УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

ПОКАЗНИКИ ПРОДУКТИВНОСТІ ВИТРАТ НА ЗАХИСТ ІНФОРМАЦІЇ

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

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

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: 80 наукових публікацій, серед яких монографії, 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: 15 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: 2 наукові статті та тези доповіді.
E-mail: rabchundima92@gmail.com

Анотація. *Розглянуто продуктивності витрат на захист інформації по зменшенню вразливості системи і зменшенню загрози нападу. Проаналізовано вплив показників інформаційної системи на міру обох продуктивностей.*

Ключові слова: *інформаційна безпека, вразливість, продуктивність витрат.*

Вступ

Розвиток інформаційної сфери проявляється, з одного боку, в зростанні обсягів інформації і їх комерційної вартості, з другого – в збільшенні кількості нападів і, відповідно, вартості втрат. Виникає необхідність постійного удосконалення систем захисту, що супроводжується збільшенням їх вартості. При цьому зростають вимоги до ефективності використання ресурсів захисту, показником якої є продуктивність витрат.

Огляд джерел

Поняття продуктивності витрат введене в [1], де була сформована математична модель інформаційної безпеки, котра одержала назву моделі Гордона – Лоеба (ГЛ). Відповідно до цієї

моделі імовірність порушення інформаційної системи описується функцією $S(y,v)$, де y - інвестиції в захист, а v - початкова вразливість системи (при $y=0$).

Функція $S(y,v)$ може приймати дві форми:

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

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

де параметри α >0 і $\beta\geq 1$ виражають міру продуктивності інформаційної безпеки, тобто ступінь зменшення імовірності $S(y,v)$ при внесенні інвестицій y.

Цільова функція в [1] виражає прибуток $b(y)$, котрий визначається як зменшення втрат за рахунок внесення коштів y в захист інформації за відрахуванням величини y:

$$b(y)=\left[v-S(y,v)\right]L-y, \quad (3)$$

де L - потенційні втрати (вартість інформації в системі).

Модель ГЛ знайшла свій розвиток в багатьох роботах і стала найбільш відомою моделлю економічного менеджменту інформаційної безпеки. Зокрема, в [2] продуктивність інформаційної безпеки поділяється на два показники: продуктивність зменшення вразливості (ПЗВ) і продуктивність зменшення загрози (ПЗЗ). Перший з цих показників визначається виразом $v^{\alpha y+1}$, а другий – $t\beta y+1$, де t - імовірність загрози, а α і β - міри продуктивності обох типів. Таким чином, внесені в захист інвестиції y впливають і на зменшення вразливостей, і на зменшення загрози. Ступінь цього впливу при заданій величині y залежить в першому випадку – від початкової вразливості, а в другому – від імовірності нападу. Введені показники продуктивності формують двомірний простір продуктивності, котрий, в залежності від значень v і y, можна поділити на 3 зони: 1) зона низької продуктивності при малих інвестиціях, коли обидві продуктивності малі; 2) зона середньої вразливості, де ПЗВ висока, а ПЗЗ низька; 3) зона високої вразливості, де ПЗЗ висока.

Звичайно, цей поділ носить приблизний характер, границі зон не можуть бути окреслені точно, і дослідження зон може надати лише якісні висновки щодо величин v і y. Розмір y^0 оптимальних інвестицій, при якому прибуток від інвестування досягає максимуму дає рішення оптимізаційної задачі. Одним з результатів такого дослідження є визначення інтервалів значень α і β, в якому $y^0=0$ - інвестування недоцільне, оскільки витрати перевищують кількість захищеної інформації.

Методика розрахунків

В [3] запропонована інша модель, в якій цільова функція $i(x,y)$ виражає відносну кількість втраченої інформації та при здійсненому нападі визначається через співвідношення ресурсів нападу і захисту - x і, відповідно, y:

$$i(x,y)=q(x,y)f(x,y), \quad (4)$$

де $q(x,y)$ - щільність імовірності виділення нападом ресурсів x при заданому рівні ресурсів y, $f(x,y)$ - частка втраченої інформації.

Функція $f(x,y)$ представляє динамічну вразливість на відміну від статичної вразливості $f(x,0)$. Наслідуючи [2], можемо вважати, що $f'_y(x,y)$ визначає продуктивність зменшення вразливості при внесенні інвестицій y в захист, а імовірнісна функція $q'_y(x,y)$ - продуктивність зменшення загрози. Міри обох продуктивностей визначаються параметрами, які входять в ці функції.

