**УДК 004.9:517.978.2**

**Грищук Р.В.**

# СПЕКТРАЛЬНА МОДЕЛЬ ПРОЦЕСУ НАПАДУ НА ІНФОРМАЦІЮ

Серед численних проблем, виникнення яких обумовлено стрімким розвитком інформаційно-комунікаційних технологій, проблема захисту інформації є ключовою [1]. Вирішення визначеної проблеми сприятиме ефективному управлінню інформаційною безпекою підприємств, установ та організацій, незалежно від форм їх власності. Небезпечний характер сучасних загроз інформаційній безпеці робить протидію їм принциповим аспектом укріплення стратегічної стабільності суспільства, національної, регіональної та міжнародної безпеки [2, 3].

Широке розповсюдження на сьогоднішній день засобів і методів НСД до інформації, яка циркулює в контурі управління технічних об'єктів, призводить до необхідності розробки превентивних мір щодо їх протидії. Однією із задач, яку потрібно розв'язати на шляху вироблення превентивних мір, спрямованих на захист інформації – це створення адекватної реальним умовам протікання інформаційного конфлікту моделі процесу нападу на інформацію [4].

Відомим моделям властивий ряд недоліків. Так модель запропонована у роботах [4-6] розвивається з позицій оптимального управління та не враховує стратегії розподілу ресурсів суб'єктів інформаційного конфлікту. У моделі [7] неврахована динаміка протікання інформаційного конфлікту. Моделі запропоновані у роботах [8-11] носять статичний характер та потребують подальшого розвитку, пов'язаного із динамічним характером протікання інформаційного конфлікту. Модель введена у [12] носить абстрактний характер. Якість її використання визначається підготовленістю експерта з інформаційної безпеки.

Метою роботи є розробка нової моделі процесу нападу на інформацію та визначення оптимальних стратегій розподілу ресурсів суб'єктів інформаційного конфлікту.

Подамо модель нападу на інформацію типовим графом процесу протікання інформаційного конфлікту (рис. 1), де $P(t)_{НСД}$ - ймовірність перебування ТО під впливом методів НСД; $P(t)_{НСД}^{МЗІ}$ - ймовірність перебування ТО під впливом методів НСД при дії методів захисту інформації (МЗІ); $P(t)_{МЗІ}^{НСД}$ - ймовірність перебування ТО під впливом МЗІ при дії методів НСД; $P(t)_{МЗІ}$ - ймовірність перебування ТО під впливом МЗІ; $\lambda_0$ $\lambda_1$ $\lambda_2$, $\mu_1$, $\mu_2$, $\mu_3$ - інтенсивності потоків захисних дій та інформаційних атак при відповідних ймовірностях; $P(t=0)_{НСД}$, $P(t=0)_{НСД}^{МЗІ}$, $P(t=0)_{МЗІ}^{НСД}$, $P(t=0)_{МЗІ}$ - початкові умови для відповідних ймовірностей.

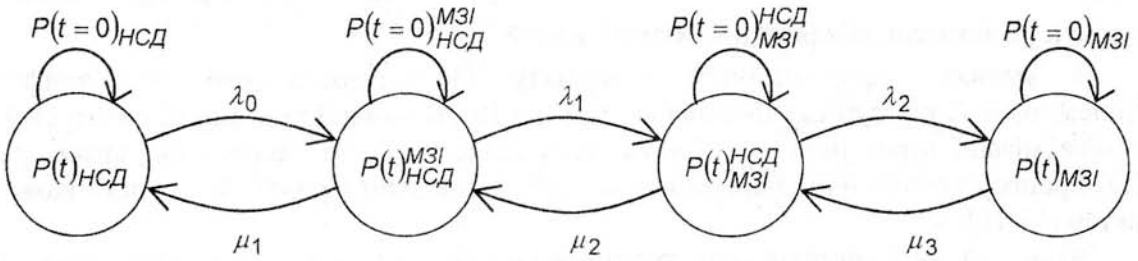


Рис. 1. Графова модель процесу нападу на інформацію

Ймовірності $P(t)_{НСД}$, $P(t)_{НСД}^{МЗІ}$, $P(t)_{МЗІ}^{НСД}$ та $P(t)_{МЗІ}$ являють собою повну групу подій:

$$P(t)_{НСД} + P(t)^{МЗІ}_{НСД} + P(t)^{НСД}_{МЗІ} + P(t)_{МЗІ} = 1. \quad (1)$$

За початкових умов

$$P(t=0)_{НСД} + P(t=0)^{МЗІ}_{НСД} + P(t=0)^{НСД}_{МЗІ} + P(t=0)_{МЗІ} = 1, \quad (2)$$

