УДК 004.9:517.978.2

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

НЕПЕРЕРВНА ДИСКРЕТНА ДИФЕРЕНЦІАЛЬНО-ІГРОВА МОДЕЛЬ ПРОЦЕСУ НАПАДУ НА ІНФОРМАЦІЮ

У статті розроблено неперервну дискретну диференціально-ігрову модель процесу нападу на інформацію. Розроблена модель дозволяє підвищувати точність спектральних диференціально-ігрових моделей процесів нападу на інформацію в області оригіналів на значних інтервалах часу.

Постановка проблеми в загальному вигляді та її зв'язок із важливими практичними завданнями. Архіскладність сучасних комп'ютерних систем (КС) та мереж [1, 2] потребує постійного підвищення ефективності комплексних систем захисту інформації (КСЗІ) [3]. З практики відомо [1, 4–8], що підвищення ефективності КСЗІ пов'язано із вирішенням ряду питань які, як правило, мають проблемний характер.

У сучасних умовах інформаційні конфлікти [9, 10] в інформаційно-комунікаційних системах динамічно розвиваються та протікають у повній або частковій невизначеності поведінки противника для системи, що захищається [11]. Тому пошук умов підвищення ефективності КСЗІ за одночасної оптимізації процесу управління захистом інформації в кожному конкретному частинному випадку зокрема та інформаційною безпекою в широкому розумінні є актуальним науково-технічним завданням.

Як один із ефективних шляхів вирішення зазначеної вище проблеми є її декомпозиція на окремі підзадачі менш складного за ієрархією, локального рівня [6]. Отже, визначення цих пізадач, їх формалізація та розв'язання, у рамках досліджуваної проблеми, носить виключно актуальний характер та потребує детального наукового дослідження.

Аналіз останніх досліджень і публікацій. Критичний аналіз останніх досліджень та публікацій [1–5, 7, 8–15] показує, що в умовах невизначеності поведінки противника ефективність КСЗІ може підвищуватися завдяки гарантованості захищеності інформації на значних інтервалах часу. На практиці під таким інтервалом часу слід розуміти тривалість життєвого циклу КС або мережі, протягом якого вона функціонує за заданим цільовим призначенням.

Суттєві недоліки відомих моделей [12–15] значно обмежують отримання кількісних показників захищеності інформації. Так, при побудові моделей [12–15], прийнято припущення про статичну природу протікання інформаційного конфлікту. Оскільки реальні інформаційні конфлікти в КС та мережах протікають у динаміці [9], то адекватність таких моделей викликає сумнів.

Ряд інших відомих моделей [8, 14] не відображає імовірнісну природу протікання інформаційного конфлікту та його теоретико-ігрові властивості, породжені антагоністичною природою цілей суб'єктів інформаційного конфлікту.

У праці автора [16] закладено математичний базис для моделювання процесів нападу на інформацію на основі методів теорії диференціальних ігор та диференціальних перетворень і розроблено відповідні математичні моделі [17–20, 22–24]. Як показано у статті [25], спектральні моделі [17–20] мають відносно низьку точність на значних інтервалах часу, хоча на відміну від відомих моделей [12–15] дозволяють досліджувати процес нападу на інформацію у динаміці. З метою підвищення точності моделей [17–20] в [21] запропоновано застосувати метод гібридного *P-L*-моделювання, а в [24] – нетейлорівські диференціальні перетворення. При нарощуванні складності диференціально-ігрових моделей [17] відповідно підвищується й аналітична складність гібридних *P-L*-моделей [22], а невдалий вибір нетейлорівської моделі недосвідченим дослідником за методом [24] може призвести до помилок при моделюванні.

Отже, як зрозуміло з аналізу літературних джерел [1–25], нагальною залишається потреба підвищення ефективності КСЗІ шляхом розробки нових науково обґрунтованих моделей процесів нападу на інформацію, застосування яких дозволить гарантувати захищеність інформації на значних інтервалах часу та отримувати область кількісних оцінок показників її захищеності.

З цією **метою** в статті розроблено неперервну дискретну диференціально-ігрову модель процесу нападу на інформацію.

