УДК 551.510.42

О.Ю. Іохов, В.Г. Малюк, О.М. Горбов

Національна академія Національної гвардії України, Харків

ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ЗАХИЩЕНИХ РАДІОКАНАЛІВ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

У статті розглядається модель захисту інформаційного обміну у радіоканалах тактичної ланки управління сил охорони правопорядку в умовах радіоелектронної протидії з боку противника.

Ключові слова: *канал радіозв'язку, коефіцієнт придушення, імітаційна модель.*

Вступ

Постановка проблеми. У даний час широке розповсюдження у тактичній ланці управління (ТЛУ) радіоканалів військового призначення отримали радіоелектронні засоби (РЕЗ) малої потужності UHV діапазону. Такі радіозасоби мають достатньо широку номенклатуру, яка задовольняє потребам системи тактичного радіозв'язку, але не відповідає вимогам щодо забезпечення захисту інформаційного обміну, оскільки порушник активно впливає на імітостійкість, розвідзахищеність та перешкодозахищеність радіоканалів [1 – 4].

Це робить актуальним питання ефективного застосування засобів радіоелектронної протидії (РЕПр) — сукупності заходів і дій, спрямованих на порушення роботи або зниження ефективності бойового застосування засобів радіоелектронної боротьби противника (ЗРЕБп) шляхом дії на них електромагнітним випромінюванням. РЕПр радіотехнічних засобів досягається застосуванням навмисних радіоперешкод, зміною характеристик відбитих об'єктами сигналів, створенням віддалених цілей і т.п. У статті розглядається варіант РЕПр у вигляді радіоелектронного придушення (РЕП) ЗРЕБп шляхом постановки навмисних радіоперешкод спеціальними групами інформаційної протидії (ГІП).

Відомо, що одним із способів підвищення захищеності інформаційного обміну каналу радіозв'язку (КРЗ) ТЛУ сил охорони правопорядку (СОПр) є використання діаграмо-спрямовуючого пристрою, змонтованого зі штатних засобів активної оборони [1, 4], нормована діаграма спрямованості якого зображена на рис. 1.

Такими діаграмо-спрямовуючими пристроями можуть бути обладнані як підрозділи СОПр, у даному випадку Національної гвардії України (ПНГ), для забезпечення розвідзахищеного радіозв'язку з командним пунктом (КП), так і ГІП у рамках задачі РЕП ЗРЕБп. Для ефективного застосування вищевказаних засобів захисту КРЗ необхідно мати модель взаємодії об'єктів у конкретній оперативній обстановці.

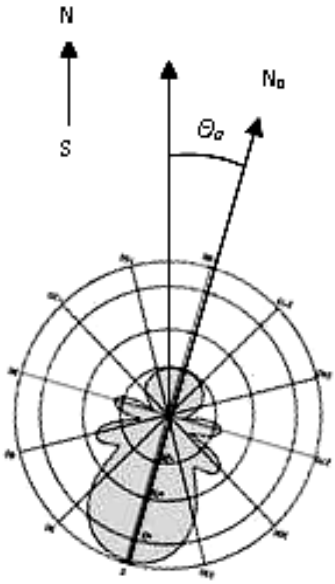

Рис. 1. Діаграма спрямованості мобільного засобу захисту приймача-передавача у радіоканалі ТЛУ СОПр

Аналіз останніх досліджень і публікацій. У роботах [1, 4] розроблена імітаційна модель роботи КРЗ ТЛУ СОПр, яка дозволяє оцінити параметри його перешкодозахищеності відносно ЗРЕБп. У даній моделі відсутні ГІП, які повинні з одного боку виконувати задачі радіоелектронного придушення ЗРЕБп та з іншого боку - не заважати роботі КРЗ. Така нова задача бойового злагоджених дій по виконанню заходів радіоелектронного протистояння потребує доопрацювання вказаної моделі.

Мета статті. Розробка імітаційної моделі радіоелектронного придушення ЗРЕБп для дослідження залежності розвідзахищеності від технічних та просторових характеристик РЕЗ у умовах РЕПр.