Оскільки, за припущенням [3], функції, які входять в (4), залежать від співвідношення x і y, в цих виразах достатньо залишити одну змінну. Розглядаючи дії захисту і покладаючи $x=1$, в якості такої змінної оберемо y. В [3] запропоновані два види функції $f(y)$ - степеневі і показникові. Враховуючи, що вони мають схожі форми (це диктується фізичними міркуваннями), обмежимось розглядом степеневої функції:

$$f(y)=\frac{1}{1+cy^{n}} \quad (5)$$

Для функції $q(y)$ запропоновано використовувати розподіли Максвела і Релея. При використанні розподілу Максвела маємо:

$$q(y)=N\frac{1}{y^{2}}e^{-\frac{h^{2}}{y^{2}}}, \quad (6)$$

де h визначає положення максимуму залежності $q(y)$: $h=y_m$. Параметри n, c в (5) можна розглядати як міри продуктивності зменшення вразливості, а параметр h в (6) – як міру продуктивності зменшення загрози.

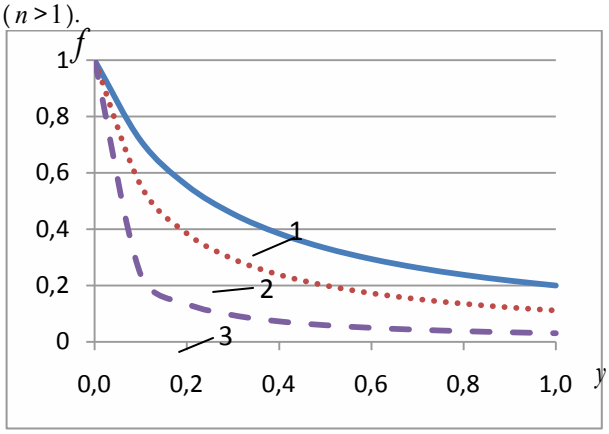
Використовуючи модель [3], в [4] здійснено першу спробу проаналізувати положення різних зон у просторі продуктивності при різних варіантах функцій $f(y)$ і $q(y)$. Проте слід зазначити, що вибір форм цих функцій, інакше кажучи – параметрів залежностей, котрі входять в цільову функцію, при розробці різних моделей носить дещо довільний, недостатньо обґрунтований характер і не має чіткого зв'язку з реальними системами.

Мета роботи – дослідження функцій динамічної вразливості і імовірності нападу та визначення на їх основі продуктивності витрат.

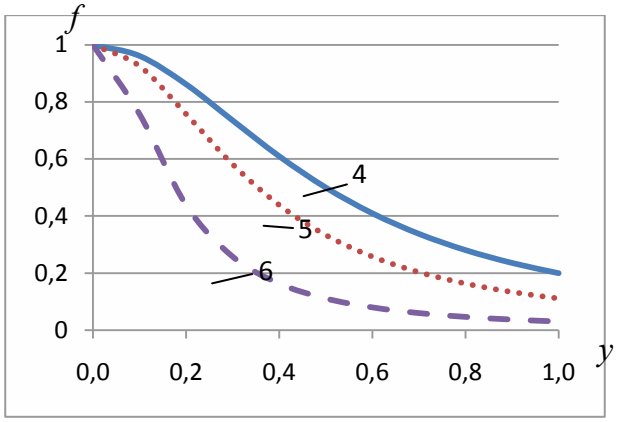
Результати досліджень

На рис.1,2 показано хід залежностей $f(y)=\frac{1}{1+cy^{n}}$ при різних n і c. На рис.1 результати скомпоновані так, щоб показати вплив параметра c при різних n, а на рис.2 – вплив параметра n при різних c. Видно, наскільки зменшуються значення $f(y)$ при збільшенні c і

