УДК 621.396 + 654.16 : 517.978.2

к.т.н. Шевченко А.С. (ВІТІ)
Артюх С.Г. (ВІТІ)

МЕТОД ОЦІНКИ ІМОВІРНОСТІ ЗБИТКУ ВНАСЛІДОК РЕАЛІЗАЦІЇ АТАК РАДІОЕЛЕКТРОННОГО ПРИДУШЕННЯ РАДІОЛІНІЙ ВІЙСЬКОВИХ СИСТЕМ РАДІОЗВ'ЯЗКУ В ХОДІ ПРОВЕДЕННЯ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

В статті викладено метод оцінки імовірності збитку внаслідок реалізації атак радіоелектронного придушення радіоліній військових систем радіозв'язку в ході проведення інформаційних операцій, з застосуванням теорій диференціальних ігор та диференціальних перетворень Пухова Г.Е.

Шевченко А.С., Артюх С.Г. Метод оценки вероятности ущерба вследствие реализации атак радиоэлектронного подавления радиолиний военных систем радиосвязи в ходе проведения информационных операций. *В статье представлено метод оценки вероятности ущерба вследствие реализации атак радиоэлектронного подавления радиолиний военных систем радиосвязи во время проведения информационных операций, с использованием теорий дифференциальных игр и дифференциальных преобразований Пухова Г.Е.*

A. Shevchenko, S. Artykh. The method of estimating the probability of damage as a result of the implementation electronic warfare attacks on military radio communication systems during the informations operations. *In the article the method of assessing the probability of loss as a result of the suppression of electronic warfare attacks of the military radio communication systems in the course of information operations, the used a differential game and differential transformations of Puhov G.E. theories.*

Ключові слова: *імовірність збитку, радіоелектронне придушення, військові системи радіозвязку, інформаційні операції.*

Вступ. Складовою частиною ведення інформаційних операцій є радіоелектронна боротьба (РЕБ), однією з функцій якої є радіоелектронне придушення (РЕП) радіоліній військових систем радіозв'язку (СРЗ).

Заходи РЕБ, в контексті інформаційних операцій, застосовуються для оперативного забезпечення ведення бойових дій. Згідно з концепціями ведення інформаційних операцій розвинутих країн світу атаки РЕП здійснюються для виведення з ладу на час проведення операцій радіонапрямків та радіомереж СРЗ збройних сил (ЗС), інших збройних формувань в загрозливий період та під час військового конфлікту. Зважаючи на те, що безпроводова компонента складає значну частину інформаційно-телекомунікаційної системи ЗС України, їх критичність та доступність середовища розповсюдження, захист військових СРЗ під час інформаційних конфліктів є актуальним на сьогоднішній час [1 − 6].

Важливою перевагою атак РЕП є їх дистанційна реалізація. Встановлення радіоелектронних завад здебільшого не вимагає проникнення в периметр, що знаходиться під охороною та розміщено СРЗ. Радіоелектронні завади придушують приймач СРЗ та блокують прийом інформації через радіоканал. Внаслідок цього здійснення інформаційного обміну та управління через СРЗ унеможливлюється [7 − 8].

В ході проведення антитерористичної операції на сході України Російська Федерація (РФ) досить активно використовує засоби РЕБ. Так під час бойових дій були зафіксовані автоматизовані станції завад Р-330Ж „Житель". РФ має потужну систему РЕБ, яка включає велику кількість зразків засобів РЕБ, радіо/радіотехнічної розвідки (РРТР). До основних засобів РЕБ, що призначенні для придушення СРЗ відносяться: Р-330 Т(У), Р-378А, РП-377Л(ЛА), Р-934Б, Леєр-2 та інші. Таким чином аналіз досвіду бойових дій та порушника (противника) показав, що реалізація атак РЕП радіоліній СРЗ залишається однією з основних загроз для радіозв'язку.

Аналіз останніх досліджень та публікацій. Останні тенденції ведення інформаційних операцій найбільш розвинутими державами показує, що РЕБ, наряду з кібернетичними операціями, залишається найбільш дієвим засобом боротьби в ході бойових дій [1, 5, 7]. З часом модернізуються методи ведення РЕБ та засоби їх реалізації. РЕП, як одна зі складових РЕБ, залишається найбільшою загрозою для СРЗ.

Одним зі складових заходів інформаційної боротьби є захист власних систем. Захист СРЗ вимагає володіння інформацією про характер загроз та можливий сценарій перебігу інформаційного конфлікту. Для спостереженням за ходом інформаційного конфлікту необхідно оцінювати атаки противника (порушника) на СРЗ та дієвість їх механізмів захисту інформації (МЗІ).

Для оцінки рівня інформаційної безпеки, на сьогоднішній час, здебільшого використовують методи оцінки ризиків [9]. Оцінювання ризиків є ключовим етапом процесу управління інформаційною безпекою. Найбільш розповсюдженими методами оцінки ризиків є методи: COBRA, CRAMM, RA2, OCTAVE, RiskWatch тощо. В даних методах при оцінці ризиків не враховується динаміка протікання інформаційного конфлікту, зміни типів атак та їх параметрів в реальному часі [10, 11].

