УДК 004.9:517.978.2

Р.В. Грищук, О.О. Хмара

Житомирський військовий інститут імені С.П. Корольова НАУ, Житомир

МЕТОДИКА ОЦІНЮВАННЯ ГАРАНТОВАНОГО РІВНЯ ЗАХИЩЕНОСТІ ТЕХНІЧНИХ ОБ'ЄКТІВ

В статті розроблено методику оцінювання гарантованого рівня захищеності технічних об'єктів від методів несанкціонованого доступу. Методика базується на диференціально-ігровій постановці задачі оцінювання і застосуванні диференціально-тейлорівських перетворень, що у сукупності дозволяють отримувати кількісні оцінки гарантованого рівня захищеності.

Ключові слова: *гарантований рівень захищеності, диференціальна гра, диференціально-тейлорівські перетворення, ціна гри, сідлова точка, стратегія.*

Вступ

Постановка проблеми. Нагальна потреба забезпечення безпечного функціонування технічних об'єктів (ТО) в складі інформаційно-телекомунікаційних систем (ІТС) потребує оцінки рівня їх захищеності від методів несанкціонованого доступу (НСД) до інформації, яка циркулює в контурі їх управління [1 – 5].

Ряд причин проблемного характеру практично ускладнюють проведення процедури оцінювання рівня захищеності ТО [6]. Серед основних проблем можна відмітити наступні: процедура оцінювання не формалізована (відсутні адекватні математичні моделі); висока різноманітність методів НСД та випадкова природа їх застосування суб'єктом, що атакує; недетермінована природа розподілу інформаційних ресурсів суб'єктів інформаційного конфлікту тощо.

Таким чином, виходячи із зазначеного, в умовах невизначеності можна стверджувати про можливість проведення процедури оцінювання, що забезпечує з деякою ймовірністю лише гарантований рівень захищеності ТО. Тому, в рамках вирішення проблеми захисту інформації, задача розробки відповідних методик є актуальною.

Аналіз останніх досліджень [1 – 5] **і публікацій** [7 – 12] показує значну увагу фахівців до розробки відповідних методик оцінювання рівня захищеності ТО. Але, станом на сьогоднішній день, чіткої і формалізованої методики оцінювання гарантованого рівня захищеності знайти не вдалося.

Так в [9 – 12] для оцінювання застосовуються якісні підходи. До недоліків таких методик можна віднести їх значну залежність від суб'єктивних факторів, що впливають на якість оцінювання.

Інші відомі методики [1-3, 5] – це кількісні. Перевагою таких методик, порівняно з якісними, є можливість отримання за ними кількісного показника, що виражає рівень захищеності на момент проведення процедури оцінювання. Недоліком – відповідно статична природа процедури оцінювання, яка носить миттєвий характер і потребує достатнього об'єму статистичних даних про ймовірність реалізації відповідних загроз.

Таким чином, як зрозуміло з проведеного аналізу, відомі методики потребують подальшого удосконалення, основними напрямами якого можуть бути такі – усунення з процедури оцінювання експерта (з метою виключення суб'єктивізму отримуваних оцінок) та розробка математичних моделей, застосування яких надасть можливість отримувати кількісну оцінку рівня захищеності ТО, не нижче гарантованої.

Метою статті є розробка методики оцінювання гарантованого рівня захищеності технічних об'єктів.

Виклад основного матеріалу

В основу методики покладено гіпотезу академіка НАН України М.З. Згуровського [13], про принципове обмеження достовірності опису ТО, гарантований рівень захищеності якого підлягає оцінюванню.

Суть гіпотези може бути інтерпретована у вигляді наступного твердження: ТО в складі ІТС принципово не може мати опису з абсолютною повнотою, абсолютною достовірністю та абсолютною точністю із застосуванням будь-яких методів і моделей будь-яких аксіоматичних теорій і (або) будь-яких методів і моделей, що ґрунтуються на використанні будь-яких баз знань і баз даних, отриманих і перевірених експериментально.

Тому, виходячи із природи інформаційних конфліктів [14, 15], основою яких є антагонізм інтересів суб'єктів конфлікту протягом деякого часу його протікання, розроблена в статті методика ґрунтується на диференціально-ігровому підході до моделювання процесів нападу на інформацію диференціально-тейлорівськими перетвореннями (ДТ-перетвореннями), основи якого розроблено в працях [16 – 22].

