DOI:10.32703/2617- 9040- 2021- 38- 198-19

УДК 681.325

***Ірина Воронко*[1]**

[1]Старший викладач, кафедра автоматизація та комп'ютерно-інтегровані технології транспорту, Державний університет інфраструктури та технологій, вул. Кирилівська, 9, м. Київ, 04071, Україна. ORCID: https://orcid.org/0000-0003-3599-6672

[1]**Автор, відповідальний за листування**: voronko_io@gsuite.duit.edu.ua

ДИФЕРЕНЦІАЛЬНО-ІГРОВА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ КОМП'ЮТЕРНИХ СИСТЕМ ТРАНСПОРТНОЇ ІНФРАСТРУКТУРИ

У статті розглядається питання надійності та захисту інформації комп'ютерних системах транспортної інфраструктури та описується синтез та аналіз диференціально-ігрових моделей та методів моделювання процесів кібернападу на сервер комп'ютерних інформаційно-діагностичних систем дистанції електропостачання залізниці. Розроблено уніфіковану диференціально-ігрову модель процесу кібернападу на мультизадачний сервер інформаційно-діагностичної комп'ютерної системи нижнього рівня залізниці, яка дозволяє отримати оптимальні стратегії захисту інформації в умовах кібератак. Представлено результати моделювання процесу кібератаки, для оцінки інтегральних показників захищеності серверу, при використанні оптимальних стратегій по кожній із функцій. Показано вигляд уніфікованої моделі комп'ютерно-інформаційної системи, та приведені графіки перехідних процесів ймовірності перебування серверу в захищеному стані та ймовірності відмови серверу по будь якій із функціональностей.

Ключові слова: *захист інформації, кібернапад, кібератака, стратегія кіберзахисту, стратегія кібернападу, диференціально-ігрові моделі, графова модель.*

Вступ. Стрімкий розвиток і ускладнення технічних комп'ютерних пристроїв та систем в транспортній інфраструктурі призвели до необхідності забезпечення високого рівня інформаційного захисту та надійності. До таких основних заходів можна віднести побудову систем по модульному принципу та з використанням функцій самодіагностики, що актуальним на сьогодні. Саме впровадження сучасних мікропроцесорних пристроїв в транспортній інфраструктурі будь якої галузі, в якості керуючих, дозволило на алгоритмічному рівні реалізовувати функції самодіагностики, із використанням ресурсів власного керуючого мікропроцесорного пристрою, або додаткових діагностичних вузлів на його основі.

Впровадження систем контролю та діагностики, до прикладу на електроенергетичних об'єктах залізниці, дає можливість подовжити терміни експлуатації основного обладнання, забезпечується можливість своєчасного виконання ремонтних робіт, що є обов'язковим, при врахуванні фізичної зношеності більшої частини основного енергетичного обладнання тягових підстанцій, і тим самим, забезпечуються умови безперебійної роботи залізничного транспорту. Тому в основі організації корпоративних комп'ютерних систем управління електричними мережами залізниць і, відповідно, локальних керуючих мереж систем електропостачання на рівні тягових підстанцій, лежить безперервний контроль режимних параметрів.

Аналізуючи структуру корпоративної системи моніторингу та діагностики перехідних режимів електроенергетичних систем транспортної інфраструктури [1], а саме залізничного транспорту, можна зробити висновок, що одним із ключових об'єктів по надійності є головний сервер інформаційної мережі дистанції електропостачання залізниці. Його функції полягають у формуванні єдиного інформаційного простору первинної інформації, яка отримується із Phasor

Measurement Units (PMUs) [2] тягових підстанцій дистанції електропостачання залізниці, реалізації процедур обміну інформацією з центральною корпоративною мережею, веденні баз даних первинної аварійної та комерційної інформації. Разом з тим, така мультизадачність головного серверу обумовлює складність застосовуваних системи захисту інформації (СЗІ) [3] та необхідність використання уточнених моделей захисту інформації для оцінки рівня захищеності даного елементу мережі. Так як на сьогоднішній день переважна більшість вразливостей інформаційної безпеки корпоративних комп'ютерних систем моніторингу та діагностики властива компонентам та технологіям верхніх рівнів ієрархії транспортної інфраструктури. При цьому інтегральна надійність нижнього вимірювального рівня, представленого пристроями реєстрації в основному визначається здатністю PMUs забезпечувати повну функціональність згідно специфікації, та рівнем їх ремонтопридатності для оперативного виявлення та усунення несправностей в процесі експлуатації. У фокусі уваги перебувають дослідження пов'язані з забезпеченням надійності стійкості серверів та концентраторів даних відносно зосереджених кібератак на реєстратори PMUs та програмне забезпечення корпоративної комп'ютерної системи моніторингу та діагностики електроенергетичних систем залізниці [4]. Слід відмітити, що до систем діагностики, а особливо до діагностичних систем стратегічних об'єктів енергосистем транспортної інфраструктури ставляться підвищені вимоги до показників надійності. Крім того, із можливості застосування інформації, отриманої з допомогою цифрових реєстраторів, для оперативного керування режимами енергопостачання, слідує, що забезпечення гарантованого рівня показників надійності, при мінімізації затрат на технічне обслуговування є важливою науковою задачею.

Аналіз останніх досліджень і постановка проблеми. Для вирішення задач знаходження моделей процесів нападу на інформацію мультизадачного серверу комп'ютерно-інформаційної діагностичної системи об'єктів енергосистем транспортної інфраструктури, визначення оптимальних стратегій розподілу ресурсів СЗІ та визначення гарантованого рівня захищеності інформації, доцільним є застосовування теорії диференціальних ігор (ДІ) та методи теорії диференціальних перетворень (ДП) [5, 6]. Ефективність моделювання процесів кібернападу методами теорії ДІ та ДП обумовлена рядом обставин які описані в [7].