На сьогоднішній час методи оцінювання ризиків здебільшого спираються на методи, що основані на врахуванні імовірності загроз ($P_{\text{загр}}$) та імовірності збитків ($P_{\text{зб}}$) [12]. Методи, які грунтуються на другому підході більш повно оцінюють рівень ризику, адже враховують і наявні вразливості систем, що не здійснюється у разі застосування для оцінки ризиків лише імовірності загроз. Таким чином, для оцінки ризиків військових СРЗ доцільно використовувати методи з урахування імовірності збитків.

Для оцінки імовірності збитків у сучасних методах оцінки ризиків використовуються два основних підходи: статистичний та на основі експертних оцінок. Обидва методи мають ряд переваг та недоліків, але обидва методи не пристосовані до динамічних змін у ході інформаційних операцій та вимагатимуть переоцінки усіх загроз.

Мета. З аналізу сучасного стану інформаційної безпеки, існуючих загроз, в ході РЕП під час бойових дій, постає питання захисту СРЗ, які б могли функціонувати в динамічних умовах впливу інформаційних атак – інформаційних конфліктах. Першочерговим є захист СРЗ військових формувань. Для цього, необхідно отримувати інформацію про характер протікання інформаційного конфлікту та ефективність роботи МЗІ в ході конфронтації.

Метою даної роботи є розробка методу оцінки імовірності збитку внаслідок реалізації атак РЕП радіоліній військових систем радіозв'язку в ході проведення інформаційних операцій, який буде дозволяти здійснювати оцінку імовірності збитку з можливістю урахування динаміки змін стратегій протиборчих сторін та визначення їх мінімальних необхідних інтенсивностей.

Постановка завдання. Завданням дослідження є моделювання атаки РЕП та захисних дій МЗІ СРЗ. Для відображення інформаційної боротьби слід побудувати шаблон нормальної поведінки (ШНП) СРЗ, який буде відображати оптимальний стан − рівновагу між платою порушника та МЗІ.

Початкові умови. Розглядається ситуація рівноімовірнісного знаходження СРЗ у крайніх станах моделі протікання інформаційного конфлікту відповідно до моделі загроз {*S*, Г} [13]. Інформаційний конфлікт описується імовірностями перебування СРЗ у різних станах інформаційного конфлікту $P_z(t)$ та стратегіями протиборчих сторін, що характеризуються функціями зміни інтенсивності дій – $\lambda_i(t)$, $\mu_j(t)$. В один і той же час t існують як атаки на СРЗ, так і самі СРЗ використовують механізми захисту від РЕП.

Необхідно. Визначити значення інтенсивності захисту та атаки при умові рівноваги гри ($\lambda_{i\max}^{\text{opt}}$, $\mu_{j\min}^{\text{opt}}$), отримати диференціально-ігрову модель шаблону нормальної поведінки $P_0(t)$ та провести імітаційне моделювання інформаційного конфлікту при різних стратегіях гравців, розрахувати ціну гри I^G (інформаційного конфлікту).

Обмеження. Розглядаються навмисні штучні атаки РЕП, що є загрозами для фізичного та канального рівнів СРЗ, ціна гри обмежена значеннями $I^G{}_{\min} \le I^G \le I^G{}_{\max}$, інтенсивності гравців знаходяться в межах $0 \le \lambda_i(t) \le \lambda_{i\max}(t)$ та $0 \le \mu_j(t) \le \mu_{j\max}(t)$. Здійснюється розгляд розвитку інформаційного конфлікту протягом однієї доби (Δt = 24 години).

Допущення. Атаки реалізуються послідовно, реалізація етапів атак є несумісними подіями, інтенсивності гравців змінюються за лінійними законами $\lambda_i(t) = \lambda_i \cdot t$ та $\mu_j(t) = \mu_j \cdot t$, $i \wedge j \in [0, 3]$.

Викладення основного матеріалу дослідження. Методи реалізації атак РЕП залежать від володіння інформацією про СРЗ протиборчої сторони, параметрів її радіосигналів, що отримуються від радіотехнічної розвідки. Порушник може встановити перешкоду СРЗ при знанні цих параметрів, чи без такого [7, 8].

Важливою особливістю атак РЕП є можливість їх віддаленої реалізації, в основному без доступу до охороняємого периметра, де знаходиться СРЗ. Обмеження застосування атак вносять особливості розповсюдження радіохвиль діапазонів частот окремих стандартів і видів СРЗ та ресурси порушника.

Наслідками реалізації атак РЕП на СРЗ є порушення цілісності та доступності інформації. Цілісність інформації порушується внаслідок виникнення помилок у сигналі, втрати частини сигналу внаслідок втрати синхронізації між передавачем та приймачем. Порушення доступності полягає в неможливості отримання інформації, яка передається через радіоканал СРЗ, на які здійснено атаку РЕП.

При розробці захищених СРЗ постає питання вибору засобів захисту, які б надійно захищали від порушення конфіденційності, цілісності та доступності інформації, що передається через радіоканали. Для цього необхідно визначитись з вимогами до механізмів захисту та провести моделювання процесів «атака-захист».

