

ПРОДУКТИВНІСТЬ ІНВЕСТИЦІЙ В ІНФОРМАЦІЙНУ БЕЗПЕКУ

Розглянуто показники продуктивності інформаційної безпеки по зменшенню вразливості і зменшенню загрози. Ці показники утворюють двовимірний простір продуктивності, який можна поділити на зони, котрі визначають різні стратегії розподілу ресурсів. Визначені границі зон в залежності від властивостей об'єктів і умов протистояння, приведені приклади розрахунків.

Вступ. Одним з основних завдань економічного менеджменту інформаційної безпеки є оптимізація кількості і розподілу ресурсів, виділених на захист інформації. Пошук оптимуму ведеться в рамках математичної моделі, котра в максимальній степені повинна відтворити реальні умови протистояння, уникаючи при цьому зайвих ускладнень. Ключовим питанням у формуванні математичної моделі є побудова цільової функції, яка дає можливість визначити потрібні показники.

Аналіз джерел. Серед кількісних моделей найбільше визнання за останній час одержала модель Гордона - Лоеба (ГЛ) [1]. В цій моделі цільова функція виражає прибуток від інвестування, який визначається як зменшення витрат від витоку інформації за відрахуванням витрат y на її захист. Суттєвим в моделі ГЛ є введення поняття вразливості v , яка залежить від інвестицій y в захист інформації (параметром в цю залежність входить початкова вразливість, котра визначається як v при $y = 0$). Основним елементом цільової функції є $p(y, v)$ - ймовірність витоку інформації з об'єкта з вразливістю v при кількості інвестицій y . Запропоновані дві формули залежностей $p(y, v)$:

$$p^I(y, v) = \frac{v}{(\alpha y + 1)^\beta} \quad (1)$$

та

$$p^{II}(y, v) = v^{\alpha y + 1}, \quad (2)$$

де параметри $\alpha > 0$ та $\beta \geq 0$ виражають міру продуктивності інформаційної безпеки.

Модель ГЛ знайшла свій розвиток в низці робіт. Зокрема в [2] продуктивність інформаційної безпеки поділяється на два показники: продуктивність зменшення вразливості і продуктивність зменшення загрози. Перший з цих показників дорівнює $v^{\alpha y + 1}$, а другий - $t^{\beta y + 1}$, де t - ймовірність загрози, а α і β - міри продуктивності обох типів. Рішення оптимізаційної задачі дозволяє знайти y^0 - розмір оптимальних інвестицій, при якому прибуток від інвестування досягає максимуму. Простір продуктивності по параметрам α і β ділиться на зони, в одних з них $y^0 = 0$, в інших визначається виразами, які впливають з розв'язку задачі.

Постановка задачі. В [3] запропоновано дещо інший підхід, в якому кількість вилученої інформації $i(x, y)$ визначається через співвідношення ресурсів нападу і захисту - x і, відповідно, y :

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

де $q(x, y)$ - ймовірність виділення нападом ресурсів x при заданому рівні ресурсів y ; $f(x, y)$ - частка вилученої інформації при заданому співвідношенні x і y .

Використовуючи підхід [2], можемо вважати, що $q(x, y)$ визначає продуктивність зменшення загрози при внесенні інвестицій y в захист, а $f(x, y)$ - продуктивність

зменшення вразливості. В [3] запропоновані можливі варіанти цих залежностей. Враховуючи, що в (3) x і y входять у вигляді співвідношення $\frac{y}{x}$, введемо нову змінну

$y_0 = \frac{y}{x}$ і оберемо залежності $f(y_0)$ і $q(y_0)$ у такому вигляді (рис.1):

$$f(y_0) = \frac{a}{1 + cy}, \quad (4)$$

$$q(y_0) = N \frac{1}{y_0^2} e^{-\frac{h^2}{y_0^2}}, \quad (5)$$

де a , c і h - параметри, а N - коефіцієнт нормування.

