ІНФОРМАТИКА, ОБЧИСЛЮВАЛЬНА ТЕХНІКА ТА АВТОМАТИЗАЦІЯ

УДК 004.9:517.978.2

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

КІЛЬКІСНА ОЦІНКА РІВНЯ ЗАХИЩЕНОСТІ ОБ'ЄКТІВ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЇ ТЕХНІКИ З УРАХУВАННЯМ ЇХ ФУНКЦІОНУВАННЯ В УМОВАХ ІНФОРМАЦІЙНОГО КОНФЛІКТУ

Представлена робота є новим підходом до кількісного оцінювання рівня захищеності об'єктів електронно-обчислювальної техніки. Розроблені моделі дозволяють отримувати гарантовану та поточні оцінки рівня захищеності об'єктів електронно-обчислювальної техніки з урахуванням їх функціонування в умовах інформаційного конфлікту.

Постановка проблеми у загальному вигляді та її зв'язок із важливими практичними завданнями. На сучасному етапі розвитку суспільства стрімкий розвиток інформаційних та комунікаційних технологій становить актуальну проблему для інформаційної безпеки держави [1, 2]. Під вплив методів несанкціонованого доступу (НСД) потрапляють як окремі об’єкти електронно-обчислювальної техніки (ЕОТ), так і елементи складних динамічних систем (СДС) [1, 3]. Можливо припустити, що і у подальшому методи НСД до об'єктів ЕОТ будуть застосовуватися не менш інтенсивно. Ефективний захист від методів НСД повинен ґрунтуватися на знаннях гарантованого та поточного рівнів захищеності об'єктів ЕОТ.

Аналіз останніх досліджень і публікацій. Процедура оцінювання рівня захищеності означується системою кількісних та якісних показників, які забезпечують розв’язання завдання захисту інформації на основі норм та вимог технічного захисту інформації, що регламентується вимогами Державного стандарту України [4].

Міжнародний стандарт [5] передбачає проведення оцінювання рівня захищеності експертами. Такому підходу властиві принципові недоліки, що призводять до низького рівня захищеності. Суть недоліків полягає у невизначеності постановки завдання і, відповідно, складності отримуваних рішень, якість яких визначається кваліфікацією та підготовленістю експертів. Виявлених недоліків можна позбавитися шляхом максимального усунення експерта від процедури оцінювання, чим самим отримувати не якісні, а кількісні оцінки.

В Україні і в світі кількісний підхід до оцінювання досліджений недостатньо, хоча йому приділяється значна увага фахівців [3, 6–9]. В роботах [6–9] не враховано динаміку інформаційного конфлікту. Під інформаційним конфліктом слід розуміти взаємодію двох суб’єктів – методів захисту інформації (МЗІ) та методів НСД, цілі яких є протилежними [1, 3]. У [3] не врахована надійність функціонування об'єктів ЕОТ та збурень, що вносяться зовнішніми і внутрішніми впливами, реалізованими у вигляді інформаційних атак. До зовнішніх відносять спеціальні впливи, у тому числі і техногенного характеру [6], до внутрішніх – впливи на об’єкти ЕОТ з боку обслуговуючого персоналу, інсайдерів тощо [10]. У роботі [11] запропоновано отримання кількісних поточних оцінок, але не наведено математичний апарат отримання гарантованої кількісної оцінки рівня захищеності. З проведеного аналізу видно, що на сьогоднішній день відсутня єдина методологія кількісного оцінювання рівня захищеності об'єктів ЕОТ, яка б дозволяла одночасно враховувати ймовірнісний характер показників функціонування об'єктів і динаміку протікання інформаційних конфліктів.

Метою даної роботи є розробка нового підходу до кількісного оцінювання рівня захищеності об'єктів ЕОТ, здатного адекватно відображати зміни динаміки процесу інформаційного конфлікту та його ймовірнісний характер протікання.

Викладення основного матеріалу. Проаналізуємо сукупність впливів на об’єкт ЕОТ в процесі інформаційного конфлікту. Для цього представимо синтезовану структурну схему процесу кількісного оцінювання рівня захищеності (рис. 1) [11].