Для проведення моделювання процесів атак та захисту пропонується використовувати диференціально-ігрове моделювання з застосуванням методу диференційних перетворень академіка Пухова Г.Є. [14, 15]. Застосування диференційних перетворень дасть змогу відійти від диференціальних рівнянь та дозволить оперувати лінійними рівняннями, при вирішенні задач диференціально-ігрового моделювання.

Розглянемо більш детально атаку РЕП радіоліній та представимо її у вигляді графа нормальної поведінки СРЗ під час інформаційної боротьби (рис.1).

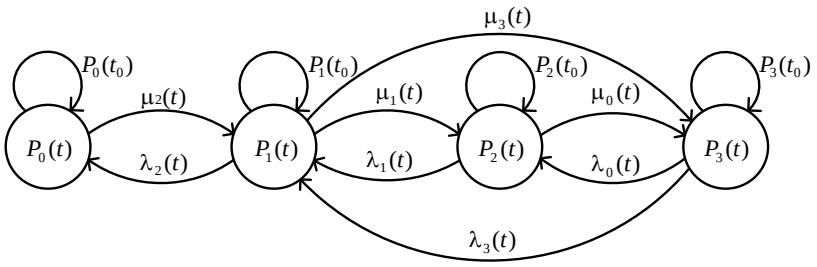


Рис. 1. Граф моделі шаблону нормальної поведінки СРЗ при реалізації атаки РЕП радіолінії

Кола представляють собою множину станів $\{P_z(t)\}$, де z = 0…3 – стани, у яких може перебувати СРЗ під час інформаційної боротьби з відповідними імовірностями. Стрілки між станами відображають результат виникнення переваги дій порушника над механізмами захисту та протилежні результати.

Граф складається з чотирьох станів (справа наліво, див. рис. 1) [13]:

− захищеності СРЗ (відображає функціонування СРЗ з ефективною роботою механізмів захисту);

− перехоплення радіосигналів (радіотехнічна розвідка);

− РЕП радіолінії СРЗ;

− отримання збитку від РЕП СРЗ (отримано збитків від порушення цілісності і доступності інформації внаслідок РЕП).

Інтенсивності потоків атак порушника та захисних дій МЗІ СРЗ для інформаційного конфлікту на основі РЕП представлені в таблиці 1.

Нехай СРЗ у довільний проміжок часу $t \in [t_0, T]$ інформаційного конфлікту перебуває в одному з трьох станів з відповідними імовірностями:

$P_0(t)$ – імовірність успішного РЕП СРЗ, що призведе до отримання збитків;

$P_1(t)$ – імовірність здійснення РЕП радіолінії СРЗ;

$P_2(t)$ – імовірність попереднього перехоплення випромінювання радіосигналу та визначення його параметрів;

$P_3(t)$ – імовірність перебування СРЗ у стані захищеності, відсутності РЕБ.

Таблиця 1

Визначення інтенсивностей атак та захисних дій МЗІ

Інтенсивність			
атак порушника		*захисних дій МЗІ*	
$\lambda_0(t)$	– перехоплення радіосигналу;	$\mu_0(t)$	- захист від перехоплення радіосигналу;
$\lambda_1(t)$	– придушення радіолінії СРЗ;	$\mu_1(t)$	- захист від придушення радіолінії СРЗ;
$\lambda_2(t)$	отримання збитків від атак;	$\mu_2(t)$	- захисні дії по зміні МЗІ (на етапі проектування);
$\lambda_3(t)$	– придушення радіолінії без попередньої радіотехнічної розвідки.	$\mu_3(t)$	- захисні дії, що примусять порушника заново проводити радіотехнічну розвідку.

Дана послідовність випадкових подій є колом Маркова з двома вихідними станами [16].

Запропонована графова модель ШНП враховує всі можливі переходи СРЗ між станами під час інформаційної боротьби зі здійсненням РЕП, враховує зміни стратегій порушника та МЗІ (далі сторін або гравців).

Саме стратегії конфліктуючих сторін визначають яким буде наслідок протистояння.

Для відображення динаміки протікання процесу атаки придушення радіолінії СРЗ під час інформаційного конфлікту на інтервалі $\overline{t_0, T}$, з урахуванням переходів між станами графа (рис. 1), застосуємо систему диференціальних рівнянь Колмогорова-Чепмена [16]:

$$\begin{cases} \dfrac{\partial P_0(t)}{\partial t} = -\mu_2(t)P_0(t) + \lambda_2(t)P_1(t) \\ \dfrac{\partial P_1(t)}{\partial t} = -(\lambda_2(t) + \mu_1(t) + \mu_3(t))P_1(t) + \mu_2(t)P_0(t) + \lambda_1(t)P_2(t) + \lambda_3(t)P_3(t) \\ \dfrac{\partial P_2(t)}{\partial t} = -(\lambda_1(t) + \mu_0(t))P_2(t) + \mu_1(t)P_1(t) + \lambda_0(t)P_3(t) \\ \dfrac{\partial P_3(t)}{\partial t} = -(\lambda_0(t) + \lambda_3(t))P_3(t) + \mu_0(t)P_2(t) + \mu_3(t)P_1(t). \end{cases} \quad (1)$$

Система рівнянь (1) дозволить визначити розподіл імовірностей знаходження СРЗ в кожному стані множини $\{P_z(t)\}$ на протязі інформаційного конфлікту з урахуванням поведінки порушника та МЗІ.

