Національний університет цивільного захисту України

Кафедра організації та технічного забезпечення аварійно-рятувальних робіт

Вказівки до виконання розрахункової роботи
з дисципліни «Інформаційна безпека у сфері професійної діяльності»

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

для здобувачів вищої освіти денної та
заочної форми навчання;
освітньо-кваліфікаційного рівня «магістр»
за спеціальністю 261 «Пожежна безпека»,
спеціалізацією «Управління пожежною безпекою»

Укладачі: Борисова Л.В., Собина В.О.

Харків, 2024

Зміст

Введення

У методичному посібнику надано вказівки до виконання розрахункової роботи з дисципліни «Інформаційна безпека у сфері професійної діяльності».

У роботі передбачається проведення аналізу об’єкту критичної інфраструктури, оцінки ризику для об’єкту, та (або) системи, які підпадають під небезпеку.

Методичні вказівки містять визначення мети роботи та перелік завдань, що розв’язуються, опис завдань на послідовно виконуваних етапах підготовчої самостійної роботи та вимоги до змісту звіту по контрольній роботі.

Методичні вказівки містять:

контрольні питання для самоперевірки;

список рекомендованої літератури по тематиках виконуваних робіт.

Мета роботи та питання, що досліджуються

Мета роботи: аналізу ризиків внаслідок надзвичайних ситуацій для об’єктів обчислювальної техніки з урахуванням динаміки зміни небезпечних подій у часі.

1. Питання, що досліджуються:

1.1. Аналіз та прогноз стану безпеки об’єкту обчислювальної техніки в умовах надзвичайних ситуацій.

1.2. Прогноз стану безпеки об’єкту обчислювальної техніки в умовах надзвичайних ситуацій з урахуванням динаміки зміни небезпечних подій у часі.

2. Рекомендований план виконання розрахункової роботи

2.1. Аналіз об’єкту критичної інфраструктури (за вибором здобувача вищої освіти), формування переліку вихідних даних та вимог.

2.2. Обчислити часткові ризики від подій кожного виду небезпеки.

2.3. Обчислити комбінований ризик.

2.3. Визначити часткові та сумарні функції безпеки та ризику

2.4. Підсумки роботи з оцінкою результатів виконання завдання.

3. Підготовка до розрахункової роботи

Вивчити теоретичний матеріал з рекомендованої літератури з питань, що розглядаються у розрахунковій роботі.

1. Проаналізувати схему нарахування загального ризику (рис.2) відповідно до вибраного об’єкту критичної інфраструктури.
2. Виділити небезпечні події з ймовірними показниками.
3. Проаналізувати і обчислити часткові ризики від подій кожного виду.
4. Обчислити комбінований ризик.
5. Проаналізувати і обчислити динаміку зміни небезпечних подій у часі.
6. Приклад оформлення курсової роботи (по тексту теоретично матеріалу).

4. Вимоги до змісту звіту

1. Титульний аркуш – за зразком у додатку 1.
2. Опис вихідних даних і вимог до роботи.
3. Опис і результати розрахунків часткових ризиків від подій кожного виду; обчислення комбінованого ризику.
4. Опис і результати розрахунків динаміки зміни небезпечних подій у часі.

5. Контрольні питання для самоперевірки

1. Як називається кількісна характеристика оцінки ступеня небезпеки?
2. Що таке кількісна оцінка ризику?
3. Як поділяються ризики?
4. Яким ефектом супроводжується ризик?
5. Що є показником уразливості об’єкта?
6. Що необхідно з’ясувати для оцінювання ступеня ризику?
7. Як визначаються виправдані ризики?
8. Які рівні ризику є не допустимими?
9. На яких принципах ґрунтується прийняття рішень за результатами аналізу небезпеки й оцінки ризику?

6. Література

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

2. Гавриш О.А., Кавун В.А. Критичний аналіз нормативних засад управління проектними ризиками. Економічний вісник НТУУ «КПІ». 2017. № 14. С. 216–222.

3. Визначення ризику як міри небезпеки потенційно небезпечних об’єктів / В.В. Бєгун // Актуальні проблеми цивільного захисту. Тези VI Всеукраїнської науково-практичної конференції рятувальників. – К., 2004. – С. 23-25.

