УДК 621.396 + 654.16 : 517.978.2 **Шевченко А.С., Мазулевський О.Є.**

МОДЕЛЮВАННЯ АТАК РАДІОЕЛЕКТРОННОГО ПРИДУШЕННЯ РАДІОЛІНІЙ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В ХОДІ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

В статті викладено методику моделювання атак придушення радіолінійних безпроводових інформаційно-телекомунікаційних систем, що функціонують під час ведення інформаційної боротьби, з застосуванням теорій диференціальних ігор та диференціальних перетворень Пухова Г.Е.

Ключові слова: телекомунікаційна система, радіоелектронна боротьба, радіоелектронне придушення, радіолінійні безпроводні системи.

Вступ. Складовою частиною ведення інформаційних операцій є радіоелектронна боротьба (РЕБ), однією з функцій якої є радіоелектронне придушення (РЕП) радіоліній безпроводових інформаційно-телекомунікаційних систем (БІТС).

Заходи РЕБ, в контексті інформаційної боротьби, застосовуються для оперативного забезпечення ведення бойових дій. Згідно з концепціями ведення інформаційної боротьби розвинутих країн атаки РЕП здійснюються для виведення з ладу на час проведення операцій радіоліній та радіомереж БІТС збройних сил, інших збройних формувань та органів державного управління в загрозливий період та під час військового конфлікту. Зважаючи на те, що безпроводова складова інформаційно-телекомунікаційної системи державних структур складає значну частину, на її вразливості, критичним стає захист саме БІТС спеціального призначення під час інформаційних конфліктів [1 −5].

Важливою перевагою атак РЕП є їх дистанційна реалізація. Встановлення радіоелектронних завад здебільшого не вимагає проникнення в периметр, що знаходиться під охороною в якому розміщено БІТС. Радіоелектронні завади придушують приймач БІТС та на цей час блокують передачу інформації через радіоканал. В наслідок цього здійснення інформаційного обміну та управління через БІТС унеможливлюється [6 − 7].

Засоби РЕБ встановлюються на всі види платформ: наземного, повітряного або морського базування. Характерними прикладами станцій РЕБ, що знаходяться на озброєнні армії США, є станції радіо/радіотехнічної розвідки та радіоелектронної війни „Profit”, літак радіоелектронної розвідки ЕС-130Е „Commando Solo 3”, літаки РЕБ ЕА-16G „Growler” та ЕА-6В „Prowler”. На озброєнні Російської Федерації новим озброєнням РЕБ стали комплекс Р-330 БМВ, Р-330Ж, комплекс радіоконтролю та встановлення завад „Шиповник”.

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 [2-5]. З часом модернізуються методи ведення РЕБ та засоби їх реалізації. РЕП, як одна зі складових РЕБ, залишається найбільшою загрозою для БІТС.

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

Існуючі математичні моделі відображення процесів нападу на інформацію та її захисту, на яких грунтується оцінка рівня захищеності систем, не враховують динаміку протікання інформаційного конфлікту, зміну типів атак та їх параметрів в реальному часі [8].

Мета. З аналізу сучасного стану інформаційної безпеки держави та існуючих загроз постає питання захисту БІТС, які б могли функціонувати в динамічних умовах інформаційної боротьби. Першочерговим є захист БІТС військових формувань, державних органів, які приймають участь в процесах управління державою, не залежно від форм власності БІТС. Для цього, необхідно отримувати інформацію про характер протікання інформаційного конфлікту та ефективність роботи МЗІ в ході конфронтації.

Дослідженню, результати якого представлені в даній роботі, підлягає процес реалізації атак РЕП радіоліній БІТС, як складового етапу інформаційних операцій.

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

Початкові умови. Розглядається ситуація рівноімовірнісного знаходження системи у крайніх станах моделі протікання інформаційного конфлікту. В один і той же час t існують як атаки на БІТС, так і самі БІТС використовують механізми захисту від РЕП. Здійснюється розгляд розвитку інформаційного конфлікту на протязі однієї доби (t = 24 години).

Обмеження. В роботі розглядаються навмисні штучні атаки РЕП порушників, що є загрозами для фізичного та канального рівнів БІТС.