Виклад основного матеріалу. Для КРЗ військового призначення введемо поняття захищеності від радіорозвідки, при якому ГІП з одного боку ЗРЕБп подавлені, а з іншого боку вони не впливають на характеристики власних КРЗ. Таким чином, головним завданням при проведенні заходів РЕПр, є дослідження імітаційної моделі РЕП ЗРЕБп.

Імітаційна модель РЕП ЗРЕБп для дослідження залежності захищеності від радіорозвідки відносно технічних та просторових характеристик РЕЗ у умовах РЕП містить об'єкти, які облаштовані РЕЗ із антенами двох типів:

a) **тип 0** – антена ненаправленої дії з рівномірною діаграмою спрямованості;

b) **тип 1** – скритих мобільна направлена антена (СМНА) з діаграмою спрямованості, представленою на рис. 1.

Типовим варіантом будемо вважати ситуацію, коли КП та ЗРЕБп мають тип антени 0, ПНГ та ГІП - тип антени 1. Розглянемо схему утворення перешкод від ГІП для захисту інформаційного обміну ПНГ (рис.2). Параметри об'єктів наведені у табл. 1.

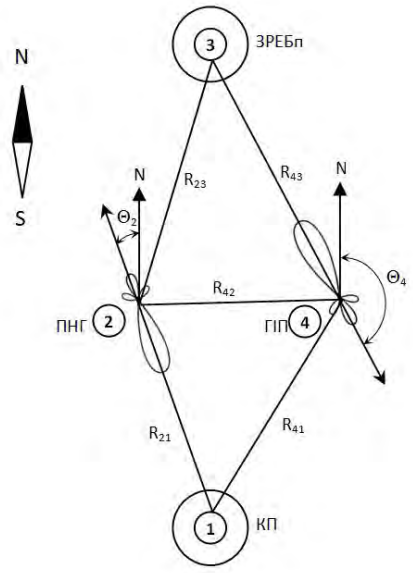

Рис. 2. Схема РЕПр ЗРЕБп для захисту інформаційного обміну від КРЗ ТЛУ СОПр

Відомо, що за енергетичним критерієм приймач засобу радіозв'язку може бути придушений у тому випадку, якщо потужність перешкоди перебільшує деяке порогове значення, характерне для даного виду перешкоди та сигналу, умов їх взаємодії та способу обробки суми сигналу-перешкоди [5].

Коефіцієнт придушення за потужністю є відношення потужностей перешкоди $P_з$ та сигналу $P_с$ на вході приймача, що придушується:

$$K = P_з / P_с . \qquad (1)$$

Простір, в межах якого $K_п$ перевищує задане порогове значення $K_{пор}$, визначається як зона придушення РЕЗ.

За результатами робіт [1, 4] коефіцієнт придушення K_{12} сигналу об'єкту 1 (КП) у точці розташування об'єкту 2 (ПНГ) в присутності джерела перешкод від ГІП маємо у nfгому вигляді:

$$K_{12} = \frac{P_4 G_4 (A_{42} - \theta_4) R_{21}^2}{P_1 G_2 (A_{21} - \theta_2) R_{42}^2}, \qquad (2)$$

Таблиця 1

Параметри об'єктів імітаційної моделі

Об'єкт		Параметр	
№	Назва	Назва	Познач.
1	Командний пункт (КП)	Координати на мапі	x, y
		Потужність передавача	P_1
		Тип антени	TA_1
		Відстань до ЗРЕБп	R_{13}
2	Підрозділ СОПр (ПНГ)	Координати на мапі	x, y
		Потужність передавача	P_1
		Тип антени	TA_1
		Азимут на КП	A_{21}
		Азимут на ЗРЕБп	A_{23}
		Відстань до КП	R_{21}
		Відстань до ЗРЕБп	R_{23}
		Орієнтація	Θ_2
3	ЗРЕБп	Координати на мапі	x, y
		Потужність передавача	P_3
		Тип антени	TA_3
4	Група інформаційної протидії (ГІП)	Координати на мапі	x, y
		Потужність передавача	P_4
		Тип антени	TA_4
		Азимут на КП	A_{41}
		Азимут на ПНГ	A_{42}
		Азимут на ЗРЕБп	A_{43}
		Відстань до КП	R_{41}
		Відстань до ПНГ	R_{42}
		Відстань до ЗРЕБп	R_{43}
		Орієнтація	Θ_4

де G_2 та G_4 - функції залежності коефіцієнту підсилення від азимуту антен приймача ПНГ та передавача радіосигналу ГІП відповідно.