Постановка задачі. Протягом усього періоду функціонування об’єкта ЕОТ за призначенням $[t_0, T]$ із заданим ймовірнісним показником надійності $P(t_i)_{НАД}$ йому загрожують методи НСД, зовнішні та внутрішні впливи з відповідними ймовірностями $P(t_i)_{НСД}$, $P(t_i)_{\alpha\ ЗВ}$ та $P(t_i)_{\beta\ ВН}$, де $t_0 \geq 0$, t_0, T – моменти початку та припинення функціонування об’єкта відповідно; t_i – поточний час перебування об’єкта ЕОТ в інформаційному конфлікті, $t_i \in [t_0, T]$, $i = \overline{1, m}$, m – кількість моментів поточного часу, у які проводитиметься оцінювання; $\alpha = \overline{1, M}$, M – кількість зовнішніх впливів, $\beta = \overline{1, N}$, N – кількість внутрішніх впливів.

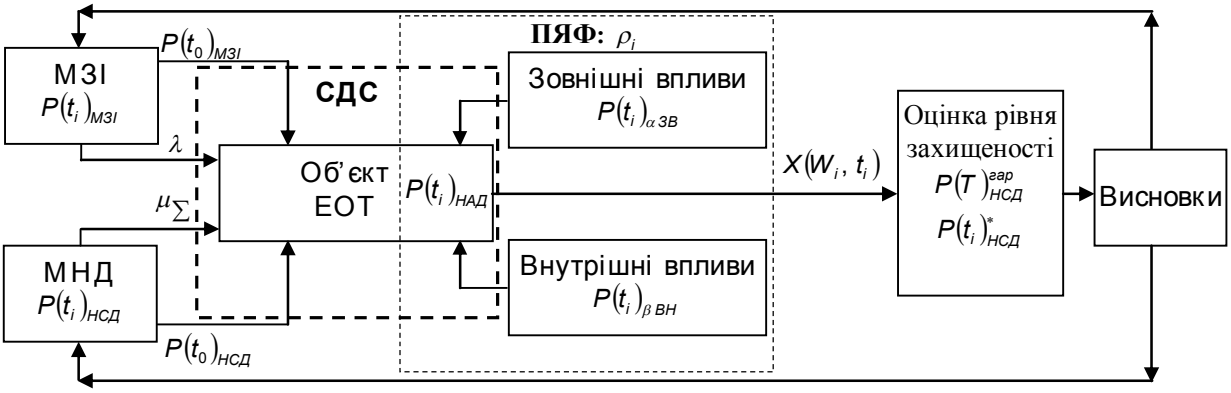

Рис. 1. Схема кількісного оцінювання рівня захищеності об'єкта електронно-обчислювальної техніки

Нехай об'єкт ЕОТ перебуває у одному з двох інформаційних станів – стані нападу або стані захищеності. Ймовірності перебування об'єкта під впливом методів НСД $P(t_i)_{НСД}$ та МЗІ $P(t_i)_{МЗІ}$ являють собою повну групу подій:

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

У поточний момент часу t_i модель інформаційного конфлікту описується вектором стану $X(W_i, t_i)$ (див. рис. 1) загального вигляду:

$$X(W_i, t_i) = X\left(P(t_i)_{МЗІ}, P(t_i)_{НСД}, \lambda, \mu_\Sigma, \rho_i, t_i\right), \quad (2)$$

де λ – інтенсивність потоку захисних дій; μ_Σ – сумарна інтенсивність потоку інформаційних атак ($\mu_\Sigma = \mu_{ЗВ} + \mu_{ВН}$, де $\mu_{ЗВ}, \mu_{ВН}$ – інтенсивності зовнішніх і внутрішніх атак відповідно); ρ_i – ймовірнісний показник якісного функціонування (ПЯФ) об'єкта ЕОТ, який у поточний момент часу t_i враховує показник надійності функціонування об'єкта $P(t_i)_{НАД}$, зовнішні $P(t_i)_{\alpha ЗВ}$ та внутрішні $P(t_i)_{\beta ВН}$ загрози, що становлять групу випадкових, але сумісних подій. Тобто ймовірнісний ПЯФ ρ_i є функціоналом вигляду:

$$\rho_i = f\left(P(t_i)_{НАД}, P(t_i)_{\alpha ЗВ}, P(t_i)_{\beta ВН}\right). \quad (3)$$

