[5] Смирнов Н.В., Дунин-Барковський И.В. Краткий курс математической статистики для технических приложений. – М: Физматшз, 1959. – 436 с.

[6] Левченко Є.Г., Демчишин М.В., Рабчун А.О. Математичні моделі економічного менеджменту інформаційної безпеки // Системні дослідження та інформаційні технології. – 2011. – №4. – С. 88-96.

УДК 004.681 (045)

Демчишин М.В., Левченко Е.Г. Многокритериальная оптимизация в задачах информационной безопасности: четкий и нечеткий подходы

Аннотация. *Рассмотрено применение нечеткого и многокритериального четкого подходов к расчету рентабельности затрат в системе содержащей два объекта с различными уязвимостями. Сравнение результатов позволяет разработать рекомендации по формированию функций принадлежности.*

Ключевые слова: *информационная безопасность, нечеткий подход, функции принадлежности.*

Demchyshyn M.V., Levchenko.E.G. Multi-criteria optimization problems in information security: clear and fuzzy approaches

Abstract. *The application of fuzzy and multi-criteria approach to the calculation of return on costs in a system containing two objects with different vulnerabilities. Comparison of the results can provide guidance on the formation of membership functions.*

Keywords: *information security, fuzzy approach, the membership function.*

Отримано *14 березня 2012 року,* затверджено редколегією *08 червня 2012 року*
(рецензент д.т.н., професор О.Г. Корченко)

ОПТИМІЗАЦІЯ РОЗПОДІЛУ РЕСУРСІВ ЗАХИСТУ ІНФОРМАЦІЇ В ДИНАМІЧНОМУ РЕЖИМІ

Руслана Прус

Національний авіаційний університет

ПРУС Руслана Богданівна

Рік та місце народження: 1986 рік, с. Великі Селища, Рівненська область, Україна.
Освіта: Національний авіаційний університет, 2008 рік.
Посада: аспірант кафедра засобів захисту інформації.
Наукові інтереси: інформаційна безпека.
Публікації: 14 наукових публікацій, серед яких наукові статті та тези доповідей
E-mail: ruslana_prus@meta.ua

Анотація. *Розглянуто питання оптимального розподілу ресурсів захисту інформації із врахуванням дій нападу. Запропоновано модель динамічного управління ресурсами в сфері інформаційної безпеки, яка включає ключові показники системи захисту. Приведено приклади пошуку оптимального рішення в динамічному режимі. Розроблений метод дозволяє надати рекомендації щодо розподілу ресурсів між об'єктами захисту інформації незалежно від заданих умов.*

Ключові слова: *інформаційна безпека, теорія ігор, математична модель, цільова функція, сідлова точка, оптимальний розподіл ресурсів*

Вступ

Статистика показників протистояння в інформаційній сфері свідчить про те, що у зв'язку з постійним зростанням потоків інформації і їх важливості збільшується інтенсивність нападів, і їх можна розглядати як неперервний процес [1]. Це викликає необхідність прийняття адекватних заходів з боку захисту інформації. Проте націленість атак з часом може змінюватись, супроводжуючись перерозподілом ресурсів нападу між об'єктами. Подібна ситуація виникає, зокрема, при проведенні розвідки, коли напад не має відомостей про розподіл інформації по об'єктах і в результаті розвідки має можливість спрямувати свої зусилля у вигідному для себе напрямку [2]. Перерозподіл ресурсів нападу викликає відповідну реакцію захисту, який також перерозподіляє свої ресурси. Одним з контрзаходів захисту є адаптивне управління ресурсами, сутність якого полягає в тому, що розподіл ресурсів

проводиться з затримкою – після того, як визначиться націленість атак [3]. Таким чином, постає проблема розробки методів динамічного управління ресурсами захисту, котре забезпечує досягнення оптимальних показників в ситуаціях, які постійно змінюються. В термінології теорії ігор це є позиційна гра.