де $P(t=0)_{НСД} = 1$, $P(t=0)^{МЗІ}_{НСД} = P(t=0)^{НСД}_{МЗІ} = P(t=0)_{МЗІ} = 0$, динаміку протікання інформаційного конфлікту можна описати системою диференціальних рівнянь Колмогорова-Чепмена [13]:

$$\begin{cases} \dfrac{dP(t)_{НСД}}{dt} = -\lambda_0 P(t)_{НСД} + \mu_1 P(t)^{МЗІ}_{НСД}; \\ \dfrac{dP(t)^{МЗІ}_{НСД}}{dt} = -(\lambda_1 + \mu_1) P(t)^{МЗІ}_{НСД} + \lambda_0 P(t)_{НСД} + \mu_2 P(t)^{НСД}_{МЗІ}; \\ \dfrac{dP(t)^{НСД}_{МЗІ}}{dt} = -(\lambda_2 + \mu_2) P(t)^{НСД}_{МЗІ} + \lambda_1 P(t)^{МЗІ}_{НСД} + \mu_3 P(t)_{МЗІ}; \\ \dfrac{dP(t)_{МЗІ}}{dt} = \lambda_2 P(t)^{НСД}_{МЗІ} - \mu_3 P(t)_{МЗІ}, \end{cases} \quad (3)$$

де $t$ – поточний (дискретний) час перебування ТО у інформаційному конфлікті.

Протягом тривалості інтервалу здійснення інформаційних атак (спроб НСД) на ТО

$$t \in [0, T], \quad (4)$$

де $T$ - тривалість інтервалу, відомими вважаються обмеження на ресурси захисних дій

$$0 < \lambda_i \le \lambda_{i\max}, \quad (5)$$

та інформаційних атак

$$0 < \mu_j \le \mu_{j\max}, \quad (6)$$

де $\lambda_{i\max}$ - максимальні інтенсивності потоків захисних дій, $i = 0..2$; $\mu_{j\max}$ - максимальні інтенсивності потоків інформаційних атак, $j = 1..3$.

В умовах інформаційного конфлікту (3) інтереси суб'єктів конфлікту є протилежними. Один суб'єкт (наприклад методи НСД) намагається мінімізувати свої втрати при максимізації втрат іншого суб'єкта (наприклад МЗІ). За таких умов задача розробки моделі процесу нападу на інформацію має диференціально-ігровий базис та безкоаліційний характер [14-16].

Згідно до загальноприйнятої термінології [14-16] у диференціальних іграх суб'єкти інформаційного конфлікту називаються гравцями, правила поведінки гравців – стратегіями. Стратегії гравців вибираються в ігрових задачах з умови оптимізації деякого критерію, який називається платою. Рішення диференціального рівняння називається траєкторією гри (партії). Під ціною гри розуміють деякий критерій оптимізації, який виражається через оптимальні стратегії розподілу наявних ресурсів гравців диференціальної гри.

За умови диференціально-ігрової постановки задачі, під моделлю процесу нападу на інформацію слід розуміти траєкторію гри, яка підлягає визначенню.

Плата $I$ для широкого класу диференціальних ігор задається у вигляді суми інтегральної та термінальної складових [14]. Виходячи з потреби відображення динаміки протікання процесу інформаційного конфлікту (3), плата $I$ повинна мати інтегральний вид, де інтегрування проводитиметься вздовж траєкторії гри від моменту початку гри $t = 0$, до моменту її закінчення $t = T$ (4).

Нехай інтегральна плата $I_{НСД}$ для розроблюваної моделі процесу нападу на інформацію є зваженою середньою ймовірністю перебування ТО під впливом методів НСД $P(t)_{НСД}$ і виражається в загальній формі функціоналом

$$I_{НСД} = \frac{1}{T}\int_0^T P(t)_{НСД}\, dt\,. \tag{7}$$

З метою пошуку оптимальних правил поведінки у безкоаліційних диференціальних іграх гравці можуть використовувати різні види стратегій - гарантуючі, рівноважні по Нешу і стратегії, які слідують з концепції "погроз і контрпогроз" [14]. Вибір стратегії поведінки гравця у окремо взятій диференціальній грі визначається цілями гри.

При протилежних цілях гравців, як принцип вибору стратегій, обрано принцип мінімаксу.

Перший гравець згідно даного принципу формує стратегію $\lambda_0$, що мінімізує плату $I_{НСД}$ при умові максимізації плати іншим гравцем

$$I^*(\lambda_0, \mu_1)_{НСД} = \min_{\lambda_0 \in E_\lambda} \max_{\mu_1 \in E\mu} I_{НСД}\,, \tag{8}$$

де $I^*(\lambda_0, \mu_1)_{НСД}$ - плата, що відповідає гарантованій стратегії поведінки гравців; $E_\lambda$, $E_\mu$ - замкнені обмежені у евклідових просторах $R_\lambda$ і $R_\mu$ множини, що визначають можливі стратегії гравців.

Другий гравець формує стратегію $\mu_1$, що максимізує плату $I_{НСД}$ при умові мінімізації плати першим гравцем

$$I^*(\lambda_0, \mu_1)_{НСД} = \max_{\mu_1 \in E\mu} \min_{\lambda_0 \in E_\lambda} I_{НСД}\,. \tag{9}$$

Якщо вважати, що $\lambda_0^{ОПТ}$ і $\mu_1^{ОПТ}$ - оптимальні стратегії розподілу наявних ресурсів (5) і (6) відповідно, то при виконанні співвідношення

$$I^*\left(\lambda_0^{ОПТ}, \mu_1^{ОПТ}\right)_{НСД} = \min_{\lambda_0 \in E_\lambda} \max_{\mu_1 \in E\mu} I_{НСД} = \max_{\mu_1 \in E\mu} \min_{\lambda_0 \in E_\lambda} I_{НСД} \tag{10}$$

існує сідлова точка гри.