Мета і завдання дослідження. Розробити диференціально-ігрову модель процесу кібернападу на мультизадачний сервер комп'ютерно-інформаційних діагностичних систем дистанції електропостачання залізниці, яка дозволяє отримати оптимальні стратегії захисту інформації в умовах кібератак і забезпечити безперебійну роботу залізничного транспорту.

Матеріали та методи дослідження. Нехай сервер у складі системи моніторингу перехідних режимів у поточний момент часу перебуває в одному з типових станів, та під впливом інформаційних атак або під впливом методів захисту інформації змінює стани, з відповідними ймовірностями, протягом деякого часу T, що дорівнює тривалості інтервалу здійснення інформаційних атак.

$$t \in [0,\ T] \tag{1}$$

Для складання диференціальних рівнянь Колмогорова-Чепмена [8, 9], побудуємо графову модель [10] процесу нападу на інформацію, при цьому ймовірності станів системи визначимо таким чином:

$P_{F0}(t)$ – ймовірність відмови серверу – порушення, або не виконання будь-якої з передбачених функцій;

$P_{F1}(t)$ – ймовірність відмови комунікації з системою нижнього рівня;

$P_{F2}(t)$ – ймовірність відмови комунікації з системою верхнього рівня;

$P_{F3}(t)$ – ймовірність відмови функцій адміністрування бази даних аварійних параметрів;

$P_{F4}(t)$ – ймовірність відмови функцій адміністрування комерційної бази даних;

$P_{S0}(t)$ – ймовірність забезпечення сервером повної функціональності;

$P_{S1}(t)$ – ймовірність забезпечення комунікаційних функцій з системою нижнього рівня;

$P_{S2}(t)$ – ймовірність забезпечення комунікаційних функцій з системою верхнього рівня;

$P_{S3}(t)$ – ймовірність забезпечення функцій адміністрування бази даних аварійних параметрів;

$P_{S4}(t)$ – ймовірність забезпечення функцій адміністрування комерційної бази даних;

$P_{SF1}(t)$ – ймовірність атаки на комунікаційні функції з системою нижнього рівня, при дії методів захисту інформації (МЗІ);

$P_{SF2}(t)$ – ймовірність атаки на комунікаційні функції з системою верхнього рівня, при дії МЗІ;

$P_{SF3}(t)$ – ймовірність атаки на функцій адміністрування бази даних аварійних параметрів, при дії МЗІ;

$P_{SF4}(t)$ – ймовірність атаки на функцій адміністрування комерційної бази даних, при дії МЗІ.

На рис. 1 приведено графову модель процесу інформаційної атаки на сервер.

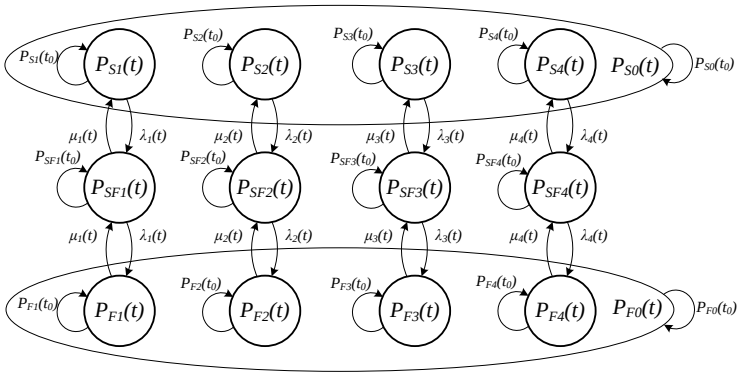

Рис. 1. **Графова модель процесу інформаційної атаки**

У вузлах графу вказано ймовірності станів, а над стрілками переходів, що переводять сервер зі стану в стан, відмічено інтенсивності потоків захисних дій $\mu_j(t)$ та інформаційних атак $\lambda_i(t)$, чим зазначено їх нестаціонарну природу, яка, в загальному випадку визначається функціональними часопараметричними залежностями.

Як видно з приведених визначень станів інформаційної системи, безвідмовна робота серверу S_0 передбачає забезпечення повної функціональності, тобто одночасного перебування системи в станах S_1 .. S_4, що можна вважати незалежними подіями. Відмова серверу F_0, по будь-якій із функціональностей, відповідно, є подією, що настає при виникненні хоча б однієї з незалежних відмов F_1 .. F_4. Таким чином, для ймовірностей станів S_0 та F_0 можна записати:

$$\begin{cases} P_{S0}(t) = \prod_{i=1}^{4} P_{Si}(t)\,; \\ P_{F0}(t) = 1 - \prod_{i=1}^{4}(1 - P_{Fi}(t))\,. \end{cases} \tag{2}$$

На основі графової моделі запишемо систему диференціальних рівнянь, що описує динаміку незалежних атак на функціональність мультизадачного серверу:

$$\begin{cases} \frac{dP_{Si}(t)}{dt} = -\mu_i(t)P_{Si}(t) + \lambda_i(t)P_{SFi}(t); \\ \frac{dP_{SFi}(t)}{dt} = -(\lambda_i(t) + \mu_i(t))P_{SFi}(t) + \lambda_i(t)P_{Si}(t) + \mu_i(t)P_{Fi}(t); \\ \frac{dP_{Fi}(t)}{dt} = -\mu_i(t)P_{Fi}(t) + \lambda_i(t)P_{SFi}(t), \quad i = 1..4. \end{cases} \tag{3}$$

Для ймовірностей станів інформаційної системи слід враховувати умову нормування, що задається у вигляді виразу для повної групи подій:

$$P_{Si}(t) + P_{Fi}(t) + P_{SFi}(t) = 1, \quad i = 1..4. \tag{4}$$

Таким, чином для інтегрального розгляду процесів кібернападу на сервер слід доповнити (3) рівняннями (2) та (4), в результаті чого отримуємо математичну модель розглядуваного інформаційного конфлікту:

$$\begin{cases} P_{S0}(t) = \prod_{i=1}^{4} P_{Si}(t); \\ P_{F0}(t) = 1 - \prod_{i=1}^{4}(1 - P_{Fi}(t)); \\ P_{Si}(t) = 1 - P_{Fi}(t) - P_{SFi}(t); \\ \frac{dP_{SFi}(t)}{dt} = -(\lambda_i(t) + \mu_i(t))P_{SFi}(t) + \lambda_i(t)P_{Si}(t) + \mu_i(t)P_{Fi}(t); \\ \frac{dP_{Fi}(t)}{dt} = -\mu_i(t)P_{Fi}(t) + \lambda_i(t)P_{SFi}(t), \quad i = 1..4. \end{cases} \tag{5}$$

