[7] Information technology. Security techniques. Information security management systems. Overview and vocabulary [Текст]: international standard ISO/IEC 27000:2009(E). – Geneva: ISO/IEC, 2009. – 26 p.

[8] Information Security Management Systems (ISMS) [Текст]: BSI Standard 100-1, Version 2.0. – Bonn: BSI, 2008. – 38 p.

[9] IT-Grundschutz Methodology [Текст]: BSI Standard 100-2, Version 2.0. – Bonn: BSI, 2008. – 93 p.

УДК 004.056:336 (045)

Домарев Д.В., Домарев В.В. методика управления информационной безопасностью в банковских учреждениях с помощью СУИБ «Матрица»

Аннотация. *Обоснована актуальность вопросов управления информационной безопасностью. Теоретической основой предлагаемой методики является системный подход к информационной безопасности. Для практической реализации предлагаемой методики применена система управления информационной безопасностью «Матрица». Приведены процедуры формирования нормативной базы об информации с ограниченным доступом, описания критических бизнес-процессов и программно-технических комплексов, обеспечивающих их функционирование, описания организационной структуры банка, которую охватывает СУИБ, назначения ответственных за внедрение СУИБ, оценивания рисков информационной безопасности банковского учреждения, создания плана возобновления в случае чрезвычайных обстоятельств. Сделаны выводы о применимости предлагаемой методики в управлении информационной безопасностью банковских учреждений.*

Ключевые слова: *управление информационной безопасностью, СУИБ «Матрица», системный подход к ИБ, система управления информационной безопасностью, формирование нормативных документов, ОСТУ СУИБ, ISO 27000, оценка рисков ИБ.*

Domarev D.V., Domarev V.V. Method of information security management in banking institutions using ISMS "Matrix"

Abstract: *Actuality of information security management is proved. Theoretical basis of the proposed method is the system approach to information security. For the practical realization of the offered method, the information security management system "Matrix" is applied. The following procedures are described: forming of normative base about classified information, description of critical business-processes and hardware/software infrastructures supporting them, description of the bank's organizational structure covered by an ISMS, assignment of staff responsible for the implementation of the ISMS, estimation of information security risks of a banking institution, creation of the emergency recovery plan. Conclusion is made about the applicability of ther proposed method to the information security management in banking institutions.*

Key words: *information security management, ISMS "Matrix", system approach to information security, information security management system, production of normative documents, ISMS branch standard of Ukraine, ISO 27000, information security risk estimation.*

Отримано *12 лютого 2013 року*, затверджено редколегією *14 березня 2013 року*

УМОВИ ІСНУВАННЯ СІДЛОВОЇ ТОЧКИ В БАГАТОРУБІЖНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Євген Левченко[1], Руслана Прус[1], Дмитро Рабчун[2]

[1] Національний авіаційний університет, Україна
[2] Державний університет інформаційно-комунікаційних технологій, Україна

ЛЕВЧЕНКО Євген Григорович, к.ф.-м.н., доцент

Рік та місце народження: 1937 рік, Черкаська область, Україна.
Освіта: Київський державний університет ім. Т.Г. Шевченка, 1959 рік.
Посада: доцент кафедри засобів захисту інформації з 2002 року.
Наукові інтереси: інформаційна безпека.
Публікації: 100 наукових публікацій, серед яких монографія, навчальні посібники, наукові статті та патенти на винаходи.

ПРУС Руслана Богданівна

Рік та місце народження: 1986 рік, Рівненська область, Україна.
Освіта: Національний авіаційний університет, 2008 рік.
Посада: аспірант.
Наукові інтереси: інформаційна безпека.
Публікації: 16 наукових публікацій, серед яких наукові статті та тези доповідей
E-mail: ruslana_prus@meta.ua

РАБЧУН Дмитро Ігорович

Рік та місце народження: 1992 рік, Хмельницька область, Україна.
Освіта: Державний університет інформаційно-комунікаційних технологій.
Посада: студент.
Наукові інтереси: інформаційна безпека.
Публікації: 3 наукові статті та тези доповіді.
E-mail: rabchundima92@gmail.com