Викладення основного матеріалу. Неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію розробляється, виходячи з умов конкретного інформаційного конфлікту, що протікає в системі захисту інформації (СЗІ) окремо взятої КС або мережі.

Вихідні дані, обмеження та припущення. Розглянемо деяку СЗІ, яка піддається впливу методів несанкціонованого доступу (НСД) та методів захисту інформації (МЗІ). Гіпотетично припустимо, що в деякий момент часу t, що належить інтервалу часу, на якому здійснюється моделювання процесу нападу

на інформацію в СЗІ ($t \in [0, T]$), система може перебувати в одному зі станів $P_z(t)$, $z = \overline{0, c}$. Усі стани системи задані зліченною множиною станів системи $\{P_z(t)\}$, у яких вона може перебувати під впливом методів НСД або МЗІ.

Наприклад, якщо $z = 0$, то це означає, що в момент часу t СЗІ перебуває під впливом методів НСД, у результаті чого реалізується процес нападу на інформацію $P_0(t)$, що підлягає моделюванню на значному інтервалі часу $t \in [0, T]$.

Формалізований опис динаміки інформаційного конфлікту в СЗІ подамо системою лінійних диференціальних рівнянь Колмогорова-Чепмена зі змінними параметрами у векторному вигляді

$$\frac{dP_z(t)}{dt} = f\left(t, P_z(t), \lambda_z(t), \mu_z(t)\right), \tag{1}$$

де $P_z(t)$ – вектор, що визначає ймовірності знаходження системи в заданих z-станах;

f – аналітична функція, вигляд якої визначається з умов складання системи рівнянь Колмогорова-Чепмена [26];

$\lambda_z(t)$ – вектор інтенсивностей розподілу інформаційних ресурсів у z-му стані, що виділено системі для захисту інформації;

$\mu_z(t)$ – вектор інтенсивностей розподілу інформаційних ресурсів противника у z-му стані, що виділено ним для здійснення НСД (проведення атак на систему).

Система (1) справедлива за початкових умов

$$P_0(0) = 1,\ P_2(0) = \ldots = P_c(0) = 0 \tag{2}$$

та умов нормування

$$P_0(0) + P_2(0) + \ \ldots \ + P_c(0) = 1. \tag{3}$$

Обмеження на інформаційні ресурси системи та противника, в загальному вигляді задаються як

$$\lambda_{z\,\min} \le \lambda_z \le \lambda_{z\,\max}, \tag{4}$$

$$\mu_{z\,\min} \le \mu_z \le \mu_{z\,\max}, \tag{5}$$

де $\lambda_{z\min}$ і $\mu_{z\min}$ – мінімальні, а $\lambda_{z\max}$ і $\mu_{z\max}$ – максимальні інтенсивності потоків захисних дій та інформаційних атак у z-му стані відповідно.

Формалізація диференціально-ігрового базису та процедура Р-моделювання. У найпростішому випадку (при однокритерійній постановці задачі [17–24]) плата I (функція виграшу), що виступатиме критерієм оптимізації, задається як середня ймовірність перебування СЗІ під впливом методів НСД на визначеному інтервалі, тобто

$$I = \frac{1}{T}\int_0^T P_0(t)\,dt. \tag{6}$$

У подальших викладках суб'єкта інформаційного конфлікту – противника та систему називатимемо відповідно до термінології диференціальних ігор – гравцями [27–29].

Єдиною гарантованою стратегією поведінки гравців в умовах антагонізму є дотримання ними принципу мінімаксу [11, 27–29]. Тобто першому гравцеві, що захищається, доцільно дотримуватися стратегії $\lambda_z(t)$, що мінімізує плату (6)

$$I\left(\lambda_z(t), \mu_z(t)\right) = \min_{\lambda_z(t) \in E_\lambda} \max_{\mu_z(t) \in E_\mu} I, \tag{7}$$

