УДК 004.9:517.978.2

Р.В. Грищук

*Житомирський військовий інститут імені С.П. Корольова Національного авіаційного університету, Житомир*

# Р-МОДЕЛЮВАННЯ ПРОЦЕСІВ НАПАДУ НА ІНФОРМАЦІЮ ПРИ НЕСТАЦІОНАРНІЙ ПРИРОДІ ПОТОКІВ ЗАХИСНИХ ДІЙ ТА ІНФОРМАЦІЙНИХ АТАК

*На основі методу Р-моделювання в диференціально-ігровому базисі в статті розроблено аналітичну модель процесу нападу на інформацію, яка відрізняється від відомих нестаціонарною природою потоків захисних дій та інформаційних атак. Визначено оптимальну траєкторію диференціальної гри та оптимальні стратегії розподілу інформаційних ресурсів гравців, розраховано ціну гри. Наведено результати імітаційного моделювання.*

***Ключові слова:*** *диференціальна гра, траєкторія, ціна гри, спектральна модель, процес нападу на інформацію.*

## Вступ

В умовах світової економічної кризи додатковим джерелом загроз для успішного ведення бізнесу компанією, підприємством, установою або організацією, незалежно від форми власності, можна вважати несанкціонований доступ (НСД) до інформації, яка циркулює в контурі управління їх інформаційно-комунікаційних систем (ІКС) [1, 2]. Як показує практика, НСД до інформації, як засіб реалізації загрози, може призводити до суттєвих матеріальних витрат, а інколи і паралізувати роботу цілих мереж, розгорнутих на базі ІКС [2]. Таким чином, проблема захисту інформації в ІКС є нагальною та потребує свого вирішення.

**Аналіз останніх досліджень і публікацій.** Проведений аналіз останніх досліджень [2, 3] і публікацій [4, 5] показав, що станом на сьогоднішній день першим кроком на шляху до вирішення даної проблеми можна вважати розробку нової методології, спрямованої на моделювання процесів нападу на інформацію, яка дозволить оцінювати рівень захищеності технічних об'єктів від методів НСД.

Відомі якісні (абстрактні) [6] та кількісні [5] моделі на основі апарата мереж Петрі-Маркова, теорії нечітких множин тощо характеризуються статичною природою, що не забезпечує повноту опису процесів, що моделюються.

 

Зрозуміло, що повнота опису процесів нападу на інформацію в ІКС, що моделюються, може бути забезпечена при використанні принципово нової концепції моделювання. Така концепція повинна бути консистенцією відомих теорій, таких як: теорія масового обслуговування; теорія ймовірностей; теорія ігор; теорія оптимального управління; теорія графів; теорія диференціально-тейлорівських перетворень.

Таким чином, як видно з проведеного аналізу, розробка нових аналітичних моделей процесу нападу на інформацію, спроможних відображати динаміку інформаційного конфлікту, є актуальним практичним завданням.

**Метою статті** є розробка аналітичної моделі процесу нападу на інформацію, що дозволить відображати динамічну природу протікання інформаційних конфліктів в ІКС та гнучко адаптуватися до зміни інформаційних ресурсів, що виділяються на захист інформації при управлінні інформаційною безпекою.

## Виклад основного матеріалу

Нехай технічний об'єкт (ТО) в складі ІКС у поточний момент часу $t$ перебуває в одному з типових станів – під впливом методів НСД або під впливом методів захисту інформації (МЗІ), з відповідними ймовірностями $P_0(t)$ та $P_3(t)$. Тривалість інформаційного конфлікту $T$ обмежується тривалістю реалізації НСД до ТО, тобто

$$t \in [0, T]. \qquad (1)$$

Графова модель процесу нападу на інформацію, що відповідає заданій множині станів, подана на рис. 1.

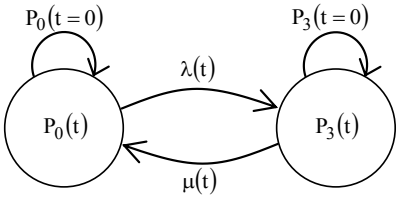


Рис. 1. Графова модель процесу нападу на інформацію зі змінними інтенсивностями потоків

На відміну від відомих моделей [7] над стрілками переходів (рис. 1), що переводять ТО у відповідні стани, відмічено інтенсивності потоків захисних дій $\lambda(t)$ та інформаційних атак $\mu(t)$, чим зазначено їх нестаціонарну природу, яка визначається функціональною часопараметричною залежністю.