Методика складається з таких етапів.

1 етап: формалізація задачі.

Математична модель інформаційного конфлікту описується системою диференціальних рівнянь Колмогорова-Чепмена загального вигляду

$$\frac{dP_i(t)}{dt} = f_i(\lambda_i(t), \mu_i(t), P_1(t), P_2(t), \dots P_{n-1}(t)); \quad i = 0,1,\dots,n-1, \tag{1}$$

де $P_i(t)$ – змінні, $n-1$ - вимірного фазового простору R_{n-1}, що характеризує процеси в області $P \in R_{n-1}$ з відповідним значенням ймовірності перебування у даному стані;

$\lambda_i(t)$, $\mu_i(t)$ - інтенсивності потоків розподілу інформаційних ресурсів гравців, що захищається і нападає, які відповідно належать $\Lambda \in E_\lambda$, $M \in E_\mu$ замкненим обмеженим у евклідових просторах R_λ і R_μ множинам, що визначають можливі стратегії гравців за наступних початкових умов $P_0(0) = 1$, $P_1(0) = \dots = P_{n-1}(0) = 0$ і умов нормування $\sum_{i=0}^{n-1} P_i(t) = 1$.

2 етап: припущення та обмеження.

Передбачається, що процедура оцінювання проводиться на деякому інтервалі часу t, що дорівнює

$$t \in [t_0, T], \tag{2}$$

де t_0 – час початку інформаційного конфлікту;

T – час закінчення інформаційного конфлікту.

Вважається, що розподіли інформаційних ресурсів гравців описуються нестаціонарними моделями загального вигляду

$$\lambda_i(t) = \lambda_{i0} + \lambda_{i1} t, \tag{3}$$

$$\mu_i(t) = \mu_{i0} + \mu_{i1} t, \tag{4}$$

де λ_{i0}, μ_{i0} – початкові значення інформаційних ресурсів відповідних гравців на момент початку інформаційного конфлікту t_0;

λ_{i1}, μ_{i1} – інтенсивності зміни інформаційних ресурсів відповідних гравців в процесі інформаційного конфлікту на інтервалі (2).

У окремих частинних випадках моделі (3) і (4) можуть мати і стаціонарну природу, яка випливає з рівності параметрів λ_{i1} і μ_{i1} нулю.

Ресурс гравців (3) і (4), на інтервалі (2), обмежений лінійними нерівностями вигляду

$$\lambda_{i\min}(t) \le \lambda_i(t) \le \lambda_{i\max}(t), \tag{5}$$

$$\mu_{i\min}(t) \le \mu_i(t) \le \mu_{i\max}(t), \tag{6}$$

де $\lambda_{i\min}(t)$ і $\mu_{i\min}(t)$ – мінімальні, а $\lambda_{i\max}(t)$ і $\mu_{i\max}(t)$ – максимальні інтенсивності потоків захисних дій та інформаційних атак, відповідно.

3 етап: визначення оптимальних стратегій поведінки гравців.

Визначення оптимальних стратегій поведінки гравців $\lambda_i^{opt}(t)$ і $\mu_i^{opt}(t)$ здійснюється з метою вибору із множин допустимих стратегій E_λ і E_μ тільки тих, що доставлятимуть інтегральному критерію оптимізації – платі I_0, що дорівнює

$$I_0 = \frac{1}{T}\int_0^T P_0(t)\,dt, \tag{7}$$

деякий максимінний виграш, тобто

$$I_0^* = \min_{\lambda_i(t) \in E_\lambda} \max_{\mu_i(t) \in E\mu} I_0. \tag{8}$$

Плата I_0 (7) є усередненою на інтервалі моделювання (2) ймовірністю перебування ТО під впливом методів НСД, де $P_0(t)$ - модель процесу нападу на інформацію, що є ймовірністю перебування ТО під впливом методів НСД.

Для пошуку оптимальних стратегій $\lambda_i^{opt}(t)$ і $\mu_i^{opt}(t)$ згідно сформульованого принципу (8) потрібно плату (7) подати аналітичною моделлю та дослідити її на екстремум.

Аналітичний вираз для плати (7) знаходиться за допомогою ДТ-перетворень академіка НАН України Г.Є. Пухова [23 – 25]. Метод отримання таких моделей запропоновано у [26].

