УДК 004.9:517.978.2

Грищук Р. В. (ЖВІРЕ НАУ, Житомир)

КОНЦЕПЦІЯ ПОБУДОВИ ДИФЕРЕНЦІАЛЬНО-ІГРОВИХ ГАРАНТОВАНО ЗАХИЩЕНИХ РОЗПОДІЛЕНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Постановка проблеми в загальному вигляді та її зв'язок з важливими практичними завданнями. Питання захисту об'єктів критичної інфраструктури (ОКІ) державного та приватного секторів економіки, побудованих за архітектурою відкритих систем від розподілених атак знаходиться сьогодні в центрі уваги більшості провідних фахівців з інформаційної безпеки [1-6]. Основною причиною такої уваги є високий ступінь загрози, який несе розподілена атака – від фінансових збитків до загроз національній безпеці [1, 5, 6, 8]. Таким чином, проблема забезпечення гарантованої захищеності ОКІ від розподілених атак на сьогодні є актуальною [5, 9].

Аналіз останніх досліджень і публікацій. З аналізу публікацій [4, 6, 8-13] присвячених вирішенню зазначеної проблеми встановлено, що побудова гарантовано захищених відкритих систем відноситься до класу алгоритмічно нерозв'язних проблем. Але, як показано в [4, 11, 12] єдиним підходом до вирішення даної проблеми є декомпозиційний підхід, що передбачає розв'язання двох частинних задач захисту. Перша частинна задача зводиться до коректного формулювання політики безпеки, друга – до розробки системи захисту інформації (СЗІ), яка цю політику гарантовано підтримує.

На сьогодні відомо достатню кількість політик безпеки та підходів до розробки розподілених СЗІ, які ґрунтовно описано в працях [4, 6, 8-13] та іншій спеціалізованій літературі. В дослідженні автора [14] обґрунтовано новий перспективний напрям забезпечення гарантованої захищеності ОКІ, а саме – диференціально-ігровий підхід, що дозволяє синтезувати гарантовано захищені диференціально-ігрові СЗІ. Стосовно розподілених систем даний підхід потребує подальшого розвитку.

Метою статті є розробка концептуальних основ побудови диференціально-ігрових гарантовано захищених розподілених СЗІ.

Викладення основного змісту дослідження. З публікацій [4, 8-13, 15-18] присвячених захисту ОКІ від розподілених атак, наприклад *DDoS- атак* на відмову, атак типу розсилка спаму, комп'ютерних черв'яків тощо встановлено, що взаємодія суб'єктів нападу та об'єктів захисту має конфліктну природу, яка обумовлена антагонізмом їх інтересів [8, 17, 19]. Тому відповідно до термінології диференціальних ігор [20] в подальшому суб'єкти та об'єкти інформаційного конфлікту називатимуться гравцями.

Спираючись на ідею захисту від розподілених атак шляхом побудови розподілених систем захисту [6, 21], для розробки гарантовано захищених розподілених СЗІ застосуємо диференціально-ігровий підхід відповідно до [14]. В основу концепції покладемо декомпозиційний підхід, що не суперечить дослідженням інших авторів [4, 11, 12] і, в рамках визначеної проблеми, на першому етапі розв'яжемо задачу розробки диференціально-ігрової політики безпеки.

Диференціально-ігрова політика безпеки: формалізація задачі. Вихідні дані, припущення та обмеження. Відомо [21], що при реалізації розподіленої атаки декількома гравцями мережевий трафік не має самоподібної структури. З цього випливає, що моделі потоків пакетів заявок, як приклад фальшивих запитів на припинення TCP- з'єднання або звуження смуги пропускання каналу передачі даних, повідомлень електронної пошти з файлами повідомлень до яких інтегровано комп'ютерні черв'яки тощо не можливо описати моделями найпростіших потоків. Тому передбачається, що стратегії гравців, які задіяні в інформаційному конфлікті описуються нелінійними функціоналами загального вигляду

$$\lambda_i(t) = F_i(\lambda_i, T, t) \qquad (1)$$

– для гравців, що захищаються при обмеженнях

$$\lambda_{i\min}(t) \le \lambda_i(t) \le \lambda_{i\max}(t) \quad (2)$$

та для гравців, що атакують (реалізують процес нападу на інформацію [14])

