

ПОКАЗНИКИ НАДІЙНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ У ВИПАДКУ СИСТЕМИ ІЗ КІНЦЕВИМ ЧИСЛОМ ДІАЛогоВИХ КАНАЛІВ

У статті представлено підхід до узагальнення задачі на випадок системи захисту із кінцевим числом діалогових каналів спілкування з користувачами. Введення додаткових діалогових каналів спілкування не міняє показників надійності захисту інформації, здійснюваної системою захисту об'єкта; динаміка зміни цих показників на розглянутому календарному періоді залишається такою ж, що й для одноканальної системи.

The article presented an approach to generalize the problem to the case of the protection system with a finite number of interactive channels of communication with users. The introduction of additional interactive channels of communication does not alter the reliability of information security, ongoing system of protection of the facility; dynamics of change in these indicators for the consideration of the calendar period is the same as that for single-channel system.

Ключові слова: система захисту, імовірність станів, основний функціональний показник.

Вступ. Інформаційна безпека є складовою частиною інформаційних технологій – області, що розвивається надзвичайно високими темпами. Розробка сучасної системи інформаційної безпеки вимагає, з одного боку, відстеження швидких змін в інформаційних технологіях і погрозах, що з'являються, а з іншого боку – обліку реальних характеристик апаратного й програмного забезпечення корпоративних мереж і систем. Постановка й проведення дослідження можливостей програмно – апаратних засобів захисту електронних джерел інформації являє собою актуальну дослідницьку задачу і має за мету розробку математичної моделі функціонування системи захисту на розглянутому проміжку часу тривалістю t .

Постановка задачі. Марківський процес, описаний у [2,3], у якому діюча система захисту (СЗ) послідовно накопичує у вершинах S_{2k} графа станів, кількість пропущених нелегальних користувачів визначимо як процес *одноканального діалогового спілкування*. У цьому процесі безпосередньо «робочими» вершинами служать вершини S_{2k+1} графа, $k=0,1,2,\dots$. Саме в цих вершинах відбувається контрольний діалог програмно – апаратної структури СЗ із користувачами, що входять у контакт із інформаційною системою.

За своїм інтелектно-конструкторським рішенням схема побудови діалогу всередині кожної вершини S_{2k+1} залишається незмінною протягом усього процесу, що відбувається. У цьому значенні вершини S_{2k+1} графа нерозрізнені: у будь-який момент t (у будь-яку добу) це одна і та ж одноканальна типова СМО, яка характеризується своїми параметрами, дисципліною черги й основними показниками функціонування. Зокрема, це може бути одноканальна система з відмовами (рис. 1-а), або одноканальна СМО з обмеженим числом місць у черзі (рис. 1-б).

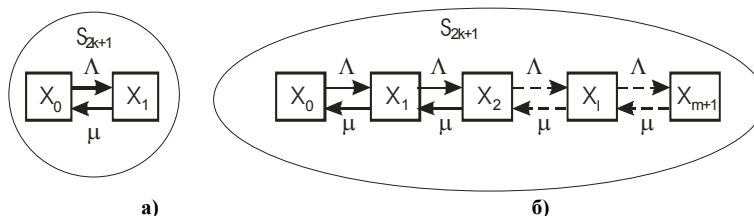


Рис. 1. Внутрішня структура робочих вершин графа станів процесу відбиття-невідбиття атак нелегальних користувачів

Λ – інтенсивність вхідного потоку користувачів (у тому числі нелегальних); μ – інтенсивність діалогу (інтенсивність обслуговування); X_j – стан процесу діалогу; X_0 – канал вільний; X_1 – канал зайнятий, черги немає; X_{m+1} – канал зайнятий, m – кількість користувачів у черзі (m – обмеження по числу місць у черзі).