Для відповідних ймовірностей станів справедливі такі початкові умови:

$$\begin{cases} P_{S0}(t_0) = 1, \ P_{F0}(t_0) = 0; \\ P_{SF1}(t_0) = P_{SF2}(t_0) = P_{SF3}(t_0) = P_{SF4}(t_0) = 0. \end{cases} \tag{6}$$

Система рівнянь (5) дозволяє визначити розподіл ймовірностей перебування сервера в кожному стані протягом інформаційного конфлікту з урахуванням інтенсивностей потоків атак та захисних дій МЗІ.

В наслідок того, що в реальних умовах зміна стратегій сторін обумовлюється багатьма чинниками, яких в більшості випадків врахувати не має можливості, припустимо, нехай стратегії гравців розподілені за лінійними законами загального вигляду:

$$\begin{aligned} \lambda_i(t) &= \lambda_i \cdot t, \\ \mu_j(t) &= \mu_j \cdot t, \end{aligned} \tag{7}$$

де t – часовий аргумент згідно (1),

i, j – кількість переходів між станами у результаті успішних атак порушника та у наслідок дії МЗІ;

λ_i та μ_j – параметри апроксимації законів розподілу стратегій гравців.

На ресурси захисних дій μ_j та інформаційних атак λ_i накладаються обмеження вигляду:

$$\begin{aligned} \lambda_{i\,min}(t) \le \lambda_i(t) \le \ \lambda_{i\,max}(t), \\ \mu_{j\,max}(t) \le \mu_j(t) \le \ \mu_{j\,max}(t), \end{aligned} \tag{8}$$

де відповідно $\lambda_{i\,min}(t)$, $\mu_{j\,min}(t)$ – мінімальні та $\lambda_{i\,max}(t)$, $\mu_{j\,max}(t)$ – максимальні інтенсивності потоків інформаційних атак та захисних дій.

Інтенсивності дій гравців $\lambda_i(t)$, та $\mu_j(t)$, які визначають ресурси сторін гри, лежать у межах замкнутих множин $\Lambda \in V_\lambda$ та $M \in V_\mu$, які в свою чергу обмежені в евклідовими просторами E_λ та E_μ відповідно [10-12].

Під час інформаційного конфлікту гравці намагаються досягти протилежних цілей. Гравець, або МЗІ, що захищається від атак, намагається забезпечити функціональну стійкість серверу шляхом гарантування його захищеності, а гравець, що атакує – досягнути відмови серверу від обслуговування по певній функціональності. Для цього гравець, що захищається від атаки, намагається забезпечити найменший програш за рахунок вибору такої власної стратегії $\mu_i(t)$, яка мінімізує плату за умови її максимізації іншим гравцем, що формалізується у вигляді:

$$\min_{\mu_j(t)\in V_\mu}\max_{\lambda_i(t)\in V_\lambda} I\Big(t,\ P_{F0}(t),\ \lambda_i(t),\ \mu_j(t)\Big). \quad (9)$$

Порушник максимізує плату I, при мінімізації власних втрат під час нанесення атак:

$$\max_{\lambda_i(t)\in E_\lambda}\min_{\mu_j(t)\in E_\mu} I\Big(t,\ P_{F0}(t),\ \lambda_i(t),\ \mu_j(t)\Big). \quad (10)$$

При рівності плат обох сторін (9) та (10) виконується співвідношення:

$$\min_{\mu_j(t)\in E_\mu}\max_{\lambda_i(t)\in E_\lambda} I = \max_{\lambda_i(t)\in E_\lambda}\min_{\mu_j(t)\in E_\mu} I = I^*\Big(t,\ P_{F0}^{opt}(t),\ \lambda_i^{opt}(t),\mu_j^{opt}(t)\Big). \quad (11)$$

Стратегії гравців $\lambda_i^{opt}(t)$ та $\mu_j^{opt}(t)$є оптимальними для розглядуваної гри, а $P_{F0}^{opt}(t)$є оптимальною траєкторією, яка розраховується з системи рівнянь (5) за критерієм (11). Відхилення будь-якого із гравців від своєї оптимальної стратегії, призводить до відповідних втрат в платі (11).

Отже, гарантований рівень захищеності серверу досягається за рахунок вибору гравцями оптимальних стратегій $\lambda_i^{opt}(t)$ та $\mu_j^{opt}(t)$:

$$I^*\Big(t,\ P_{F0}^{opt}(t),\ \lambda_i^{opt}(t),\mu_j^{opt}(t)\Big) = I^G \quad (12)$$

де I^G – ціна гри, що визначає гарантований рівень захищеності серверу.

В умовах динамічного інформаційного конфлікту, плату гри I, можна представити в інтегральному вигляді [6-13]:

$$I = \frac{1}{T}\int_{t_o}^{T} P_{F0}(t)dt, \quad (13)$$

при обмеженнях

$$0 \le I \le 1. \quad (14)$$

Інтегрування здійснюється вздовж траєкторії гри від початкового моменту часу $t = t_0$ до моменту закінчення інформаційного конфлікту $t = T$.

Представлення диференціально-ігрової моделі в області зображень. Моделювання процесу нападу на функціональність серверу з використанням (5) в аналітичному вигляді є складною математичною процедурою, яка потребує обробки великого обсягу інформації у реальному та прискореному часі.