$$\mu_j(t) = F_j(\mu_j, T, t) \quad (3)$$

при обмеженнях

$$\mu_{j\min}(t) \le \mu_j(t) \le \mu_{j\max}(t), \quad (4)$$

де λ_i та μ_j – параметри законів розподілу стратегій i-го та j-го гравців, які невідомі ($i = 0..X$, $j = 0..Y$, де X і Y – кількість гравців захисту та нападу відповідно); t – часовий аргумент, $t \in [t_0, T]$ (t_0 – початок атаки, T – тривалість інформаційного конфлікту); $\lambda_{i\min}(t)$ і $\mu_{j\min}(t)$ – мінімальні, а $\lambda_{i\max}(t)$ і $\mu_{j\max}(t)$ – максимальні інтенсивності потоків захисних дій та інформаційних атак i-го та j-го гравців. Стратегії гравців $\lambda_i(t)$ та $\mu_j(t)$, що визначають правила розподілу їх ресурсів, належать замкненим множинам $\Lambda \in E_\lambda$ та $M \in E_\mu$, які обмежені в евклідових просторах R_λ і R_μ.

Виходячи з прийнятих вище припущень та обмежень, та спираючись на дослідження [15, 16, 19, 21] на рис. 1 в загальному вигляді графічно подано моделі стратегій поведінки гравців в інформаційному конфлікті під час розподіленої атаки на ОКІ.

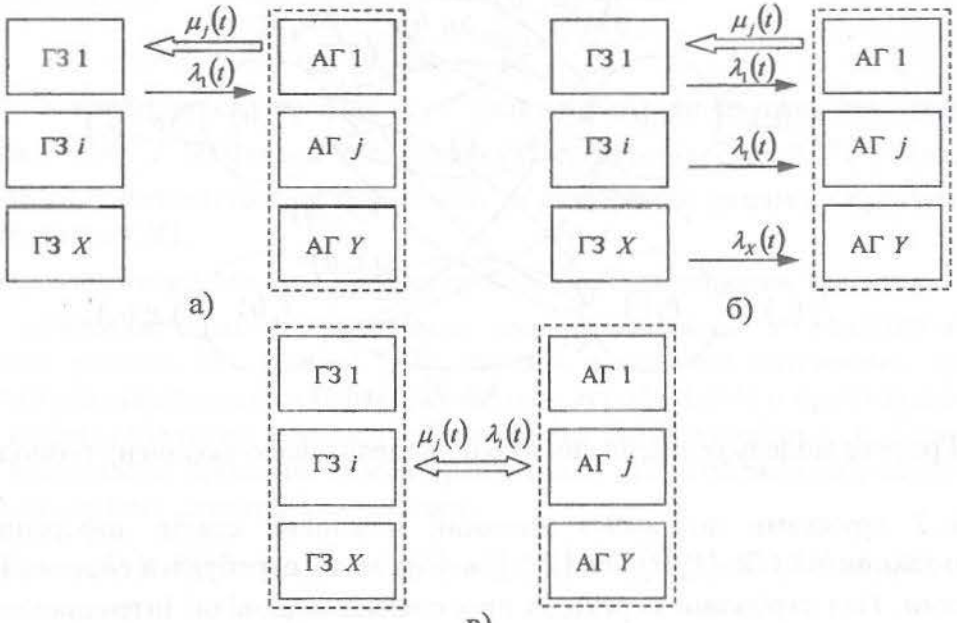

Рис 1. Стратегії гравців під час інформаційного конфлікту:
а) розподілена атака на ОКІ ГЗ 1; б) розподілена атака на ОКІ ГЗ 1 при індивідуальному захисті гравців; в) розподілена атака на розподілену СЗІ

На рис. 1 прийнято такі позначення: ГЗ 1 – перший об'єкт захисту (перший гравець, що захищає ОКІ); ГЗ i – i-й об'єкт захисту тощо; АГ 1 – перший гравець, що атакує, АГ j – j-й гравець, що атакує. Штрихпунктирні лінії навколо атакуючих гравців АГ j позначають гравців, стратегії яких спрямовано на реалізацію розподіленої атаки на ОКІ, а навколо об'єктів захисту – розподілену СЗІ. Тонкими стрілками позначено інтенсивності інформаційних ресурсів гравців захисту, товстими – розосередження інтенсивностей інформаційних ресурсів атакуючих гравців та гравців захисту.

