УДК 004.9:517.978.2 **Грищук Р. В.**

ДИФЕРЕНЦІАЛЬНО-ІГРОВИЙ МЕТОД АНАЛІЗУ НАДІЙНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ, НА ОСНОВІ ЇХ СПЕКТРАЛЬНИХ Р-МОДЕЛЕЙ

Постановка проблеми в загальному вигляді та її зв'язок з важливими практичними завданнями. Теорія і практика проектування та побудови високоефективних систем захисту інформації (СЗІ), неминуче пов’язана з потребою проведення аналізу їх надійності [1-4]. Процедура проведення такого аналізу відкриває замовнику можливість обґрунтованого вибору методів та засобів захисту інформації та сприяє оптимізації режиму захисту об’єктів [5].

Аналіз останніх досліджень і публікацій. Кількість наукових публікацій, що присвячені сформульованій проблемі на сьогоднішній день обмежена. Серед відомих методів аналізу СЗІ з літератури [2, 3, 5] зрозуміло, що такі методи не дозволяють в повній мірі враховувати динаміку протікання інформаційного конфлікту в СЗІ під впливом варіацій ресурсу противника. Це значно обмежує область застосування таких методів та потребує їх доопрацювання.

Відомо, що потреба врахування динаміки зміни станів СЗІ під впливом довільних стратегій розподілу інформаційних ресурсів суб’єктами інформаційного конфлікту значно впливає на показники надійності СЗІ [4]. Таким чином, задача розробки методу аналізу надійності СЗІ, з урахуванням динаміки процесів, що в ній протікають, є актуальною та потребує свого розв’язання.

Метою статті є розробка методу аналізу надійності СЗІ.

Викладення основного змісту дослідження. Представимо запропоновану в [6] графову модель СЗІ (рис. 1) та, на її базі, розкриємо суть розроблюваного методу.