Процес $X_j(t)$, що протікає у вершинах S_{2k+1} всередині досліджуваного процесу $S_i(t)$, є так званим процесом «загибелі й розмноження» і, будучи ергодичним, виражається своїми граничними ймовірностями станів і показниками продуктивності. Так, для СМО на рис. 1 – б (одноканального діалогу СЗ із користувачами) формули граничних ймовірностей мають вигляд:

$$\left\{ \begin{array}{l} p_0 = \frac{1 - \frac{\Lambda}{\mu}}{1 - \left(\frac{\Lambda}{\mu}\right)^{m+2}}, \text{ при } \frac{\Lambda}{\mu} \neq 1, \left(\frac{\Lambda}{\mu} > 1\right) \\ p_0 = \frac{1}{m+2}, \text{ при } \frac{\Lambda}{\mu} = 1 \\ p_1 = \frac{\Lambda}{\mu} p_0, p_2 = \left(\frac{\Lambda}{\mu}\right)^2 p_0, \dots, p_l = \left(\frac{\Lambda}{\mu}\right)^l p_0, p_{m+1} = \left(\frac{\Lambda}{\mu}\right)^{m+1} p_0 \end{array} \right.$$

Імовірність відмови в обслуговуванні користувача визначається формулою:

$$p_{отк} = \frac{\left(\frac{\lambda}{\mu}\right)^{m+1} \left(1 - \frac{\lambda}{\mu}\right)}{\left(1 - \frac{\lambda}{\mu}\right)^{m+2}}.$$

Показники продуктивності будуть наступними: абсолютна пропускна здатність (середнє число користувачів, що обслуговує СЗ за одиницю часу) – $A = \Lambda(1 - p_{отк})$; середнє число користувачів, що перебувають у черзі на діалог зі СЗ:

$$\bar{r} = \frac{\left(\frac{\Lambda}{\mu}\right)^2 \left[1 - \left(\frac{\Lambda}{\mu}\right)^m \left(m + 1 - \frac{\Lambda}{\mu} m\right)\right]}{\left(1 - \frac{\Lambda}{\mu}\right) \left(1 - \left(\frac{\Lambda}{\mu}\right)^{m+2}\right)};$$

середнє число заявок (користувачів) пов'язаних зі СЗ (що стоять у черзі й беруть участь у контрольному діалозі):

$$\bar{k} = \bar{r} + \frac{\frac{\Lambda}{\mu} - \left(\frac{\Lambda}{\mu}\right)^{m+2}}{1 - \left(\frac{\Lambda}{\mu}\right)^{m+2}};$$

середній час очікування користувачем контрольного діалогу зі СЗ – $\bar{t}_{очк} = \frac{\bar{r}}{\Lambda}$; середній час перебування

користувача в діалоговій системі контролю (у СЗ): $\bar{t}_{сз} = \frac{\bar{r}}{\Lambda} + \frac{(1 - p_{відм})}{\mu}$. Наведені формули повністю характеризують СЗ як систему обслуговування користувачів інформаційною системою [2].

Методика узагальнення задачі. Внутрішній процес $X_j(t)$ у робочій вершині S_{2k+1} становить основу діючої програмно – апаратної СЗ, досліджується й моделюється на стадії її конструкторської розробки. Останнє відноситься й до вибору оптимального (або компромісного) числа діалогових каналів. У рамках роботи ми абстрагуємося від процесу $X_j(t)$, керуючись тільки вхідними результатами λ, λ_0 цього процесу. Саме цими показниками оцінюються надійність здійснюваного захисту інформації в досліджуваному (зовнішньому) процесі $S_i(t)$.

Сама по собі зміна кількості діалогових каналів позначається тільки на показниках продуктивності СЗ як системи обслуговування користувачів. Вона не міняє інтенсивностей Λ, μ внутрішнього процесу $X_j(t)$ й, отже, інтенсивностей λ, λ_0 процесу $S_i(t)$. У такому випадку необхідно очікувати, що динаміка зміни функціональних імовірнісних показників $P_i(t)$, залишиться незмінними.

Для простоти обмежимося випадком 2-хканальної внутрішньої структури робочої вершини S_{2k+1} процесу $S_i(t)$. Потім узагальнимо результат стосовно до довільного фіксованого числа n – каналів.

Зауважимо, що подвоєння числа діалогових каналів СЗ рівнозначно подвоєнню числа робочих вершин графа станів процесу $S_i(t)$, кожна з яких функціонує на накопичення пропущених до інформації нелегальних користувачів незалежно від іншої.