Для моделювання процесу нападу на інформацію у реальному і прискореному часі без втрати точності вихідної моделі (5) пропонується застосування P-перетворень [14-16], що представляють собою диференціально-тейлорівські перетворення (ДТ-перетворення), вперше запропоновані академіком НАН України Пуховим Г.Є. [17, 18].

Застосування P-перетворень має переваги у скороченні обсягу обчислень чисельними методами, яка досягається за рахунок аналітичних можливостей даного операційного методу. Представлення вихідної моделі (5) в області зображень методом ДП дозволяє зберегти точність вихідної моделі при виключенні часового аргументу. В результаті чого, моделювання процесу нападу на інформацію зводиться до виконання арифметичних операцій в області зображень.

P-перетвореннями називаються функціональні перетворення виду [14, 15]:

$$X(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \Leftrightarrow\ x(t) = \sum_{k=0}^{\infty}\left(\frac{t}{H}\right)^k X(k) \quad (15)$$

де $x(t)$ – оригінал, що являє собою безперервну, що диференціюється нескінченну кількість разів і обмежену разом із всіма своїми похідними, функцію дійсного аргументу *t*;

$X(k)$ – позначення диференційного зображення оригіналу, що представляє собою дискретну (гратчасту) функцію цілочисельного аргументу, де *k=: 0, 1, 2,..;*

H – масштабний коефіцієнт, що має розмірність аргументу *t* і часто обирається рівним відрізку часу, на якому розглядається функція $x(t)$.

В перетвореннях (15) в лівій частині знаходиться вираз для прямого перетворення, що дозволяє за оригіналом $x(t)$ знайти зображення $X(k)$, а праворуч – зворотне перетворення, що дозволяє за зображенням $X(k)$ отримати оригінал $x(t)$ у формі степеневого ряду Тейлора з центром у точці *t=0*. Диференціальні зображення $X(k)$ називаються диференціальними *T*-спектрами, а значення *T*-функції $X(k)$ при конкретних значеннях аргументу *k* називаються дискретами.

Переведемо вихідну модель (5) методом *P*-перетворень виду (15) в область *T*-зображень, при цьому масштабний коефіцієнт *H* приймемо рівним тривалості інформаційних атак *T*. Тоді, система в області зображень прийме вигляд:

$$\begin{cases} P_{S0}(k) = \prod_{i=1}^{4} P_{Si}(k); \\ P_{F0}(k) = 1 - \prod_{i=1}^{4}(1 - P_{Fi}(k)); \\ P_{Si}(k) = 1 - P_{Fi}(k) - P_{SFi}(k); \\ P_{SFi}(k+1) = \frac{T}{k+1}[(-(\Lambda_i(k) + M_i(k))P_{SFi}(k) + \Lambda_i(k)P_{Si}(k) + M_i(k)P_{Fi}(k)], \\ P_{Fi}(k+1) = \frac{T}{k+1}[(-M_i(k)P_{Fi}(k) + \Lambda_i(k)P_{SFi}(k)], \ i = 1..4. \end{cases} \quad (16)$$

де $P_z(k)$, $\Lambda_i(k)$, $M_j(k)$ – диференційні зображення оригіналів функцій $P_z(t)$, $\lambda_i(t)$, $\mu_j(t)$ відповідно.

Зважаючи на прийняті допущення, що стратегії гравців у ході інформаційного протистояння змінюються за лінійним законами (7), при переході в область *P*-зображень необхідно врахувати властивості *T*-добутків диференціальних зображень $\Lambda_i(k)\ P_z(k)$ та $M_j(k)P_z(k)$ [14-18], один з доданків в яких являє собою сталі λ та μ множені на цілу степінь незалежного змінного T^m (при *m*=1), в загальному вигляді:

$$\Lambda_i(k)P_z(k) = \lambda_i T P_z(k-1) = \begin{cases} \lambda_i T P_z(k-1), & k \geq 1, \\ 0, & k < 1, \end{cases}$$
$$M_j(k)P_z(k) = \mu_j T P_z(k-1) = \begin{cases} \mu_j T P_z(k-1), & k \geq 1, \\ 0, & k < 1. \end{cases} \quad (17)$$

З урахуванням перетворень добутків в області зображень (18), система спектральних рівнянь (17) матиме вигляд:

$$\begin{cases} P_{S0}(k) = \prod_{i=1}^{4} P_{Si}(k); \\ P_{F0}(k) = 1 - \prod_{i=1}^{4}(1 - P_{Fi}(k)); \\ P_{Si}(k) = 1 - P_{Fi}(k) - P_{SFi}(k); \\ P_{SFi}(k+1) = \frac{T^2}{k+1}[-(\lambda_i + \mu_i)P_{SFi}(k-1) + \lambda_i P_{Si}(k-1) + \mu_i P_{Fi}(k-1)]; \\ P_{Fi}(k+1) = \frac{T^2}{k+1}[-\mu_i P_{Fi}(k-1) + \lambda_i P_{SFi}(k-1)], \quad i = 1..4. \end{cases} \quad (18)$$

Використовуючи спектральну модель експлуатації системи (19) та початкові умови (6),

визначимо дискрети ймовірностей $P_{Fi}(k)$, при $k:=0,1,\ 2\ldots$, в результаті отримуємо:

$$P_{Fi}(0)=P_{Fi}(1)=P_{Fi}(2)=0; \tag{19}$$

$$P_{Fi}(3)=\frac{T^4}{3}\lambda_i^2; \tag{20}$$

$$P_{Fi}(4)=\frac{T^4}{8}\left(\lambda_i^2-T^2\lambda_i^3\right); \tag{21}$$

$$P_{Fi}(5)=\frac{T^4}{15}\left(-2T^2\mu_i\lambda_i^2-2T^2\lambda_i^3+\lambda_i^2\right); \tag{22}$$

$$P_{Fi}(6)=\frac{T^4}{24}\left(-T^2\mu_i\lambda_i^2+T^4\mu_i\lambda_i^3+T^4\lambda_i^4-T^2\lambda_i^3+\lambda_i^2\right). \tag{23}$$