В реальних обставинах зміна стратегій сторін обумовлюється багатьма чинниками, які здебільшого врахувати немає можливості, припустимо, що інтенсивності сторін в ході боротьби змінюються за лінійним законом. Тоді,

$$\lambda_i(t) = \lambda_i \cdot t \quad (2)$$

та

$$\mu_j(t) = \mu_j \cdot t, \quad (3)$$

де λ_i та μ_j – параметри законів розподілу стратегій гравців, t – час інформаційного конфлікту РЕП; i, j – кількість переходів між станами в результаті успішних атак порушника та внаслідок дії МЗІ відповідно, причому $i \wedge j \in [0, z-1]$.

Ресурси гравців визначені та обмежені їх стратегіями (2) − (3). Для порушника вони знаходяться в межах

$$\lambda_{i\min}(t) \le \lambda_i(t) \le \lambda_{i\max}(t). \quad (4)$$

Інтенсивності механізмів захисту, при протидії РЕП СРЗ, змінюються в межах

$$\mu_{j\min}(t) \le \mu_j(t) \le \mu_{j\max}(t). \quad (5)$$

Параметри керування гравців $\lambda_i(t)$ та $\mu_j(t)$, які визначають ресурси сторін гри лежать в межах замкнутих множин $\Lambda \in \mathrm{K}_\lambda$ та $\mathrm{M} \in \mathrm{K}_\mu$, які в свою чергу обмежені евклідовими просторами E_λ і E_μ відповідно [8].

В ході атаки РЕП радіолінії СРЗ гравець (порушник) намагається завдати максимальних втрат іншому гравцю (МЗІ). Під час цього він маневрує власними ресурсами та намагається мінімізувати особисті втрати при максимізації втрат іншого суб'єкта.

Розгляд процесів нападу на СРЗ та захисту від цих атак відповідає диференційно-ігровому підходу з безкоаліційним характером ведення гри [17].

Під час інформаційної боротьби при здійсненні заходів РЕП кожна із сторін цієї гри намагається завдати іншій найбільших втрат. Порушник намагається за допомогою штучних радіозавад придушити радіолінію СРЗ по якій здійснюється передача інформації. Це призведе до порушення цілісності інформації, що передавалась безпосередньо в час встановлення завади, чи до порушення доступності ресурсів каналів зв'язку СРЗ, тим самим завдавши збитків. Гравець, що захищається, намагається наявними МЗІ протистояти атакам з боку порушника, та зберегти власні активи.

В результаті, стратегії гравців є протилежними.

Порушник – максимізує плату $I(t, P_0(t), \lambda_i(t), \mu_j(t))$ при мінімізації власних втрат під час нанесення атак [14]:

$$\max_{\lambda_i(t)\in \mathrm{E}_\lambda} \min_{\mu_j(t)\in \mathrm{E}_\mu} = I\left(t, P_0(t), \lambda_i(t), \mu_j(t)\right). \quad (6)$$

Гравець, що захищається (МЗІ) – мінімізує плату $I(\mathrm{t}, P_0(t), \lambda_i(t), \mu_j(t))$ за умови її максимізації іншим гравцем [14]:

$$\min_{\mu_j(t)\in \mathrm{K}_\mu} \max_{\lambda_i(t)\in \mathrm{K}_\lambda} = I\left(t, P_0(t), \lambda_i(t), \mu_j(t)\right), \quad (7)$$

де $I\left(t, P_0(t), \lambda_i(t), \mu_j(t)\right) = I$ − плата, що є усередненою імовірністю перебування СРЗ у стані впливу РЕП.

При рівності плат гравців (6) та (7):

$$\begin{aligned} &\max_{\lambda_i(t)\in \mathrm{E}_\lambda} \min_{\mu_j(t)\in \mathrm{E}_\mu} = I\left(t, P_0(t), \lambda_i(t), \mu_j(t)\right) = \\ &= \min_{\mu_j(t)\in \mathrm{K}_\mu} \max_{\lambda_i(t)\in \mathrm{K}_\lambda} = I\left(t, P_0(t), \lambda_i(t), \mu_j(t)\right) = \\ &= I\left(t, P_0^{opt}(t), \lambda_i^{opt}(t), \mu_j^{opt}(t)\right) = I^{\mathrm{G}}, \end{aligned} \quad (8)$$

стратегії $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$ є оптимальними для цієї гри, а $P_0^{opt}(t)$ – оптимальна траєкторія, яка розраховується з системи (1) за критерієм (6), і представляє собою диференційно-ігрову модель ШНП СРЗ для порушника в ході радіорозвідки.