На рисунку 2-а побудований граф процесу функціонування СЗ із двома каналами діалогового спілкування. Перетворенням цього графа до виду, показаному на рисунку 2-б, розгалуження можна уникнути, однак для наступного інтегрування системи диференціальних рівнянь така операція незначна.

Охарактеризуємо стан процесу по графу, зображеному на рисунку 2-б: $S_i, i=0, 3, 6, 9, \dots$ – стани, коли обидва канали вільні; S_{i+1} – стани, коли перший з каналів зайнятий і взаємодіє з нелегальним користувачем; S_{i+2} – стан, коли другий з каналів зайнятий і взаємодіє з нелегальним користувачем.

$\bigcup_{i=0}^{\infty} S_i$ – об'єднання безкінечної множини станів процесу, що характеризують універсум J подій,

що виражаються графом станів СЗ, $P(J)=1$ – імовірність універсума J .

$\bigcup_{i=0}^2 S_i$ – об'єднання станів процесу, що визначає подію, коли за час t системою захисту не допущено

жодного нелегального доступу до інформації.

$J \setminus \bigcup_{i=0}^2 S_i$ – об'єднання станів, якими виражається подія, коли за час t системою захисту допущено

не менше одного нелегального доступу до інформації.

$\bigcup_{i=3}^5 S_i, \bigcup_{i=6}^8 S_i, \bigcup_{i=9}^{11} S_i, \dots$ – об'єднання станів, якими виражається подія, що полягає в тому, що за

час t системою захисту допущено рівно два (чотири, шість, ...) нелегальних доступів до інформації.

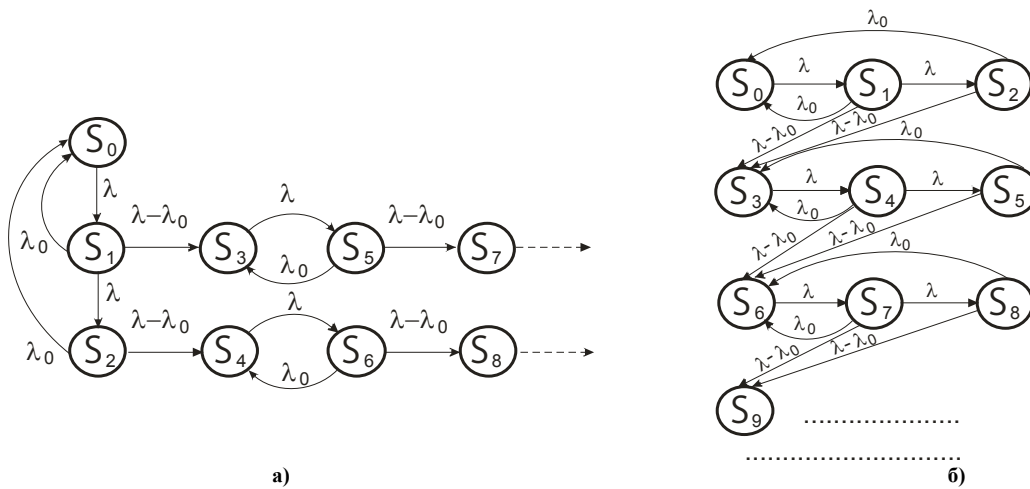


Рис. 2 – Граф станів СЗ із 2-ма фіксованими каналами діалогового спілкування

Складемо систему диференціальних рівнянь імовірностей станів процесу по розміченому графі на рисунку 2-б. Отримаємо:

$$\left\{ \begin{aligned} \frac{dp_0(t)}{dt} &= -\lambda p_0(t) + \lambda_0(p_1(t) + p_2(t)) \\ \frac{dp_1(t)}{dt} &= \lambda p_0(t) - 2\lambda p_1(t) \\ \frac{dp_2(t)}{dt} &= \lambda p_1(t) - \lambda p_2(t) \\ &\dots \\ \frac{dp_j(t)}{dt} &= (\lambda - \lambda_0)(p_{j-2}(t) + p_{j-1}(t)) - \lambda p_j(t) + \lambda_0(p_{j+2}(t) + p_{j+1}(t)) \\ \frac{dp_{j+1}(t)}{dt} &= \lambda p_j(t) - 2\lambda p_{j+1}(t) \\ \frac{dp_{j+2}(t)}{dt} &= \lambda p_{j+1}(t) - \lambda p_{j+2}(t), j = 3, 6, 9, \dots \\ &\dots \end{aligned} \right. \quad (1)$$