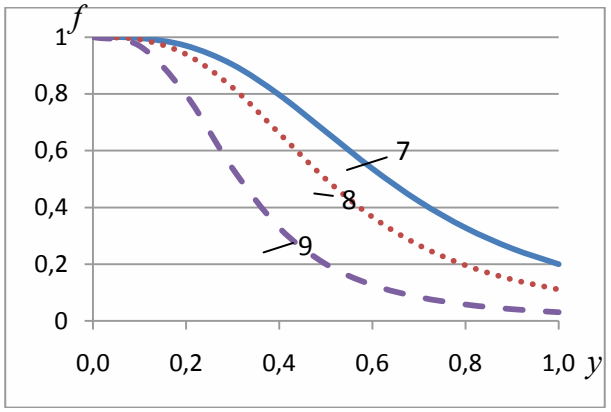
сталому y і зростають при збільшенні n. Вважаємо, що $y<1$ — для зламу системи необхідно виділити більше коштів ніж внесено в захист. Враховуючи, що зменшення $f(y)$ означає зменшення вразливості, можемо оцінити ступінь зростання ПЗВ при збільшенні c і зменшенні n. Цим підкреслюється важливість встановлення значень n і c, котрі відображають об'єктивні характеристики інформаційної системи. З загальних міркувань можна зробити висновок, що властивості фізичних систем краще описують дробно-лінійні функції ($n=1$), а властивості електронних – дробно-нелінійні ($n>1$).



а)



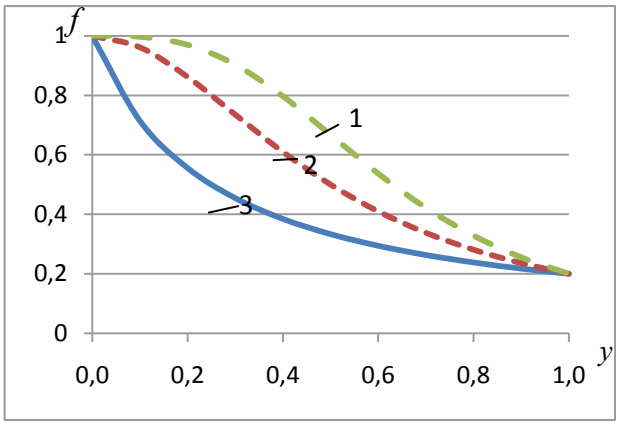
б)



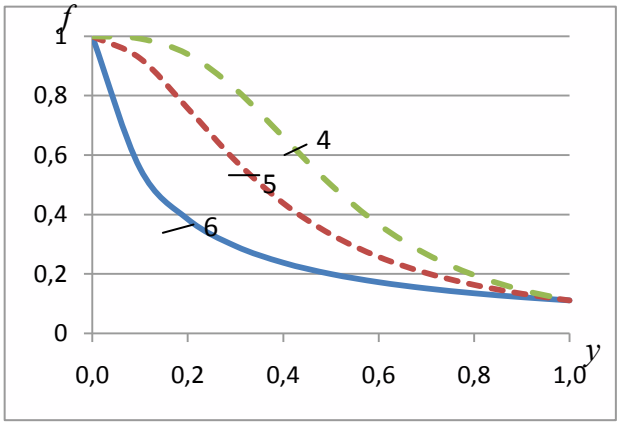
в)

Рис. 1. Вплив параметра c в залежностях $f(y)=\dfrac{1}{1+cy^n}$ при різних n: а) $n=1$; б) $n=2$; в) $n=3$

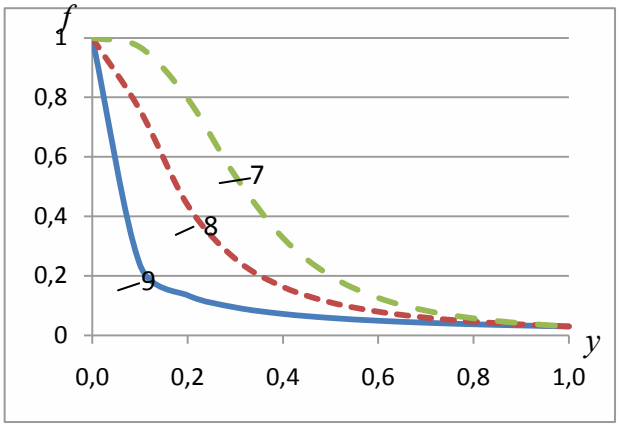
1, 4, 7 — $c=4$; ***2, 5, 8*** — $c=8$; ***3, 6, 9*** — $c=32$



а)



б)



в)

Рис. 2. Вплив параметра n в залежностях $f(y)=\dfrac{1}{1+cy^n}$ при різних c: а) $c=4$; б) $c=8$; в) $c=32$

Залежність ПЗВ від розміру інвестицій y визначається крутизною кривої $f(y)$. При дробно-лінійних залежностях зона високої продуктивності обмежується низькими значеннями y (рис.1,а). Цим відображається той факт, що в фізичних системах необхідні певні початкові заходи, котрі не потребують великих витрат, проте можуть суттєво зменшити вразливість. При зростанні розміру інвестицій їх ефективність зменшується, що

відповідає відомому економічному закону про зменшення граничної норми прибутку.