Анотація. *При проектуванні комплексних систем захисту інформації важливим питанням є визначення оптимальної кількості ресурсів, котрі слід виділяти на захист, та їх розподіл між об'єктами, які відрізняються кількістю інформації, вразливістю, імовірністю нападу. Пошук рішення ускладнюється через невизначеність дій суперника. В цих умовах задовільним можна вважати рішення, що відповідає сідловій точці цільової функції, яка може виражати один з показників системи захисту – частку втраченої інформації, прибуток від інвестицій в захист, їх рентабельність – в залежності від співвідношення ресурсів нападу і захисту X і, відповідно, Y. Проведені розрахунки дозволяють проаналізувати умови існування сідлової точки в одно- і дворівневих системах, котрі відрізняються кількістю об'єктів і перешкод, які їх захищають. Показано, що сідлова точка існує в певних інтервалах значень $Z = \frac{X}{Y}$, котрі визначаються формою динамічної вразливості об'єктів і розподілом інформації по об'єктах.*

Ключові слова: *інформаційна безпека, математична модель, цільова функція, динамічна вразливість, сідлова точка.*

Вступ

Інформаційне протистояння відбувається частіше всього в умовах невизначеності, коли можливості, наміри, а іноді і дії суперника невідомі. В цій ситуації здається доцільним шукати таку стратегію поведінки, котра забезпечує певний результат при будь-яких діях суперника. Така ситуація спостерігається в сідловій точці цільової функції, де кожна з сторін досягає найкращого для себе результату і не зацікавлена в тому, щоб змінювати свою стратегію [1-3]. Стратегія кожної з сторін полягає в певному розподілі своїх ресурсів між об'єктами, які відрізняються кількістю інформації, вразливістю та імовірністю нападу. Зростання вартості інформації, а також збитків від її можливого витоку приводить до ускладнення і подорожчання систем захисту. В цих умовах питання про визначення оптимальної кількості ресурсів захисту і оптимізації їх розподілу між об'єктами стає дедалі більш актуальним.

Мета – визначити умови існування сідлової точки в складних багаторубіжних системах (котрі відрізняються структурою, розподілом інформації між об'єктами, їх вразливістю та співвідношенням між кількістю ресурсів нападу і захисту).

Методика розрахунків

Цільова функція, котра визначає частку втраченої інформації, має вигляд [4]:

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

де x і y - ресурси нападу і, відповідно, захисту, $\sum_{k=1}^{l} x_k = X$, $\sum_{k=1}^{l} y_k = Y$;

$k = \overline{1,l}$ - номер об'єкта;

g_k - частка інформації на k-му об'єкті;

p_k - імовірність нападу на об'єкт;

$q_k(x,y)$ - щільність імовірності виділення ресурсів y на захист;

$f_k(x,y)$ - частка втраченої інформації на об'єкті.

Величини, котрі входять в (1) – відносні. Величини $i(x,y)$, $i_k(x,y)$ та g_k віднесені до загальної вартості інформації, $f_k(x,y)$ - до вартості інформації на об'єкті. Останню величину можна розглядати як імовірність втрати інформації при нападі на об'єкт, або як його динамічну вразливість. При $y = 0$ маємо

$f(x,0)$ - статичну вразливість, котра визначається початковою або природною захищеністю об'єкта.

Маючи на меті виявлення впливу характеристик системи, покладемо $p_k = 1$, $q_k(x,y) = const = 1$. Тоді (1) переходить в більш простий вираз:

$$i(x,y) = \sum_{k=1}^{l} g_k f_k(x,y). \qquad (2)$$

Вирази (1), (2) придатні для застосування до однорівневих систем. Найпростіша з таких систем зображена на рис.1,а, де два об'єкти g_1 і g_2 захищені індивідуальними перешкодами 1 і 2. Однорівнева система (рис.1,б) містить три об'єкти з трьома індивідуальними перешкодами.