В області зображень плата I_0 (7) з використанням ДТ-перетворень матиме вигляд [23]

$$I_0^* = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1}, \tag{9}$$

де $P_0(k)$ – зображення моделі процесу нападу на інформацію області зображень [24];

k – цілочисельний аргумент $k =: 0, 1, 2, \dots$.

Необхідні умови мінімуму в задачі оптимізації функціонала (9)

$$\begin{cases} \dfrac{\partial I_0^*(\lambda_i(t),\ \mu_i(t))}{\partial \lambda_i} = 0; \\ \dfrac{\partial I_0^*(\lambda_i(t),\ \mu_i(t))}{\partial \mu_i} = 0, \end{cases} \tag{10}$$

зводяться до системи лінійних алгебраїчних рівнянь (СЛАР) з двома невідомими відносно $\lambda_i^{opt}(t)$ і $\mu_i^{opt}(t)$.

Отримані розв'язки СЛАР

$$\lambda_i^{opt}(t) \text{ і } \mu_i^{opt}(t)$$

забезпечують мінімум (10) при виконанні достатніх умов:

$$\begin{cases} \dfrac{\partial^2 I_0^*\left(\lambda_i^{opt}(t),\ \mu_i^{opt}(t)\right)}{\partial \lambda_i^{opt\,2}} > 0; \\ \dfrac{\partial^2 I_0^*\left(\lambda_i^{opt}(t),\ \mu_i^{opt}(t)\right)}{\partial \mu_i^{opt\,2}} < 0. \end{cases} \tag{11}$$

4 етап: оцінювання гарантованого рівня захищеності.

Оцінка рівня захищеності ТО, не нижче гарантованого, забезпечується застосуванням гарантуючої стратегії розподілу інформаційних ресурсів гравцем, що захищається на основі сформульованого принципу мінімакса (8).

При цьому враховується, що другий гравець, який атакує, обирає стратегію $\mu_i(t)$, що максимізує плату (7), за умови її мінімізації першим гравцем

$$I_0^* = \max_{\mu_i(t)\ \in E\mu}\ \min_{\lambda_i(t)\ \in E\lambda} I_0. \tag{12}$$

Якщо виконується умова рівності нижньої (8) і верхньої границь (12)

$$\begin{aligned} &I_0^*\left(\lambda_i^{opt}(t),\ \mu_i^{opt}(t)\right) = \\ &= \min_{\lambda_i(t)\in E\lambda}\ \max_{\mu_i(t)\in E\mu} I_0 = \\ &= \max_{\mu_i(t)\in E\mu}\ \min_{\lambda_i(t)\in E\lambda} I_0, \end{aligned} \tag{13}$$

то в диференціальній грі існує сідлова точка.

Плата $I_0^*\left(\lambda_i^{opt}(t),\ \mu_i^{opt}(t)\right)$ (13) при такому виборі гравцями оптимальних стратегій називається ціною гри, а відповідно і гарантованим рівнем захищеності технічного об'єкту від методів несанкціонованого доступу.

Гарантованість оцінювання рівня захищеності технічного об'єкту не менше оціненого (13) забезпечується тим, що відхилення гравцями від своїх оптимальних стратегій призведе до програшу ними в платі

$$\begin{aligned} &I_0^*\left(\lambda_i(t), \mu_i^{opt}(t)\right) \ge \\ &\ge \min_{\lambda_i(t)\ \in E\lambda} I_0\left(\lambda_i^{opt}(t), \mu_i^{opt}(t)\right); \end{aligned} \tag{14}$$

$$\begin{aligned} &I_0^*\left(\lambda_i^{opt}(t), \mu_i(t)\right) \le \\ &\le \max_{\mu_i(t)\ \in E\mu} I_0\left(\lambda_i^{opt}(t), \mu_i^{opt}(t)\right). \end{aligned} \tag{15}$$

Дане твердження забезпечується властивістю сідлової точки гри [27].

Продемонструємо працеспроможність розробленої методики на модельному прикладі.

Нехай ТО, в складі ІТС, що вводиться в експлуатацію може перебувати у трьох станах – незахищеному, захищеному з відомими вразливостями та захищеному з відповідними ймовірностями $P_0(t)$, $P_1(t)$ та $P_2(t)$. На момент введення в експлуатацію ТО перебуває під впливом методів НСД, тобто $P_0(t_0 = 0) = 1$. Графова модель процесу нападу на інформацію для таких станів ТО подана на рис. 1.