Викладення основного матеріалу дослідження. Методи реалізації атак РЕП залежать від володіння інформацією про БІТС протиборчої сторони, параметрів її радіосигналів, що отримуються від радіотехнічної розвідки. Порушник може встановити перешкоду БІТС при знанні цих параметрів, чи без такого [6 – 7].

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

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

При розробці захищених БІТС 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. [9]. 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 графу нормальної поведінки БІТС під час інформаційної боротьби (рис. 1).

Кола представляють собою множину станів $\{P_z(t)\}$, де $z = 0\ldots3$ – стани, у яких може перебувати БІТС 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:

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

− перехоплення радіосигналів (радіотехнічна розвідка);

− РЕП радіолінії БІТС;

− отримання збитку від РЕП БІТС (отримано збитків від порушення цілісності і доступності інформації в наслідок РЕП).

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

Нехай БІТС 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 БІТС, що призведе до отримання збитків;

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

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

$P_3(t)$ – імовірність перебування БІТС в стані захищеності, відсутності РЕБ.

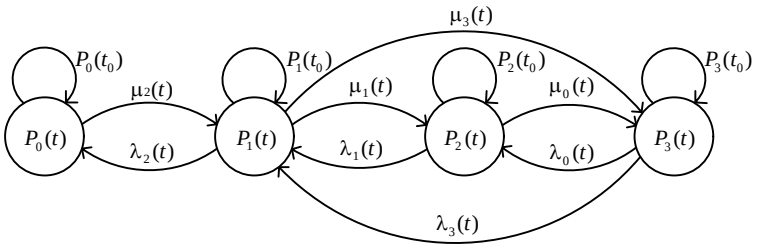

Рис. 1. Граф моделі шаблону нормальної поведінки безпроводових і нформаційно-телекомунікаційних систем при реалізації атаки РЕП радіолінії

Визначення інтенсивностей атак та захисних дій МЗІ Таблиця 1

Інтенсивність			
атак порушника		***захисних дій МЗІ***	
$\lambda_0(t)$	− перехоплення радіосигналу;	$\mu_0(t)$	− захист від перехоплення радіосигналу;
$\lambda_1(t)$	− придушення радіолінії БІТС;	$\mu_1(t)$	− захист від придушення радіолінії БІТС;
$\lambda_2(t)$	− 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 [10].

Запропонована графова модель ШНП враховує всі можливі переходи БІТС 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 БІТС під час інформаційного конфлікту на інтервалі $\overline{t_0, T}$, з урахуванням переходів між станами графу (рис. 1), застосуємо систему диференціальних рівнянь Колмогорова-Чепмена [10]:

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

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

В реальній обстановці зміна стратегій сторін обумовлюється багатьма чинниками, які здебільшого врахувати не має можливості, припустимо, що інтенсивності сторін в ході боротьби змінюються по лінійному закону. Тоді,

$$\lambda_i(t) = \lambda_i \cdot t \tag{2}$$

та

$$\mu_j(t) = \mu_j \cdot t, \tag{3}$$

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 в наслідок дії МЗІ відповідно, при чому $i \wedge j \in [0,\ z-1]$.

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

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

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

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

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 БІТС 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 БІТС та захисту від цих атак відповідає диференційно-ігровому підходу з безкоаліційним характером ведення гри [11].

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 БІТС 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 БІТС, 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:

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

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

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

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

При рівності плат обидвох сторін (6) та (7):

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

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 БІТС для порушника в ході радіорозвідки.

Гарантований рівень захищеності БІТС 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:

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

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

Інтегрування здійснюється напротязі 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 в платі [9].

Знаходження диференційно-ігрової моделі ШНП БІТС $P_0^{opt}(t)$ здійснимо за загальною методологією, що представлена в працях [9], з використанням P-перетворень академіка Пухова Г.Є. [10].

Перейдемо в область зображень, для чого використаємо пряме диференційне перетворення [9]. В результаті інформаційний конфлікт, що описаний системою (1), в області P-зображень матиме вигляд:

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

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 $k = 0, 1, 2\ldots$.

В наслідок 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 $\mathrm{M}_j(k) * P_z(k)$ [9].

