УДК 621.396 + 654.16 : 517.978.2

Шевченко А.С. (ВІТІ ДУТ)
к.т.н. Липський О.А. (ІСЗЗІ НТУУ „КПІ”)

МЕТОД ОЦІНКИ ІМОВІРНОСТІ ЗБИТКУ ВНАСЛІДОК РЕАЛІЗАЦІЇ АТАК ПЕРЕХОПЛЕННЯ РАДІОСИГНАЛУ СИСТЕМ РАДІОЗВ’ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В статті викладено математичний апарат методу оцінки імовірності збитку внаслідок реалізації атак перехоплення радіосигналів систем радіозв’язку спеціального призначення, що функціонують в умовах інформаційних операцій, з застосуванням теорії диференціальних ігор та диференціальних перетворень Пухова Г.Е.

Шевченко А. С., Липский А. А. Метод оценки вероятности ущерба вследствии реализации атак перехвата радиосигналов систем радиосвязи специального назначения. *В статье представлен математический аппарат метода оценки вероятности ущерба от реализации атак перехвата радиосигналов систем радиосвязи, которые функционируют во время информационных операций, с использованием теорий дифференциальных игр и дифференциальных преобразований Пухова Г.Е.*

A.Shevchenko, A.Lipskiy The method of evaluation the probability of loss as a result of the attacks intercept radio radio systems special purpose. *In the article the mathematical vehicle method of estimation probability detriment is presented from realization attacks of intercept radio signals of the systems radio contacts which function during informative operations, with the use differential game and differential transformations of Puhov G. theories*

Ключові слова: *системи радіозв’язку, інформаційні атаки, диференційно-ігрова модель, радіорозвідка, перехоплення радіосигналів, оцінка імовірності збитку, оцінка ризиків.*

Вступ. В ході ведення інформаційних операцій, основний акцент ставиться на атаки, що реалізують вплив на інформаційну інфраструктуру інформаційно-телекомунікаційних системи (ІТС) [1] спеціального призначення, які призначені для управління збройними силами та іншими структурами державного управління.

Найбільш уразливою частиною ІТС, в ході реалізації інформаційних атак, є її безпроводова складова – системи радіозв’язку (СРЗ), внаслідок доступності середовища розповсюдження сигналів.

Аналіз методів ведення інформаційних операцій показав, що до основних інформаційних атак, в яких СРЗ є об’єктом чи засобом реалізації, є атаки реалізації: радіоелектронної розвідки (РЕР), радіоелектронного придушення (РЕП) та інформаційного впливу через засоби масової інформації (радіомовлення, телебачення, інформаційні ресурси, тощо) [2 − 3].

Одним з видів РЕР є радіорозвідка, яка реалізує атаки перехоплення радіосигналів від джерел випромінювання та аналіз інформації, яка отримана. В результаті аналізу інформації після демодуляції (детектування) та декодування перехоплених радіосигналів може бути порушена конфіденційність інформації, що передавалась через радіоканал.

СРЗ є транспортом для передачі різного типу інформації. З огляду на це та враховуючі доступність середовища розповсюдження сигналів, з боку порушника виникає інтерес до проведення атак радіорозвідки, які направлені на перехоплення радіосигналів від СРЗ. Особливістю даного класу атак є складність їх виявлення, що значно розширює межі їх застосування.

Для успішного здійснення несанкціонованого доступу до інформації, що передається через СРЗ необхідне володіння апріорними знаннями про характеристики сигналів, діапазон частот в якому вони передаються, місце розташування джерела сигналів. Тому порушнику необхідно під час радіоперехоплення визначити параметри радіосигналів. До таких параметрів відносяться: вид модуляції, рівень сигналу, смуга частот, частота несучої та інші характеристики радіосигналів в залежності від виду СРЗ.