Ресурси y_k, котрі виділяються на захист об'єктів, витрачаються фактично на облаштування перешкод і визначають їх вразливості $f_k(x,y)$, які характеризують одночасно вразливості об'єктів. Цільова функція для системи (рис. 1,а) має вигляд:

$$i(x,y) = g_1 f_1(x_1,y_1) + g_2 f_2(x_2,y_2), \qquad (3)$$

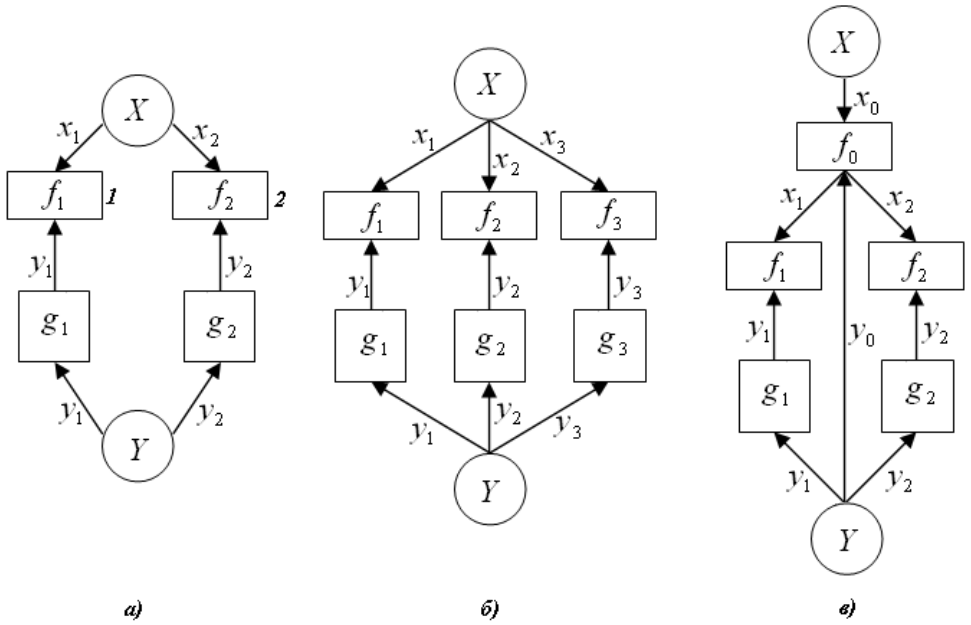

Рис. 1. Схеми однорівневих (а, б) та дворівневої (в) систем захисту

На рис.1,в показана дворівнева система, котра містить спільну для обох об'єктів перешкоду f_0 і дві індивідуальні перешкоди – f_1 і f_2. Для цієї системи цільова функція описується виразом:

$$i(x,y) = f_0(x_0,y_0) \cdot \left[g_1 f_1(x_1,y_1) + g_2 f_2(x_2,y_2) \right]. \qquad (4)$$

Тут і надалі через k позначається номер перешкоди, а $f_k(x_k,y_k)$ виражає вразливість перешкоди, тобто безумовну імовірність її подолання. Форма і значення цільової функції (4) в значній мірі визначаються залежностями $f_k(x_k,y_k)$. При формуванні цих залежностей слід врахувати такі міркування. По-перше, вважаємо, що змінні x, y входять у вирази $f_k(x,y)$ у вигляді відношення x/y. По-друге, з фізичних причин ці залежності повинні задовольняти умовам: при $x/y \to 0$ $f_k(x,y) \to 0$, при $x/y \to \infty$ $f_k(x,y) \to 1$. Найпростіші функції, котрі задовольняють цим вимогам – дробно-степеневі функції виду:

$$f(x,y) = \frac{\left(x/y\right)^n}{\left(x/y\right)^n + c} = \frac{1}{1 + c\left(y/x\right)^n}, \qquad (5)$$

де параметри n і c визначають форму і кривизну ліній.

Схеми (рис.1) можуть представляти як фізичні, так і електронні системи. Прикладом фізичної системи (рис.1,в) може бути система, в котрій спільна перешкода f_0 являє собою захищений периметр території, об'єкти g_1, g_2 - приміщення, а перешкоди f_1, f_2 - засоби, які захищають ці приміщення (замки на дверях, грати на вікнах, генератори шуму, камери відеоспостереження тощо).

Електронна система (рис.1,в) представляє, приміром, комп'ютери g_1, g_2, захищені спільною (firewall) та індивідуальними перешкодами (антивірусне програмне забезпечення, шифрування даних, антиспамфільтри).