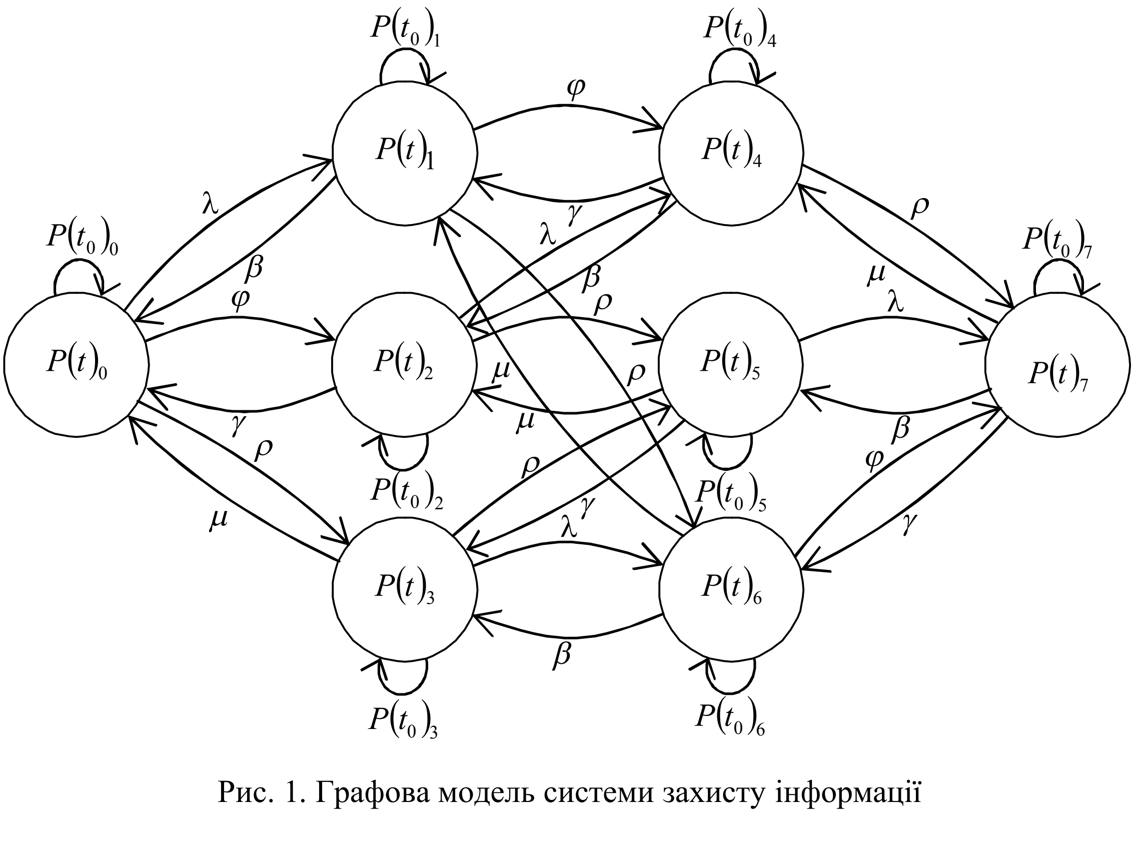

Рис. 1. Графова модель системи захисту інформації

В моделі (див. рис. 1) кружечками позначено стани, в яких може перебувати СЗІ під впливом відповідних інтенсивностей: λ - інтенсивність потоку захисних дій (інтенсивність перевірки СЗІ з приведенням її до робочого стану); μ - інтенсивність потоку атак (спроб несанкціонованого доступу (НСД)); β - інтенсивність відмов СЗІ; γ - інтенсивність знаходження вразливостей в СЗІ; φ - інтенсивність усунення вразливостей; ρ - інтенсивність створення нової інформації. В кружечках записано ймовірності станів СЗІ, які розподілено відповідно до таблиці.

Таблиця 1. Таблиця розподілу ймовірностей станів СЗІ

Стан СЗІ	$P(t)_0$	$P(t)_1$	$P(t)_2$	$P(t)_3$	$P(t)_4$	$P(t)_5$	$P(t)_6$	$P(t)_7$
вразлива (+); невразлива (-)	+	+	-	+	-	-	+	-
роботоспроможна (+); відмова (-)	-	+	-	-	+	-	+	+
спроба НСД (+); без НСД (-)	+	+	+	-	+	-	-	-

За графовою моделлю (див. рис. 1) модель інформаційного конфлікту в СЗІ у формалізованій постановці може бути подана системою лінійних диференціальних рівнянь Колмогорова-Чепмена

$$\begin{aligned}
\frac{dP_0(t)}{dt} &= -(\lambda+\varphi+\rho)P_0(t)+\beta P_1(t)+\gamma P_2(t)+\mu P_3(t);\\
\frac{dP_1(t)}{dt} &= -(\beta+\varphi+\rho)P_1(t)+\lambda P_0(t)+\gamma P_4(t)+\mu P_6(t);\\
\frac{dP_2(t)}{dt} &= -(\gamma+\lambda+\rho)P_2(t)+\varphi P_0(t)+\beta P_4(t)+\mu P_5(t);\\
\frac{dP_3(t)}{dt} &= -(\mu+\varphi+\lambda)P_3(t)+\rho P_0(t)+\gamma P_5(t)+\beta P_6(t);\\
\frac{dP_4(t)}{dt} &= -(\gamma+\beta+\rho)P_4(t)+\varphi P_1(t)+\lambda P_2(t)+\mu P_7(t);\\
\frac{dP_5(t)}{dt} &= -(\mu+\gamma+\lambda)P_5(t)+\rho P_2(t)+\varphi P_3(t)+\beta P_7(t);\\
\frac{dP_6(t)}{dt} &= -(\mu+\beta+\varphi)P_6(t)+\rho P_1(t)+\lambda P_3(t)+\gamma P_7(t);\\
\frac{dP_7(t)}{dt} &= -(\mu+\beta+\gamma)P_7(t)+\rho P_4(t)+\lambda P_5(t)+\varphi P_6(t).
\end{aligned} \tag{1}$$

Кількість рівнянь у системі (1) відповідає кількості станів, в яких може перебувати СЗІ. Система рівнянь (1) справедлива за умов нормування

$$\sum_{z=0}^{7} P_z(t) = 1\,. \tag{2}$$

У початковий момент t_0 СЗІ перебуває в захищеному стані з ймовірністю $P_7(t_0)=1$ ($P_0(t_0)=\cdots=P_6(t_0)=0$). Перехід СЗІ зі стану $P_7(t)$ в інші стани, відповідно до графової моделі (рис. 1), здійснюється під впливом відповідних інтенсивностей. Замовником СЗІ висунуто вимоги, відповідно до яких відомими вважаються інтенсивності β , γ , φ та ρ .