Форми залежностей $f(y_0)$ і $q(y_0)$ вибрані з наступних міркувань. Залежність $f(y_0)$ повинна задовольняти умовам: при $y_0 \rightarrow 0$ $f \rightarrow a$ (початкова вразливість, яка визначається природною захищеністю об'єкта), при $y_0 \rightarrow \infty$ $f \rightarrow 0$. Залежність $q(y_0)$ являє собою розподіл Максвела, який відображає той факт, що при $x \rightarrow 0$ і $x \rightarrow \infty$ $q(x, y) \rightarrow 0$. При деякому значенні y_0 , що визначається параметром h , функція має максимум. З точки зору продуктивності інвестицій вважатимемо, що $\alpha = c$ є міра продуктивності зменшення вразливості, а $\beta = h^2$ - міра продуктивності зменшення загрози.

Побудуємо цільову функцію, яка визначає прибуток від інвестицій у вигляді:

$$b(x, y) = i(x, 0) - i(x, y) - y, \quad (6)$$

або

$$b(y) = i(0) - \frac{N}{y^2} e^{-\frac{\beta}{y^2}} \cdot \frac{a}{1 + \alpha y} - y, \quad (7)$$

де $i(0) = 1$ - кількість інформації, вилученої при $y = 0$. В цьому виразі для спрощення запису покладено $x = 1$. З умови $\frac{db}{dy} = 0$ одержуємо вираз для знаходження оптимального значення y^0 :

$$b'(y) = \frac{N}{y^3} \cdot \frac{1}{1 + \alpha y} \cdot \left(2 - 2\beta \cdot \frac{1}{y^2} + \frac{\alpha y}{1 + \alpha y}\right) \cdot e^{-\frac{\beta}{y^2}} - 1 = 0. \quad (8)$$

Результати досліджень. Дослідимо отриману функцію за допомогою програмних засобів математичного моделювання. На рис.2 зображено хід функції $b'(y)$ (8) при обраних значеннях $\alpha_1 = 0.1$, $\beta_1 = 0.05$ (суцільна крива) і $\alpha_2 = 0.1$, $\beta_2 = 0.16$ (штрихова). Значення параметрів α і β вибрані так, щоб проілюструвати різні ситуації у визначенні мір продуктивності.

