеми. Одним із найбільш ефективних факторів зниження виникнення надзвичайних ситуацій 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.

Інформація, інформаційний фонд за умов надзвичайної ситуації стає основним ресурсом ефективного прийняття рішень, спрямованих на ліквідацію надзвичайної ситуації.

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.

Аналіз останніх досліджень і публікацій показав, що 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 [1,2]. Безпека системи – це показник її якості, цілісності, стан у процесі функціонування. 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 [4]. Вибір конкретної математичної моделі оцінки ризику залежить від кожної із ситуацій. Як наслідок – існує значна кількість як самих моделей, так і підходів до моделювання оцінок ризику [3].

Постановка завдання та його вирішення. 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 [3] припускає, що за певний проміжок часу середній ризик, спричинений подією А, можна визначити за допомогою виразу (1)

$$R(A) = P(A)Y(A), \tag{1}$$

де $R(A)$ – частота події А, що має розмірність, обернену до часу; $Y(A)$ – можливий одноразовий збиток, спричинений подією А, що має розмірність втрат.

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

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

$$R(A) = \frac{\nu(t)}{T}, \tag{2}$$

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

Тоді формула (1) набуває вигляду, визначаючи зміст показника $R(A)$ як кількість підданих ризику протягом періоду спостереження елементів:

$$R(A) = \frac{\nu(t)}{T}Y(A), \tag{1}$$

Ризик, що трапився під час події, є однією з характеристик небезпеки негативної події і є показником уразливості об’єкта. Скористаємося показником ступеня уразливості $C_y(A)$ (або $R(A\ )$), який є відношенням уражених об’єктів (елементів) $C_{вр.ул.}$ до їхньої загальної кількості $M_{заг.}$ (число загальних елементів – кількість елементів ООТ, які опинилися в зоні ураження), зафіксований для події певної інтенсивності:

$$C_y(A) = \frac{M_{вр.ел.}}{M_{заг.}}. \tag{3}$$

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

$$Y(A) = C_y(A)Y_n(A), \tag{4}$$

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

З урахуванням виразу (2) і (4), формула (1) набуде наступного вигляду:

$$R(A)=\frac{\nu(t)}{T}C_y(A)Y_n(A). \qquad (5)$$

Ця формула є загальною для обчислення ризику. При її практичному використанні в кожному конкретному випадку необхідно вносити уточнення. При розгляді окремих ризиків, притаманних саме для певного типу елементів ООТ, які підпали під вплив небезпечної події, до формули (5) вводяться необхідні уточнення. Тоді ризик розраховується за наступною модифікованою формулою:

$$R_ч(A)=\frac{\nu(t)}{T}P(H)C_{уч}(A)H, \qquad (6)$$

де $R_ч(A)$ – частний ризик; $P(H)$ – ймовірність перебування елементів певного типу в зоні ураження; $C_{уч}(A)$ – ступінь ураження цієї групи елементів; H – кількість елементів, що відповідає умовному повному збитку $Y_n(A)$ згідно з формулою (5).

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

Зазначимо, що кількість компонент кожного з рівнів може варіюватися відповідно до частних випадків, як і число рівнів декомпозиції. Слід брати до уваги, що небезпечні події можуть класифікуватися за масштабом, тяжкістю наслідків та іншими ознаками. Існують відомчі (галузеві), національні та міжнародні системи класифікації таких подій.