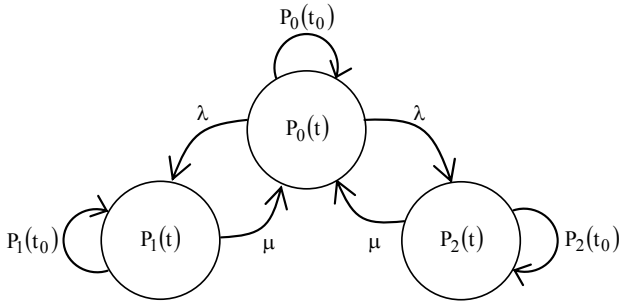

Рис. 1. Графова модель

Потрібно визначити гарантований рівень захищеності ТО, якщо інформаційний конфлікт триває 1 сек. Розподіл інформаційних ресурсів гравців – стаціонарний.

1. Формалізуємо задачу згідно (1). Тоді математична модель інформаційного конфлікту матиме вигляд (рис. 1)

$$\begin{cases} \dfrac{dP_0(t)}{dt} = -2\lambda P_0(t) + \mu P_1(t) + \mu P_2(t); \\ \dfrac{dP_1(t)}{dt} = -\mu P_1(t) + \lambda P_0(t); \\ \dfrac{dP_2(t)}{dt} = -\mu P_2(t) + \lambda P_1(t). \end{cases} \tag{16}$$

2. Припущення та обмеження. Інформаційний конфлікт триває протягом деякого часу t, що дорівнює

$$t \in [0, 1] \text{ сек.} \tag{17}$$

Стаціонарний розподіл інформаційних ресурсів під час інформаційного конфлікту може бути подано моделями

$$\lambda(t) = \lambda \Rightarrow \text{const}, \tag{18}$$

$$\mu(t) = \mu \Rightarrow \text{const}. \tag{19}$$

В силу стаціонарної природи розподілу інформаційних ресурсів гравців (18) і (19), обмеження (3) і (4), на інтервалі (17), трансформуються до виразів вигляду

$$\lambda(t)=\lambda_{min}=\lambda_{max}=\lambda, \quad (20)$$

$$\mu(t)=\mu_{min}=\mu_{max}=\mu. \quad (21)$$

3. Визначення оптимальних стратегій.

З використанням ДТ-перетворень [23] палата (7) запишеться аналітичним виразом вигляду

$$I_0^*=1-\lambda T+\frac{1}{3}\lambda\left(2\lambda+\mu\right)T^2- \\ -\frac{1}{12}\lambda^3\left(\mu^2+4\lambda+2\mu+2\lambda\mu\right)T^3. \quad (22)$$

Виконання необхідних умов (10) зводиться до СЛАР вигляду

$$\begin{cases}1-\frac{1}{3}\left(4\lambda^{opt}+\mu^{opt}\right)T=0;\\ 1-\frac{1}{2}\left(2\lambda^{opt}+\mu^{opt}\right)T=0.\end{cases} \quad (23)$$

Рішення СЛАР (23) методом виключання Гауса дає змогу визначити оптимальні стратегії розподілу ресурсів гравцями

$$\lambda^{opt}=\frac{1}{2T}, \quad (24)$$

$$\mu^{opt}=\frac{1}{T}. \quad (25)$$

Оскільки достатні умови (11) виконуються, тобто

$$\begin{cases}\frac{\partial^2 I_0^*\left(\lambda_i^{opt}(t),\ \mu_i^{opt}(t)\right)}{\partial\lambda_i^{opt\,2}}=\frac{4}{3}T^2>0;\\ \frac{\partial^2 I_0^*\left(\lambda_i^{opt}(t),\ \mu_i^{opt}(t)\right)}{\partial\mu_i^{opt\,2}}=-\frac{1}{12}T^2<0,\end{cases} \quad (26)$$

де $T>0$, то відповідні стратегії є оптимальними і існує сідлова точка гри.

4. Оцінювання гарантованого рівня захищеності.