Гарантований рівень захищеності СРЗ досягається вибором гравців оптимальних стратегій $\lambda_i^{opt}(t)$ та $\mu_j^{opt}(t)$:

$$I\left(t, P_0^{opt}(t), \lambda_i^{opt}(t), \mu_j^{opt}(t)\right) = I^{\mathrm{G}} \tag{9}$$

при цьому ціна I^G – ціна гри.

Для динамічного інформаційного конфлікту плата I матиме інтегральний вигляд, та відносно $P_0(t)$ розраховується за виразом [14]:

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

де $0 \le I \le I_{\max}$, $I_{\max}$= 1.

Інтегрування здійснюється протягом всієї гри від моменту початку t_0 = 0 до моменту закінчення $t_0 = T$ інформаційного конфлікту. Якщо будь-який гравець відхилиться від оптимальної стратегії, то це призведе до втрат у платі.

Знаходження диференційно-ігрової моделі ШНП СРЗ $P_0^{opt}(t)$ здійснимо за загальною методологією, що представлена в монографії [14] з використанням P-перетворень академіка Пухова Г.Є. [15].

Перейдемо в область зображень, для чого використаємо пряме диференційне перетворення [15]. В результаті інформаційний конфлікт, що описаний системою (1), в області P-зображень матиме вигляд:

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}(-\mathrm{M}_2(k)P_0(k) + \Lambda_2(k)P_1(k)); \\ P_1(k+1) = \dfrac{T}{k+1}(-(\Lambda_2(k) + \mathrm{M}_1(k) + \mathrm{M}_3(k))P_1(k) + \mathrm{M}_2(k)P_0(k) + \\ \qquad\qquad + \Lambda_1(k)P_2(k) + \Lambda_3(k)P_3(k)); \\ P_2(k+1) = \dfrac{T}{k+1}(-(\Lambda_1(k) + \mathrm{M}_0(k))P_2(k) + \mathrm{M}_1(k)P_1(k) + \Lambda_0(k)P_3(k)); \\ P_3(k+1) = \dfrac{T}{k+1}(-\left(\Lambda_0(k) + \lambda_3(k)\right)P_3(k) + \mathrm{M}_0(k)P_2(k) + \mathrm{M}_3(k)P_1(k)). \end{cases} \tag{11}$$

де $P_z(k)$, $\Lambda_i(k)$, $\mathrm{M}_j(k)$ – диференційні зображення оригіналів функцій $P_z(t)$, $\lambda_i(t)$, $\mu_j(t)$ відповідно, і дискретними функціями цілочислового аргументу k = 0, 1, 2… .

Внаслідок динаміки інформаційного конфлікту та прийнятого допущення, стратегії гравців в ході інформаційного протистояння змінюються за лінійними законами (2)–(3), тобто є функціями. В результаті, при переході в область P-зображень необхідно врахувати властивості T-добутків диференційних зображень $\Lambda_i(k) * P_z(k)$ та $\mathrm{M}_j(k) * P_z(k)$ [15].

Вказані T-добутки матимуть вигляд для всіх $k \ge 1$:

$$\Lambda_i(k) * P_z(k) = \lambda T \cdot P_z(k-1), \tag{12}$$

$$\mathrm{M}_j(k) * P_z(k) = \mu T \cdot P_z(k-1)\,. \tag{13}$$

З урахуванням перетворень добутків в області зображень (12) – (13), система диференціальних рівнянь Колмогорова-Чепмена для атаки РЕП радіолінії матиме вигляд:

$$\begin{cases} P_0(k+1) = \dfrac{T^2}{k+1}\left(-\mu_2 P_0(k-1) + \lambda_2 P_1(k-1)\right); \\ P_1(k+1) = \dfrac{T^2}{k+1}\left(-(\lambda_2+\mu_1+\mu_3)P_1(k-1) + \mu_2 P_0(k-1) + \lambda_1 P_2(k-1) + \lambda_3 P_3(k-1)\right); \\ P_2(k+1) = \dfrac{T^2}{k+1}\left(-(\lambda_1+\mu_0)P_2(k-1) + \mu_1 P_1(k-1) + \lambda_0 P_3(k-1)\right); \\ P_3(k+1) = \dfrac{T^2}{k+1}\left(-(\lambda_0+\lambda_3)P_3(k-1) + \mu_0 P_2(k-1) + \mu_3 P_1(k-1)\right). \end{cases} \quad (14)$$

Визначимо дискрети диференціального спектра диференційно-ігрової моделі ШНП СРЗ під час РЕП. Для знаходження дискрет послідовно присвоюємо цілочислові значення аргументу *k*.