Основною властивістю сідлової точки гри є твердження про те, що будь-яке відхилення від оптимальної стратегії одним гравцем призводить до втрат в платі при умові вибору оптимальної стратегії іншим гравцем [14], тобто

$$I^*\left(\lambda_0,\ \mu_1^{ОПТ}\right)_{НСД} \geq \min_{\lambda_0 \in E_\lambda} I\left(\lambda_0,\ \mu_1^{ОПТ}\right)_{НСД}, \tag{11}$$

$$I^*\left(\lambda_0^{ОПТ},\ \mu_1\right)_{НСД} \leq \max_{\mu_1 \in E\mu} I\left(\lambda_0^{ОПТ},\ \mu_1\right)_{НСД}. \tag{12}$$

Ціною гри називається плата $I^*\left(\lambda_0^{ОПТ},\ \mu_1^{ОПТ}\right)_{НСД}$, яка відповідає оптимальним стратегіям $\lambda_0^{ОПТ}$ і $\mu_1^{ОПТ}$.

Урахування інтегральної плати (7) дозволяє подати ціну гри (10) виразом виду

$$I^*\left(\lambda_0^{ОПТ},\ \mu_1^{ОПТ}\right)_{НСД} = \min_{\lambda_0 \in E_\lambda} \max_{\mu_1 \in E\mu} \left(\frac{1}{T}\int_0^T P(t)_{НСД}\, dt\right). \tag{13}$$

Як видно з моделі процесу інформаційного конфлікту (3), задача моделювання процесу нападу на інформацію потребує обробки великого об'єму інформації у реальному та прискореному часі.

Розв'язання задач моделювання у реальному і прискореному часі вперше запропоновував академік НАН України Пухов Г.Є. [17, 18]. Основна ідея Пухова Г.Є. полягає у скороченні об'єму обчислень чисельними методами, яка досягається за рахунок аналітичних можливостей операційного методу диференціальних перетворень. Переведення математичної моделі інформаційного конфлікту у вигляді системи диференціальних рівнянь (3) в область зображень точним операційним методом зберігає точність вихідної моделі, але виключає часовий аргумент в області зображень. У результаті розв'язання задачі моделювання процесу нападу на інформацію значно спрощується в області зображень та зводиться до виконання чотирьох арифметичних операцій: додавання, віднімання, множення та ділення.

*Р-перетворення* [19] - новий операційний метод, який на відміну від відомих інтегральних перетворень Лапласа і Фур'є, заснований на переводі оригіналів у область зображень за допомогою операції диференціювання [17, 18]. *Р-перетвореннями* (диференціально-тейлорівськими перетвореннями, ДТ-перетвореннями) називаються функціональні перетворення виду [17]

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \quad \underline{\bullet} \quad x(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \tag{14}$$

де $x(t)$ - оригінал, що являє собою безперервну, що диференціюється нескінченне число разів і обмежену разом із всіма своїми похідними, функцію дійсного аргументу $t$; $X(k)$ і $\underline{x}(k)$ рівноцінні позначення диференціального зображення оригіналу, що представляє дискретну (гратчасту) функцію цілочисельного аргументу $k =: 0, 1, 2, \ldots$; $H$ - масштабна стала, яка має розмірність аргументу $t$ і часто обирається рівною відрізку $0 \leq t \leq H$, на якому розглядається функція $x(t)$; $\underline{\bullet}$ - символ відповідності між оригіналом $x(t)$ і його диференціальним зображенням $X(k) = \underline{x}(k)$.

У перетвореннях (14) зліва від символу $\underline{\bullet}$ стоїть пряме перетворення, що дозволяє за оригіналом $x(t)$ знайти зображення $X(k)$, а праворуч – зворотне перетворення, що дозволяє за зображенням $X(k)$ отримати оригінал $x(t)$ у формі степеневого ряду, який є ні чим іншим, як інакше записаним рядом Тейлора з центром у точці $t = 0$. Диференціальні

зображення $X(k)$ називаються диференціальними *Т-спектрами*, а значення *Т-функції* $X(k)$, при конкретних значеннях аргументу $k$, називаються дискретами.

Переведемо у область зображень систему рівнянь (3) із застосуванням *р-перетворень* (14) і подамо окремо її доданки.

Згідно формули [17] *Т-похідні* від $\frac{dP(t)_{НСД}}{dt}$, $\frac{dP(t)^{МЗІ}_{НСД}}{dt}$, $\frac{dP(t)^{НСД}_{МЗІ}}{dt}$ та $\frac{dP(t)_{МЗІ}}{dt}$ визначаються як

$$\frac{dP(t)_{НСД}}{dt} \div \bullet \; DP(k)_{НСД} = \frac{k+1}{H} P(k+1)_{НСД}, \tag{15}$$

$$\frac{dP(t)^{МЗІ}_{НСД}}{dt} \div \bullet \; DP(k)^{МЗІ}_{НСД} = \frac{k+1}{H} P(k+1)^{МЗІ}_{НСД}, \tag{16}$$

$$\frac{dP(t)^{НСД}_{МЗІ}}{dt} \div \bullet \; DP(k)^{НСД}_{МЗІ} = \frac{k+1}{H} P(k+1)^{НСД}_{МЗІ}, \tag{17}$$

$$\frac{dP(t)_{МЗІ}}{dt} \div \bullet \; DP(k)_{МЗІ} = \frac{k+1}{H} P(k+1)_{МЗІ}, \tag{18}$$

де $D$ - символ *Т-диференціювання*.