Динаміка протікання процесу інформаційного конфлікту описується системою диференціальних рівнянь Колмогорова-Чепмена [4] загального вигляду

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda(t)P_0(t) + \mu(t)P_3(t); \\ \dfrac{dP_3(t)}{dt} = \lambda(t)P_0(t) - \mu(t)P_3(t), \end{cases} \qquad (2)$$

за початкових умов:

$$P_0(t=0) = 1, \; P_3(t=0) = 0 \qquad (3)$$

та умов нормування

$$P_0(t=0) + P_3(t=0) = 1. \qquad (4)$$

Нестаціонарна природа захисних дій та інформаційних атак описується функціональними залежностями вигляду

$$\lambda(t) = \lambda t; \qquad (5)$$

$$\mu(t) = \mu t. \qquad (6)$$

На інформаційні ресурси (5) та (6) накладаються обмеження:

$$\lambda_{min} \le \lambda \le \lambda_{max}; \qquad (7)$$

$$\mu_{min} \le \mu \le \mu_{max}, \qquad (8)$$

де $\lambda_{min}$ і $\mu_{min}$ – мінімальні, а $\lambda_{max}$ і $\mu_{max}$ – максимальні інтенсивності потоків захисних дій та інформаційних атак, відповідно. У окремому частинному випадку: $\lambda_{min} = 0$ – ресурси, що виділяються на захист інформації – відсутні; $\mu_{min} = 0$ – атаки на ТО не проводяться.

З використанням процедури *P*-моделювання на основі операційного методу диференціально-тейлорівських перетворень [8] вихідна математична модель (2), з урахуванням умов нормування (4) і функціональних залежностей (5) та (6), зводиться до спектральної моделі вигляду

$$P_0(k+1) = \frac{T}{k+1}\left(-\lambda T P_0(k-1) + \right.$$
$$\left. + \mu T ъ(k-1) - \mu T P_0(k-1)\right), \qquad (9)$$

де $\dfrac{k+1}{T}P_0(k+1)$ – зображення похідної $\dfrac{dP_0(t)}{dt}$ в області зображень; $H$ – масштабна стала, яка має розмірність аргументу $t$ і обрана рівною тривалості диференціальної гри $H = T$, на якій розглядається функція $P_0(t)$; $k$ – цілочисельний аргумент $k =: 0, 1, 2, \ldots$; $-\lambda T P_0(k-1) = \begin{cases} -\lambda T P_0(k-1), & k \ge 1, \\ 0, & k < 1; \end{cases}$;

$\mu T ъ(k-1) = \begin{cases} \mu T, & k = 1, \\ 0, & k \ne 1; \end{cases}$, де $ъ(k-1)$ – зміщена теда;

$-\mu T P_0(k-1) = \begin{cases} -\mu T P_0(k-1), & k \ge 1, \\ 0, & k < 1. \end{cases}$.

Присвоюючи послідовно відповідні значення цілочисельному аргументу $k$, визначимо перші

шість дискрет диференціального спектра (9):

$$P_0(0) = P_0(t=0) = 1; \quad (10)$$

$$k =: 0,\ P_0(1) = 0; \quad (11)$$

$$k =: 1,\ P_0(2) = -\frac{1}{2}\lambda T^2; \quad (12)$$

$$k =: 2,\ P_0(3) = 0; \quad (13)$$

$$k =: 3,\ P_0(4) = \frac{1}{8}\left(\lambda^2 + \lambda\mu\right)T^4; \quad (14)$$

$$k =: 4,\ P_0(5) = 0; \quad (15)$$

$$k =: 5,\ P_0(6) = -\frac{1}{48}\left(\lambda^2 + \lambda\mu\right)(\lambda+\mu)T^6. \quad (16)$$

Диференціально-ігровий базис задачі моделювання передбачає вибір критерію оптимізації, що називається платою [7]. Задамо плату інтегральною моделлю вигляду

$$I_0 = \frac{1}{T}\int_0^T P_0(t)\,dt, \quad (17)$$

яка в області зображень [8] набуває вигляду

$$I_0^* = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1}. \quad (18)$$

Антагонізм інтересів гравців під час інформаційного конфлікту вимагає від них дотримання єдиної гарантованої стратегії поведінки згідно принципу мінімакса

$$I_0^*\left(\lambda(t), \mu(t)\right) = \min_{\lambda(t)\in E_\lambda}\ \max_{\mu(t)\in E\mu} I_0, \quad (19)$$

де $E_\lambda$, $E_\mu$ – замкнені обмежені у евклідових просторах $R_\lambda$ і $R_\mu$ множини, що визначають можливі стратегії гравців. При існуванні сідлової точки гри стратегії гравців $\lambda^{opt}(t)$ і $\mu^{opt}(t)$ є оптимальними, а плата (18) називається ціною гри. Наслідком відхилення від оптимальних стратегій гравців є їх втрати в платі.

