УДК 004.9:517.978.2

Р.В. Грищук, к.т.н., Ph.D., н.с.
Житомирський військовий інститут імені С.П. Корольова
Національного авіаційного університету

ВЕРИФІКАЦІЯ І ДОСЛІДЖЕННЯ СПЕКТРАЛЬНИХ *P*- ТА ГІБРИДНИХ *P-L*-МОДЕЛЕЙ ПРОЦЕСУ НАПАДУ НА ІНФОРМАЦІЮ

У статті представлено результати верифікації і дослідження спектральних P- та гібридних P-L-моделей процесу нападу на інформацію. У результаті отримано практичні рекомендації щодо моделювання процесів нападу на інформацію за моделями, що досліджувалися.

Постановка проблеми в загальному вигляді та її зв'язок із важливими практичними завданнями. Починаючи з 1977 року, для моделювання процесів нападу на інформацію в інформаційно-комунікаційних системах (ІКС) широкого використання набули теоретичні моделі безпеки, які досить грунтовно описані в літературі [1]. Концептуальною засадою теоретичних моделей є високий рівень абстрагування процесів, що моделюються. Неможливість отримання за такими моделями гарантованих стратегій розподілу інформаційних ресурсів, що виділяються на захист інформації, значно звужує область їх практичного застосування.

Сучасною вимогою до моделювання процесів нападу на інформацію в ІКС можна вважати потребу відображення в моделях динамічних властивостей інформаційних конфліктів, як у реальному, так і у прискореному часі [2, 3], а дослідження таких моделей є актуальною задачею, що потребує свого розв'язання.

Аналіз останніх досліджень і публікацій. Якість моделювання процесів нападу на інформацію за теоретичними моделями визначається підготовленістю експертів з безпеки, чим визначає значну залежність результатів моделювання від суб'єктивного фактора [4]. Недоліком моделей [1–8] є їх статична природа, що практично виключає можливості вивчення динамічних властивостей процесу інформаційного конфлікту.

У роботі [9] запропоновано розглянути нестаціонарні моделі систем інформаційного забезпечення процесів захисту об'єктів, але застосування відомого K_y-методу дослідження нестаціонарних моделей виключає можливості визначення оптимальних стратегій поведінки сторін інформаційного конфлікту.

В роботах [10–17] автором розроблено теоретичні засади побудови спектральних *P*- і гібридних *P-L*-моделей процесу нападу на інформацію, але не наведено результати їх верифікації та дослідження, що становить значний інтерес з точки зору їх подальшого практичного застосування.

Метою статті є верифікація і дослідження спектральних *P*- та гібридних *P-L*-моделей [10–17], а також розробка практичних рекомендацій, спрямованих на захист інформації, на їх основі.

Викладення основного матеріалу. Спектральні *P*- і гібридні *P-L*-моделі будуються за схемою *P*- та *P-L*-операційних перетворень вихідної динамічної моделі, що описується системою диференціальних рівнянь Колмогорова-Чепмена [10–17]. Перевагою таких моделей, порівняно з відомими, є можливість їх подальших аналітичних досліджень [10–17].

Вихідні дані. Для досліджень оберемо три типи спектральних *P*- і гібридних *P-L*-моделей – найпростішу (*НП*) (рис. 1, *а*), GIGW (рис. 1, *б*) та розгалужену (*РГ*) (рис. 1, *в*). На рис. 1 кружечками позначено стани у яких може перебувати технічний об'єкт (ТО) ІКС під час інформаційного конфлікту з відповідними ймовірностями $P_i(t)$, $i = 0, \ldots, 3$. Стрілками позначено напрямки переходів ТО із одного стану в інший. Над стрілками зазначено інтенсивності потоків інформаційних атак μ, μ_1, μ_2 та захисних дій λ, λ_1 та λ_2, що переводять об'єкт у даний стан, на які накладаються відповідні лінійні обмеження у вигляді нерівностей:

для моделі (рис. 1, *а*)

$$0 \le \lambda \le \lambda_{\max}, \tag{1}$$

$$0 < \mu \le \mu_{\max}, \tag{2}$$

для моделей (рис. 1, *б, в*)

$$0 \le \lambda_1 \le \lambda_{1\max}, \tag{3}$$

$$0 \le \lambda_2 \le \lambda_{2\max}, \tag{4}$$

$$0 < \mu_1 \le \mu_{1\max}, \tag{5}$$

$$0 < \mu_2 \le \mu_{2\max}, \tag{6}$$

де $\lambda_{\max}$, $\lambda_{1\max}$, $\lambda_{2\max}$ і $\mu_{\max}$, $\mu_{1\max}$, $\mu_{2\max}$ – максимальні інтенсивності потоків захисних дій та інформаційних атак відповідно. $P_i(t=0)$ – відповідні початкові умови.