Якщо передбачити, що ТО підпадає під максимальні ресурси гравців $\lambda_{i\max}$ та $\mu_{j\max}$, то операції добутку в рівняннях системи (3) визначатимуться в області зображень наступними співвідношеннями [20]

$$\begin{aligned}
-\lambda_{0\max} P(t)_{НСД} &\div \bullet -\lambda_{0\max} P(k)_{НСД}, \\
\mu_{1\max} P(t)^{МЗІ}_{НСД} &\div \bullet \mu_{1\max} P(k)^{МЗІ}_{НСД}, \\
-(\lambda_{1\max} + \mu_{1\max}) P(t)^{МЗІ}_{НСД} &\div \bullet -(\lambda_{1\max} + \mu_{1\max}) P(k)^{МЗІ}_{НСД},
\end{aligned} \tag{19}$$

$$\begin{aligned}
\lambda_{0\max} P(t)_{НСД} &\div \bullet \lambda_{0\max} P(k)_{НСД}, \\
\mu_{2\max} P(t)^{НСД}_{МЗІ} &\div \bullet \mu_{2\max} P(k)^{НСД}_{МЗІ}, \\
-(\lambda_{2\max} + \mu_{2\max}) P(t)^{НСД}_{МЗІ} &\div \bullet -(\lambda_{2\max} + \mu_{2\max}) P(k)^{НСД}_{МЗІ},
\end{aligned} \tag{20}$$

$$\begin{aligned}
\lambda_{1\max} P(t)^{МЗІ}_{НСД} &\div \bullet \lambda_{1\max} P(k)^{МЗІ}_{НСД}, \\
\mu_{3\max} P(t)_{МЗІ} &\div \bullet \mu_{3\max} P(k)_{МЗІ},
\end{aligned} \tag{21}$$

$$\begin{aligned}
\lambda_{2\max} P(t)^{НСД}_{МЗІ} &\div \bullet \lambda_{2\max} P(k)^{НСД}_{МЗІ}, \\
-\mu_{3\max} P(t)_{МЗІ} &\div \bullet -\mu_{3\max} P(k)_{МЗІ}
\end{aligned} \tag{22}$$

З урахуванням (15)-(22), вихідна модель інформаційного конфлікту (3) матиме в області зображень вид *р-моделі* виду

$$\begin{cases} \frac{k+1}{H} P(k+1)_{НСД} = -\lambda_{0\max} P(k)_{НСД} + \mu_{1\max} P(k)^{МЗІ}_{НСД}; \\ \frac{k+1}{H} P(k+1)^{МЗІ}_{НСД} = -(\lambda_{1\max} + \mu_{1\max}) P(k)^{МЗІ}_{НСД} + \lambda_{0\max} P(k)_{НСД} + \mu_{2\max} P(k)^{НСД}_{МЗІ}; \\ \frac{k+1}{H} P(k+1)^{НСД}_{МЗІ} = -(\lambda_{2\max} + \mu_{2\max}) P(k)^{НСД}_{МЗІ} + \lambda_{1\max} P(k)^{МЗІ}_{НСД} + \mu_{3\max} P(k)_{МЗІ}; \\ \frac{k+1}{H} P(k+1)_{МЗІ} = \lambda_{2\max} P(k)^{НСД}_{МЗІ} - \mu_{3\max} P(k)_{МЗІ}. \end{cases} \quad (23)$$

Згрупуємо доданки в *р-моделі* (23) відносно $P(k+1)_{НСД}$, $P(k+1)^{МЗІ}_{НСД}$, $P(k+1)^{НСД}_{МЗІ}$ та $P(k+1)_{МЗІ}$, при цьому значення масштабної сталої $H$ оберемо рівним тривалості інтервалу інформаційних атак $T$ (4), тобто $H = T$. Тоді, з урахуванням процедури групування доданків, вихідна спектральна *р-модель* матиме кінцевий вид

$$\begin{cases} P(k+1)_{НСД} = \frac{T}{k+1}\left(-\lambda_{0\max} P(k)_{НСД} + \mu_{1\max} P(k)^{МЗІ}_{НСД}\right); \\ P(k+1)^{МЗІ}_{НСД} = \frac{T}{k+1}\left(-(\lambda_{1\max} + \mu_{1\max}) P(k)^{МЗІ}_{НСД} + \lambda_{0\max} P(k)_{НСД} + \mu_{2\max} P(k)^{НСД}_{МЗІ}\right); \\ P(k+1)^{НСД}_{МЗІ} = \frac{T}{k+1}\left(-(\lambda_{2\max} + \mu_{2\max}) P(k)^{НСД}_{МЗІ} + \lambda_{1\max} P(k)^{МЗІ}_{НСД} + \mu_{3\max} P(k)_{МЗІ}\right); \\ P(k+1)_{МЗІ} = \frac{T}{k+1}\left(\lambda_{2\max} P(k)^{НСД}_{МЗІ} - \mu_{3\max} P(k)_{МЗІ}\right). \end{cases} \quad (24)$$

Присвоюючи послідовно цілочисельні значення аргументу $k =: 0, 1, 2$, за *р-моделлю* (24) знайдемо дискрети диференціальних спектрів рівнянь системи (3).

