# УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATIONSECURITY MANAGEMENT

# ВПЛИВ ФОРМИ ПРОТИСТОЯННЯ НА ОПТИМІЗАЦІЮ ПРОЦЕСУ УПРАВЛІННЯ РЕСУРСАМИ ЗАХИСТУ ІНФОРМАЦІЇ

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

*[1]Національний авіаційний університет, Україна*
*[2]Державний університет телекомунікацій, 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:* 105 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:* 17 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 телекомунікацій.
*Посада:* студент.
*Наукові інтереси:* інформаційна безпека.
*Публікації:* 4 наукові статті та тези доповіді.
*E-mail:* rabchundima92@gmail.com

***Анотація.*** *Оптимізація кількості ресурсів, які необхідно виділяти на захист інформації, та їх розподілу між об'єктами є важливою задачею економічного менеджменту інформаційної безпеки. Складність пошуку оптимального рішення обумовлена невизначеністю дій суперника в інформаційному протистоянні. В цих умовах особливе значення має пошук сідлової точки матричної гри, яка відображає ситуацію, коли ні одна з сторін не зацікавлена в зміні своєї стратегії. Можливість існування сідлової точки залежить від кількості об'єктів, розподілу інформації між об'єктами, ступеня нелінійності функції* $f(x,y)$*, яка відображає динамічні вразливості об'єктів, а також форми протистояння. При цьому сідлова точка існує лише в певних інтервалах значень* $\Delta Z$*, де* $Z = X/Y$ *- співвідношення ресурсів двох сторін. У випадку однонаправленого протистояння, коли одна з сторін захищає свою інформацію, а друга прагне її вилучити, при дробно-лінійній формі залежностей* $f(x,y)$ *в системі з двох об'єктів сідлова точка існує при всіх* $Z$*, а при переході до дробно-нелінійної форми* $f(x,y)$ *або ускладненні системи за рахунок введення нових об'єктів*

*інтервал $\Delta Z$ стає обмеженим. При різнонаправленому протистоянні, коли кожна з сторін захищає свою інформацію і прагне здобути інформацію суперника, залежності $\Delta Z$ від параметрів системи стають складнішими. Наведені результати розрахунків дозволяють виявити ці закономірності.*

***Ключові слова:*** *інформаційне протистояння, розподіл ресурсів, оптимізація, сідлова точка.*

**Вступ**

Інформаційне протистояння відбувається частіше всього в умовах невизначеності, коли дії суперника нам невідомі і можуть бути передбачені лише з певною імовірністю. Це утруднює оптимізацію розподілу ресурсів між об'єктами захисту і управління ресурсами в динамічному режимі (об'єкти можуть мати як фізичну, так і електронну форми). Проте можлива ситуація, коли змінювати розподіл ресурсів невигідно ні одній з сторін.

У термінології теорії ігор така ситуація відображає сідлову точку матричної гри. Визначення умов існування сідлової точки є важливою задачею економічного менеджменту інформаційної безпеки. Пошук розв'язку ускладнюється його залежністю від значної кількості параметрів і характеристик інформаційної системи. Існування сідлової точки можливе лише в певному інтервалі значень зазначених параметрів.У[1,2] розглянуто деякі аспекти сформу-льованої проблеми для найпростішої форми протистояння, коли дії однієї з сторін направлені на здобуття інформації, а другої – на її захист. Подібна задача розглядалась в [3], де пошук оптимального набору механізмів захисту, який забезпечує мінімум ризику втрат інформації, проводиться на прикладі системи районних відділень банку. Обсяг інформації в кожному відділенні пропорційний потенційній кількості клієнтів, тобто чисельності жителів району. Імовірність реалізації окремих загроз, а також вартість і ефективність кожного з механізмів захисту визначається методом експертної оцінки. При цьому припускається, що імовірність реалізації загрози проти кожного об'єкта однакова і залежить тільки від виду загрози.

Розглядаючи різні комбінації елементів захисту для кожного з відділень, розраховується сумарний збиток для всієї системи (який і характеризує ступінь ризику) і оптимальний набір елементів захисту для кожного відділення за умови введення обмеження на загальну вартість системи захисту. При розрахунку повного ризику залишається відкритим питання про величину перехресних членів, котрі виражають частку інформації, втраченої при реалізації різних видів загроз (ці події вважаємо сумісними).

