

## МОДЕЛЬ ПРОЦЕСУ ПЕРЕХОПЛЕННЯ РАДІОСИГНАЛІВ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В ХОДІ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

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

**Ключові слова:** радіосигнал, атака, інформація, інформаційно-телекомунікаційна система.

**Вступ.** В ході ведення інформаційної боротьби, основний акцент ставиться на атаки, що реалізують вплив на інформаційно-телекомунікаційні системи (ІТС) [1], які призначені для управління збройними силами та іншими структурами державного управління, та системи мовлення, які використовуються засобами масової інформації (ЗМІ). Для здійснення цих атак як основні методи впливу розглядаються: радіоелектронна розвідка (РЕР), радіоелектронне придушення (РЕП) та інформаційний вплив через засоби масової інформації (радіомовлення, телебачення, інформаційні Інтернет ресурси, тощо) [2–3].

Найбільш уразливою частиною ІТС є її безпроводова складова – безпроводові інформаційно-телекомунікаційні системи (БІТС), що є наслідком доступності середовища розповсюдження сигналів.

Невід’ємним етапом реалізації атак РЕР є радіорозвідка – перехоплення радіосигналів від джерел протидіючої сторони 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.

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

Для успішного здійснення інформаційно-психологічного впливу, через засоби БІТС 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 модуляції.

Визначенням характеристик радіосигналів займається радіотехнічна розвідка (РТР). Аналіз сучасних підходів ведення РЕР розвинутих країн, показує, що завдання, які вирішують радіорозвідка та РТР, об’єднані та здійснюються станціями радіо та радіотехнічної розвідки (РПТР). Засоби РПТР призначені для проведення зовнішньої розвідки сигналів – так званої SIGINT (Signals Intelligence) [4]. Характерними прикладами таких станцій є станція РПТР та радіоелектронної війни „Profit” [5], літак радіоелектронної розвідки EC-130E „Commando Solo” [2].

**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 [6–8]. З часом модернізуються методи ведення РЕР та засоби їх реалізації. Радіорозвідка (РПТР), як одна зі складових РЕР, залишається найбільшою загрозою для БІТС.

Для спостереження 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 ґрунтується оцінка рівня захищеності систем, не враховують динаміку протікання інформаційного конфлікту [9], зміну типів атак та їх параметрів в реальному часі.

**Мета.** Зважаючи на приведені доводи постає питання захисту БІТС, які б могли функціонувати в динамічних умовах інформаційної боротьби. Критичним є захист БІТС військових формувань, державних органів, які приймають участь в процесах управління державою, не залежно від форм власності БІТС. 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 моделювання атаки перехоплення радіосигналів та захисних дій МЗІ БІТС. 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 рівноімовірного 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 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 каналному рівнях БІТС.

**Викладення основного матеріалу дослідження.** В процесі розробки захищених БІТС 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. [10]. 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 БІТС (рис. 1).

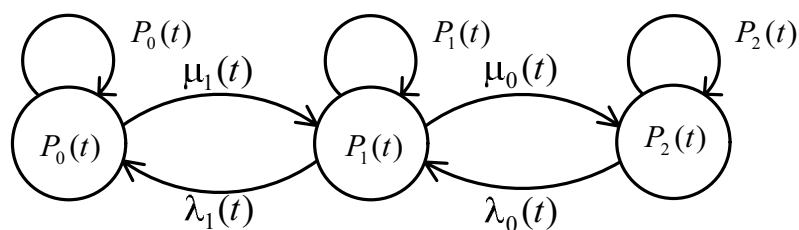


Рис. 1. Граф моделі шаблону нормальної поведінки безпроводових інформаційно-телекомунікаційних систем при перехопленні

Кола представляють собою множину станів  $\{P_z(t)\}$ , де  $z = 0...2$  – 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 трьох станів:

- захищеності БІТС (відображає надійне функціонування БІТС з ефективною роботою механізмів захисту);
- перехоплення радіосигналів (перехоплення та оцінка характеристик радіосигналу БІТС);

– 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 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 перехоплення радіосигналів БІТС, що призведе до отримання збитків;

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

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

Дана послідовність випадкових подій є колом Маркова з двома вихідними станами [11].

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

Саме стратегії конфліктуючих сторін визначають яким буде наслідок протистояння.