Нульові дискрети згідно [17] визначаються через початкові умови (2)

$$P(0)_{НСД} = 1,\ P(0)^{МЗІ}_{НСД} = 0,\ P(0)^{НСД}_{МЗІ} = 0,\ P(0)_{МЗІ} = 0. \quad (25)$$

При значеннях цілочисельного аргументу $k =: 0, 1, 2$ дискрети диференціальних спектрів *р-моделі* матимуть вид

$$P(1)_{НСД} = -\lambda_{0\max} T, \quad (26)$$

$$P(2)_{НСД} = \frac{1}{2}\left(\lambda^2_{0\max} T + \mu_{1\max} P(1)^{МЗІ}_{НСД}\right) T, \quad (27)$$

$$P(3)_{НСД} = \frac{1}{3}\left(-\lambda_{0\max} \frac{T}{2}\left(\lambda^2_{0\max} T + \mu_{1\max} P(1)^{МЗІ}_{НСД}\right) + \mu_{1\max} P(2)^{МЗІ}_{НСД}\right) T, \quad (28)$$

$$P(1)^{МЗІ}_{НСД} = \lambda_{0\max} T, \quad (29)$$

$$P(2)^{МЗІ}_{НСД} = \frac{1}{2}\left(-(\lambda_{1\max} + \mu_{1\max}) \lambda_{0\max} T - \lambda^2_{0\max} T + \mu_{2\max} P(1)^{НСД}_{МЗІ}\right) T, \quad (30)$$

$$P(3)^{МЗІ}_{НСД} = \frac{1}{3}\left(-(\lambda_{1\max} + \mu_{1\max})\left(\frac{T}{2}\left(-(\lambda_{1\max} + \mu_{1\max}) \lambda_{0\max} T - \lambda^2_{0\max} T + \mu_{2\max} P(1)^{НСД}_{МЗІ}\right)\right) + \right.$$
$$\left. + \lambda_{0\max} \frac{T}{2}\left(\lambda^2_{0\max} T + \mu_{1\max} \lambda_{0\max} T\right) + \mu_{2\max} P(2)^{НСД}_{МЗІ}\right) T, \quad (31)$$

$$P(1)^{НСД}_{МЗІ} = 0, \quad (32)$$

$$P(2)^{НСД}_{МЗІ} = \frac{1}{2}\left(\lambda_{0\max} \lambda_{1\max} T + \mu_{3\max} P(1)_{МЗІ}\right) T, \quad (33)$$

$$P(3)_{M3I}^{HCД} = \frac{1}{3}\left(-\left(\lambda_{2\max}+\mu_{2\max}\right)\left(\frac{T}{2}\left(\lambda_{0\max}\,\lambda_{1\max}\,T+\mu_{3\max}\,P(1)_{M3I}\right)\right)+\right.$$
$$\left.+\lambda_{1\max}\left(\frac{T}{2}\left(-\left(\lambda_{1\max}+\mu_{1\max}\right)\lambda_{0\max}\,T-\lambda_{0\max}^{2}\,T\right)\right)+\mu_{3\max}\,P(2)_{M3I}\right)T, \quad (34)$$

$$P(1)_{M3I}=0, \quad (35)$$

$$P(2)_{M3I}=0, \quad (36)$$

$$P(3)_{M3I}=\frac{1}{6}\lambda_{0\max}\,\lambda_{1\max}\,\lambda_{2\max}\,T^{3}. \quad (37)$$

Аналіз дискрет (26)-(37) *р-моделі* (24) показує, що у дискрети (27) та (28) послідовно "вкладаються" дискрети наступного диференціального спектра (30) і (31), у дискрети (29) і (30) – дискрети (32) і (33), у дискрети (33) і (34) – (35)-(37) відповідно. Провівши операцію послідовної підстановки та групування дискрет при однакових множниках, отримаємо кінцеві вирази для шуканих дискрет відповідних диференціальних спектрів *р-моделі*

$$P(2)_{HCД}=\frac{1}{2}\lambda_{0\max}\left(\lambda_{0\max}+\mu_{1\max}\right)T^{2}, \quad (38)$$

$$P(3)_{HCД}=-\frac{1}{6}\lambda_{0\max}\left(\lambda_{0\max}^{2}+2\lambda_{0\max}\mu_{1\max}+\lambda_{1\max}\mu_{1\max}+\mu_{1\max}^{2}\right)T^{3}, \quad (39)$$

$$P(2)_{HCД}^{M3I}=-\frac{1}{2}\lambda_{0\max}\left(\lambda_{0\max}+\lambda_{1\max}+\mu_{1\max}\right)T^{2}, \quad (40)$$