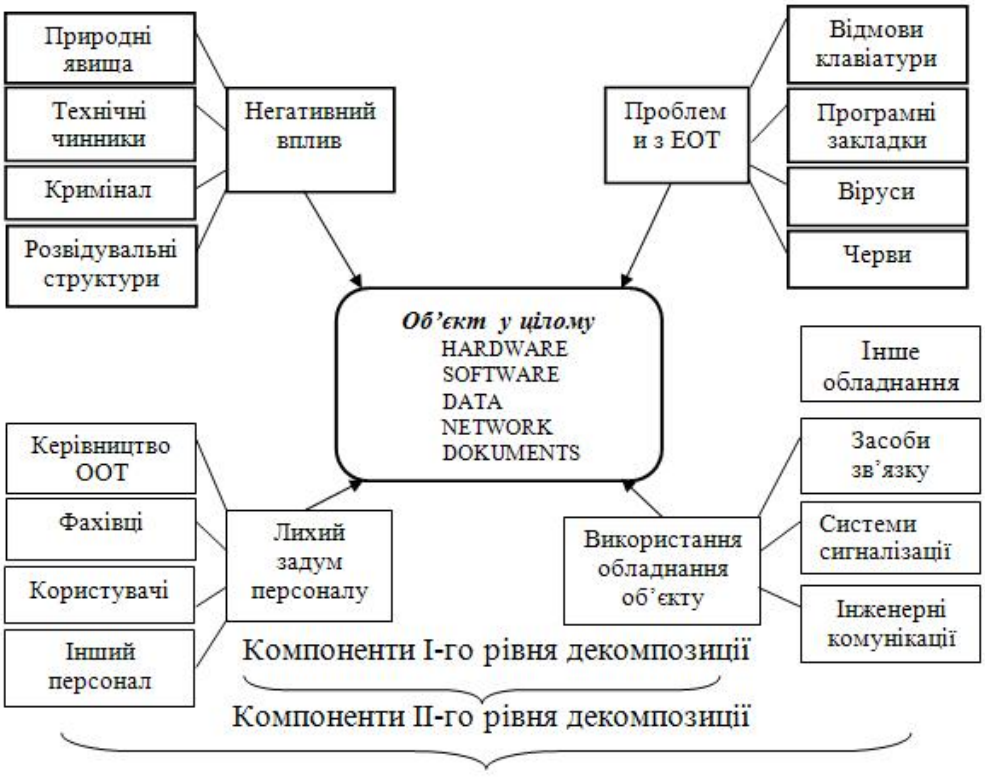

Рис. 1. Схема нарахування загального ризику

Розглянемо приклад нарахування загального ризику.

Нехай унаслідок декомпозиції до І рівня (рис.1) об'єкту ООТ із 10 комплектами ООТ виділено небезпечні події з такими ймовірними показниками:

І. ймовірність виникнення проблеми з технікою $P_I(A) = 0{,}7$;

ІІ. ймовірність перехоплення інформації або НСД через допоміжне обладнання $P_{II}(A) = 0{,}6$;

ІІІ. ймовірність лихого задуму $P_{III}(A) = 0{,}25$;

IV. ймовірність виникнення реальної техногенної або стихійної загрози ззовні $P_{IV}(A) = 0{,}06$.

Для спрощення вважаємо, що: ймовірності виникнення означених подій вже обчислені за формулою (2); повний умовний збиток дорівнює кількості всіх комплектів ООТ $Y(A) = 10$ усі події вважаємо незалежними одна від одної.

Потрібно: обчислити часткові ризики від подій кожного виду; обчислити комбінований ризик.

1. За формулою (1) середні ризики становлять:

– від подій І виду (відмови в ООТ): $R_I(A) = 0{,}7 \cdot 10 = 7$;

– від подій ІІ виду (перехоплення через допоміжне обладнання): $R_{II}(A) = 0{,}6 \cdot 10 = 6$;

– від подій ІІІ виду (злий задум персоналу): $R_{III}(A) = 0{,}25 \cdot 10 = 2{,}5$;

– від подій IV виду (негативний вплив середовища): $R_{IV}(A) = 0{,}25 \cdot 10 = 2{,}5$.

2. Обчислимо відповідні ступені ураженості елементів об'єкту за формулою (3) з урахуванням фізичного змісту формули (1):

$$C_I = \frac{7}{10};\ C_{II} = \frac{6}{10};\ C_{III} = \frac{2{,}5}{10};\ C_{IV} = \frac{0{,}06}{100}.$$

3. Можливі одномоментні збитки від тих же подій відповідно до (5) становитимуть:

$$R_{I\text{одн.}}(A) = 0{,}7 \cdot \frac{7}{10} \cdot 10 = 4{,}9; \quad R_{II\text{одн.}}(A) = 0{,}6 \cdot \frac{6}{10} \cdot 10 = 3{,}6;$$

$$R_{III\text{одн.}}(A) = 0{,}25 \cdot 0{,}25 \cdot 10 = 0{,}625; \quad R_{IV\text{одн.}}(A) = 0{,}06 \cdot \frac{6}{10} \cdot 10 = 0{,}36.$$

Комбінований одномоментний збиток дорівнює:

$$R_{K\text{одн.}}(A) = 4{,}9 + 3{,}6 + 0{,}625 + 0{,}625 + 0{,}036 = 9{,}16.$$

4. Комбінований середній збиток дорівнює:

$$R_{\text{Ксер.}}(A) = 7 + 6 + 2{,}5 + 0{,}6 = 16{,}1.$$

5. Припустимо, що на кожному з 10-ти комплектів ООТ встановлено 5 комплектів програмного забезпечення. У разі виникнення події I-го виду в зоні ураження може опинитися приблизно чверть наявних ООТ із своїм програмним забезпеченням, 2,5 комплекти апаратури і 12,5 комплектів програмного забезпечення відповідно. Часткові ступені ураження дорівнюють:

– для апаратури

$$C_{\text{ЧІ}}^{(\text{HARD})}(A) = \frac{0{,}7 \cdot 2{,}5}{10} = 0{,}175;$$

– для програмного забезпечення

$$C_{\text{ЧІ}}^{(\text{SOFT})}(A) = \frac{0{,}7 \cdot 12{,}5}{50} = 0{,}175.$$

Окремі ризики від події I-го виду за формулою (6) становитимуть відповідно:

– для апаратури

$$R_{\text{I}}^{(\text{HARD})}(A) = 0{,}7 \cdot 0{,}25 \cdot 10 \cdot 0{,}175 = 0{,}31,$$

– для програмного забезпечення

$$R_{\text{I}}^{(\text{SOFT})}(A) = 0{,}7 \cdot 0{,}25 \cdot 50 \cdot 0{,}175 = 1{,}53.$$

У разі виникнення події II-го виду в зоні ураження може опинитися приблизно половина наявних ООТ зі своїм програмним забезпеченням, тобто 5 комплектів апаратури і 25 комплектів програмного забезпечення відповідно. Звідси

– для апаратури

$$C_{\text{ЧІІ}}^{(\text{HARD})}(A) = \frac{0{,}6 \cdot 5}{10} = 0{,}3;$$

– для програмного забезпечення

$$C_{\text{ЧІІ}}^{(\text{SOFT})}(A) = \frac{0{,}6 \cdot 25}{50} = 0{,}3.$$

Тоді окремі ризики від події II-го виду за формулою (6) відповідно становитимуть:

– для апаратури

$$R_{II}^{(HARD)}(A) = 0{,}6 \cdot 0{,}5 \cdot 10 \cdot 0{,}3 = 0{,}9;$$

– для програмного забезпечення

$$R_{II}^{(SOFT)}(A) = 0{,}6 \cdot 0{,}5 \cdot 50 \cdot 0{,}3 = 4{,}5.$$

У разі виникнення події III-го і IV-го виду у зоні ураження опиняться всі наявні ЕОМ із своїм програмним забезпеченням. Звідси

– для апаратури

$$C_{ЧIII}^{(HARD)}(A) = \frac{0{,}25 \cdot 10}{10} = 0{,}25; \quad C_{ЧIV}^{(HARD)}(A) = \frac{0{,}06 \cdot 10}{10} = 0{,}06;$$

– для програмного забезпечення

$$C_{ЧIII}^{(SOFT)}(A) = \frac{0{,}06 \cdot 10}{10} = 0{,}25; \quad C_{ЧIV}^{(SOFT)}(A) = \frac{0{,}06 \cdot 50}{50} = 0{,}06.$$

Тоді окремі ризики від події III-го виду за формулою (6) становитимуть:

– для апаратури

$$R_{III}^{(HARD)}(A) = 0{,}25 \cdot 1{,}0 \cdot 10 \cdot 0{,}25 = 0{,}625;$$

– для програмного забезпечення

$$R_{III}^{(SOFT)}(A) = 0{,}25 \cdot 1{,}0 \cdot 0{,}25 \cdot 50 = 3{,}125.$$

Відповідно, окремі ризики від події IV-го виду становитимуть:

– для апаратури

$$R_{IV}^{(HARD)}(A) = 0{,}06 \cdot 1{,}0 \cdot 10 \cdot 0{,}06 = 0{,}036;$$

– для програмного забезпечення

$$R_{IV}^{(SOFT)}(A) = 0{,}06 \cdot 1{,}0 \cdot 0{,}06 \cdot 50 = 0{,}18.$$

6. Повний ризик для даного об’єкта:

$$R_{пов.}(A) = 0{,}31 + 1{,}53 + 0{,}9 + 4{,}5 + 0{,}625 + 3{,}125 + 0{,}036 + 0{,}18 = 8{,}206.$$

Без введення в дію СТЗ інформації робота даного *ООТ неможлива.*

Висновки. Інформаційні потоки сприймаються як різні відомості про стан елементів НС та оточуючого середовища, про впливи на інші дані, що необхідні для досягнення мети.

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). При виборі засобів захисту перевагу надавати таким, які при однакових витратах забезпечують найбільше зниження ризику.

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 / И.П. Кузьмин, С.В. Романов // Радиационная безопасность и защита АЭС. – 1991. – Вып. 13. – С. 82-105.

3. 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.

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

В.А. Собина, Л.В. Борисова, А.В. Елизаров

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. При выборе средств защиты преимущество предоставлять таким, которые при одинаковых затратах обеспечивают самое большое снижение риска.

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

V.A. Sobina, L.V. Borisova, A.V. Elizarov

Analysis and forecast object computing security in emergencies

It is proposed to adapt the previously developed teaching aids risk analysis due to emergency facilities for computer equipment. In managing the security object computing should be guided by the following: a risk assessment to introduce the whole range of hazards, possible for the object under study computer engineering at its work; risk reduction measures are taken in the most unfavorable direction. When selecting remedies provide such an advantage that for the same cost provide the greatest reduction in risk.

Keywords: object computing, security status, risk analysis.