Застосування системо-аналогового моделювання [12] до функціоналу (3) дає змогу представити ймовірнісний ПЯФ у формалізованій постановці [8]:

$$\rho_i = \left(P(t_i)_{НАД} \prod_{\alpha=1}^{M}\left(1 - P(t_i)_{\alpha ЗВ}\right)\prod_{\beta=1}^{N}\left(1 - P(t_i)_{\beta ВН}\right)\right). \quad (4)$$

У формалізованій постановці поточне значення вектора стану об'єкта ЕОТ $X(W_i, t_i)$ (2) може бути описане системою звичайних диференціальних рівнянь першого порядку (Колмогорова-Чепмена) [3]. З урахуванням ймовірнісного ПЯФ ρ_i (4), який враховує випадковий характер функціонування об'єкта, модель (2) матиме вигляд [11]:

$$X(W_i, t_i) \equiv \begin{cases} \dfrac{dP(t_i)_{НСД}}{dt_i} = \left(-\lambda P(t_i)_{НСД} + \mu_\Sigma P(t_i)_{МЗІ}\right)\rho_i; \\ \dfrac{dP(t_i)_{МЗІ}}{dt_i} = \left(\lambda P(t_i)_{НСД} - \mu_\Sigma P(t_i)_{МЗІ}\right)\rho_i. \end{cases} \quad (5)$$

Захисні дії здійснюються на інтервалі часу, який визначається від початку до припинення функціонування об'єкта ЕОТ за призначенням:

$$t_i \in [t_0, T]. \quad (6)$$

На ресурси захисних та атакуючих дій накладаються відповідні обмеження:

$$0 < \lambda \le \lambda_{\max}, \quad (7)$$

$$0 \le \mu \le \mu_{\sum \max}, \quad (8)$$

де $\lambda_{\max}$ – максимальна інтенсивність потоку захисних дій; $\mu_{\sum \max}$ – максимальна сумарна інтенсивність потоків інформаційних атак.

В умовах невизначеності інтенсивності інформаційних атак, що діють на об'єкт ЕОТ, критерій якості захищеності матиме інтегральний вигляд, який описується функціоналом:

$$I = \frac{1}{T} \int_{t_0}^{T} P(t)_{НСД} \, dt . \tag{9}$$

Задача оцінки рівня захищеності об'єктів ЕОТ має на меті знайти закон зміни інтенсивності захисних дій $\lambda(t)_o$ на інтервалі (7), який мінімізує значення функціонала (9), при довільному законі зміни інтенсивності потоку інформаційних атак $\mu(t)_{\sum}$, в границях обмежень (8). Таким чином, задача зводиться до прийняття оптимального рішення $\lambda(t)_o$ на захисні дії в умовах конфлікту (5).

Поставлена задача має диференціально-ігровий базис та безкоаліційний характер [13]. З метою пошуку оптимальних стратегій у безкоаліційних диференціальних іграх гравці (суб'єкти) можуть використовувати різні види стратегій (правил поведінки): гарантуючі, рівноважні по Нешу і стратегії, які слідують з концепції "погроз і контрпогроз" [13].

Для розв'язання поставленої задачі застосовано гарантуючу (мінімаксну) стратегію. Застосування принципу мінімаксу обґрунтовується тим, що гравець, який захищається, може отримати гарантовану оцінку рівня захищеності об'єкта ЕОТ при буд-якому довільному поводженні атакуючої сторони в межах обмежень (8):

$$I^* = \min_{\lambda} \max_{\mu_{\sum}} I , \tag{10}$$

або з урахуванням (9)

$$I^* = \min_{\lambda} \max_{\mu_{\sum}} \left(\frac{1}{T} \int_{t_0}^{T} P(t)_{НСД} \, dt \right). \tag{11}$$

У випадках найгіршого (максимального) сполучення дії потоку інформаційних атак з невідомим законом зміни, обмежених за величиною (8), застосування мінімаксної стратегії гарантує мінімізацію функціонала (11).

