7. Макаров И.М. – Теория выбора и принятия решений/ Макаров И.М., Виноградская Т.М., Рубчинский А.А., Соколов В.Б.-М.: Наука, 1982-с.328.

8. Емельянов С.В. - Многокритериальные методы принятия решений / Емельянов С.В., Ларичев О.И.-М.: Знания, 1985-с.31.

9. Корнійчук М.Т. – Ризик і безпека: кореляція категорій/ Корнійчук М.Т., Хорошко В.О., Дирнов В.М. // Захист інформації, Спец.випуск, 2008-с.15-21.

Разработаны математические модели угроз и рисков позволяющие , включать события, которые вызывают угрозу или риск, в иерархию целей программ по защите информации. Разработан способ количественного оценивания угрозы и риска.

Ключевые слова: система защиты информации, количественные показатели относительной эффективности система защиты информации, модели угроз и рисков, порог угрозы, фактор риска, индикатор риска.

Рецензент:д.т.н., проф. Козловський В.В.
Надійшла 10.10.2010

УДК 004:004.65

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц. **Пампуха І.В.** (ВІКНУ)
Джулій А.В. (УЕП, м.Хмельницький)

УЗАГАЛЬНЕННЯ ЗАДАЧІ НА ВИПАДОК СИСТЕМИ ЗАХИСТУ ІЗ КІНЦЕВИМ ЧИСЛОМ ДІАЛОГОВИХ КАНАЛІВ СПІЛКУВАННЯ З КОРИСТУВАЧАМИ

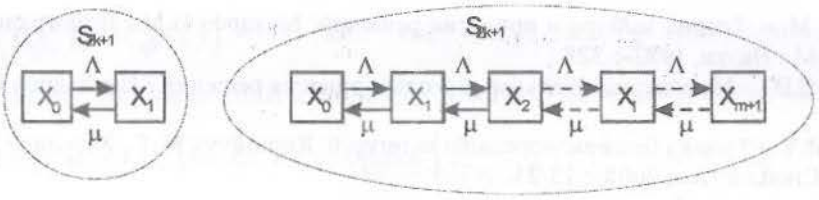
Вступ

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. Процедура придбання пристроїв інформаційної безпеки не складна. Істотно більш складним є рішення проблем, як захищати і які засоби безпеки застосовувати. Це рішення охоплює й керування інформаційною безпекою, включаючи планування, розробку політики безпеки й проектування необхідних процедур безпеки[1].

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,... ... 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).



а) 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 (інтесивніость 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 імовірностей мають вигляд:

$$\begin{cases} p_0 = \dfrac{1-\dfrac{\Lambda}{\mu}}{1-\left(\dfrac{\Lambda}{\mu}\right)^{m+2}}, \; при \; \dfrac{\Lambda}{\mu} \neq 1, \left(\dfrac{\Lambda}{\mu} > 1\right) \\ p_0 = \dfrac{1}{m+2}, \; при \; \dfrac{\Lambda}{\mu} = 1 \\ p_1 = \dfrac{\Lambda}{\mu} p_0, p_2 = \left(\dfrac{\Lambda}{\mu}\right)^2 p_0, \ldots, p_l = \left(\dfrac{\Lambda}{\mu}\right)^l p_0, p_{m+1} = \left(\dfrac{\Lambda}{\mu}\right)^{m+1} p_0 \end{cases}$$

Імовірність відмови в обслуговуванні користувача визначається формулою:

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

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:

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

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 – $\bar{t}_{очік} = \frac{\bar{r}}{\Lambda}$; 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 оцінюється 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.

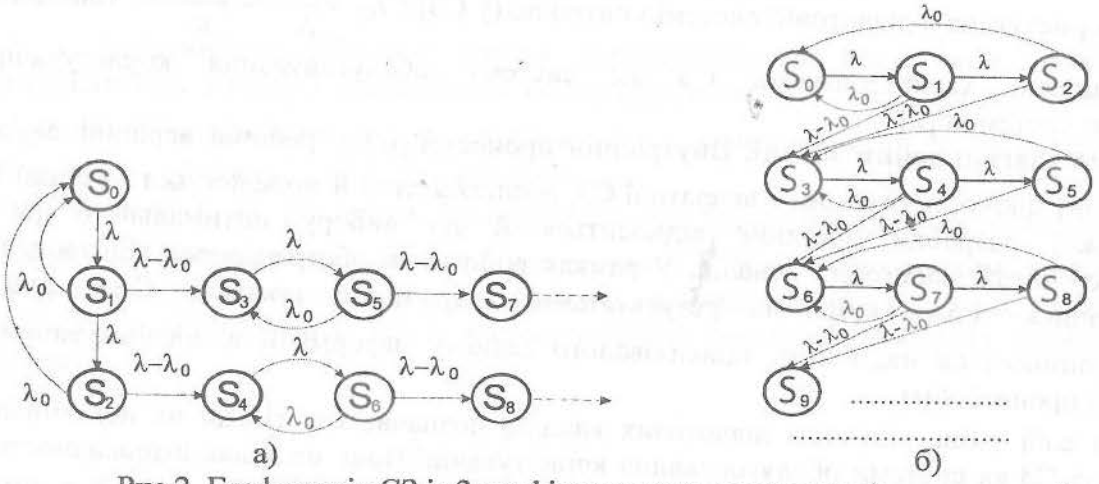
Охарактеризуємо стан процесу по графу, зображеному на рисунку 2-б: S_i, i=0, 3, 6, 9, … - стани, коли обидва канали вільні; S_{i+1} - стани, коли перший з каналів зайнятий і взаємодіє з нелегальним користувачем; S_{i+2} - стан, коли другий з каналів зайнятий і взаємодіє з нелегальним користувачем.