В умовах конкурентної боротьби кожна з сторін прагне захистити свою інформацію і здобути інформацію суперника. В цьому випадку маємо різнонаправлене, або комплексне протистояння.

**Мета роботи –** розробка математичного апарату з використанням теоретико-ігрових методів, що дасть змогу порівняти умови існування сідлової точки для різних форм протистояння.

**Постановка задачі**

Скористаємось математичною моделлю [4], відповідно до якої цільова функція $i(x,y)$ визначає частку втраченої інформації:

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

де $x$ і $y$ - ресурси сторін; $k$ - номер об'єкта; $g_k$ - частка загальної інформації, котру містить $k$-й об'єкт; $p_k$ - імовірність нападу на $k$-й об'єкт; $q_k(x,y)$ - двомірна щільність імовірності виділення ресурсів $x$ і $y$ на $k$-й об'єкт; $f_k(x,y)$ - вразливість об'єкта, котра визначається як імовірність вилучення інформації з $k$-го об'єкта при заданому співвідношенні $x$ і $y$.

Величини в (1) відносні: $i_k$, $g_k$ віднесені до всієї вартості інформації, $x$ і $y$ - до вартості інформації на об'єкті.

На можливість існування сідлової точки впливають наступні фактори:

– форма протистояння – однонаправлена чи різнонаправлена;

– кількість $l$ об'єктів;

– ступінь вразливості об'єктів, тобто форма функцій $f_k(x,y)$;

– розподіл $\{g_k\}$ інформації між об'єктами.

З врахуванням цих факторів сідлова точка може існувати при певних значеннях $Z=X/Y$, де $X=\sum_{k=1}^{l} x_k$, $Y=\sum_{k=1}^{l} y_k$ - загальна кількість ресурсів кожної з сторін. Інтервал $\Delta Z$ існування сідлової точки визначається зазначеними факторами. В наших дослідженнях основну увагу будемо приділяти впливу розподілів $\{g_k\}$ і залежностей $f_k(x,y)$ на величину $\Delta Z$. З цією метою покладемо в (1) $p_k=1$, $q_k(x,y)=1$ і одержимо

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

Відповідно до моделі [3] залежності $f_k(x,y)$ оберемо у формі дробно-степеневих функцій

$$f_k(x,y)=\frac{\left(x/y\right)^n}{\left(x/y\right)^n+c}, \qquad (3)$$

де параметр $n$ визначає кривизну залежностей, а $c$ - висоту підйому над віссю абсцис. За фізичною суттю величини $n$ і $c$ виражають продуктивність витрат.

**Результати досліджень**

У попередніх роботах [1,2] було встановлено вплив окремих факторів на $\Delta Z$ при однонаправленому протистоянні. Розглянемо, як виявлені закономірності змінюються при переході до різнонаправленого протистояння.Обидві форми протистояння ілюструє рис. 1. На рис. 1,а зображено однонаправлене протистояння в системі з двох об'єктів, котрі містять обсяги інформації $g_1$ і $g_2$. Сторона $X$ прагне здобути інформацію, сторона $Y$ її захищає. На рис. 1,б кожна з сторін має один об'єкт захисту - $g^{(1)}$ для сторони $Y$, $g^{(2)}$ - для сторони $X$ і прагне здобути інформацію з об'єкта суперника. В наших позначеннях нижній індекс – номер об'єкта в системі, верхній – номер системи.

При однонаправленому протистоянні і дробно-лінійній формі функцій вразливості (3) (тобто при $n_1 = n_2 = n = 1$) сідлова точка в системі, що містить два об'єкти (рис. 1,а), існує при всіх значеннях $Z$. При зростанні кількості $l$ об'єктів інтервал $\Delta Z$ стає обмеженим, і його ширина зменшується зі збільшенням $l$. Якщо в системі (рис. 1,а) хоч одна з залежностей $f_k(x, y)$ стає дробно-нелінійною, то інтервал $\Delta Z$ також стає обмеженим. При збільшенні вразливості за рахунок зростання показника $n$ або зменшення параметра $c$ цей інтервал звужується і зміщується в сторону менших $Z$.