Противник, варіюючи власним ресурсом нападу μ , який належить замкненій множині $\mathrm{M} \in E_\mu$, обмеженій в евклідовому просторі R_μ , намагається зменшити захищеність СЗІ та отримати найменший програш в платі I_1 . Для цього він обирає таку стратегію розподілу власних ресурсів μ , яка мінімізує плату

$$\min_{\mathrm{M}\in E_\mu} = I_1(t,\, P_7(t),\, \mu)\ , \tag{3}$$

де

$$I_1 = \frac{1}{T}\int\limits_{t_0}^{T} P_7(t)\,dt\,. \tag{4}$$

Ресурс противника μ та плата за зменшення захищеності СЗІ I_1, обмежені за величиною

$$\mu_{\min} \le \mu \le \mu_{\max}\,, \tag{5}$$

та

$$0 \le I_1 \le I_{1\max}\,,\ \text{де}\ I_{1\max} = 1\,, \tag{6}$$

відповідно.

Накладення обмежень на ресурс противника вигляду (5), для досягнення цілі (3), вимагає від нього економних його витрат I_2, тобто

$$\min_{\mathrm{M} \in E_\mu} = I_2(t,\, \mu), \tag{7}$$

де

$$I_2 = \frac{1}{T}\int\limits_{0}^{T} \mu^2 dt\,. \tag{8}$$

На критерій (8) накладаються обмеження вигляду

$$0 \le I_2 \le I_{2\max}\,,\ I_{2\max} = 1\,. \tag{9}$$

Цілі противника (3) та (7) можуть бути представлені у вигляді узагальненого векторного критерію I , як

$$\min_{\mathrm{M} \in E_\mu} I = \alpha_1 I_1 + \alpha_2 I_2\,, \tag{10}$$

де α_1, α_2 - вагові коефіцієнти, що визначають пріоритет відповідних частинних критеріїв I_1 та I_2. Коефіцієнти обираються з умови $\sum\limits_{i=1}^{2} \alpha_i = 1$. Оскільки для противника критерії (3) та (7) мають однаковий пріоритет, то можна перейти від схеми інтегральної оптимальності (10) до оптимізаційної задачі вигляду [7]

$$\min_{\mathrm{M} \in E_\mu} I^* = I_1 + I_2\,. \tag{11}$$

Процедура диференціально-ігрового аналізу надійності СЗІ зводиться до визначення за спектральною Р- моделлю системи (1) ймовірності функціонування СЗІ без вразливостей при відсутності спроб НСД $P_7(t)$, плати I^*, стратегій противника μ і СЗІ λ та, на їх основі, $T_{СЗІ}$ – середнього часу подолання СЗІ.

Для знаходження вказаних показників надійності перейдемо від оригіналів вигляду (1) та (11) до їх спектральних Р- моделей. Дану операцію здійснимо з використанням диференціальних перетворень академіка НАН України Г. Є. Пухова [8], відповідно до [9].

Спектральна Р-модель, з урахуванням [8], набуватиме вигляду

$$P_7(k+1) = \frac{T}{k+1}\left(-(\mu+\beta+\gamma)P_7(k) + \rho\, P_4(k) + \lambda\, P_5(k) + \varphi\, P_6(k)\right), \tag{12}$$

де $\{P_z(k)\}$ – диференціальні зображення відповідних оригіналів $\{P_z(t)\}$ ($z = 0,\ldots,7$), що представляють собою дискретні (гратчасті) функції цілочисельного аргументу $k =: 0, 1, 2, \ldots$

Дискрети спектральної Р-моделі, при $k =: 0, 1, 2$, дорівнюють

$$P_0(0) = [P_7(t_0)] = 1\,, \tag{13}$$

$$P_7(1) = -(\mu+\beta+\gamma)T\,, \tag{14}$$

$$P_7(2) = \frac{1}{2}\left((\mu+\beta+\gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\gamma\right)T^2\,, \tag{15}$$

$$\begin{aligned} P_7(3) = -\frac{1}{6}\Big((\mu+\beta+\gamma)\left((\mu+\beta+\gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\gamma\right) + \rho\,\mu\,(2\gamma + 2\beta + \rho + \mu) + \\ + \lambda\,\beta\,(2\mu + 2\gamma + \lambda + \beta) + \varphi\gamma\,(2\mu + 2\beta + \varphi + \gamma)\Big)T^3\,. \end{aligned} \tag{16}$$

