$3{,}1 \cdot 10^{-1}$ с) и поэтому не вносят больших погрешностей при переходе в режим адсорбции и измерения аналитического сигнала.

УДК 35.078.3

МАТЕМАТИЧНИЙ АПАРАТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДРОЗДІЛУ ДСНС

В.О. Собина, канд. техн. наук, доцент, НУЦЗУ,
Л.В. Борисова, канд. юр. наук, доцент, НУЦЗУ

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. Одним із кроків 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; 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 $\overrightarrow{W} = \langle w_1, w_2, ...w_m, ...w_M \rangle$, 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; обчислювальні ресурси, необхідні для забезпечення нормального функціонування кожного модуля a_n, $n = (\overline{1, N})$, який вводиться 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, $(k = \overline{1, K})$, який є потрібним системі S для організації захисту, і

$$q_{nk} \begin{cases} 1, \text{ яякщ } z_k \in G_n, \\ 0 - \text{в іншому випадку.} \end{cases}$$

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 $(k = \overline{1, K})$, 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 Sy 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 $a_n, n = (\overline{1, N})$. 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.

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 $Y(A) = C_y(A)Y_n(A)$, де $Y_n(A)$– умовний повний збиток, який чисельно рівний кількості або вартості всіх елементів, які опинилися в зоні ураження, оцінку за бальною шкалою (рангову оцінку). 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 пріоритетності. За означенням, елемент матриці буде приймати значення: $a_{ij} \begin{cases} 1, \text{якщ } i\text{-й елемент досліджуваної множини;} \\ \text{отримує } j\text{-ту оцінку;} \\ 0, \text{в іншому випадку} \end{cases}$

Кожен із елементів множини, який потрапляє до матриці

інцидентності, отримує «вагу» W відповідно до своєї значимості в загальній системі. При цьому необхідно витримати умову: $\sum_{i=1}^{m} W_i = 1$, де m – число прийнятих до оцінювання параметрів.

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.

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

УДК 35.078.3

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДРОЗДІЛУ ДСНС УКРАЇНИ

В.О. Собина, канд. техн. наук, доцент, НУЦЗУ,
Л.В. Борисова, канд. юр. наук, доцент, НУЦЗУ

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. 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. Відповідно, 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 актуальним.

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.).

Як визначено у роботах повний ризик для всього об'єкта буде рівним сумі частних ризиків для груп елементів кожного типу, які складають досліджуваний об'єкт [1]. 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