Більш складні системи, котрі містять декілька спільних та індивідуальних перешкод, можуть, зрештою, бути зведені до системи (рис.1,в)

Розглядаючи системи рис.1, порівнюємо однорівневі системи (рис.1,а,б) з дворівневою системою (рис.1,в). Об'єкти відрізняються вразливістю і кількістю інформації – вони задаються в розрахунок. Незалежною змінною є $Z = \frac{X}{Y}$ –

відносна кількість ресурсів нападу і захисту. Показники, по яким ведеться порівняння систем:

− область існування сідлової точки;

− частка втраченої інформації в цій області.

Зазначені показники в значній мірі залежать від вразливостей об'єктів. Ці залежності в формі (5) зображені на рис.2 для різних значень n і c.

Параметр n впливає, в основному, на нелінійність кривих, параметр c - на їх положення.

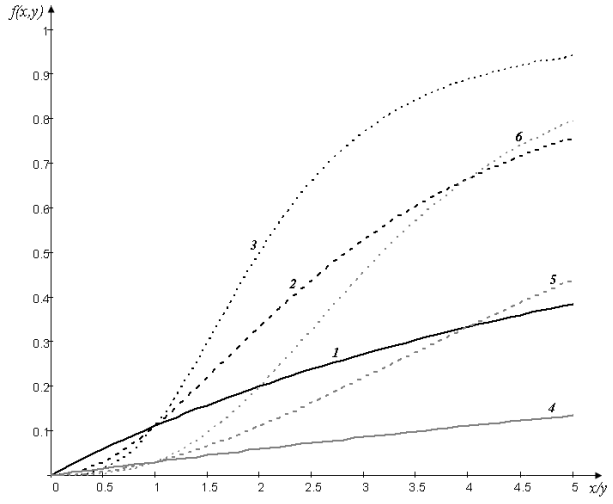

Рис. 2. Залежності $f(x)=\dfrac{x^n}{x^n+c}$ при різних значеннях n і c: криві **1-3** – $c=8$; **4-6** – $c=32$; **1, 4** – $n=1$; **2, 5** – $n=2$; **3, 6** – $n=3$

Результати розрахунків

Пошук сідлової точки ведеться з допомогою програмного комплексу MatLab шляхом почергової оптимізації ресурсів нападу і захисту [5]. Розподіл ресурсів протилежної сторони, досягнутий на попередньому кроці, вважається відомим. На першому кроці покладаємо розподіл $\{y_k\}$ ресурсів захисту на об'єктах пропорційним розподілу інформації $\{g_k\}$ і знаходимо розподіл $\{x_k\}$ ресурсів нападу, котрий забезпечує досягнення $\max\limits_x i(x,y)$ в межах заданої кількості ресурсів $\sum\limits_{k=1}^{l} x_k = X$. На другому кроці, виходячи з одержаного розподілу $\{x_k\}$, знаходимо оптимальний для захисту розподіл $\{y_k\}$, котрий забезпечує досягнення $\min\limits_y i(x,y)$ в межах заданого значення $\sum\limits_{k=1}^{l} y_k = Y$. Якщо сідлова точка для функції $i(x,y)$ існує, то цей процес є збіжним, і ми продовжуємо його до досягнення рівності $\max\limits_x i(x,y) = \min\limits_y i(x,y)$. Ця точка і визначає оптимальні розподіли $\{x_k^0\}$, $\{y_k^0\}$. Якщо сідлова точка відсутня, то після певної кількості кроків процес буде циклічно повторюватись необмежене число разів, показуючи, що стаціонарного стану не існує.

Проведені розрахунки виявили такі закономірності.

1. В найпростішій системі (рис.1,а) при дробно-лінійних залежностях $f_k(x,y)$ сідлова точка існує при всіх значеннях Z.

2. Якщо хоч одна з залежностей $f_k(x,y)$ має дробно-нелінійну форму, то сідлова точка може існувати лише в певних інтервалах значень Z. При збільшенні вразливості за рахунок зростання значення n або зменшення значення c інтервал ΔZ існування сідлової точки звужується і зміщується в сторону менших Z (рис.3). Зазначимо, що збільшення n в робочому діапазоні значень x/y, тобто при x/y>1, відповідно до (5), приводить до збільшення вразливості, а при x/y<1 – до її зменшення (рис.2). Розподіл інформації по об'єктах в наших системах визначається вразливостями об'єктів: більша кількість інформації міститься на об'єктах з меншою вразливістю.