При дробно-нелінійних залежностях $f(y)$ (рис.1,б,в) зона високої продуктивності ПЗВ відповідає середнім значенням y. При високому рівні нелінійності ($n \geq 3$) в початковій області $y \geq 0$ з'являється «поличка» (рис.1,в), яка свідчить про те, що існує певний мінімальний рівень витрат, котрий приносить відчутний ефект у зменшенні вразливості. Це відповідає висновку [2] про наявність зони низької продуктивності, в якій $y^0 = 0$.

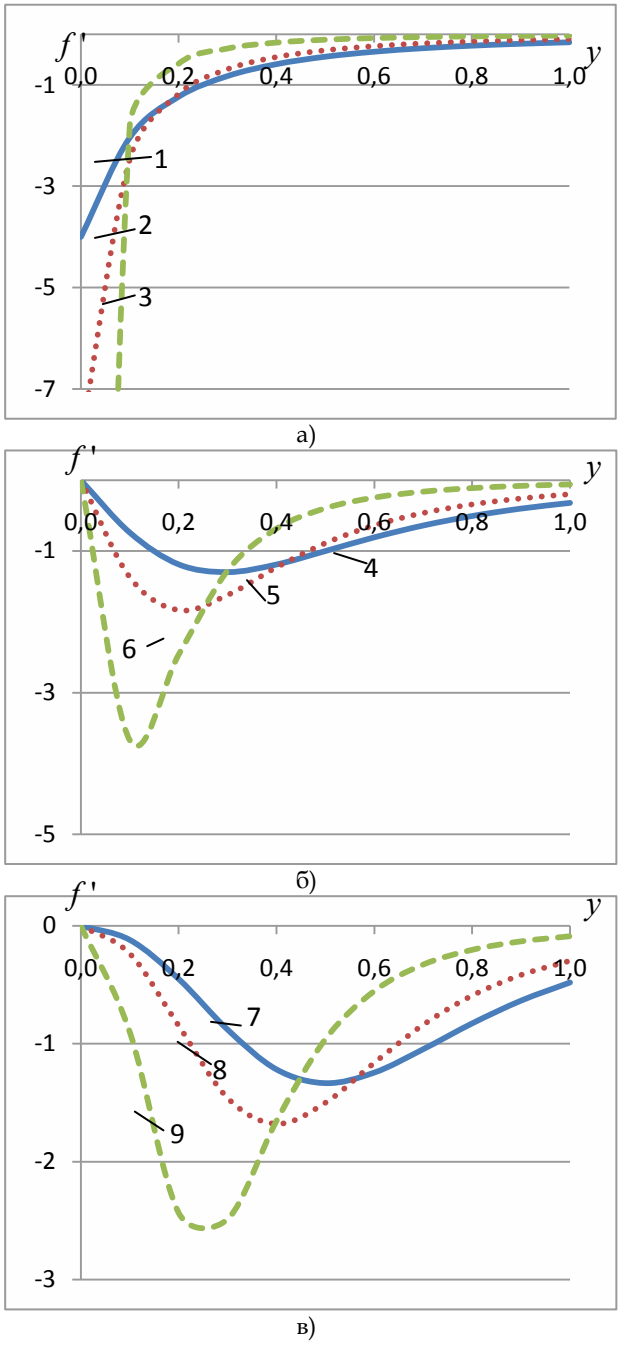


Рис. 3. Крутизна функцій $f(y)$ в залежності від c при різних n: а) $n=1$; б) $n=2$; в) $n=3$
1, 4, 7 — $c=4$; ***2, 5, 8*** — $c=8$; ***3, 6, 9*** — $c=32$