Врахуємо початкові умови : $P_3(t) = P_0(t) = 0{,}5$, $P_1(t) = P_2(t) = 0$. В результаті визначимо дискрети для $P_0(k)$:

$$P_0(1) = P_0(3) = P_0(5) = 0, \quad (15)$$

$$P_0(2) = -\frac{T^2}{4}\mu_2, \quad (16)$$

$$P_0(4) = \frac{T^4}{16}\left(\mu_2{}^2 + \lambda_2\mu_2\right), \quad (17)$$

$$P_0(6) = -\frac{T^6}{96}(\mu_2{}^3 + \mu_2{}^2 + \lambda_2\mu_2{}^2 + \lambda_2{}^2\mu_2 + \lambda_2{}^2\lambda_3 + \lambda_2\mu_1\mu_2 + \\ + \lambda_2\lambda_3\mu_1 + \lambda_2\mu_2\mu_3 + \lambda_2\lambda_3\mu_3 - \lambda_0\lambda_1 + \lambda_0\lambda_3 + \lambda_3{}^2 - \lambda_3\mu_3). \quad (18)$$

Для отримання плати гри в області зображень підставимо дискрети (15) − (18) в (10). В результаті підстановки вираз (10) матиме вигляд в якості ряду плати гри:

$$I_1 = \sum_{k=0}^{k=\infty}\frac{P_0(k)}{k+1} = \frac{1}{2} - \frac{T^2}{12}\mu_2 + \frac{T^4}{80}\left(\mu_2{}^2 + \lambda_2\mu_2\right) - \frac{T^6}{672}(\mu_2{}^3 + \mu_2{}^2 + \lambda_2\mu_2{}^2 + \lambda_2{}^2\mu_2 + \\ + \lambda_2{}^2\lambda_3 + \lambda_2\mu_1\mu_2 + \lambda_2\lambda_3\mu_1 + \lambda_2\mu_2\mu_3 + \lambda_2\lambda_3\mu_3 - \lambda_0\lambda_1 + \lambda_0\lambda_3 + \lambda_3{}^2 - \lambda_3\mu_3). \quad (19)$$

Найдемо екстремуми функції (19), для чого вирішимо систему диференційних рівнянь:

$$\begin{cases} \dfrac{\partial I(\lambda_i, \mu_j)}{\partial \lambda_i} = 0, \\ \dfrac{\partial I(\lambda_i, \mu_j)}{\partial \mu_j} = 0, \end{cases} \quad (20)$$

провівши диференціювання відносно кожного λ_i та μ_j.

Для спрощення розрахунку системи (20) приймемо $\mu_3 = 0$ та $\lambda_3 = 0$, та обмежимось лінійною складовою рівнянь, для того, щоб уникнути вирішення системи нелінійних диференційних рівнянь. Внаслідок спрощення система (20) прийме вигляд системи арифметичних рівнянь

$$\begin{cases} \dfrac{\partial I_1(\lambda_i, \mu_j)}{\partial \lambda_2} = \dfrac{T^4}{80}\mu_2 + \dfrac{T^6}{672}\left(\mu_2^2 + 2\lambda_2\mu_2\right); \\ \dfrac{\partial I_1(\lambda_i, \mu_j)}{\partial \mu_2} = -\dfrac{T^2}{12} + \dfrac{T^4}{80}\left(2\mu_2 + \lambda_2\right). \end{cases} \quad (21)$$

Оскільки розглядається поведінка СРЗ відносно стану $P_0(t)$, то нас цікавлять параметри стратегій, що безпосередньо впливатимуть на перехід СРЗ в стан отримання збитків від РЕП. Таким чином, для моделювання в якості критеріїв приймемо інтенсивності λ_2 та μ_2. Розрахунку оптимальних значень підлягають всі інтенсивності.

Розв'язання системи (21) призведе до отримання результуючих значень параметрів λ_2^{opt} та μ_2^{opt} для стратегій гравців (2) та (3), які дорівнюють:

$$\lambda_2{}^{opt} = \frac{152}{45 \cdot T^2} \approx 3{,}37 \cdot \frac{1}{T^2}, \quad (22)$$

$$\mu_2{}^{opt} = \frac{74}{45 \cdot T^2} \approx 1{,}64 \cdot \frac{1}{T^2}. \quad (23)$$

Використаємо зворотні перетворення [15], та переведемо отримані оптимальні коефіцієнти (22) − (23) стратегій гравців в область оригіналів:

$$\lambda_{2\,\max}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \cdot \Lambda(k) = 3{,}37 \cdot \frac{1}{T^2}, \quad (24)$$

$$\mu_{2\,\min}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \cdot \mathrm{M}(k) \approx 1{,}64 \cdot \frac{1}{T^2}. \quad (25)$$

Гарантований рівень захищеності I^G для СРЗ від атак РЕП в ході доби інформаційної боротьби, з врахуванням початкових умов та інтенсивностей оптимальних стратегій гравців дорівнює $I^G \approx 0{,}3$.

