УДК 35.078.3

В.О. Собина, к.т.н., нач. каф., НУЦЗУ,
Л.В. Борисова, к.ю.н., доцент, НУЦЗУ,
О.В. Біляєва, нач. відділу, ІДУЦЗ

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДРОЗДІЛУ ДСНС УКРАЇНИ

(представлено д.т.н. Соловйом В.В.)

Показано, що при управлінні безпекою слід керуватися оцінками ризику всього спектру небезпек, можливих для досліджуваного об'єкту при його роботі, прийняття заходів щодо зниження ризику на найбільш несприятливих напрямках, відтворення потоку небезпечних подій та їх впливу на роботу організації, використовувати інші типи потоків поді. Вагомі перспективи має застосування теорії систем масового обслуговування.

Ключові слова: інтенсивність та ризик, теорія систем масового обслуговування, стратегії захисту, інтенсивність потоку подій.

Постановка проблеми. Відповідно до Стратегії національної безпеки, затвердженій Указом Президента України від 26.05.2015 № 287/2015 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).

Кожний конкретний об'єкт є індивідуальним набором параметрів та інформаційних додаткових даних. Ступінь впливу параметрів один на одного досить різний і визначає швидкість наростання аварійного процесу. Кожний параметр в інформаційній базі має: своє критичне значення, вище якого він переходить в передаварійну область; свій поріг аварійності. Слід зазначити, що всі параметри інформаційної бази взаємозалежні, впливаючи один на одного тою чи іншою мірою. 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. Метою роботи є аналіз ризиків інформаційної безпеки, що становлять собою усвідомлену небезпеку (загрозу) настання в будь-якій системі негативної події з окреслиними у часі та просторі наслідками або існування чи можливість виникнення ситуації при якій формуються передумови протидії реалізації задач і функції підрозділу ДСНС і забезпеченню й безпеки є актуальною.

Аналіз останніх досліджень і публікацій показав, що перші дослідження інформаційної безпеки в умовах надзвичайних ситуацій зроблені в роботах І. Давидова [7], Р. Гайковича і А. Першина [3]. У подальшому проблематиці було присвячено цілу низку наукових праць [2, 3, 4, 5] тощо. Разом з тим, особливе значення для нормального функціонування об'єктів має забезпечення безпеки інформаційної інфраструктури країни при аваріях, катастрофах і стихійних лихах. Безпека – це комплексний критерій оцінки якості будь-якої сучасної системи, яка характеризує як динаміку системи, так і її технічне втілення, що визначило мету публікації.

Постановка завдання та його вирішення. На кожному з етапів процесу побудови стратегії інформаційного забезпечення безпеки необхідно отримати числовий показник ризику або чіткості захисту. Повний ризик для всього об'єкта буде рівним сумі частих ризиків для груп елементів кожного типу, які складають досліджуваний об'єкт. Відправною точкою в процесі забезпечення безпеки є аналіз потреб і проблем, які виникли або можуть виникнути із плином часу. Головне при цьому – гарантувати повноцінний обіг інформації (рис. 1.).