Засоби РЕР призначені для проведення зовнішньої розвідки сигналів – так званої SIGINT (Signals Intelligence) [4]. До таких засобів відносяться станції радіорозвідки, або станції радіо, радіотехнічної розвідки (РРТР). Характерними прикладами таких станцій є

станція РРТР та радіоелектронної війни „Profit” (США) [5], РБ-531Б „Інфауна” (Росія) [6], „Беркут” (Україна) [7] тощо.

Аналіз останніх досліджень та публікацій. Огляд останніх змін концепцій ведення інформаційних операцій найбільш розвинутими державами показує, що РЕР, наряду з кібернетичними операціями, залишається найбільш дієвим засобом боротьби в ході конфронтації [8 − 10]. З часом модернізуються методи ведення РЕР та засоби їх реалізації. Радіорозвідка (РРТР), як одна зі складових РЕР, залишається найбільшою загрозою для СРЗ.

Для спостереження за ходом інформаційного конфлікту необхідно оцінювати атаки противника (порушника) на СРЗ та дієвість їх механізмів захисту інформації (МЗІ).

Існуючі методи оцінки інформаційної безпеки СРЗ спеціального призначення ґрунтуються на визначенні часу вскриття системи зв’язку. Даний підхід не відображає процесів нападу на інформацію та її захисту, оцінки рівня захищеності інформації та критичності інформаційних ресурсів, не враховує динаміку протікання інформаційного конфлікту [11], зміну типів атак та їх параметрів в реальному часі.

Мета. Зважаючи на приведені доводи постає питання захисту СРЗ, які б могли функціонувати в динамічних умовах інформаційних атак. Критичним є захист СРЗ військових формувань, державних органів, які приймають участь в процесах управління державою, не залежно від форм власності СРЗ. Для чого, необхідно отримувати інформацію про характер протікання інформаційного конфлікту та ефективність роботи МЗІ в ході конфронтації.

Дослідженню підлягає процес реалізації атаки перехоплення радіосигналів – радіорозвідки (РРТР), як складової інформаційної операції.

Постановка завдання. Завданням дослідження є розробка методу оцінки імовірності збитку та моделювання атаки перехоплення радіосигналів та захисних дій МЗІ СРЗ. Для цього слід побудувати шаблон нормальної поведінки (ШНП) МЗІ та порушника, 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 СРЗ, так і самі СРЗ використовують механізми захисту від радіоперехоплення. Здійснюється розгляд розвитку інформаційного конфлікту на протязі однієї доби (t = 24 години).

Обмеження. В роботі розглядаються навмисні штучні атаки порушників, що є загрозами для інформації на фізичному та канальному рівнях СРЗ. Ціна гри обмежена значеннями $I^G_{\min} \le I^G \le I^G_{\max}$, інтенсивність атак в межах $0 \le \lambda_i(t) \le \lambda_{i\max}(t)$, інтенсивність захисних дій $0 \le \mu_j(t) \le \mu_{j\max}(t)$.

Викладення основного матеріалу дослідження. В процесі розробки захищених СРЗ постає питання вибору засобів захисту, які б надійно захищали від порушення конфіденційності, цілісності та доступності інформації, що передається через радіоканали. В наслідок цього необхідно провести моделювання процесів «атака-захист», та визначитись з вимогами до механізмів захисту.

В процесі проведення моделювання процесів атак та захисту пропонується використовувати диференціально-ігрове моделювання з застосуванням методу диференційних перетворень академіка Пухова Г.Є. [12]. Застосування диференційних перетворень дозволить оперувати лінійними рівняннями, при вирішенні задач диференціально-ігрового моделювання.

Розглянемо більш детально атаку перехоплення радіосигналів та представимо її у вигляді графу нормальної поведінки СРЗ (рис.1).