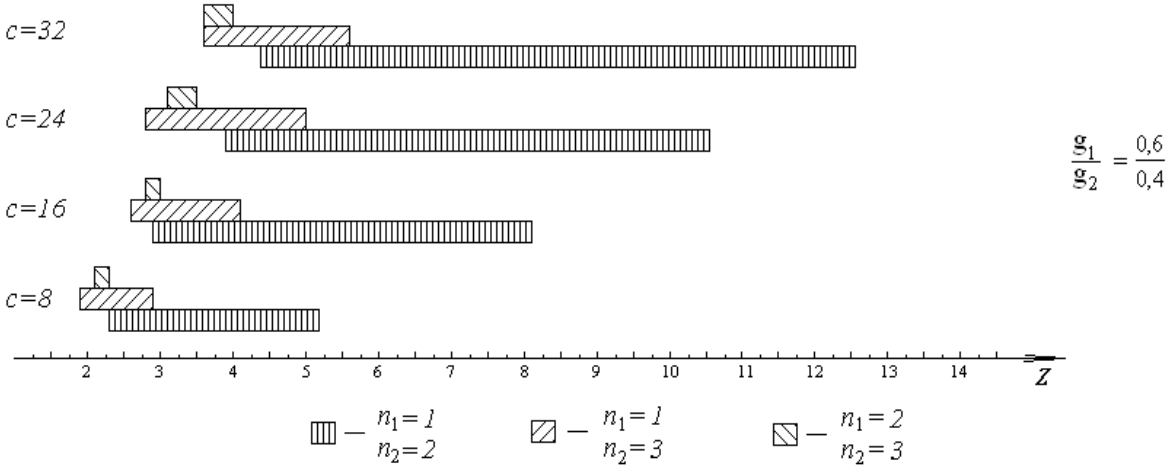

Рис. 3. Вплив форми функцій $f(x,y)$ на інтервал існування сідлової точки в системі (рис.1,а)

3. Ступінь зростання $i(Z)$ визначається вразливостями об'єктів і близьке по формі до залежностей $f_k(x,y)$ (функція $i(Z)$ фактично усереднює залежності $f_k(x,y)$ з ваговими

коефіцієнтами g_k (3), (4)). При зміні форм $f_k(x,y)$ і переході до залежностей з більшим n, що відображає більшу вразливість об'єктів, криві $i(Z)$ зміщуються в бік більших значень i (рис.4).

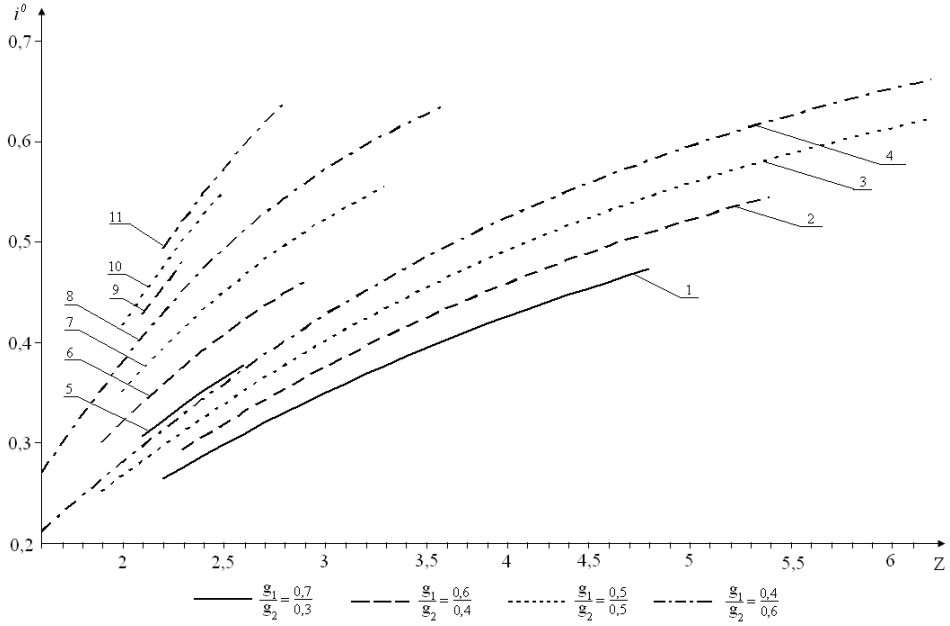

Рис. 4. Частка втраченої інформації в інтервалах існування сідлової точки в системі (рис.1,а) при $c=8$ і різних значеннях g_1/g_2 і n: **1-4** – $n_1=1$, $n_2=2$; **5-8** – $n_1=1$, $n_2=3$; **9-11** – $n_1=2$, $n_2=3$