Аналіз рис. 1 показує, що підходи до організації захисту інформації на ОКІ ГЗ 1 відображені на рис. 1 а та рис. 1 б є менш ефективними порівняно з третім варіантом

(рис. 1 в), що реалізує розподілену СЗІ. Дане твердження потребує додаткових досліджень, що в рамках даної статті не приводяться.

Згідно з теоремою захисту інформації захищеність системи визначається захищеністю її найменш захищеного об'єкта (ОКІ) [11]. Спираючись на дану теорему можливо сформулювати диференціально-ігрову політику безпеки. Диференціально-ігрова політика безпеки передбачає організацію процесу захисту інформації на ОКІ у вигляді розподіленої СЗІ (рис. 1 в), суть якої зводиться до зменшення потужності атаки на критичний об'єкт шляхом розосередження її інтенсивності між відповідними гравцями захисту та залученні інформаційних ресурсів цих гравців для забезпечення гарантованого рівня захищеності I^*.

Другий етап концепції побудови гарантовано захищених СЗІ полягає у вирішенні задачі розробки СЗІ, яка гарантовано підтримує диференціально-ігрову політику безпеки.

Розробка диференціально-ігрової гарантовано захищеної розподіленої СЗІ. Відповідно до рис. 1 в та виходячи з [14] в загальному вигляді подамо графову модель розподіленої атаки на гарантовано захищену розподілену СЗІ (рис. 2).

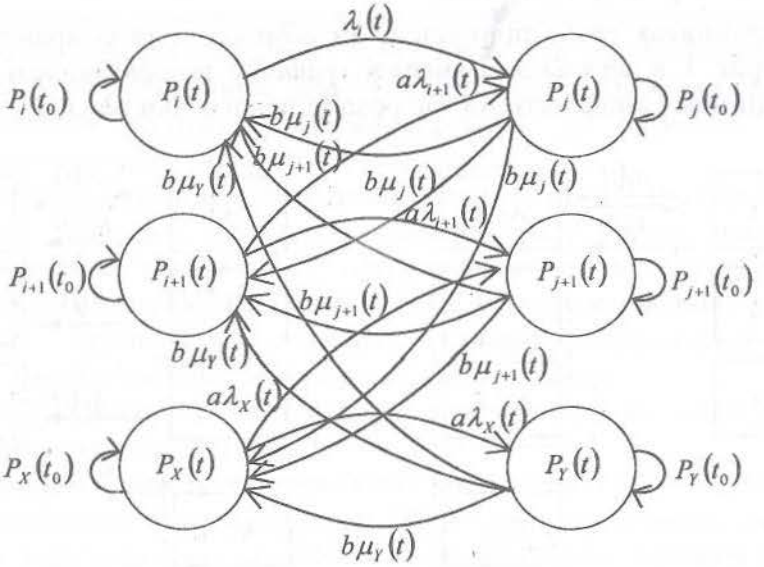

Рис 2. Графова модель розподіленої атаки на гарантовано захищену розподілену СЗІ

На рис. 2 кружками позначено множини можливих станів диференціально-ігрової гарантовано захищеної СЗІ $\{P_X(t)\}$ та $\{P_Y(t)\}$ в яких може перебувати система з відповідними ймовірностями. Над стрілками переходів проставлено відповідні інтенсивності потоків, які переводять систему у відповідні стани. Виходячи з диференціально-ігрової політики безпеки в розподіленій СЗІ вагові коефіцієнти a обирають виходячи з стратегії половинного захисту свого об'єкта та підтримки захисту ОКІ ГЗ 1 і визначають як $a = 1/2$. В основу вибору вагових коефіцієнтів b покладено стратегію розподілу інтенсивності атаки гравців, що атакують рівномірно між усіма гравцями, які захищаються. Вагові коефіцієнти b визначають як $b = 1/Y$.