Система рівнянь (1) інтегрується за початковими умовами

$$p_0(0) = 1, p_1(0) = p_2(0) = \dots = p_j(0) = \dots = 0. \quad (2)$$

Виконаємо інтегрування для першої трійки рівнянь. Диференціюючи першу рівність і виконавши заміни на підставі другої й третьої рівностей, отримаємо:

$$\frac{d^2 p_0(t)}{dt^2} = -\lambda \frac{dp_0(t)}{dt} + \lambda \lambda_0 p_0(t) - \lambda \lambda_0 (p_1(t) + p_2(t)) .$$

В отриманій рівності вираження $\lambda_0(p_1(t) + p_2(t))$ замінимо за допомогою першого рівняння з (1). Це дасть лінійне рівняння 2-го порядку наступного виду:

$$\frac{d^2 p_0(t)}{dt^2} + 2\lambda \frac{dp_0(t)}{dt} + \lambda(\lambda - \lambda_0)p_0(t) = 0 \tag{3}$$

з приєднаним до нього рівнянням

$$p_1(t) + p_2(t) = \frac{1}{\lambda_0} \left(\frac{dp_0(t)}{dt} + \lambda p_0(t) \right) \tag{4}$$

Результат (3), (4) і за формою й по суті співпадає з показаними раніше рівняннями [2] для одноканальної СЗ. Відмінність тільки в тому, що там на сукупності станів $\{S_0, S_1\}$ - тільки один діалоговий канал, а тут на сукупності станів $\{S_0, S_1, S_2\}$ - два діалогових канали. Тому там стан S_1 визначається функцією $p_1(t)$, а тут об'єднання станів $S_1 \cup S_2$ визначається сумою імовірнісних функцій $p_1(t) + p_2(t)$.

У силу відзначеної аналогії наступне рішення рівнянь (3), (4) нічим не відрізняється від уже наведених формул [2,3], у яких необхідно виконати формальну заміну змінної $p_1(t)$ на суму функцій $p_1(t) + p_2(t)$. Таким чином, у випадку 2-х каналної системи вираження основного функціонального показника ефективності захисту видозмінюється тільки структурна змінна, а саме вираження імовірнісної функції $P_0(t)$ залишається в незмінному виді. Інакше кажучи, при заміні 1-канальної СЗ 2-хканальною системою є в наявності наступні структурні рівності між імовірностями станів, які характеризуються тотожними аналітичними виразами:

$$\begin{cases} P_0(t)_{(1)} = P_0(t)_{(2)} = \frac{1}{2} \left(e^{-(\lambda - \sqrt{\lambda \lambda_0})t} + e^{-(\lambda + \sqrt{\lambda \lambda_0})t} \right) \\ P_1(t)_{(1)} = P_1(t)_{(2)} + P_2(t)_{(2)} = \frac{1}{2} \sqrt{\frac{\lambda}{\lambda_0}} \left(e^{-(\lambda - \sqrt{\lambda \lambda_0})t} - e^{-(\lambda + \sqrt{\lambda \lambda_0})t} \right) \\ P_0(t)_{(1)} = P_0(t)_{(1)} + P_1(t)_{(1)} = P_0(t)_{(2)} + P_1(t)_{(2)} + P_2(t)_{(2)} = \\ = \frac{1}{2} \left[\left(1 + \sqrt{\frac{\lambda}{\lambda_0}} \right) e^{-(\lambda - \sqrt{\lambda \lambda_0})t} + \left(1 - \sqrt{\frac{\lambda}{\lambda_0}} \right) e^{-(\lambda + \sqrt{\lambda \lambda_0})t} \right] \end{cases} \tag{5}$$