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 отримає вигляд:

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

Визначимо дискрети диференціального спектра диференційно-ігрової моделі ШНП БІТС 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 представлення (10) в якості ряду плата гри матиме вигляд:

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

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. В наслідок 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 БІТС відносно стану $P_0(t)$, то нас цікавлять параметри стратегій, що безпосередньо впливатимуть на перехід БІТС 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:

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

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

Використаємо зворотні перетворення [9], та переведемо отримані оптимальні коефіцієнти (22) − (23) стратегій гравців в область оригіналів:

$$\lambda_{2\ \max}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \cdot \Lambda(k) = 36,8 \cdot \frac{1}{T^2}, \tag{24}$$

$$\mu_{2\ \min}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \cdot \mathrm{M}(k) \approx -15,06 \cdot \frac{1}{T^2}. \tag{25}$$

Гарантований рівень захищеності I^G для БІТС 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 БІТС, при виборі гравцями оптимальних стратегій (24) − (25), в області оригіналів матиме вигляд:

$$\begin{aligned} P_0^{opt}(t) &= \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt}\\ \mu=\mu^{opt}}} \approx \sum_{k=0}^{k=6}\left(\frac{t}{T}\right)^k \left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt}\\ \mu=\mu^{opt}}} = \\ &= 0,5 - 0,4111 \cdot \left(\frac{t}{T}\right)^2 + 0,5161 \cdot \left(\frac{t}{T}\right)^4 - 0,3650 \cdot \left(\frac{t}{T}\right)^6 \end{aligned} \tag{26}$$

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

Диференціально-ігрова модель ШНП БІТС області оригіналів матиме вигляд:

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

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 (27). Аналогічну процедуру проведемо змінюючи μ_2.

В результаті моделювання змін ШНП БІТС, в залежності від зміни параметрів інтенсивності атак та захисних дій МЗІ, отримали залежності, що представлені на рис. 2 та рис. 3.

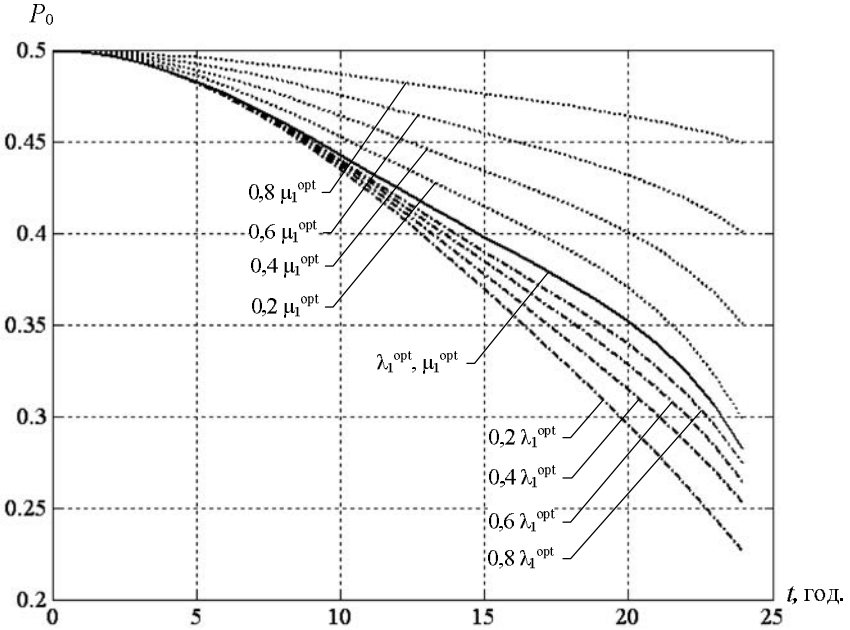

Рис. 2. Графіки ШНП БІТС під час РЕП радіоліній БІТС.