Аналогічним чином одержуємо коефіцієнт придушення K_{21} сигналу об'єкту 2 (ПНГ) у точці розташування об'єкту 1 (КП)

$$K_{21} = \frac{P_4 G_4 (A_{41} - \theta_4) R_{21}^2}{P_2 G_2 (A_{21} - \theta_2) R_{41}^2}, \qquad (3)$$

а також коефіцієнт придушення K_{13} сигналу об'єкту 1 (КП) у точці розташування об'єкту 3 (ЗРЕБп)

$$K_{13} = \frac{P_4 G_4 (A_{43} - \theta_4) R_{13}^2}{P_1 R_{43}^2}, \qquad (4)$$

та коефіцієнт придушення K_{23} сигналу об'єкту 2 (ПНГ) у точці розташування об'єкту 3 (ЗРЕБп)

$$K_{23} = \frac{P_4 G_4 (A_{43} - \theta_4) R_{23}^2}{P_2 G_2 (A_{23} - \theta_2) R_{43}^2}. \qquad (5)$$

Бойову задачу ГІП можна вважати виконаною, якщо при заданих параметрах об'єктів оперативної обстановки та порогових значень коефіцієнтів придушення одночасно виконуються логічні співвідношення

$$L_1 = K_{12} \le K_{пор1}, \qquad (6.1)$$

$$L_2 = K_{21} \le K_{пор1}, \qquad (6.2)$$

$$L_3 = K_{13} \ge K_{пор2}, \qquad (6.3)$$

$$L_4 = K_{23} \ge K_{пор2}. \qquad (6.4)$$

тобто КРЗ між КП та ПНГ працює у штатному режимі (співвідношення 6.1 та 6.2), а ЗРЕБп опиняється у зоні придушення (співвідношення 6.3 та 6.4). Виконання задачі (2-6) досягається у першу чергу шляхом зміни орієнтації антен ПНГ та ГІП (параметри θ_2 та θ_4 відповідно), а також зміною потужності РЕЗ КП, ПНГ, ГІП та їх взаємного розташування.

У разі необхідності кількість ГІП може бути збільшена. Для комплексу радіоелектронного придушення, який складається з N джерел перешкод, утворюваних ГІП, за принципом суперпозиції маємо

$$К_{12} = \frac{R_{21}^2}{P_1 G_2 (A_{21} - \theta_2)} \sum_{i=1}^{N} \frac{P_{4_i} G_{4_i} (A_{42_i} - \theta_{4i})}{R_{42_i}^2}, \quad (7)$$

$$К_{21} = \frac{R_{21}^2}{P_2 G_2 (A_{21} - \theta_2)} \sum_{i=1}^{N} \frac{P_{4_i} G_{4_i} (A_{41_i} - \theta_{4i})}{R_{41_i}^2}, \quad (8)$$

$$К_{13} = \frac{R_{13}^2}{P_1} \sum_{i=1}^{N} P_{4_i} G_{4_i} (A_{43_i} - \theta_{4i}) \Big/ R_{43_i}^2, \quad (9)$$

$$К_{23} = \frac{R_{23}^2}{P_2 G_2 (A_{23} - \theta_2)} \sum_{i=1}^{N} \frac{P_{4_i} G_{4_i} (A_{43_i} - \theta_{4i})}{R_{43_i}^2}, \quad (10)$$

де G_{4_i} – функція коефіцієнту підсилення антени передавача радіосигналу і -ї ГІП (i = 1..N); P_{4_i}, та R_{41_i}, R_{42_i}, R_{43_i} – відповідні параметри і -ої ГІП (i = 1..N) (табл.1).

Виконання задачі (6-10) досягається шляхом зміни параметру θ_2 для ПНГ та відповідної множини параметрів $\Theta_4 = \{\theta_{4_1}, \theta_{42}, ..., \theta_{4N}\}$ для комплексу ГІП.