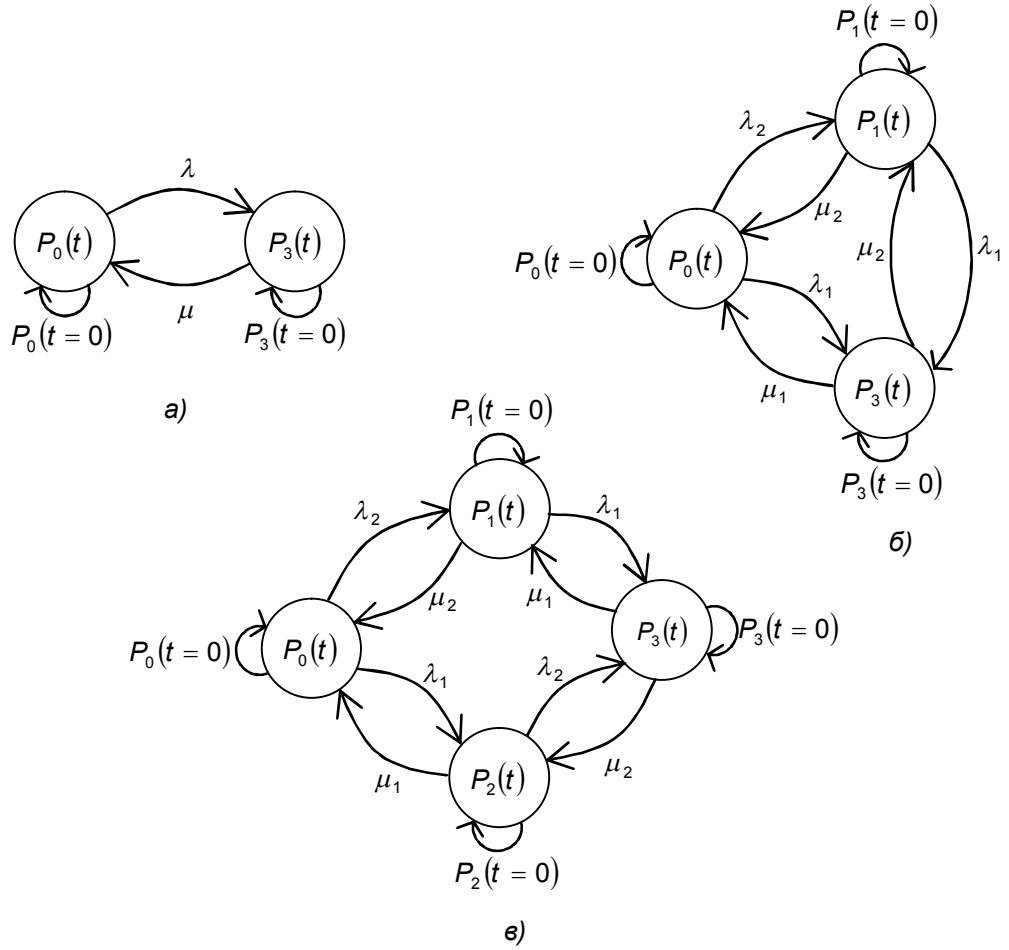


Рис. 1. Графові моделі процесу нападу на інформацію: а) найпростіша; б) GIGW; в) розгалужена

Ймовірності $P_i(t)$ на практиці можуть бути інтерпретовані як: $P_0(t)$ – ймовірність перебування ТО під впливом методів несанкціонованого доступу (НСД); $P_1(t)$ – ймовірність перебування ТО під впливом методів НСД при дії методів захисту інформації (МЗІ); $P_2(t)$ – ймовірність перебування ТО під впливом МЗІ при дії методів НСД; $P_3(t)$ – ймовірність перебування ТО під впливом МЗІ тощо.

Процес нападу на інформацію здійснюється протягом деякого короткого часового інтервалу,

$$[0,\ T]\ , \tag{7}$$

де поточний час $t \in [0,\ T]$.

Математичні моделі. Вважається, що інформаційний конфлікт протікає в умовах антагонізму, а тому може бути формалізований як безкоаліційна диференціальна гра [17]. Застосування методів диференціально-ігрового *P*- та гібридного *P*-*L*-моделювання дозволяє отримати в аналітичній формі вирази, що описують процес нападу на інформацію за графовими моделями (рис. 1, *а*–*в*), а також визначити відповідні їм оптимальні стратегії гравців, що відповідають гарантованим правилам їх поведінки, які до цього були невідомими [10–17].