При цьому виникає низка питань:

1) за яких умов в цій грі існує сідлова точка для величини, яка визначається цільовою функцією і як на її положення впливають умови протистояння – відносна кількість $Z = X/Y$ ресурсів нападу (X) і захисту (Y), розподіл $\{g_k\}$ інформації між об'єктами (k - номер об'єкта), вразливості f_k об'єктів;

2) яким повинен бути розподіл $\{y_k\}$ ресурсів захисту в умовах невизначеності у випадку, коли сідлова точка відсутня;

3) яким чином в ситуації, коли націленість атак стає відомою, перерозподілити інформацію $\{g_k\}$ між об'єктами з різною вразливістю так, щоб загальні втрати стали мінімальними;

4) як відрізняються алгоритми управління при використанні різних критеріїв оптимальності і різних цільових функцій, котрі визначають такі величини, як кількість втраченої інформації, прибуток від внесення інвестицій, їх рентабельність і яким буде результат при використанні багатоцільової функції;

5) яким буде алгоритм управління при комплексному протистоянні, коли кожна із сторін втрачає одну частину ресурсів на захист своєї інформації, а іншу на здобуття інформації суперника.

Мета роботи – дослідження процесів динамічного протистояння і розробка рекомендацій по розподілу ресурсів між об'єктами захисту в динамічному режимі.

Постановка задачі і методика розрахунків

Розглянемо систему з декількох об'єктів, котрі відрізняються один від одного обсягами інформації, вразливістю і продуктивністю витрат.

Цільову функцію, котра визначає відносний сумарний обсяг втраченої інформації $i(x,y)$, задамо у вигляді [4]:

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

де x і y – змінні величини, які визначають ресурси нападу і, відповідно, захисту;

k – номер об'єкта;

g_k – обсяг інформації на об'єкті;

$p_k(x,y)$ – імовірність нападу на об'єкт;

$q_k(x,y)$ – щільність імовірності виділення нападом ресурсів нападу x на об'єкт при виділених ресурсах y ;

$f_k(x,y)$ – частка втраченої інформації.

Вважатимемо, що функціональні залежності, які входять в (1), визначаються співвідношенням x і y. Можливі форми залежностей $q(x,y)$ і $f(x,y)$ проаналізовано в [4]. Позначивши $x/y = \tilde{x}$, подамо $q_k(\tilde{x})$ у формі розподілу Максвела:

$$q_k(\tilde{x}) = N_k \tilde{x}_k^2\, e^{-h_k^2 \tilde{x}_k^2}, \quad (2)$$

де N_k - нормований коефіцієнт, а стала h_k визначає положення максимума функції: $x_{k\max} = \dfrac{1}{h_k}$

Залежність $f_k(\tilde{x})$ задамо у вигляді степеневої функції [4]:

$$f_k(\tilde{x}) = \frac{\tilde{x}_k^n}{\tilde{x}_k^n + c_k}$$

Перейшовши до змінної $\tilde{y} = \dfrac{y}{x}$, одержимо

$$f_k(\tilde{y}) = \frac{1}{1 + c_k \tilde{y}_k^n} \quad (3)$$

В позначенні функціональних залежностей величин q_k і f_k індекси при змінних x та y для спрощення запису не ставимо. При n=1 в (3) одержуємо дробно-лінійну функцію, при $n > 1$ – дробно-нелінійну. Величини n_k і c_k назвем продуктивностями витрат на захист інформації, а залежність $f_k(\tilde{y})$ - динамічною вразливістю об'єкта.

Умови динамічного протистояння визначимо наступним чином. Напад і захист роблять почергові "ходи", знаючи на даний момент розподіл ресурсів суперника і на цій основі перерозподіляючи свої ресурси. Захист припиняє гру, коли черговий хід є для нього невигідним або він несе загрозу наступного ходу суперника, котрий приведе до значних втрат.

Розглянемо випадок, коли в інтервалі зміни x_k, який вважаємо реальним, $q_k(\tilde{x}) = const = 1$ і $p_k = 1$ (напад відбувся). Тоді одержимо замість (1) спрощений вираз:

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

Варіанти розрахунків будуть відрізнятись розподілом $\{g_k\}$ інформації по об'єктах, значеннями n_k, c_k (продуктивності витрат), а також параметром $Z = X/Y$, де $X = \sum_{k=1}^{l} x_k$, $Y = \sum_{k=1}^{l} y_k$, який характеризує всю систему і визначає загальне співвідношення ресурсів нападу і захисту.

Результати розрахунків

На першому етапі розглянемо систему з двох об'єктів, для якої

$$i(\tilde{y}) = g_1 f_1(\tilde{y}) + g_2 f_2(\tilde{y})$$

Систему характеризують такі величини:

- співвідношення обсягів інформації по об'єктах g_1/g_2;

- динамічні вразливості об'єктів $f_1(x,y), f_2(x,y)$;

- співвідношення ресурсів нападу і захисту Z.