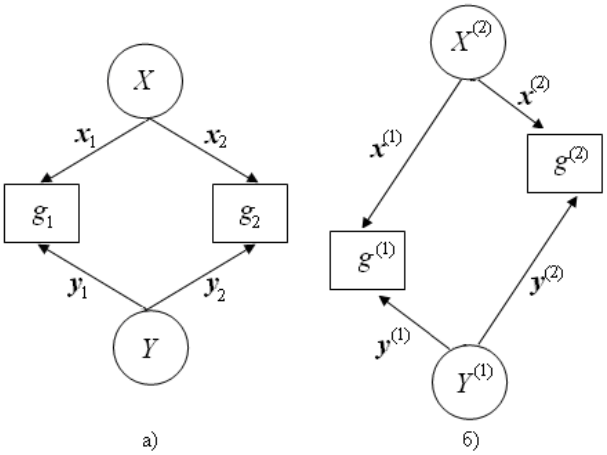


Рис. 1. Схеми протистояння: а) однонаправлене; б) різнонаправлене

При переході до різнонаправленого протистояння навіть в системі з двох об'єктів (рис. 1,б) з дробно-лінійними функціями вразливості інтервал $\Delta Z$ стає обмеженим. Залежність $\Delta Z(n)$ якісно зберігає свій характер: при зростанні $n$ величина $\Delta Z$ зменшується. Ці залежності для обох форм протистояння зображено на рис. 2, формування інтервалу $\Delta Z(n)$ - на рис. 3.

Результати (рис. 2,3) отримані при однаковому розподілі інформації по об'єктах: $g_1/g_2 = g^{(1)}/g^{(2)} = 0,5/0,5$. Інші розрахункові параметри мали такі значення: $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 32$.

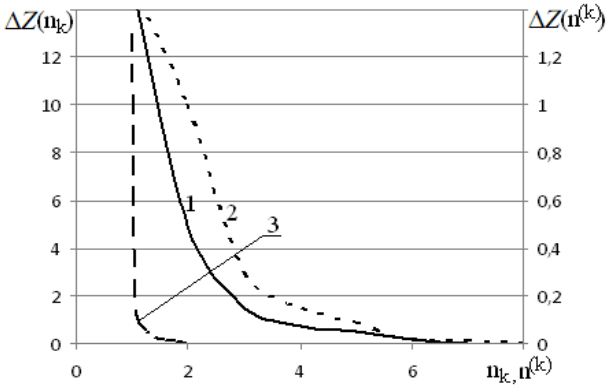


Рис. 2. Залежності ширини інтервалу $\Delta Z$ від $n$ для двох систем: **1** - $\Delta Z(n_1)$, **2** - $\Delta Z(n_2)$ для системи (рис. 1,а); **3** - $\Delta Z(n)$ для системи (рис. 1,б)

Залежності $\Delta Z(n_1)$ і $Z(n_1)$ розраховані при $n_2 = 1$, $\Delta Z(n_2)$ і $Z(n_2)$ - при $n_1 = 1$, залежності $\Delta Z(n)$ - при $n^{(1)} = n^{(2)} = n = 1$. Криві 1,2 на рис. 2, а також аналогічні залежності на рис. 3 відображають вплив параметрів $c_k$.

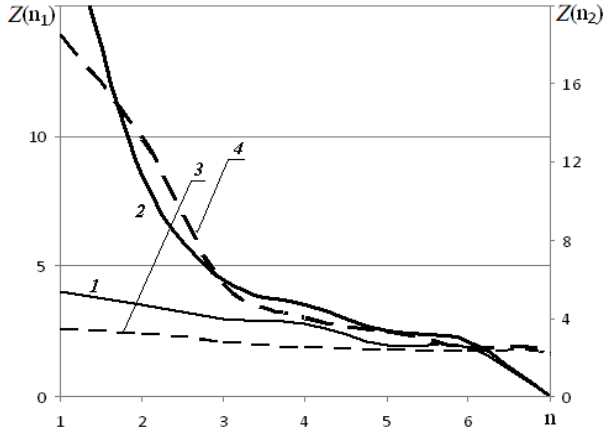


Рис. 3. Межі інтервалу $\Delta Z$ в залежності від $n$ для системи (рис. 1,а): **1**- $Z_{\min}(n_1)$, **2** - $Z_{\max}(n_1)$, **3** - $Z_{\min}(n_2)$, **4** - $Z_{\max}(n_2)$

Результати (рис. 3) отримані для однонаправленого протистояння (рис. 1,а) і дозволяють знайти ширину інтервалу $\Delta Z = Z_{\max} - Z_{\min}$, показану на рис. 2.