За початкових умов $P_i(t_0) = 1$, $P_{i+1}(t_0) = \ldots = P_Y(t_0) = 0$ та умов нормування $P_i(t_0) + \ldots + P_X(t_0) + P_j(t_0) + \ldots + P_Y(t_0) = 1$ при відповідних обмеженнях (2) та (4) на ресурси гравців (1) та (3), інформаційний конфлікт в системі (див. рис. 2) описується системою нелінійних диференціальних рівнянь Колмогорова-Чепмена

$$\begin{cases} \dfrac{dP_i(t)}{dt} = -\lambda_i(t)P_i(t) + b\,\mu_j(t)P_j(t) + b\,\mu_{j+1}(t)P_{j+1}(t) + b\,\mu_Y(t)P_Y(t); \\ \dfrac{dP_{i+1}(t)}{dt} = -2a\,\lambda_{i+1}(t)P_{i+1}(t) + b\,\mu_j(t)P_j(t) + b\,\mu_{j+1}(t)P_{j+1}(t) + b\,\mu_Y(t)P_Y(t); \\ \vdots \\ \dfrac{dP_Y(t)}{dt} = -3b\,\mu_Y(t)P_Y(t) + a\,\lambda_X(t)P_X(t). \end{cases} \tag{5}$$

Рівень захищеності ОКІ ГЗ 1 I при реалізації розподіленої атаки, яка породжує інформаційний конфлікт (5) в СЗІ (див. рис. 2) є платою гравців, що захищаються за витрати власних захисних інформаційних ресурсів (1). Плата I на інтервалі $t \in [t_0, T]$ в загальному вигляді може бути подана інтегральною моделлю

$$I = \frac{1}{T}\int_{t_0}^{T} P_i(t)\,dt. \tag{6}$$

З метою забезпечення гарантованої захищеності шляхом дотримання диференціально-ігрової політики безпеки гравцями обираються стратегії відповідно до принципу мінімаксу [20]. При цьому політика безпеки виконується за умови існування в даній диференціальній грі сідлової точки, тобто

$$\min_{\lambda_i(t)\in E_\lambda} \max_{\mu_j(t)\in E_\mu} = \max_{\mu_j(t)\in E_\mu} \min_{\lambda_i(t)\in E_\lambda} = I^*. \tag{7}$$

Якщо умова (7) виконується, то плата I^* називається ціною гри, що гарантує рівень захищеності не гірше I^*. Шукана з системи (5) траєкторія гри $P_i^{opt}(t)$ при дотриманні політики безпеки (7) називається оптимальною та відображає динаміку протікання процесу розподіленої атаки на ОКІ.

Оцінювання гарантованого рівня захищеності I^* та визначення траєкторії гри $P_i^{opt}(t)$, пов'язано з обчислюваними труднощами, що випливають з нелінійності системи диференціальних рівнянь (5). Відомо [22], що для подолання визначених труднощів на сьогодні широко використовують операторні методи. В роботі [14] обґрунтовано доцільність застосування диференціальних перетворень академіка НАН України Г. Є. Пухова [22] для моделювання відповідних процесів. Тому з урахуванням [22] в області зображень систему (5) можна подати як систему спектральних рівнянь

$$\begin{cases} \dfrac{k+1}{H}P_i(k+1) = -\lambda_i(k) * P_i(k) + b\,\mu_j(k) * P_j(k) + b\,\mu_{j+1}(k) * P_{j+1}(k) + b\,\mu_Y(k) * P_Y(k); \\ \dfrac{k+1}{H}P_{i+1}(k+1) = -2a\,\lambda_{i+1}(k) * P_{i+1}(k) + b\,\mu_j(k) * P_j(k) + b\,\mu_{j+1}(k) * P_{j+1}(k) + b\,\mu_Y(k) * P_Y(k); \\ \vdots \\ \dfrac{k+1}{H}P_Y(k+1) = -3b\,\mu_Y(k) * P_Y(k) + a\,\lambda_X(k) * P_X(k), \end{cases} \tag{8}$$

де H – масштабна стала, яка має розмірність аргументу t і обирається рівною тривалості диференціальної гри, яка дорівнює тривалості інформаційного конфлікту T, $H = T$; $P_i(k), \ldots, P_Y(k)$ – диференціальні спектри для відповідних процесів, що протікають в СЗІ, k – цілочисловий аргумент, $k =: 0, 1, 2, \ldots$; $*$ – символ операції Т-множення.