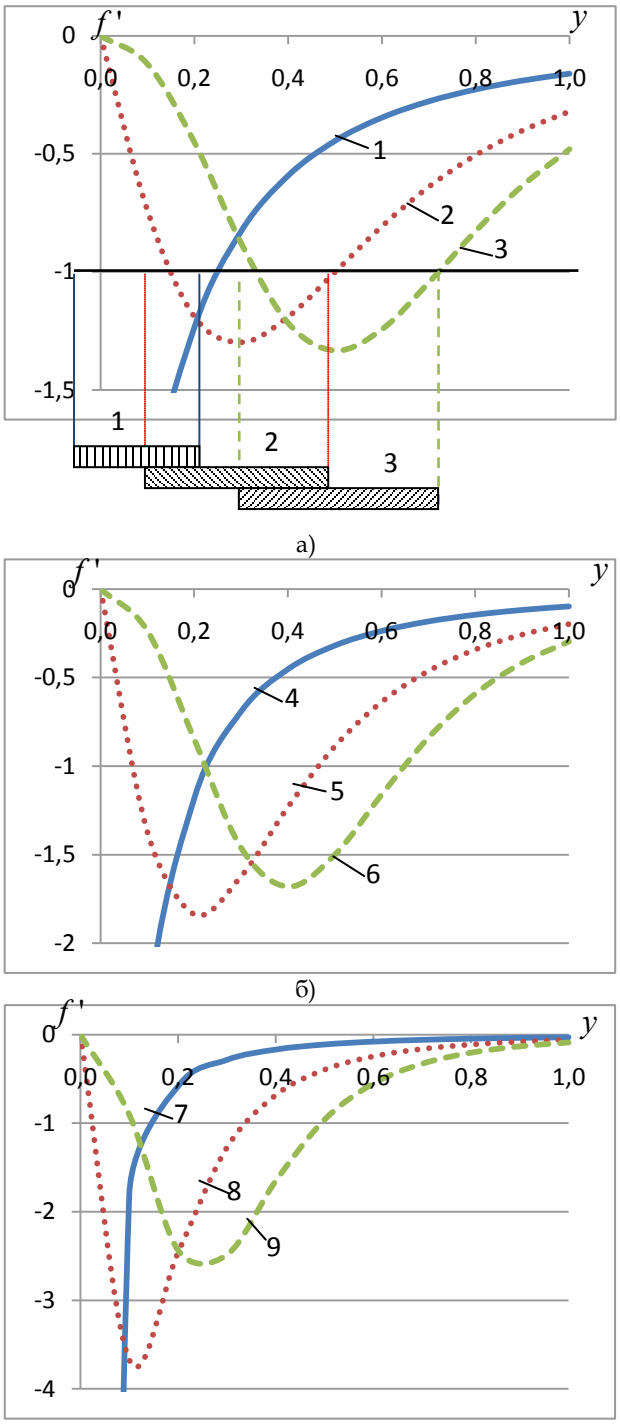


Рис. 4. Крутизна функцій $f(y)$ в залежності від n при різних c: а) $c=4$; б) $c=8$; в) $c=32$;
1, 4, 7 — $n=4$; ***2, 5, 8*** — $n=8$; ***3, 6, 9*** — $n=32$

На рис.3,4 показано хід похідних $f'(y)$ при різних значеннях n і c. За даними цих рисунків визначимо зони високої ПЗВ, границі яких встановимо значенням $f'(y) = -1$ (рис.4,а). Аналізуючи положення зон в залежності від параметрів n і c, відзначимо такі закономірності. При $n=1$ ліва границя співпадає зі значенням $y=0$. В цій точці крутизна $f'(y)$ і, відповідно, ПЗВ

досягають найбільших значень, поступово зменшуючись і прямуючи до нуля при зростанні y.

При $n > 1$ ліва границя зміщується вправо, свідчачи про те, що при дробно-нелінійній формі динамічної вразливості невеликі за розміром інвестиції в захист неефективні. В тому ж напрямку зміщується права границя. Зміщення інтервалів зростає зі збільшенням n і зменшується при збільшенні c. Таким чином, можлива ситуація, коли зміщення інтервалів при одночасній зміні значень n і c буде частково компенсуватись за умови їх різнобічної зміни. Повна компенсація не може бути досягнута, оскільки ці параметри мають різний вплив на залежність $f(y)$: при збільшенні c значення $f(y)$ узгоджено зменшуються при всіх y (рис.1), а при збільшенні n в початковій області значень y змінюється форма залежності – з'являється «поличка» (рис.2). Найбільші значення ПЗВ слабо залежать від n і суттєво – від c : при збільшенні $n \geq 2$ максимальне значення $|f'(y)|$ залишається майже незмінним (рис.4), а при збільшенні c значно зростає, хоча це зростання зменшується при збільшенні n (рис.3).