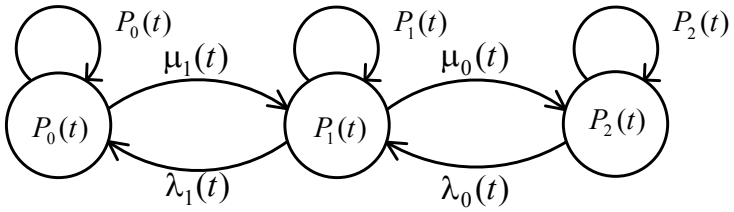

Рис. 1. Граф моделі шаблону нормальної поведінки систем радіозв'язку при перехопленні

Кола представляють собою множину станів $\{P_z(t)\}$, де $z = 0…2$ – стани, у яких може перебувати СРЗ під час інформаційного конфлікту з відповідними імовірностями. Стрілки між станами відображають результат виникнення переваги дій порушника над механізмами захисту та протилежні результати.

Граф складається з трьох станів:

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

− перехоплення радіосигналів (перехоплення та оцінка характеристик радіосигналу СРЗ);

− отримання збитку від перехоплення радіосигналів (отримано збитків від порушення конфіденційності інформації в наслідок перехопленні радіосигналу).

Інтенсивності потоків атак перехоплення радіосигналів та переходів в стан цілковитої поразки дорівнюють $\lambda_0(t)$ та $\lambda_1(t)$ відповідно; $\mu_0(t)$ та $\mu_1(t)$ − інтенсивності потоку захисних дій від відповідних атак.

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 перехоплення радіосигналів СРЗ, що призведе до отримання збитків;

$P_1(t)$ – імовірність здійснення перехоплення радіосигналів СРЗ;

$P_2(t)$ – імовірність перебування СРЗ в стані захищеності, відсутності радіорозвідки.

Дана послідовність випадкових подій є колом Маркова з двома вихідними станами [13].

Запропонована графова модель ШНП враховує всі можливі переходи СРЗ між станами під час інформаційного конфлікту з урахуванням змін стратегій порушника та МЗІ (далі сторін або гравців).

Саме стратегії конфліктуючих сторін визначають яким буде наслідок протистояння.

Для відображення інформаційного конфлікту перехоплення радіосигналів за час $\overline{t_0, T}$ застосуємо систему диференціальних рівнянь Колмогорова-Чепмена [13]:

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

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 наслідок того, що 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; 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 радіоперехопленню, 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 $\Lambda \in K_\lambda$ та $M \in K_\mu$, які в свою чергу обмежені евклідовими просторами E_λ і E_μ відповідно [11].

В ході атаки перехоплення радіосигналів 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 [14].

Під час інформаційної операції при здійсненні заходів радіоперехоплення кожна із сторін цієї гри намагається завдати іншій найбільших втрат. Порушник намагається перехопити радіосигнал від джерела, відносно якого здійснюється радіорозвідка, та після обробки сигналу отримати корисну інформацію (дані, параметри сигналу, місце розташування джерела радіовипромінювання, тощо), 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:

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

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

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

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

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 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:

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

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

Інтегрування здійснюється вздовж траєкторії 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 СРЗ $P_0^{opt}(t)$ здійснимо за загальною методологією, що представлена в роботі [11], з використанням P-перетворень академіка Пухова Г.Є. [12].

Для подальшого переходу в область зображень використаємо пряме диференційне перетворення [12]. В результаті інформаційний конфлікт, що описаний системою (1), в області P-зображень матиме вигляд:

$$\begin{cases} P_0(k+1) = \dfrac{T}{k+1}\left(-\mathrm{M}_1(k)P_0(k) + \Lambda_1(k)P_1(k)\right) \\ P_1(k+1) = \dfrac{T}{k+1}\left(-(\Lambda_1(k) + \mathrm{M}_0(k))P_1(k) + \mathrm{M}_1(k)P_0(k) + \Lambda_0(k)P_2(k)\right) \\ P_2(k+1) = \dfrac{T}{k+1}\left(-\Lambda_0(k)P_2(k) + \mathrm{M}_0(k)P_1(k)\right), \end{cases} \tag{11}$$

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 $M_j(k) * P_z(k)$ [10].