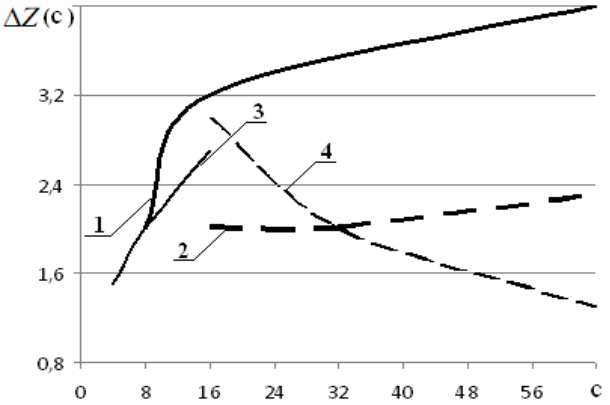


Рис. 4. Залежності $\Delta Z$ від $c$ для двох систем: **1** - $\Delta Z(c_1)$, **2** - $\Delta Z(c_2)$ для системи (рис. 1,а); **3** - $\Delta Z(c^{(1)})$, **4** - $\Delta Z(c^{(2)})$ для системи (рис. 1,б)

Для системи (рис. 1,б) аналогічні залежності не приводяться, оскільки $Z_{\min}(n^{(1)}) = Z_{\min}(n^{(2)}) = 0$, і верхня межа $Z_{\max}$ визначає ширину інтервалу (крива 3, рис. 2).

На рис. 4 зображені залежності $\Delta Z(c)$. Криві 1,2 одержані при $n_1 = n_2 = 2$, оскільки в системі (рис. 1,а) при $n_1 = n_2 = 1$ $\Delta Z \to \infty$, криві 3,4 – при $n_1 = n_2 = 1$, через те, що в системі (рис. 1,б) при $n_1 = n_2 > 1$ $\Delta Z \to 0$.

В функціях $\Delta Z(c)$ суттєво проявляються відмінності двох форм протистояння. Залежності $\Delta Z(c^{(1)})$ і $\Delta Z(c^{(2)})$ (рис. 4) мають якісно протилежний характер: величина $\Delta Z(c^{(1)})$ зростає (крива 3), так само, як $\Delta Z(c)$ для системи (рис. 1,а) (криві 1 і 2), в той час, як $\Delta Z(c^{(2)})$ спадає (крива 4). Це можна пояснити тим, що внесення ресурсів у захист і напад має різний ефект: система захисту повинна бути більш ефективна, ніж система нападу, тобто для зламу системи необхідно вкласти більше ресурсів, ніж було вкладено в захист. Формально це обумовлено тим, що у вирази вразливості (3) $x$ входить в чисельники дробів, а $y$ - в знаменники, і зміна цих величин на $\Delta x$ та, відповідно, $\Delta y$ приводить до різної зміни $\Delta f$ вразливості.