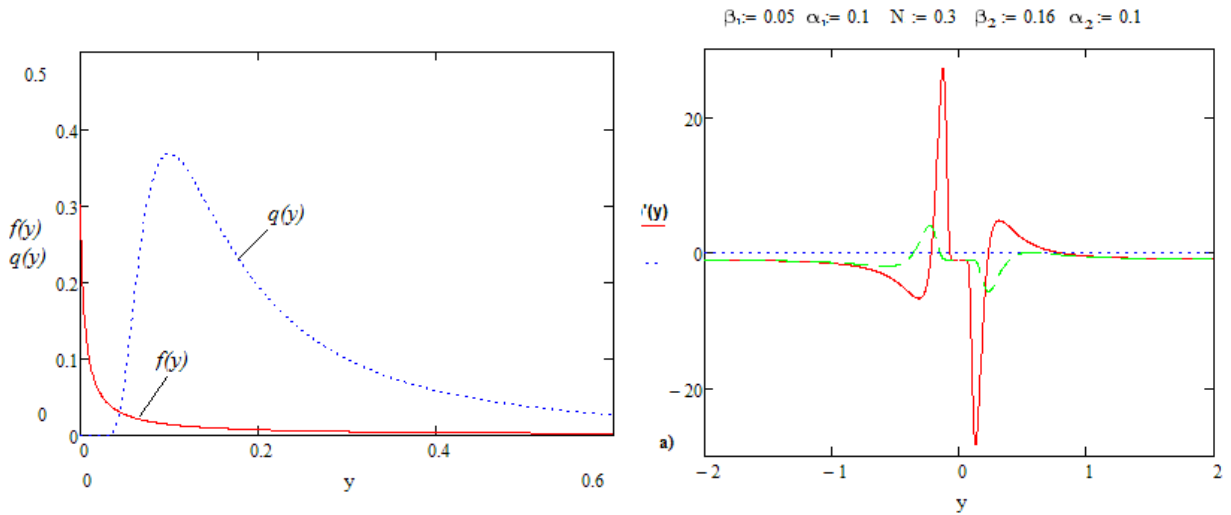


Рис.1 Залежності $f(y)$ і $q(y)$ при $a = 0.3$ $N = 0.01$ $c = 200$ $h = 0.1$

Рис.2 Допоміжні графіки для визначення зон

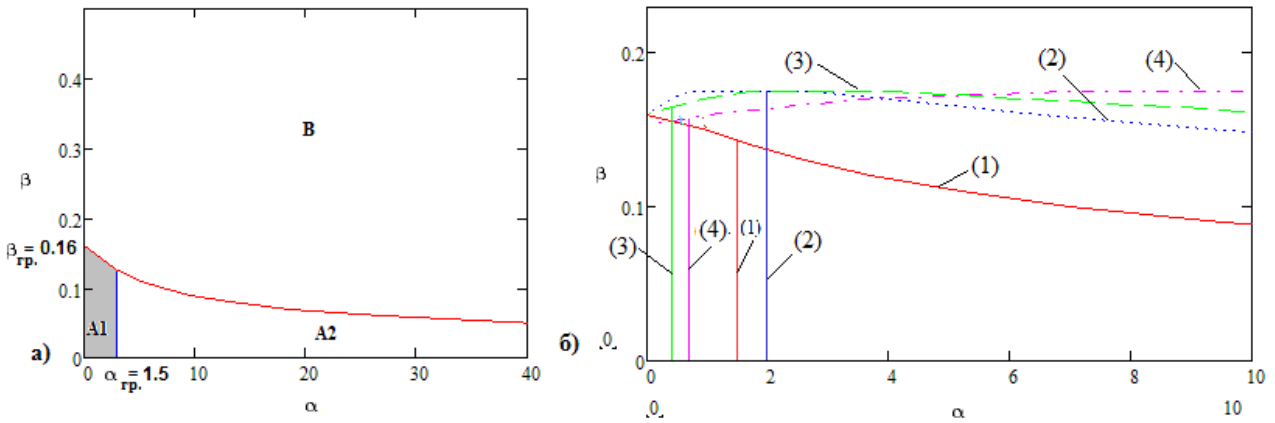


Рис.3 Простір продуктивності при різних варіантах цільової функції

Розглядаючи рівняння (8), звернемо увагу на розв'язки, що знаходяться в додатній частині осі y . Точка першого перетину з віссю y є точкою мінімуму $b(y)$, а друга - максимуму. При зростанні мір продуктивності α та β форма кривої (рис.2) змінюється, і при деяких значеннях параметрів α та β крива є дотичною до осі y (пунктирна лінія). Ці значення α та β є граничними, що обмежують зону існування значень y^0 . Граничні значення показників формують спадаючу криву на рис.3а.

Простір продуктивності поділяється на три зони (рис.3а). A1 - малі α та малі β , A2 - великі α та малі β , B - великі β . A1 - зона збитковості, в якій інвестування позбавлене сенсу, оскільки більш вигідно відшкодувати збитки від втрати інформації, ніж вносити інвестиції. A2 - зона, в якій можливо знайти оптимальне відношення ресурсів, виходячи з рівняння (8). B - зона, яка характеризується досить високими мірами продуктивності. Захист інформації в ній не потребує значних грошових надходжень, і потрібний рівень захисту можливо досягти при невеликих грошових витратах. В зоні B максимум прибутку досягається при інвестиціях, близьких до нуля і не існує як такої точки максимізації. Можна зробити висновок, що для зони B рівень інвестицій в інформаційну безпеку можливо визначити залежно від допустимої кількості вилученої інформації.