Згідно другого рівняння системи (19) та виразів (20) – (24) отримаємо відповідні дискрети ймовірності відмови серверу:

$$P_{F0}(0)=P_{F0}(1)=P_{F0}(2)=0; \tag{24}$$

$$P_{F0}(3)=1-\prod_{i=1}^{4}(1-\frac{T^4}{3}\lambda_i^2); \tag{25}$$

$$P_{F0}(4)=1-\prod_{i=1}^{4}(1-\frac{T^4}{8}\left(\lambda_i^2-T^2\lambda_i^3\right)); \tag{26}$$

$$P_{F0}(5)=1-\prod_{i=1}^{4}(1-\frac{T^4}{15}\left(-2T^2\mu_i\lambda_i^2-2T^2\lambda_i^3+\lambda_i^2\right)); \tag{27}$$

$$P_{F0}(6)=1-\prod_{i=1}^{4}(1-\frac{T^4}{24}\left(-T^2\mu_i\lambda_i^2+T^4\mu_i\lambda_i^3+T^4\lambda_i^4-T^2\lambda_i^3+\lambda_i^2\right)). \tag{28}$$

Знаходження оптимальних стратегій кіберзахисту. Для отримання ціни гри в області зображень слід застосувати диференціальне перетворення (15) до виразу ціни гри в часовій області (13), тоді отримуємо [7, 13-16]:

$$I=\sum_{k=0}^{\infty}\frac{P_{F0}(k)}{k+1}. \tag{29}$$

З врахуванням (30), відповідним чином в області зображень будемо розглядати максимінний критерій (11), який формалізуємо у вигляді:

$$\min_{\mu_{jk}\in E_\mu}\max_{\lambda_{ik}\in E_\lambda} I=\max_{\lambda_{ik}\in E_\lambda}\min_{\mu_{jk}\in E_\mu} I=I^*\left(t,\ P_{F0}^{opt}(k),\ \lambda_{ik}^{opt},\mu_{jk}^{opt}\right). \tag{30}$$

Знайдемо ціну гри підставивши дискрети (25)-(29) в (30), отримуємо:

$$I\approx\sum_{k=0}^{6}\frac{P_{F0}(k)}{k+1}=1+\frac{1}{4}(1-\prod_{i=1}^{4}(1-\frac{T^4}{3}\lambda_i^2))+\frac{1}{5}(1-\prod_{i=1}^{4}(1-\frac{T^4}{8}\left(\lambda_i^2-T^2\lambda_i^3\right)))+\frac{1}{6}(1-\prod_{i=1}^{4}(1-\frac{T^4}{15}\left(-2T^2\mu_i\lambda_i^2-2T^2\lambda_i^3+\lambda_i^2\right)))+\frac{1}{7}(1-\prod_{i=1}^{4}(1-\frac{T^4}{24}\left(-T^2\mu_i\lambda_i^2+T^4\mu_i\lambda_i^3+T^4\lambda_i^4-T^2\lambda_i^3+\right.$$
$$\left.+\lambda_i^2\right))). \tag{31}$$

Знайдемо екстремуми функції (32) для чого вирішимо систему алгебраїчних рівнянь:

$$\begin{cases} \frac{\partial I}{\partial \lambda_i}:\left[\frac{T^4}{6}\lambda_i\right](1-\prod_{j=1,j\neq i}^{4}\left(1-\frac{T^4}{3}\lambda_j^2\right))+\left[\frac{T^4}{40}(2\lambda_i-3T^2\lambda_i^2)\right](1-\prod_{j=1,j\neq i}^{4}(1-\frac{T^4}{8}(\lambda_j^2-T^2\lambda_j^3)))+ \\ +\left[\frac{T^4}{45}(-2T^2\mu_i\lambda_i-3T^2\lambda_i^2+\lambda_i)\right]\left(1-\prod_{j=1,j\neq i}^{4}\left(1-\frac{T^4}{15}(-2T^2\mu_j\lambda_j^2-2T^2\lambda_j^3+\lambda_j^2)\right)\right)+ \\ +\left[\frac{T^4}{168}(-2T^2\mu_i\lambda_i+3T^4\mu_i\lambda_i^2+4T^4\lambda_i^3-3T^2\lambda_i^2+2\lambda_i)\right]\times \\ \times\left(1-\prod_{j=1,j\neq i}^{4}\left(1-\frac{T^4}{24}(-T^2\mu_j\lambda_j^2+T^4\mu_j\lambda_j^3+T^4\lambda_j^4-T^2\lambda_j^3+\lambda_j^2)\right)\right)=0; \\ \frac{\partial I}{\partial \mu_i}:\left[-\frac{T^6}{45}\lambda_i^2\right](1-\prod_{j=1,j\neq i}^{4}\left(1-\frac{T^4}{15}(-2T^2\mu_j\lambda_j^2-2T^2\lambda_j^3+\lambda_j^2)\right))+ \\ +\left[\frac{T^6}{168}\lambda_i^2(T^2\lambda_i-1)\right]\left(1-\prod_{j=1,j\neq i}^{4}\left(1-\frac{T^4}{24}(-T^2\mu_j\lambda_j^2+T^4\mu_j\lambda_j^3+T^4\lambda_j^4-T^2\lambda_j^3+\lambda_j^2)\right)\right)=0. \end{cases} \quad (32)$$

Беручи до уваги умову незалежності здійснення кібератак, стратегії захисту для кожної із інформаційних задач серверу можна відшукати припустивши відсутність конфліктів по інших функціях. Таким чином отримуємо:

$$\begin{cases} \frac{\partial I}{\partial \lambda_i}:\frac{T^4}{6}\lambda_i+\frac{T^4}{40}(2\lambda_i-3T^2\lambda_i^2)+\frac{T^4}{45}(-2T^2\mu_i\lambda_i-3T^2\lambda_i^2+\lambda_i)+ \\ +\frac{T^4}{168}(-2T^2\mu_i\lambda_i+3T^4\mu_i\lambda_i^2+4T^4\lambda_i^3-3T^2\lambda_i^2+2\lambda_i)=0; \\ \frac{\partial I}{\partial \mu_i}:-\frac{T^6}{45}\lambda_i^2+\frac{T^6}{168}\lambda_i^2(T^2\lambda_i-1)=0. \end{cases} \quad (33)$$