В області зображень плата (6) виражається через дискрети диференціального спектра $P_i(k)$ моделі (8) як

$$I = \sum_{k=0}^{k=\infty} \frac{P_i(k)}{k+1}. \quad (9)$$

Для дотримання диференціально-ігрової політики безпеки (7) визначенню підлягають оптимальні стратегії гравців $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$. Шляхом дослідження функціоналу (9) на екстремум маємо

$$\begin{cases} \dfrac{\partial I(\lambda_i, \mu_j)}{\partial \lambda_i} = 0; \\ \dfrac{\partial I(\lambda_i, \mu_j)}{\partial \mu_j} = 0; \end{cases} \Rightarrow \begin{cases} \lambda_i^{opt}; \\ \mu_j^{opt}. \end{cases} \quad (10)$$

Перевірка достатніх умов дозволяє визначити знаки знайдених в (10) екстремумах, тобто

$$\begin{cases} \dfrac{\partial^2 I(\lambda_i, \mu_j)}{\partial \lambda_i^2} > 0; \\ \dfrac{\partial^2 I(\lambda_i, \mu_j)}{\partial \mu_j^2} < 0; \end{cases} \Rightarrow \begin{cases} \lambda_{i\min}^{opt}; \\ \mu_{j\max}^{opt}. \end{cases} \quad (11)$$

У результаті виконання умов (10) та (11) стратегії $\lambda_{i\min}^{opt}(t)$ і $\mu_{j\max}^{opt}(t)$ є оптимальними. Існування в грі сідлової точки, яку визначають відповідні оптимальні стратегії (11) дозволяє визначити рівень захищеності об'єкта критичної інфраструктури від розподіленої який гарантує синтезована диференціально-ігрова СЗІ (див. рис. 2)

$$I^* = \sum_{k=0}^{k=\infty} \frac{P_i^{opt}(k)}{k+1}. \quad (12)$$

Кількість дискрет $P_i^{opt}(k)$ в моделі (12) варіюється залежно від вимог, що висуваються до точності оцінювання гарантованого рівня захищеності. На практиці, як правило, доцільно обмежитися чотирма дискретами $P_i^{opt}(0),\ldots,P_i^{opt}(3)$.

Траєкторія (реалізація) процесу розподіленої атаки в часовій області [22] при виборі гравцями оптимальних стратегій $\lambda_{i\min}^{opt}(t)$ і $\mu_{j\max}^{opt}(t)$ визначається за моделлю

$$P_0^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{T}\right)^k P_0^{opt}(k). \quad (13)$$

Таким чином, розподілена СЗІ, яка розробляється і функціонує за диференціально-ігровою концепцією є гарантовано захищеною. Гарантований рівень захищеності I^* (7) досягається за рахунок дотримання гравцями оптимальних стратегій $\lambda_{i\min}^{opt}(t)$ і $\mu_{j\max}^{opt}(t)$.

Висновки та перспективи подальший досліджень. Вперше розроблено концепцію побудови диференціально-ігрових гарантовано захищених розподілених СЗІ, що відрізняється від відомих диференціально-ігровою формалізацією політики безпеки, дотримання якої дозволяє гарантовано захищати ОКІ від розподілених атак. Отримані теоретичні результати не суперечать дослідженням інших авторів, наприклад [6, 18, 21].

Подальші дослідження буде спрямовано на оцінювання ефективності моделей диференціально-ігрових гарантовано захищених розподілених СЗІ.

Список літератури

1. *Хорошко В. О.* Информационная безопасность Украины. Основные проблемы и перспективы / В. О. Хорошко // Захист інформації. – К. : ДУІКТ, 2008. – № 40 (спец. вип.). – С. 6–9.

2. *Голубенко А. Л.* Информационные технологии и киберпреступность / А. Л. Голубенко, В. А. Хорошко, А. С. Петров, Е. В. Белозеров // Вісник Східноукраїнського національного університету ім. В.Даля. – Луганськ : СНУ ім. В. Даля, 2006. – № 9 (103). – С. 7–10.