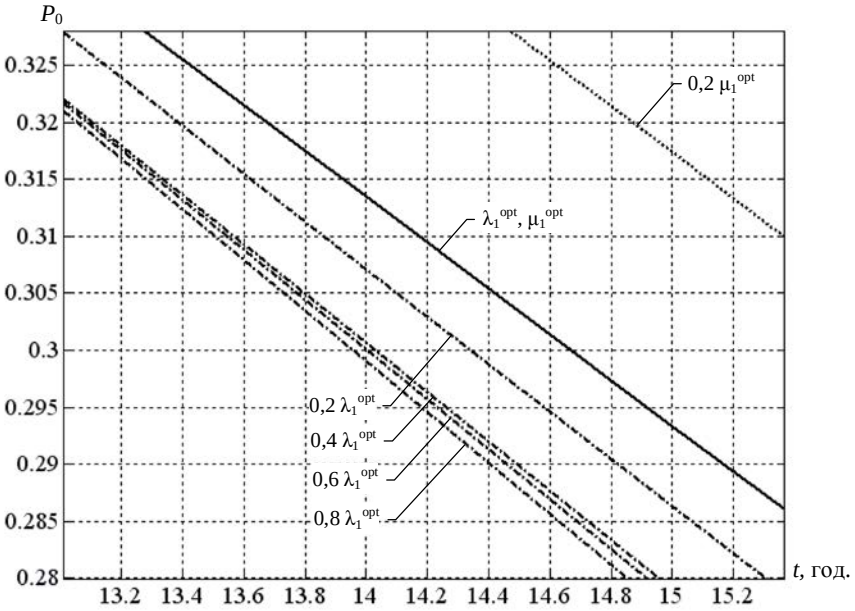

Рис. 3. Маштабована частина графіків ШНП БІТС.

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

Висновки. В результаті роботи було проведено моделювання процесів атак радіоелектронного придушення радіоліній та захисних дій механізмів захисту інформації безпроводових інформаційно-телекомунікаційних систем, що функціонують в умовах інформаційного конфлікту. Шаблон нормальної поведінки БІТС відображає зміни в розвитку конфлікту при будь-яких змінах в стратегіях протиборчих сторін в ході інформаційної боротьби протягом доби.

Отримані оптимальні значення інтенсивностей атак придушення радіолінії та захисту від них, які характеризують рівновагу диференціальної гри та ціну гри. Для отримання переваги над противником необхідно досягти збільшення плати протилежною стороною, що б складала більше ціни гри. В цьому разі необхідно змінювати власну стратегію в бік збільшення інтенсивності атак радіоелектронного придушення БІТС.

Результати дослідження показали роботу методики диференційно-ігрового моделювання з використанням диференційних перетворень Пухова Г.Е. при моделюванні атак радіоелектронного придушення в ході інформаційного конфлікту.

Практична важливість результатів обумовлюється можливістю застосування даної методики в процесі проектування захищених БІТС. В результаті знання ресурсів порушника, можливо застосовувати ефективні механізми захисту, що надійно захистять БІТС в ході інформаційної боротьби.

ЛІТЕРАТУРА

1. Иванов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века / И. Иванов, И. Чадов // Зарубежное военное обозрение. − 2011. − № 1. – С. 14−21.
2. Information operations primer. Fundamentals of Information Operations. − Philadelphia, U.S. Army War College, 2006.− p. 168.
3. Information Operations / Joint Publication 3-13. – DOD, 2006. − P. 119.
4. Adam T. Elsworth. Electronic warfare. New York.: Nova Science Publishers, 2009. − P. 192.
5. Иванов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века / И. Иванов, И. Чадов // Зарубежное военное обозрение. − 2011. − № 1. – С. 14−21.
6. Борисов В.И., Зинчук В.М. Помехозащищенность систем радиосвязи. Вероятностно-временной подход. Изд. 2-е, исправленное / – М.: РадиоСофт, 2008. – 260 с.
7. Палий А. И. Радиоэлектронная борьба. – 2-е изд., перераб. и доп. − М. Воениздат, 1989. – 350 с.
8. 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.
9. Пухов Г.Е. Преобразования тейлора и их применение в электротехнике и электроние. / Пухов Г.Е. - К.: Наукова думка, 1978. – 260 с.
10. 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.
11. Петросян Л.А. Теория игр: учебное пособие / Петросян Л.А., Зенкевич Н.А., Семна Е.А. − М.: Высшая школа, Книжный дом Университет, 1998 − 304 с.

Надійшла: 12.10.2012р.

Рецензент: д.т.н., проф. Ленков С.В.