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

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

$$M_j(k) * P_z(k) = \mu T \cdot P_z(k-1). \tag{13}$$

З урахуванням перетворень добутків в області зображень (12) – (13), система диференціальних рівнянь Колмогорова-Чепмена для атаки перехоплення радіосигналів отримає вигляд:

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

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

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

$$P_0(1) = P_0(3) = P_0(5) = 0, \tag{15}$$

$$P_0(2) = -\frac{T^2}{4}\mu_1, \tag{16}$$

$$P_0(4) = \frac{T^4}{16}\left(\mu_1{}^2 + \lambda_1 \cdot (\mu_1 + \lambda_0)\right), \tag{17}$$

$$P_0(6) = -\frac{T^6}{96}(\mu_1{}^3 - \lambda_0\lambda_1\mu_1 - \lambda_1^2\mu_1 - \lambda_0\lambda_1{}^2 - \lambda_1\mu_0\mu_1 - \lambda_0\lambda_1\mu_0 + \lambda_0^2\lambda_1). \tag{18}$$

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

$$\begin{aligned} I_1 = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1} = \frac{1}{2} - \frac{T^2}{12}\mu_1 + \frac{T^4}{80}\left(\mu_1^2 - \lambda_1\mu_1 - \lambda_0\lambda_1\right) - \\ - \frac{T^6}{672}(\mu_1{}^3 - \lambda_0\lambda_1\mu_1 - \lambda_1^2\mu_1 - \lambda_0\lambda_1{}^2 - \lambda_1\mu_0\mu_1 - \lambda_0\lambda_1\mu_0 + \lambda_0^2\lambda_1). \end{aligned} \tag{19}$$

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

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

провівши диференціювання відносно кожного λ_i та μ_j.

Для спрощення розрахунку системи (20) приймемо $\mu_0 = 0$, та обмежимось лінійною складовою рівнянь, для того щоб уникнути вирішення системи диференційних рівнянь. В наслідок спрощення система (20) прийме вигляд системи арифметичних рівнянь

$$\begin{cases} \dfrac{\partial I_1(\lambda_i, \mu_j)}{\partial \lambda_0} = \dfrac{T^4}{80}\lambda_1 + \dfrac{T^6}{672}\left(\lambda_1\mu_1 - 2\lambda_0\lambda_1 + \lambda_1^2\right); \\ \dfrac{\partial I_1(\lambda_i, \mu_j)}{\partial \lambda_1} = \dfrac{T^4}{80}\left(\mu_1 + \lambda_0\right); \\ \dfrac{\partial I_1(\lambda_i, \mu_j)}{\partial \mu_0} = \dfrac{T^6}{672}\left(\lambda_1\mu_1 + \lambda_0\lambda_1\right); \\ \dfrac{\partial I_1(\lambda_i, \mu_j)}{\partial \mu_1} = -\dfrac{T^4}{12} + \dfrac{T^4}{80}\left(2\mu_1 + \lambda_1\right). \end{cases} \tag{21}$$

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 радіоперехоплення. Таким чином, для моделювання в якості критеріїв приймемо інтенсивності λ_1 та μ_1. Розрахунку оптимальних значень підлягають всі інтенсивності.

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

$$\lambda_0{}^{opt} = \frac{226}{15 \cdot T^2} \approx 1{,}5 \cdot \frac{1}{T^2}, \tag{22}$$

$$\lambda_1{}^{opt} = \frac{184}{5 \cdot T^2} = 3{,}68 \cdot \frac{1}{T^2}, \tag{23}$$

$$\mu_1{}^{opt} = -\frac{226}{15 \cdot T^2} \approx 1{,}5 \cdot \frac{1}{T^2}. \tag{24}$$