Оскільки розподіл інформаційних ресурсів гравців (18) і (19) стаціонарний та виконуються необхідні і достатні умови (10) і (26) відповідно, то ціна гри (13) дорівнює

$$I_0^*\left(\lambda^{opt},\ \mu^{opt}\right)=\frac{2}{3}. \quad (27)$$

Таким чином, гарантований рівень захищеності ТО від методів НСД за заданих умов дорівнює $2/3$.

Покажемо, що відхилення гравцями від оптимальних стратегій призведе до програшів та виграшів ними у платі, відповідно до (14) і (15) (табл. 1).

Таблиця 1

Розрахунок плати при відхилення гравцями від оптимальних стратегій

Гравець	Стратегія	Плата
I	$\lambda=\frac{1}{2}\lambda^{opt}$	$\frac{53}{64}$
II	μ^{opt}	
I	λ^{opt}	$\frac{2}{3}$
II	μ^{opt}	
I	λ^{opt}	$\frac{21}{32}$
II	$\mu=\frac{1}{2}\mu^{opt}$	

Як видно із таблиці умови (14) та (15) виконуються, що свідчить про коректність постановки задачі оцінювання гарантованого рівня захищеності і, власне, отриманих результатів.

Висновки

Набула подальшого розвитку методологія оцінювання рівня захищеності технічних об'єктів від методів несанкціонованого доступу, що відрізняється від відомих можливістю отримання кількісних оцінок гарантованого рівня захищеності. Достовірність отримуваних оцінок підтверджується коректною постановкою задачі оцінювання у вигляді диференціальної гри двох гравців з антагоністичними інтересами і застосуванням теоретично обґрунтованого і широко апробованого на практиці методу ДТ-перетворень.

Напрямом подальших досліджень є розробка оптимальної (раціональної) системи захисту інформації ТО, з метою забезпечення гарантованого рівня захищеності, розрахованого за отриманою методикою.

Список літератури

1. Козлов В.С. Количественная оценка защищённости информации / В.С. Козлов, В.А. Хорошко // Захист інформації. – К. : НАУ, 2003. – № 4. – С. 67-73.

2. Андреев В.И. Количественная оценка защищённости технических объектов с учётом их функционирования / В.И. Андреев, В.С. Козлов, В.А. Хорошко // Захист інформації. – К. : НАУ, 2004. – № 2. – С. 47-50.

3. Козлова К.В. Кількісна оцінка захисту радіоелектронних об'єктів (РЕО) / К.В. Козлова, В.О. Хорошко // Захист інформації. – К. : ДІТС, 2007. – № 1. – С. 30-32.

4. ДСТУ 3396.0-96. Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

5. Метод количественной оценки защищённости информации в компьютерной системе / Т.В. Григорьева, С.М. Иванов, А.П. Панфилов и др. // Информационное противодействие угрозам терроризма. – М. : ФГПУ НТЦ, 2008. – Вып. 11. – С. 153-162.

6. Хорошко В.А. Информационная безопасность Украины: основные проблемы и перспективы / В.А. Хо-

рошко // Захист інформації – К. : ДУІКТ, 2008. – № 40 (спец. випуск) – С. 6-9.

7. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник / Поповский В.В., Персиков А.В. – Х.: ООО "Компания СМИТ", 2006. – 238 с.

8. Ленков С.В. Методы и средства защиты информации: в 2-х т. / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К. : Арий, 2008. – 464 с.

9. Домарев В.В. Безопасность информационных технологий. Системный подход / В.В. Домарев. – К. : ООО "ТИД "ДС", 2004. – 992 с.

10. Бабак В.П. Теоретичні основи захисту інформації: Підручник. – К. : Книжкове вид-во НАУ, 2008. – 752 с.

11. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников. – М. : Финансы и статистика, 2003. – 368 с.

12. ISO 15408. The Common Criteria for Information Technology Security Evaluation.

13. Згуровський М.З. Основи системного аналізу / Згуровський М.З., Панкратова Н.Д. – К. : Видавнича група BHV, 2007. – 544 с.

14. Дружинин В.В. Введение в теорию конфликта / В.В. Дружинин, Д.С. Конторов, М.Д. Дружинин – М. : Радио и связь, 1989. – 288 с.

15. Ігнатов В.О. Динаміка інформаційних конфліктів в інтелектуальних системах / В.О. Ігнатов, М.М. Гузій // Проблеми інформатизації та управління. – К. : НАУ, 2005. – Вип. 15. – С. 88-92.