де E_λ, E_μ – замкнені обмежені у евклідових просторах R_λ і R_μ множини, що визначають можливі стратегії гравців. Другому гравцеві (противнику) доцільно дотримуватися стратегії $\mu_z(t)$, що максимізує плату (6), за умови мінімізації плати першим гравцем

$$I\left(\lambda_z(t), \mu_z(t)\right) = \max_{\mu_z(t) \in E_\mu} \min_{\lambda_z(t) \in E_\lambda} I. \tag{8}$$

При виборі гравцями оптимальних стратегій $\lambda_z^{opt}(t)$ і $\mu_z^{opt}(t)$ та виконанні співвідношення

$$I\left(\lambda_z^{opt}(t),\ \mu_z^{opt}(t)\right) = \min_{\lambda_z(t) \in E_\lambda} \max_{\mu_z(t) \in E_\mu} I = \max_{\mu_z(t) \in E_\mu} \min_{\lambda_z(t) \in E_\lambda} I = I^* \tag{9}$$

існує сідлова точка гри [28], що свідчить про недоцільність відхилення гравцями від оптимальних стратегій, тобто

$$I\left(\lambda_z(t),\ \mu_z^{opt}(t)\right) \ge \min_{\lambda_z(t) \in E_\lambda} I\left(\lambda_z(t),\ \mu_z^{opt}(t)\right), \tag{10}$$

$$I\left(\lambda_z^{opt}(t),\ \mu_z(t)\right) \ \le \ \max_{\mu_z(t)\ \in E_\mu} \ I\left(\lambda_z^{opt}(t),\ \mu_z(t)\right). \tag{11}$$

Як видно з нерівностей (10) та (11), будь-яке відхилення від оптимальної стратегії одним із гравців призводить до втрат в платі, при умові вибору оптимальної стратегії іншим гравцем. Величина I^*, вираз (9), в диференціальних іграх називається ціною гри.

Процедура *P*-моделювання зводиться розв'язання диференціальної гри (1)–(11) [23] операційним методом диференціальних перетворень, який ґрунтовно описано в [30–32].

Застосування диференціальних перетворень [30–32] до системи (1) дозволяє подати її системою спектральних рівнянь векторного вигляду

$$P_z(k+1) \ = \frac{T}{k+1}\Phi\left(k,\ P_z(k),\ \lambda_z(k),\ \mu_z(k)\right), \tag{12}$$

де $P_z(k)$ – диференціальне зображення оригіналу $P_z(t)$.

Диференціальне зображення $P_z(k)$ представляє дискретну (гратчасту) функцію цілочисельного аргументу $k =: 0, 1, 2, \ldots$. Масштабна стала H має розмірність аргументу t і, в системі (7), обрана рівною тривалості процесу моделювання $H = T$.

Знаходження відповідних дискрет диференціальних спектрів $P_z(k)$ з системи (12), при значеннях цілочисельного аргументу $k =: 0, 1, 2, \ldots$, дозволяє визначити в області оригіналів модель процесу нападу на інформацію загального вигляду

$$P_0(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k P_0(k). \tag{13}$$

Диференціально-ігровий базис моделювання процесу нападу на інформацію диференціальними перетвореннями передбачає знаходження ціни гри I^*, оптимальних стратегій гравців $\lambda_z^{opt}(t)$ і $\mu_z^{opt}(t)$ і траєкторії диференціальної гри $P_0^{opt}(k)$, що є спектральною моделлю процесу нападу на інформацію.

Для знаходження оптимальних стратегій гравців $\lambda_z^{opt}(t)$ і $\mu_z^{opt}(t)$ плату I , вираз (6), подають в області зображень спектральною моделлю

$$I^* = \sum_{k=0}^{k=\infty}\frac{P_0(k)}{k+1}. \tag{14}$$

Дослідивши плату (14) на існування необхідних

$$\begin{cases} \dfrac{\partial I^*\left(\lambda_{z\max},\ \mu_{z\max}\right)}{\partial \lambda_{z\max}} = 0; \\ \dfrac{\partial I^*\left(\lambda_{z\max},\ \mu_{z\max}\right)}{\partial \mu_{z\max}} = 0 \end{cases} \tag{15}$$