При цьому зауважимо, що з рівнянь (3), (4) із залученням початкових умов (2) однозначно перебуває й функція $p_0(t)$ й сумарна функція $p_1(t) + p_2(t)$, якими далі визначаються ймовірності

$$P_2(t) = p_3(t) + p_4(t) + p_5(t), P_4(t) = p_6(t) + p_7(t) + p_8(t), \tag{*}$$

рівно двох, чотирьох і т.д. невідвернених системою захисту проникнень до інформації (взагалі, парного числа нелегальних вторгнень). Потрібно підкреслити, що особливої необхідності в обчисленні кожного з доданків $p_1(t), p_2(t)$ окремо немає. Втім, як тільки з рівнянь (3), (4) отримані двопараметрична функція $p_0(t, c_1, c_2)$ й часткове рішення $p_0(t)$, то інтегруванням другого рівняння з (1) по початковій умові $p_1(0) = 0$ визначається спочатку імовірнісна функція $p_1(t)$, потім із третього рівняння (1) отримуємо і функцію $p_2(t)$. Опускаючи громіздкі викладення й розрахунки, приведемо, для довідки, остаточні вирази:

$$p_1(t) = \frac{\lambda}{2} \left[\frac{e^{-(\lambda - \sqrt{\lambda \lambda_0})t}}{\lambda + \sqrt{\lambda \lambda_0}} + \frac{e^{-(\lambda + \sqrt{\lambda \lambda_0})t}}{\lambda - \sqrt{\lambda \lambda_0}} \right] - \frac{\lambda e^{-2\lambda t}}{\lambda - \lambda_0} \tag{6}$$

$$p_2(t) = \frac{\lambda^2}{2} \left[\frac{e^{-(\lambda - \sqrt{\lambda \lambda_0})t}}{\sqrt{\lambda \lambda_0} (\lambda + \sqrt{\lambda \lambda_0})} - \frac{e^{-(\lambda + \sqrt{\lambda \lambda_0})t}}{\sqrt{\lambda \lambda_0} (\lambda - \sqrt{\lambda \lambda_0})} \right] - \frac{\lambda e^{-2\lambda t}}{\lambda - \lambda_0} \tag{7}$$

Необхідно зробити акцент на тому, що із графа станів СЗ без розгалуження процесу, рисунок 2-б, не можна одержати імовірнісні функції непарного числа неприпинених вторгнень в інформаційне поле об'єкта. Необхідно розглядати граф з розгалуженням (рисунок 2-а), і відповідно цьому графові систему диференціальних рівнянь станів. Тоді ймовірність, наприклад, тільки одного нелегального проникнення за час t до інформації, не припиненого системою захисту буде виражатися ймовірністю події

$$(S_3 \cup S_4 \cup S_5 \cup S_6) \setminus (S_3 \cup S_5) \cap (S_4 \cup S_6), \tag{8}$$

де перераховані стани відносяться до графа з розгалуженням.

Структурна формула шуканої ймовірності $P_1(t)$ витікає з (8), якщо стани замінити їхніми ймовірностями, операцію \cup замінити додаванням, операцію \cap - множенням, операцію \setminus - вирахуванням. Отримаємо:

$$P_1(t) = p_3(t) + p_4(t) + p_5(t) + p_6(t) - (p_3(t)p_4(t) + p_4(t)p_5(t) + p_3(t)p_6(t) + p_5(t)p_6(t)) \quad (9)$$

З (9) бачимо, що тут доводиться враховувати сумісність (спільність) подій.

Повернемося до системи (1), з якої на підставі результатів (3), (4), (5) була встановлена інваріантність (незмінність) основного функціонального показника $P_0(t)$ надійності захисту стосовно числа діалогових каналів. Покажемо, що властивість інваріантності зберігається й для інших функціональних показників, не тільки для $P_0(t)$.

Знайдемо вираз ймовірності:

$$P_2(t) = p_3(t) + p_4(t) + p_5(t), \quad (10)$$

яке відповідно до графа на рисунку 2-б визначається ймовірністю рівно двох неприпинених системою захисту нелегальних проникнень до інформації.

