3. Гинзбург С.Г. Методы решения задач по переходным процессам в электрических цепях. – 2-е изд., перераб. и доп. – М.: Советское радио, 1959. – С. 404.

Надійшла 13.4.2011 р.

УДК 004: 004.65

А.В. ДЖУЛІЙ
Хмельницький національний університет

ПОНЯТІЙНИЙ АПАРАТ, ВИКОРИСТОВУВАНИЙ ПРИ РОЗРОБЦІ МОДЕЛЕЙ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті досліджено переваги застосування пуасоновських потоків при розробці моделей функціонування системи захисту інформаційних ресурсів. Постулювання такого типу потоків набагато спрощує дослідження і призводить до конструктивних рішень. Пуасоновські потоки є граничними для різних інших "непуасоновських" потоків. Зокрема, при накладенні великого числа таких потоків один на одного сумарний потік виявляється близьким до пуасоновського для широкого класу умов. Та ж картина має місце, якщо довільно взятий потік піддати випадковому розрідженню, викидаючи з нього ті чи інші події.

The article examines the benefits of puasonovskyh flows in developing models of the system of protection of information resources. Postulating this type of flow is much easier and results in research design decisions. Puasonovski flows are limiting for various other "nepuasonovskyh" flows. In particular, when imposing a large number of such flows on each total flow appears to be close to puasonovskoho for a wide range of conditions. The same pattern occurs when subjected to flow freely taken accidentally releasing, throwing him from certain events.

Ключові слова: система захисту, пуасоновський потік, марківський процес, потоки подій.

Вступ. Проблема розробки і вибору ефективних методів і засобів захисту комп'ютерних систем від атак в значній мірі залежить від ресурсів, на які спрямовані атаки, зовнішніх проявів, можливостей порушень характеристик безпеки та інших факторів. Ефективність її рішення в першу чергу пов'язана з визначенням того, на які класи атак розраховані ті чи інші методи та засоби протидії [1].

Зростання погрози несанкціонованого доступу нелегальних користувачів до електронних джерел інформації вимагає розробки й впровадження адекватних заходів щодо припинення подібних спроб. Протидія можливим незаконним проникненням в інформаційне поле об'єкта здійснюється програмно-апаратними засобами, сукупність яких утворює *систему захисту* цього об'єкта [2].

Постановка і предметне дослідження побудови ймовірнісної моделі оцінки якості системи захисту інформаційних риск\урсів в рамках формулюємих умов і обмежень вимагають залучення і використання певного математичного апарату. Таким апаратом, найбільш підходящим для цілей дослідження є детально розроблена теорія пуасоновський систем і марківських процесів, використовувана повсюдно в задачах подібного роду дисциплінах, які вивчають проблеми масового обслуговування, надійності і управління. Не заглиблюючись в аспекти цієї теорії, тут, все ж, доречно зупинитися на окремих положеннях, посилання на які неминучі по ходу викладу матеріалу дисертаційної роботи [3].

Основні положення. Пов'язуючи ці поняття з дискретними станами досліджуваних процесів і безперервним часом їх протікання, зазвичай виділяють такі *базові функціональні та числові показники [3],* якими характеризують випадкове час звершення подій:

1. Функція розподілу часу настання події –

$$F(t) = P(T < t),$$

якої визначається ймовірність того, що випадкова величина T прийме значення, менше заданого t.

2. Імовірність події, протилежної події $T < t$ –

$$\overline{F}(t) = R(t) = P(T > t).$$

3. Імовірність настання події в проміжку $(t, t + \Delta t)$ тривалістю Δt –

$$\Delta F(t, \Delta t) = F(t + \Delta t) - F(t).$$

4. Щільність розподілу ймовірностей часу настання події –

$$f(t) = \lim_{\Delta t \to 0} \frac{\Delta F(t, \Delta t)}{\Delta t} = \frac{dF(t)}{dt}.$$

5. Умовна ймовірність настання події за час Δt в інтервалі $(t, t + \Delta t)$ за умови, що в інтервалі (*0, t*) воно не наступило –

$$F(t, \Delta t) = \frac{\Delta F(t, \Delta t)}{R(t)} = \frac{\Delta F(t, \Delta t)}{1 - F(t)}.$$

6. Умовна ймовірність ненастання події за час Δt в інтервалі $(t, t + \Delta t)$ за умови, що в інтервалі (*0, t*) воно не наступило –

$$R(t,\Delta t)=1-F(t,\Delta t)=1-\frac{\Delta F(t,\Delta t)}{R(t)}.$$

7. Умовна щільність розподілу або інтенсивність настання подій –

$$\lambda(t)=\frac{f(t)}{1-F(t)}$$

– середнє число подій в одиницю часу (за досить малий проміжок часу).