Основна мета динамічного управління – пошук сідлової точки, яка відповідає найбільш сприятливому для кожної сторони розподілу ресурсів і забезпечує таким чином стабільність ситуації. Існування сідлової точки залежить від приведених вище показників, зокрема від значення Z. Якщо вразливості описуються дробно-лінійними функціями, то сідлова точка існує при всіх значеннях Z, якщо хоча б одна з функцій є більш складною (дробно-квадратичною, дробно-кубічною), то існує в певних інтервалах значень Z. На рис. 1 показано процес динамічного управління при різних Z в системі, де одна з залежностей $f_k(x,y)$ описується дробно-лінійною функцією, а друга – дробно-кубічною.

При $Z=1$ (рис. 1,а) спостерігаємо близький до коливального процес, при якому відбувається повна почергова перекачка з одного об'єкта на інший як ресурсів нападу, так і ресурсів захисту. Цей процес обумовлений обмеженістю коштів нападу ($Z=1$), за якої при концентрації ресурсів на одному з об'єктів напад здобуває більше інформації, ніж при їх розподілі між об'єктами. Захист відслідковує дії нападу і направляє свої ресурси на той об'єкт, де зосереджені ресурси нападу. Зубчаста лінія $i(n)$ на рис. 1,а показує, що після кожного кроку нападу зростає кількість втраченої інформації, а після наступного кроку захисту вона зменшується. В точках M кількість втраченої інформації значно більша, ніж в точках N, оскільки точки M відображають ситуацію, коли ресурси нападу направлені на другий об'єкт, де зосереджена більша частка інформації, а точки N – протилежну ситуацію. При збільшенні Z (рис. 1,б) відбувається лише часткова перекачка ресурсів, оскільки їх вже достатньо для розподілу між обома об'єктами. Розрив між максимальним і мінімальним значеннями $i(n)$ зменшується.

З рис. 1 в видно, що при $Z=2$ повна перекачка з одного об'єкта на інший відбувається не на кожному кроці. А період зміни величин збільшується від чотирьої кроків до шести.

При $Z=2{,}5$ (рис. 1,г) досягається сідлова точка, в якій розподіли ресурсів стають оптимальними: $x_1^0=0{,}015$; $x_2^0=0{,}11$; $y_1^0=0{,}01$; $y_2^0=0{,}04$, а частка втраченої інформації становить $i=0{,}166$.

На рис. 1,в процесс перерозподілу ресурсів схожий на субгармонійні коливання в нелінійних системах [5]. У ході проведених досліджень встановлено, що форми наведених на рис. 1 залежностей із збільшенням Z стають складнішими, а коливання – в більшій степені нелінійними при збільшенні нелінійності в функціях $f_k(x,y)$. Так, якщо $f_1(x,y)$ описується дробно-лінійною функцією, а $f_2(x,y)$ – дробно-квадратичною, від динамічного режиму із повною перекачкою ресурсів із одного об'єкту на інший ми одразу переходимо до режиму сідлової точки, минаючи режими, зображені на рис.1,б-в.

Закономірності впливу на інтервал існування сідлової точки таких складових цільової функції (1), як $G=g_1/g_2$ та $f_k(x,y)$ можна сформулювати наступним чином.

1. Границі інтервалу по Z визначаються величинами вразливостей f_1, f_2. Чим менші вразливості в робочій області (це виражається в збільшенні показників n і c), тим нижче ліва границя, вище права і ширше інтервал ΔZ (рис. 2). Робочою областю вважаємо інтервал x/y, де $x>y$.

2. Для розширення інтервалу параметри g_1, g_2 повинні бути узгоджені із значеннями вразливостей f_1, f_2 – об'єкти з більшою вразливістю повинні містити менше інформації.

На рис. 3 приведено інтервали існування сідлової точки в системі з трьох об'єктів для трьох варіантів розподілу дробно-лінійних (рис. 3,а) та дробно-нелінійних (рис. 3,б) функцій $\{f_k(x,y)\}$ по об'єктах. Результати підсумуємо наступним чином.

1. При дробно-лінійних функціях $f_k(x,y)$ сідлова точка існує в певних інтервалах значень Z (рис. 3,а). Правої границі не існує, а чим більші вразливості, тим нижче знаходиться ліва границя.