Використаємо зворотні перетворення [12], та переведемо отримані оптимальні коефіцієнти (23) − (24) стратегій гравців в область оригіналів:

$$\lambda_{1\max}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \cdot \Lambda(k) = 3{,}68 \cdot \frac{1}{T^2}, \tag{25}$$

$$\mu_{1\min}^{opt}(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k \cdot \mathrm{M}(k) \approx 1{,}5 \cdot \frac{1}{T^2}. \tag{26}$$

Гарантований рівень захищеності I^G для СРЗ від атак радіоперехоплення в ході доби інформаційного конфлікту, з врахуванням початкових умов та інтенсивностей оптимальних стратегій гравців дорівнює $I^G \approx 0{,}15$.

Модель процесу здійснення атаки перехоплення радіосигналів СРЗ, при виборі гравцями оптимальних стратегій (22) − (24), в області оригіналів матиме вигляд:

$$P_0^{opt}(t)=\sum_{k=0}^{k=\infty}\left(\frac{t}{T}\right)^k\left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt}\\ \mu=\mu^{opt}}}\approx\sum_{k=0}^{k=6}\left(\frac{t}{T}\right)^k\left[P_0(k)\right]_{\substack{\lambda=\lambda^{opt}\\ \mu=\mu^{opt}}}= \\ =0{,}5-0{,}7533\cdot\left(\frac{t}{T}\right)^2+0{,}5675\cdot\left(\frac{t}{T}\right)^4-0{,}1639\cdot\left(\frac{t}{T}\right)^6 \tag{27}$$

Для моделювання зміни ШНП СРЗ в якості критеріїв приймаються інтенсивності атак перехоплення радіосигналів λ_1 та захисних дій від радіоперехоплення МЗІ μ_1. Відхилення гравців від оптимальних стратегій (23) та (24) моделі ШНП означає програш в платі.

Диференціально-ігрова модель ШНП СРЗ області оригіналів матиме вигляд:

$$P_0(t)=\frac{1}{2}-\frac{1}{4}\mu_1\left(\frac{t}{T}\right)^2+\frac{1}{16}\left(\mu_1^2-\lambda_1\mu_1-\lambda_0\lambda_1\right)\left(\frac{t}{T}\right)^4- \\ -\frac{1}{96}\left(\mu_1{}^3-\lambda_0\lambda_1\mu_1-\lambda_1^2\mu_1-\lambda_0\lambda_1{}^2-\lambda_1\mu_0\mu_1-\lambda_0\lambda_1\mu_0+\lambda_0^2\lambda_1\right)\left(\frac{t}{T}\right)^6 \tag{28}$$

Крок зміни інтенсивності атак та захисту приймемо за 0,2. Почергово, при сталому іншому критерії, будемо змінювати інтенсивність λ_1, відносно λ_1^{opt}, та підставляти в (28). Аналогічну процедуру проведемо змінюючи μ_1.