З метою формалізації задачі (6-10) подамо імітаційну модель захисту КРЗ із засобами РЕП у вигляді кінцевого автомата Мура. Вхідним алфавітом моделі є множина **X** = {x_2, x_4}, де x_2 – множина режимів роботи захисту ПНГ ($x_2 = \bar{D}_2$ – захист відсутній, $x_2 = D_2$ – захист встановлено); x_4 - множина режимів роботи ГІП ($x_4 = \bar{D}_4$ – радіопридушення відсутнє, $x_4 = D_4$ – режим радіопридушення встановлено). Вихідним алфавітом моделі є множина **Y** = { Y_0, Y_1}, де Y_0 – невиконання бойової задачі, Y_1 – виконання бойової задачі (6-10).

У залежності від ситуативного сполучення параметрів засобів радіоелектронного впливу маємо множину станів **Q**={ Q_0, Q_1, Q_2, Q_3} моделі захисту інформаційного обміну КРЗ із засобами РЕП, де:

1. Q_0 – відсутність захисту. Означає відсутність захисту ПНГ ($x_2 = \bar{D}_2$) та режиму радіопридушення ГІП ($x_4 = \bar{D}_4$), що однозначно призводить до невиконання умов (6), тобто невиконання бойової задачі (Y_0).

2. Q_1 – частковий захист ПНГ. Означає встановлений захист ПНГ ($x_2 = D_2$) за умов відсутності режиму радіопридушення ГІП ($x_4 = \bar{D}_4$), що обумовлює неоднозначність виконання умов (6), тобто не завжди забезпечує виконання бойової задачі.

3. Q_2 – частковий захист ГІП. Означає відсутність захисту ПНГ ($x_2 = \bar{D}_2$) при ввімкненому режимі радіопридушення ГІП ($x_4 = D_4$), що обумовлює неоднозначність виконання умов (6), тобто не завжди забезпечує виконання бойової задачі.

4. Q_3 - комплексний захист. Означає встановлений захист ПНГ ($x_2 = D_2$) при ввімкненому режимі радіопридушення ГІП ($x_4 = D_4$), що як правило забезпечує виконання бойової задачі (Y_1).

Слід зазначити, що у перехідних станах Q_1 та Q_2 за відсутності комплексного захисту ймовірність виконання бойової задачі (6-10) залишається низькою.

При дискретному поданні модельного часу t=0,1,2,.. T_k функція переходів

$$q(t+1) = \delta(q(t), x(t))$$

та функція виходів

$$y(t) = \lambda(q(t))$$

моделі задаються співвідношеннями

$$\begin{gathered}
\delta(Q_0, \bar{D}_2, \bar{D}_4) = Q_0; \qquad \delta(Q_0, D_2, \bar{D}_4) = Q_2; \\
\delta(Q_0, \bar{D}_2, D_4) = Q_1; \\
\delta(Q_2, D_2, \bar{D}_4) = Q_2 \quad ; \quad \delta(Q_2, \bar{D}_2, \bar{D}_4) = Q_0; \\
\delta(Q_2, D_2, D_4) = Q_3; \qquad (11) \\
\delta(Q_1, \bar{D}_2, D_4) = Q_1; \qquad \delta(Q_1, \bar{D}_2, \bar{D}_4) = Q_0; \\
\delta(Q_1, D_2, D_4) = Q_3; \\
\delta(Q_3, D_2, D_4) = Q_3; \qquad \delta(Q_3, \bar{D}_2, D_4) = Q_1; \\
\delta(Q_3, D_2, \bar{D}_4) = Q_2
\end{gathered}$$

$$\lambda(q) = \begin{cases} Y_1 \text{ при виконанні співвідношень (6)} \\ Y_0 \text{ у інших випадках} \end{cases} \quad (12)$$

Граф станів моделі наведений на рис. 3, алгоритм моделювання – на рис. 4.