4. Собина В.О. Аналіз та прогноз стану безпеки об’єкту 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.

Основний текст

Вступ

Загрози інформаційній безпеці розглядаються в органічному зв’язку з питаннями захисту об’єктів критичної інфраструктури, до якої в більшості країн світу відносять інформаційні системи та комп’ютерні мережі системи надзвичайних ситуацій. Процес управління ризиками відповідає міжнародній практиці, основним принципом якої є дотримання життєвого циклу «план – виконання – перевірка – дія» та застосування визнаних галузевих стандартів таких, як BS 25999-1:2006 (Управління безперервністю бізнесом) та ISO/IEC 27001:2005 (Вимоги до системи управління інформаційною безпекою). 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.

Кожний конкретний об’єкт є індивідуальним набором параметрів та інформаційних додаткових даних. Ступінь впливу параметрів один на одного різний і визначає швидкість наростання аварійного процесу.

Найбільш уразливим об’єктами забезпечення інформаційної безпеки є системи збору і обробки інформації про можливе виникнення надзвичайних ситуацій і прийняття рішень щодо оперативних дій, пов’язаних із розвитком таких ситуацій і ходом ліквідації їх наслідків.

Кожний параметр в інформаційній базі має:

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

свій поріг аварійності;

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

Аналіз ризику здійснюється за схемою: ідентифікація небезпек, моніторинг навколишнього середовища – аналіз (оцінка й прогноз) загрози – аналіз уразливості територій – аналіз ризику надзвичайної ситуації на території – аналіз індивідуального ризику для населення.

З точки зору аналізу ризиків і управління безпекою розрізняють:

індивідуальний ризик,

потенційний територіальний ризик,

соціальний ризик,

колективний ризик (число загиблих і потерпілих у результаті можливих надзвичайних ситуацій),

прийнятний ризик (рівень ризику, з яким суспільство готове примиритися),

неприйнятний ризик,

ризик-рівень індивідуального ризику (не викликає занепокоєння й не приводить до погіршення якості життя населення), яким можна знехтувати.

