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

Анотація. *Розглянуто широкий круг задач, які виникають при протистоянні двох сторін у сфері захисту інформацій. Побудовано математичні моделі, обговорюються проблеми, які виникають при пошуку оптимальних рішень в умовах обмеженості ресурсів захисту, намічено шляхи їх подолання. Запропоновано методику, яка може бути застосована до розрахунку економічних показників систем захисту інформації. Запропонована методика враховує значну кількість основних показників та має кілька критеріїв оптимальності, що робить методику гнучкою та зручною в застосуванні.*

Ключові слова: *інформаційна безпека, математична модель, цільова функція, втрати інформації, вразливість.*

Вступ

Основним завданням менеджменту інформаційної безпеки є мінімізація можливих збитків від витоку інформації при одночасній мінімізації витрат на її захист. Ці два частинні критерії оптимальності суперечливі і не можуть бути виконані одночасно. В розрахунок можуть входити також інші показники – такі, як прибуток від внесення інвестицій, їх рентабельність, сумарні втрати, тощо. Розроблені математичні моделі [1-3] направлені на оптимізацію одного або комбінації декількох із згаданих показників. В останньому випадку доводиться розглядати компромісний варіант, в якому зазначені показники враховуються з певними ваговими коефіцієнтами. Постановка задачі в різних моделях має дві основні відмінності: вибір показників, які виражаються цільовою функцією; критерії оптимальності.

Огляд джерел

В моделі Гордона-Лоеба (ГЛ) [1] цільова функція (в наших позначеннях $b(y,v)$) визначає зменшення збитків від витоку інформації за рахунок внесення інвестицій y з відрахуванням цих витрат. В економічних термінах це прибуток від інвестицій. В функцію як параметр входить вразливість v об'єкта, яку автори визначають як імовірність того, що напад буде успішним при $y=0$. При розрахунку цільової функції враховується імовірність $S(y,v)$ порушення інформації при нападі на об'єкт з вразливістю v. Запропоновано два види цих залежностей – $S^{(1)}(y,v)=\frac{v}{(\alpha y+1)^{\beta}}$ і $S^{(2)}(y,v)=v^{\alpha y+1}$, де $\alpha>0$, $\beta\geq 1$ – параметри, які визначають ефективність захисту інформації. Критерієм оптимальності є максимум функції $b(y,v)$, а предметом дослідження – визначення відповідних значень $y=y^0(v)$. Для обох видів залежності $S(y,v)$ маємо $y^0=0$ при $v\gtrsim 0$, і при збільшенні v значення $y^0(v)$ зростають: при $S=S^{(1)}(y,v)$ – до максимуму, який досягається при граничному значенні $v=1$, а при $S=S^{(2)}(y,v)$ – до максимуму при певному значенні v, після чого $S(y,v)$ стрімко знижується до нуля.

В [2] цільова функція являє собою суму витрат y на захист інформації і втрат $i(y)$ від її очікуваного витоку. Метою дослідження в [2] є визначення розміру витрат, при якому цільова функція досягає мінімуму. Дослідженню підлягали подані в загальному вигляді окремі форми цільової функції, які відрізнялись швидкістю зміни сподіваних збитків при зростанні витрат, причому ця величина виражалась залежністю $i'(y)=-k_1 i^{v}(y)$, де k_1 і v – показники, котрі визначаються властивостями об'єкта.

Постановка задачі

Нам видається необхідним ввести вагові коефіцієнти для величин $i(x,y)$ та y, оскільки витрати на захист інформації і збитки від її витоку нерівнозначні для підприємства. Ми будемо оцінювати значення вагових коефіцієнтів λ і $1-\lambda$ по розміру небезпеки, яку справляють величини $i(x,y)$ і y на економічній стан підприємства, хоча усвідомлюємо, що встановити дійсний розмір втрат від витоку інформації в деяких випадках досить проблематично. Розрахувати втрати, очевидно, можна лише в окремих випадках - наприклад, коли вони складають витрати на поновлення порушеної бази даних або коли відбувся витік даних, що містять інформацію про платіжні картки. Якщо ж витік інформації став причиною зменшення прибутку підприємства, об'єктивно оцінити збитки стає досить складно. Зокрема, це важко зробити в умовах конкурентної боротьби, коли в результаті витоку інформації суперник одержує змогу захопити додаткову частину ринку і використовувати цю можливість невизначений час, оскільки передбачити розвиток подій практично неможливо.