Для найпростішої моделі (рис. 1, *а*) такі стратегії дорівнюють [10–17]:

$$\lambda_{\max}^{ОПТ} = \mu_{\max}^{ОПТ} = \frac{1}{T}, \tag{8}$$

для GIGW моделі (рис. 1, *б*)

$$\lambda_{1\max}^{ОПТ} = \frac{7}{6T}, \tag{9}$$

$$\lambda_{2\max}^{ОПТ} = 0, \tag{10}$$

$$\mu_{1\max}^{ОПТ} = \frac{2}{3T}, \tag{11}$$

$$\mu_{2\max}^{ОПТ} = \frac{1}{3T}, \tag{12}$$

для розгалуженої моделі (рис. 1, *в*)

$$\lambda_{1\max}^{ОПТ} = \lambda_{2\max}^{ОПТ} = \frac{2}{3T}, \tag{13}$$

$$\mu_{1\max}^{ОПТ} = \mu_{2\max}^{ОПТ} = \frac{1}{3T}. \tag{14}$$

Спектральні *P*-моделі для найпростішої $P_0^{НП}(t)_P$ (рис. 1, *а*), GIGW $P_0^{GIGW}(t)_P$ (рис. 1, *б*) і розгалуженої $P_0^{РГ}(t)_P$ (рис. 1, *в*) моделей мають такий загальний вигляд [10–17]:

$$P_0^{НП}(t)_P = 1 - \lambda t + \frac{1}{2}\lambda(\lambda+\mu)t^2 - \frac{1}{6}\lambda(\lambda+\mu)^2 t^3, \tag{15}$$

$$\begin{aligned} P_0^{GIGW}(t)_P &= 1 - (\lambda_1 + \lambda_2)\, t + \frac{1}{2}\left((\lambda_1+\lambda_2)^2 + \lambda_1\mu_1 + \lambda_2\,\mu_2\right)t^2 - \\ &- \frac{1}{6}\left((\lambda_1+\lambda_2)\left((\lambda_1+\lambda_2)^2 + \lambda_1\,\mu_1 + \lambda_2\,\mu_2\right) + \mu_2\left((\lambda_1+\mu_2)\lambda_2 - \lambda_1\mu_2 + \lambda_2(\lambda_1+\lambda_2)\right) + \right. \\ &\left. + \mu_1\left((\mu_1+\mu_2)\lambda_1 + \lambda_1(\lambda_1+\lambda_2) - \lambda_1\lambda_2\right)\right)t^3, \end{aligned} \tag{16}$$

$$\begin{aligned} P_0^{РГ}(t)_P &= 1 - (\lambda_1 + \lambda_2)\, t + \frac{1}{2}\left((\lambda_1+\lambda_2)^2 + \lambda_1\mu_1 + \lambda_2\,\mu_2\right)t^2 - \\ &- \frac{1}{6}\left((\lambda_1+\lambda_2)\left((\lambda_1+\lambda_2)^2 + \lambda_1\,\mu_1 + \lambda_2\,\mu_2\right) + \lambda_1\mu_1(2\lambda_2 + \lambda_1 + \mu_1) + \right. \\ &\left. + \lambda_2\mu_2(2\lambda_1 + \lambda_2 + \mu_2)\right)t^3. \end{aligned} \tag{17}$$

При виборі гравцями відповідних оптимальних стратегій (8)–(14) моделі (15)–(17) визначають відповідні траєкторії диференціальної $P_0^{НП}(t)_P^{ОПТ}$, $P_0^{GIGW}(t)_P^{ОПТ}$ та $P_0^{РГ}(t)_P^{ОПТ}$ [10–17]:

$$P_0^{НП}(t)_P^{ОПТ} = 1 - \frac{t}{T} + \left(\frac{t}{T}\right)^2 - \frac{2}{3}\left(\frac{t}{T}\right)^3, \tag{18}$$

$$P_0^{GIGW}(t)_P = 1 - \frac{7}{6}\frac{t}{T} + \frac{77}{72}\left(\frac{t}{T}\right)^2 - \frac{875}{1296}\left(\frac{t}{T}\right)^3, \tag{19}$$

$$P_0^{РГ}(t)_P^{ОПТ} = 1 - \frac{4}{3}\frac{t}{T} + \frac{10}{9}\left(\frac{t}{T}\right)^2 - \frac{2}{3}\left(\frac{t}{T}\right)^3. \tag{20}$$

Гібридні *P-L*-моделі $P_0^{НП}(t)_P^L$, $P_0^{GIGW}(t)_P^L$, $P_0^{РГ}(t)_P^L$ в аналітичній формі для графових моделей (рис. 1, *а–в*) мають таке подання [10–17]:

$$P_0^{НП}(t)_P^L = e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu}\left(1 - e^{-(\lambda+\mu)t}\right), \tag{21}$$

