УДК 004.056 **Левченко Є.Г., Прус Р.Б., Швець В.А.**

РОЗПОДІЛ РЕСУРСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ДИНАМІЧНОМУ РЕЖИМІ

Розглянуто динамічний режим протистояння двох сторін в сфері інформаційної безпеки. Приведено приклади розрахунків системи з двох об'єктів з різними вразливостями і різним розподілом інформації на об'єктах. Розглянуто перехідний процес при досягненні сідлової точки та визначено інтервали її існування.

Ключові слова: цільова функція, теорія ігор, сідлова точка, динамічний розподіл ресурсів, метод Белман

Вступ. Протистояння двох сторін у сфері інформаційної безпеки відбувається в динамічному режимі [1,2]. Націленість атак з часом може змінюватись, супроводжуючись перерозподілом ресурсів нападу між об'єктами. Така ситуація виникає, зокрема, наприклад, при проведенні розвідки, коли напад не має відомостей про розподіл інформації на об'єктах і в результаті розвідки має можливість спрямувати свої зусилля у вигідному для себе напрямку. Перерозподіл ресурсів нападу викликає відповідну реакцію захисту, який також перерозподіляє свої ресурси. В цій ситуації виникає низка питань:

1) за яких умов існує сідлова точка для величини, яка визначається цільовою функцією і як на її положення впливають умови протистояння – відносна кількість ресурсів нападу (*X*) і захисту (*Y*), розподіл інформації між об'єктами g_k (*k* – номер об'єкта), вразливості f_k об'єктів;

2) яким повинен бути розподіл ресурсів захисту в умовах невизначеності, у випадку, коли сідлова точка відсутня;

3) яким чином в ситуації, коли націленість стає відомою, перерозподілити інформацію між об'єктами так, щоб загальні втрати стали мінімальними;

4) як відрізняються алгоритми управління при використанні різних критеріїв оптимальності – таких, як критерії Севіджа, Гурвіца, Лапласа, Бейєса;

5) як вплине на кінцеві рекомендації по розподілу ресурсів використання різних цільових функцій, котрі визначають такі величини, як кількість вилученої інформації, прибуток від внесеної інформації, їх рентабельність і яким буде результат при використанні багатоцільової функції;

6) яким буде алгоритм управління при комплексному протистоянні, коли кожна з сторін витрачає одну частину ресурсів на захист інформації, а іншу – на здобуття інформації суперника.

Мета досліджень – дати відповідь на деякі з поставлених питань, що дозволить наблизитись до розробки методики оптимального управління захисту інформації в умовах протистояння, які можуть відрізнятися кількістю об'єктів, їх вразливістю, розподілом інформації між об'єктами.

Постановка задачі і методика розрахунків. Використаємо цільову функцію, яка визначає частку вилученої інформації, у вигляді [3]:

$$i(x,y)=\sum_{k=1}^{l} g_k p_k q_k(x,y) f_k(x,y),$$

де k – номер об'єкта; x і y – ресурси нападу і, відповідно, захисту; g_k – відносна кількість інформації на об'єкті; p_k – імовірність нападу на об'єкт; $q_k(x,y)$ – щільність імовірності виділення нападом ресурсів x при заданому значенні y; $f_k(x,y)$ – імовірність вилучення інформації при даному співвідношенні x і y, яку розглядаємо як динамічну вразливість об'єкта.

Застосовуючи метод динамічного програмування [4], будемо розглядати ситуацію, коли напад і захист почергово роблять кроки, розподіляючи свої ресурси оптимальним чином, тобто так, щоб досягти на кожному кроці нападу $i_{\max}$ і на кожному кроці захисту $i_{\min}$. Розподіл ресурсів протилежної сторони на кожному кроці вважається відомим. Загальна кількість ресурсів як нападу $X=\sum_{k=1}^{l}x_k$, так і захисту $Y=\sum_{k=1}^{l}y_k$ залишається незмінною, при цьому $Y=0{,}05$, а X може змінюватись для різних систем, що призводить до зміни відносної величини $Z=\frac{X}{Y}$. В термінології теорії ігор це позиційна гра. У якості керуючої змінної обрано об'єм ресурсів нападу, що виділяється на перший об'єкт (x_k), залишаючи на другий об'єкт ($X-x_k$) ресурсів. Розрахунки виконано у Microsoft Excel із кроком 0,005.