Плата гри (18), з урахуванням дискрет (10)-(16), набуватиме вигляду функціонала

$$I_0^*\left(\lambda(t), \mu(t)\right) = 1 - \frac{1}{6}\lambda T^2 + \frac{1}{40}\left(\lambda^2 + \lambda\mu\right)T^4 - \frac{1}{336}\left(\lambda^2 + \lambda\mu\right)(\lambda+\mu)T^6. \quad (20)$$

Дослідження на екстремум функціонала (20) дозволяє визначити оптимальні стратегії поведінки гравців $\lambda^{opt}(t)$ і $\mu^{opt}(t)$.

Необхідні умови зводяться до рішення системи лінійних алгебраїчних рівнянь

$$\begin{cases} -\frac{1}{6}T^2 + \frac{1}{40}(2\lambda+\mu)T^4 = 0; \\ \frac{1}{40}\lambda T^4 - \frac{1}{168}\left(\lambda^2 + \lambda\mu\right)T^6 = 0, \end{cases} \quad (21)$$

рішення якої дає набір оптимальних стратегій:

$$\lambda^{opt}(t) = \frac{37}{15T^2}; \quad (22)$$

$$\mu^{opt}(t) = \frac{26}{15T^2}. \quad (23)$$

Достатні умови існування екстремуму функціонала (20) виконуються, оскільки

$$\begin{cases} \dfrac{\partial^2 I_0^*\left(\lambda(t),\ \mu(t)\right)}{\partial\lambda^2} > 0; \\ \dfrac{\partial^2 I_0^*\left(\lambda(t),\ \mu(t)\right)}{\partial\mu^2} < 0, \end{cases} \quad (24)$$

($\frac{1}{20}T^4$ і $-\frac{1}{168}\lambda T^4$, відповідно).

Таким чином, набір стратегій гравців (22) і (23) є оптимальним, а ціна гри дорівнює

$$I_0^*\left(\lambda^{opt}(t), \mu^{opt}(t)\right) = \frac{12931}{18000}. \quad (25)$$

Перехід до часової області [8] спектральної моделі (9), за умови вибору гравцями оптимальних стратегій (22) і (23), при відповідному наборі дискрет (10) – (16) дозволяє подати оптимальну траєкторію диференціальної гри $P_0^{opt}(t)$ моделлю

$$P_0^{opt}(t) = 1 - \frac{37}{30}t^2 + \frac{259}{200}t^4 - \frac{1813}{2000}t^6. \quad (26)$$

При відхиленні гравцями від оптимальних стратегій траєкторія гри $P_0(t)$ матиме вигляд

$$P_0(t) = 1 - \frac{1}{2}\lambda t^2 + \frac{1}{8}\left(\lambda^2 + \lambda\mu\right)t^4 - \frac{1}{48}\left(\lambda^2 + \lambda\mu\right)(\lambda+\mu)t^6. \quad (27)$$

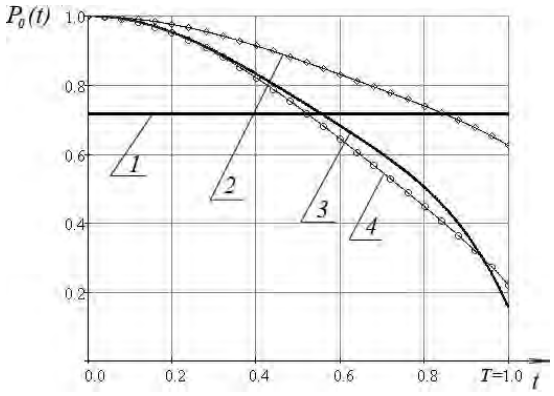


Рис. 2. Траєкторії диференціальної гри:

1 – ціна гри $I_0^*\left(\lambda^{opt}(t), \mu^{opt}(t)\right)$;

2 – $P_0(t)$ при $\lambda(t) < \lambda^{opt}(t)$, $\mu^{opt}(t)$;

3 – $P_0^{opt}(t)$ при $\lambda^{opt}(t)$, $\mu^{opt}(t)$;

4 – $P_0(t)$ при $\lambda^{opt}(t)$, $\mu(t) < \mu^{opt}(t)$

Результати імітаційного моделювання траєкторій диференціальної гри, що визначають динаміку протікання процесу нападу на інформацію за моделями (26) і (27) наведено на рис. 2. Аналіз результатів моделювання показує, що вибір гравцями оптимальних стратегій (22) і (23) гарантує протікання динаміки гри вздовж оптимальної траєкторії $P_0^{opt}(t)$, а при відхиленнях гравцями від оптимальних стратегій суб'єкти інформаційного конфлікту програють у платі.