Дослідимо зміни границь зон продуктивності функції залежно від зміни складових $f(y)$ та $q(y)$. Вважаючи розглянутий варіант, в якому $b(y)$ задається виразом (7), варіантом 1, розглянемо наступні варіанти.

2. Залежність $f(y)$ (4) змінюємо на квадратичну:

$$b(y) = 1 - \frac{N}{y^2} \cdot e^{-\frac{\beta}{y^2}} \cdot \frac{1}{1 + \alpha y^2} - 1, \quad (9)$$

$$b'(y) = \frac{2N}{y^3} e^{-\frac{\beta}{y^2}} \frac{1}{1 + \alpha y^2} \left(1 - \frac{\beta}{y^2} + \frac{\alpha y^2}{1 + \alpha y^2}\right) - 1.$$

3. Залежність $q(y)$ змінюється з квадратичної (розподіл Максвелла) на лінійну (розподіл Релея):

$$b(y) = 1 - \frac{N}{y} \cdot e^{-\frac{\beta}{y}} \cdot \frac{1}{1 + \alpha y} - 1, \quad (10)$$

$$b'(y) = \frac{N}{y^2} e^{-\frac{\beta}{y}} \frac{1}{1 + \alpha y} \left(1 - \frac{\beta}{y} + \frac{\alpha y}{1 + \alpha y}\right) - 1.$$

4. Використовуються обидві змінені залежності $f(y)$ і $q(y)$:

$$b(y) = 1 - \frac{N}{y} \cdot e^{-\frac{\beta}{y}} \cdot \frac{1}{1 + \alpha y^2} - 1, \quad (11)$$

$$b'(y) = \frac{N}{y^2} e^{-\frac{\beta}{y}} \frac{1}{1 + \alpha y^2} \left(1 - \frac{\beta}{y} + \frac{2\alpha y^2}{1 + \alpha y^2}\right) - 1.$$

На рис.3б зображений простір продуктивності для різних варіантів функції $b(y)$. Цифрами позначені лінії, що зображають границі зон для відповідних варіантів. При заміні $f(y) = \frac{1}{1 + \alpha y}$ на $f(y) = \frac{1}{1 + \alpha y^2}$, перехід від варіанту 1 до варіанту 2, дещо збільшується зона нульових інвестицій A1 (гранична пряма між зонами A1 та A2 трохи зміщується вправо) і розширюється зона A2 за рахунок підйому границі між зонами A2 та B. При заміні $q(y) = N \frac{1}{y^2} e^{-\frac{\beta}{y^2}}$ на $q(y) = N \frac{1}{y} e^{-\frac{\beta}{y}}$ варіант 3, відбувається значне зменшення зони нульових інвестицій та відносно невелике збільшення зони A2. Таким чином, для варіанту 2 ми маємо найбільшу зону нульових інвестицій, для варіанту 3 – найменшу, для варіанту 4 – найбільшу зону A2. Варіант 1 відповідає найменшій зоні A2.

Для варіанту 2 при зміні $f(y)$ ми отримуємо функцію з більшою чутливістю до міри α . В цьому випадку, враховуючи що $0 \leq y < 1$, для збереження попереднього рівня захисту інформації, порівнюючи з варіантом 1, потрібно збільшити рівень інвестицій y або збільшити показники a та β . Варіант 2 може демонструвати об'єкт із більш застарілим обладнанням захисту інформації, в обслуговуванні якого потрібна більша кількість персоналу.

Для варіанту 3 при зміні $q(y)$ ми отримуємо функцію з меншою чутливістю до міри β . Порівнюючи (7) і (9) приходимо до висновку, що рівень захисту інформації буде зберігатись і при зниженні рівня інвестицій або при зниженні показників a та β .