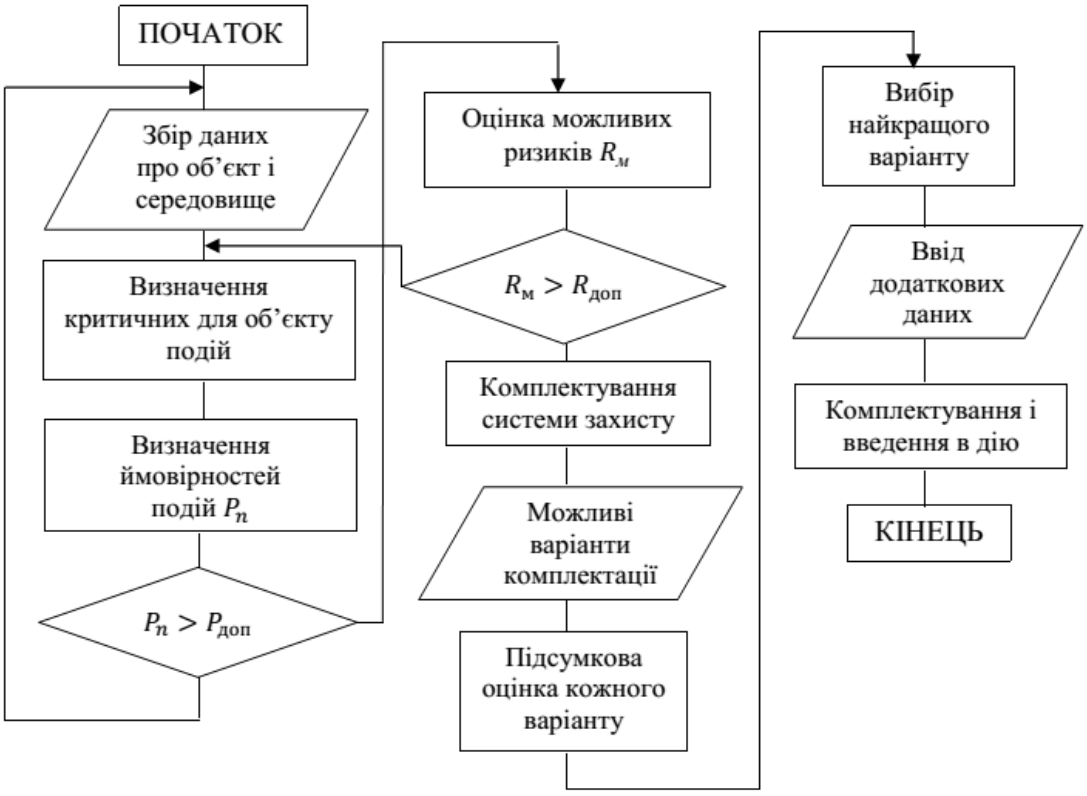

Рис. 1. Алгоритм обігу інформації

Як визначено у роботах повний ризик для всього об'єкта буде рівним сумі частих ризиків для груп елементів кожного типу, які складають досліджуваний об'єкт [6]. Але пуассонівський потік має обмеження щодо застосування на практиці, головне з яких – прийнято, що події відбуваються рівномірно у часі, а системи безпеки реагують на кожну із таких

подій. Такий опис прийнятний для систем, де $P(A) \to 1$ (на підставі аналізу) та $\rho \to 1$ (на підставі прогнозу) [2].

Такий потік виправдовує себе у разі однакової значущості ресурсів, що захищаються, або можливих загроз. Реально ж можливі джерела загроз і ресурси, які підлягають захисту – нерівноцінні. Тобто до оцінки всього спектра небезпек та можливих засобів захисту слід підходити комплексно, а до формування і оцінки конкретного варіанту стратегії захисту – фрагментарно.

Розглянемо варіант функції безпеки/ризику, що ґрунтується на застосуванні нормованому розподілу Ерланга. Системи безпеки реагують на можливу загрозу тільки в тому випадку, коли ймовірність виникнення небезпечної події і-го виду (наприклад, в певні пори доби) перевищує гранично допустимий рівень, тобто інтенсивність потоку подій зростає. У такому разі середній інтервал між подіями, незалежно від значення їх ймовірності, рівний

$$\tau = \frac{1}{\lambda_i}, \tag{1}$$

де λ_i – інтенсивність потоку подій, обчислена за формулою

$$\lambda_i = \frac{a_i(t)}{T}, \tag{2}$$

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

Тоді часткова функція безпеки для загроз і-го виду дорівнює

$$S_i(t) = k\lambda_i \frac{(k\lambda_i t)^{k-1}}{(k-1)!} e^{-k\lambda_i t}, \tag{3}$$

де k – для наближених обчислень можна за порядок потоку приймати кількість потоків ймовірністю вище допустимої (наприклад, 2 потоки (k=2), 5 потоків (k=5) і т.д.