Розрахунок ПЗВ дозволяє визначити вплив внесення інвестицій на показники ефективності систем захисту. Якщо в (4) не враховується розподіл $q(y)$, то $i(y) = f(y)$ і ПЗВ одночасно визначає продуктивність зменшення втрат інформації (ПЗІ).

В системі, котра містить декілька об'єктів з різними характеристиками $f_k(x, y)$ (k - номер об'єкта) на ПЗВ буде впливати також розподіл інформації між об'єктами. У випадку двох об'єктів цільова функція, яка визначає відносну кількість втраченої інформації, має вигляд:

$$i(y_1, y_2) = g_1 f_1(y_1) + g_2 f_2(y_2)$$

Цю функцію можна представити у вигляді просторової фігури (рис.5). Види функціональних залежностей на цьому рисунку вибрані довільно, оскільки він має лише ілюстративний характер. Улоговина просторової фігури визначає мінімальні значення $i_{\min}(y_1, y_2)$ при різних величинах сумарного ресурсу захисту $y_1 + y_2 = Y$ і одночасно дозволяє знайти оптимальний розподіл (y_1^0, y_2^0) для кожного значення Y та напрямок зміни цього розподілу при збільшенні Y, котрий, в свою чергу, визначає ПЗВ. Вона показана на рис.5 жирною лінією. Це лінія найшвидшого спуску, котру можна поділити на 3 дільниці: 1 – всі кошти вкладають в перший об'єкт, $y_2 = 0$; 2 – y_1 зменшується, а y_2 зростає (перерозподіл ресурсів); 3 – y_1 та y_2 зростають.

Форми залежностей $q(y)$ і їх похідні $q'(y)$, котрі визначають ПЗЗ, показані на рис.6. В загальному випадку цільова функція для системи з двох об'єктів має вигляд:

$$i(y_1, y_2) = g_1 q_1(y_1) f_1(y_1) + g_2 q_2(y_2) f_2(y_2) \quad (7)$$

Оптимальний розподіл ресурсів $\{y_1^0, y_2^0\}$ визначається умовою: продуктивність зменшення втрат інформації, тобто величина $di(y_1^0, y_2^0)$ повинна бути максимальною порівняно з усіма іншими розподілами.

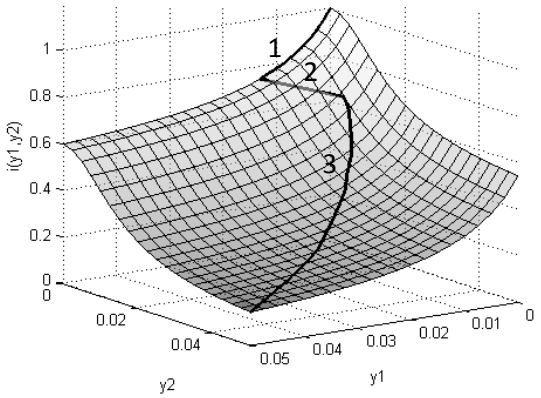
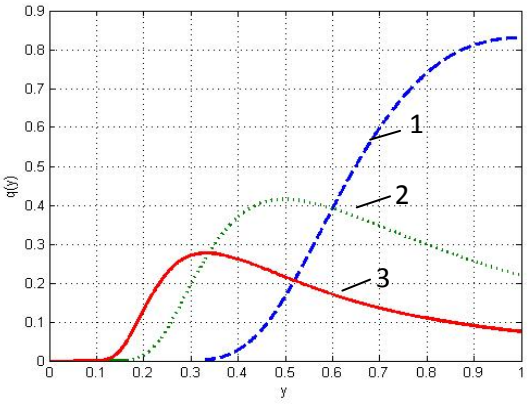
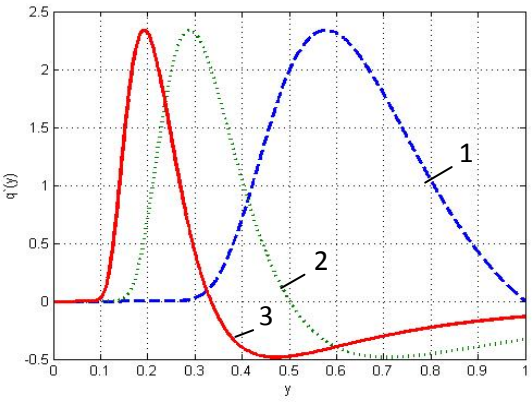