З (1) випишемо диференціальні рівняння ймовірностей станів S_3, S_4, S_5 . Отримаємо:

$$\begin{cases} \frac{dp_3(t)}{dt} = (\lambda - \lambda_0)(p_1(t) + p_2(t)) - \lambda p_3(t) + \lambda_0(p_4(t) + p_5(t)) \\ \frac{dp_4(t)}{dt} = \lambda p_3(t) - 2\lambda p_4(t) \\ \frac{dp_5(t)}{dt} = \lambda p_4(t) - \lambda p_5(t) \end{cases} \quad (11)$$

Диференціюванням першого рівняння з (11) і наступними замінами за допомогою двох інших рівностей з (11) і виражень похідних $\frac{dp_1(t)}{dt}, \frac{dp_2(t)}{dt}$ система (11) приводиться до еквівалентного виду –

$$\begin{cases} \frac{d^2 p_3(t)}{dt^2} + 2\lambda \frac{dp_3(t)}{dt} + (\lambda^2 - \lambda\lambda_0)p_3(t) = \lambda(\lambda - \lambda_0)p_0(t) \\ p_4(t) + p_5(t) = \frac{1}{\lambda_0} \left[\frac{dp_3(t)}{dt} - (\lambda - \lambda_0)(p_1(t) + p_2(t)) + \lambda p_3(t) \right] \end{cases}, \quad (12)$$

де функції $p_0(t), p_2(t) + \lambda p_3(t)$ відомі й визначаються формулами (5).

Лінійне неоднорідне рівняння 2-го порядку в (12) – з постійними коефіцієнтами. Воно вирішується стандартним методом варіації довільних постійних. У результаті отримаємо наступну функцію:

$$p_3(t) = c_1 e^{-(\lambda - \sqrt{\lambda\lambda_0})t} + c_2 e^{-(\lambda + \sqrt{\lambda\lambda_0})t} + \frac{\lambda(\lambda - \lambda_0)}{4\sqrt{\lambda\lambda_0}} \left[e^{-(\lambda - \sqrt{\lambda\lambda_0})t} \left(t - \frac{1}{2\sqrt{\lambda\lambda_0}} \right) - e^{-(\lambda + \sqrt{\lambda\lambda_0})t} \left(t + \frac{1}{2\sqrt{\lambda\lambda_0}} \right) \right] \quad (13)$$

з (13) по початкових умовах (2) знаходимо рівність

$$c_1 + c_2 = \frac{\lambda - \lambda_0}{4\lambda_0}, \quad (14)$$

єднальні довільні постійні інтегрування.

Диференціюємо (13). Отримаємо

$$\begin{aligned} \frac{dp_3(t)}{dt} &= -(\lambda - \sqrt{\lambda\lambda_0})c_1 e^{-(\lambda - \sqrt{\lambda\lambda_0})t} - (\lambda + \sqrt{\lambda\lambda_0})c_2 e^{-(\lambda + \sqrt{\lambda\lambda_0})t} + \\ &+ \frac{\lambda(\lambda - \lambda_0)}{4\sqrt{\lambda\lambda_0}} \left[-(\lambda - \sqrt{\lambda\lambda_0})e^{-(\lambda - \sqrt{\lambda\lambda_0})t} \left(t - \frac{1}{2\sqrt{\lambda\lambda_0}} \right) + e^{-(\lambda - \sqrt{\lambda\lambda_0})t} + \right. \\ &\left. + (\lambda + \sqrt{\lambda\lambda_0})e^{-(\lambda + \sqrt{\lambda\lambda_0})t} \left(t + \frac{1}{2\sqrt{\lambda\lambda_0}} \right) - e^{-(\lambda + \sqrt{\lambda\lambda_0})t} \right] \end{aligned} \quad (15)$$

Виразення (13), (15) підставимо в друге рівняння системи (2) і за тими ж початковими умовами у результаті досить громіздких обчислень знайдемо другу рівність

$$c_1 - c_2 = 0, \quad (16)$$

яка зв'язує постійні інтегрування. З (14), (16) отримаємо $c_1 = c_2 = \frac{\lambda - \lambda_0}{8\lambda_0}$.

