УДК 004.9:517.978.2 **Грищук Р. В. (ЖВІРЕ НАУ)**

ДИФЕРЕНЦІАЛЬНО-ІГРОВА МОДЕЛЬ ГАРАНТОВАНО ЗАХИЩЕНОЇ РОЗПОДІЛЕНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Вперше представлено ідею розробки диференціально-ігрової моделі розподіленої системи захисту інформації. Диференціально-ігрова модель, на відміну від відомих, дозволяє гарантувати захищеність інформації від розподілених атак на об’єктах критичної інфраструктури, що функціонують за технологією відкритих систем за моделлю OSI.

Постановка проблеми в загальному вигляді та її зв'язок з важливими практичними завданнями. Підвищення рівня захищеності інформації в розподілених системах є однією з ключових проблем безпеки відкритих систем [1]. На сьогоднішній день дана проблема вирішується шляхом застосування заходів і засобів захисту, що суттєво дозволяє підвищити рівень захищеності інформації. Поряд з тим невирішеною залишається проблема забезпечення гарантованої захищеності інформації у відкритих системах.

Аналіз останніх досліджень і публікацій. Відомо [1, 2], що реалізація заходів захисту передбачає розроблення політики безпеки інформації в інформаційно-телекомунікаційній системі, яка дозволяє захистити розподілену систему від атак. Основними з таких заходів є міжмережне екранування та виявлення вразливостей і атак.

Заходи міжмережного екранування передбачають використання міжмережних екранів (брандмауерів), що захищають внутрішні ресурси системи від атак шляхом шлюзування потоків трафіку між її елементами. Незважаючи на ефективність міжмережних екранів [], їх використання в класичній конфігурації не дозволяє гарантувати безпеку розподіленої системи та захищеність інформації в ній.

Відомі рішення на основі систем виявлення атак (СВА) реалізують базові принципи захисту розподіленої системи [1–3]. Але для гарантування захищеності інформації в розподіленій системі, в якій застосовано як засіб захисту СВА потрібно доопрацьовувати шаблони її поведінки, які мають різні профілі для різних систем.

Перспективним підходом до організації захисту інформації від розподілених атак є побудова розподілених систем захисту інформації (РСЗІ). Даному напряму присвячено публікації [4, 5] та інших авторів. В цих працях зазначено необхідність розробки РСЗІ, але не запропоновано та не розроблено підходи до гарантування захищеності інформації в таких системах. Тому актуальною на сьогоднішній день задачею є розробка гарантовано захищених РСЗІ.

Метою статті є підвищення рівня захищеності інформації у розподілених системах, шляхом розробки диференціально-ігрової моделі гарантовано захищеної РСЗІ.

Викладення основного змісту дослідження. Для досягнення поставленої мети застосуємо декомпозиційний підхід. Декомпозиція вихідної задачі дозволить звести алгоритмічно нерозв’язну проблему побудови гарантовано захищеної РСЗІ до двох тривіальних задач – задачі розробки політики безпеки, як заходу захисту та задачі розробки системи захисту інформації, як засобу яка цю політику гарантовано підтримує.

В рамках подальшого розвитку досліджень автора [6] є можливість синтезу гарантовано захищених РСЗІ шляхом розробки їх диференціально-ігрових моделей. Тому спираючись на дослідження [6] розробимо відповідну політику безпеки.

Розробка диференціально-ігрової політики безпеки: формалізація задачі. Вихідні дані, припущення та обмеження. При розробці диференціально-ігрової моделі гарантовано захищеної РСЗІ за основу взято ідею протидії розподіленим атакам на об’єкт критичної інфраструктури (ОКІ) шляхом залучення інформаційних ресурсів захисту не тільки об’єкта, що піддається атаці, а й захисних інформаційних ресурсів лояльних партнерів – гравців захисту.

Виходячи з теореми про захищеність інформації [7] суть диференціально-ігрової політики безпеки полягає в зменшенні потужності атаки на ОКІ шляхом розосередження її інтенсивності між відповідними гравцями захисту та залученні захисних інформаційних ресурсів цих гравців для забезпечення гарантованого рівня захищеності інформації I^*.

Покажемо це на прикладі трьох об'єктів ОБ 1, ОБ 2, ОБ 3, що функціонують за технологією відкритих систем за моделлю *OSI*, серед яких перший об'єкт ОБ 1 є об'єктом критичної інфраструктури, що піддається розподіленій атаці (наприклад DDoS- атаці на відмову). На рис. 1 графом подано моделі процесів нападу на інформацію в цих системах.