Спектральна Р-модель плати (11) в області зображень має вигляд

$$I^{*}=\sum_{k=0}^{k=\infty}\frac{P_{7}(k)}{k+1}+\sum_{k=0}^{k=\infty}\frac{M^{2}(k)}{k+1}, \tag{17}$$

де *Р-зображення* диференціального спектру $M^{2}(k)$, визначається як

$$M^{2}(k)=\begin{cases}\mu^{2}, & k=0;\\ 0, & k\geq 1.\end{cases} \tag{18}$$

Відповідні дискрети для *Р-зображення* (18), дорівнюватимуть

$$M^{2}(0)=\mu^{2}, \text{ де } M^{2}(k\geq 1)=0. \tag{19}$$

Для знаходження оптимальних стратегій розподілу ресурсів нападу μ^{opt} та захисту λ^{opt} в конфлікті (1) дослідимо плату (17) на екстремум [10]

$$\begin{cases}\dfrac{\partial I^{*}(\lambda,\mu)}{\partial\lambda}=0;\\ \dfrac{\partial I^{*}(\lambda,\mu)}{\partial\mu}=0.\end{cases} \tag{20}$$

У результаті система (20) зводиться до системи лінійних алгебраїчних рівнянь (СЛАР)

$$\begin{cases}-T+\dfrac{1}{3}(2\mu+2\beta+2\gamma+\rho)+\mu=0;\\ 1-\dfrac{1}{4}(3\mu+3\gamma+2\beta+2\lambda)T=0.\end{cases} \tag{21}$$

Рішення СЛАР (21) методом Гауса, дозволяє визначити шукані стратегії

$$\lambda^{opt}=\frac{48-12(2\beta+3\gamma)T-T^{2}+(2\beta+3\rho)T^{3}}{4\left(6+T^{2}\right)T}, \tag{22}$$

$$\mu^{opt}=\frac{(3-(2\gamma+2\beta+\rho)T)T}{2\left(6+T^{2}\right)}. \tag{23}$$

Для знаходження знаку знайдених екстремумів (22) та (23), перевіримо фунціонал (17) на виконання достатніх умов

$$\begin{cases}\dfrac{\partial^{2} I^{*}(\lambda,\mu)}{\partial\lambda^{2}}>0;\\ \dfrac{\partial^{2} I^{*}(\lambda,\mu)}{\partial\mu^{2}}<0,\end{cases}\quad\Rightarrow\quad\begin{cases}\dfrac{1}{3}T^{2}+2>0;\\ -\dfrac{1}{12}\beta T^{3}<0,\end{cases} \tag{24}$$

де $T>0$, завжди. Тоді в (22) стратегія розподілу захисного ресурсу СЗІ є мінімально допустимою $\lambda_{\min}^{opt}$, а стратегія противника $\mu_{\max}^{opt}$ – максимально допустимою, в інформаційному конфлікті (1).

Знайдемо Δ – сідлову точку даної диференціальної гри як [10]

$$\Delta=\left(\frac{\partial^{2} I^{*}(\lambda,\mu)}{\partial\lambda\,\partial\mu}\right)^{2}-\left(\frac{\partial^{2} I^{*}(\lambda,\mu)}{\partial\lambda^{2}}\right)\left(\frac{\partial^{2} I^{*}(\lambda,\mu)}{\partial\mu^{2}}\right)\approx\frac{1}{64}\beta^{2}T^{6}-\left(\frac{1}{3}T^{2}+2\right)\left(-\frac{1}{12}\beta T^{3}\right)>0. \tag{25}$$

Існування в грі сідлової точки (25) свідчить про правильність твердження щодо оптимальності стратегій $\lambda_{\min}^{opt}$ та $\mu_{\max}^{opt}$.