Модель процесу здійснення атаки РЕП радіоліній СРЗ, при виборі гравцями оптимальних стратегій (24) − (25), в області оригіналів матиме вигляд:

$$P_0^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt} \\ \mu=\mu^{opt}}} \approx \sum_{k=0}^{k=6}\left(\frac{t}{T}\right)^k \left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt} \\ \mu=\mu^{opt}}} =$$

$$= 0{,}5 - 0{,}4111 \cdot \left(\frac{t}{T}\right)^2 + 0{,}5161 \cdot \left(\frac{t}{T}\right)^4 - 0{,}3650 \cdot \left(\frac{t}{T}\right)^6. \quad (26)$$

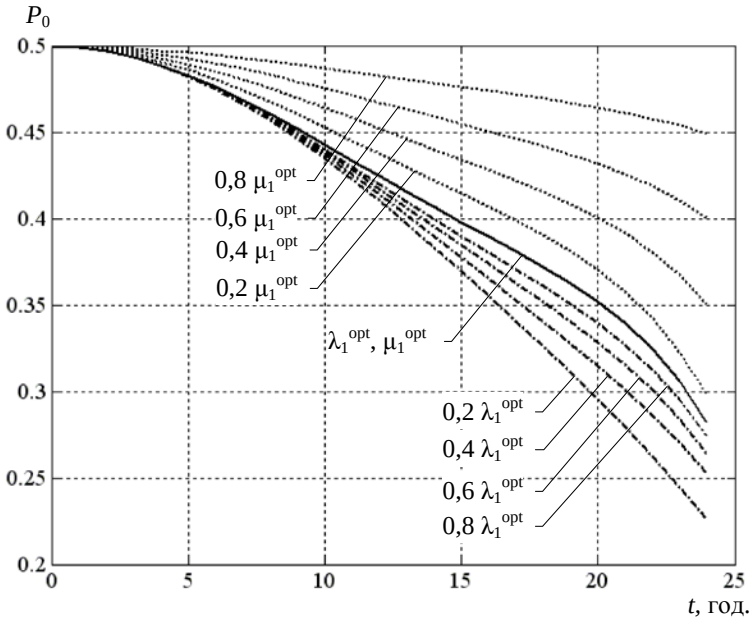
Для моделювання зміни ШНП СРЗ в якості критеріїв приймаються інтенсивності атак придушення радіоліній СРЗ λ_2 та захисних дій МЗІ від РЕП μ_2. Відхилення гравців від оптимальних стратегій (24) та (25) моделі ШНП означає програш у платі.

Диференціально-ігрова модель ШНП СРЗ області оригіналів матиме вигляд:

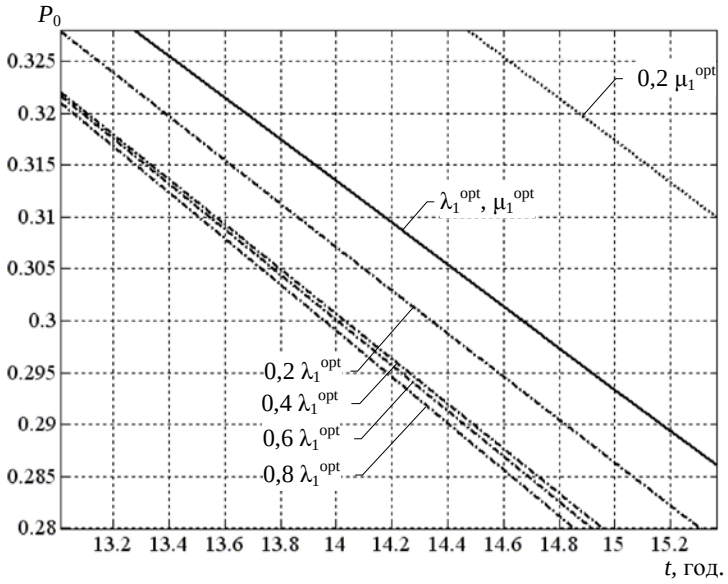
$$P_0(t) = \frac{1}{2} - \frac{T^2}{4}\mu_2 + \frac{T^4}{16}\left(\mu_2{}^2 + \lambda_2 \cdot \mu_2\right) -$$
$$- \frac{T^6}{96}(\mu_2{}^3 + \mu_2{}^2 + \lambda_2\mu_2{}^2 + \lambda_2{}^2\mu_2 + \lambda_2{}^2\lambda_3 + \lambda_2\mu_1\mu_2 + \quad (27)$$
$$+ \lambda_2\lambda_3\mu_1 + \lambda_2\mu_2\mu_3 + \lambda_2\lambda_3\mu_3 - \lambda_0\lambda_1 + \lambda_0\lambda_3 + \lambda_3{}^2 - \lambda_3\mu_3)^6.$$

Крок зміни інтенсивності атак та захисту приймемо за 0,2. Почергово, при сталому іншому критерію, будемо змінювати інтенсивність λ_2, відносно λ_2^{opt}, та підставляти в формулі (27). Аналогічну процедуру проведемо змінюючи μ_2.

В результаті моделювання змін ШНП СРЗ, в залежності від зміни параметрів інтенсивності атак та захисних дій МЗІ, отримали залежності, що представлені на рис. 2.



а)



б)

Рис. 2. Графіки залежності імовірності збитку від змін стратегій протиборчих сторін в ході реалізації РЕП радіоліній СРЗ: а) загальний вигляд графіків , б) маштабована частина графіків

Результати моделювання показують, що при збільшенні інтенсивності нанесення атак РЕП радіолінії СРЗ порушником, імовірність нанесення збитків $P_0(t)$ збільшується. Аналогічна ситуація відбувається при зниженні інтенсивності захисних дій МЗІ.