та достатніх умов

$$\begin{cases} \dfrac{\partial^2 I^*\left(\lambda_{z\max},\ \mu_{z\max}\right)}{\partial \lambda_{z\max}^2} > 0; \\ \dfrac{\partial^2 I^*\left(\lambda_{z\max},\ \mu_{z\max}\right)}{\partial \mu_{z\max}^2} < 0, \end{cases} \tag{16}$$

визначають оптимальні стратегії гравців $\lambda_z^{opt}(t)$ і $\mu_z^{opt}(t)$, ціну гри I^* та вигляд спектральної моделі процесу нападу на інформацію $P_0^{opt}(k)$, яка відповідає таким стратегіям.

Таким чином, з урахуванням $\lambda_z^{opt}(t)$ і $\mu_z^{opt}(t)$, модель (13) в області оригіналів [30–32] набуває вигляду

$$P_0^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k P_0^{opt}(k). \tag{17}$$

Для моделювання процесу нападу на інформацію на значному часовому інтервалі застосуємо чисельно-аналітичний метод, запропонований у [33]. Основною перевагою методу чисельно-аналітичного моделювання над відомим методом припасовування [33–35], є можливість зменшення об'єму обчислень, що відкриває можливість організації процесу моделювання у реальному масштабі часу.

Динаміку процесу нападу на інформацію, з урахуванням моделі (17), можна подати як систему локальних диференціальних рівнянь вигляду

$$\frac{dP_0^{opt}{}_i(t)}{dt} = \varphi_i\left(t,\ P_0^{opt}{}_i(t)\right),\ P_0^{opt}(0) = 1,\ t\ \in\ [0,\ T], \tag{18}$$

де $i = \overline{0, n}$, n – кількість рівних частин, на які розбивається інтервал $t\ \in\ [0,\ T]$.

Моделювання процесу нападу на інформацію проведемо із застосуванням методу зміщених диференціальних перетворень [33, 34]. Для цього часовий відрізок $[0,\ T]$ розіб'ємо на n рівних частин, а систему локальних векторних рівнянь (18) розглянемо в двох точках t_i та t_{i+1}, де $t_{i+1} = t_i + T$.

У точці $t = t_i$, при $h = \frac{T}{2}$, застосування зміщених диференціальних перетворень

$$P_0^{opt}{}_i(k) = \frac{h^k}{k!}\left[\frac{d^k P_0^{opt}{}_i(t)}{dt^k}\right]_{t=t_i} \quad \div \quad P_0^{opt}{}_i(t) = \sum_{k=0}^{k=\infty}\left(\frac{t-t_i}{h}\right)^k P_0^{opt}{}_i(k), \tag{19}$$

де $\div$ – символ відповідності між оригіналом $P_0^{opt}{}_i(t)$ і його диференціальним зображенням $P_0^{opt}{}_i(k)$, зводить систему (18) до наступного вигляду

$$P_0^{opt}{}_i(k+1) = \frac{h}{k+1}\Psi_i\left(T_i(k), P_0^{opt}{}_i(k)\right),\ P_0^{opt}{}_i(0) = \left[P_0^{opt}{}_i(k)\right]_{k=0} = 1, \tag{20}$$

де $i = \overline{0, n-1}$.

Рекурентний вираз (20) застосовується для знаходження прямих диференціальних спектрів $P_0^{opt}{}_i(k)$ у чисельному вигляді в кожній точці t_i. На відрізку $[t_i, t_i + h]$, при зміні часового аргументу t в напрямку його збільшення від точки t_i до точки $t_i + h$, прямі диференціальні спектри $P_0^{opt}{}_i(k)$ на основі зворотних перетворень (19) дозоляють відновити оригінал – функцію $P_0^{opt}{}_i(t)$.