$$\begin{aligned} P_0^{GIGW}(t)_P^L &= \frac{1}{(\lambda_2-\mu_1)(\lambda_1+\mu_1+\mu_2)(\lambda_1+\lambda_2+\mu_2)}\left(-\mu_1\mu_2^2 + (\lambda_1\mu_2 + \lambda_2^2 + \lambda_1\lambda_2 - \lambda_2\mu_1)\times\right. \\ &\times(\lambda_1+\mu_1+\mu_2)e^{-(\lambda_1+\lambda_2+\mu_2)t} + \lambda_1(\mu_2-\mu_1)(\lambda_1+\lambda_2+\mu_2)e^{-(\lambda_1+\mu_1+\mu_2)t} + \lambda_2(\lambda_1\mu_1 + \mu_1\mu_2 + \\ &\left. + \mu_2^2) - \mu_1^2(\lambda_1+\mu_2)\right), \end{aligned} \tag{22}$$

$$P_0^{PГ}(t)_P^L = \frac{1}{(\lambda_1+\mu_1)(\lambda_2+\mu_2)}\left(\left(\lambda_2 e^{-(\lambda_1+\lambda_2+\mu_1+\mu_2)t} + \mu_2 e^{-(\lambda_1+\mu_1)t}\right)\lambda_1 + \right. \\ \left. + \left(\mu_2 + \lambda_2 e^{-(\lambda_2+\mu_2)t}\right)\mu_1\right). \quad (23)$$

З урахуванням (8)–(14) гібридні *P*-*L*-моделі (21)–(23) матимуть вигляд:

$$P_0^{НП}(t)_P^{L\,ОПТ} = \frac{1}{2}\left(1 + e^{-2\frac{t}{T}}\right), \quad (24)$$

$$P_0^{GIGW}(t)_P^{L\,ОПТ} = \frac{40}{117} + \frac{7}{18}e^{-\frac{3}{2}\left(\frac{t}{T}\right)} + \frac{7}{26}e^{-\frac{13}{6}\left(\frac{t}{T}\right)}, \quad (25)$$

$$P_0^{PГ}(t)_P^{L\,ОПТ} = \frac{1}{9} + \frac{4}{9}\left(e^{-\frac{t}{T}} + e^{-2\frac{t}{T}}\right). \quad (26)$$

Верифікація моделей. Достовірність моделей (15)–(26) перевірялась на основі розв'язання модельного прикладу [18] шляхом порівняння результатів моделювання з відомими K_γ та Δt-методами [9, 19] згідно з загальноприйнятою методологією дослідження моделей [20]. В силу збіжності результатів Δt- та K_γ-методів у подальшому, для модельного прикладу, скористаємося Δt-методом, що базується на роботах А.К. Ерланга і А.М. Колмогорова [20–22]. Знаходження ймовірностей $P_i(t)$ за даним методом є простішою ітераційною процедурою, порівняно із K_γ-методом.

Для модельного прикладу проведено порівняння точності досліджуваних моделей y^* (15)–(26) і точного рішення $y^{\Delta t}$ за критерієм δ_l^n [23]:

$$\delta_l^n = \frac{1}{n}\varepsilon_l^{n2}, \quad (27)$$

де l – відповідні точки перетину часової осі t на інтервалі розбиття (3) для моделей, що досліджуються, $l = 1, 2, \ldots n$; ε_l^{n2} – квадрат нев'язки, що розраховується відповідно до виразу:

$$\varepsilon_l^{n2} = \left(y^* - y^{\Delta t}\right)^2. \quad (28)$$

На критерій (27) накладаються обмеження вигляду:

$$0 \le \delta_l^n \le \delta_{\max}, \quad (29)$$

де $\delta_{\max}$ – максимальне значення критерію δ_l^n (27), яке залежить від довжини розрядної сітки вихідних даних r, $\delta_{\max} = 10^{-2r}$ [24]. Застосування критерію δ_l^n (27) виключає випадковий вплив розкиду вихідних параметрів моделей, що є його перевагою над іншими критеріями дослідження точності [23].

Результати верифікації моделей (15)–(17) і (21)–(23) у якісному та кількісному вираженні подано на рис. 2 та у таблиці відповідно.

Аналіз результатів (рис. 2 та табл.) показав, що при фіксованих значеннях інтенсивностей інформаційних потоків (1)–(6):

– спектральні *P*-моделі (15)–(17) збіжні на інтервалі $[0, 0{,}3 \cdot T]$ за критерієм (27) і розбігаються з модельним прикладом, отриманим на основі Δt-методу, на інтервалі $(0{,}3 \cdot T, T]$, оскільки їх значення виходять за межі обмежень (28);

– гібридні *P*-*L*-моделі (21)–(23) є більш точними. Ці моделі збігаються з результатами моделювання за Δt-методом на інтервалі (7), а на інтервалі $[0, 0{,}3 \cdot T]$ зі спектральними *P*- моделями (15)–(17).