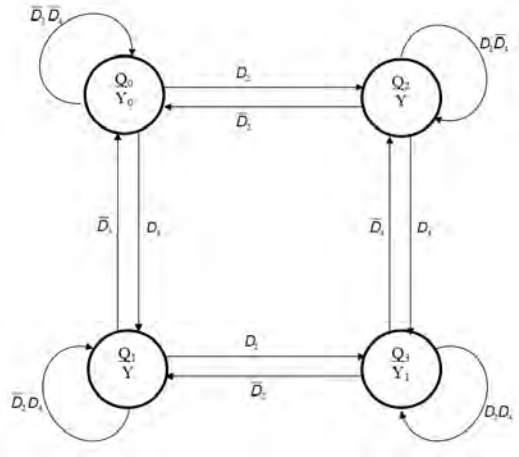

Рис. 3. Граф станів моделі захисту інформаційного обміну КРЗ із засобами РЕП

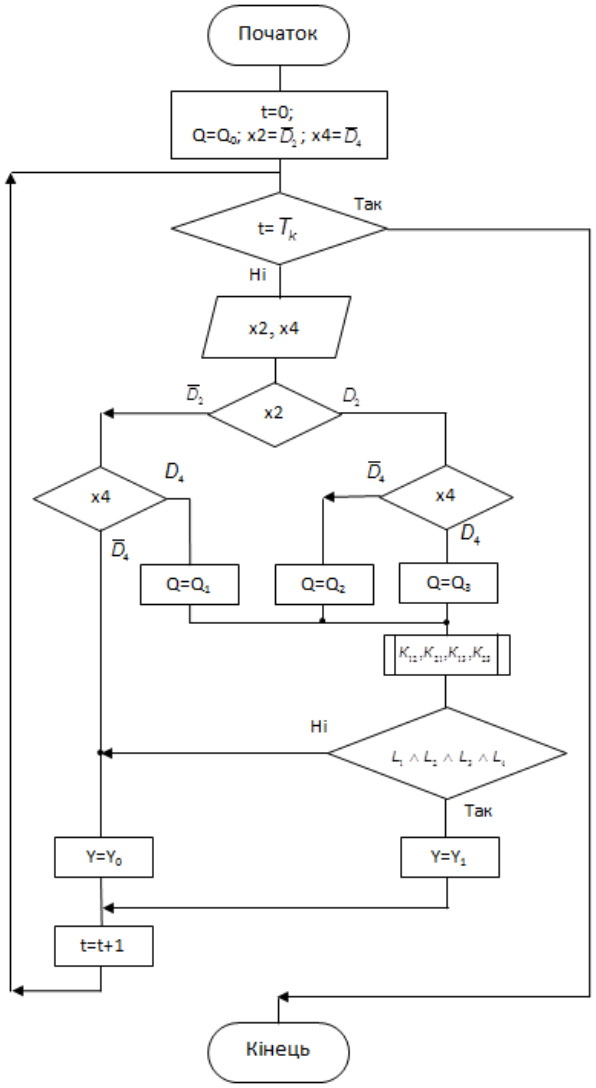

Рис. 4. Алгоритм моделювання захисту інформаційного обміну КРЗ із засобами РЕП

Для обчислення оптимальних параметрів захисту інформаційного обміну КРЗ військового призначення із засобами РЕП розроблена програма комп'ютерного моделювання роботи груп інформаційної протидії «ІМІР», інтерфейс якої представлений на рис. 5. Головна форма програми має рядок меню, панель інструментів, фрейми об'єктів, фрейми режимів роботи з мапою, інформаційні фрейми. Центральним елементом інтерфейсу програми є мапа, на якій за допомогою мишки вказується розміщення КП, ПНГ, ЗРЕБп та ГІП.

Робота з програмою починається із завантаження з файлу схематичного або супутникового зображення мапи місцевості. Далі необхідно виконати операцію калібрування, тобто обчислення масштабу мапи шляхом протягування маркеру миші уздовж об'єкту на мапі, довжина якого заздалегідь відома.

Обчислення коефіцієнтів придушення та аналіз стану виконання бойової задачі за співвідношеннями (6-10) вмикаються автоматично після визначення параметрів усіх об'єктів. Ця операція також виконується автоматично при зміні орієнтації РЕЗ ПНГ або ГІП.