Аналогічна процедура здійснюється над системою (18) і в точці $t = t_{i+1}$ з використанням зміщених диференціальних перетворень

$$P_0^{opt}{}_{i+1}(k) = \frac{h^k}{k!}\left[\frac{d^k P_0^{opt}{}_{i+1}(t)}{dt^k}\right]_{t=t_{i+1}} \div P_0^{opt}{}_{i+1}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t-t_{i+1}}{h}\right)^k P_0^{opt}{}_{i+1}(k). \tag{21}$$

Застосувавши прямі диференціальні перетворення (21) до системи локальних векторних рівнянь (18), отримаємо її зображення у вигляді системи спектральних рівнянь

$$P_0^{opt}{}_{i+1}(k+1) = \frac{h}{k+1}\Psi_{i+1}\left(T_{i+1}(k), P_0^{opt}{}_{i+1}(k)\right),\ P_0^{opt}{}_{i+1}(0) = \left[P_0^{opt}{}_{i+1}(k)\right]_{k=0} = P_0^{opt}{}_{i+1}, \tag{22}$$

де $P_0^{opt}{}_{i+1}$ – невідома нульова дискрета.

За рекурентним виразом (22) знаходиться аналітичний вигляд зворотного диференціального спектра $P_0^{opt}{}_{i+1}(k)$. Застосування зворотного перетворення, яке стоїть ліворуч від символу $\div$ у виразі (21), в точці $t = t_{i+1}$ дозволяє відновити оригінал $P_0^{opt}{}_{i+1}(t)$ в аналітичному вигляді на відрізку від $[t_i + h,\ t_i + 2h]$ при зменшенні часового аргументу t від точки $t_i + 2h$ до точки $t_i + h$.

Спряження функцій $P_0^{opt}{}_i(t)$ та $P_0^{opt}{}_{i+1}(t)$ здійснюється у спільній для двох функцій точці $t_i + h$, тобто

$$P_0^{opt}{}_i(t_i + h) = P_0^{opt}{}_{i+1}(t_i + h), \tag{23}$$

звідки невідома величина $P_0^{opt}{}_{i+1}$ визначається з точного рівняння загального вигляду

$$\sum_{k=0}^{k=\infty} P_0^{opt}{}_i(k) = \sum_{k=0}^{k=\infty}(-1)^k P_0^{opt}{}_{i+1}(k). \tag{24}$$

Обмежившись на практиці деякою кількістю дискрет q, що враховуються при моделюванні відповідних диференціальних спектрів $P_0^{opt}{}_i(k)$ та $P_0^{opt}{}_{i+1}(k)$, розрахунок невідомих дискрет здійснюється за наближеним виразом

$$\sum_{k=0}^{k=q} P_0^{opt}{}_i(k) \approx \sum_{k=0}^{k=q}(-1)^k P_0^{opt}{}_{i+1}(k). \tag{25}$$

Величина q обирається, виходячи із заданої точності заміни нескінченного ряду (24) скінченним (25), шляхом розв'язання задачі Коші.

Чисельно-аналітична процедура (19)–(25) повторюється до тих пір, поки неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію $P_0^{opt}(t)$ не досягне заданої точності моделювання на визначному часовому інтервалі $[0,T]$.

Як доведено в [34, 36], застосування методу чисельно-аналітичного моделювання на одому кроці дозволяє в 2^q разів зменшити оцінку зверху похибки визначення функції $P_0^{opt}{}_i(t)$, порівняно, наприклад, із відомим методом припасовування [35], де q-кількість дискрет, які враховуються для диференціальних спектрів $P_0^{opt}{}_i(k)$ та $P_0^{opt}{}_{i+1}(k)$.

Висновки та перспективи подальших досліджень. Вперше розроблена неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію, що відрізняється від відомих застосуванням методу чисельно-аналітичного моделювання на базі зміщених диференціальних перетворень, що дозволило значно розширити діапазони моделювання нестаціонарних процесів при заданих діапазонах точності. Подальшим напрямом розвитку розробленої моделі є її прикладні дослідження та числові експерименти.