Підставимо значення c_1, c_2 в (3) і виконаємо алгебраїчні перетворення з урахуванням виражень для функцій $p_0(t), p_1(t) + \lambda p_2(t)$ 2-х каналної системи з (5). Остаточо отримаємо

$$p_3(t) = \frac{\lambda - \lambda_0}{2} t (p_1(t) + p_2(t)) \quad (17)$$

Розгорнуте вираження для функцій $p_4(t) + p_5(t)$ має вигляд:

$$p_4(t) + p_5(t) = \frac{1}{\lambda_0} \left\{ \frac{\lambda - \lambda_0}{4} (p_1(t) + p_2(t)) - (\lambda - \lambda_0) (p_1(t) + p_2(t)) + \frac{\lambda(\lambda - \lambda_0)}{4\sqrt{\lambda\lambda_0}} \left[t\sqrt{\lambda\lambda_0} \left(e^{-(\lambda - \sqrt{\lambda\lambda_0})t} + e^{-(\lambda + \sqrt{\lambda\lambda_0})t} \right) + \frac{1}{2} \left(e^{-(\lambda - \sqrt{\lambda\lambda_0})t} - e^{-(\lambda + \sqrt{\lambda\lambda_0})t} \right) \right] \right\} \quad (18)$$

На підставі формул (5) рівність (18) матиме вигляд:

$$p_4(t) + p_5(t) = \frac{\lambda - \lambda_0}{2\lambda_0} [\lambda t p_0(t) - (p_1(t) + p_2(t))] \quad (19)$$

Сумою функцій (17), (19) визначається по формулі (10) імовірність $P_2(t)$ рівно двох нелегальних проникнень. Поєднуючи всі ці формули, отримаємо

$$\begin{cases} p_3(t) = \frac{(\lambda - \lambda_0)}{2} t (p_1(t) + p_2(t)) \\ p_4(t) + p_5(t) = \frac{(\lambda - \lambda_0)}{2\lambda_0} [\lambda t p_0(t) - (p_1(t) + p_2(t))] \\ P_2(t) = \frac{(\lambda - \lambda_0)}{2\lambda_0} [\lambda t p_0(t) + (p_1(t) + p_2(t))(\lambda_0 t - 1)] \end{cases} \quad (20)$$

Порівняємо перші дві рівності з (20) з формулами [2], якими виражається ймовірність двох нелегальних проникнень до інформації для одноканальної СЗ. Бачимо їхній повний збіг з точністю до структурних рівностей (5). Таким чином, для функціонального показника $P_2(t)$, як і для $P_0(t)$, характерна властивість інваріантності стосовно числа діалогових каналів.

Аналогічним чином зазначена властивість установлюється для інших імовірнісних функцій (*) двокаанальної системи захисту. Те ж показується для 3-х, 4-х, і, взагалі, n – каналних СЗ із фіксованим числом каналів.

Висновки. Введення додаткових діалогових каналів спілкування не міняє показників надійності захисту інформації, здійснюваної СЗ об'єкта; динаміка зміни цих показників на розглянутому календарному періоді залишається тією ж, що й в одноканальній системі.

Незмінність показників надійності захисту інформації по відношенню до числа каналів не вимагає, у свою чергу, і внесення яких – небудь змін у програмне забезпечення задачі.

Підводячи підсумок, підкреслимо, що одним із прихованих (неявних) факторів, що сприяють виявленню нелегальних користувачів і, виходить, збільшенню статистичного значення λ_0 , може служити стратегія організації черги, що нав'язується багатоканальною СЗ користувачам інформаційної системи. Ця стратегія полягає в їхньому рівномірному розподілі й по вільних, і по зайнятих діалогових каналах на противагу тій стратегії, кращої для нелегалів, коли існує їхнє прагнення атакувати той самий канал і утворювати чергу переважно на якомусь одному каналі, якщо всі вони виявляються зайнятими.

Показані методики апробовані стосовно наявних реальних статистик припинених спроб нелегального доступу до інформації.

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. Методика розрахунку показників надійності захисту інформації в умовах невизначеності. / Мясіщев О.А., Джулій А.В.; // Вимірвальна та обчислювальна техніка в технологічних процесах. – 2008. – № 2, – С.143 -148

3. 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
4. Эльсгольц Л. Э. Дифференциальные уравнения и вариационное исчисление. / Эльсгольц Л.Э.; «Наука». М. 1969.: 424 с.
5. Овчаров Л.А. Прикладные задачи теории массового обслуживания. / Овчаров Л.А.; «Машиностроение». М.1969.: 324с.