Виконання задачі (6-10) досягається шляхом зміни параметру θ_2 для ПНГ та відповідної множини параметрів

$$\Theta_4 = \left\{\theta_{4_1}, \theta_{42}, ..., \theta_{4N}\right\}$$

для комплексу ГІП. Перемикачами «Вручну» та «Автоматично» у розділі «Орієнтація» фреймів ПНГ та ГІП можна змінювати режим вибору орієнтації РЕЗ цих об'єктів. У ручному режимі кути θ_2 та θ_{4N} визначаються за допомогою відповідних лічильників, розташованих на формі.

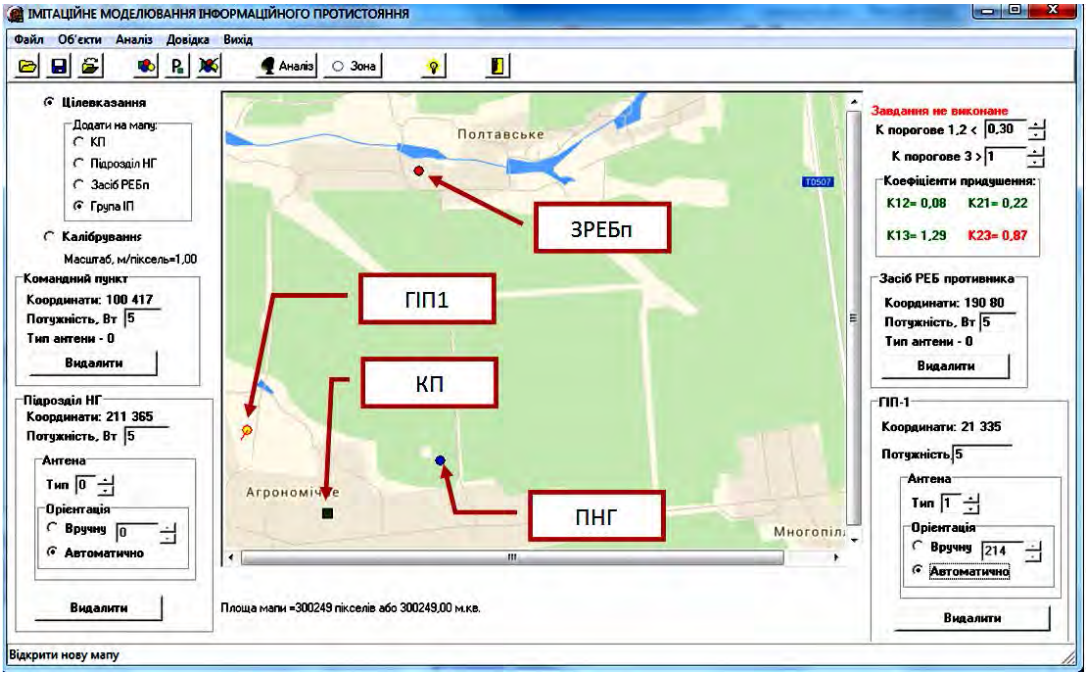

Рис. 5. Програма моделювання захисту інформаційного обміну КРЗ із засобами РЕП

У автоматичному режимі оптимальний кут θ_2^* обчислюється таким чином, щоб у точці розташування ПНГ придушення сигналу з КП з боку ЗРЕБп було мінімальним:

$$K_2\left(\theta_2^*\right) = \frac{P_3 G_2\left(A_{23} - \theta_2^*\right) R_{21}^2}{P_1 G_2\left(A_{21} - \theta_2^*\right) R_{23}^2} \to \min . \quad (13)$$

Множина оптимальних кутів

$$\Theta_4^* = \left\{\theta_{4_1}^*, \theta_{4_2}^*, ..., \theta_{4_N}^*\right\}$$

обчислюється з використанням співвідношення (10) таким чином, щоб у точці розташування ЗРЕБп придушення сигналу ПНГ з боку ГІП було максимальним:

$$K_{23}\left(\Theta_4^*\right) = R_{23}^2 \Big/ \left(P_2 G_2\left(A_{23} - \theta_2\right)\right) \times$$
$$\times \sum_{i=1}^{N} P_{4_i} G_{4_i}\left(A_{43_i} - \theta_{4_i}^*\right) \Big/ R_{43_i}^2 \to \max . \quad (14)$$

Після обчислень (6-10) визначається стан моделі за співвідношеннями (11) та функція виходів (12). Розраховані значення, K_{12}, K_{21}, K_{13} або K_{23}, які не задовольняють умовам (6), виводяться на форму червоним кольором, а ті, що задовольняють - зеленим кольором.