ЛІТЕРАТУРА:

1. *Гейер Д.* Беспроводные сети. Первый шаг : пер. с англ. / *Д. Гейер.* – М. : Издательский дом "Вильямс", 2005. – 192 с.
2. *Казарин О.В.* Теория и практика защиты программ / *О.В. Казарин*. – М. : МГУЛ, 2004. – 450 с.
3. *Завгородний В.И.* Комплексная защита информации в компьютерных системах / *В.И. Завгородний.* – М. : Логос, 2001. – 264 с.
4. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации / *А.А. Малюк*. – М. : Горячая линия – Телеком, 2004. – 280 с.
5. *Хорошко В.О.* Информационная безопасность Украины. Основные проблемы и перспективы / *В.О. Хорошко* // Захист інформації. – К. : ДУІКТ, 2008. – № 40 (спеціальний випуск). – С. 6–9.
6. *Грищук Р.В.* Інформаційна безпека України: сучасний стан, проблеми та шляхи їх вирішення / *Р.В. Грищук, В.О. Хорошко* // Проблеми створення, розвитку та застосування інформаційних систем спеціального призначення, Житомир, 9 квіт. 2009 р. : міжвузівська наук.-практ. конф. – Житомир : ЖВІ НАУ, 2009. – С. 154–155.
7. *Ленков С.В.* Методы и средства защиты информации: в 2-х т / *С.В. Ленков, Д.А. Перегудов, В.А. Дорошко.* – К. : Арий, 2008. – 464 с.
8. *Поповский В.В.* Защита информации в телекоммуникационных системах : учебник / *В.В. Поповский, А.В. Персиков.* – Харьков : ООО "Компания СМИТ", 2006. – 238 с.
9. *Ігнатов В.О.* Динаміка інформаційних конфліктів в інтелектуальних системах / *В.О. Ігнатов, М.М. Гузій* // Проблеми інформатизації та управління. – К. : НАУ, 2005. – Вип. 15. – С. 88–92.
10. *Дружинин В.В.* Введение в теорию конфликта / *В.В. Дружинин, Д.С. Конторов, М.Д. Дружинин.* – М. : Радио и связь, 1989. – 288 с.
11. *Кунцевич В.М.* Управление в условиях неопределённости: гарантированные результаты в задачах управления и идентификации / *В.М. Кунцевич.* – К. : Наук. думка, 2006. – 264 с.
12. *Девянин П.Н.* Модели безопасности компьютерных систем / *П.Н. Девянин.* – М. : Издательский центр "Академия", 2005. – 144 с.
13. *Домарев В.В.* Безопасность информационных технологий. Системный подход / *В.В. Домарев.* – К. : ООО "ТИД "ДС", 2004. – 992 с.
14. *Бабак В.П.* Теоретичні основи захисту інформації : підручник / *В.П. Бабак.* – К. : Книжкове вид-во НАУ, 2008 – 752 с.
15. *Мельников В.В.* Безопасность информации в автоматизированных системах / *В.В. Мельников.* – М. : Финансы и статистика, 2003. – 368 с.
16. *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.
17. *Грищук Р.В.* Диференціально-ігрова розгалужена спектральна модель процесу нападу на інформацію / *Р.В. Грищук* // Вісник ЖДТУ / Технічні науки. – 2009. – № 1 (48). – С. 152–159.
18. *Грищук Р.В.* Диференціально-ігрова модель кількісної оцінки захищеності технічних об'єктів / *Р.В. Грищук* // Захист інформації. – К. : ДУІКТ, 2008. – № 40 (спец. випуск). – С. 24–29.