## Висновки

У статті вирішено актуальну наукову задачу, яка полягала в розробці аналітичної моделі процесу нападу на інформацію. Модель відрізняється від відомих нестаціонарною природою потоків захисних дій та інформаційних атак. Отримані результати мають важливе прикладне значення та можуть бути використані для кількісного оцінювання рівня захищеності технічних об'єктів в складі ІКС від методів НСД.

## Список літератури

*1. Хорошко В.А. Информационная безопасность Украины: основные проблемы и перспективы / В.А. Хорошко // Захист інформації: зб. наук. пр. – К.: ДУІКТ, 2008. – № 40 (спец. випуск). – С. 6-9.*

*2. Поповский В.В. Защита информации в телекоммуникационных системах: учебник / В.В. Поповский, А.В. Персиков. – Х.: ООО "Компания СМИТ", 2006. – 238 с.*

*3. Ленков С.В. Методы и средства защиты информации: в 2-х т / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К.: Арий, 2008. – 464 с.*

*4. Ігнатов В.О. Динаміка інформаційних конфліктів в інтелектуальних системах / В.О. Ігнатов, М.М. Гузій // Проблеми інформатизації та управління. – К.: НАУ, 2005. – Вип. 15. – С. 88-92.*

*5. Метод количественной оценки защищѐнности информации в компьютерной системе / Т.В. Григорьева, С.М. Иванов, А.П. Панфилов и др. // Информационное противодействие угрозам терроризма. – М.: ФГПУ НТЦ, 2008. – Вып. 11. – С. 153-162.*

*6. Бабак В.П. Теоретичні основи захисту інформації: підручник / В.П. Бабак. – К.: НАУ, 2008 – 752 с.*

*7. Грищук Р.В. Спектральна модель процесу нападу на інформацію / Р.В. Грищук // Захист інформації: зб. наук. пр. – К.: ДУІКТ, 2009. – № 2. – С. 71-81.*

*8. Пухов Г.Е. Дифференциальные спектры и их модели / Г.Е. Пухов. – К.: Наук. думка, 1990.– 184 с.*

*Надійшла до редколегії 24.03.2009*

**Рецензент:** д-р техн. наук, проф. В.Л. Баранов, Державний університет інформаційно-комунікаційних технологій, Київ.

**Р-МОДЕЛИРОВАНИЕ ПРОЦЕССОВ НАПАДЕНИЯ НА ИНФОРМАЦИЮ ПРИ НЕСТАЦИОНАРНОЙ ПРИРОДЕ ПОТОКОВ ЗАЩИТНЫХ ВОЗДЕЙСТВИЙ ТА ИНФОРМАЦИОННЫХ АТАК**

Р.В. Грищук

*На основе метода Р-моделирование в дифференциально-игровом базисе в статье разработано аналитическую модель процесса нападения на информацию, которая отличается от известных нестационарной природой потоков защитных действий и информационных атак. Определена оптимальная траектория дифференциальной игры и оптимальные стратегии распределения информационных ресурсов игроков, рассчитана цена игры. Приведены результаты имитационного моделирования.*

***Ключевые слова:*** *дифференциальная игра, траектория, цена игры, спектральная модель, процесс нападения на информацию.*

**P-SIMULATION OF THE ATTACK PROCESS ON THE INFORMATION WITH THE NON-STATIONARY KIND OF THE PROTECTIVE AND INFORMATION ATTACK**

R.V. Gryschuk

*On base of the method P-Моделирование in differential-игровом base in article is designed analytical model of the process of the hold up to information, which differs from the known нестационарной by nature flow defensive action and information attacks. It Is Determined optimum path of the differential play and optimum strategies of the distribution information resource player, is calculated value of game. The Broughted results of simulation modeling.*

***Keywords****: differential play, path, value of game, spectral model, process of the hold up to information*.