8. Математичне очікування часу (середній час) настання події ($t> 0$) –

$$\theta=M[T]=\int_0^\infty tf(t)dt=\int_0^\infty R(t)dt.$$

9. Дисперсія часу настання події –

$$D[T]=\int_0^\infty t^2 f(t)dt-\theta^2.$$

Перераховані показники загальновідомі і навряд чи потребують будь-яких пояснень. Зазначимо тільки, що принципова відмінність щільності $f(t)$ і умовної щільності $\lambda(t)$ наочно з'ясовується з порівняння диференціальних форм

$$f(t)=-\frac{d}{dt}(R(t)),\quad \lambda(t)=-\frac{d}{dt}(\ln R(t)),$$

з яких слідує, що: щільністю $f(t)$ виражається швидкість зміни ймовірності того, що за час t подія не відбудеться; умовною щільністю $\lambda(t)$ виражається швидкість зміни натурального логарифма тієї ж ймовірності.

Зазначена відмінність проявляється в розходженності невласного інтеграла

$$\int_0^\infty \lambda(t)dt=-\int_0^1\frac{d(1-F(t))}{1-F(t)}=-\ln(1-F(t))\Big|_0^1=-\ln\lim_{F(t)\to 1}(1-F(t))-\ln 1=-\ln e^{-\infty}-0=\infty,$$

в той час як власний інтеграл

$$\int_0^\infty f(t)dt=\int_0^\infty dF(t)=F(t)\Big|_0^\infty=\lim_{t\to\infty}F(t)-F(0)=1$$

сходиться.

Основна частина. В [3] докладно вивчені властивості функції $\lambda(t)$. Зупинимося на одній з цих властивостей, якою усуваються неточності.

Покажемо, що не має похилих асимптот виду $y = at + b$ крива

$$\lambda(t)=\frac{f(t)}{1-F(t)}=\frac{f(t)}{1-\int_0^t f(t)dt} \tag{1}$$

За відомими формулами диференціального обчислення обчислимо коефіцієнти a, b рівняння прямої. Будемо мати, використовуючи правило Лопіталя, –

$$a=\lim_{t\to\infty}\frac{\lambda(t)}{t}=\left(\frac{0}{\infty.0}\right)=\frac{\lim\limits_{t\to\infty}f(t)}{\lim\limits_{t\to\infty}\dfrac{1-\int_0^t f(t)dt}{t}}=\frac{\lim\limits_{t\to\infty}f(t)}{\lim\limits_{t\to\infty}\dfrac{-f(t)}{-\dfrac{1}{t^2}}}=\lim_{t\to\infty}\frac{1}{t^2}=0$$

Таким чином, $a=0$ для будь-яких безперервних розподілів, оскільки вираз (1) – це загальна формула незалежно від виду розподілів. З рівності $a=0$ слідує відсутність похилих асимптот.

Відзначимо, що з (1) слідує наступне диференціальне рівняння:

$$-\lambda(t)dt=\frac{d(1-F(t))}{1-F(t)},$$

Звідки знайдемо, інтегруючи з точки $t = 0$ в поточну точку, такі формули:

$$\begin{cases} F(t)=1-e^{-\int_0^t \lambda(t)dt}, R(t)=e^{-\int_0^t \lambda(t)dt} \\ f(t)=\lambda(t)e^{-\int_0^t \lambda(t)dt} \end{cases} \quad (2)$$

Виразами (2) визначається так званий узагальнений показовий розподіл, з якого при $\lambda(t)=\lambda=const$ отримаємо канонічний експоненційний розподіл з параметром – λ:

$$F(t)=1-e^{-\lambda t},\ R(t)=e^{-\lambda t},\ f(t)=\lambda e^{-\lambda t},\ t\geq 0. \quad (2')$$