Рис. 5. Вид залежності $i(y_1, y_2)$ при $g_1 = g_2 = 0{,}5$,

$$f_1(y_1) = \frac{1}{1+16y_1},\ f_2(y_2) = \frac{1}{1+16y_2^2}$$



а)



б)

Рис. 6. Залежності $q(y)$ (а) та $q'(y)$ (б) при різних значеннях h: **1** – $h = 1$, **2** – $h = 0{,}5$, **3** – $h = 0{,}33$

Прибуток від внесення інвестицій визначається виразом

$$b(y) = 1 - i(y) - y = j(y) - y,$$

де $i(0) = 1$ - втрати при відсутності інвестицій, $j(y)$ - відносна кількість захищеної інформації. Оскільки $b'(y) = |i'(y)| - 1$, то ПЗІ визначає також продуктивність збільшення прибутку.

Ще один показник – рентабельність інвестицій

$$R(y) = \frac{b(y)}{y}.$$

Продуктивність цього показника:

$$R'(y) = \frac{b'(y)y - b(y)}{y^2}.$$

Висновки

Проведений аналіз висвітлює той факт, що в функції $f(x, y)$ переплелися два важливих поняття інформаційної безпеки – вразливість системи і продуктивність внесення ресурсів на її захист. Їх показники тісно пов'язані між собою. Перший з них визначається видом функціональної залежності – в степеневих функціях, в основному, значенням n, яке характеризує ступінь нелінійності. При заданому значенні n другий показник – коефіцієнт c, який впливає на кривизну залежності, не міняючи суттєво її форми.

Значущість цих показників зростає в складних системах з великою кількістю об'єктів, котрі містять різні обсяги інформації, мають різні імовірності нападу і відрізняються вразливістю і продуктивністю витрат. Правильна оцінка значень n_k і c_k в таких системах може суттєво вплинути на прийняття рішення про розподіл ресурсів між об'єктами.

Слід відзначити, що, не дивлячись на формальні відмінності, прийнята модель дає результати, котрі якісно, а при певному виборі параметрів – кількісно співпадають з результатами Гордона-Лоеба, котрі знайшли емпіричне підтвердження [5].

Це дає підстави вважати, що одержані результати будуть корисними при проектуванні комплексних систем захисту інформації. Це ж торкається і значення h у виразі $q(y)$.

Показники n, c і h разом відображають властивості системи і кон'юнктуру ринку та, враховуючи (7), дозволяють визначити продуктивність витрат.

Література

[1] 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.

[2] 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, 2008, Hanover, USA.

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

[4] Кулініч Р.В., Левченко Є.Г. Продуктивність інвестицій в інформаційну безпеку // Захист інформації. – 2011. - №1. – С. 80-84.

[5] 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 621.396:004.621.3(045)

Левченко Е.Г., Прус Р.Б., Рабчун Д.И. Показатели производительности затрат на защиту информации

Аннотация. *Рассмотрены производительности затрат на защиту информации по уменьшению уязвимости системы и по уменьшению угрозы нападения. Проанализировано влияние показателей информационной системы на степень обеих производительностей.*

Ключевые слова**:** *информационная безопасность, уязвимость, производительность затрат.*

Levchenko E.G., Prus R.B., Rabchun D.I. Indicators of costs productivity of information security

Abstract. *Costs productivities of information security to reduce the vulnerability of the system and reduce the threat of attack are considered. Influence of information system indicators on measure of both productivities is analyzed.*

Keywords: *information security, vulnerability, costs productivity.*

Отримано *3 вересня 2012 року*, затверджено редколегією *7листопада 2012 року*
(рецензент д.т.н., професор В.П. Квасніков)