Відновлення оригіналу $P_{7}(t)$ за спектральною Р-моделлю (12) по її дискретах (13)-(16) доцільно провести за схемою нетейлорівських перетворень, де оригінал $P_{7}(t)$ відновлюється у формі деякої апроксимуючої функції $P_{7}(t)=\varphi(t,C)$ з вільними параметрами $C=(C_{0},C_{1},\ldots,C_{n})$ вираженими через відповідні дискрети диференціального спектра $P_{7}(k)$. Доцільність застосування такої схеми обґрунтована більшою точністю нетейлорівських моделей, порівняно з тейлорівськими [8], за умови правильно обраної апроксимуючої функції [10].

У якості апроксимуючої функції доцільно обрати функцію, яка являє собою модель, де оригінал відновлюється у вигляді експоненціальних функцій, що є відрізком ряду Діріхле [11]

$$P_7(t) = A_1 \exp(u_1\, t) + A_2 \exp(u_2\, t). \tag{26}$$

В моделі (26) коефіцієнти A_1, A_2, u_1 та u_2 підлягають визначенню за спектральним рівнянням

$$A_1\, u_1^k + A_2\, u_2^k = \frac{k!\, P_7(k)}{T^k} = P_{7k},\ P_{7k} = \left[\frac{d^k P_7(t)}{dt^k}\right]_{t=0}, \tag{27}$$

яке після підстановки цілочисельного аргументу $k =: 0, 1, 2$ зводиться до системи алгебраїчних рівнянь

$$\begin{array}{|c|c|}\hline 1 & 1 \\ \hline u_1 & u_2 \\ \hline u_1^2 & u_2^2 \\ \hline u_1^3 & u_2^3 \\ \hline \end{array} \quad \begin{array}{|c|}\hline A_1 \\ \hline A_2 \\ \hline \end{array} \quad = \quad \begin{array}{|c|}\hline P_{70}; \\ \hline P_{71}; \\ \hline P_{72}; \\ \hline P_{73}. \\ \hline \end{array} \tag{28}$$

Праві частини в системі (28) знаходяться з рівняння (27), з урахуванням дискрет (13)-(16) спектральної Р-моделі (12), і дорівнюють

$$P_0(0) = [P_7(t_0)]\ = 1, \tag{29}$$

$$P_7(1) = -(\mu + \beta + \gamma), \tag{30}$$

$$P_7(2) = \left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right), \tag{31}$$

$$\begin{aligned} P_7(3) = -\Big((\mu + \beta + \gamma)\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right) + \rho\,\mu\,(2\gamma + 2\beta + \rho + \mu) + \\ + \lambda\,\beta\,(2\mu + 2\gamma + \lambda + \beta) + \varphi\,\gamma\,(2\mu + 2\beta + \varphi + \gamma)\Big)\ . \end{aligned} \tag{32}$$

З урахуванням дискрет (29)-(32) система (28) може бути подана як

$$\begin{aligned} u_1 = -\frac{1}{\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma - u_2^2 A_2\right)}\Big((\mu + \beta + \gamma)\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right) + \\ + \rho\,\mu\,(2\gamma + 2\beta + \rho + \mu)\ \ + \lambda\,\beta\,(2\mu + 2\gamma + \lambda + \beta) + \varphi\,\gamma\,(2\mu + 2\beta + \varphi + \gamma)\Big) - u_2^3 A_2, \end{aligned} \tag{33}$$

$$\begin{aligned} A_1 = \frac{1}{u_1^3}\Big(-\Big((\mu + \beta + \gamma)\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right) + \rho\,\mu\,(2\gamma + 2\beta + \rho + \mu) + \\ + \lambda\,\beta\,(2\mu + 2\gamma + \lambda + \beta) + \varphi\,\gamma\,(2\mu + 2\beta + \varphi + \gamma)\Big) - u_2^3 A_2\Big)\ , \end{aligned} \tag{34}$$

$$u_2 = \frac{-(\mu + \beta + \gamma) - u_1\, A_1}{1 - A_1}, \tag{35}$$

$$A_2 = \frac{-(\mu + \beta + \gamma) - u_1\, A_1}{u_2}. \tag{36}$$

Результат рішення системи вигляду (33)-(36) дозволяє визначити точні аналітичні вирази для невідомих коефіцієнтів u_1, u_2 та A_1, A_2 в апроксимуючій функції (26)