Якщо $\lambda(q)$ приймає значення Y_0, на форму виводиться повідомлення «Завдання не виконане» червоним кольором, для $\lambda(q)=Y_1$ – повідомлення «Завдання виконане» зеленим кольором.

Маніпулюючи такими параметрами ПНГ та ГІП, як потужність, орієнтація та тип антени, можна переводити модель у стан Q_1, Q_2 або Q_3.

Слід зазначити, що у перехідних станах Q_1 та Q_2 за відсутності комплексного захисту ймовірність виконання бойової задачі (6-10) залишається низькою.

Висновки

Розроблена імітаційна модель захисту інформаційного обміну КРЗ військового призначення, на відміну від відомих, враховує дії ГІП, з використанням різних типів засобів РЕПр, та дозволяє визначити залежність розвідзахищеності радіоліній ПНГ та КП від коефіцієнта взаємного впливу ЗРЕБп та засобів ГІП.

Програмна реалізація імітаційної моделі захисту інформаційного обміну КРЗ дозволяють простежити залежність захищеності від радіорозвідки та визначити оптимальні параметри використання скритих мобільних направлених антен, у складі ГІП та радіоліній ПНГ ефективність ГІП в умовах РЕПр з боку порушника.

Список літератури

1. Оцінювання завадостійкості каналу радіозв'язку тактичної ланки управління підрозділами внутрішніх військ методом імітаційного моделювання [Текст] / О.Ю. Іохов, І.В. Кузьминич, В.Г. Малюк, О.В. Сєвєрінов // Системи управління, навігації та зв'язку : збірник наукових праць. – Полтава : ПНТУ, 2013. – Вип. 3 (27). – С. 153-158.

2. Основні аспекти радіоелектронного захисту системи радіозв'язку тактичної ланки управління внутрішніх військ МВС України під час виконання завдань за призначенням [Текст] / О.Ю. Іохов, В.В. Антонець, О.М. Горбов, І.В. Кузьминич, В.В. Овчаренко // Честь і Закон. – Х. : Академія ВВ МВС України, 2012. – № 4. – С. 40-48.

3. Захист інформації у каналах управління підрозділів внутрішніх військ МВС України / Ю.П. Белокурський, О.М. Горбов, О.Ю. Іохов, В.Є. Козлов, І.В. Кузьминич, О.О. Щербина // Збірник наукових праць Академії ВВ МВС України. – Х. : АВВ МВС України, 2013. – № 1. – С. 63-66.

4. Малюк В.Г. Метод визначення меж зони стійкого радіообміну підрозділів внутрішніх військ в умовах радіопридушення [Текст] / В.Г. Малюк, О.Ю. Іохов, І.В. Кузьминич // Системи озброєння та військова техніка. – 2014. – № 1 (37). – С. 56-61.

5. Куприянов А.И. Теоретические основы радиоэлектронной борьбы [Текст]: Учеб, пос. / А.И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.

Надійшла до редколегії 29.01.2015

Рецензент: д-р техн. наук проф. О.О. Морозов, Національна академія Національної гвардії України, Харків.

ИМИТАЦИОННОЕ МОДЕЛИРОВАНИЕ ЗАЩИЩЕННЫХ РАДИОКАНАЛОВ ВОЕННОГО НАЗНАЧЕНИЯ

А.Ю. Иохов, В.Г. Малюк, А.М. Горбов

Рассматриваются принципы построения компьютерной модели информационной защиты радиоканала связи тактического звена управления сил охраны правопорядка в условиях работы средств радиоэлектронной борьбы противника.

Ключевые слова: *канал радиосвязи, коэффициент подавления, имитационная модель.*

SIMULATION OF PROTECTED MILITARY RADIO CHANNELS

O.Yu. Iohov, V.H. Malyuk, O.M. Gorbov

The principles of construction of computer models of information security radio communication tactical control of the security forces in the working conditions of electronic warfare enemy.

Keywords*: radio channel, the suppression factor, simulation model.*