В реальних умовах ринкової економіки сумарний ресурс захисту $y=\sum_k y_k$ (k - номер об'єкта) обмежений, і використати визначені оптимальні значення y_{ko} не завжди видається можливим. В цьому випадку постає задача пошуку компромісного (з врахуванням різних критеріїв) розподілу обмежених ресурсів між об'єктами.

Сформульовані в [1, 2] проблеми утворюють двоїсту задачу. При нашому підході маємо дві задачі з протилежними цілями. Перша з них направлена на мінімізацію багатоцільової функції, котра містить складові загальних втрат з певними ваговими коефіцієнтами:

$$w(x,y)=\lambda i(x,y)+(1-\lambda)y, \qquad (1)$$

а друга направлена на пошук максимуму функції, що виражає відносний прибуток від інвестицій:

$$b(x,y)=i(x,0)-i(x,y)-y \qquad (2)$$

В цих виразах $b(x,y)=\frac{B(x,y)}{G}$; $i(x,y)=\frac{I(x,y)}{G}$; $y=\frac{Y}{G}$; $x=X/G$; $w=W/G$, G – загальна вартість інформації на об'єкті; B – прибуток від внесення

інвестицій в захист інформації; I – вартість вилученої з об'єкта інформації; Y – внесені інвестиції в захист інформації (ресурси захисту); X – ресурси нападу; λ та $(1-\lambda)$ – вагові коефіцієнти відповідних величин (в [1], [2] вони відсутні); W(x,y) – загальна сума потенційних втрат в інформаційній системі; Маленькими літерами b, i, y, x, w позначені відповідні відносні величини.

Результати дослідження

Нам здається більш доцільним використовувати вираз (2), оскільки він дає змогу розглядати без додаткових перетворень більшу кількість оптимізаційних задач, зокрема, розраховувати рентабельність інвестицій. При переході до розрахунків ключовим питанням є вибір залежності $i(x,y)$. Представимо її у вигляді [3]:

$$i(x,y) = q(x)\cdot f(x,y) \qquad (3)$$

де $q(x)$ – щільність імовірності виділення суперником ресурсів x; $f(x,y)$ – залежність частки вилученої інформації від співвідношення x і y.

Маючи на меті порівняння з результатами [2], визначимо y_b з умови $b(x,y_b) - \max$, для випадку, коли $f(x,y) = \dfrac{x/y}{x/y+1}$, $q(x) = 1$ в інтервалі $x = [0;1]$.

Ця залежність зображена на рис. 1, де максимально доцільний відсоток витрат на захист інформації складає 25% від її вартості, що співпадає з висновком [2] за умови використання залежності $i'(y) = -k_1 i^{\nu}(y)$ при $\nu = 2$.