2. При дробно-нелінійних вразливостях інтервали існування сідлової точки вужчі порівняно із системою з двох об'єктів. З переходом від дробно-лінійних до дробно-нелінійних функцій $f_k(x,y)$ звужується інтервал існування сідлової точки по Z. Із збільшенням c інтервали переміщуються в область більш високих значень Z (рис. 3,б).

Розглянемо детальніше процес досягнення сідлової точки в залежності від Z. Для цього побудуємо матрицю рішень, враховуючи різні варіанти розподілу ресурсів нападу і захисту. Відповідні розрахунки значень цільової функції (1) приведено у таблиці 1, де стовпчики відповідають варіантам розподілу ресурсів нападу, а рядки – ресурсів захисту.

Ліворуч приведені значення $\max\limits_{\{y_k\}} i$ для кожного рядка, тобто максимальне значення кількості втраченої інформації i для кожного варіанту розподілу ресурсів захисту. Ці значення зображені на рис. 4,а у вигляді кривої 1. Нижній рядок таблиці містить значення $\min\limits_{\{x_k\}} i$ для кожного стовпчика, тобто мінімально досяжне значення кількості втраченої інформації i для кожного варіанту розподілу ресурсів нападу. На рис. 4,а значення $\max\limits_{\{y_k\}} i$ для кожного варіанту розподілу ресурсів захисту відображає крива 2. На осі абсцис приведено номери варіантів розподілу ресурсів нападу для кривої 1 та захисту для кривої 2.