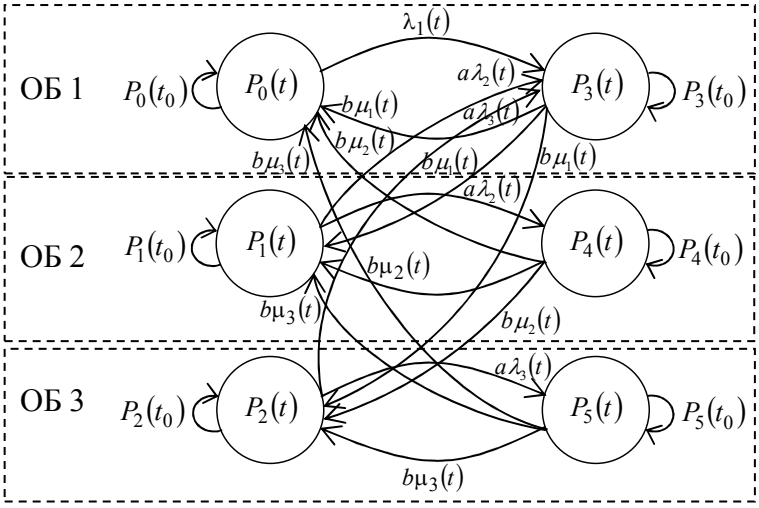

Рис. 1. Графова модель процесу нападу на інформацію в РСЗІ

На рис. 1 прийнято такі позначення: ОБ 1 – перший об'єкт захисту (перший гравець, що захищає ОКІ); ОБ 2, ОБ 3 – 2-й та 3-й об'єкти захисту відповідно. Усі об'єкти на рис. 1 виокремлено штрихпунктирними лініями. Кружками позначено можливі стани системи. Над стрілками переходів проставлено відповідні інтенсивності потоків, які переводять систему в даний стан. $P_z(t_0)$ - нульові початкові умови при перебуванні системи в z - му стані ($z = \overline{0,5}$), де t_0 - час початку гри. $\lambda_i(t)$ - інтенсивність потоку захисних дій при переведенні системи в z - й стан, $i = \overline{0,3}$; $\mu_j(t)$ - інтенсивність потоку інформаційних атак при переведенні системи в z - й стан, $j = \overline{0,3}$. В термінах теорії диференціальних ігор $\lambda_i(t)$ та $\mu_j(t)$ – це стратегії гравців [8]. Стратегії гравців $\lambda_i(t)$ та $\mu_j(t)$, що визначають правила розподілу їх інформаційних ресурсів, належать замкненим множинам $\Lambda \in E_\lambda$ та $\mathrm{M} \in E_\mu$, які обмежені в евклідових просторах R_λ і R_μ. Тривалість диференціальної гри T обирається рівною тривалості інформаційного конфлікту, що визначається тривалістю інформаційних атак на систему, де $t \in [t_0, T]$. Гравцем ОБ 1, що захищається вжито організаційні, технічні, криптографічні та програмні методи захисту інформації.

Виходячи з диференціально-ігрової політики безпеки в РСЗІ вагові коефіцієнти a обирають виходячи з стратегії половинного захисту свого об'єкта та підтримки захисту ОКІ – ОБ 1 і визначають як $a = 1/2$. В основу вибору вагових коефіцієнтів b покладено стратегію розподілу інтенсивності атаки гравців, що атакують рівномірно між усіма гравцями, які захищаються. Вагові коефіцієнти b визначають як $b = 1/3$.

Розподілена атака на ОКІ, що здійснюється декількома гравцями призводить до поступової втрати мережевим трафіком самоподібної структури. У результаті цього не всі моделі потоків пакетів заявок можуть бути описані моделями найпростіших потоків. Тому передбачається, що інтенсивності потоків захисних дій $\lambda_i(t)$ та інформаційних атак $\mu_j(t)$, для гравців які задіяні в інформаційному конфлікті описуються моделями загального вигляду:

– для гравців, що захищаються

$$\lambda_1(t) = \lambda, \tag{1}$$

$$\lambda_2(t) = \lambda t, \tag{2}$$

$$\lambda_3(t) = e^{\lambda t} \tag{3}$$

при обмеженнях

$$\lambda_{\min} \le \lambda_i(t) \le \lambda_{\max}; \tag{4}$$

– для гравців, що атакують (реалізують процес нападу на інформацію)

$$\mu_1(t) = \mu, \tag{5}$$

$$\mu_2(t) = \mu t, \tag{6}$$

$$\mu_3(t) = e^{\mu t} \tag{7}$$

при обмеженнях

$$\mu_{\min} \le \mu_j(t) \le \mu_{\max} \tag{8}$$

відповідно, де λ та μ – параметри законів розподілу стратегій i-го та j-го гравців, які невідомі; $\lambda_{\min}$ і $\mu_{\min}$ – мінімальні, а $\lambda_{\max}$ і $\mu_{\max}$ – максимальні інтенсивності потоків захисних дій та інформаційних атак i-го та j-го гравців.

Розробка диференціально-ігрової моделі гарантовано захищеної РСЗІ.

Аналіз диференціально-ігрової політики безпеки, сформульованої вище, дозволяє формалізувати інформаційний конфлікт в РСЗІ при протіканні процесу нападу на інформацію під час розподіленої атаки у вигляді системи диференціальних рівнянь Колмогорова-Чепмена

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -\lambda_1(t)P_0(t) + b\,\mu_1(t)P_3(t) + b\,\mu_2(t)P_4(t) + b\,\mu_3(t)P_5(t); \\ \dfrac{dP_1(t)}{dt} = -2a\,\lambda_2(t)P_1(t) + b\,\mu_1(t)P_3(t) + b\,\mu_2(t)P_4(t) + b\,\mu_3(t)P_5(t); \\ \dfrac{dP_2(t)}{dt} = -2a\,\lambda_3(t)P_2(t) + b\,\mu_1(t)P_3(t) + b\,\mu_2(t)P_4(t) + b\,\mu_3(t)P_5(t); \\ \dfrac{dP_3(t)}{dt} = -3b\,\mu_1(t)P_3(t) + \lambda_1(t)P_0(t) + a\,\lambda_2(t)P_1(t) + a\,\lambda_3(t)P_2(t); \\ \dfrac{dP_4(t)}{dt} = -3b\,\mu_2(t)P_4(t) + a\lambda_2(t)P_1(t); \\ \dfrac{dP_5(t)}{dt} = -3b\,\mu_3(t)P_5(t) + a\,\lambda_3(t)P_2(t). \end{cases} \tag{9}$$

Система (9) справедлива за наступних початкових умов $P_0(t_0) = 1$, $P_2(t_0) = \text{K} = P_5(t_0) = 0$ та умов нормування $P_0(t_0) + \text{K} + P_5(t_0) = 1$ при відповідних обмеженнях (4) та (8) на ресурси гравців (1)–(3) та (5)–(7) відповідно.

Плата I, що є критерієм оптимізації, може бути подана як модель інтегральної оптимальності

$$I = \frac{1}{T}\int_{t_0}^{T} P_0(t)\,dt\,. \tag{10}$$

Для гарантування захищеності інформації в РСЗІ гравці захисту обирають свої стратегії відповідно до принципу мінімаксу [8]. Тобто стратегії $\lambda_i(t)$, що обираються гравцями захисту мінімізують плату (10), за умови її максимізації гравцями нападу

$$\min_{\lambda_i(t)\in E_\lambda}\ \max_{\mu_j(t)\in E_\mu} = I\,. \tag{11}$$

Гравці нападу обирають стратегії $\mu_j(t)$, що максимізують плату при умові мінімізації плати гравцями захисту

$$\max_{\mu_j(t)\in E_\mu}\ \min_{\lambda_i(t)\in E_\lambda} = I\,. \tag{12}$$

При виконанні умови

$$\min_{\lambda_i(t)\in E_\lambda}\ \max_{\mu_j(t)\in E_\mu} = \max_{\mu_j(t)\in E_\mu}\ \min_{\lambda_i(t)\in E_\lambda} = I^* \tag{13}$$

стратегії гравців є оптимальними $\lambda_i(t)\Rightarrow\lambda_i^{opt}(t)$ і $\mu_j(t)\Rightarrow\mu_j^{opt}(t)$, а в диференціальній грі існує сідлова точка. Основною властивістю сідлової точки є нераціональність відхилення гравцями від своїх оптимальних стратегій, оскільки кожен з них неминуче програє в платі (2). Дотримання гравцями захисту оптимальних стратегій гарантує захищеність інформації в РСЗІ не гірше I^*. Плата I^* називається ціною гри, а шукана траєкторія $P_0^{opt}(t)$, що описує процес нападу на інформацію при розподіленій атаці на ОКІ є оптимальною.

