18. *Борисов В.И.* Помехозащищённость систем радиосвязи. Вероятностно-временной подход / Борисов В.И., Зинчук В.М. – [изд. 2-е, исправленное] – М.: Радио Софт, 2008. – 260 с.

19. *Кристофидес Н.* Теория графов. Алгоритмический подход. – М. Мир, 1978. – 432 с.

Рецензент: Єрохін В.Ф.
Надійшла 24.01.2011

УДК 004.681

Левченко Є. Г., Рабчун А. О. (нац. авіац. унів.)

НЕПЕРЕРВНІ МАРКОВСЬКІ ЛАНЦЮГИ В ЗОБРАЖЕННІ СТАНІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ми розглянули спроби вилучення інформації як кроки марковського ланцюга з дискретними станами і дискретним часом. В реальних ситуаціях ці спроби можуть здійснюватись не в певні дискретні, а й у будь-які моменти, тобто являють собою марковські випадкові процеси з дискретними станами і неперервним часом, або неперервні марковські ланцюги [2,3]. В цьому випадку стан інформаційної безпеки оцінюється не кількістю кроків, а при заданій інтенсивності потоку подій – часовою залежністю імовірностей переходу системи зі стану в стан. Імовірність $p_i(t)$ знаходження системи в i-му стані в момент t визначається системою диференціальних рівнянь Колмогорова:

$$\frac{dp_i(t)}{dt} = -\sum_{i=1}^{n} \lambda_{ij} p_i(t) + \sum_{j=1}^{n} \lambda_{ij} p_j(t), \quad i = \overline{1,n}, \quad t \geq 0,$$

де i та j - номери станів;

$\lambda_{ij} = \lambda_{ij}(t) = \lim\limits_{\Delta t \to 0} \frac{p_{ij}(t, \Delta t)}{\Delta t}$ - щільність імовірності переходу системи зі стану S_i в стан S_j;

$p_{ij}(t, \Delta t)$ - імовірність переходу системи зі стану S_i в стан S_j.

Розглянемо інформаційну систему, яка складається з трьох однакових об'єктів, захищених чотирма перешкодами, розташованими за послідовно-паралельною схемою (рис.1).

Одна з перешкод є загальною (це може бути периметр території, що охороняється), інші – індивідуальні (окремі приміщення). Кожен з об'єктів містить об'єм інформації g. Через X і Y позначено загальна кількість ресурсів нападу і, відповідно, захисту.

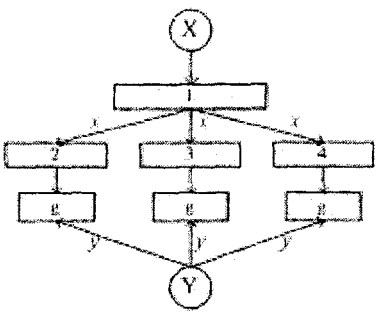

рис. 1

На подолання кожної з перешкод напад виділяє кількість ресурсів x ($X=4x$), на захист кожного з об'єктів – кількість ресурсів y ($Y=3y$).

Вважатимемо, що напади здійснюються послідовно, утворюючи ординарний пуассонівський випадковий потік, який формує неперервний марковський ланцюг. Протистояння відбувається за такою схемою. Напад спрямовується спочатку на першу перешкоду, а після її подолання напади розподіляються рівномірно на подолання всіх інших перешкод. Стани інформаційної системи визначимо наступним чином:

S_1 – вся система непорушна;

S_2 – подолана тільки перша перешкода (інформація ще не вилучена);

S_3 – подолана одна з індивідуальних перешкод, вилучена інформація кількістю g з одного об'єкта;

S_4 – подолані дві індивідуальні перешкоди, вилучено $2g$ інформації;

S_5 – подолані всі перешкоди, вилучена вся інформація кількістю $3g$.