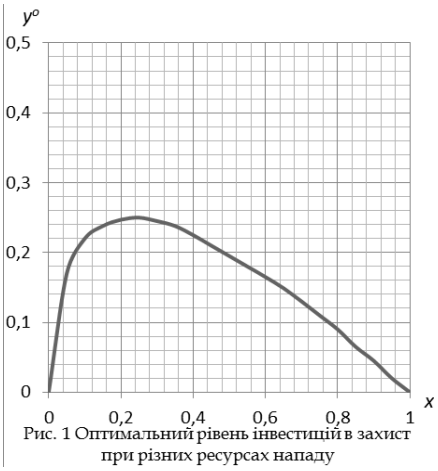

Рис. 1 Оптимальний рівень інвестицій в захист при різних ресурсах нападу

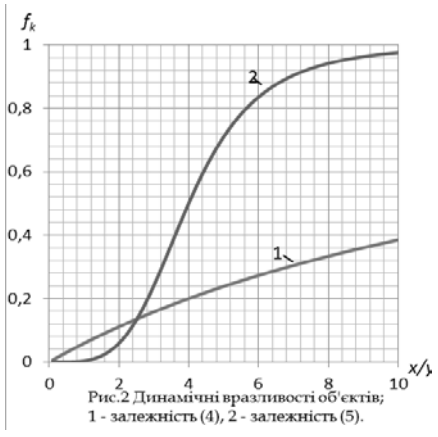

Рис.2 Динамічні вразливості об'єктів; 1 - залежність (4), 2 - залежність (5).

Повертаючись до нашої методики, розглянемо систему з двох об'єктів і поставимо задачу: знайти оптимальний розмір інвестицій в кожний з об'єктів, використовуючи різні критерії оптимальності. Зосередимо увагу на залежностях $f_k(x,y)$. Для цього покладемо $q(x) = 1$, звідки випливає $i(x,y) = f(x,y)$. Враховуючи вимоги до зазначених залежностей і можливі форми [3], оберемо їх у вигляді:

$$f_1(x,y) = \frac{x/y}{(x/y) + 2^4} \qquad (4)$$

$$f_2(x,y) = \frac{(x/y)^4}{(x/y)^4 + 4^4} \qquad (5)$$

Основна відмінність виразів (4) і (5) полягає в напрямку опуклості при $x \gtrless 0$ (рис. 2). Ця особливість, як і вся функція $f(x,y)$, на наш погляд, відображає вразливість об'єкта в залежності від співвідношення ресурсів нападу і захисту. На першому етапі ми не враховуємо вагові коефіцієнти λ і $(1-\lambda)$.

На рис. 3 приведені значення частки захищеної інформації $j(x,y) = 1 - i(x,y)$ і прибутку $b(x,y) = j(x,y) - y$ в залежності від розміру інвестицій y при використанні функцій $f(x,y)$ у формі (4) (рис. 3,а) і (5) (рис. 3,б). На цих рисунках і далі покладено $x = 0{,}25$. Штрихова пряма зображає розмір інвестицій і служить для розрахунку $b(x,y)$. Максимальні значення b_{1m}, b_{2m} визначають відповідні величини y_{1b}, y_{2b}.

Рентабельність інвестицій дорівнює $r(x,y) = \dfrac{b(x,y)}{y}$. Значення y_{kr}, яке відповідає максимальній величині рентабельності, визначається дотичною, проведеною з початку координат до кривої $b(y)$: $r_{\max} = tg\alpha$, де α – кут між дотичною і віссю x (рис. 3,б). Для першого об'єкта $y_{1r} = 0$, для другого $0 < y_{2r} < y_{2b}$. Оптимальне значення y_{ko} для кожного об'єкта знаходиться в інтервалі між y_{kr} і y_{kb} і визначається в залежності від пріоритетів, які надаються відповідним показникам – рентабельності і прибутку від внесення інвестицій. З рис. 3 маємо $\dfrac{y_{1b}}{x} = 0{,}48$, $\dfrac{y_{2b}}{x} = 0{,}56$. Враховуючи прийняте значення $x = 0{,}25$, одержуємо $y_{1b} = 0{,}12$, $y_{2b} = 0{,}14$. Таким чином, необхідні для одержання максимального прибутку інвестиції становлять 12% від вартості інформації для першого об'єкта і 14% - для другого. Прибуток при цих значеннях y складає, відповідно, $b_{1m} = 0{,}76$, $b_{2m} = 0{,}82$. Максимальна рентабельність інвестицій для першого об'єкта досягається при $y_{1r} = 0$, а для другого – при $y_{2r} = 0{,}324 \cdot 0{,}25 = 0{,}08$ і становить $r_{2m} = \dfrac{b_{2r}}{y_{2r}} = \dfrac{0{,}67}{0{,}08} = 8{,}37$.