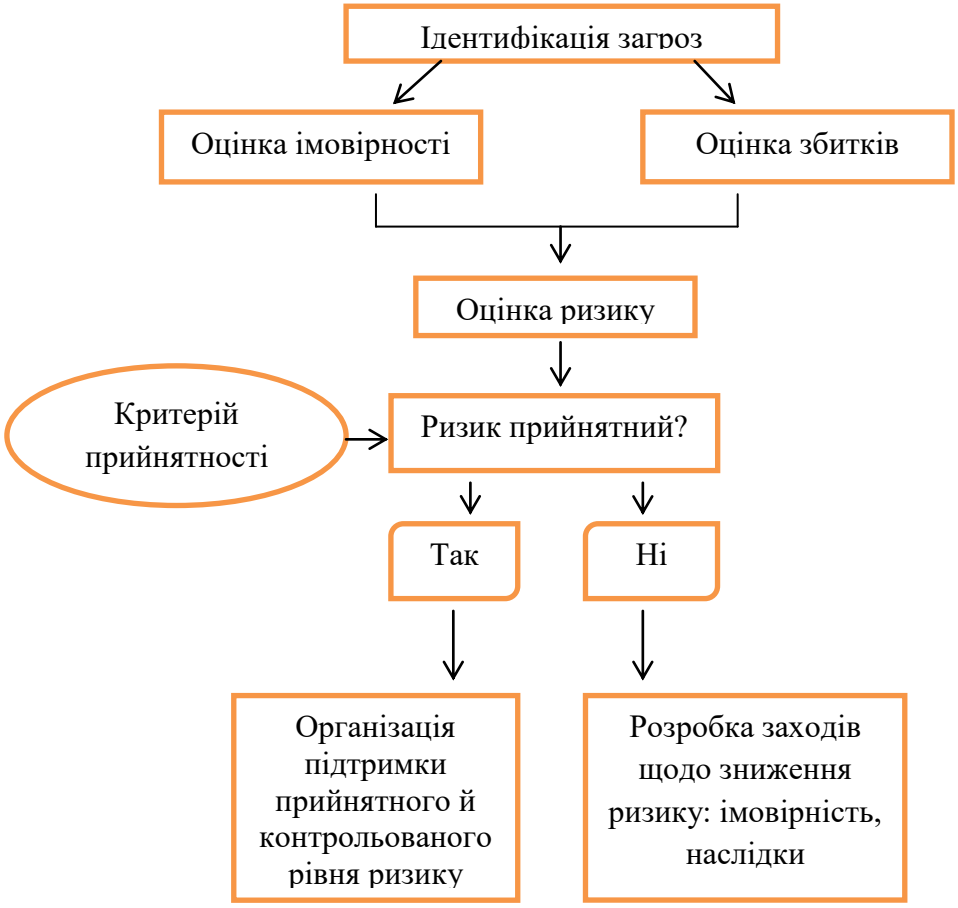

Рисунок 1 – Блок-схема аналізу ризику

Найважливішим елементом аналізу ризику є оцінка ймовірностей і повторюваності несприятливих подій. Для прогнозування НС застосовуються закони розподілу ймовірності Пуассона й статечні розподіли.

Приймемо раніше розроблені методичні апарати аналізу ризиків для обґрунтування рішень і дій посадових осіб за збереження всіх основних якостей інформації – конфіденційності, цілісності та доступності. Модель оцінки ризику припускає, що за певний проміжок часу середній ризик, спричинений подією A, можна визначити за допомогою виразу (1)

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

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 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 A (ризик, що трапився під час події) дорівнює

$$P(A) = \frac{\nu(t)}{T}\,, \qquad (2)$$

де $\nu(t)-$ кількість проявів події A за час t;

T – період спостереження.

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

$$R(A) = \frac{\nu(t)}{T}\ Y(A)\,, \qquad (1')$$

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) $M_{\text{вр.ел.}}$ до їхньої загальної кількості $M_{\text{заг.}}$ (число загальних елементів – кількість елементів ООТ, які опинилися в зоні ураження), зафіксований для події певної інтенсивності:

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

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

$$Y(A) = C_y(A)Y_n(A)\,, \qquad (4)$$

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.

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

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

Ця формула є загальною для обчислення ризику. При її практичному використанні в кожному конкретному випадку необхідно вносити уточнення. При розгляді частних 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:

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

де $R_ц(A)$ – частний ризик;

$P(H)$ – ймовірність перебування елементів певного типу в зоні ураження;

$C_{уц}(A)$ – ступінь уражаємості цієї групи елементів;

H – кількість елементів, що відповідає умовному повному збитку $Y_n(A)$ згідно з формулою (5).