Для визначення стратегій гравців $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$, що забезпечують дотримання диференціально-ігрової політики безпеки застосуємо операційний метод диференціальних перетворень академіка НАН України Г. Є. Пухова [9]. Відповідно до [9] перейдемо від моделі (9) в області оригіналів до її спектральної моделі в області зображень, врахувавши: по-перше що масштабна стала в диференціальних перетвореннях H дорівнює тривалості інформаційного конфлікту T, тобто $H = T$; по-друге зображення для стратегій (1)–(3) та (5)–(7) відповідно, мають вигляд

$$\lambda_1(k) = \lambda\,\text{ъ}(k) = \begin{cases}\lambda, & k=0;\\ 0, & k\ge 1,\end{cases}\quad \lambda_2(k) = \lambda T\,\text{ъ}(k-1) = \begin{cases}\lambda T, & k=1;\\ 0, & k\ne 1,\end{cases}\quad \lambda_3(k) = \frac{(\lambda T)^k}{k!}\,, \tag{14}$$

$$\mu_1(k) = \mu\,\text{ъ}(k) = \begin{cases}\mu, & k=0;\\ 0, & k\ge 1,\end{cases}\quad \mu_2(k) = \mu T\,\text{ъ}(k-1) = \begin{cases}\mu T, & k=1;\\ 0, & k\ne 1,\end{cases}\quad \mu_3(k) = \frac{(\mu T)^k}{k!}\,, \tag{15}$$

де $\text{ъ}(k)$ - теда. У результаті отримаємо систему спектральних рівнянь

$$\begin{cases} P_0(k+1)=\dfrac{T}{k+1}\left[-\lambda P_0(k)+\dfrac{1}{3}\mu P_3(k)+\dfrac{1}{3}\mu T P_4(k-1)+\dfrac{1}{3}\sum\limits_{l=0}^{k}\dfrac{(\mu T)^{k-l}}{(k-l)!}P_5(l)\right]; \\ P_1(k+1)=\dfrac{T}{k+1}\left[-\lambda T P_1(k-1)+\dfrac{1}{3}\mu P_3(k)+\dfrac{1}{3}\mu T P_4(k-1)+\dfrac{1}{3}\sum\limits_{l=0}^{k}\dfrac{(\mu T)^{k-l}}{(k-l)!}P_5(l)\right]; \\ P_2(k+1)=\dfrac{T}{k+1}\left[-\sum\limits_{l=0}^{k}\dfrac{(\lambda T)^{k-l}}{(k-l)!}P_2(l)+\dfrac{1}{3}\mu P_3(k)+\dfrac{1}{3}\mu T P_4(k-1)+\dfrac{1}{3}\sum\limits_{l=0}^{k}\dfrac{(\mu T)^{k-l}}{(k-l)!}P_5(l)\right]; \\ P_3(k+1)=\dfrac{T}{k+1}\left[-\mu P_3(k)+\lambda P_0(k)+\dfrac{1}{2}\lambda T P_1(k-1)+\dfrac{1}{2}\sum\limits_{l=0}^{k}\dfrac{(\lambda T)^{k-l}}{(k-l)!}P_2(l)\right]; \\ P_4(k+1)=\dfrac{T}{k+1}\left[-\mu T P_4(k-1)+\dfrac{1}{2}\lambda T P_1(k-1)\right]; \\ P_5(k+1)=\dfrac{T}{k+1}\left[-\sum\limits_{l=0}^{k}\dfrac{(\mu T)^{k-l}}{(k-l)!}P_5(l)+\dfrac{1}{2}\sum\limits_{l=0}^{k}\dfrac{(\lambda T)^{k-l}}{(k-l)!}P_2(l)\right], \end{cases} \tag{16}$$

де $\{P_z(k)\}$ - диференціальні спектри для відповідних процесів, що протікають в РСЗІ, k - цілочисловий аргумент, $k =: 0, 1, 2$.