Розглянемо як приклад інформаційну систему, яка містить три об'єкти з об'ємами інформації $g_1 = 0.2$, $g_2 = 0.3$, $g_3 = 0.5$. Міри продуктивності для об'єктів обрані такими, щоб оптимальні значення інвестицій знаходились в різних зонах: $\alpha_1 = 50$, $\beta_1 = 0.02$, $a_2 = 100$, $\beta_2 = 0.2$, $\alpha_3 = 100$, $\beta_3 = 0.01$. Границі зон нульових інвестицій визначаються з умови $b(y) = 0$ (7) і становлять: $\alpha_{zp.1} = 2000$, $\alpha_{zp.2} = 500$, $\alpha_{zp.3} = 40$. З (8) знаходимо оптимальний розмір інвестицій: для першого об'єкту оптимум знаходиться в зоні A1 і становить $y_1^0 = 0$, для третього об'єкту оптимум – в зоні A2 і становить $y_3^0 = 0.239$. Для другого об'єкту оптимум знаходиться в зоні B і визначається з (3), за допомогою рис.5, і лежить в інтервалі $y_2^0 \in (0; 0.12)$. При $y_2^0 > 1$ $i(y) \rightarrow 0$, але ці значення не можна вважати оптимумом, оскільки вони відповідають великим розмірам інвестицій. На рис.4 побудовано зони продуктивності для представленої системи.

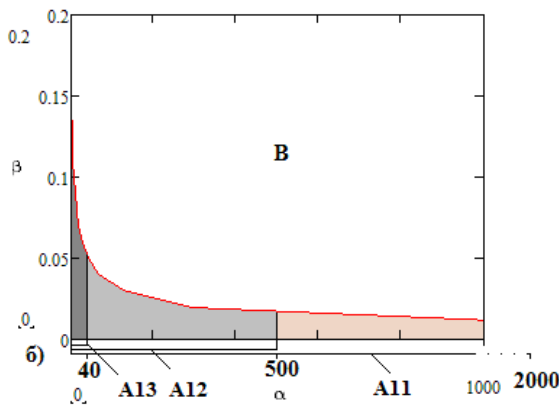


Рис.4 Зони продуктивності для систем з трьох об'єктів

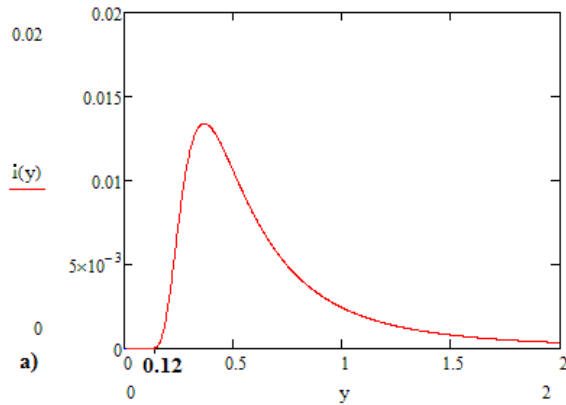


Рис.5 Допоміжний рисунок для визначення y_2^0 у зоні B.

де A11 – зона нульових інвестицій для першого об'єкту, A12 – другого, A13 –третього.

Висновки. Проведені розрахунки дозволяють розробити стратегію вибору оптимального значення ресурсів захисту в залежності від заданих мір продуктивності зниження загрози і зниження вразливості. Описана методика може бути застосована на об'єктах з різними значеннями вразливості, різними ймовірностями нападу і кількості ресурсів.

Література

1. Gordon L.A.: The economics of information security investment. /Loeb M.P. — ACM Trans. on Information and System Security, 5(2002), p.438-457.
2. Matsuura K., Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, The Seventh Workshop on the Economic of Information Security 25-28 June 2008, Hanover, USA.
3. Левченко Є.Г. Оптимізаційні задачі менеджменту інформаційної безпеки, НТЖ "Сучасний захист інформації" /Рабчун А.О., 2010 №1, С.16-23.

Надійшла: 12.03.11

Рецензент: д.т.н., проф. Квасніков В.П.