$$\begin{aligned} u_1 = -\frac{1}{\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right)}\Big((\mu + \beta + \gamma)\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right) + \\ + \rho\,\mu\,(2\gamma + 2\beta + \rho + \mu)\ \ + \lambda\,\beta\,(2\mu + 2\gamma + \lambda + \beta) + \varphi\,\gamma\,(2\mu + 2\beta + \varphi + \gamma)\Big), \end{aligned} \tag{37}$$

$$\begin{aligned} A_1 = \left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right)^3 \Big/ \Big(-\Big((\mu + \beta + \gamma)\left((\mu + \beta + \gamma)^2 + \rho\,\mu + \lambda\,\beta + \varphi\,\gamma\right) + \\ + \rho\,\mu\,(2\gamma + 2\beta + \rho + \mu) + \lambda\,\beta\,(2\mu + 2\gamma + \lambda + \beta) + \varphi\,\gamma\,(2\mu + 2\beta + \varphi + \gamma)\Big)^2\Big)\ , \end{aligned} \tag{38}$$

$$
\begin{aligned}
u_2 = &-(\mu+\beta+\gamma)-\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^2\Big/\Big(-\left(\mu+\beta+\gamma\right)\Big(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\\
&+\lambda\,\beta+\varphi\gamma\Big)+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)\Big)\Big/1-\\
&-\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^3\Big/\Big(-\Big(\left(\mu+\beta+\gamma\right)\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)+\\
&+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)^2\Big)\ ,
\end{aligned}
\tag{39}
$$

$$
\begin{aligned}
A_2 = 1&-\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^3\Big/\Big(-\Big(\left(\mu+\beta+\gamma\right)\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)+\\
&+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)^2\Big)\ .
\end{aligned}
\tag{40}
$$

Отже, відновлена за дискретами (29)-(32) нетейлорівської моделі (26) за розрахованими коефіцієнтами (37)-(40) точна аналітична модель, що визначає ймовірність функціонування СЗІ без вразливостей при відсутності спроб НСД $P_7(t)$, визначається як

$$
\begin{aligned}
P_7(t) = &\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^3\Big/\Big(-\Big(\left(\mu+\beta+\gamma\right)\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)+\\
&+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)^2\Big)\ \times\\
&\times\exp\Bigg(-\frac{1}{\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)}\Big(\left(\mu+\beta+\gamma\right)\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)+\\
&+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)\ +\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)t\ \Bigg)+\\
&+\Big(1-\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^3\Big/\Big(-\Big(\left(\mu+\beta+\gamma\right)\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)+\\
&+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)^2\Big)\ \Big)\times\\
&\times\exp\Big(-(\mu+\beta+\gamma)-\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^2\Big/\Big(-\left(\mu+\beta+\gamma\right)\Big(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\\
&+\lambda\,\beta+\varphi\gamma\Big)+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)\Big)\Big/1-\\
&-\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)^3\Big/\Big(-\Big(\left(\mu+\beta+\gamma\right)\left(\left(\mu+\beta+\gamma\right)^2+\rho\,\mu+\lambda\,\beta+\varphi\gamma\right)+\\
&+\rho\,\mu\left(2\gamma+2\beta+\rho+\mu\right)+\lambda\,\beta\left(2\mu+2\gamma+\lambda+\beta\right)+\varphi\gamma\left(2\mu+2\beta+\varphi+\gamma\right)\Big)^2\Big)\ t\Big).
\end{aligned}
\tag{41}
$$

Середній час подолання СЗІ $T_{СЗІ}$ (в термінах теорії надійності напрацювання на відмову [4]) може бути визначений за моделлю зального вигляду

$$
T_{СЗІ} = T\sum_{k=0}^{k=\infty}\left[\left(1\right)^{k+1}-\left(\frac{t_0}{T}\right)^{k+1}\right]\frac{P_7(k)}{k+1}\,. \tag{42}
$$

В окремому частинному випадку, при $t_0 = 0$, модель (42) спрощується та набуває вигляду

$$
T_{СЗІ} = T\sum_{k=0}^{k=\infty}\frac{P_7(k)}{k+1}\,. \tag{43}
$$

Висновки та перспективи подальших досліджень Отже, розроблений в статті диференціально-ігровий метод аналізу надійності СЗІ, на основі їх спектральних Р-моделей складається з наступних кроків:

1. Замовником СЗІ визначається множина станів $\{P_z(t)\}$, в яких може перебувати система під впливом відповідних інтенсивностей β, γ, φ, ρ, λ та μ, де величини двох останніх параметрів – невідомі.
2. На основі визначеної множини $\{P_z(t)\}$ формалізується інформаційний конфлікт в СЗІ (1).
3. Визначаються цілі суб’єкта (противника), що атакує СЗІ (11).

