УДК 004.681

М.В. Демчишин, Є.Г. Левченко (НАУ)

ЕФЕКТИВНІСТЬ РОЗВІДКИ ПРИ ПРОТИСТОЯННІ ДВОХ СТОРІН В ІНФОРМАЦІЙНІЙ СФЕРІ

Вступ. Протистояння двох сторін в інформаційній сфері здійснюється в умовах невизначеності відносно дій протилежної сторони. В цій ситуації природно виникає питання про доцільність проведення розвідки. Для нападу розвідка може додати відомості про об'єми інформації на об'єктах і рівень їх природної і технічної захищеності (проведення розвідки зафіксовано, зокрема, в хакерських атаках). Захист проводить контррозвідку з метою визначення розміру ресурсів нападу і їх націленості на окремі об'єкти. Кожна сторона прагне передбачити дії суперника. З цих міркувань, ставлячи за мету розробку оптимальної стратегії захисту, будемо розглядати дії нападу.

Постановка задачі. Пошук оптимального рішення приводить до необхідності визначення таких величин:

1) загальної кількості ресурсів нападу X, яка забезпечує досягнення необхідного значення однієї або кількох заданих величин – кількості вилученої інформації, прибутку від вилучення, рентабельності витрат, тощо.

2) розподілу ресурсів між об'єктами $\{x_k\}$, (k – номер об'єкта) з врахуванням кількості інформації на кожному з них, їх природної і технічної захищеності.

Першим кроком на шляху розробки оптимальної стратегії є вирішення питання про доцільність проведення розвідки при заданій кількості ресурсів і властивостях об'єктів та визначення оптимального співвідношення між кількістю ресурсів, які виділяються на розвідку і на витік інформації. Це і є метою дослідження.

Методика розрахунку і результати. Питання про ефективність розвідки розглядалось в [1], проте постановка задачі і прийняті допущення значно ускладнюють використання одержаних результатів (зокрема, це стосується прийнятої моделі Гросса).

Ми використаємо іншу модель [2]. Цільову функцію, яка визначає кількість вилученої інформації, представимо у вигляді:

$$I(\tilde{x}) = \sum_{k=1}^{l} g_k \cdot p_k \cdot q_k(\tilde{x}) \cdot f_k(\tilde{x}), \quad (1)$$

де $\tilde{x} = x/y$ – відносна величина, яка характеризує співвідношення ресурсів нападу і захисту – x і ,відповідно, y;

g_k – відносна кількість інформації на k-му об'єкті;

p_k – імовірність нападу на k-й об'єкт;

$q_k(\tilde{x})$ – імовірність виділення нападом ресурсів x на k-ий об'єкт;

$f_k(\tilde{x})$ – залежність частки вилученої інформації від ресурсів x та y.

Розглянемо спрощений варіант, коли система складається з двох об'єктів, причому $p_k = 1; g_1 = g_2 = g/2 = \frac{1}{2}$; $q_k(\tilde{x}) = q = 1/3$. Останнє значення знаходимо з умови $\int_0^{\tilde{x}_{гр}} q(\tilde{x})d\tilde{x} = 1$, де $\tilde{x}_{гр} = 3$ – границя інтервалу можливих, на наш погляд, значень $\tilde{x}$.

Відносна кількість вилученої інформації $i(\tilde{x}) = \frac{I(\tilde{x})}{g}$ з двох об'єктів становить:

$$i(\tilde{x}) = \frac{1}{2} \cdot \frac{1}{3}\left(f_1(\tilde{x}) + f_2(\tilde{x})\right). \quad (2)$$

В [2] зазначено, що залежності $f(x)$ можна описати двома типами функцій – степеневою $f(\tilde{x}) = \frac{a\tilde{x}^n}{\tilde{x}^n + c}$ і показниковою $f(\tilde{x}) = 1 - e^{-m\tilde{x}^n}$, де сталі a, c, n, m визначають положення і нахил кривих. Враховуючи, що при певному виборі параметрів ці залежності можуть стати досить близькими, обмежимось в подальшому розгляді функціями першого типу.

На рис. 1-10 приведені результати розрахунків, виконаних з використанням пакету Optimization Toolbox програмного комплексу Matlab при різних видах функцій $f(\tilde{x})$ та різних значеннях кількості ресурсів нападу $X = X^{(1)} + X^{(2)}$, де $X^{(1)}$ і $X^{(2)}$ – ресурси, направлені на розвідку і, відповідно, на вилучення інформації. В подальших розрахунках і на рисунках прийнято загальний ресурс захисту $Y = 0{,}05$ рівномірно розподілений між об'єктами: $y_1 = y_2 = 0{,}025$. На лівих частинах рисунків приведені залежності $i(\tilde{x})$ та їх похідні для кожного з двох об'єктів, які описуються степеневими функціями $f(\tilde{x}) = \frac{\tilde{x}^n}{\tilde{x}^n + c}$ в різних інтервалах зміни загальної кількості ресурсів x – від 0 до 0,05, що відповідає максимальному відношенню $\frac{x_{\max}}{y} = \frac{0{,}05}{0{,}025} = 2$, і від 0 до 0,2 ($\frac{x_{\max}}{y} = \frac{0{,}2}{0{,}025} = 8$). Підкреслимо, що в області $x \gtrsim 0$ ці функції мають різний характер: при $n = 1$ опуклість функції $f(\tilde{x})$ направлена вгору, а при $n > 1$ – вниз, що відображає різну вразливість об'єктів в початковій області і дозволяє виявити вплив цього фактору. Вибір параметрів a, c в наших розрахунках не має принципового значення і обумовлений бажанням найбільш яскраво відобразити описані нижче закономірності.