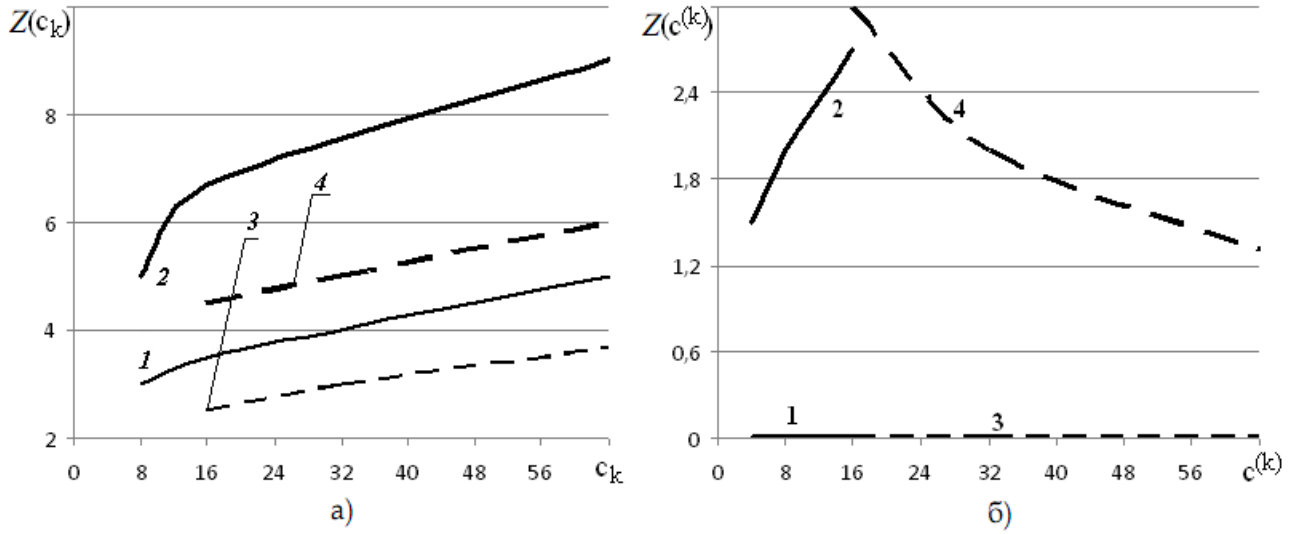


Рис. 5. Межі інтервалу $\Delta Z$ в залежності від $c$ : а) **1** – $Z_{\min}(c_1)$, **2** - $Z_{\max}(c_1)$, **3** - $Z_{\min}(c_2)$, **4** - $Z_{\max}(c_2)$ для системи (рис. 1,а); б) **1** - $Z_{\min}(c^{(1)})$, **2** - $Z_{\max}(c^{(1)})$, **3** - $Z_{\min}(c^{(2)})$, **4** - $Z_{\max}(c^{(2)})$ для системи (рис. 1,б)

Нижня межа інтервалу $\Delta Z(c)$ для системи (рис. 1,б) так, як і в залежності $\Delta Z(n)$, співпадає з віссю абсцис (рис. 5,б). Таким чином, верхня межа залежності $Z(c)$ визначає одночасно ширину інтервалу $\Delta Z(c)$.

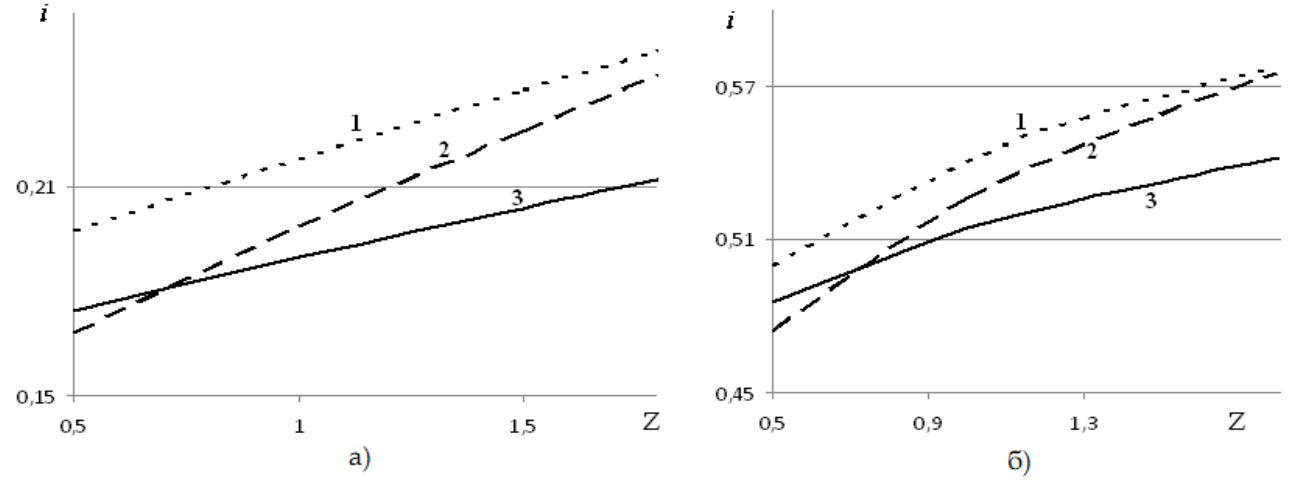


Рис. 6. Частка втраченої інформації в інтервалах існування сідлової точки в залежності від $c$ для двох форм протистояння при $g_1 = g_2 = 0{,}5$ та $n_1 = 1$, $n_2 = 1$: а) для системи (рис. 1,а); б) для системи (рис. 1,б)