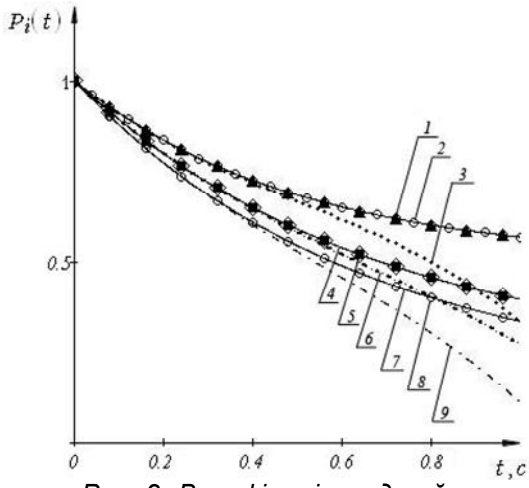


Рис. 2. Верифікація моделей:

1) $\Delta t^{НП}$ *;* *2)* $P_0^{НП}(t)_P^L$; 3) $P_0^{НП}(t)_P$; 4) Δt^{GIGW} ;

5) $P_0^{GIGW}(t)_P^L$; 6) $P_0^{GIGW}(t)_P$; 7) $\Delta t^{РГ}$; 8) $P_0^{РГ}(t)_P^L$; 9) $P_0^{РГ}(t)_P$

Таблиця

Результати верифікації моделей (15)-(26) методом модельних прикладів

Умови		(8)		(9)-(12)		(13), (14)	
Модель		$P_0^{НП}(t)_P$	$P_0^{НП}(t)_P^L$	$P_0^{GIGW}(t)_P$	$P_0^{GIGW}(t)_P^L$	$P_0^{РГ}(t)_P$	$P_0^{РГ}(t)_P^L$
Значення критерію	δ_0^{10}	0	0	0	0	0	0
	δ_1^{10}	$1.027\cdot10^{-10}$	0	$2.536\cdot10^{-11}$	0	$9.180\cdot10^{-11}$	0
	δ_2^{10}	$2.434\cdot10^{-8}$	0	$6.126\cdot10^{-9}$	0	$2.181\cdot10^{-8}$	0
	δ_3^{10}	$5.788\cdot10^{-7}$	0	$1.483\cdot10^{-7}$	0	$5.198\cdot10^{-7}$	0
	δ_4^{10}	$5.375\cdot10^{-6}$	0	$1.401\cdot10^{-6}$	0	$4.837\cdot10^{-6}$	0
	δ_5^{10}	$2.984\cdot10^{-5}$	0	$7.902\cdot10^{-6}$	0	$2.691\cdot10^{-5}$	0
	δ_6^{10}	$1.197\cdot10^{-4}$	0	$3.220\cdot10^{-5}$	0	$1.082\cdot10^{-4}$	0
	δ_7^{10}	$3.840\cdot10^{-4}$	0	$1.048\cdot10^{-4}$	0	$3.477\cdot10^{-4}$	0
	δ_8^{10}	$1.046\cdot10^{-3}$	0	$2.896\cdot10^{-4}$	0	$9.493\cdot10^{-4}$	0
	δ_9^{10}	$2.517\cdot10^{-3}$	0	$7.063\cdot10^{-4}$	0	$2.288\cdot10^{-3}$	0
	δ_{10}^{10}	$5.491\cdot10^{-3}$	0	$1.561\cdot10^{-3}$	0	$5.002\cdot10^{-3}$	0
$\delta_{\max}$		$1\cdot10^{-6}$					

Достовірність результатів моделювання підтверджена, оскільки моделі (15)–(26) на визначених інтервалах працюють з необхідною і достатньою точністю, чим обґрунтовується адекватність моделей реальним процесам нападу на інформацію.

Дослідження моделей. Динаміку протікання процесу нападу на інформацію на ТО в ІКС під час інформаційного конфлікту $0 \le t \le T$ $(T = 1)$ досліджено за наступної варіації набору вхідних даних (1)–(6).

Моделі (15), (21) за умов (2) при:

$$\lambda_{\max}^{ОПТ} = \frac{1}{T}, \tag{30}$$

$$\lambda = \frac{1}{2T}, \tag{31}$$

$$\lambda = 0.01; \tag{32}$$

моделі (16), (22) за умов (10)–(12) при:

$$\lambda_{1\max}^{ОПТ} = \frac{7}{6T}, \tag{33}$$

$$\lambda_1 = \frac{7}{12T}, \tag{34}$$

$$\lambda_1 = \frac{7}{36T}; \tag{35}$$

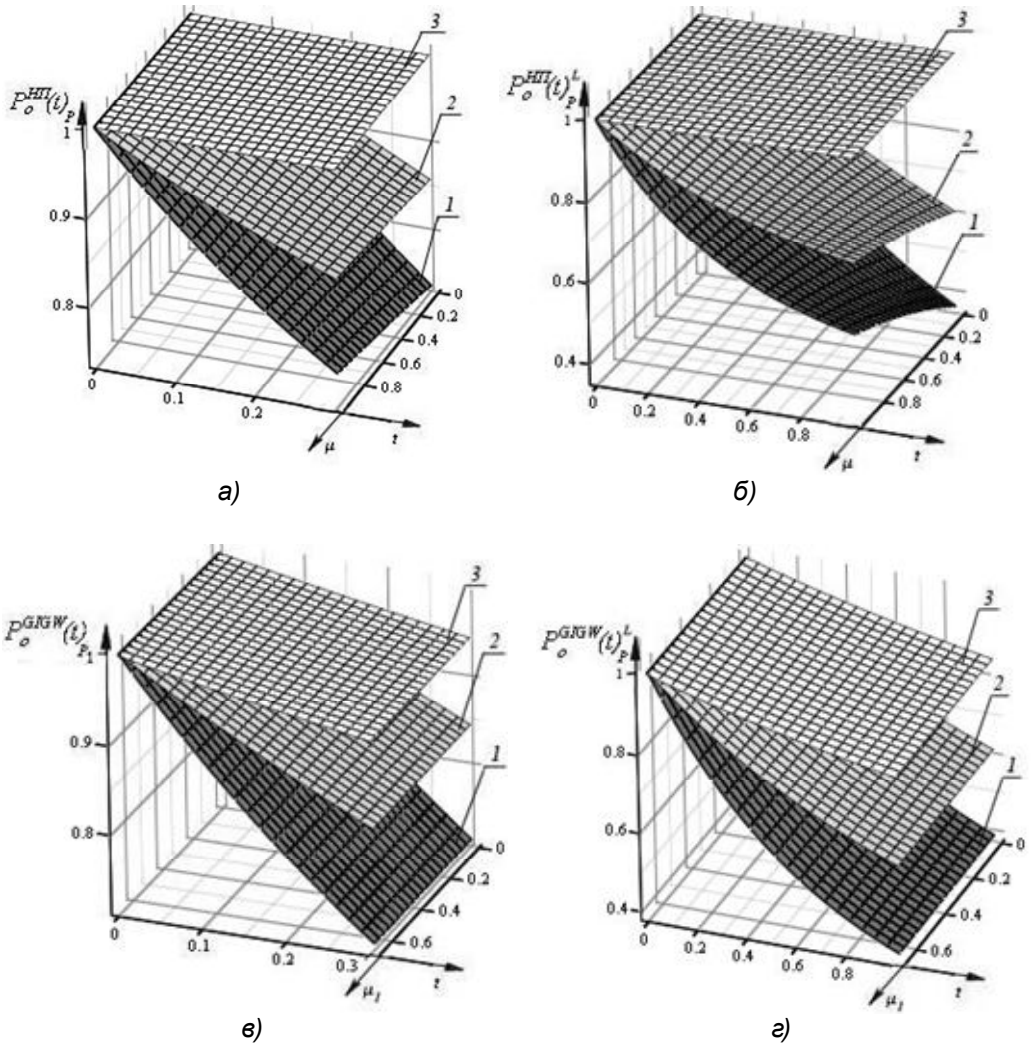
моделі (17), (23) за умов (13), (14) при :

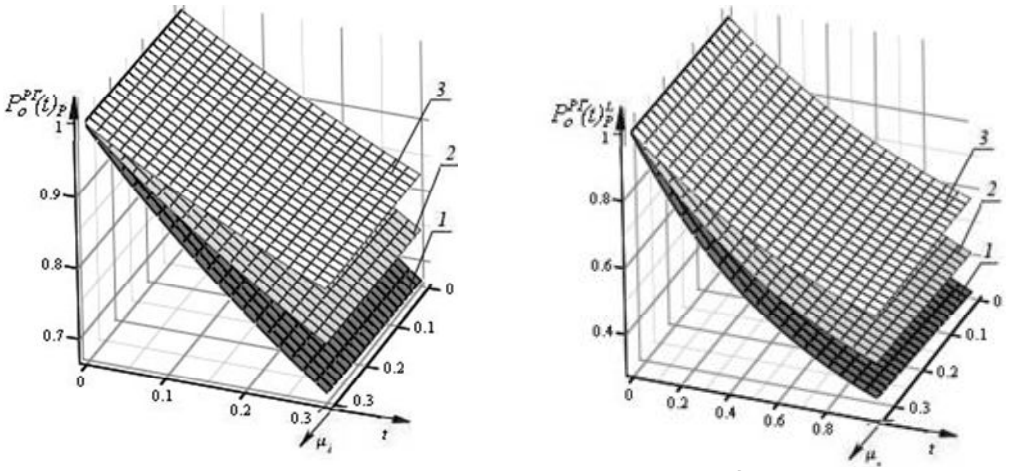
$$\lambda_{1\max}^{ОПТ} = \frac{2}{3T}, \tag{36}$$

$$\lambda_1 = \frac{2}{6T}, \tag{37}$$

$$\lambda_1 = 0.01. \tag{38}$$

Результати досліджень спектральних *P*- (15)–(20) та гібридних *PL*-моделей (21)–(26) подано на рис. 3.