Маючи на меті виявити вплив таких показників, як g_k, i, $f_k(x,y)$ на динамічний режим $i(n)$ (n - номер кроку), покладемо $p_k=1$ (напад відбувся) і $q_k(x,y)=1$ (залежність $q_k(x,y)$ слід враховувати при переході до стохастичної задачі). Розглядаючи систему з двох об'єктів, маємо спрощений вираз для цільової функції: $i(x,y)=g_1f_1(x,y)+g_2f_2(x,y)$.

Результати досліджень. Існування сідлової точки при заданому виді функцій вразливості $f_k(x,y)$ і співвідношення $\frac{g_1}{g_2}$ залежить від відносної кількості ресурсів Z. При використанні дробно-лінійних залежностей $f_k(x,y)$ сідлова точка існує при всіх значеннях Z. Якщо хоч одна із залежностей є дробно-нелінійною, то сідлова точка існує в певних інтервалах зміни Z, які для деяких функцій $f_k(x,y)$ приведені у табл. 1 та на рис. 1.

Знайдені інтервали Z носять складний характер, так як залежать від величин $f_k(x,y)$, x_k, y_k, g_k, що вирізняються широким діапазоном можливих значень.

Перейдемо до розгляду динамічного режиму в оремих ситуаціях. Почнемо з випадку, коли сідлова точка відсутня.

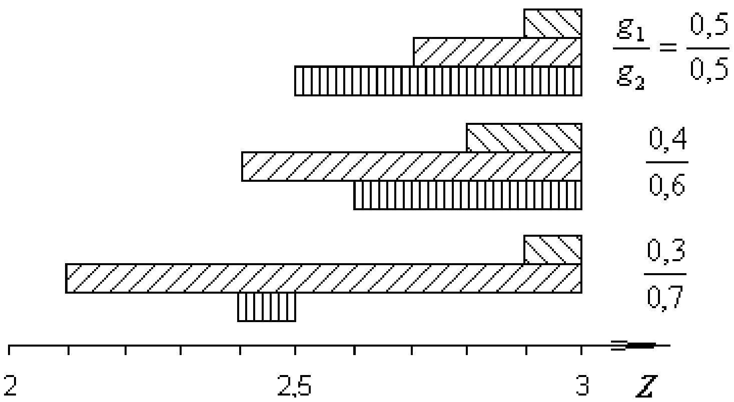


Рис. 1. Графічне зображення інтервалів існування сідлової точки:

- варіант 1, - варіант 2, - варіант 3

Інтервали існування сідлової точки Таблиця 1

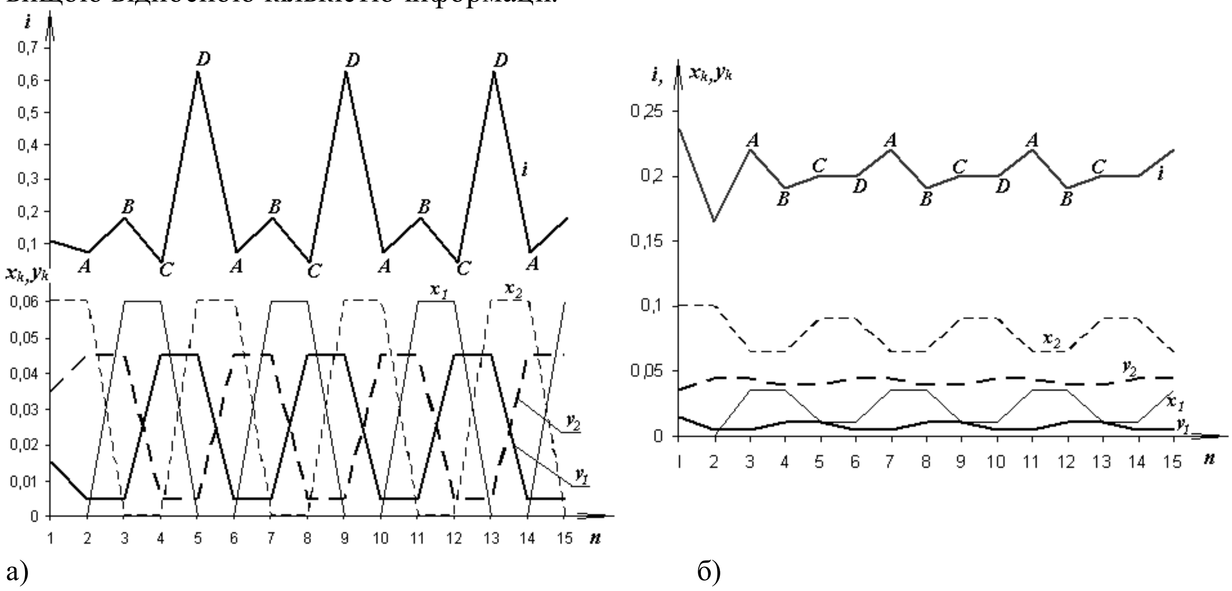
<table>
<tr><td rowspan="2">№ варіанта</td><td rowspan="2">Вразливості об'єктів</td><td colspan="3">Інтервали значення Z</td></tr>
<tr><td>$\frac{g_1}{g_2}=\frac{0,3}{0,7}$</td><td>$\frac{g_1}{g_2}=\frac{0,4}{0,6}$</td><td>$\frac{g_1}{g_2}=\frac{0,5}{0,5}$</td></tr>
</table>