**1** - $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 16$; **2** - $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 32$; **3** - $c_1 = c^{(1)} = 16$, $c_2 = c^{(2)} = 32$

Крім ширини інтервалу $\Delta Z$ важливим показником є значення $i(Z)$ в межах цього інтервалу (рис. 6). При збільшенні $c$, що відображає зменшення вразливості об'єктів, криві $i(Z)$ зміщуються в бік менших значень $i$ (перехід від кривої 1 до кривих 2,3). При збільшенні $n$, тобто

зростанні вразливості, значення $i$ в системі (рис. 1,а) збільшуються (ці залежності приведені в [2]). В системі (рис. 1,б) залежність $i(Z)$ при $n>1$ не існує, оскільки $\Delta Z = 0$.

Залежність ширини інтервалу $\Delta Z$ від розподілу інформації по об'єктах видно з рис. 7. Зі збільшенням відношення $g_1/g_2$ величина $\Delta Z$ в системі (рис. 1,а) зростає, а в системі (рис. 1,б) звужується.

Зауважимо, що для обох форм протистояння зміна параметрів системи ($n$, $c$, $g_1/g_2$) приводить до зміни основних показників - $i$ та $\Delta Z$, причому ці зміни мають протилежний характер: найкращі показники по $i(Z)$ досягаються при найгірших показниках $\Delta Z$.

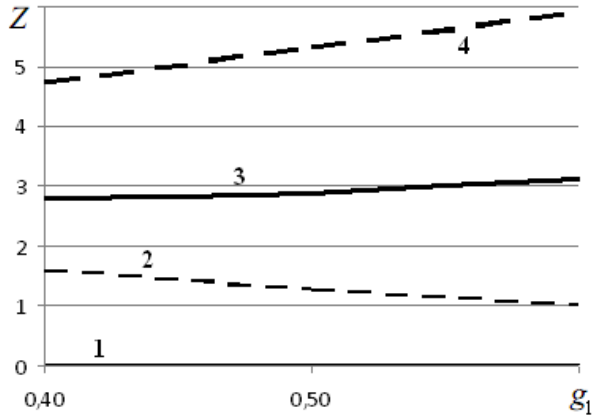


Рис. 7. Межі інтервалу $\Delta Z$ в залежності від $g_1/g_2$ при $c_1 = c^{(1)} = 8$, $c_2 = c^{(2)} = 32$, $n_1 = n^{(1)} = n_2 = n^{(2)} = 1$ для двох систем:

**1** - $Z_{\min}$, **2** - $Z_{\max}$ для системи (рис. 1,б);

**3** - $Z_{\min}$, **4** - $Z_{\max}$ для системи (рис. 1,а)

Для системи (рис. 1,а) найменші втрати інформації, але при найвужчій ширині інтервалу існування сідлової точки відповідають розподілу інформації, обернено пропорційному вразливостям об'єктів: для кривої 1 $g_1/g_2 = 0,7/0,3$ при $n_1 = 1$, $n_2 = 2$. Найширша смуга $\Delta Z$ (при найбільших значеннях $i$) має місце при «неправильному» розподілі інформації, коли більша частина інформації розміщена на більш вразливих об'єктах: для кривої 4 $g_1/g_2 = 0,6/0,4$ при $n_1 = 1$, $n_2 = 2$.

**Висновки**

При однонаправленому протистоянні ускладнення інформаційної структури за рахунок збільшення кількості об'єктів та зростання ступеня нелінійності залежностей, що описують динамічну вразливість об'єктів, приводить до звуження інтервалу $\Delta Z$ існування сідлової точки. Розподіл інформації по об'єктах обернено пропорційно їх вразливостям дозволяє зменшити втрати інформації, проте при одночасному зменшенні $\Delta Z$.