$$P(3)_{HCД}^{M3I}=\frac{1}{6}\lambda_{0\max}\left(\lambda_{0\max}^{2}+\lambda_{1\max}^{2}+\mu_{1\max}^{2}+2\lambda_{1\max}\,\mu_{1\max}+2\lambda_{0\max}\,\mu_{1\max}+\right.$$
$$\left.+\lambda_{0\max}\,\lambda_{1\max}+\lambda_{1\max}\,\mu_{2\max}\right)T^{3}. \quad (41)$$

$$P(2)_{M3I}^{HCД}=\frac{1}{2}\lambda_{0\max}\,\lambda_{1\max}\,T^{2}, \quad (42)$$

$$P(3)_{M3I}^{HCД}=-\frac{1}{6}\lambda_{0\max}\,\lambda_{1\max}\left(\lambda_{0\max}+\lambda_{1\max}+\lambda_{2\max}+\mu_{1\max}+\mu_{2\max}\right)T^{3}. \quad (43)$$

Таким чином, обмежившись значеннями цілочисельного аргументу $k=\overline{0,1,2}$, спектральна модель процесу нападу на інформацію $P(k+1)_{HCД}$ є набором дискрет диференціального спектра – нульової дискрети $P(0)_{HCД}=1$ та дискрет (26), (38) і (39).

Якщо вважати, що $\lambda_{1\max}=0$, а ресурси гравців $\lambda_0$ і $\mu_1$ обмежені в заданих границях (5) і (6) відповідно, то застосування зворотного перетворення (14) до дискрет (25), (26), (38) і (39) дозоляє перейти від спектральної моделі процесу нападу на інформацію $P(k+1)_{HCД}$ в області зображень до загальної моделі процесу нападу на інформацію $P(t)_{HCД}$ у часовій області, яка матиме вид

$$P(t)_{HCД}=1-\lambda_0\,t+\frac{1}{2}\lambda_0\left(\lambda_0+\mu_1\right)t^{2}-\frac{1}{6}\lambda_0\left(\lambda_0+\mu_1\right)^{2}t^{3}. \quad (44)$$

Ціна гри $I^{*}\left(\lambda_0^{ОПТ},\ \mu_1^{ОПТ}\right)_{HCД}$ (13) визначатиметься через відповідні дискрети (25), (26), (38) і (39) диференціального спектра $P(k+1)_{HCД}$ виразом виду [17]

$$I^*_{НСД} = \sum_{k=0}^{k=\infty} \frac{P(k)_{НСД}}{k+1}. \tag{45}$$

Підстановка дискрет (25), (26), (38) та (39) у вираз (45), дозволяє подати ціну гри у вигляді функції двох змінних

$$I^*\left(\lambda^{ОПТ}_{0max}, \mu^{ОПТ}_{1max}\right)_{НСД} = 1 - \frac{1}{2}\lambda_{0max} T + \frac{1}{6}\lambda_{0max}\left(\lambda_{0max} + \mu_{1max}\right)T^2 - \\ - \frac{1}{24}\lambda_{0max}\left(\lambda^2_{0max} + 2\lambda_{0max}\mu_{1max} + \lambda_{1max}\mu_{1max} + \mu^2_{1max}\right)T^3 . \tag{46}$$

Необхідні умови існування сідлової точки гри $I^*\left(\lambda^{ОПТ}_{0max}, \mu^{ОПТ}_{1max}\right)_{НСД}$ мають вид системи кінцевих рівнянь

$$\begin{cases} \dfrac{\partial I^*\left(\lambda^{ОПТ}_{0max}, \mu^{ОПТ}_{1max}\right)_{НСД}}{\partial \lambda^{ОПТ}_{0max}} = 0; \\ \dfrac{\partial I^*\left(\lambda^{ОПТ}_{0max}, \mu^{ОПТ}_{1max}\right)_{НСД}}{\partial \mu^{ОПТ}_{1max}} = 0. \end{cases} \tag{47}$$

Знаходження частинних похідних за кожним з рівнянь системи (47) звелося до системи лінійних алгебраїчних рівнянь (СЛАР) виду

$$\begin{cases} -1 + \frac{2}{3}\lambda^{ОПТ}_{0max} T + \frac{1}{3}\mu^{ОПТ}_{1max} T = 0; \\ 1 - \frac{1}{2}\lambda^{ОПТ}_{0max} T - \frac{1}{4}\lambda^{ОПТ}_{1max} T - \frac{1}{2}\mu^{ОПТ}_{1max} T = 0, \end{cases} \tag{48}$$

розв'язання якої відносно шуканої сідлової точки гри матиме вид

$$\begin{cases} \lambda^{ОПТ}_{0max} = \frac{3}{2T} - \frac{1}{2}\mu^{ОПТ}_{1max}; \\ \mu^{ОПТ}_{1max} = \frac{2}{T} - \lambda^{ОПТ}_{0max} - \frac{1}{2}\lambda^{ОПТ}_{1max}. \end{cases} \tag{49}$$