19. *Грищук Р.В.* Диференціально-тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу / *Р.В. Грищук* // Захист інформації. – К. : ДУІКТ, 2009. – № 1 (42). – С. 19–27.
20. *Грищук Р.В.* Спектральна модель процесу нападу на інформацію / *Р.В. Грищук* // Захист інформації. – К. : ДУІКТ, 2009. – № 2 (43). – С. 71–81.
21. *Грищук Р.В.* Метод гібридного P-L-моделювання процесів нападу на інформацію / *Р.В. Грищук* // Вісник наукових праць ВІКНУ. – 2009. – № 46. – С. 102–105.
22. *Грищук Р.В.* GIGW гібридна P-L-модель процесу нападу на інформацію / *Р.В. Грищук, В.О. Хорошко* // Вісник СНУЯЭиП. – 2009. – № 46 (III). – С. 31–39.
23. *Грищук Р.В.* P-моделювання процесів нападу на інформацію при нестаціонарній природі потоків захисних дій та інформаційних атак / *Р.В. Грищук* // Системи обробки інформації. – Харків : ХУПС ім. І.Кожедуба, 2009. – № 7 (79). – С. 98–101.
24. *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.
25. *Грищук Р.В.* Верифікація і дослідження спектральних P- та гібридних P-L-моделей процесу нападу на інформацію / *Р.В. Грищук* // Вісник ЖДТУ / Технічні науки. –2009. – № 2 (49). – С. 152–159.
26. *Вентцель Е.С.* Исследование операций: задачи, принципы, методология / *Е.С. Вентцель.* – М. : Гл. ред. физ.-мат. лит., 1980. – 208 с.
27. *Айзекс Р.* Дифференциальные игры / *Р.Айзекс.* – М. : Мир, 1967. – 479 с.
28. *Васильев В.В.* Моделирование задач оптимизации и дифференциальных игр / *В.В. Васильев, В.Л. Баранов*. – К. : Наукова думка, 1989. – 286 с.
29. *Вайсборд Э.М.* Введение в дифференциальные игры нескольких лиц и их приложения / *Э.М. Вайсборд, В.И. Жуковский.* – М. : Советское радио, 1980. – 304 с.
30. *Пухов Г.Е.* Дифференциальные спектры и модели / *Г.Е. Пухов.* – К. : Наук. думка, 1990. – 184 с.
31. *Пухов Г.Е.* Дифференциальные преобразования функций и уравнений / *Г.Е. Пухов*. – К. : Наук. думка, 1984. – 420 с.
32. P-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.
33. *Баранов В.Л.* Численно-аналитический метод моделирования динамических процессов в системах защиты информации / *В.Л. Баранов, К.В. Молодецкая* // Захист інформації. – К. : ДУІКТ, 2009. – № 4 (45). – С. 21–24.
34. *Баранов В.Л.* Порівняння методів моделювання динамічних процесів основними та зміщеними диференціальними перетвореннями / *В.Л. Баранов, Г.Л. Баранов, О.Г. Фролова* // Проблеми інформатизації та управління. – К. : НАУ, 2004. – Вип. 10. – С. 72–77.
35. *Баранов В.Л.* Метод моделювання фізичних процесів на основі диференціальних перетворень нелінійних крайових задач / *В.Л. Баранов, С.В. Водоп'ян, Р.М. Костюченко* // Вісник ЖДТУ / Технічні науки. – 2007. – № 2 (41). – С. 59–65.
36. *Засядько А.А.* Методи розв'язання некоректних задач на основі багатокритерійної оптимізації і диференціальних перетворень для автоматизованих систем управління: автореф. дис. ... д-ра тех. наук : спец. 05.13.06 "Автоматиз. сист. упр. та прогрес. інформац. технології" / *А.А. Засядько*. – К., 2006. – 37 с.

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

Наукові інтереси:

– моделювання процесів нападу на інформацію та її захисту.

Подано 26.12.2009

Грищук Р.В. Неперевна дискретна диференціально-ігрова модель процесу нападу на інформацію
Грищук Р.В. Непрерывная дискретная дифференциально-игровая модель процесса нападения на информацию
Gryschuk R.V. Continuous discrete differential-gaming model of the attack process on the information

УДК 004.9:517.978.2

Непрерывная дискретная дифференциально-игровая модель процесса нападения на информацию / Р.В. Грищук

В статье разработано непрерывную дискретную дифференциально-игровую модель процесса нападения на информацию. Разработанная модель позволяет повышать точность спектральных дифференциально-игровых моделей процессов нападения на информацию в области оригиналов на значительных интервалах времени.

УДК 004.9:517.978.2

Continuous discrete differential-gaming model of the attack process on the information / R.V. Gryschuk

Continuous discrete differential-gaming model of the attack process on the information is developed in the article. The developed model enables to improve accuracy of the spectral differential-gaming models of the attack processes on the information in original domain on the considerable time slices.