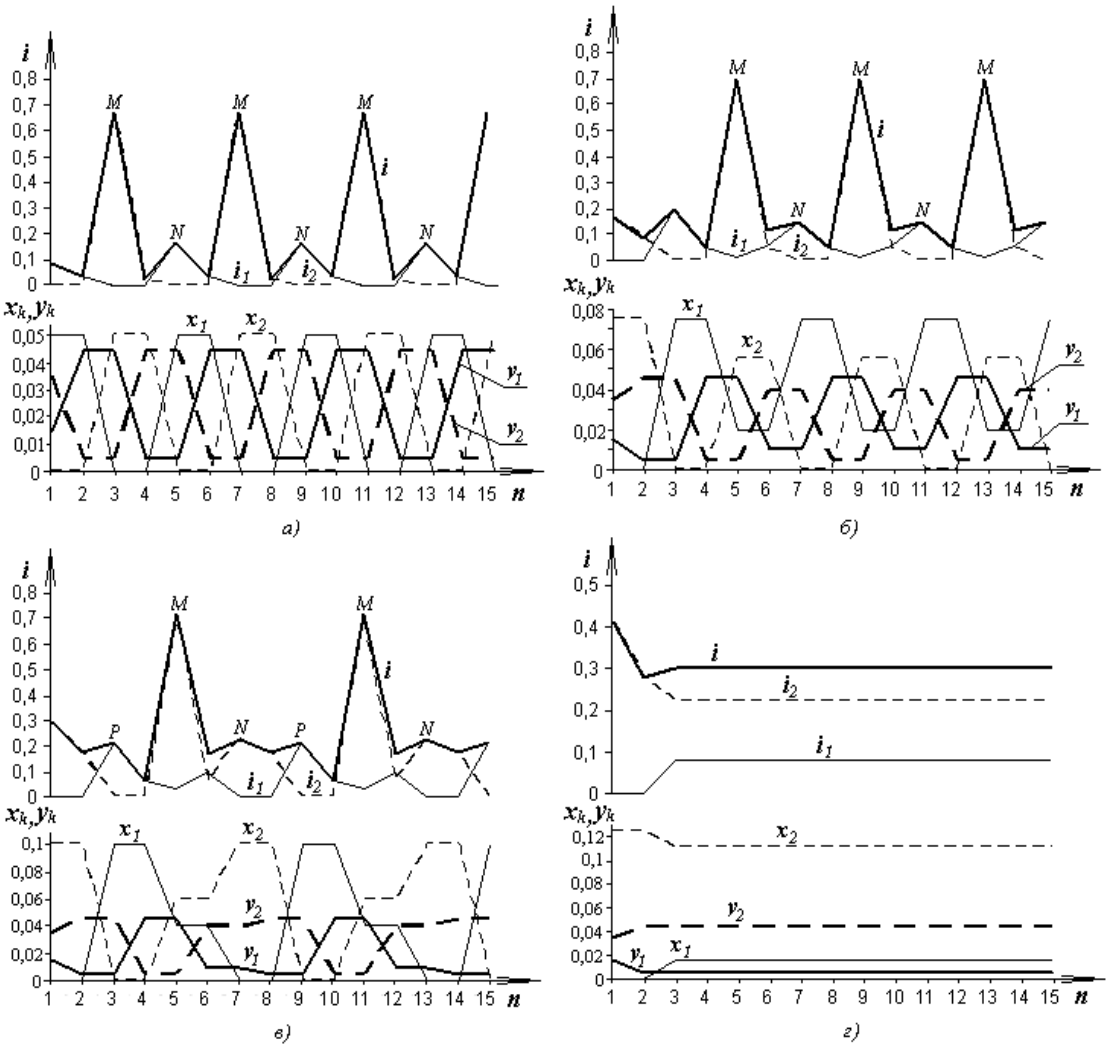


Рис. 1. Динамічний режим протистояння нападу і захисту при g_1=0,3; g_2=0,7; $f_1(x,y)=\frac{x/y}{x/y+8}$; $f_2(x,y)=\frac{(x/y)^3}{(x/y)^3+32}$ і різних Z: а) $Z=1$; б) $Z=1{,}5$; в) $Z=2$; г) $Z=2{,}5$

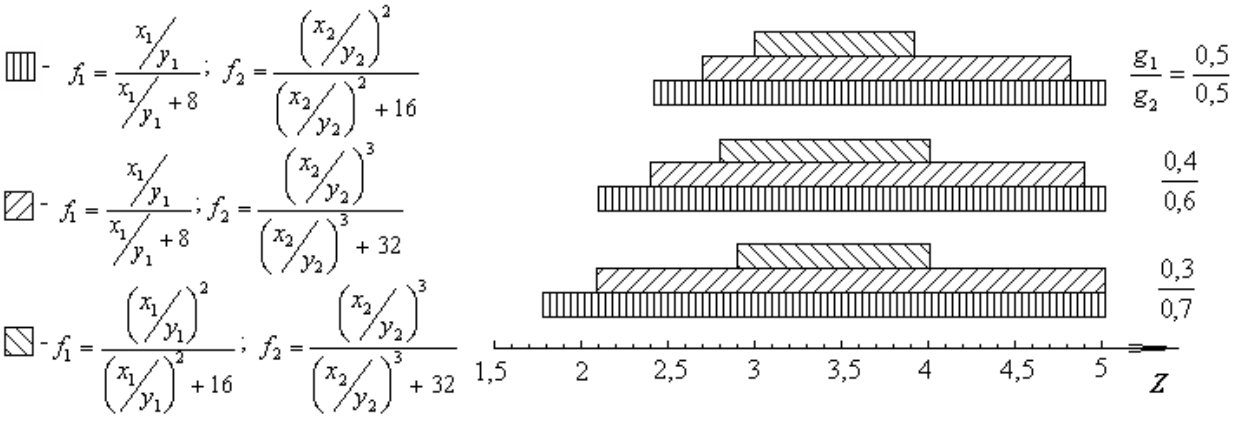
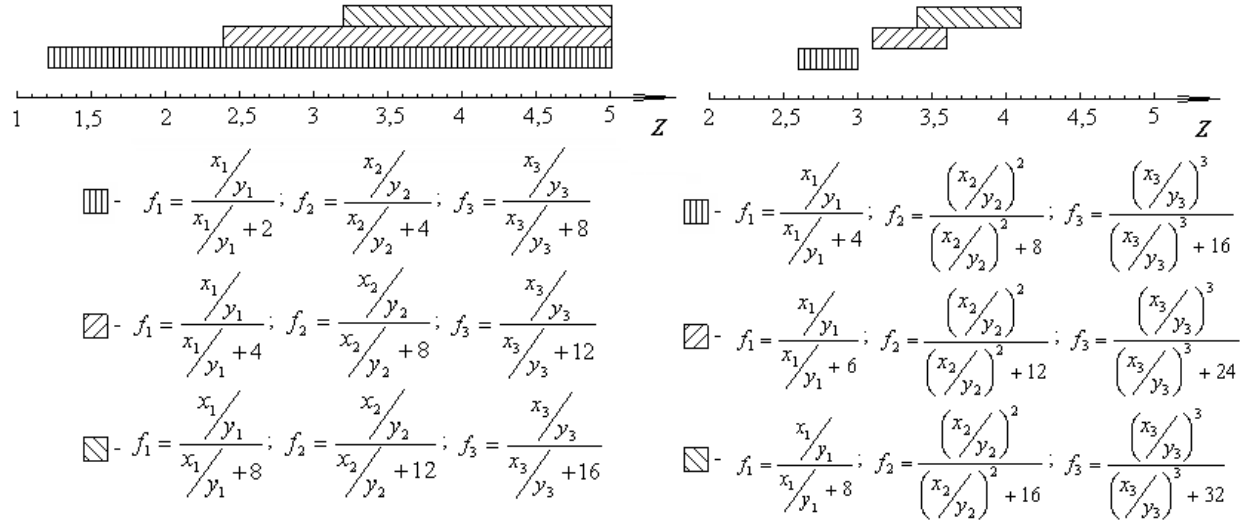