Для відображення динаміки протікання процесу перехоплення радіосигналів під час інформаційного конфлікту на інтервалі  $t_0, T$  застосуємо систему диференціальних рівнянь Колмогорова-Чепмена [11]:

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

Система рівнянь (1) дозволить визначити розподіл імовірностей знаходження БІТС 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,

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

та

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

де  $\lambda_i$  та  $\mu_j$  – 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

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

Інтенсивності механізмів захисту, при протидії радіоперехопленню, змінюються в межах

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

Параметри керування гравців  $\lambda_i(t)$  та  $\mu_j(t)$ , які визначають ресурси сторін гри лежать в межах замкнених множин  $\Lambda \in K_\lambda$  та  $M \in K_\mu$ , які в свою чергу обмежені евклідовими просторами  $E_\lambda$  і  $E_\mu$  відповідно [9].

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 БІТС та захисту від цих атак відповідає диференційно-ігровому підходу з безкоаліційним характером ведення гри [12].

Під час інформаційної боротьби 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:

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

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

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

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

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

$$\begin{aligned} \max_{\lambda_i(t) \in E_\lambda} \min_{\mu_j(t) \in E_\mu} &= I(t, P_0(t), \lambda_i(t), \mu_j(t)) = \\ &= \min_{\mu_j(t) \in K_\mu} \max_{\lambda_i(t) \in K_\lambda} = I(t, P_0(t), \lambda_i(t), \mu_j(t)) = \\ &= I(t, P_0^{opt}(t), \lambda_i^{opt}(t), \mu_j^{opt}(t)) = I^G, \end{aligned} \quad (8)$$

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 БІТС для порушника в ході радіорозвідки.

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

$$I(t, P_0^{opt}(t), \lambda_i^{opt}(t), \mu_j^{opt}(t)) = I^G \quad (9)$$

при цьому ціна  $I^G$  – ціна гри.

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

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

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

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

Для подальшого переходу в область зображень використаємо пряме диференційне перетворення [10]. В результаті інформаційний конфлікт, що описаний системою (1), в області  $P$ -зображень матиме вигляд:

$$\begin{cases} P_0(k+1) = \frac{T}{k+1}(-M_1(k)P_0(k) + \Lambda_1(k)P_1(k)) \\ P_1(k+1) = \frac{T}{k+1}(-(\Lambda_1(k) + M_0(k))P_1(k) + M_1(k)P_0(k) + \Lambda_0(k)P_2(k)) \\ P_2(k+1) = \frac{T}{k+1}(-\Lambda_0(k)P_2(k) + M_0(k)P_1(k)), \end{cases} \quad (11)$$

де  $P_z(k)$ ,  $\Lambda_i(k)$ ,  $M_j(k)$  – диференційні зображення оригіналів функцій  $P_z(t)$ ,  $\lambda_i(t)$ ,  $\mu_j(t)$  відповідно, і дискретними функціями цілочислового аргументу  $k = 0, 1, 2, \dots$ .

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  $k \geq 1$ :

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

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

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

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

Визначимо дискрети диференціального спектра диференційно-ігрової моделі ШНП БІТС 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  $P_0(k)$ :

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

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

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

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

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

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

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

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

провівши диференціювання відносно кожного  $\lambda_i$  та  $\mu_j$ .

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

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

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 радіоперехоплення. Таким чином, для моделювання в якості критеріїв приймемо інтенсивності  $\lambda_1$  та  $\mu_1$ . Розрахунку оптимальних значень підлягають всі інтенсивності.

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

$$\lambda_0^{opt} = \frac{226}{15 \cdot T^2} \approx 15,06 \cdot \frac{1}{T^2}, \quad (22)$$

$$\lambda_1^{opt} = \frac{184}{5 \cdot T^2} = 36,8 \cdot \frac{1}{T^2}, \quad (23)$$

$$\mu_1^{opt} = -\frac{226}{15 \cdot T^2} \approx -15,06 \cdot \frac{1}{T^2}. \quad (24)$$

Використаємо зворотні перетворення [10], та переведемо отримані оптимальні коефіцієнти (23) – (24) стратегій гравців в область оригіналів:

$$\lambda_{1 \max}^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{T}\right)^k \cdot \Lambda(k) = 36,8 \cdot \frac{1}{T^2}, \quad (25)$$

$$\mu_{1 \min}^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{T}\right)^k \cdot M(k) \approx -15,06 \cdot \frac{1}{T^2}. \quad (26)$$

Гарантований рівень захищеності  $I^G$  для БІТС від атак радіоперехоплення в ході доби інформаційного конфлікту, з врахуванням початкових умов та інтенсивностей оптимальних стратегій гравців дорівнює  $I^G \approx 15,2$ .