Надійшла до редакції
5.10.2010 р.

УДК 004.925

О.Н. РОМАНЮК, М.Д. ОБІДНИК

Вінницький національний технічний університет

Г.Г. СЕРГЄЄВ

Севастопольський національний технічний університет

МЕТОД ПРОБНИХ ПЕРЕВІРОК ДЛЯ ІДЕНТИФІКАЦІЇ ВІДБЛИСКУ

Запропоновано метод ідентифікації відблиску на основі пробних перевірок, що забезпечує зменшення обчислювальної складності зафарбовування. Для запропонованого методу розроблено апроксимаційні формули, а також блоки апаратної підтримки.

The method of identification based on experimental checks to decrease the computational complexity of coloring is suggested. Approximation formulas and units of hardware support were developed for proposed method.

Ключові слова: зафарбовування, вектори нормалей, апроксимація, інтенсивність кольору.

Вступ

Комп'ютерна графіка дозволяє суттєво збільшити пропускну спроможність інформаційного каналу, через який здійснюється двосторонній зв'язок користувача і комп'ютера, у зв'язку з чим роль і значення графічного зображення результатів обчислень у промисловості та науково-дослідній практиці безупинно зростає. На даному етапі розвитку комп'ютерної графіки особливу увагу приділяється формуванню просторових зображень, які є найбільш інформативними та реалістичними. При синтезі реалістичних зображень на верхніх етапах графічного конвеєра обробляються математичні моделі та їх складові, а на нижньому (рендерингу) – формуються елементи зображення.

Однією з найбільш трудомістких процедур рендерингу є процедура зафарбовування, згідно з якою для кожної точки поверхні визначається інтенсивність кольору та екранні координати. При обчисленні інтенсивностей кольору точок зображення враховують розташування джерела світла та спостерігача, оптичні властивості матеріалу, спектральні характеристики джерела світла, кривизну поверхні. У зв'язку з цим зафарбовування характеризується значними обчислювальними витратами, що обумовлює необхідність розробки методів і засобів для підвищення продуктивності її реалізації. Особливо гостро ця проблема постає при формуванні динамічних зображень.

Аналіз останніх досліджень

Методи, які використовуються для моделювання освітлення, оперують з відбитим світлом, що передбачає обчислення фонові, дифузної і спекулярної складових кольору [1, 2].

Розсіяне світло (фонова складова кольору) – це світло, яке відбивається від навколишнього середовища. Точне моделювання даної складової світла вимагає великих обчислювальних витрат і тому воно апроксимується константою [3].

Інтенсивність дифузної складової залежить від матеріалу, з якого виготовлено об'єкт, та місця розташування об'єкта і джерела світла. Оскільки дифузне світло розсіюється рівномірно за всіма напрямками, то місце розташування спостерігача не впливає на інтенсивність кольору дифузної складової світла. Дифузне світло точкового джерела відбивається від поверхні згідно закону косинусів Ламберта [3]: інтенсивність відбитого світла пропорційна косинусу кута між напрямком світла та нормаллю до поверхні.

Поверхні деяких матеріалів можуть відбивати світло направлено, у результаті чого утворюються яскраві відблиски на поверхні об'єктів [3-5]. Має місце максимальна концентрація світлової енергії в епіцентрі відблиску з подальшим її затуханням із віддаленням від нього. Місце розташування відблиску на поверхні об'єкта у такому випадку залежить від розміщення джерела світла, самого об'єкта, а також спостерігача у тривимірному просторі.

Для того, щоб описати пік відблиску, доцільно використовувати таку функцію відбивної здатності поверхні, яка б достатньо реалістично відтворювала зону відблиску. Б.Т. Фонг запропонував використовувати функцію [4]:

$$f_{r, \text{Фонг}}(\vec{L}, \vec{V}) = k_s \cdot \cos^n \theta,$$

де θ – кут між вектором спостереження \vec{V} та вектором, який визначає напрямок відбитого світла \vec{R} ,