Показано [6], що при $k \geq 5$ нормований розподіл Ерланга може бути апроксимований як нормальний.

Вид функції безпеки нормального розподілу

$$S_i = \frac{1}{\sqrt{2\pi\sigma}} \exp\left\{-\frac{1}{2}\left(\frac{t-M}{\sigma}\right)\right\}. \tag{4}$$

Тут $\sigma = \sqrt{D}$, $M = \tau$, де D і M – дисперсія і математичне очікування розподілу відповідно.

Наступним кроком формалізації може бути застосування теорії систем масового обслуговування різних видів.

1. Проаналізуємо систему S, яка підлягає захисту. До розгляду беруться наступні формалізовані об'єкти опису:

– множина $Z = \{z_1, z_2, ...z_k, ...z_K\}$ – клас захисних послуг, які, виходячи із результату попереднього етапу, необхідно надати системі S для забезпечення її безпеки;

– вектор значень $\overrightarrow{U} = \langle u_1, u_2, ...u_m, ...u_M \rangle$, де u_m – значення потреби системи S в m-му види ресурсу, що обчислюється, для її нормального функціонування;

– вектор значень $\vec{W} = \langle w_1, w_2, ...w_m, ...w_M \rangle$, де w_m – величина обсягу потреби m-го виду обчислювального ресурсу, який виділяється системі *S* з урахуванням організації її підсистеми захисту.

2. Комплекс модульних засобів, з яких комплектуються підсистеми забезпечення безпеки інформації програмно-апаратних систем класу S. Аналізуються наступні об'єкти формалізованого опису цього комплексу:

– програмні модулі різних служб захисту і функціональних процесів у вигляді множини $A = \{a_1, a_2, ...a_n, ...a_N\}$, в якій кожний модуль a_n служби захисту реалізує деякі підмножини послуг $G_n = \{g_{n1}, g_{n2}, ...g_{ni}, ...g_{nk}\}$;

– обчислювальні ресурси, необхідні для забезпечення нормального функціонування кожного модуля a_n, $n = \overline{(1, N)}$, який буде введений до складу підсистем захисту як матриця значень $V = \|V_{nm}\|$, $n = \overline{1, N}$, $m = \overline{1, M}$, де зміна n визначає модуль a_n, а зміна m – вид обчислювального ресурсу, що спожито, вектор значень $\vec{C} = \langle c_1, c_2, ...c_n, ...c_N \rangle$ – показники вартості пристроїв захисту інформації, встановлення і супроводу служб захисту.

Для вирішення поставленого завдання формуємо первинну матрицю інцидентності $Q = \|q_{nk}\|$, в якій кожному рядку взаємно однозначно відповідає модуль a_n, $n = \overline{(1, N)}$ захисту із множини A, а кожному стовпцю вид послуги z_k, $\overline{(k = 1, K)}$, який є потрібним системі S для організації захисту, і

$$q_{nk} \begin{cases} 1, \text{ якщо } z_k \in G_n \\ 0 \text{ - в іншому випадку.} \end{cases} \quad (5)$$

По матриці інцидентності $Q = \|q_{nk}\|$ відшукаємо всі варіанти мінімального покриття сукупностями рядків (захисних модулів) всіх стовпців (захисних послуг, які використовує система S. Стовпець z_k $\left(k = \overline{1,K}\right)$, вважаємо покритим, якщо в обраній сукупності h_i рядків a_{ir} є хоч один елемент $a_j \in h_i$ такий, що $q_{jk} = 1$. Мінімальність покриття інтерпретується як відсутність лишнього рядка у вибраній сукупності множини всіх видів послуг, що можуть бути надані для виконання захисних функцій в системі S у вимогах до підмножини h_i.

Алгоритм знаходження множини мінімальних покрить матриці інцидентності, базований на булевій алгебрі:

1. Сформувати матрицю інцидентності $Q = \|q_{nk}\|$.