Визначимо гарантуючу стратегію гравця, який захищається. Враховуючи умову нормування (1), зведемо перше рівняння системи (5) до диференціально-ігрової моделі виду

$$\frac{dP(t_i)_{НСД}}{dt_i} = \left(-\lambda P(t_i)_{НСД} + \mu_{\sum} \left(1 - P(t_i)_{НСД}\right) \right) \rho_i . \tag{12}$$

Покриємо простір станів диференціальної гри ($P(t)_{НСД}$, T) квадратною решіткою, сторони якої паралельні осям координат $P(t)_{НСД}$ і t , та з'єднаємо сусідні вузли решітки діагоналями (рис. 2).

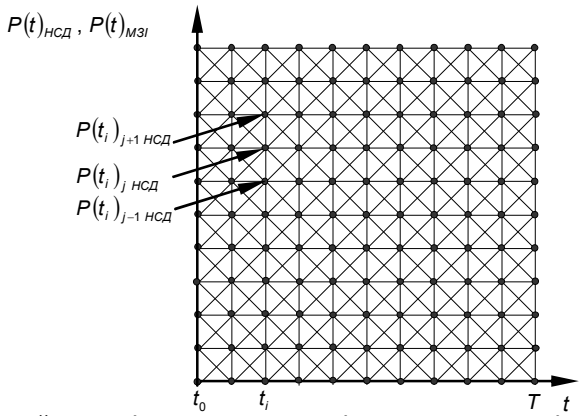

Рис. 2. Фазовий простір, що визначає рівень захищеності об'єкта електронно-обчислювальної техніки

Представимо квадратну решітку (рис. 2) у вигляді графа з вершинами, яким присвоїмо координати стану ($P(t_i)_{j\ НСД}$, t_i), і ребрами, що з'єднують сусідні вершини по горизонталі, вертикалі і діагоналі, де $j = \overline{1, n}$, n – крок решітки (для квадратної решітки $n = m$). У процесі керування захистом об'єкта ЕОТ, модель якого задана диференціально-ігровою моделлю (12), можливий перехід з однієї вершини графа до

іншої і навпаки. Тому сусідні вершини графа з'єднуються двома ребрами графа, вага яких може бути різною.

Вагу ребер графа визначимо з умови максимізації збільшення критерію (11) за набором керувань другого гравця у процесі переходу стану гри з однієї вершини графа у іншу, що з'єднується даним ребром. Перехід стану гри з однієї вершини графа в іншу здійснюється під дією керування першого гравця (рис. 3).

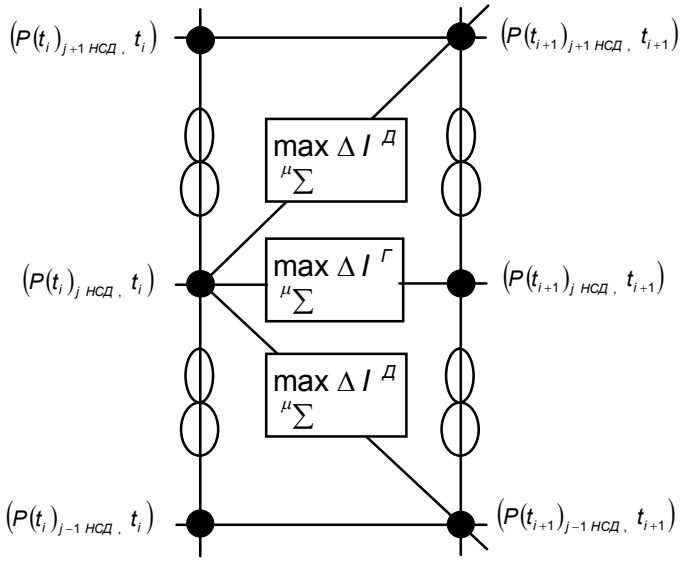

Рис. 3. Динаміка переходу стану гри

З j-ї вершини графа відкривається ряд можливих переходів диференціальної гри (рис. 3). Обчислимо вагу та керування першого гравця для кожного з переходів.