4. Інтервал існування сідлової точки залежить також від розподілу $\{g_k\}$ інформації між об'єктами (в системі (рис.1,а) – від співвідношення g_1/g_2 – рис.4). В наших розрахунках в перших варіантах інформація розподілялась між об'єктами обернено пропорційно їх вразливостям. Слід зазначити, однак, що співвідношення x/y на різних об'єктах обирається таким чином, що забезпечує досягнення оптимального значення $i(x,y)$.

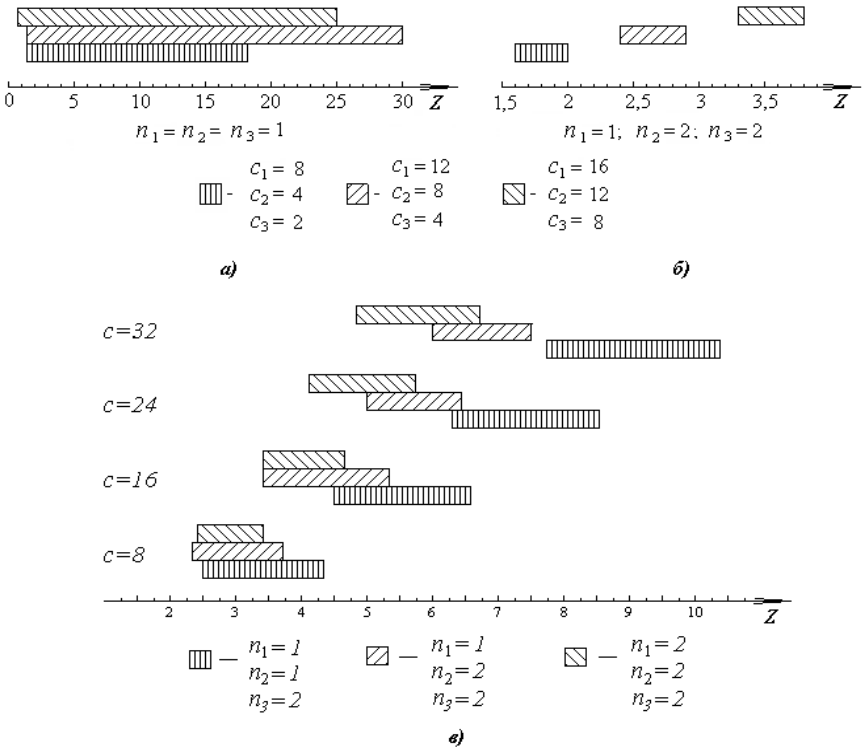

Рис. 5. Інтервали існування сідлової точки в однорівневій системі з трьох об'єктів (рис.1,б) при $g_1=0,4$, $g_2=0,3$, $g_3=0,3$ і різних функціях вразливості: а) дробно-лінійні функції, різні значення c_k; б) дробно-нелінійні функції, різні значення c_k; в) дробно-нелінійні функції, однакові c_k

При зміні Z ці значення також змінюються. В результаті співвідношення між динамічними вразливостями різних об'єктів за наявності нелінійності деяких з них може змінитись на протилежне (на рис.2 при x >1 виконується нерівність $f_3(x) > f_1(x)$, а при x <1 – $f_3(x) < f_1(x)$). Вплив розподілу інформації g_1/g_2 показано на рис.4. Видно, що при «неправильному» розподілі кількості інформації по об'єктах, а саме при її розподілі, пропорційному вразливостям (варіант 4), величини $i(Z)$ досягають більших значень порівняно з іншими варіантами, проте зростає й інтервал ΔZ. При переході до розподілу ресурсів, обернено пропорційного вразливостям об'єктів, значення $i(Z)$ зменшуються, але й зменшується інтервал ΔZ (варіант 1). Ступінь зменшення інтервалу ΔZ зростає із збільшенням нелінійності функцій $f_k(x, y)$ і при $g_1/g_2 = 0,7/0,3$, $n_1 = 2$, $n_2 = 3$ інтервал ΔZ зникає.