2. Визначити підмножину B базових модулів $a_n, n = \left(\overline{1,N}\right)$. Модуль a_n є базовим, якщо існує стовпець z_j такий, що $q_{ij} = 0$ для всіх i=1,2,…n–1,n+1,…N. Модулі $a_n \in B$ повинні входити в усі варіанти мінімальних покрить, а відповідні рядки можна викреслити із матриці інцидентності.

3. Зменшити розмірність матриці Q, що отримана у п. 2 шляхом послідовного викреслення зайвих стовпців, а далі – зайвих рядків. Стовпець z_k є зайвим, якщо існує стовпець z_j такий, що $q_{nk} = q_{nj}$ для всіх стовпців z_k, що залишилися.

4. Якщо матриця Q, отримана в п.3 виявиться порожньою, то в якості множин H можливих варіантів рішення зафіксувати підмножину B базових модулів і перейти до п.8. Якщо ж матриця Q не порожня, то перейти до п. 5.

5. Знайти варіанти мінімальних покрить матриці Q, яка отримана в п.3, для чого:

– побудувати диз'юнктивний терм по змінним $a_n \in A$, які відповідають рядкам у матриці Q. Для стовпця z_k, який залишився, диз'юнктивний терм утворюють тільки змінні a_n, для яких $q_{nk} = 1$;

– записати булевий вираз у вигляді кон'юнкції диз'юнктивних термів, отриманих вище;

– розкрити дужки і спростити отриманий булевий вираз, подавши кінцевий результат у вигляді диз'юнктивної нормальної форми.

6. Сформувати множину H можливих варіантів рішення. Для цього у відповідності із кожним кон'юнктивним термом отриманого кінцевого булевого виразу, отриманого у п.5, створити окрему підмножину модулів захисту і доповнити його елементами базової підмножини B.

7. Перевірити виконання заданих обмежувальних умов. У підмножині $H = \{h_i\}$ залишити варіанти, які задовольняють обмежувальні умови.

8. Якщо множина H не порожня, то вона визначає область допустимих рішень, яка підлягає подальшому аналізу для вибору оптимального рішення.

Для спрощення обчислень пропонуємо наперед установити рівні рентабельності захисних засобів і відповідно до них поставити у відповідність абсолютним значенням, (отриманим за формулою, яка визначає можливі одномоментні збитки

$$Y(A) = C_y(A) Y_n(A), \tag{6}$$

де $Y_n(A)$ – умовний повний збиток, який чисельно рівний кількості або вартості всіх елементів (або кількості або вартості тих елементів, які опинилися в зоні ураження), оцінку за бальною шкалою (рангову оцінку). Наприклад, якщо B < 1 – оцінка 2; B =1– оцінка 3; B > 1– оцінка 4; *B* >> 1 – оцінка 5. Позначимо рангову оцінку через B.

Утворимо вторинну матрицю інцидентності: (0,1) – матрицю розмірності mxn (у загальному випадку $m \neq n$) для кожної із множин $h_1 - h_4$: розставивши по стовпцях можливі значення оцінок в порядку спадання зліва направо (n), а по рядках – елементи множин $h_1 - h_4 (m)$в порядку зменшення їх важливості (пріоритетності).

За означенням, елемент матриці буде приймати значення

$$a_{ij} \begin{cases} 1, \text{якщо i - й елемент досліджуваної множини} \\ \text{отримує j - ту оцінку} \\ 0, \text{в іншому випадку.} \end{cases} \tag{7}$$

Наприклад, при чотирьох бальній системі оцінок матриця матиме вигляд (табл. 1)

Табл. 1. Матриця оцінок інциндентності

Ел-ти, що оцінюються	Рівень пріоритетності	«5»	«4»	«3»	«2»
Елемен.1	k-й найвищий	0	1	0	0
Елемен.2		1	0	0	0
…	……	..	..	..	..
Елем. i-1	j-й	1	0	0	0
Елем. i	j-й	0	0	1	0
Елем. i+1	j-й	0	0	1	0
…	……	..	..	..	..
Елем. m-1	1-й	0	0	0	1
Елем. m	(найнижчий)	0	0	0	1

Зрозуміло, що в кожному рядку може бути лише одна одиниця (кожен елемент отримує лише одну оцінку), тоді як на колонки це прави-

ло не поширюється (дану оцінку може не отримати жоден із елементів, або її отримали всі елементи).