Вага горизонтального ребра, яке виходить з j-ї вершини графа, визначається як середня ймовірність $P(\Delta t)^{сер}_{j\ НСД}$ знаходження об'єкта ЕОТ у стані несанкціонованого доступу на інтервалі (6), де $\Delta t = t_{i+1} - t_i$, $T = m\,\Delta t$:

$$\Delta I^{\Gamma} = P(\Delta t)^{сер}_{j\ НСД} = \frac{1}{m} P(\Delta t)_{j\ НСД}\ . \tag{13}$$

При переході по горизонтальному ребру виконується умова (див. рис. 3):

$$\frac{dP(t_i)_{j\ НСД}}{dt_i} = 0\,. \tag{14}$$

Керування потоком захисних дій на горизонтальному ребрі λ^{Γ}, при максимізації потоку інформаційних атак $\mu_{\sum \max}$ та виконанні умови (14), визначається з моделі (12) як

$$\lambda^{\Gamma} = \frac{\mu_{\sum \max}\left(1 - P(t_{i+1})_{j\ НСД}\right)}{P(t_{i+1})_{j\ НСД}}\,. \tag{15}$$

Горизонтальні ребра графа, на яких не виконується обмеження (7), потрібно виключити з процесу моделювання. Присвоїмо цим ребрам нескінченну вагу. Для цього введемо функцію заборони для горизонтальних ребер σ^{Γ}:

$$\sigma^{\Gamma} = \begin{cases} 1\,, & 0 < \lambda^{\Gamma} \le \lambda_{\max}\ ; \\ 0\,, & \lambda^{\Gamma} > \lambda_{\max}. \end{cases} \tag{16}$$

Ребра графа, на яких функція заборони σ^{Γ} (16) приймає нульове значення, виключають з розгляду шляхом заборони цих ребер (на рис. 3 прийнято позначкою ∞). Ребрам графа, на яких функція заборони σ^{Γ} (16) приймає одиничне значення, надають максимальну вагу, обумовлену $\mu_{\sum \max}$, яке максимізує вагу ребра графа. Керування першого гравця, що забезпечує перехід стану гри уздовж ребра графа, визначають за співвідношенням (15) і приписують відповідному горизонтальному ребру графа.

Вага діагональних ребер, які виходять з j -ї вершини графа, визначається як

$$\Delta I^{Д} = \frac{1}{T}\int_{t_i}^{t_{i+1}} P(t_i)_{j\,НСД}^{сер}\, dt = \frac{1}{m} P(t_{i+1})_{j\pm1\,НСД}^{сер}, \tag{17}$$

де $P(t_{i+1})_{j\pm1\,НСД}^{сер}$ – середня ймовірність переходу по діагоналі з j -ї вершини $\left(P(t_i)_{j\,НСД}, t_i\right)$ у вершину з координатами $\left(P(t_{i+1})_{j+1\,НСД}, t_{i+1}\right)$ або $\left(P(t_{i+1})_{j-1\,НСД}, t_{i+1}\right)$, яка дорівнює:

$$P(t_{i+1})_{j\pm1\,НСД}^{сер} = P(t_i)_{j\,НСД} + \frac{P(t_{i+1})_{j\pm1\,НСД} - P(t_i)_{j\,НСД}}{2}. \tag{18}$$

Приймемо швидкість нахилу діагоналей $\frac{dP(t_i)_{НСД}}{dt_i}$ в моделі (12) рівною деякій величині K , тобто

$$\frac{dP(t_i)_{НСД}}{dt_i} = \mathrm{K}. \tag{19}$$

Нахил діагоналей врахуємо знаком перед K :

$$\begin{cases} \mathrm{K} > 0, & \textit{діагональ вверх}; \\ \mathrm{K} < 0, & \textit{діагональ вниз}. \end{cases} \tag{20}$$