Виконавши відповідні перетворення системи (34), отримуємо вирази для оптимальних стратегій гравців в області зображень:

$$\begin{cases} \mu_i=-\frac{60T^4\lambda_i^2-402T^2\lambda_i+602}{45T^4\lambda_i-142T^2}; & \mu_i\approx 16.35\frac{1}{T^2}; \\ \lambda_i=\frac{213}{45}\frac{1}{T^2}; & \lambda_i\approx 4.73\frac{1}{T^2}. \end{cases} \quad (34)$$

Після переходу до часової області згідно (15) отримуємо вирази для оптимальних стратегій захисту та кібератак:

$$\begin{cases} \mu_i(t)\approx 16.35\frac{t}{T^2}; \\ \lambda_i(t)\approx 4.73\frac{t}{T^2}. \end{cases} \quad (35)$$

На основі (3) та (6) з використанням (36) побудовано математичну модель в середовищі MATLAB (Simulink) та виконано математичне моделювання процесу зміни ймовірностей станів комп'ютерно-інформаційної діагностичної системи на транспорті в процесі здійснення кібератаки, результати якого показано на рис. 2.

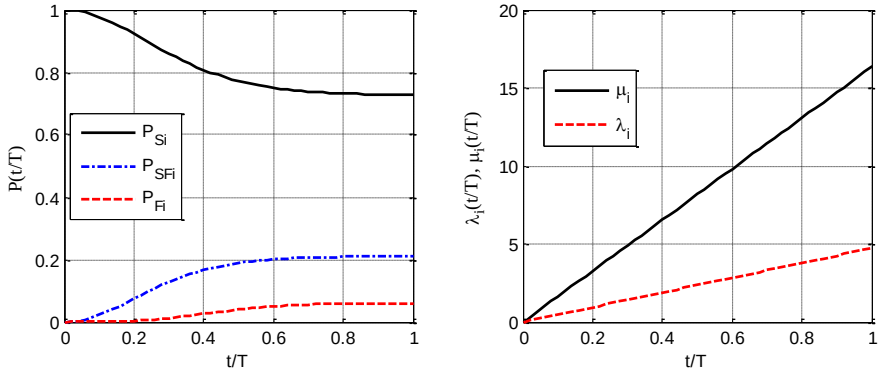

Рис. 2. **Графіки перехідних процесів ймовірностей станів *i*-ї функції сервера при реалізації кібернападу з використанням оптимальних стратегій (36)**

Як можна бачити з приведених результатів (рис. 2), при використанні отриманих оптимальних стратегій гарантований рівень ймовірності забезпечення захисту окремої функції серверу в умовах зосередженої кібератаки на кінець умовного періоду розгляду складає 0.73. В той же час, імовірність відмови серверу по окремій функціональності рівна 0.06. При відхиленні гравців-учасників інформаційного конфлікту від оптимальних стратегій відповідним чином зміняться значення ймовірностей станів, проте значення плати не відповідатиме мінімальному.

Приведені графіки ілюструють динаміку протікання інформаційного конфлікту в розглядуваній системі в умовах здійснення атаки на виділену функцію багатозадачного серверу дистанції електропостачання залізниці. Моделювання процесу кібератаки виконано, для оцінки інтегральних показників захищеності серверу на основі (2), (3) та (6), при використанні оптимальних стратегій (36) по кожній із функцій.

На рис. 3 приведені графіки перехідних процесів ймовірності перебування серверу в захищеному стані та ймовірності відмови серверу по будь-якій із функціональностей.

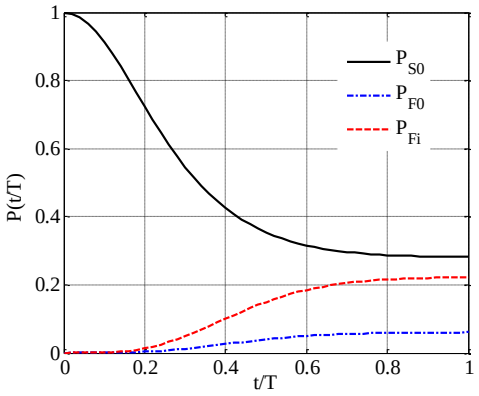

Рис. 3. **Графіки перехідних процесів ймовірностей станів інформаційної системи при реалізації кібернападу на загальну функціональність сервера**

Як можна бачити з приведених результатів (рис. 3), при використанні отриманих оптимальних стратегій гарантований рівень захищеності серверу в умовах кібератак на кінець умовного періоду розгляду складає 0.28. В той же час, імовірність відмови серверу по будь-якій із функцій досягає 0.22.

Висновки. Проведено дослідження застосування методів диференціально-ігрового моделювання процесів кібернападу та захисту інформації розширено на спеціалізовані

інформаційно-діагностичні та керуючі комп'ютерні системи транспортної інфраструктури, а саме залізниці, для яких ставляться підвищені вимоги відносно надійності, інформаційної безпеки та безперебійної роботи. Розроблено диференціально-ігрову модель процесу кібернападу на мультизадачний сервер інформаційно-діагностичної комп'ютерної системи нижнього рівня залізниці, яка дозволяє отримати оптимальні стратегії захисту інформації в умовах кібератак.