г) *д)*

Рис. 3. Дослідження динаміки протікання процесу нападу на інформацію:
а) $P_0^{НП}(t)_P$; *б)* $P_0^{НП}(t)_P^L$; *в)* $P_0^{GIGW}(t)_P$; *г)* $P_0^{GIGW}(t)_P^L$; *ґ)* $P_0^{РГ}(t)_P$; *д)* $P_0^{РГ}(t)_P^L$

Цифрами 1, 2 та 3 на рис. 3 *а–д* позначено ймовірності перебування ТО під впливом методів НСД при виборі гравцями:

1) оптимальних стратегій (8)–(14), для моделей (15), (21);
2) стратегій (31), (34) та (37), для моделей (16), (22);
3) стратегій (32), (35) та (38) для моделей (17), (23).

Аналіз результатів дослідження моделей (15)–(26) (рис. 3, *а–д*) показав, що за мінімального відхилення стратегій гравців (1)–(6) від оптимальних (8)–(14) на інтервалі (7) неминуче підвищується ймовірність перебування ТО під впливом методів НСД.

Практичні рекомендації.

1. Спектральні *P*- (15)–(20) та гібридні *PL*-моделі (21)–(26) є адекватними моделями процесу нападу на інформацію, тому їх доцільно застосовувати для моделювання динаміки поведінки ТО в умовах інформаційного конфлікту в ІКС.

2. Застосування спектральних *P*- (15)–(20) та гібридних *PL*-моделей (21)–(26) визначається множиною станів, у яких може перебувати об'єкт, а також тривалістю НСД до інформації. При реалізації швидкоплинних процесів нападу на інформацію в межах $[0,\ 0{,}3 \cdot T]$ доцільно застосовувати спектральні *P*-моделі (15)–(20). Поза визначеним інтервалом – гібридні *PL*-моделі (21)–(26).

Висновки. Верифікацію і дослідження спектральних *P*- (15)–(20) та гібридних *PL*-моделей (21)–(26) процесу нападу на інформацію проведено із дотриманням загальних правил, що висуваються до перевірки достовірності й правильності моделей. Збіжність результатів моделювання за досліджуваними моделями і модельним прикладом свідчить про відповідність і коректність використання спектральних *P*- та гібридних *PL*-моделей для моделювання процесів нападу на інформацію. Численні експериментальні контрольні прогони моделей (15)–(26) показали їх стійкість до зміни вхідних даних, чим підтверджується правильність їх роботи. Урахування в спектральних *P*- моделях наступних дискрет (старше 4), дозволяє отримувати моделі більш точні, ніж (15)–(20). При збільшенні кількості дискрет до 18 спектральні *P*- моделі (15)–(20) абсолютно збіжні з гібридними *PL*-моделями (21)–(26). Збільшення кількості числа дискрет не завжди сприяє спрощенню загального вигляду моделей (15)–(20) і призводить до ускладнення математичних розрахунків.

Напрямом подальших досліджень є використанням на практиці досліджених моделей для моделювання реальних процесів нападу на інформацію.

ЛІТЕРАТУРА:

1. *Бабак В.П.* Теоретичні основи захисту інформації: Підручник. – К. : Книжкове вид-во НАУ, 2008. – 752 с.
2. *Ігнатов В.О.* Динаміка інформаційних конфліктів в інтелектуальних системах // Проблеми інформатизації та управління. – Вип. 15. – К.: НАУ, 2005. – С. 88–92.
3. *Поповский В.В.* Защита информации в телекоммуникационных системах: Учебник. – Том 1. – Харьков: ООО "Компания СМИТ", 2006. – 238 с.
4. *Мельников В.В.* Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
5. *Браіловський М.М.* Кількісно-якісна оцінка рівня інформаційної безпеки // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2006. – № 9 (103). – Ч. 1. – С. 14–17.