На правих частинах рисунків – втрати інформації з обох об'єктів під час розвідки, під час нападу і сумарні. По осі абсцис відкладені ресурси, вкладені в кожний об'єкт під час розвідки. Ми вважаємо, що протистояння здійснюється в умовах повної невизначеності і ресурси, виділені на розвідку, діляться між об'єктами порівну: $x_1^{(1)} = x_2^{(1)} = x^{(1)}$, загальний ресурс розвідки $X^{(1)} = x_1^{(1)} + x_2^{(1)} = 2x^{(1)}$, залишок ресурсів після розвідки використовується на напад. Максимальні значення на осі абсцис правих рисунків вдвічі менші, ніж на лівих (ці значення відображають той крайній випадок, коли всі ресурси вкладають порівну між об'єктами). Точки $x = 0$ на правих рисунках відповідають іншій граничній ситуації – всі ресурси вкладають в один з об'єктів. Квадратики на кривих – екстремальні значення залежностей.

Наші дослідження направленні на виявлення ролі двох основних факторів, які впливають на ефективність розвідки:

1) вразливості кожного з об'єктів, яка виражається залежністю $f_k(\tilde{x})$;

2) загального розміру X ресурсів нападу.

Кінцевою метою є визначення доцільності проведення розвідки в кожній конкретній ситуації і у випадку позитивного рішення цього питання – визначення оптимального співвідношення $X^{(1)}/X^{(2)}$ ресурсів, виділених на розвідку і на вилучення інформації, а також оптимального розподілу ресурсів між об'єктами. Критерієм оптимуму є досягнення максимальної кількості вилученої інформації $i(\tilde{x})$.

Застосування цього критерію в умовах невизначеності потребує деяких зауважень.

1. Вважаємо, що після проведення розвідки напад робить правильний вибір об'єкта, на котрий слід направляти весь залишок ресурсів, і кількість вилученої інформації визначається на кожній дільниці верхньою з двох кривих, які зображають сумарний витік.

2. Єдиною точкою, де існує повна визначеність відносно кінцевого результату є точка $X^{(1)} = X^{(1)}_{\max}$ (на рис.1б це $x^{(1)} = 0{,}025$), в якій два етапи (розвідка і вилучення) зливаються в один, тобто фактично розвідка не проводиться, а всі ресурси направляються порівну на об'єкти. Значення $i_{\Pi}(\tilde{x})$ в цій точці і буде орієнтиром при вирішенні питання про доцільність проведення розвідки.