4. Формулюється множина показників надійності, що підлягатимуть визначенню. Наприклад: ймовірність функціонування СЗІ без вразливостей при відсутності спроб НСД $P_7(t)$; плата I^*, що інтерпретується як рівень захищеності СЗІ від спроб НСД; стратегії противника μ і СЗІ λ, які є відповідними інтенсивностями потоків атак та захисних дій; середнього часу подолання СЗІ $T_{СЗІ}$ тощо.

5. Виходячи з (1) складаються спектральні Р-моделі для $P_7(t)$ вигляду (12) та для плати I^* вигляду (17), за якими визначаються стратегії розподілу ресурсів противником μ та системою λ (вирази (22) та (23), відповідно).

6. На основі визначених стратегій визначається плата I^* (17).

7. Складається спектральне рівняння (27) для визначення параметрів нетейлорівської моделі (26).

8. За виразом (42) або (43) визначається середній час подолання СЗІ.

9. Аналізуються отримані оцінки показників надійності на відповідність висунутих замовником вимог. Знаходься шляхи їх оптимізації та процедура аналізу повторюється до тих пір, поки визначені показники не відповідатимуть висунутим замовником вимогам або перевищуватимуть їх.

Таким чином, вперше розроблений диференціально-ігровий метод аналізу надійності СЗІ, на основі їх спектральних Р-моделей відрізняється від відомих можливістю урахування динамічних змін, що вносяться в процедуру аналізу показників надійності систем за рахунок застосування базових положень теорії диференціальних ігор. Застосування методу дозволяє проводити процедуру оцінювання надійності СЗІ, як в реальному, так і прискореному масштабі часу й прогнозувати надійність систем через заданий інтервал часу. Крім того, розроблений метод дозволяє отримувати точні аналітичні моделі для оцінки показників надійності СЗІ, що забезпечується за рахунок аналітичних можливостей операційного методу диференціальних перетворень.

У перспективі передбачається розв’язання модельних прикладів за розробленим методом.

Список літератури

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

2. *Кобозева А. А.* Анализ информационной безопасности / А. А. Кобозева, В. А. Хорошко. – К. : Изд. ГУИКТ, 2009. – 251 с.

3. *Згуровський М. З.* Основи системного аналізу / М. З. Згуровський, Н. Д. Панкратова – К. : Видавнича група BHV, 2007. – 544 с.

4. *Левин Б. Р.* Теория надёжности радиотехнических систем / Б. Р. Левин – М. : Сов. радио, 1978. – 264 с.

5. *Гайворонський М. В.* Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новиков. За заг. ред. академіка НАН України М. З. Згуровського. – К. : Видавнича група BHV, 2009. – 608 с.

6. *Пономарёв А. А.* Решение задачи оценки времени преодоления систем защиты информации / А. А. Пономарёв // Актуальные проблемы безопасности информационных технологий. Сб. материалов Международной научно-практической конференции. – М. : ФГУП, 2008. – С. 81-85.

7. Брахман Т. Р. Многокритериальность и выбор альтернативы в технике / Т. Р. Брахман – М. : Радио и связь, 1984. – 288 с.

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

9. *Грищук Р. В.* Теоретичні основи моделювання процесів нападу на інформацію методами теорії диференціальних ігор / Р. В. Грищук // Збірник наукових праць Донецького ІЗТ УДАЗТ. – Донецьк : ДІЗТ, 2009. – № 19. – С. 43-51.

10. *Васильев В. В.* Моделирование задач оптимизации и дифференциальных игр / В. В. Васильев, В. Л. Баранов – К. : Наукова думка, 1989. – 286 с.

11. *Грищук Р. В.* Нетейлорівська модель процесу нападу на інформацію / Р. В. Грищук // Вісник Східноукраїнського національного університету ім. Володимира Даля. – Луганськ : СНУ ім. В. Даля, 2009. – № 6 (136). – С. 60-64.

Рецензент: Ігнатов В.О.

Надійшла 11.10.2010