6. *Андреев В.И., Козлов В.С., Хорошко В.А.* Количественная оценка защищённости технических объектов с учётом их функционирования / Захист інформації. – 2004. – К.: НАУ. – № 2. – С. 47–50.
7. *Козлов В.С.* Количественная оценка защищённости информации / В.С. Козлов, В.А. Хорошко // Захист інформації. – 2003. – К.: НАУ. – № 4. – С. 67–73.
8. *Козлова К.В.* Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) / К.В. Козлова, В.О. Хорошко // Захист інформації. – 2007. – К.: ДІТС. – № 1. – С. 30–32.
9. *Пархуць Л.Т., Хорошко В.А.* Нестационарные модели систем информационного обеспечения процессов защиты объектов / Защита информации. – Спеціальний випуск. – 2008. – К.: НАУ. – С. 225–227.
10. *Грищук Р.В.* Кількісна оцінка рівня захищеності радіоелектронного об'єкта в складній динамічній системі під час інформаційного конфлікту // Управління розвитком: Зб. наук. пр. – № 6. – Харків: ХНЕУ, 2008. – С. 57–59.
11. *Грищук Р.В.* Кількісна оцінка рівня захищеності об'єктів електронно-обчислювальної техніки з урахуванням їх функціонування в умовах інформаційного конфлікту // Вісник ЖДТУ: Зб. наук. пр. – 2008. – Житомир: ЖДТУ. – № 46 (ІІІ). – С. 113–120.
12. *Грищук Р.В.* Диференціально-ігрова модель кількісної оцінки захищеності технічних об'єктів // Захист інформації: Зб. наук. пр. – № 40 (спец. випуск). – 2008. – С. 24–29.
13. *Грищук Р.В.* Диференціально-тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу // Захист інформації: Зб. наук. пр. – 2009. – № 1 (42). – С. 19–27.
14. *Грищук Р.В.* Спектральна модель процесу нападу на інформацію // Захист інформації: Зб. наук. пр. – 2009. – № 2 (42). – С. 71–81.
15. *Грищук Р.В.* Оцінка захищеності технічних об'єктів: постановка задачі // IV Міжнародна науково-технічна конференція "Сучасні інформаційно-комунікаційні технології": Збірник тез. – 2008. – С. 136–137.
16. *Грищук Р.В.* Методологічні основи кількісного оцінювання рівня захищеності технічних об'єктів // 3-й Международный радиоэлектронный форум "Прикладная радиоэлектроника. Состояние и перспективы развития" МРФ-2008: Сб. наук. тр.; Международная конференция "Информационные компьютерные технологии и системы".– Харьков: АНПРЭ, ХНУРЕ, 2008. – С. 245–248.
17. *Грищук Р.В.* Вибір оптимальної стратегії захисту радіоелектронного об'єкта від методів несанкціонованого доступу // Зб. тез. – 2008. – Житомир. – С. 24.
18. *Засядько А.А.* Решение задачи восстановления методом модельных примеров при лазерном масс-спектрометрическом анализе / А.А. Засядько, С.Б. Краюшкин, Г.Н. Дубровская // Электронное моделирование. – Т. 22 (№ 5). – 2000. – С. 31–39.
19. *Кёнинг Д.* Методы теории массового обслуживания / Д.Кёнинг, Д.Штойян. – М.: Радио и связь, 1981. – 128 с.
20. *Томашевський В.М.* Моделювання систем / За ред. академ. НАН України М.З. Згуровського. – К.: Видавнича група BHV, 2005. – 352 с.
21. *Гнеденко Б.В.* Введение в теорию массового обслуживания / Б.В. Гнеденко, И.Н. Коваленко. – М.: Наука, 1987. – 336 с.
22. *Клейнрок Л.* Теория массового обслуживания: Пер. с англ. / И.И. Пер. Грушко; ред. В.И. Нейман. – М.: Машиностроение, 1979. – 432 с.
23. *Balci O.* Verification, validation and accreditation of simulation models // Proceedings of the 29th conference on Winter simulation. – N.Y.: ACM Press, 1997. – P. 135–141.
24. *Засядько А.А.* Методи розв'язання некоректних задач на основі багатокритеріальної оптимізації і диференціально-тейлорівських перетворень для автоматизованих систем управління: Автореф. дис. док. техн. наук. – Київ, 2006. – 30 с.

ГРИЩУК Руслан Валентинович – кандидат технічних наук, Ph.D., науковий співробітник наукового центру Житомирського військового інституту імені С.П. Корольова Національного авіаційного університету.

Наукові інтереси:

– моделювання процесів нападу та захисту інформації.

Подано 04.03.2009

Грищук Р.В. Верифікація і дослідження спектральних Р- та гібридних Р-L-моделей процесу нападу на інформацію
Грищук Р.В. Верификация и исследование спектральных Р- и гибридных Р-L-моделей процесса нападения на информацию
Gryschuk R.V. Verification and research P- spectral and hybrid P-L – model of attack process on the information

УДК 004.9:517.978.2

Верификация и исследование спектральных Р- и гибридных Р-L-моделей процесса нападения на информацию / Р.В. Грищук

В работе представлено результаты верификации и исследования спектральных Р- и гибридных Р-L-моделей процесса нападения на информацию. В результате получено практические рекомендации для моделирования процессов нападения на информацию.

УДК 004.9:517.978.2

Verification and research P- spectral and hybrid P-L – model of attack process on the information / R.V. Gryschuk

The given work present results verification and research P- spectral and hybrid P-L – model of attack process on the information. Practical recommendation to research the dynamic properties of attack process on the information during the information conflict in the information–communication system is given.