Аналіз графової моделі (рис. 1) показує, що внаслідок непрямого впливу захисних ресурсів $\lambda^{ОПТ}_{1max}$ на стан ТО $P(t)_{НСД}$, їх величиною можна знехтувати, тобто

$$\lambda^{ОПТ}_{1max} = 0. \tag{50}$$

Рішення СЛАР (49), з урахуванням (50), дозволяє визначити оптимальні стратегії гравців $\lambda^{ОПТ}_{0max}$ та $\mu^{ОПТ}_{1max}$, що дорівнюватимуть

$$\lambda_{0\max}^{ОПТ} = \frac{1}{T}, \tag{51}$$

$$\mu_{1\max}^{ОПТ} = \frac{1}{T}. \tag{52}$$

Достатніми умовами існування сідлової точки $I^*\left(\lambda_{0\max}^{ОПТ}, \mu_{1\max}^{ОПТ}\right)_{НСД}$ (46) є

$$\begin{cases} \dfrac{\partial^2 I^*\left(\lambda_{0\max}^{ОПТ}, \mu_{1\max}^{ОПТ}\right)_{НСД}}{\partial \lambda_{0\max}^{ОПТ\ 2}} > 0; \\ \dfrac{\partial^2 I^*\left(\lambda_{0\max}^{ОПТ}, \mu_{1\max}^{ОПТ}\right)_{НСД}}{\partial \mu_{1\max}^{ОПТ\ 2}} < 0. \end{cases} \tag{53}$$

Оскільки

$$\begin{cases} \dfrac{\partial^2 I^*\left(\lambda_{0\max}^{ОПТ}, \mu_{1\max}^{ОПТ}\right)_{НСД}}{\partial \lambda_{0\max}^{ОПТ\ 2}} = \dfrac{2}{3}T; \\ \dfrac{\partial^2 I^*\left(\lambda_{0\max}^{ОПТ}, \mu_{1\max}^{ОПТ}\right)_{НСД}}{\partial \mu_{1\max}^{ОПТ\ 2}} = -\dfrac{1}{12}\lambda_{0\max}^{ОПТ} T^3, \end{cases} \tag{54}$$

то достатня умова (53) існування сідлової точки (46) виконується.

З урахуванням (51) і (52), при $t = T$, ціна гри, виражена функцією двох змінних виду (46), дорівнює

$$I^*\left(\lambda_{0\max}^{ОПТ}, \mu_{1\max}^{ОПТ}\right)_{НСД} = \frac{2}{3}. \tag{55}$$

Траєкторію диференціальної гри $P(t)_{НСД}$, представлену в загальному вигляді набором дискрет (25), (26), (38) та (39), яка відповідає оптимальним стратегіям (51) і (52), отримаємо в аналітичному виді. Для цього застосуємо операцію зворотного перетворення (14) у область оригіналів до першого рівняння *р-моделі* (24) за її дискретами (25), (26), (38), (39) та набором оптимальних стратегій (51) і (52)

$$P(t)_{НСД} = 1 - \frac{t}{T} + \left(\frac{t}{T}\right)^2 - \frac{2}{3}\left(\frac{t}{T}\right)^3. \tag{56}$$

Траєкторія (56), отримана на основі *р-моделі* (24), відображає динаміку перебування технічного об'єкта під впливом методів НСД у заданий момент часу $t$ на визначеному часовому інтервалі (4) і є моделлю процесу нападу на інформацію в часовій області, за умови вибору гравцями оптимальних стратегій (51) та (52).

Таким чином, диференціальна гра (1)-(7) вирішена повністю. Знайдено ціну гри (55), оптимальні стратегії розподілу ресурсів (51), (52) і траєкторію гри (56), яка відповідає оптимальним стратегіям.

Висновки та перспективи подальших досліджень. Модель (24) є адекватною моделлю протікання реального процесу нападу на інформацію. Розроблена спектральна модель нападу на інформацію $P(k+1)_{НСД}$ дозволила в аналітичній формі отримати вирази (44) та (56), що відображають динаміку перебування технічного об'єкта під впливом методів несанкціонованого доступу, під час нападу на інформацію, на часовому інтервалі (4), при відхиленні гравцями від оптимальних стратегій (51) і (52) та при їх виборі, відповідно.

Застосування моделей (44) та (56), отриманих на основі спектральної моделі $P(k+1)_{НСД}$, дозволяє визначати стан перебування ТО під впливом методів НСД для моментів часу у минулому, теперішньому і порівняно недалекому майбутньому.

У подальшому планується провести дослідження моделі (56) при відхиленнях поведінки гравців від оптимальних стратегій (51) і (52).