Рис. 2. Інтервали існування сідлової точки
в системі з двох об'єктів



а) б)

Рис. 3. Інтервали існування сідлової точки в системі з трьох об'єктів при $g_1=0{,}2$, $g_2=0{,}3$, $g_3=0{,}5$ і різних функціях вразливості

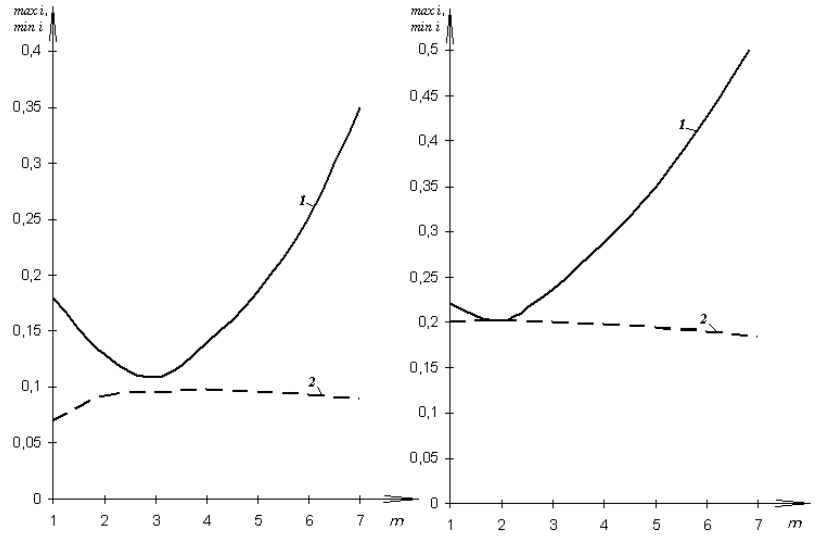
З таблиці видно, що при $Z=1{,}2$ $\min\max i \neq \max\min i$ (ці значення виділено жирним шрифтом), при цьому криві 1 і 2 на рис. 4,а не дотикаються. При збільшенні Z до $Z=2$ (рис.4,б) досягається сідлова точка, що відображається у правій частині таблиці та на рис.4,б.

Точка дотику і є сідловою точкою. У таблиці ця точка відповідає значенню $\min\max i = \max\min i = 0{,}2$. Відхилення від неї небажане для кожної з сторін, оскільки веде до порушення її показників.

Таблиця 1

Матриця рішень сторін при g_1=0,3; g_2=0,7; $f_1(x,y)=\frac{x/y}{x/y+8}$; $f_2(x,y)=\frac{(x/y)^2}{(x/y)^2+16}$ і різних Z