Висновки. В результаті роботи був розроблений метод оцінки імовірності збитку внаслідок реалізації атак радіоелектронного придушення радіоліній військових систем радіозв'язку в ході проведення інформаційних операцій, який на відміну від відомих ґрунтується на визначенні імовірності збитку внаслідок інформаційних атак, що дозволяє отримати мінімальні необхідні інтенсивності стратегій гравців та шаблони нормальної поведінки СРЗ спеціального призначення в умовах реалізації інформаційних атак.

На основі запропонованого методу було проведено моделювання поведінки СРЗ під час реалізації атак радіоелектронного придушення радіоліній.

Результати моделювань поведінки СРЗ представлені в якості аналітичних виразів шаблонів нормальної поведінки СРЗ, які відображають зміни в розвитку конфлікту при будь-яких змінах у стратегіях протиборчих сторін у ході інформаційного конфлікту. Інтервал розгляду конфлікту складав 24 години та може змінюватись без подальших модифікацій в методі розрахунків. Отримані співвідношення дозволяють оцінювати, з урахуванням можливостей порушника та МЗІ, характер розвитку інформаційного конфлікту.

Визначені оптимальні значення інтенсивності атак радіоелектронного придушення та захисту від них, характеризують рівновагу диференціальної гри та ціну гри. Для отримання переваги над противником необхідно досягти збільшення плати протилежною стороною, що складала б більше ціни гри.

Визначено, що при відхиленні інтенсивності захисних дій від оптимального значення, імовірність отримання збитків від них змінюється з більшим кроком, ніж при аналогічному відхиленні інтенсивності атак. Даний факт підкреслює критичність розгляду систем захисту інформації, що необхідно врахувати на етапі їх проектування.

Результати дослідження показали адекватну роботу методу оцінки імовірності збитку внаслідок реалізації атак радіоелектронного придушення радіоліній військових систем радіозв'язку в ході проведення інформаційних операцій при моделюванні поведінки систем радіозв'язку в ході реалізації атак.

Практична важливість результатів обумовлюється можливістю застосування даного методу для оцінки імовірності збитку внаслідок успішної реалізації інформаційних атак на етапі проектування захищених СРЗ.

Напрямком подальших досліджень є вровадження методу для оцінки стану інформаційної безпеки під час веденння бойових дій в умовах реалізації РЕП.

ЛІТЕРАТУРА

1. Daniel Wentre. Information warfare / Daniel Wentre. − San Francisco : Wiley-ISTE, 2012. − 320 p.

2. Information operations primer. Fundamentals of Information Operations. − Philadelphia, U.S. Army War College, 2006. − 168 p.

3. Information Operations : Joint Pub 3-13.1. – DOD US. – Government Printing Office. – 2012. – 69 p.

4. Медведєв В. К. Сучасна інформаційна війна та її обрис. / Медведєв В. К., Кучеренко Ю. Ф., Гузько О. М. // Системи озброєння і військова техніка. – 2008. – № 1(13) – С. 52 – 54.

5. Шестаков В. І. Інформаційні операції : сьогодення та перспективи розвитку. Інформаційні системи / В. І. Шестаков, О. В. Манько, О. І. Пінчук // Збірник наукових праць ЖВІ НАУ. – 2008. – № 1. – С. 23 – 31.

6. Сушко О. О. Оцінка спільного впливу компонент військової наступальної інформаційної операції на лінії зв'язку / О. О. Сушко // Збірник ВІКНУ. – 2005. – № 2. – С. 154 – 158.

7. Adam T. Electronic warfare / T. Adam. – New York : Nova Science Publishers, 2009. – 192 p.

8. Палий А. И. Радиоэлектронная борьба. – 2-е изд., перераб. и доп. − М. Воениздат, 1989 г. – 350 с.

9. Information security standards [Електроний ресурс]. – Режим доступу : http://www.iso27001security.com. – Назва з екрану.

10. Астахов А. М. Искусство управления информационными рисками / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с.

11. Петренко С. А. Анализ рисков в области защиты информации / С. А. Петренко. – СПб. : Афина, 2009. – 153 с.

12. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // Науково-практичний журнал "Безпека інформації". – 2014. – № 1. – С. 7 – 11.

13. Шевченко А. С. Модель загроз для відомчих безпроводових інформаційно-комунікаційних систем в умовах інформаційної боротьби при впливі комплексу навмисних атак порушника / А. С. Шевченко // Сучасний захист інформації. – 2011. – № 3. – С. 58 – 65.

14. 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.

15. Пухов Г. Е. Преобразования тейлора и их применение в электротехнике и электронике / Г. Е. Пухов. – К. : Наукова думка. – 1978. – 260 с.

16. Кельберт М. Я. Вероятность и статистика в примерах и задачах. Т. II: Марковские цепи как отправная точка теории случайных процессов и их приложения / Кельберт М. Я., Сухов Ю.М. − М.: МЦНМО, 2009. − 295 с.

17. Петросян Л. А. Теория игр : учебное пособие / Л. А. Петросян, Н. А. Зенкевич, Е. В. Шевкопляс. – СПб. : БХВ-Петербург, 2012 − 432 с.