Кожен із елементів досліджуваної множини, який потрапляє до матриці інцидентності, отримує «вагу» W відповідно до своєї значимості в загальній системі. При цьому необхідно витримати умову

$$\sum_{i=1}^{m} W_i = 1, \qquad (8)$$

де m – число прийнятих до оцінювання параметрів.

У загальному випадку, в досліджуваній системі кількість рівнів пріоритетності може не співпадати з кількістю елементів (j< >j), тобто декілька (або всі) елементи можуть мати однакову важливість, і, відповідно, рівень пріоритетності буде однаковий (табл. 1).

З огляду на значне коло охоплюваних при оцінці елементів і чинників, в процесі практичного застосування даного алгоритму може виникнути потреба в накладанні обмежень та допущень на окремі елементи, що досліджуються, для більш змістовного дослідження тих елементів, що становлять найбільший інтерес.

Висновки. Забезпечення безпеки може бути досягнуте двома способами: по-перше, вжиттям всіх практично можливих заходів, по-друге, зниженням ризиків до прийнятного рівня.

Використання запропонованого математичного апарату дозволить обґрунтовано розробити практичні заходи для досягнення потрібного рівня безпеки інформації.

ЛІТЕРАТУРА

1. Біленчук П.Д. Аналіз та прогноз стану об’єкту обчислювальної техніки / П.Д. Біленчук, В.Б. Міщенко, Л.В. Борисова // Открытые информационные и компьютерные интегрированные технологии: Сб. научн. Трудов. – Х.:НАКУ «ХАИ», 2002. – Вип. 13. – С. 127-135.

2. Брагин О.В. Аналитическое обеспечение мероприятий безопастности – 2 / О.В. Брагин // Бизнес и безопастность. – 2001. – №2. – С. 5-7.

3. Солоп А.А. Формирование комплекса экономической безопастности предприятия / А.А. Солоп // Бизнес и безопастность. – 2001. – №1. – С. 6-7.

4. 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.

5. 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. на-

ук. пр. – Вип. 21. – Х.: НУЦЗУ, 2015. – С. 89-96. – Режим доступу: http://nuczu.edu.ua/sciencearchive/ProblemsOf Emergencies/vol21/Sobina.pdf.

6. Шубенкин В.А. Прикладные модели теории массового обслуживания / В.А. Шубенкин, В.С. Донченко. – К.: НМК ВО, 1992. – 298 с.

Отримано редколегією 12.10.2016

В.А. Собина, Л.В. Борисова, О.В. Биляева

Теоретико – прикладные засады информационной безопасности подразделения ГСЧС Украины

Показано, что при управлении безопасностью следует руководствоваться оценками риска всего спектра опасностей, возможных для исследуемого объекта при его работе, принятие мер по снижению риска на наиболее неблагоприятных направлениях, воспроизведение потока опасных событий и их влияния на работу организации, использовать другие типы потоков событий. Весомые перспективы имеет применение теории систем массового обслуживания.

Ключевые слова: интенсивность и риск, теория систем массового обслуживания, стратегии защиты, интенсивность потока событий.

V.A. Sobina, L.V. Borisova, O.V. Biljajeva

Theoretical and applied ambush information security divisions of PSES Ukraine

It is shown that the security management should be guided by risk assessments of the entire spectrum of dangers that are possible for the test object during its operation, the adoption of risk reduction measures on the most unfavourable directions, playing a stream of dangerous events and their impact on the work of the organization, to use other types of event streams. Significant prospects for the application of the theory of queueing systems.

Keywords: intensity and risk, the theory of mass service systems, defense strategies, the intensity of the flow of events.