**Список літератури**


1. *Стратегія* управління інформаційною безпекою / В.І. Андрєєв, В.Д. Козюра, Л.М. Скачек, В.О. Хорошко. – К.: ДУІКТ, 2007. – 272 с.
2. *Хорошко В.О.* Информационная безопасность Украины. Основные проблемы и перспективы // Захист інформації. – К.: ДУІКТ, 2008. – № 40 (спеціальний випуск). – С. 6-9.
3. *Даник Ю.Г.* Національна безпека: запобігання критичним ситуаціям: Монографія / Даник Ю.Г., Катков Ю.І., Пічугін М.Ф. – Житомир: Рута, 2006. – 388 с.
4. *Ігнатов В.О.* Динаміка інформаційних конфліктів в інтелектуальних системах / Ігнатов В.О., Гузій М.М. // Проблеми інформатизації та управління. – К.: НАУ, 2005. – Вип. 15. – С. 88-92.
5. *Игнатов В.*А. Оптимальное управление скаляризацией векторных критериев в конфликтующих системах / Игнатов В.А., Гузий М.М. // Проблеми інформатизації та управління. – К.: НАУ, 2004. – Вип. 11. – С. 118-126.
6. *Игнатов В.*А. Оптимальное управление информационной безопасностью / Игнатов В.А., Гузий М.М. // Проблеми інформатизації та управління. – К.: НАУ, 2004. – Вип. 14. – С. 71-74.
7. *Мельников В.В.* Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
8. *Браіловський М.М.* Кількісно-якісна оцінка рівня інформаційної безпеки / Браіловський М.М., Габович А.Г., Горобець А.Ю., [та ін.] // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2006. - № 9 (103), Частина 1. – с. 14-17.
9. *Андреев В.И.* Количественная оценка защищённости технических объектов с учётом их функционирования / Андреев В.И., Козлов В.С., Хорошко В.А. // Захист інформації. – К.: НАУ, 2004. - № 2. – С. 47-50.
10. *Козлов В.С.* Количественная оценка защищённости информации / Козлов В.С., Хорошко В.А. // Захист інформації. – К.: НАУ, 2003. – № 4. – С. 67-73.
11. *Козлова К.В.* Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) / Козлова К.В., Хорошко В.О. // Захист інформації. – К.: ДІТС, 2007. - № 1. С. 30-32.
12. *ISO 15408.* The Common Criteria for Information Technology Security Evaluation.
13. *Гнеденко Б.В.* Введение в теорию массового обслуживания / Гнеденко Б.В., Коваленко И.Н. – М.: Наука, 1987. – 336 с.
14. *Васильев В.В.* Моделирование задач оптимизации и дифференциальных игр / В.В. Васильев, В.Л. Баранов. – К.: Наукова думка, 1989. – 286 с.
15. *Вайсборд Э.М.* Введение в дифференциальные игры нескольких лиц и их приложения / Э.М. Вайсборд, В.И. Жуковский. – М.: Советское радио, 1980. – 304 с.

16. *Гермейер Ю.Б.* Игры с противоположными интересами. – М.: Наука, 1976.

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

18. *Пухов Г.Е.* Дифференциальные преобразования функций и уравнений. – К.: Наук. думка, 1984. – 420 с.

19. *Р-моделювання* складних динамічних систем / [Г.Л. Баранов, М.М. Браіловський, А.А. Засядько та ін.]; за ред. проф. Г.Л. Баранова та проф. В.О. Хорошко. – К.: ДУІКТ, 2008 – 132 с.

20. *Диференціальні* перетворення для комп'ютерного моделювання керуючих систем: [навч. посібн. для студ. вищ. навч. закл.] / О.І. Стасюк, В.Л. Баранов, Г.Л. Баранов, О.Г. Фролова. – К.: КУЕТТ, 2005. – 135 с.

*Надійшла 25.12.2008*

**УДК 004.681** **Дудикевич Я.В., Прокопишин І.А.**

## ВАРТІСТЬ РИЗИКУ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Кількісна оцінка інформаційних ризиків є актуальною проблемою, насамперед для побудови ефективних систем захисту інформації [1,2]. Більшість праць у напрямі оцінки ефективності та оптимізації систем захисту інформації використовують критерії ефективності, які ґрунтуються на таких класичних мірах ризику як математичне сподівання та дисперсія втрат [3-7].

У сучасному фінансовому ризик-менеджменті ефективно використовують міру ризику Value at Risk (VaR), з англійської – вартість (капітал) під ризиком [8]. Ця міра визначається максимально можливими, з деякою ймовірністю, втратами і зручна для оцінки сумарних ризиків, зумовлених чинниками різної природи.

В роботі запропонована методика оцінки ризику для систем захисту інформації з використанням вартості ризику VaR. Для опису можливих втрат для системи захисту інформації використана дискретна ймовірнісна модель.

**Вартість ризику Value at Risk**

Нехай $\xi$ – випадкова величина втрат в абсолютному або відносному вимірі за деякий період, наприклад, за рік. Вартістю (ціною) ризику за рівня значущості (довіри) $0 < \alpha < 1$ називають максимальні можливі з ймовірністю $\alpha$ втрати за цей період:

$$VaR_\alpha = \sup\{x \mid P\{\xi < x\} \le \alpha\}. \qquad (1)$$

Іншими словами " з ймовірністю $\alpha$ втрати за період не перевищать величини $VaR_\alpha$ " або "лише з ймовірністю $1-\alpha$ втрати будуть більшими за $VaR_\alpha$ ".

Рівень довіри $\alpha$ виражає відношення до ризику. Для банківського сектору Базельський комітет з банківського нагляду рекомендує рівень довіри 0,99 (99%), на практиці застосовують і нижчий рівень – до 95 % [8].

Означимо функцію розподілу випадкової величини втрат [9]:

$$F(x) = P\{\xi < x\}. \qquad (2)$$

Тоді, означення вартості ризику (1) можна переписати так