Обидва розподіли (переважно, (2')) грають фундаментальну роль у побудові пуасоновських систем теорії масового обслуговування і теорії надійності, оскільки, наприклад, з (2') ясно вбачається зв'язок між імовірнісними функціями $R(t)$, $F(t)$ і нескінченним дискретним розподілом Пуасона. Насправді, величина $a=\lambda t$ – це середнє число (математичне очікування) подій у проміжку тривалістю *t*, тому порівнюючи вирази $R(t)$, $F(t)$ з формулою ймовірностей

$$P_k=\frac{a^k e^{-a}}{k!},\ k=1,2,...,$$

пуасоновського розподілу, неважко бачити, що $R(t)=P_0$ є вірогідність того, що за час t відбудеться 0 подій, а $F(t)=1-P_0$ є ймовірність того, що за той же час відбудеться не менше однієї події.

Умовні ймовірності $R(t,\Delta t)$, $F(t,\Delta t)$ для розподілу (2') визначаються формулами без змінної *t* –

$$\begin{cases} F(t,\Delta t)=1-e^{-\lambda\Delta t} \\ R(t,\Delta t)=e^{-\lambda\Delta t} \end{cases}. \quad (3)$$

Отже, завершення (чи ні) події в інтервалі $(t,t+\Delta t)$, що примикає до інтервалу (*0, t*), не залежить від минулого часу *t* (від "минулого"). Виникнення (не виникнення) події в якийсь момент $t+\Delta t$ в "майбутньому"залежить виключно від тривалості часу Δt.

Зазначена незалежність від минулого властива тільки експоненціальним розподілом (2') і становить суть характеристичного властивості цього розподілу, яке формулюється наступним чином: на об'єднанні $(0,t]\cup(t,t+\Delta t)$, $\Delta t>0$ – будь-яке, умовне розподілення часу Δt виражається тим же законом, що і безумовне розподілення часу *t*.

У загальному випадку (2) замість (3) будемо мати

$$\begin{cases} F(t,\Delta t)=1-e^{-\lambda(t)\Delta t} \\ R(t,\Delta t)=e^{-\lambda(t)\Delta t} \end{cases}, \quad (4)$$

де залежність від минулого часу *t* очевидна і визначається видом функції $\lambda(t)$, на яку не накладається жодних обмежень, крім безперервності і невід'ємності. Відмінність (4) від (3) полягає ще й у тому, що в (3) тривалість часу Δt, взагалі кажучи, довільна, в (4), навпаки, Δt передбачається достатньо малою величиною.

Залежність (незалежність) умовних розподілів від "минулого" має дуже принципове значення при використанні апарату марковських ланцюгових процесів. Доповнимо сказане низкою положень, на які в процесі дисертаційного дослідження доводиться робити посилання.

Потоком подій називається їх послідовність, розподілена по випадкових моментам часу звершення цих подій. Геометрично потік подій зображується на числовій осі часу *0t* випадковим набором точок $t_1,t_2,...,$ що відповідають моментам часу звершення подій.

Серед різних за своєю структурою потоків подій в інженерних додатках та завдання дослідницького характеру переважне застосування знаходять так звані пуасоновські потоки. Це пояснюється не тільки тим, що постулювання такого типу потоків набагато спрощує дослідження і призводить до конструктивних рішень, але ще й тим, що пуасоновські потоки є граничними для різних інших "непуасоновських" потоків. Зокрема, при накладенні великого числа таких потоків один на одного сумарний потік виявляється близьким до пуасоновського для широкого класу умов. Та ж картина має місце, якщо довільно взятий потік піддати випадковому розрідженню, викидаючи з нього ті чи інші події. Сказане обгрунтовується доказом граничних теорем, показаних в [4].

Потік називається пуасоновським, якщо він має властивості *ординарності* і *відсутності післядії*.

Властивість ординарності полягає в тому, що ймовірність звершення двох або більше подій за досить малий проміжок часу пренебрежимо мала в порівнянні з імовірністю появи однієї події.

Властивість відсутності післядії полягає в тому, що для будь-яких двох непересічних інтервалів часу осі *0t* випадкове число подій, що відбуваються на одному з них, не залежить від того, скільки подій відбулося на іншому.

У фізичній системі *S* відбувається випадковий марківський процес, якщо вона з часом переходить із

стану в стан під дією пуасоновських потоків випадкових подій. При цьому система *S* називається системою з дискретними станами, якщо вона має перераховану (або кінцеву) множину можливих станів $S_0, S_1, S_2, ..., S_k, ...$ і перехід з одного стану в інший здійснюється скачком.