Виходячи з спектральної моделі інформаційного конфлікту (16) дискрети спектральної диференціально-ігрової моделі процесу нападу на інформацію $P_0(k)$ при відповідних значеннях цілочислового аргументу $k =: 0, 1, 2$ дорівнюють

$$P_0(0)=[P_0(t_0)]=1, \tag{17}$$

$$P_0(1)=-\lambda T, \tag{18}$$

$$P_0(2)=\frac{1}{2}\lambda\left(\lambda+\frac{1}{3}\mu\right)T, \tag{19}$$

$$P_0(2)=-\frac{1}{6}\lambda\left(\lambda\left(\lambda+\frac{1}{3}\mu\right)+\frac{1}{3}\mu(\lambda+\mu)\right)T^3. \tag{20}$$

Спектральна модель для плати (10) з урахуванням дискрет (17)–(20) визначатиметься як

$$I=\sum_{k=0}^{k=\infty}\frac{P_0(k)}{k+1}\approx 1-\lambda T+\frac{1}{2}\lambda\left(\lambda+\frac{1}{3}\mu\right)T-\frac{1}{6}\lambda\left(\lambda\left(\lambda+\frac{1}{3}\mu\right)+\frac{1}{3}\mu(\lambda+\mu)\right)T^3. \tag{21}$$

Для знаходження оптимальних стратегій $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$, знайдемо стаціонарні точки для функціонала (21) як

$$\begin{cases} \dfrac{\partial I(\lambda,\mu)}{\partial\lambda}=0; \\ \dfrac{\partial I(\lambda,\mu)}{\partial\mu}=0. \end{cases} \tag{22}$$

Дослідження функціонала (21) на екстремум (22) зводиться до розв'язання системи лінійних алгебраїчних рівнянь вигляду

$$\begin{cases} -\dfrac{1}{2}T+\dfrac{1}{6}\left(\lambda+\dfrac{1}{3}\mu\right)T^2+\dfrac{1}{6}\lambda T^2=0; \\ \dfrac{1}{18}\lambda T^2-\dfrac{1}{36}\lambda(\lambda+\mu)T^3=0, \end{cases} \tag{23}$$

звідки

$$\begin{cases} \lambda^{opt} = \dfrac{7}{5T}; \\ \mu^{opt} = \dfrac{3}{5T}. \end{cases} \tag{24}$$

Виконання достатніх умов

$$\begin{cases} \dfrac{\partial^2 I(\lambda,\mu)}{\partial \lambda^2} > 0; \\ \dfrac{\partial^2 I(\lambda,\mu)}{\partial \mu^2} < 0, \end{cases} \Rightarrow \begin{cases} \dfrac{1}{3}T^2 > 0; \\ -\dfrac{1}{36}\lambda T^3 < 0, \end{cases} \tag{25}$$

дозволяє стверджувати, що параметри законів розподілу (24) стратегій гравців є відповідно

$$\begin{cases} \lambda^{opt}_{\min} = \dfrac{7}{5T}; \\ \mu^{opt}_{\max} = \dfrac{3}{5T}. \end{cases} \tag{26}$$

Виконання необхідних (22) і достатніх (25) умов дозволяє стверджувати, що набір стратегій гравців (1)–(3) та (5)–(7) з параметрами (26) є оптимальним і в даній диференціальній грі існує сідлова точка.

Ціна гри, що визначає гарантований рівень захищеності інформації в РСЗІ (див. рис. 1) з урахуванням (26) дорівнює

$$I^* \approx 0.5193. \tag{27}$$

В часовій області при виборі гравцями оптимальних стратегій диференціально-ігрова модель процесу нападу на інформацію матиме вигляд

$$P_0^{opt}(t) \approx 1 - \frac{7}{5}\frac{t}{T} + \frac{28}{25}\left(\frac{t}{T}\right)^2 - \frac{77}{125}\left(\frac{t}{T}\right)^3. \tag{28}$$

Таким чином, для забезпечення гарантованої захищеності інформації в РСЗІ гравцям потрібно дотримуватися таких стратегій:

– для гравців, що захищаються

$$\lambda_1^{opt}(t) = \frac{7}{5T}, \tag{29}$$

$$\lambda_2^{opt}(t) = \frac{7}{5}\frac{t}{T}, \tag{30}$$

$$\lambda_3^{opt}(t) = e^{\frac{7}{5}\frac{t}{T}}; \tag{31}$$

– для гравців, що атакують

$$\mu_1^{opt}(t) = \frac{3}{5T}, \tag{32}$$

$$\mu_2^{opt}(t) = \frac{3}{5}\frac{t}{T}, \tag{33}$$

$$\mu_3^{opt}(t) = e^{\frac{3}{5}\left(\frac{t}{T}\right)}. \tag{34}$$

Оцінювання ефективності розробленої моделі. Здійснимо порівняння рівнів захищеності інформації, що забезпечують диференціально-ігрові моделі при розподіленій атаці для розробленої моделі (див. рис. 1) та для моделі, що реалізує класичну систему захисту інформації (рис. 2) за однакових початкових умов (1)–(8).