В статті отримано графіки що ілюструють динаміку протікання інформаційного конфлікту в розглядуваній системі в умовах здійснення атаки на виділену функцію багатозадачного серверу. Виконано моделювання процесу кібератаки, для оцінки інтегральних показників захищеності серверу дистанції електропостачання залізниці, при використанні оптимальних стратегій по кожній із функцій. Показано вигляд моделі комп'ютерно-інформаційної діагностичної системи, та приведені графіки перехідних процесів ймовірності перебування серверу в захищеному стані та ймовірності відмови серверу дистанції електропостачання залізниці по будь якій із функціональностей, що не може забезпечити безперебійну роботу залізничного транспорту.

Результати роботи можуть бути використані при формуванні планових заходів технічного обслуговування існуючих, мікропроцесорних пристроїв та систем транспортної інфраструктури, які мають аналогічну модульну структуру, а також, для оцінки показників надійності і відповідної корекції, на етапі розробки систем, для безперебійної роботи транспорту.

ЛІТЕРАТУРА

1. Калинюк І. О. Організація корпоративної системи моніторингу та діагностики тягових електричних мереж // Зб. наук. праць ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. 2011. № 61. С. 37-41.
2. Aminifar F., Fotuhi-Firuzabad M., Safdarian A., Davoudi A., and Shahidehpour M. Synchrophasor measurement technology in power systems: Panorama and state-of-the-art // Access, IEEE. 2014. Vol. 2. P. 1607-1628. DOI: 10.1109/ACCESS.2015.2389659.
3. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. [Чинний від 1999-05-28]. Київ: адміністрація Держспецзв'язку, 1999. С. 26.
4. Воронко І. О. Основні проблеми вразливості WAMS та відповідні принципи захисту систем моніторингу та діагностики // Modern directions of scientific research development: the 4 th International scientific and practical conference Chicago, September 28-30, 2021. Chicago, USA: BoScience Publisher, 2021. С 128-131.
5. Воронко І. О. Захист інформації в комп'ютерних системах і мережах на основі теорії ігор // Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: мат. всеукр. наук.-практ. інтернет-конф., м. Черкаси 18-22 березня 2013 р. Черкаси, 2013. С. 54-57.
6. Воронко І. О. Застосування методів теорії ігор для моделювання процесів нападу на інформацію в промислових комп'ютерних системах та мережах // Проблемы экономики и управления на железнодорожном транспорте: мат. VIII межд. науч.-практ. конф., г. Судак 08-11 октября 2013 г., г. Судак, АР Крым, 2013. С. 256-258.
7. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія. Житомир: Рута, 2010. 280 с.
8. Вентцель Е. С. Исследование операций: Задачи, принципы, методология [2-е изд.]. М.: Наука, 1988. 208 с.
9. Manshaei M., Zhu Q. and Alpcan T. Basar, T., & Hubaux, J. P. Game theory meets network security and privacy // ACM Computing Surveys. 2013. Vol. 48. P. 51-61. DOI: https://doi.org/10.1145/2480741.2480742
10. Lin, Wei. Differential Games For Multi-agent Systems Under Distributed Information// Electronic Theses and Dissertations, University of Central Florida, 2013. 128 P. URL: http://digital.library.ucf.edu/cdm/ref/collection/ETD/id/5973 (дата звернення 2.11.2021).
11. Грищук Р.В. Корченко О. Г. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси // Захист інформації. 2012. № 3. С. 115-122.
12. Грабар І. Г. Р. В. Грищук, К. В. Молодецька. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія; за заг. ред. д.т.н., проф. Р. В. Грищука. Житомир : ЖНАЕУ, 2019. 280 с.
13. Воронко І. О. Диференціально-ігрова модель надійності мікропроцесорних систем моніторингу тягових електричних мереж // Інформаційно-керуючі системи на залізничному транспорті. Х.: УкрДАЗТ, 2013. № 5. С. 8-15.
14. Стасюк О. І., Баранов В. Л., Баранов Г. Л., Фролова О. Г. Диференціальні перетворення для комп'ютерного моделювання керуючих систем: [навч. посібн. для студ. вищ. навч. закл.]. К.: КУЕТТ, 2005. 135 с.
15. Stasiuk A. I., Hryshchuk R. V., Goncharova L. L. A Mathematical Cybersecurity Model of a Computer Network for the Control of Power Supply of Traction Substations //Cybernetics and Systems Analysis. 2017. Vol 53. P 476–484. DOI:https://doi.org/10.1007/s10559-017-9949-z
16. Zhi Li, Haitao Xu, Yanzhu Liu. A differential game model of intrusion detection system in cloud computing // International Journal of Distributed Sensor Networks. 2017. Vol. 13(1). DOI: https://doi.org/10.1177/1550147716687995
17. Пухов Г. Е. Дифференциальные спектры и их модели. К.: Наук. думка, 1990. 184 с.
18. Пухов Г.Е. Дифференциальные преобразования функций и уравнений. К.: Наук. думка, 1984. 420 с.

REFERENCES

1. Kalyniuk I. O. (2011). Orhanizatsiia korporatyvnoi systemy monitorynhu ta diahnostyky tiahovykh elektrychnykh merezh [Organization of corporate system of monitoring and diagnostics of traction electric networks] // *Zb. nauk. prats in-tu problem modeliuvannia v enerhetytsi im. H.Ie. Pukhova NAN Ukrainy*, 61. 37-41. [in Ukrainian].

2. Aminifar F., Fotuhi-Firuzabad M., Safdarian A., Davoudi A., and Shahidehpour M. (2014) Synchrophasor measurement technology in power systems: Panorama and state-of-the-art // *Access, IEEE,* 2. 1607-1628. DOI: 10.1109/ACCESS.2015.2389659.

3. Tekhnichnyi zakhyst informatsii na prohramno-kerovanykh ATS zahalnoho korystuvannia. Osnovni polozhennia [Technical protection of information on software-controlled public PBXs. Substantive provisions] (1999). *ND T3I 1.1-001-99 from 28th May 1999.* Kyiv: administratsiia Derzhspetszviazku. [in Ukrainian].