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

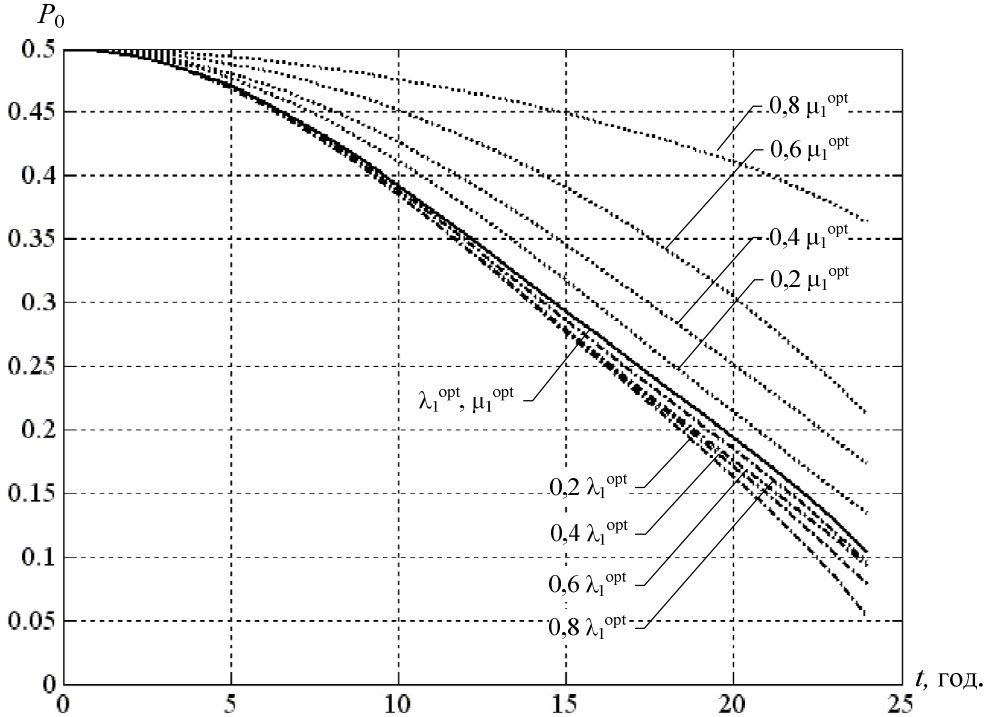

Рис. 2. Графіки ШНП СРЗ під час атаки перехоплення радіосигналів

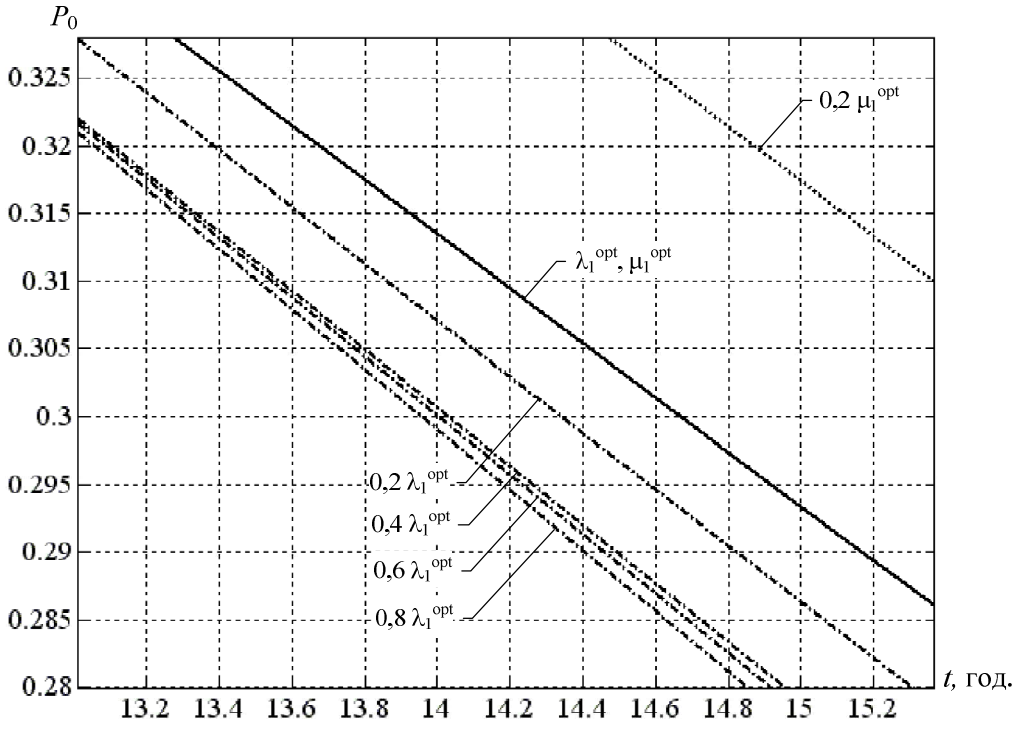

Рис. 3. Маштабована частина графіків ШНП СРЗ

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

Висновки.