1	$f_1 = \dfrac{x_1/y_1}{x_1/y_1 + 8},\ f_2 = \dfrac{\left(x_2/y_2\right)^2}{\left(x_2/y_2\right)^2 + 16}$	2,4 – 2,5	2,6 – 3	2,5 – 3
2	$f_1 = \dfrac{x_1/y_1}{x_1/y_1 + 8},\ f_2 = \dfrac{\left(x_2/y_2\right)^3}{\left(x_2/y_2\right)^3 + 32}$	2,1 – 3	2,4 – 3	2,7 – 3
3	$f_1 = \dfrac{\left(x_2/y_2\right)^2}{\left(x_2/y_2\right)^2 + 16},\ f_2 = \dfrac{\left(x_2/y_2\right)^3}{\left(x_2/y_2\right)^3 + 32}$	2,9 – 3	2,8 – 3	2,9 – 3

На рис. 2 а приведено динамічний режим $i(n)$ і відповідні розподіли x_k, y_k в системі, де $g_1 = 0{,}3$; $g_2 = 0{,}7$; $Z = 1{,}2$; функції $f_k(x, y)$ мають вигляд:

$$f_1 = \frac{x_1/y_1}{x_1/y_1 + 8},\ f_2 = \frac{\left(x_2/y_2\right)^2}{\left(x_2/y_2\right)^2 + 16}.$$

Перший крок відповідає рішенню нападу. Розподіл y_k вважаємо пропорційним співвідношенню g_k на об’єтах. Використовуючи алгоритм методу Белмана, знаходимо розподіл ресурсів нападу, що забезпечує максимальну кількість вилученої інформації. Це варіант, за якого усі ресурси $X = Z \cdot Y = 1{,}2 \cdot 0{,}05 = 0{,}06$ слід виділити на другий об’єкт з вищою відносною кількістю інформації.



а) б)

Рис. 2. Динамічний режим протистояння при відсутності сідлової точки

На другому кроці, котрий виконує захист, знаходимо розподіл y_k, при якому за усіх можливих варіантів дій нападу кількість вилученої інформації буде мінімальною (на рис. 2а це відповідає значенню $i = 0{,}06$ в точці A при $n = 2$). Такий розподіл передбачає, що мінімальну неподільну частку ресурсів $y_k = 0{,}005$ (у разі $y_k = 0$ усю інформацію з k-го об'єкту буде вилучено) необхідно виділити на перший об'єкт, на якому $x_1 = 0$, а решту ресурсів вкласти у другий об'єкт, де $x_2 = X = 0{,}06$. На наступному кроці нападу максимальна кількість вилученої інформації досягається в точці *B* при розподілі, за якого усі ресурси X виділено на перший, найменш захищений об'єкт. Враховуючи, що $g_1 = 0{,}3$, одержуємо $i_{\max} = 0{,}18$.

На четвертому кроці захисту алгоритм пропонує мінімальну частину ресурсів залишити на другому об'єкті, а решту виділити на перший, при цьому кількість вилученої інформації зменшиться до $i_{\min} = 0{,}04$ (точка *C* на рис. 2а). Однак, таке рішення являється ризикованим з огляду на те, що на наступному кроці напад переходить у точку *D* на рис. 2а та $i_{\max}$ досягає значення 0,63. Зростання $i_{\max}$ пояснюється тим, що напад знову усі ресурси направить на другий, більш важливий об'єкт, який до того ж являється найменш захищеним.

З рис. 2а можна зробити висновок, що захисту необхідно розподілити свої ресурси між об'єктами наступним чином: $y_1 = 0{,}005$; $y_2 = 0{,}045$. При цьому кількість вилученої інформації за будь-яких умов не перевищить значення $i_{\max} = 0{,}18$, що відповідає точці *B* на рис. 2а.