3. *Критическая* инфраструктура оказалась в киберопасности [Електронний ресурс]. – Режим доступу : http://news.rambler.ru/8181024/.

4. *Гайворонський М. В.* Безпека інформаційно-комунікаційних систем / М. В. Гайворонський, О. М. Новиков. За заг. ред. академіка НАН України М. З. Згуровського. – К. : Видавнича група BHV, 2009. – 608 с.

5. *Голубев В. А.* Киберпреступность – угрозы и прогнозы / В. А. Голубев // Управління розвитком. – Х. : ХНЕУ, 2008. – С. 103–106.

6. *Панасенко С. П.* Принципы разработки серверных модулей распределенных систем защиты информации, часть 1 / С. П. Панасенко // Вопросы защиты информации. – 2009. – № 2 – С. 30–34.

7. *Даник Ю. Г.* Національна безпека: запобігання критичним ситуаціям : монографія / Ю. Г. Даник, Ю. І. Катков, М. Ф. Пічугін. – Житомир : Рута, 2006. – 388 с.

8. *Mirkovic J.* Internet Denial of Service: Attack and Defense Mechanisms / J. Mirkovic, S. Dietrich, D. Dittrich, P. Reiher. – N.J. : Prentice Hall, 2005. – 400 p.

9. *Андон П. І.* Атаки на відмову в мережі Інтернет: опис проблеми та підходів до її вирішення / П. І. Андон, О. П. Ігнатенко. – К. : Ін-т ПС, 2008. – 52 с. – (Препринт / НАН України, Ін-т програмних систем).

10. *Ленков С. В.* Методы и средства защиты информации: в 2-х т / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко. – К. : Арий, 2008. – Том І. Несанкционированное получение информации. – 464 с.

11. *Грушо А. А.* Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. – М. : Яхтсмен, 1996. – 187 с.

12. *Мельников В. В.* Защита информации в компьютерных системах / В. В. Мельников. – М. : Финансы и статистика; Электоринформ, 1997. – 368 с.

13. *Бабак В. П.* Теоретичні основи захисту інформації: Підручник / В. П. Бабак. – К. : НАУ, 2008. – 752 с.

14. *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.

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. *Ігнатенко О. П.* Конфліктна задача взаємодії двох гравців у відкритому інформаційному середовищі / О. П. Ігнатенко // Проблеми програмування. – К. : НАН України, Ін-т програмних систем, 2009. – № 2. – С. 1–9.

17. *Милокум Я. В.* Метод конфликтного управления системой распределённой активной защиты от компьютерных угроз / Я. В. Милокум // Системний аналіз та інформаційні технології : XI міжнар. накук.-техн. конф. (Київ, 26-30 трав. 2009 р.). – К. : НАУ, 2009. – С. 525.

18. *Peng T.* Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems / T. Peng, C. Leckie, K. Ramamohanarao // ACM Computing Surveys. – 2007. – Vol. 39, N 1. – 42 p.

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

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

21. *Милокум Я. В.* Моделі та методи забезпечення якості обслуговування у захищених комп'ютерних мережах: автореф. дис. на здобуття наук. ступеня канд. тех. наук : спец. 05.13.05 "Комп'ютерні системи та компоненти" / Я. В. Милокум. – К., 2009. – 20 с.

22. *Пухов Г. Е.* Дифференциальные спектры и модели / Г. Е. Пухов – К. : Наук. думка, 1990. – 184 с.

В статті розроблено концепцію побудови систем захисту інформації об'єктів критичної інфраструктури від розподілених атак. Концепцією передбачено диференціально-ігрову політику безпеки, яка гарантовано підтримує заданий рівень захищеності об'єкта.

Ключові слова: захищені системи захисту інформації, розподілені атаки, рівень захищеності.

В статье разработано концепцию построения систем защиты информации объектов критической инфраструктуры от распределенных атак. Концепциею предусмотрено дифференциально-игровую политику безопасности, которая гарантированно поддерживает заданный уровень защищённости объекта.

Conception of the making of the information protection systems of the critical infrastructure objects from the distributed attacks is developed in the article. Conception provides differential-gaming security politics which supports guaranteed given level of the object privacy.

Рецензент:д.т.н., проф.Щербак Л.М.
Надійшла 28.10.2010