Якщо такі переходи можливі в будь-який момент часу, то відбувається в системі *S* процес називається процесом з неперервним часом.

Для опису випадкового марківського процесу з дискретними станами $S_0, S_1, ...$ і безперервним часом користуються ймовірностями станів

$$p_0(t), p_1(t), p_2(t), ..., p_k(t), ..., \quad (5)$$

де $p_k(t)$ - ймовірність того, що система (процес) у момент *t* знаходиться в стані S_k.

При вивченні процесів, що протікають в системах, однією з основних завдань дослідження є визначення ймовірностей (5) по поставлених початкових умовах і умові нормування

$$\sum p_k(t) = 1.$$

Дані ймовірності, хоча і не описують процес вичерпним чином, все ж таки дають про нього досить повне представлення.

Висновок. Геометрично марківський процес зображується розміченим графом станів, відповідно до яких за певними правилами складається система лінійних диференціальних рівнянь ймовірностей станів $S_0, S_1, ...$[4]. Будь – якому графу однозначно відповідає система диференціальних рівнянь шуканих ймовірностей (5), і навпаки [4].

Фізичні системи, в яких відбуваються марківські процеси з неперервним часом, називають пуасонівськими системами. При цьому пуасонівська система є канонічною (або простої), якщо потоки, що визначають її стан, крім властивостей ординарності і відсутності післядії наділені властивістю стаціонарності, тобто, незмінністю у часі. Такою властивістю, як це випливає з (3), (4), мають лише ті потоки, в яких час між подіями розподілено за законом (2 ’).

Література

1. Галицкий А.В. Защита информации в сети – анализ технологий и синтез решений. / Галицкий А.В., Рябко С.Д., Шаньган В.Ф. – М.: ДМК Пресс, 2004. – 616 с.: ил.

2. Мясіщев О.А. Напрямки вирішення проблем захисту інформації в мережах. / Мясіщев О.А., Джулій А.В // Вісник Хмельницького національного університету – 2009. – № 4. – С. 107 – 111

3. Овчаров Л.А. Прикладные задачи теории массового обслуживания. / Овчаров Л.А. – М.: «Машиностроение», 1969. – 324с.

4. Эльсгольц Л. Э. Дифференциальные уравнения и вариационное исчисление. / Эльсгольц Л.Э. – М.: «Наука», 1969. – 424 с.

Надійшла 6.4.2011 р.

УДК 004: 004.65

В.М. ДЖУЛІЙ, О.Ю. ХМЕЛЬНИЦЬКИЙ
Хмельницький національний університет

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У КОМП’ЮТЕРНИХ СИСТЕМАХ

У статті проведено дослідження аналізу методів захисту інформації, що пересилається комп’ютерними системами та становить близько 75 % обсягу інформації, що пересилається через мережі. Часто в таких системах для забезпечення безвідмовності мережі та/або прискорення завантаження, дані зберігаються з надмірним використанням копії файлів або їхніх частин на різних комп’ютерах в мережі. Також можливий варіант, при якому файл ділиться на n частин так, що будь-яких K (K < n) з них досить, щоб відновити файл. Для забезпечення захисту та конфіденційності інформації в когмп’ютерних системах часто використаються криптосистеми з відкритим ключем. Зокрема, їх можна використати для побудови математичної моделі контролю доступу в комп’ютерній системі.

Research of analysis methods for protecting the information that peresylayet computer systems and is about 75 % of the amount of information sent over the network. Often in such systems to ensure the reliability of network and/or faster, the data stored with excessive use of copies of files or their parts on different computers on the network. Also possible in which the file is divided into five parts so that any K (K <n) are enough to restore the file. To ensure the security and confidentiality of information in computer systems are frequently used public key cryptosystem. In particular, they can be used to construct a mathematical model for access control in computer systems.

Ключові слова: система захисту інформації, комп’ютерні системи, конфіденційність інформації.

Вступ. Фахівці в області захисту інформації пропонують розділяти систему безпеки на дві частини: внутрішню і зовнішню [1]. У внутрішній частині здійснюється, в основному, контроль доступу шляхом ідентифікації і аутентифікації користувачів при допуску в мережу і при доступі в базу даних. Крім цього