	m	$Z=1{,}2$								$Z=2$							
	$\{x_k\}$ / $\{y_k\}$	0; 0,06	0,035; 0,025	0,04; 0,02	0,045; 0,015	0,05; 0,01	0,055; 0,005	0,06; 0	*max i*	0,01; 0,09	0,017 0,083	0,03 0,07	0,04 0,06	0,05 0,05	0,06 0,04	0,07 0,03	*max i*
i	0,005; 0,045	0,180	0,140	0,132	0,122	0,110	0,093	0,070	0,180	0,200	0,212	0,221	0,220	0,217	0,213	0,210	0,221
	0,01; 0,04	0,129	0,103	0,101	0,099	0,096	0,092	0,086	0,129	0,199	0,200	0,196	0,190	0,182	0,176	0,171	**0,200**
	0,015; 0,035	0,100	0,093	0,096	0,099	0,102	0,106	0,109	**0,109**	0,228	0,219	0,200	0,184	0,167	0,153	0,141	0,228
	0,02; 0,03	0,082	0,095	0,103	0,112	0,121	0,131	0,140	0,140	0,270	0,255	0,225	0,200	0,175	0,152	0,132	0,270
	0,025; 0,025	0,069	0,110	0,124	0,139	0,154	0,170	0,185	0,185	0,328	0,309	0,269	0,235	0,200	0,166	0,136	0,382
	0,03; 0,02	0,060	0,141	0,163	0,186	0,209	0,231	0,252	0,252	0,403	0,383	0,337	0,295	0,248	0,200	0,154	0,403
	0,035; 0,015	0,053	0,202	0,235	0,267	0,297	0,325	0,350	0,350	0,495	0,477	0,433	0,388	0,332	0,268	0,200	0,495
	min i	0,053	0,093	0,096	**0,099**	0,096	0,092	0,070		0,199	**0,200**	0,196	0,184	0,167	0,152	0,132	



а) $Z = 1{,}2$ *б)* $Z = 2$

Рис. 4. Досягнення сідлової точки при g_1=0,3; g_2=0,7; $f_1(x,y) = \frac{x/y}{x/y + 8}$; $f_2(x,y) = \frac{\left(x/y\right)^2}{\left(x/y\right)^2 + 16}$; 1 - $\max\limits_{\{y_k\}} i$, 2 - $\min\limits_{\{x_k\}} i$

Коливальний характер процесів перерозподілу ресурсів наводить на думку побудувати фізичну модель інформаційної системи.

Для процесів (рис. 1) механічною моделлю може бути пара пружно зв'язаних подвійних маятників (рис. 5). Жорсткий зв'язок між окремими кульками кожного з подвійних маятників виражає незмінність ресурсів як нападу, так і захисту: $x_1 + x_2 = X$, $y_1 + y_2 = Y$. Пружний зв'язок між подвійними маятниками забезпечує узгодженість їх коливань. При належних початкових умовах, тобто умовах збудження протифазних коливань в консервативній системі коливання будуть тривати необмежено довго.

При $Z \neq 1$ симетрія картини порушується, оскільки $x_{\max} \neq y_{\max}$. На моделі це проявляється в тому, що маси кульок m_1 і m_2 перестають бути однаковими. При малих відхиленнях можна вважати, що $\frac{m_x}{m_y} = \frac{y_{\max}}{x_{\max}}$.

При подальшому зростанні нелінійності (за рахунок показника n в функції $f(\tilde{y})$ та значення Z процеси перерозподілу ресурсів залишаються періодичними, але вже не можуть моделюватись вільними коливаннями.

Процеси на рис. 1 б можна розглядати як гармонічні коливання коло точки, яка не є точкою рівноваги, а процеси на рис. 1,в – як субгармонічні коливання періоду $1/2$.

Періодичну зміну величини $i(n)$ можна трактувати як вимушені коливання в дисипативному середовищі з субгармонійною зовнішньою силою.

Строго кажучи, процеси, зображені на рис. 1,а кусочно-лінійними відрізками, не є гармонічними, проте гармонічна модель в достатній степені відображає основні закономірності процесів.

Більш того, в реальних умовах процес переходу з одного стану $\{x_k\}$ (чи $\{y_k\}$) в інший можна вважати миттєвим, і ці коливання наближаються до релаксаційних. Моделлю таких систем є релаксаційні генератори.