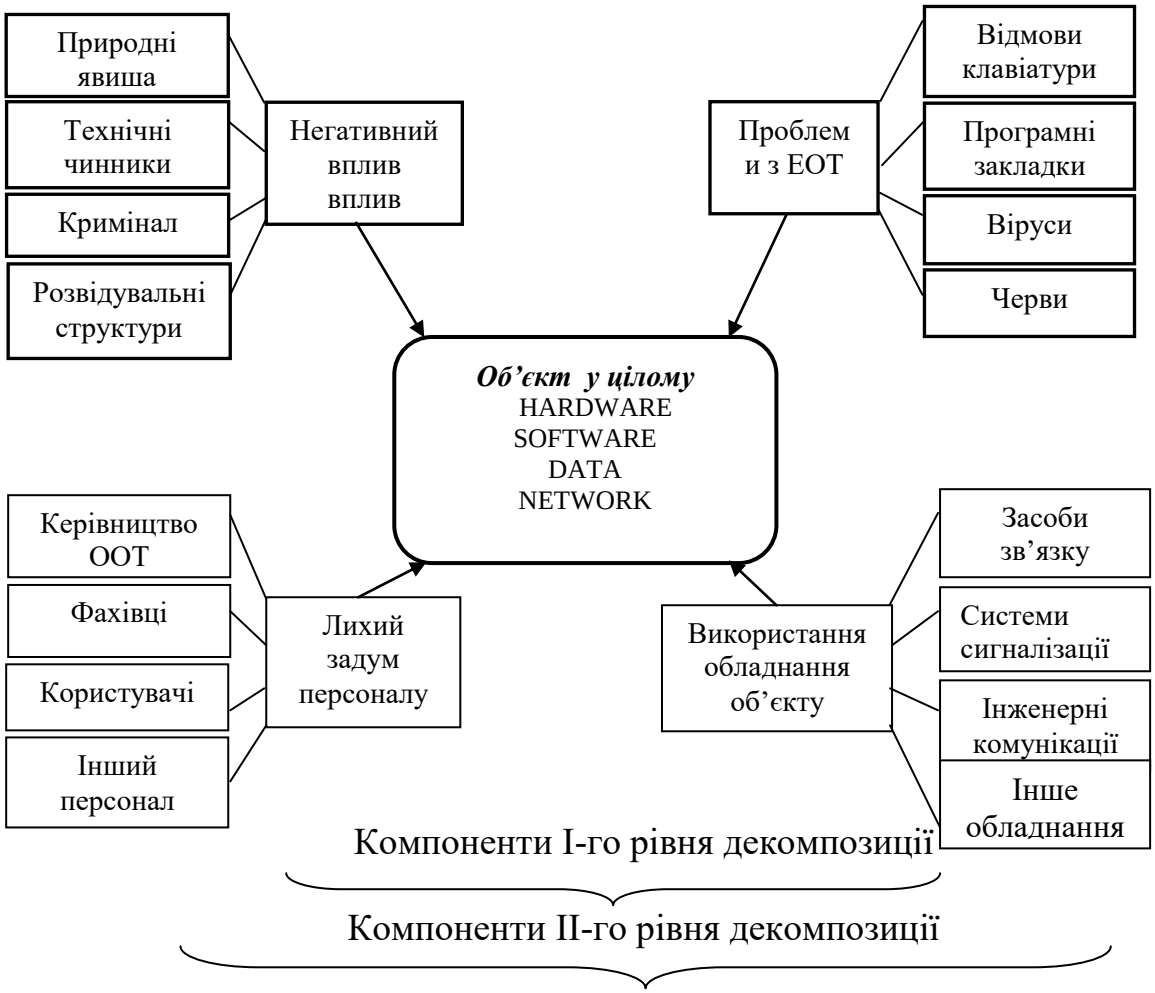

Рисунок 2 – Схема нарахування загального ризику

Розглянемо приклад нарахування загального ризику.

Дано.

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 $P_{\text{I}}(A) = 0{,}7$;

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

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

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): $R_{\text{I}}(A) = 0{,}7 \cdot 10 = 7$;

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

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

– 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):

$$C_{\text{I}} = \frac{7}{10}\ ;\ C_{\text{II}} = \frac{6}{10}\ ;\ C_{\text{III}} = \frac{2{,}5}{10} = 0{,}25;\ C_{IV} = \frac{0{,}6}{100}.$$

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

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

$$R_{\text{IIIодн.}}(A) = 0{,}25 \cdot 0{,}25 \cdot 10 = 0{,}625;$$

$$R_{\text{IV}\text{одн.}}\,(A) = \ 0{,}06 \cdot \frac{6}{100} \cdot 10 = \ 0,36.$$

Комбінований одномоментний збиток дорівнює:

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

4. Комбінований середній збиток дорівнює:

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

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 уражаємості дорівнюють:

– для апаратури

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

– для програмного забезпечення

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

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

– для апаратури

$$R_I^{(HARD)}(A) = 0{,}7 \cdot 0{,}25 * 10 \cdot 0{,}175 = 0{,}31\ ;$$

– для програмного забезпечення

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

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

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

– для програмного забезпечення

$$C_{ЧII}^{(SOFT)}(A) = \frac{0{,}6 \cdot 25}{50} = 0{,}3\ ;$$

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

– для апаратури

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

– 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

$$\mathrm{C}_{\mathrm{ЧIII}}^{(\mathrm{HARD})}(\mathrm{A}) = \frac{0{,}25 \cdot 10}{10} = 0{,}25\ ;$$

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

– для програмного забезпечення

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

$$C_{ЧIV}^{(SOFT)}(A) = \frac{0{,}06 \cdot 50}{50} = 0{,}06.$$

Тоді частні 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, частні 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:

7.

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

Безпека – це комплексний критерій оцінки якості будь-якої сучасної системи, яка характеризує як динаміку системи, так і її технічне втілення.