$\bigcup_{i=0}^{\infty} S_i$ - 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.

$\bigcup_{i=3}^{5} S_i$, $\bigcup_{i=6}^{8} S_i$, $\bigcup_{i=9}^{11} S_i$, … - 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.



а) б)

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:

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

Система рівнянь (1) інтегрується за початковими умовами

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

Виконаємо інтегрування для першої трійки рівнянь. Диференціюючи першу рівність 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:

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

з приєднаним до нього рівнянням

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

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 канальної 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:

$$\begin{cases} p_0(t)_{(1)} = p_0(t)_{(2)} = \dfrac{1}{2}\left(e^{-\left(\lambda - \sqrt{\lambda\lambda_0}\right)t} + e^{-\left(\lambda + \sqrt{\lambda\lambda_0}\right)t}\right) \\ p_1(t)_{(1)} = p_1(t)_{(2)} + p_2(t)_{(2)} = \dfrac{1}{2}\sqrt{\dfrac{\lambda}{\lambda_0}}\left(e^{-\left(\lambda - \sqrt{\lambda\lambda_0}\right)t} - e^{-\left(\lambda + \sqrt{\lambda\lambda_0}\right)t}\right) \\ P_0(t)_{(1)} = p_0(t)_{(1)} + p_1(t)_{(1)} = p_0(t)_{(2)} + p_1(t)_{(2)} + p_2(t)_{(2)} = \\ \quad = \dfrac{1}{2}\left[\left(1 + \sqrt{\dfrac{\lambda}{\lambda_0}}\right)e^{-\left(\lambda - \sqrt{\lambda\lambda_0}\right)t} + \left(1 - \sqrt{\dfrac{\lambda}{\lambda_0}}\right)e^{-\left(\lambda + \sqrt{\lambda\lambda_0}\right)t}\right] \end{cases} \qquad (5)$$

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

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

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:

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

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

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:

$$\begin{aligned} P_1(t) &= p_3(t) + p_4(t) + p_5(t) + p_6(t) - \\ &- \left(p_3(t)p_4(t) + p_4(t)p_5(t) + p_3(t)p_6(t) + p_5(t)p_6(t)\right) \end{aligned} \tag{9}$$

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:

$$P_2(t) = p_3(t) + p_4(t) + p_5(t), \tag{10}$$

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:

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

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

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

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:

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

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

$$c_1 + c_2 = \frac{\lambda - \lambda_0}{4\lambda_0}, \tag{14}$$

єднальні довільні постійні інтегрування.

Диференціюємо (13). Отримаємо

$$\frac{dp_3(t)}{dt} = -\left(\lambda - \sqrt{\lambda\lambda_0}\right)c_1 e^{-\left(\lambda-\sqrt{\lambda\lambda_0}\right)t} - \left(\lambda + \sqrt{\lambda\lambda_0}\right)c_2 e^{-\left(\lambda+\sqrt{\lambda\lambda_0}\right)t} +$$

$$+\frac{\lambda(\lambda-\lambda_0)}{4\sqrt{\lambda\lambda_0}}\left[-\left(\lambda-\sqrt{\lambda\lambda_0}\right)e^{-\left(\lambda-\sqrt{\lambda\lambda_0}\right)t}\left(t-\frac{1}{2\sqrt{\lambda\lambda_0}}\right)+e^{-\left(\lambda-\sqrt{\lambda\lambda_0}\right)t}+\right. \quad (15)$$

$$\left.+\left(\lambda+\sqrt{\lambda\lambda_0}\right)e^{-\left(\lambda+\sqrt{\lambda\lambda_0}\right)t}\left(t+\frac{1}{2\sqrt{\lambda\lambda_0}}\right)-e^{-\left(\lambda+\sqrt{\lambda\lambda_0}\right)t}\right]$$

Вираження (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 канальної системи з (5). Остаточно 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:

$$p_4(t) + p_5(t) = \frac{1}{\lambda_0}\left\{\frac{\lambda-\lambda_0}{4}(p_1(t)+p_2(t)) - (\lambda-\lambda_0)(p_1(t)+p_2(t)) + \right.$$

$$\frac{\lambda(\lambda-\lambda_0)}{4\sqrt{\lambda\lambda_0}}\left[t\sqrt{\lambda\lambda_0}\left(e^{-\left(\lambda-\sqrt{\lambda\lambda_0}\right)t} + e^{-\left(\lambda+\sqrt{\lambda\lambda_0}\right)t}\right) + \right. \quad (18)$$

$$\left.\left.+\frac{1}{2}\left(e^{-\left(\lambda-\sqrt{\lambda\lambda_0}\right)t} - e^{-\left(\lambda+\sqrt{\lambda\lambda_0}\right)t}\right)\right]\right\}$$

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

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

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

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

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 (*) двоканальної системи захисту. Те ж показується для 3-х, 4-х, і, взагалі, n - канальних 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 многоканальною 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.

Список літератури

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

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

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

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

5. Овчаров Л. А. Прикладные задачи теории массового обслуживания. «Машиностроение». М.1969.: 324с.

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.

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

В статье представленный подход к обобщению задачи на случай системы защиты с конечным числом диалоговых каналов общения с пользователями. Введение дополнительных диалоговых каналов общения не меняет показатели надежности защиты информации, осуществляемой системой защиты объекта; динамика изменения этих показателей на рассмотренном календарном периоде остается той же, что и для одноканальной системы.

Ключевые слова: система защиты, вероятность состояний, основной функциональный показатель.

The paper 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.

Keywords: security system, the probability of states, the basic functional parameters.

Рецензент:д.т.н., проф. Петров О.С.
Надійшла 11.11.2010