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

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

Для моделювання зміни ШНП БІТС в якості критеріїв приймаються інтенсивності атак перехоплення радіосигналів  $\lambda_1$  та захисних дій від радіоперехоплення МЗІ  $\mu_1$ . Відхилення гравців від оптимальних стратегій (23) та (24) моделі ШНП означає програш в платі.

Диференціально-ігрова модель ШНП БІТС області оригіналів матиме вигляд:

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

Крок зміни інтенсивності атак та захисту прийемо за 0,2. Почергово, при сталому іншому критерії, будемо змінювати інтенсивність  $\lambda_1$ , відносно  $\lambda_1^{opt}$ , та підставляти в (28). Аналогічну процедуру проведемо змінюючи  $\mu_1$ .

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.

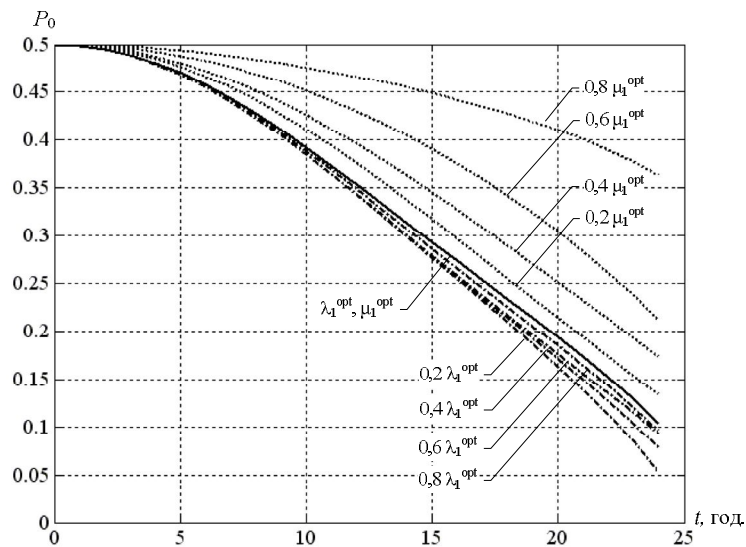


Рис. 2. Графіки ШНП БІТС під час радіоперехоплення

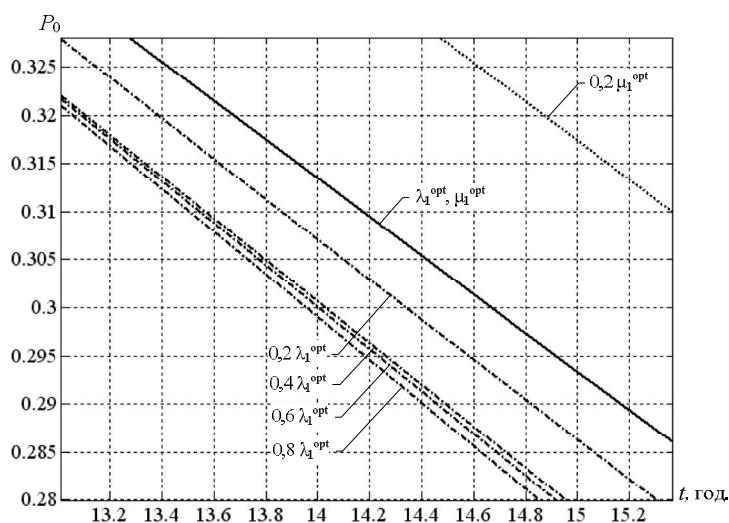


Рис. 3. Масштабована частина графіків ШНП БІТС

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 було проведено моделювання процесів атак перехоплення радіосигналів 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 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 РРТР.

Результати дослідження показали адекватну роботу методики 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 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. 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. Information operations primer. Fundamentals of Information Operations. – Philadelphia, U.S. Army War College, 2006.– p. 168.
7. Information Operations / Joint Publication 3-13. – DOD, 2006.– p. 119.
8. Adam T. Elsworth. Electronic warfare. New York.: Nova Science Publishers, 2009.– p. 192.
9. *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.
10. *Пухов Г.Е.* Преобразования тейлора и их применение в электротехнике и электронике. К.: Наукова думка. – 1978. – 260 с.
11. *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.
12. *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: 26.08.2012р.

Рецензент: д.т.н., проф. Шокало В.М.