5. В системі з трьома перешкодами (однорівневій або дворівневій) ситуація змінюється. Інтервал ΔZ стає обмеженим навіть при використанні дробно-лінійних функцій (рис.5,а; 6), хоча він займає досить широку смугу. Вплив параметрів n і c залишається незмінним: при зростанні n і зменшенні c інтервал ΔZ зменшується і зміщується в сторону менших Z (рис.5,в).

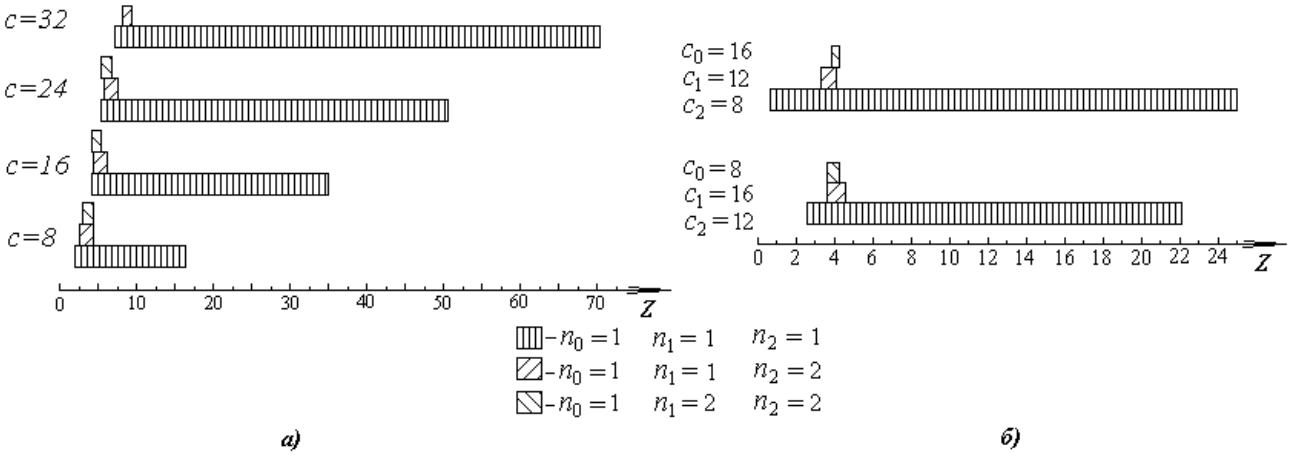

Рис. 6. Інтервали існування сідлової точки в дворівневій системі (рис.1,в) при $g_1 = 0,6$, $g_2 = 0,4$

В системі з дробно-нелінійними функціями введення третього об'єкта (рис.1,б) чи третьої перешкоди (рис.1,в) приводить до звуження інтервалу ΔZ і при деяких значеннях параметрів цей інтервал зникає – сідлова точка відсутня. Збільшення будь-якого із значень n_k порівняно з рис.5,6 приводить саме до такої ситуації – $\Delta Z = 0$. Зміна показника вразливостей c_k на $c_0 = 8$, $c_0 = 8$, $c_0 = 8$ не має суттєвого впливу на інтервали ΔZ.

Висновки

Наведені результати показують, що ускладнення системи приводить до звуження інтервалу існування сідлової точки. Це зрозуміло: введення нових перешкод чи нових об'єктів збільшує число ступенів свободи в розподілі ресурсів, і забезпечити умови, котрі задовольняють обидві сторони, стає складніше. Пояснення потребує вплив вразливості об'єктів на умови існування сідлової точки. Зауважимо, що при дробно-лінійних залежностях $f(x)$ зростання $i(x)$ відбувається монотонно, майже лінійно в широкому інтервалі значень x. Деякі з цих значень відповідають умовам існування сідлової точки. При переході до дробно-нелінійних функцій зростання $i(x)$ відбувається більш стрімко, у вужчому інтервалі значень x. При збільшенні нелінійності ми наближаємось до ступінчастої функції $i(x)$, в котрій зростання $i(x)$ відбувається стрибком в одній точці, і значення $i(x)$ в цій точці стає невизначеним. Задовольнити умовам стаціонарності в цій точці неможливо.