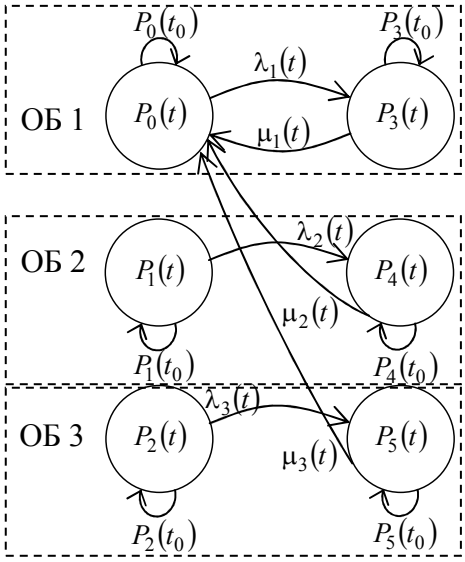

Рис. 2. Графова модель процесу нападу на інформацію в СЗІ

Результати оцінювання наведено в табл. 1.

Таблиця 1

Оцінка ефективності диференціально-ігрової гарантовано захищеної РСЗІ

Тривалість атаки, Т с.	Модель процесу нападу на інформацію	Стратегії, c^{-1}						Рівень захищеності	Ефективність
		гравців нападу			гравців захисту				
1	$P_0^{opt}(t)$	$\mu_1^{opt}(t)$	$\mu_2^{opt}(t)$	$\mu_3^{opt}(t)$	$\lambda_1^{opt}(t)$	$\lambda_2^{opt}(t)$	$\lambda_3^{opt}(t)$	I^*	E, %
	$1-\frac{7}{5}t+\frac{28}{25}t^2-\frac{77}{125}t^3$	$\frac{3}{5}$	$\frac{3}{5}t$	$\exp(\frac{3}{5}t)$	$\frac{7}{5}$	$\frac{7}{5}t$	$\exp(\frac{7}{5}t)$	0.5193	покращено на 22 %
	$1-t+t^2-\frac{2}{3}t^3$	1	t	$\exp(t)$	1	t	$\exp(t)$	0.6667	-

Аналіз результатів оцінювання показує, що застосування розробленої диференціально-ігрової гарантовано захищеної РСЗІ дозволяє на 22% підвищити захищеність інформації на ОКІ під час розподіленої атаки.

Висновки та перспективи подальших досліджень. В результаті проведених досліджень встановлено, що побудова диференціально-ігрових моделей гарантовано

захищених РСЗІ дозволяє підвищувати захищеність об'єктів критичної інфраструктури. Розроблена модель може бути використана для покращення математичного забезпечення діючих та перспективних брандмауерів, реалізація в яких диференціально-ігрової політики безпеки дозволить ефективно здійснювати функцію шлюзування потоків трафіка в розподіленій системі.

Література

1. *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.

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

3. *Поповский В. В.* Защита информации в телекоммуникационных системах : учеб. Т. 1 / В. В. Поповский, А. В. Персиков. – Х. : ООО "Компания СМИТ", 2006. – 238 с.

4. *Милокум Я. В.* Метод конфликтного управления системой распределённой активной защиты от компьютерных угроз / Я. В. Милокум // Системний аналіз та інформаційні технології : XI міжнар. накук.-техн. конф. (Київ, 26-30 трав. 2009 р.). – К. : НАУ, 2009. – С. 525.

5. *Панасенко С. П.* Принципы разработки серверных модулей распределенных систем защиты информации, часть 1 / С. П. Панасенко // Вопросы защиты информации. – 2009. – № 2 – С. 30–34.

6. *Грищук Р. В.* Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.

7. *Грушо А. А.* Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М. : Яхтсмен, 1996. – 187 с.

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

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

Надійшла: 10.03.11

Рецензент: д.т.н., проф. Щербак Л.М.