Позначимо: λ – інтенсивність нападів, тобто їх кількість в одиницю часу, p – імовірність того, що напад буде успішним і перешкода буде подолана. Тоді λp – інтенсивність успішних нападів, яка в нашій системі виражає щільність імовірності λ_{ij} переходу систем з i-го в j-ий стан. За рахунок рівномірності зміни станів ця величина однакова для всіх переходів: $\lambda_{ij} = \lambda p$.

Граф сформульованої задачі завдяки ординарності пуассонівського потоку носить не розгалужений, а послідовний характер (рис.2).

рис. 2

Приведеному графу відповідає система рівнянь Колмогорова:

$$\frac{dp_1}{dt} = -\lambda p p_1$$

$$\frac{dp_2}{dt} = -\lambda p p_2 + \lambda p p_1$$

$$\frac{dp_3}{dt} = -\lambda p p_3 + \lambda p p_2$$

$$\frac{dp_4}{dt} = -\lambda p p_4 + \lambda p p_3$$

$$\frac{dp_5}{dt} = \lambda p p_3.$$

Початкові умови:

$$p_1(0) = 1, p_2(0) = p_3(0) = p_4(0) = p_5(0) = 0.$$

В цій системі імовірність p досягнення результату при нападі – величина відома, а імовірності станів p_i - невідомі, які необхідно визначити. Розв'язок почнемо з першого рівняння, яке є відокремленим, оскільки містить лише одну невідому – p_1. Застосуємо перетворення Лапласа:

$$p_1(t) \to \tilde{p}_1(\nu).$$

Змінну в перетворенні Лапласа позначаємо через ν, оскільки через p ми позначаємо імовірність. Перше рівняння після перетворення має вигляд:

$$\tilde{p}_1(\nu) - p_1(0) = -\lambda p \tilde{p}_1(\nu) \Rightarrow \tilde{p}_1(\nu) = \frac{1}{\nu + \lambda p}, \quad p_1(t) = e^{-\lambda p t}.$$

Друге рівняння після перетворення має вигляд:

$$\tilde{p}_2(\nu) - p_2(0) = -\lambda p \tilde{p}_2(\nu) + \frac{\lambda p}{\nu + \lambda p} \Rightarrow \tilde{p}_2(\nu) = \frac{\lambda p}{(\nu + \lambda p)^2},$$

$$p_2(t) = \frac{\lambda p t}{1!} e^{-\lambda p t}.$$

Аналогічно маємо для наступних рівнянь:

$$\tilde{p}_3(\nu) - p_3(0) = -\lambda p \tilde{p}_3(\nu) + (\frac{\lambda p}{\nu + \lambda p})^2 \Rightarrow \tilde{p}_3(\nu) = (\frac{\lambda p}{\nu + \lambda p})^2,$$

$$p_3(t) = \frac{(\lambda p t)^2}{2!} e^{-\lambda p t}.$$

$$\tilde{p}_4(\nu) - p_4(0) = -\lambda p \tilde{p}_4(\nu) + (\frac{\lambda p}{\nu + \lambda p})^3 \Rightarrow \tilde{p}_3(\nu) = (\frac{\lambda p}{\nu + \lambda p})^3,$$

$$p_4(t) = \frac{(\lambda p t)^3}{3!} e^{-\lambda p t}.$$

І нарешті:

$$p_5(t) = 1 - (1 + \lambda p t + \frac{(\lambda p t)^2}{2!} + \frac{(\lambda p t)^3}{3!}) e^{-\lambda p t}.$$

При практичному застосуванні одержаних виразів необхідно задати кількість успішних нападів за одиницю часу λp. Величину інтенсивності потоку нападів λ визначимо з аналізу статистичних даних, а імовірність p подолання перешкоди визначимо через співвідношення ресурсів нападу і захисту X і Y, або в статистичному плані – як частку f вилученої з об'єкта інформації при заданому співвідношенні x/y [ ]. Цю залежність задамо у вигляді дробно-лінійної функції:

$$f(x, y) = \frac{(x/y)^2}{(x/y)^2 + 16}.$$

Числові параметри в знаменнику цієї залежності визначаються з умови досягнення реальних, з нашої точки зору, величин f при певних значеннях x/y (наприклад, при $x/y=1$ $f(x,y)=0.10$; при $x/y=3$ $f(x,y)=0.21$; при $x/y \to \infty$ $f(x,y) \to 0.5$, а не 1, що в основному визначається початковою, природною захищеністю об'єкта).