З урахуванням (20) і моделі (12) керування на діагональних ребрах $\lambda^{Д}$, у загальному вигляді, визначатиметься як

$$\lambda^{Д} = \frac{\mu_{\Sigma\,\max}\left(1 - P(t_{i+1})_{j\pm1\,НСД}^{сер}\right) \pm \frac{\mathrm{K}}{\rho_i}}{P(t_{i+1})_{j\pm1\,НСД}^{сер}}. \tag{21}$$

Кінцевий вираз для керування захисними діями на діагональних ребрах $\lambda^{Д}$ отримаємо, провівши підстановку у керування (21) середньої ймовірності переходу по діагоналях (18) та ймовірнісного ПЯФ (4):

$$\lambda^{Д} = \frac{\mu_{\Sigma\,\max}\left(1 - P(t_i)_{j\,НСД} + \frac{P(t_{i+1})_{j\pm1\,НСД} - P(t_i)_{j\,НСД}}{2}\right)}{\left(P(t_i)_{j\,НСД} + \frac{P(t_{i+1})_{j\pm1\,НСД} - P(t_i)_{j\,НСД}}{2}\right)} \pm$$

$$\pm \frac{\mathrm{K}}{\left(P(t_i)_{j\,НСД} + \frac{P(t_{i+1})_{j\pm1\,НСД} - P(t_i)_{j\,НСД}}{2}\right)\left(P(t_i)_{НАД}\prod_{\alpha=1}^{M}\left(1 - P(t_i)_{\alpha\,ЗВ}\right)\prod_{\beta=1}^{N}\left(1 - P(t_i)_{\beta\,ВН}\right)\right)}. \tag{22}$$

Функція заборони для діагональних ребер $\sigma^{Д}$ матиме вигляд:

$$\sigma^{Д} = \begin{cases} 1, & 0 < \lambda^{Д} \le \lambda_{\max}; \\ 0, & \lambda^{Д} > \lambda_{\max}. \end{cases} \tag{23}$$

Зауваження. Вага вертикальних ребер не розраховується. Перехід по вертикалях заборонено, оскільки величина $\frac{dP(t_i)_{НСД}}{dt_i}$ є скінченною.

Таким чином, вихідну задачу кількісного оцінювання рівня захищеності об’єктів ЕОТ на основі диференціально-ігрової моделі (12) зведено до знаходження найкоротшого шляху між початковим і кінцевим вузлами. Розв’язок даної задачі отримують, використовуючи алгоритми, запропоновані у [14], або застосовують паралельні структури на основі аналогових, цифрових або гібридних моделей [15]. Застосування відомих алгоритмів [14, 15] дає змогу отримати аналітичний вигляд моделі кількісної оцінки гарантованого рівня захищеності:

$$P(T)_{НСД}^{гар} = \frac{\mu_{\Sigma\,\max}}{\mu_{\Sigma\,\max} + \lambda}. \tag{24}$$

Динамічну модель поточної оцінки рівня захищеності об’єктів ЕОТ $P(t_i)_{НСД}^{*}$ отримаємо з моделі (12) шляхом розв'язання задачі Коші відносно $P(t_i)_{НСД}$, за початкових умов

$$P(T)_{НСД}^{зар} \le P(t_0)_{НСД} \le 1, \qquad 0 \le P(t_0)_{МЗІ} \le P(T)_{НСД}^{зар}. \tag{25}$$

і застосування перетворень Лапласа [12].

Представимо окремо доданки моделі (12) при застосуванні до неї прямого перетворення:

$$L\left\{\frac{dP(t_i)_{НСД}}{dt_i}\right\} = \int_0^{\infty} \frac{dP(t_i)_{НСД}}{dt_i} e^{-S_i t_i} dt_i = -P(S_0)_{НСД} + S_i P(S_i)_{НСД};$$

$$L\{\rho_i \mu_\Sigma\} = \rho_i \mu_\Sigma L\{1\} = \rho_i \frac{\mu_\Sigma}{S_i}; \tag{26}$$

$$L\{-\rho_i(\lambda + \mu_\Sigma) P(t_i)_{НСД}\} = -\rho_i(\lambda + \mu_\Sigma) L\{P(t_i)_{НСД}\} = -\rho_i(\lambda + \mu_\Sigma) P(S_i)_{НСД}.$$