Перехід від однонаправленого до різнонаправленого протистояння підтверджує зазначені тенденції, однак, виявляє деякі нові закономірності. Відмінності двох форм протистояння суттєво проявляються при дослідженні залежностей інтервалів $\Delta Z$ існування сідлової точки від параметра $c$, що входить до функції вразливості як продуктивність витрат.

Проведені розрахунки дозволяють встановити вплив окремих факторів на оптимальне рішення і розробити рекомендації по досягненню режиму сідлової точки в умовах конкурентної боротьби.

**Література**

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

[2] Левченко Є.Г., Прус Р.Б., Рабчун Д.І. Умови існування сідлової точки в багаторубіжних системах захисту інформації // Безпека інформації. — 2013. — №1. — С. 70-76.

[3] Глушак В.В., Новіков О.М. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника // Системні дослідження та інформаційні технології. — 2013. — №2. — С. 89-100.

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

**УДК 004.056.5 (045)**

***Левченко Е.Г., Прус Р.Б., Рабчун Д.И. Влияние формы противостояния на оптимизацию процесса управления ресурсами защиты информации***

***Аннотация.*** *Оптимизация количества ресурсов, которые необходимо выделять на защиту информации, и их распределения между объектами является важной задачей экономического менеджмента информационной безопасности. Сложность поиска оптимального решения обусловлена неопределенностью действий соперника в информационном противостоянии. В этих условиях особое значение имеет поиск седловой точки матричной игры, которая отображает ситуацию, когда ни одна из сторон не заинтересована в изменении своей стратегии. Возможность существования седловой точки зависит от количества объектов, распределения информации между объектами, степени нелинейности функции $f(x, y)$, которая отображает динамические уязвимости объектов, а также формы противостояния. При этом седловая точка существует только в определенных интервалах значений $\Delta Z$, где $Z = X/Y$ - соотношение ресурсов обеих сторон. В случае однонаправленного противостояния, когда одна из сторон защищает свою информацию, а другая пытается ее*

*изъять, при дробно-линейной форме зависимостей $f(x,y)$ в системе из двух объектов седловая точка существует при всех $Z$, а при переходе к дробно-нелинейной форме $f(x,y)$ или усложнении системы за счет введения новых объектов интервал $\Delta Z$ становится ограниченным. При разнонаправленном противостоянии, когда каждая из сторон защищает свою информацию и пытается изъять информацию соперника, зависимости $\Delta Z$ от параметров системы становятся сложнее. Приведенные результаты расчетов позволяют обнаружить эти закономерности.*
***Ключевые слова:*** *информационное противостояние, распределение ресурсов, оптимизация, седловая точка.*

***Levchenko Ye.G., Prus R.B., Rabchun D.I. Influence of confrontation form on optimization of information security resource allocation process***

***Abstract.*** *Optimization of resource amount which must be appropriated for information security and resource allocation between objects is major problem of information security economic management. Complexity of search for solution is conditioned by uncertainty of opponent's actions in information confrontation. In these conditions of particular importance is search for saddle point that represent situation when neither of sides is interested in changing their strategies. Possibility of saddle point existence depends on number of objects, information distribution between objects, extent of function $f(x,y)$ nonlinearity, which defines dynamic vulnerabilities of objects, and form of confrontation. Also saddle point exists only in certain intervals of values $\Delta Z$, where $Z = X/Y$ - proportion of both sides' resources. In case of unidirectional confrontation, when one of sides defends its information and other attempts to get information, with linear-fractional form of functions $f(x,y)$ in system of two objects saddle point exists on all $Z$ and when convert to nonlinear-fractional form $f(x,y)$ or complexification of system by adding new objects interval $\Delta Z$ become limited. In multidirectional confrontation, when each of sides defends its information and simultaneously attempts to get opponent's information, relations $\Delta Z$ to parameters of system become more complex. Given calculation results enable to reveal these relations.*
***Key words****: information confrontation, resource allocation, optimization, saddle point.*

Отримано *15 жовтня 2013 року*, затверджено редколегією *31 жовтня 2013 року*