Врахуємо тепер вагові коефіцієнти λ. На рис.4 зображені залежності (2) з використанням (4), (5) при

λ=0,8: крива 1 - $b_1(x,y)=1-0{,}8\,f_1(x,y)-0{,}2y$, крива 2 - $b_2(x,y)=1-0{,}8\,f_2(x,y)-0{,}2y$.

Як видно з рис. 4, оптимальні значення y_{sm}, при $x=0{,}25$ дещо змінились: $y_{sm}=0{,}23$; $b_{1m}=0{,}90$ для першого об'єкту і, відповідно, $y_{sm}=0{,}18$, $b_{2m}=0{,}95$ для другого.

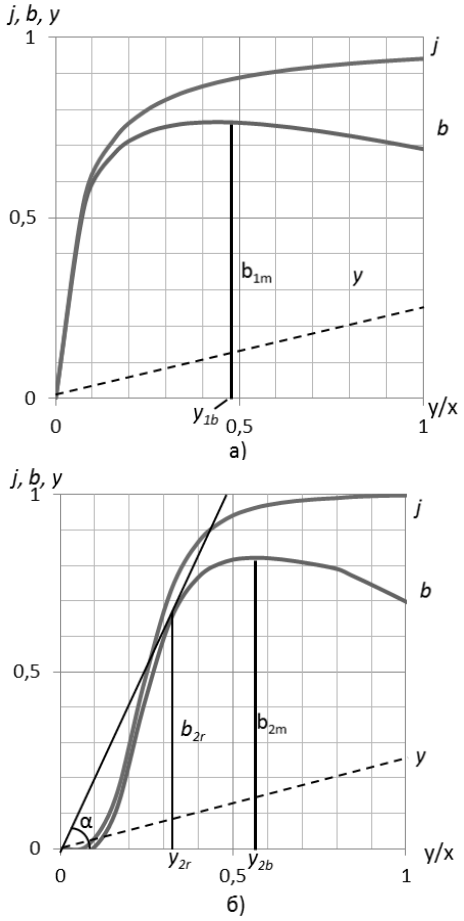

Рис. 3. Економічні показники об'єкта при різних видах динамічної вразливості: а – дробно-лінійна, б – дробно-нелінійна

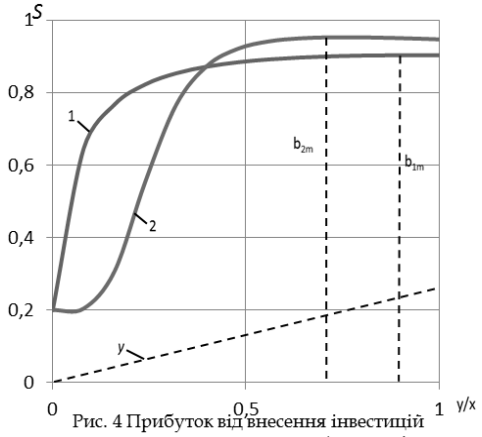

Рис. 4 Прибуток від внесення інвестицій з врахуванням вагового коефіцієнта λ.