Особливе значення для нормального функціонування зазначених об’єктів має *забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах*.

Широке використання систем 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.

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.

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.

Проаналізуємо динаміку зміни небезпечних подій у часі. Якщо розуміти під безпекою ООТ відсутність неприпустимого ризику враження об'єкта при виникненні небезпечних ситуацій, то для її оцінки вводиться функція S_i.

Сукупність характеристик небезпечних подій, «зважених» з ймовірностями їх виникнення визначимо як функцію ризику H_i.

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

$$S_i(t) = exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}\right\} \quad (1)$$

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

де λ_i – інтенсивність небезпечних подій *i*-го порядку;

ρ_{ij} – ймовірність враження подією *i*-го виду *j*-ї компоненти досліджуваного

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

де $a_i(t)$ – математичне очікування числа подій *i*-го типу за період спостереження *T*;

T – період спостереження.

Наближено можна вважати, що

$$\rho_{ij} = \frac{n_{ij}}{n_i}$$

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

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

$$H_\Sigma(t) = \prod_{j=1}^{k} H_i(t) = 1 - exp\left\{-\mathrm{t} \sum_{j=1}^{k} \Lambda_j\right\}$$

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

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

Дано.

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

I. ймовірність виникнення проблеми із технікою $\rho_I\ (A)$ = 2,74;

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

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 частні 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 $Y = (A)$;

3. усі події вважаємо незалежними одна від одної;

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

Потрібно:

обчислити частні ризики від подій кожного виду;

обчислити комбінований ризик.

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

– для апаратури

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

– для програмного забезпечення

$$\rho_I{}^{SOFT} = \frac{15}{50} = 0{,}4;\ \rho_{II}{}^{SOFT} = \frac{2}{10} = 0{,}2;\ \rho_{III}{}^{SOFT} = \frac{5}{5} = 1;$$

$$\rho_{IV}{}^{SOFT} = \frac{1}{2} = 0{,}5;$$

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

– функції безпеки для апаратного забезпечення

$$S^{HARD}(t) = exp\left\{-t\sum_i^n \lambda_i\, \rho_{ij}{}^{HARD}\right\} =$$

$$= exp\,\{-t\,(2{,}74 \cdot 0{,}3 + 1{,}37 \cdot 0{,}3 + 0{,}8 \cdot 0{,}2 + 0{,}5 \cdot 0{,}5)\} = exp\,\{-1{,}643\,t\}$$

– функція ризику для апаратного забезпечення

$$H^{HARD}(t) = 1 - S^{HARD}(t) = 1 - exp\left\{-t\sum_i^n \lambda_i\, \rho_{ij}{}^{HARD}\right\} =$$

$$= 1 - exp\,\{-1{,}643\,t\}$$

– функції безпеки для програмного забезпечення

$$S^{SOFT}(t) = exp\left\{-t\sum_i^n \lambda_i\, \rho_{ij}{}^{SOFT}\right\} =$$

$$= exp\,\{-t\,(2{,}74 \cdot 0{,}4 + 1{,}37 \cdot 0{,}2 + 0{,}8 \cdot 1{,}0 + 0{,}5 \cdot 0{,}5)\} = exp\,\{-2{,}42\,t\}$$

– функція ризику для програмного забезпечення

$$H^{SOFT}(t) = 1 - S^{SOFT}(t) = 1 - exp\left\{-t\sum_i^n \lambda_i\, \rho_{ij}{}^{SOFT}\right\} =$$

$$= 1 - exp\,\{-2{,}42\,t\}$$

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

$$S_{\sum}(t) = S^{SOFT}(t) \cdot S^{HARD}(t) =$$

$$= exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{SOFT} + \sum_{i}^{n} \lambda_i \rho_{ij}{}^{HARD}\right\} = \exp\{-4{,}063\}$$

$$H_{\sum}(t) = H^{SOFT}(t) \cdot H^{HARD}(t) =$$

$$= 1 - exp\left\{-t \sum_{i}^{n} \lambda_i \rho_{ij}{}^{SOFT} + \sum_{i}^{n} \lambda_i \rho_{ij}{}^{HARD}\right\} = \exp\{-4{,}063\}$$

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

Висновки

1. 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.

2. 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.