Із збільшенням Z у нападу з'являється можливість розподілити свої ресурси між двома об'єктами, а не зосереджувати їх на одному з них, як це було у попередньому випадку, і при цьому вилучити більше інформації. Це ілюструє рис. 2б, де показано динамічний розподіл ресурсів при $Z = 2$. Різниця між $i_{\min} = 0{,}19$ та $i_{\max} = 0{,}22$ зменшилась, як і величина співвідношення ресурсів нападу $\frac{x_1}{x_2}$ і захисту $\frac{y_1}{y_2}$ на об'єктах.

Рис.3 ілюструє динамічний режим при при $Z = 2{,}5$, коли сідлова точка вже існує.

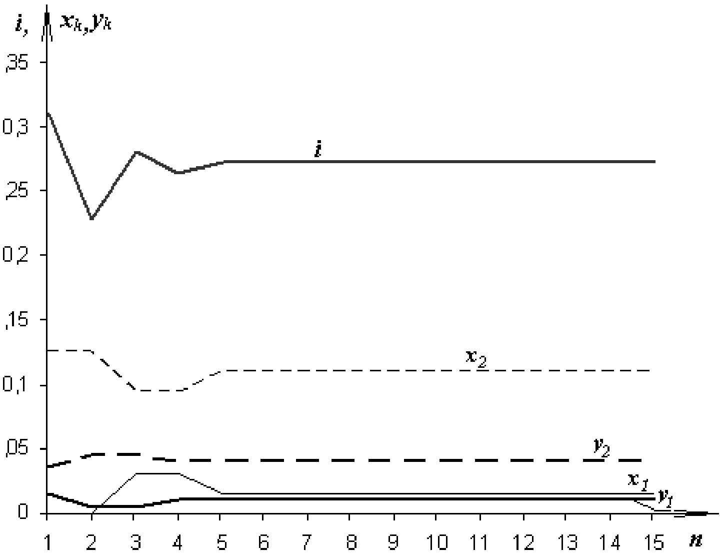


Рис. 3. Процес досягнення сідлової точки

Тривалість перехідного процесу $N_П$ залежить від того, наскільки вдалим обрано початковий розподіл, тобто наскільки близьким до $i_с$ є початкове значення *i*.

Сідлова точка реалізується при наступному розподілі ресурсів: $y_1^0 = 0{,}01$; $y_2^0 = 0{,}04$; $x_1^0 = 0{,}015$; $x_2^0 = 0{,}11$ При цьому кількість вилученої інформації становить $i^0 = 0{,}27$. Ця точка є оптимальною для обох сторін: відхилення від x_k^0 приводить до зменшення *i*, а відхилення від y_k^0 - до його збільшення.

Висновки. Головним завданням економічного менеджменту інформаційної безпеки є розробка оптимальної стратегії, тобто визначення при заданій кількості ресурсів захисту їх оптимального розподілу між об'єктами. Кращим варіантом є розподіл, який відповідає сідловій точці. Цей варіант гарантує одержання певних граничних показників, оскільки нападу також не вигідно відступати від сідлової точки. При відсутності сідлової точки загальної оптимальної стратегії не існує: оптимальний розподіл залежить від кількості і розподілу ресурсів нападу і розраховується при досягненні екстремального значення цільової функції в кожному окремому випадку. Для досягнення режиму сідлової точки при побудові інформаційної системи слід прагнути до того, щоб відмінності між об'єктами (як по кількості зосередженої інформації, так і по вразливості) були по можливості меншими. При заданих розподілах наявність сідлової точки визначається величиною Z. Таким чином, відомості про суперника, необхідні при побудові оптимальної системи захисту – це оцінка ресурсів X, які він може виділити на здобуття інформації.

ЛІТЕРАТУРА

1. Tatsumi K. Optimal timing of information security investment: A real options approach / K. Tatsumi, G. Makoto // WEIS 2009, University College of London. – July 21, 2009.

2. Bohme R. The Iterated weakest link: A model of adaptive security investment / R. Bohme, T. Moor // WEIS 2009, University College of London. – June 24, 2009.

3. Левченко Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки / Є.Г. Левченко, А.О. Рабчун // НТЖ Сучасний захист інформації. – 2010. – №1. – С. 16-23.

4. Беллман Р. Динамическое программирование. – М.: ИЛ, 1960. – 400 с.

Надійшла: 16.12.2011

Рецензент: д.т.н., проф. Корченко О.Г.