З урахуванням (26) модель (12) зведеться до наступного рівняння:

$$-P(S_0)_{НСД} + S_i P(S_i)_{НСД} = \rho_i \frac{\mu_\Sigma}{S_i} - \rho_i(\lambda + \mu_\Sigma) P(S_i)_{НСД}, \tag{27}$$

розв'язок якого відносно $P(S_i)_{НСД}$ матиме вигляд:

$$P(S_i)_{НСД} = \frac{P(S_0)_{НСД} + \rho_i \frac{\mu_\Sigma}{S_i}}{S_i + \rho_i(\lambda + \mu_\Sigma)} = P(S_0)_{НСД} \frac{1}{S_i + \rho_i(\lambda + \mu_\Sigma)} + \\ + \rho_i \frac{\mu_\Sigma}{S_i}\left(\frac{1}{S_i} - \frac{1}{S_i + \rho_i(\lambda + \mu_\Sigma)}\right). \tag{28}$$

Застосувавши до (28) зворотне перетворення Лапласа

$$L\{f(t)\} = P(S_0)_{НСД} \frac{1}{S_i + \rho_i(\lambda + \mu_\Sigma)}, \text{ то}$$

$$f(t) = P(t_0)_{НСД} \exp(-\rho_i(\lambda + \mu_\Sigma) t_0),$$

$$L\{f_1(t)\} = \frac{\mu_\Sigma}{\lambda + \mu_\Sigma}\left(\frac{1}{S_i} - \frac{1}{S_i + \rho_i(\lambda + \mu_\Sigma)}\right), \text{ то} \tag{29}$$

$$f_1(t) = \frac{\mu_\Sigma}{\lambda + \mu_\Sigma}(1 - \exp(-\rho_i(\lambda + \mu_\Sigma) t_i)),$$

отримаємо загальний розв'язок задачі Коші для моделі (12) за початкових умов (25):

$$P(t_i)_{НСД}^{*} = P(t_0)_{НСД} \exp(-\rho_i(\lambda + \mu_\Sigma) t_0) + \frac{\mu_\Sigma}{\lambda + \mu_\Sigma}(1 - \exp(-\rho_i(\lambda + \mu_\Sigma) t_i)). \tag{30}$$

Врахувавши у (30) величину ймовірнісного ПЯФ (4), динамічна модель поточної оцінки рівня захищеності об'єктів ЕОТ $P(t_i)_{НСД}^{*}$ набуває кінцевого вигляду:

$$P(t_i)_{НСД}^{*} = P(t_0)_{НСД} \exp\left(-\left(P(t_i)_{НАД} \prod_{\alpha=1}^{M}(1 - P(t_i)_{\alpha\,ЗВ}) \prod_{\beta=1}^{N}(1 - P(t_i)_{\beta\,ВН})\right)(\lambda + \mu_\Sigma) t_0\right) + \\ + \frac{\mu_\Sigma}{\lambda + \mu_\Sigma}\left(1 - \exp\left(-\left(P(t_i)_{НАД} \prod_{\alpha=1}^{M}(1 - P(t_i)_{\alpha\,ЗВ}) \prod_{\beta=1}^{N}(1 - P(t_i)_{\beta\,ВН})\right)(\lambda + \mu_\Sigma) t_i\right)\right). \tag{31}$$

Висновки та перспективи подальших досліджень. У представленій роботі, на основі системного підходу, вперше запропоновано методичні основи та подано математичні вирази для отримання кількісної оцінки рівня захищеності об'єктів електронно-обчислювальної техніки.

Вперше оцінку рівня захищеності об'єктів ЕОТ сформульовано у формі диференціальної гри. Запропонована диференціально-ігрова модель (12) дискретизована на графах і зведена до задачі про найкоротший шлях, що дозволяє отримати гарантовану оцінку рівня захищеності (24). Динамічна модель (31) дозволяє отримувати поточні оцінки рівня захищеності в умовах інформаційного конфлікту з урахуванням функціонування об'єктів у задані моменти часу.