В результаті роботи були отримані математичні вирази для оцінки імовірності збитку внаслідок атак перехоплення радіосигналів, проведено моделювання процесів атак перехоплення радіосигналів та захисних дій механізмів захисту інформації систем радіозв'язку, що функціонують в умовах інформаційного конфлікту. Шаблон нормальної поведінки СРЗ відображає зміни в розвитку конфлікту при будь-яких змінах в стратегіях протиборчих сторін в ході інформаційного конфлікту протягом доби.

Отримані оптимальні значення інтенсивності атак перехоплення радіосигналу 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 радіоперехоплення.

Інтервал розгляду конфлікту складав 24 години, але може бути змінений без подальших змін в методиці розрахунків. Отримані співвідношення дозволяють оцінювати, з урахуванням можливостей порушника та МЗІ, характер розвитку інформаційного конфлікту в ході радіорозвідки.

Результати моделювання показують, що при збільшенні інтенсивності нанесення атак перехоплення радіосигналів СРЗ порушником, імовірність нанесення збитків $P_0(t)$

Результати дослідження показали адекватну роботу методу диференційно-ігрового моделювання з використанням диференційних перетворень Пухова Г.Е. при моделюванні атак перехоплення радіосигналів в ході інформаційного конфлікту.

Практична важливість результатів обумовлюється можливістю застосування даного методу в процесі оцінки імовірності збитку, а відповідно і ризиків інформаційної безпеки, при проектування захищених СРЗ. В результаті знання ресурсів порушника, можливо

застосовувати ефективні механізми захисту, що надійно захистять СРЗ в ході впливу інформаційних атак.

В подальших дослідженнях доцільно розробити методи оцінки інформаційної безпеки конкретних видів та стандартів СРЗ та розробити методологію захисту СРЗ в умовах інформаційних операцій. Вирішення комплексу визначених завдань дозволить підвищити захищеність інформаційних ресурсів, що передаються через інформаційну інфраструктуру систем радіозв'язку спеціального призначення в умовах впливу інформаційних атак.

ЛІТЕРАТУРА

1. Про телекомунікації. Закон України. [Електронний ресурс]: за станом на 3 липня 2012 р. / Верховна Рада України. – Офіц. вид. − Режим доступу: http://zakon2.rada.gov.ua/laws/show/1280 – 15.

2. Иванов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века / И. Иванов, И. Чадов // Зарубежное военное обозрение. − 2011. − № 1. – С. 14 − 21.

3. Горбачев Ю. Подготовка ВВС США к кибероперациям / Ю. Горбачев // Зарубежное военное обозрение. − 2011. − № 2. – С. 54 − 59.

4. Signals intelligence. [Електронний ресурс] / National Security Agency. – Режим доступу: http://www.nsa.gov/sigint/index.shtml.

5. Кондратьев А. Перспективный комплекс РРТР и РЭВ сухопутных войск США «Профет» / А. Кондратьев // Зарубежное военное обозрение. − 2008. − № 7. – С. 14 − 21.

6. РБ-531Б Инфауна. [Електронний ресурс] / Military Russia. Отечественная военная техника (после 1945 г.). – Режим доступу: http://militaryrussia.ru/blog/topic – 628.html.

7. Мобильный комплекс радиоразведки. [Електронний ресурс] / Государственное предприятие "Научно-исследовательский институт комплексной автоматизации". – Режим доступу: http://niika.dn.ua/rus/?portfolio=mobilnuy-complex.

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

9. Information Operations / Joint Publication 3-13. – DOD, 2006.− p. 119.

10. Adam T. Elsworth. Electronic warfare. New York.: Nova Science Publishers, 2009.− p. 192.

11. 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.

12. Пухов Г.Е. Преобразования тейлора и их применение в электротехнике и электроние. К.: Наукова думка. – 1978. – 260 с.

13. 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.

14. 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.