Наприклад, візьмемо $\lambda=5/міс$ (5 нападів на місяць); $x/y=1$, звідки $p=f(x,y)=0.1$. При цьому $\lambda p=0.5$ $1/міс$ (імовірність подолання однієї перешкоди за 1 місяць складає 50%). Імовірності станів, визначені приведеними виразами, зображені на рис.3.

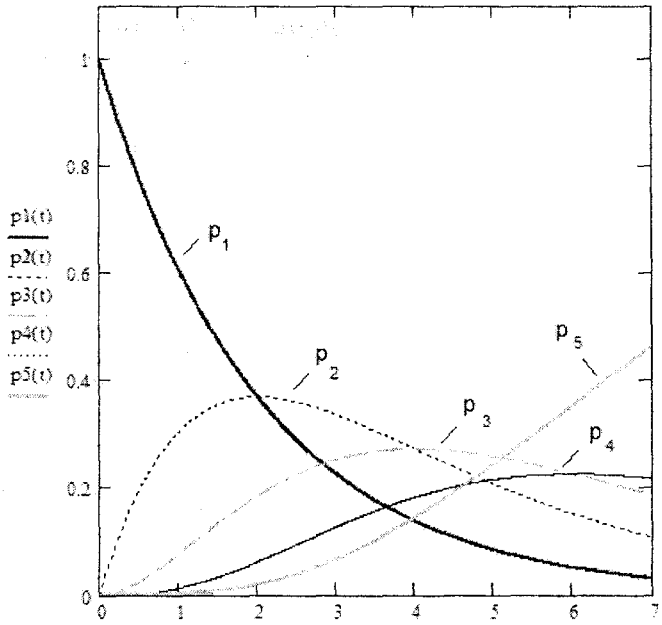

рис.3 Імовірності станів в залежності від часу.

Значення t_{im} , при яких досягаються максимальні значення p_{im} імовірностей p_i, можна знайти з виразів для p_i . При $i = \overline{2,4}$ $t_{im} = \dfrac{i-1}{\lambda p}$. $p_1(t)$ досягає максимуму $p_{1max} = 1$ при $t_{1max} = 0$, для $p_5(t)$ максимальне значення $p_{5max} = 1$ досягається при $t_{5max} = \infty$.

Приведена методика носить ілюстративний характер і може бути розповсюджена на складніші системи, які відрізняються такими показниками:

1) кількість об'єктів і розташування перешкод;

2) співвідношення ресурсів нападу і захисту $\dfrac{X}{Y}$;

3) кількість інформації g_k на об'єктах і форма залежності $f(x,y)$ вразливості від величин x та y на об'єктах;

4) розподіл x_k по об'єктах.

Подальший розвиток методики може вестись як в напрямку розрахунку додаткових показників (наприклад, кінцевого стану інформаційної системи), так і в бік ускладнення умов, зокрема комплексного протистояння, коли кожна сторона частину ресурсів витрачає на захист своїх об'єктів, а другу частину – на здобуття інформації про суперника.

Список літератури

1. Левченко Є.Г., Рабчун А.О. Марковські ланцюги у визначенні станів інформаційної безпеки. – Інф. безпека: Матеріали наук.-практ. Конф. (Київ, ДУІКТ, 26-27 березня 2009 р.), с. 239-242.

2. Вентцель Е.С. Исследование операций. – М.: Сов.радио,1972. – 552с.

3. Тихонов В.И., Миронов М.А. Марковские процессы. – М.: Сов. радио, 1977. – 448с.

Рецензент: Козловський В.В.
Надійшла 03.02.2011