У подальшому планується дослідити поведінку моделей (24) і (31) при різних початкових умовах (7), (8) та (4).

ЛІТЕРАТУРА:

1. *Хорошко В.А., Чекатов А.А.* Методы и средства защиты информации. – К.: Юниор, 2003. – 478 с.
2. *Даник Ю.Г., Катков Ю.І., Пічугін М.Ф.* Національна безпека: запобігання критичним ситуаціям: Монографія. – Житомир: Рута, 2006. – 388 с.
3. *Ігнатов В.О., Гузій М.М.* Динаміка інформаційних конфліктів в інтелектуальних системах // Проблеми інформатизації та управління. – К.: НАУ, 2005. – Вип. 15. – С. 88-92.
4. ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.
5. ISO 15408. The Common Criteria for Information Technology Security Evaluation.
6. *Андреев В.И., Козлов В.С., Хорошко В.А.* Количественная оценка защищённости технических объектов с учётом их функционирования // Захист інформації. – К.: НАУ, 2004. – № 2. – С. 47–50.
7. *Козлов В.С., Хорошко В.А.* Количественная оценка защищённости информации // Захист інформації. – К.: НАУ, 2003. – № 4. – С. 67–73.
8. *Козлова К.В., Хорошко В.О.* Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) // Захист інформації. – К.: ДІТС, 2007. – № 1. – С. 30–32.
9. *Мельников В.В.* Безопасность информации в автоматизированных системах. – М.: Финансы и статистика, 2003. – 368 с.
10. *Кавун С.В., Сорбат И.В.* Инсайдер – угроза экономической безопасности // Управління розвитком. – Х.: ХНЕУ, 2008. – № 6. – С. 7–11.
11. *Грищук Р.В.* Кількісна оцінка рівня захищеності радіоелектронного об'єкта в складній динамічній системі під час інформаційного конфлікту // Управління розвитком. –Х.: ХНЕУ, 2008. – № 6. – С. 57–59.
12. *Андреєв В.І., Козюра В.Д., Скачек Л.М., Хорошко В.О.* Стратегія управління інформаційною безпекою. – К.: ДУІКТ, 2007. – 277 с.
13. *Вайсборд Э.М., Жуковский В.И.* Введение в дифференциальные игры нескольких лиц и их приложения. – М.: Советское радио, 1980. – 304 с.
14. *Васильев В.В., Баранов В.Л.* Моделирование задач оптимизации и дифференциальных игр. – К.: Наукова думка, 1989. – 286 с.
15. *Мартынова О.П.* Параллельный алгоритм маршрутизации на графах и сетях // Проблеми інформатизації та управління: Зб. наук. праць – К.: НАУ, 2005. – Вип. 12. – С. 113–119.

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

Наукові інтереси:

– безпека інформації в інформаційних та комунікаційних системах.

Подано 07.08.2008

Грищук Р.В. Кількісна оцінка рівня захищеності об'єктів електронно-обчислювальної техніки з урахуванням їх функціонування в умовах інформаційного конфлікту
Грищук Р.В. Количественная оценка уровня защищённости объектов электронно-вычислительной техники с учётом их функционирования в условиях информационного конфликта.
Gryschuk R.V. A quantitative estimation protected level is taking into account functioning objects of electron-computing devices in the conditions of informative conflict

УДК 004.9:517.978.2

Количественная оценка уровня защищённости объектов электронно-вычислительной техники с учётом их функционирования в условиях информационного конфликта / Р.В. Грищук

В работе предложен новый подход к количественной оценке уровня защищённости объектов электронно-вычислительной техники. Разработанные в статье модели позволяют получать гарантированные и текущие оценки уровня защищённости с учётом функционирования объектов в условиях информационного конфликта.

УДК 004.9:517.978.2

A quantitative estimation protected level is taking into account functioning objects of electron-computing devices in the conditions of informative conflict / R.V. Gryschuk

The given work present a novel approach to quantity estimation protection level of objects of electron-computing devices. The developed model allows to compute quantified protection level and current estimations of objects of electron-computing devices For this purpose is developed a new quantity estimation models and its physical interpretation is given.