Звертаючись до реальних систем, зазначимо, що дробно-лінійні залежності можуть відображати властивості фізичних систем, в яких збільшення ресурсів приводить до приблизно пропорційного зменшення вразливості. Прикладом різко нелінійної залежності $f(x, y)$ є шифрування даних. В цьому випадку вкладання коштів не дає результату до того моменту, коли вдається зламати шифр, що приводить до стрибкоподібного зростання значення $i(x, y)$.

На завершення зазначимо, що підтвердженням коректності застосування наведеної методики є її порівняння з моделлю Гордона-Лоеба [6], котра знайшла своє емпіричне підтвердження [7,8]. Показано, що обидві методики дають схожі, а при певному виборі параметрів – співпадаючі результати [9].

Література

[1] Вентцель Е.С. Исследование операций. – М.: Сов. Радио. – 1972. – 552 с.

[2] Шикин Е.В., Шикина Г.Е. Исследование операций. – М.: Проспект. – 2006. – 280 с.

[3] Лабскер Л.Г., Бабешко Л.О. Игровые

методы в управлении экономикой и бизнесом. – М.: Дело, 2001. – 464 с.

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

[5] Прус Р.Б. Оптимізація розподілу ресурсів захисту інформації в динамічному режимі // Безпека інформації. – 2012. – №1. – С. 26-32.

[6] Gordon L.A., Loeb M.P. The Economics of Information Security Investment // ACM Transactions on Information and System Security, Nov. 2002. - Vol. 5. - №4. - P.438-457.

[7] Matsuura K., Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model // The Seventh Workshop on the Economics of Information Security. June 25-28, Hanover, USA – 2008.

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

[9] 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 004.056.5 (045)

Левченко Е.Г., Прус Р.Б., Рабчун Д.И. Условия существования седловой точки в многоуровневых системах защиты информации

Аннотация. *При проектировании комплексных систем защиты информации важным вопросом является определение оптимального количества ресурсов, которые необходимы для защиты, и их распределение между объектами, которые отличаются количеством информации, уязвимостью, вероятностью нападения. Поиск решения усложняется из-за неопределенности действий противника. В этих условиях подходящим можно считать решение, соответствующее седловой точке целевой функции, которая может выражать один из показателей системы защиты – потери информации, прибыль от инвестиций в защиту, их рентабельность – в зависимости от соотношения ресурсов нападения и защиты – X и, соответственно, Y. Произведенные расчеты позволяют проанализировать условия существования седловой точки в одно- и двухуровневых системах, которые отличаются количеством объектов и препятствий, которые их защищают. Показано, что седловая точка существует в определенных интервалах значений $Z = \frac{X}{Y}$, которые определяются формой динамической уязвимости объектов и распределением информации по объектам.*

Ключевые слова: *информационная безопасность, математическая модель, целевая функция, динамическая уязвимость, седловая точка.*

Levchenko E.G., Prus R.B., Rabchun D.I. Conditions of saddle point existence in multilevel information security systems

Abstract. *When planning the unified information security systems calculation of optimal resource amount needed for defence and their allocation between the objects, which differ in amount of information, vulnerability or attack probability, are important problems. Search for solution gets more complex over uncertainty of attackers actions. Under the circumstances appropriate is considered solution that match with saddle point of objective function, which express one of security system indicators – part of lost information, benefits of an investment in information security, investment efficiency – depending on correlation of attack X and defence Y resources. Carried out calculations enable to analyse conditions of saddle point existence in one- and multilevel systems, which differ in quantity of objects and obstacles that defend them. It is demonstrated that saddle point exists in certain intervals of values $Z = \frac{X}{Y}$; intervals are determined by form of objects dynamic vulnerability and distribution of information between the objects.*

Key words*: information security, mathematical model, objective function, dynamic vulnerability, saddle point.*

Отримано *31 січня 2013 року*, затверджено редколегією *5 березня 2013 року*