Перейдемо до залежностей $q(x)$ в (3). Зрозуміло, що імовірність виділення нападом ресурсів x не може бути однаковою для різних x і при умові реалізації нападу повинна мати максимум при певному $x=x_m$. З міркувань, викладених в [3], оберемо залежність $q(x)$ у вигляді розподілу Максвела $q(x)=Nx^2e^{-h^2x}$, де N – нормовочний коефіцієнт, а h визначає положення максимуму залежності $q(x)$: $x_m=\frac{1}{n}$. Задамо для прикладу $x_m=0{,}3$ (максимально імовірний розмір ресурсів нападу становить 30% від вартості інформації), інтервал можливих значень x візьмемо в межах $0..0{,}5$. Коефіцієнт N визначаємо з умови $\int_{x=0}^{0,5}q(x)dx=1$ і одержуємо:

$$q(x)=96x^2(e^{-11x^2}) \qquad (6)$$

Перейдемо до залежностей $q(x)$ в (3). Зрозуміло, що імовірність виділення нападом ресурсів x не може бути однаковою для різних x і при умові реалізації нападу повинна мати максимум при певному $x=x_m$. З міркувань, викладених в [3], оберемо залежність $q(x)$ у вигляді розподілу Максвела $q(x)=Nx^2e^{-h^2x}$, де N – нормовочний коефіцієнт, а h визначає положення максимуму залежності $q(x)$: $x_m=\frac{1}{n}$. Задамо для прикладу $x_m=0{,}3$ (максимально імовірний розмір ресурсів нападу становить 30% від вартості інформації), інтервал можливих значень x візьмемо в межах $0..0{,}5$. Коефіцієнт N визначаємо з умови $\int_{x=0}^{0,5}q(x)dx=1$ і одержуємо:

$$q(x)=96x^2(e^{-11x^2}) \qquad (7)$$

Ця функція зображена на рис. 6.

Використовуючи (7), визначимо максимально доцільний обсяг витрат на захист інформації. Як видно з рис.6, ці обсяги за наведених умов складають $y_{1m}=0{,}5$, $y_{2m}-0{,}36$ для першого і другого об'єктів, і показують вплив функцій (4), (5) на оптимальний рівень захисту. При певному значенні x крива 2 різко обривається, засвідчуючи той факт, що інвестиції в захист недоцільні: простіше відшкодувати збитки.

Розглянемо тепер систему з двох об'єктів.

$$i(x,y)=\frac{I(x,y)}{g}=g_1f_1(x,y)+g_2f_2(x,y); \qquad (8)$$

$$f_1(x,y)=\frac{x/y}{x/y+2^4};\ f_2(x,y)=\frac{(x/y)^4}{(x/y)^4+4^4} \qquad (9)$$

Визначимо оптимальний розподіл ресурсів (y_{1o},y_{2o}), де $y_{1o}+y_{2o}=Y_o$ і відповідні значення b_{1o}, b_{2o}. Якщо одержане значення Y_o перевищує допустимий рівень витрат: тобто $Y_o>Y_{zp}$ (наприклад $Y_{zp}=0{,}10g$), то зменшуємо Y, причому зменшення ведемо по тому об'єкту, для якого b_k менше за інший об'єкт, до того моменту, коли значення похідних не зрівняються: $b_1'(y)=b_2'(y)$. Після цього зменшення ведеться по іншому об'єкту. Візьмемо для прикладу g_1=0,75, $g_2=0{,}25$, $g_1+g_2=g=1$, $Y_{zp}=0{,}20$. Використаємо результати попередніх розрахунків. Для $q=const$, $x=0{,}25$, визначимо b для y_{km}:

$$i=0{,}75*0{,}097+0{,}25*0{,}05=0{,}0853;$$

$b = 1 - i(x, y) = 0{,}9148$

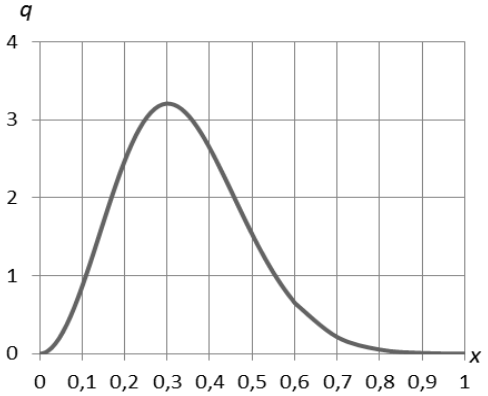

Рис.5 Щільність імовірності виділення ресурсів нападу

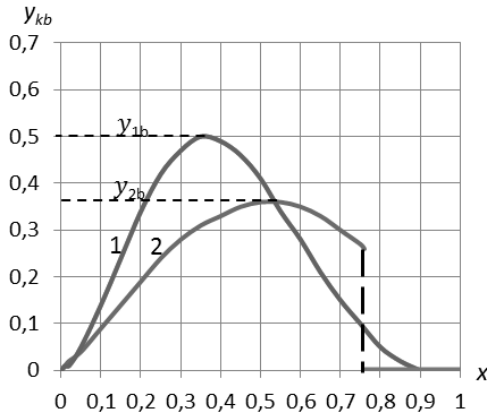

Рис.6 Оптимальний рівень інвестицій з врахуванням залежності $q(x)$.

Але при цьому :
$Y = 0{,}75 * 0{,}23 + 0{,}25 * 0{,}18 = 0{,}2175$, що перевищує $Y_{гр}$. Необхідно зменшити витрати на захист та обрати інші y_k. Оскільки $b_1 < b_2$, зменшуємо y_1. Тоді $y_1 = 0{,}20$ при цьому $Y = 0{,}20$, що дорівнює граничному значенню. Загальний виграш зменшився несуттєво: $b = 0{,}9125$. Отже, оптимальний розподіл буде $y_{1o} = 0{,}20$; $y_{2o} = 0{,}18$.

Висновки

Як показано вище, наведена методика при певному виборі параметрів розрахунку дає результати, котрі співпадають з [2]. В [4] викладено її порівняння з [1] і показано, що однакові результати можна досягти і в цьому випадку. Отже, методика [3] близька до найбільш вживаних методик [1,2], проте, на наш погляд, більш повно відображає властивості об'єктів, дає можливість оцінити ширше коло їх показників і дати більш розгорнуті рекомендації по їх оптимізації. Це дає підстави вважати, що наведена методика може бути застосована до розрахунку економічних показників систем захисту інформації, котрі відрізняються кількістю об'єктів, вразливістю, розподілом інформації по об'єктах при різних значеннях ресурсів нападу.

Література

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

[2] Задірака В.К., Олексюк О.С., Смоленюк Р.П., Штабалюк П.І. Фінансування витрат на захист інформації в економічній діяльності // Університетські наукові записки. – 2006. – № 3-4 (19-20). – С. 479-490.

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

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

УДК 004.056:621 (045)

Рабчун А.О. Оптимизация суммарных потерь в сфере защиты информации

Аннотация. *Рассмотрено широкий круг задач, которые возникают при противостоянии двух сторон в сфере защиты информации. Построены математические модели, обсуждаются проблемы, которые возникают при поиске оптимальных решений в условиях ограниченных ресурсов защиты, предложены пути их преодоления. Предложено методику, которую можно применить для расчета экономических показателей систем защиты информации. Предложенная методика учитывает значительное количество основных показателей и имеет несколько критериев оптимальности, что делает методику гибкой и удобной для применения.*

Ключевые слова: *информационная безопасность, математическая модель, целевая функция, потери информации, уязвимость.*

Rabchun A.O. Optimization of total losses in information security sphere

Abstract. *We consider a wide range of problems which appear from the confrontation between the two sides in the field of information security. The mathematical models are built, the problems arising during the process of searching for optimal solutions in the resource-limited protection are discussed, and the ways of overcoming them are suggested. The method can be used for calculating of the economic data of information security systems. The proposed method considers the significant number of key indicators and has several criteria of optimality that makes the method flexible and easy to use.*

Keywords: *information security, mathematical model, objective function, information losses, vulnerability.*

Отримано *30 березня 2012 року*, затверджено редколегією *06 червня 2012 року*
(рецензент д.т.н., проф. В.О. Хорошко)