4. Voronko I. O. (2021) Osnovni problemy vrazlyvosti WAMS ta vidpovidni pryntsypy zakhystu system monitorynhu ta diahnostyky [The main problems of WAMS vulnerability and the corresponding principles of protection of monitoring and diagnostic systems]// *Modern directions of scientific research development:* the 4 th International scientific and practical conference (128-131) Chicago, USA: BoScience Publisher. [in Ukrainian].

5. Voronko I. O. (2013) Zakhyst informatsii v kompiuternykh systemakh i merezhakh na osnovi teorii ihor [Information security in computer systems and networks based on game theory] // *Avtomatyzatsiia ta kompiuterno-intehrovani tekhnolohii u vyrobnytstvi ta osviti: stan, dosiahnennia, perspektyvy rozvytku*: mat. vseukr. nauk.-prakt. internet-konf., (54-57). Cherkasy. [in Ukrainian].

6. Voronko I. O. (2013) Zastosuvannia metodiv teorii ihor dlia modeliuvannia protsesiv napadu na informatsiiu v promyslovykh kompiuternykh systemakh ta merezhakh [Application of game theory methods for modeling information attack processes in industrial computer systems and networks] // *Problemы эkonomyky y upravlenyia na zheleznodorozhnom transporte:* mat. VIII mezhd. nauch.-prakt. konf., (256-258) h. Sudak, AR Krыm. [in Ukrainian].

7. Hryshchuk R. V. (2010) Teoretychni osnovy modeliuvannia protsesiv napadu na informatsiiu metodamy teorii dyferentsialnykh ihor ta dyferentsialnykh peretvoren [Theoretical bases of modeling of processes of attack on information by methods of theories of differential games and differential transformations]: *monohrafiia*. Zhytomyr: Ruta. 280. [in Ukrainian].

8. Venttsel E. S. (1988) Yssledovanye operatsyi: Zadachy, pryntsypы, metodolohyia [Operations research: Tasks, principles, methodology]. M.: Nauka. 208. [in Russian].

9. Manshaei M., Zhu Q. and Alpcan T. Basar, T., & Hubaux, J. P. (2013) Game theory meets network security and privacy// *ACM Computing Surveys, 48.* 51-61. DOI: https://doi.org/10.1145/2480741.2480742.

10. Lin, Wei (2013). Differential Games For Multi-agent Systems Under Distributed Information// *Electronic Theses and Dissertations*.128. Retrieved from URL: http://digital.library.ucf.edu/cdm/ref/collection/ETD/id/5973.

11. Hryshchuk R.V. Korchenko O. H. (2012) Metodolohiia syntezu ta analizu dyferentsialno-ihrovykh modelei ta metodiv modeliuvannia protsesiv kibernapadu na derzhavni informatsiini resursy [Methodology of synthesis and analysis of differential game models and methods of modeling cyberattack processes on state information resources] // *Zakhyst informatsii*, 3. 115-122. [in Ukrainian].

12. Hrabar I. H. R. V. Hryshchuk, K. V. Molodetska (2019) Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty [Security synergetics: cybernetic and informational aspects]: *monohrafiia; za zah. red. d.t.n., prof. R. V. Hryshchuka*. Zhytomyr: ZhNAEU. 280. [in Ukrainian].

13. Voronko I. O. (2013) Dyferentsialno-ihrova model nadiinosti mikroprotsesornykh system monitorynhu tiahovykh elektrychnykh merezh [Differential game model of reliability of microprocessor monitoring systems of traction electric networks]// *Informatsiino-keruiuchi systemy na zaliznychnomu transporti.* Kh.: UkrDAZT, 5. 8-15. [in Ukrainian].

14. Stasiuk O. I., Baranov V. L., Baranov H. L., Frolova O. H. (2005) Dyferentsialni peretvorennia dlia kompiuternoho modeliuvannia keruiuchykh system [Differential transformations for computer modeling of control systems]: *navch. posibn. dlia stud. vyshch. navch. zakl.* K.: KUETT. 135. [in Ukrainian].

15. Stasiuk A. I., Hryshchuk R. V., Goncharova L. L. (2017) A Mathematical Cybersecurity Model of a Computer Network for the Control of Power Supply of Traction Substations //*Cybernetics and Systems Analysis, 53*. 476–484. DOI: https://doi.org/10.1007/s10559-017-9949-z.

16. Zhi Li, Haitao Xu, Yanzhu Liu. (2017) A differential game model of intrusion detection system in cloud computing // *International Journal of Distributed Sensor Networks, 13(1).* DOI: https://doi.org/10.1177/1550147716687995

17. Pukhov H. E. (1990) Dyfferentsyalnыe spektrы y ykh modely [Differential spectra and their models]. K.: Nauk. dumka.184. [in Russian].

18. Pukhov H.E. (1984) Dyfferentsyalnыe preobrazovanyia funktsyi y uravnenyi[Differential transformations of functions and equations]. K.: Nauk. dumka. 420. [in Russian].

***Iryna Voronko*[1]**

[1]*Senior Lecturer, Department of automation and computer-integrated transport technologies, State University of Infrastructure and Technologies, 9, Kyrylivska str., Kyiv, 04071, Ukraine*

DIFFERENTIAL-GAME MODEL OF INFORMATION PROTECTION FOR COMPUTER SYSTEMS OF TRANSPORT INFRASTRUCTURE

The article considers the reliability and protection of information of computer systems of transport infrastructure and describes the synthesis and analysis of differential game models and methods of modeling cyberattack processes on the server of computer information and diagnostic systems of the railway power supply distance. A unified differential-game model of the cyberattack process on the multi-task server of the information-diagnostic computer system of the lower level of the railway has been developed, which allows to obtain optimal strategies for information protection in cyberattacks. The results of modeling the cyberattack process are presented, to assess the integrated indicators of server security, using the optimal strategies for each of the functions. The appearance of the unified model of the computer information system is shown, and the graphs of the transient processes of the probability of the server being in a protected state and the probability of server failure for any of the functionalities are given.

Keywords: *information security, cyberattack, cybersecurity strategy, cyberattack strategy, differential game models, graph model.*