16. Грищук Р.В. Кількісна оцінка рівня захищеності радіоелектронного об'єкта в складній динамічній системі під час інформаційного конфлікту / Р.В. Грищук // Управління розвитком. – Х., ХНЕУ, 2008. – № 6. – С. 57-59.

17. Грищук Р.В. Диференціально-ігрова модель кількісної оцінки захищеності технічних об'єктів / Р.В. Грищук // Захист інформації. – К. : ДУІКТ, 2008. – № 40 (спец. випуск). – С. 24-29.

18. Грищук Р.В. Кількісна оцінка рівня захищеності об'єктів електронно-обчислювальної техніки з урахуванням їх функціонування в умовах інформаційного конфлікту / Р.В. Грищук // Вісник ЖДТУ. – Житомир, ЖДТУ, 2008. – № 46 (ІІІ). – С. 113-120.

19. Грищук Р.В. Диференціально – тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу / Р.В. Грищук // Захист інформації. – К. : ДУІКТ, 2009. – № 1 (42). – С. 19-27.

20. Грищук Р.В. Спектральна модель процесу нападу на інформацію / Р.В. Грищук // Захист інформації. – К. : ДУІКТ, 2009. – № 2 (43). – С. 71-81.

21. Грищук Р.В. Диференціально-ігрова розгалужена спектральна модель процесу нападу на інформацію / Р.В. Грищук // Вісник ЖДТУ. – Житомир, ЖДТУ, 2009. – № 48 (І). – С. 152-159.

22. Грищук Р.В. Р-моделювання процесів нападу на інформацію при нестаціонарній природі потоків захисних дій та інформаційних атак / Р.В. Грищук // Системи обробки інформації. – Х.: ХУПС ім. І.Кожедуба, 2009. – № 7 (79). – С. 98-101.

23. Пухов Г.Е. Дифференциальные спектры и их модели. – К. : Наук. думка, 1990.– 184 с.

24. Р-моделювання складних динамічних систем / [Г.Л. Баранов, М.М. Браіловський, А.А. Засядько та ін.]; за ред. проф. Г.Л. Баранова та проф. В.О. Хорошко. – К. : ДУІКТ, 2008 – 132 с.

25. Пухов Г.Е. Дифференциальные преобразования функций и уравнений. – К. : Наук. думка, 1984. – 420 с.

26. Грищук Р.В. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію // Інформаційна безпека: Матеріали наук.-практ. конференції (Україна, Київ, 26-27 березня 2009 р.) / Ред. кол. В.Г. Кривуца, В.О. Хорошко, М.Т. Корійчук та ін. – К. : ДУІКТ, 2009. – С. 3-7.

27. Васильев В.В. Моделирование задач оптимизации и дифференциальных игр / В.В. Васильев, В.Л. Баранов. – К. : Наук. думка, 1989. – 286 с.

Надійшла до редколегії 19.05.2009

Рецензент: д-р техн. наук, проф. В.Л. Баранов, Державний університет інформаційно-комунікаційних технологій, Київ.

МЕТОДИКА ОЦЕНИВАНИЯ ГАРАНТИРОВАННОГО УРОВНЯ ЗАЩИЩЁННОСТИ ТЕХНИЧЕСКИХ ОБЪЕКТОВ

Р.В. Грищук, А.А. Хмара

В статье разработана методика оценивания гарантированного уровня защищённости технических объектов от методов несанкционированного доступа. Методика базируется на дифференциально-игровой постановке задачи оценивания и применения дифференциально-тейлоровских преобразований, которые в совокупности позволяют получить количественные оценки гарантированного уровня защищённости.

Ключевые слова: *гарантированный уровень защищенности, дифференциальная игра, дифференциально-тейлоровские преобразования, цена игры, седловая точка, стратегия.*

THE METHODOLOGY FOR ESTIMATING OF THE GUARANTEED PROTECTED LEVEL OF TECHNICAL OBJECTS

R.V. Gryschuk, A.A. Khmara

In article it is developed a technique for estimation of the guaranteed level of security of technical objects from methods of unapproved access. The technique is based on differential-game statement of a problem of estimation and application differential-tejlor transforms which in aggregate allow to receive quantitative estimations of the guaranteed level of security.

Keywords: *assured level of protected, differential game, differential-taylor transformations, cost of game, saddle point, strategy.*