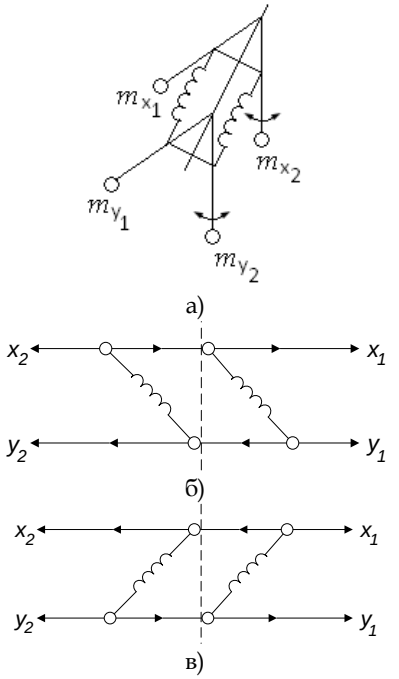


Рис. 5. Механічна модель системи, в котрій відбувається перерозподіл ресурсів

Відношення Z ресурсів нападу до ресурсів захисту відображають на еквівалентній схемі величиною зв'язку між коливальними системами (на механічній моделі – жорсткістю пружин, на електричній – величиною ємності зв'язку). Величина зв'язку впливає на швидкість перекачки ресурсів і їх величину. При малих Z зв'язок повинен бути більшим, ніж при великих. При $Z = 1$ ресурси на кожному кроці повністю переводяться на інший об'єкт, що дозволяє

потрапити на ділянку залежності $f(x,y)$ з високою крутизною для цього об'єкта і забезпечити максимальну кількість вилученої інформації. На наступному кроці захист переводить на цей об'єкт всі свої ресурси. В результаті робоча точка переміщується на положисту ділянку залежності $f(x,y)$, де $x/y \geq 0$, значення $i(x,y)$ зменшується, що примушує напад переводити свої ресурси на інший, незахищений об'єкт.

Висновки. Запропонована модель пошуку оптимального рішення дозволяє надати рекомендації щодо оптимального розподілу ресурсів захисту інформації із врахуванням дій нападу. Проведені розрахунки показали вплив відносної кількості ресурсів нападу, вразливостей об'єктів та кількості інформації на об'єктах на інтервали існування сідлової точки по Z, що є важливим фактором для побудови оптимальної системи захисту інформації.

Література

[1] Liu W. Empirical-Analysis Methodology for Information-Security Investment and Application to Reliable Survey of Japanese Firms / Tanaka H., Matsuura K. // IPSJ Journal, September 2007. – Vol. 48, № 9. – P. 3204-3218.

[2] Демчишин М.В. Ефективність розвідки при протистоянні двох сторін в інформаційній сфері / Левченко Є.Г. // Сучасний захист інформації. – 2011. – №2. – С. 5-15.

[3] Bohme R. The Iterated Weakest Link: A Model of Adaptive Security Investment / Moor T. – WEIS. – London. – 24 June. – 2009.

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

[5] Хаяси Т. Нелинейные колебания в электрических системах. – М.: Мир. – 1968. – 293 с.

УДК 004.056.5 (045)

Прус Р.Б. Оптимизация распределения ресурсов защиты информации в динамическом режиме

Аннотация. *Рассмотрен вопрос оптимального распределения ресурсов защиты информации с учетом действий нападения. Предложена модель динамического управления ресурсами в сфере информационной безопасности, которая содержит ключевые показатели системы защиты. Приведены примеры поиска оптимального решения в динамическом режиме. Разработанный метод позволяет дать рекомендации для распределения ресурсов между объектами защиты информации независимо от заданных условий.*

Ключевые слова: *информационная безопасность, теория игр, математическая модель, целевая функция, седловая точка, оптимальное распределение ресурсов.*

Prus R.B. Optimization of information security resource allocation in dynamic mode

Abstract. *Problem of optimal information security resource allocation with taking into account attack actions is examined. Dynamic resource allocation model which includes key indices of information security system is proposed. Examples of optimal solution search in dynamic mode are represented. Devised method enables to recommend appropriate resource allocation between information security objects with any desired conditions.*

Keywords: *information security, game theory, mathematical model, objective function, saddle point, optimal resource allocation.*

Отримано *29 березня 2012 року,* затверджено редколегією *06 червня 2012 року*
(рецензент д.т.н., професор В.П. Кваснiков)

ОПТИМІЗАЦІЯ СУМАРНИХ ВТРАТ В СФЕРІ ЗАХИСТУ ІНФОРМАЦІЇ

Андрій Рабчун

Державний університет інформаційно-комунікаційних технологій

РАБЧУН Андрій Олександрович

Рік і місце народження: 1988 року народження, м. Краснодар.
Освіта: повна вища за спеціальністю «Системи захисту від несанкціонованого доступу».
Посада: аспірант.
Наукові інтереси: інформаційна безпека.
Публікації: 14 публікацій.
E-mail: retouchp@gmail.com