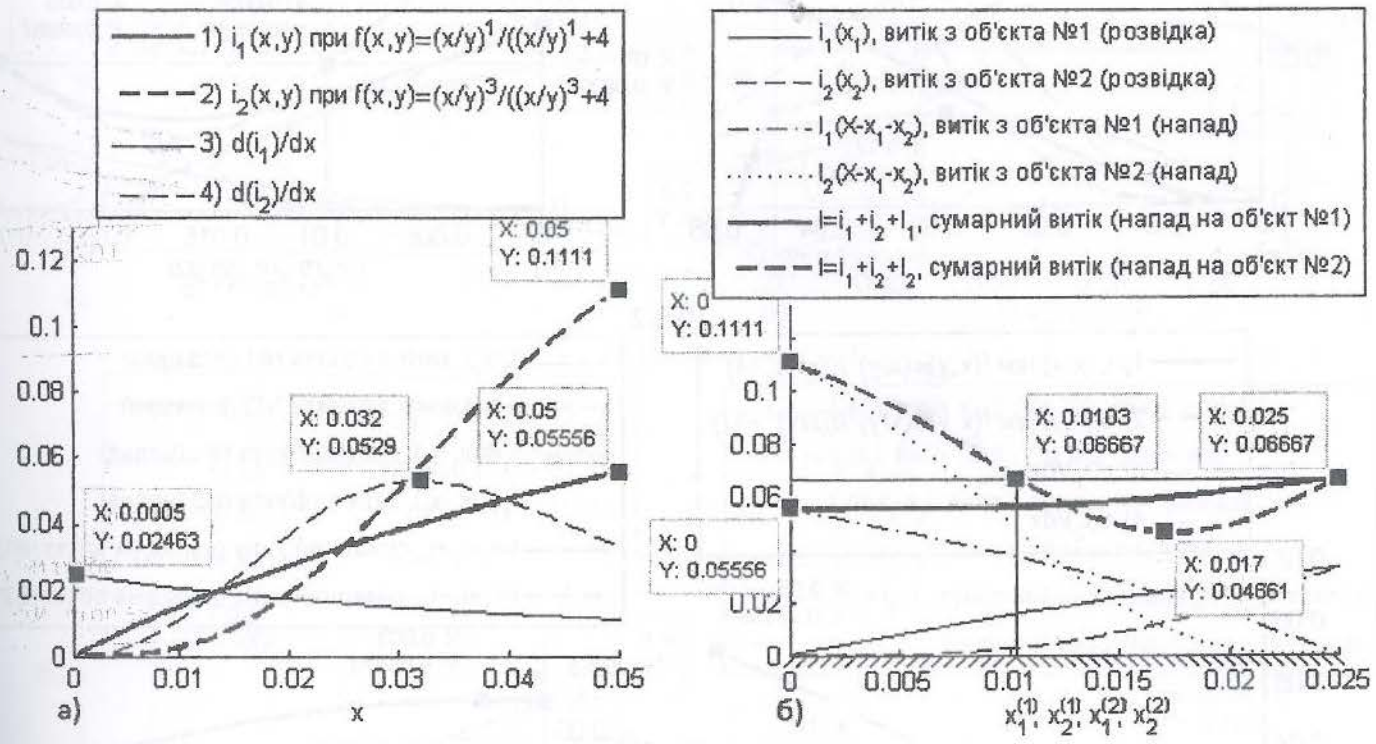

Рис.1

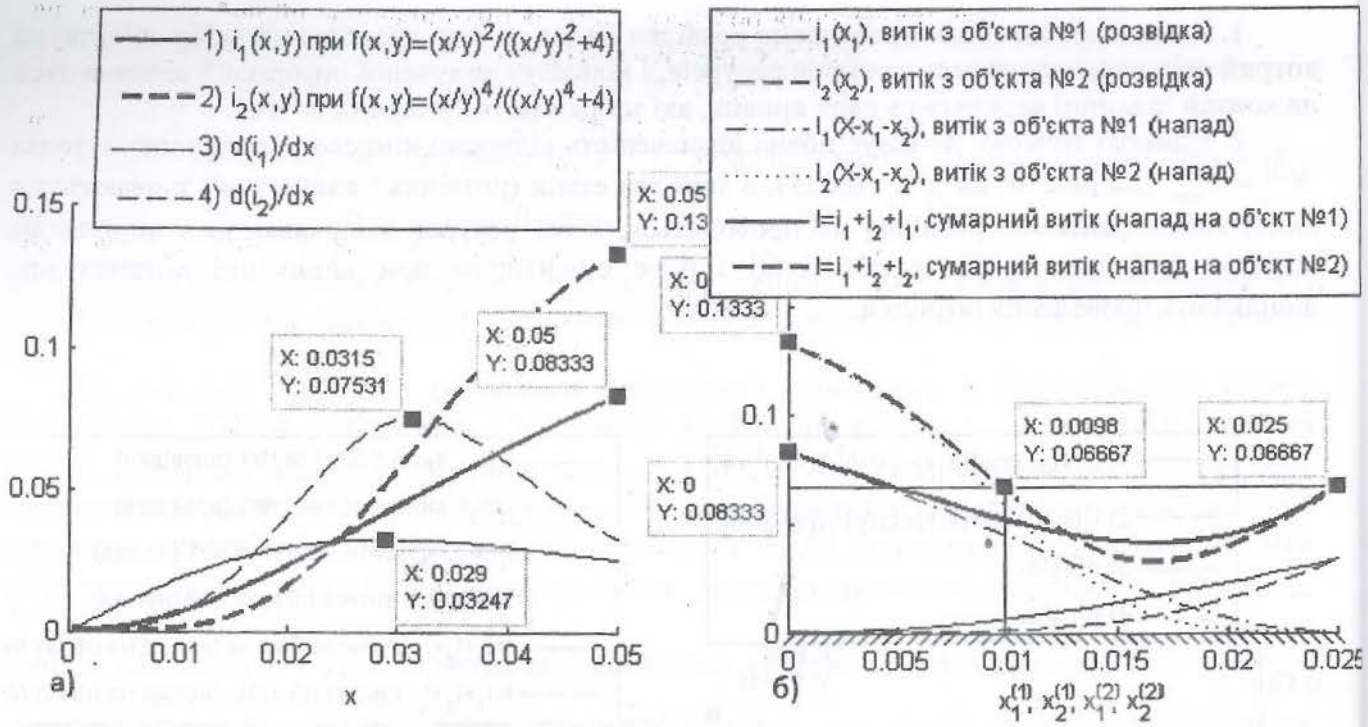

Рис.2

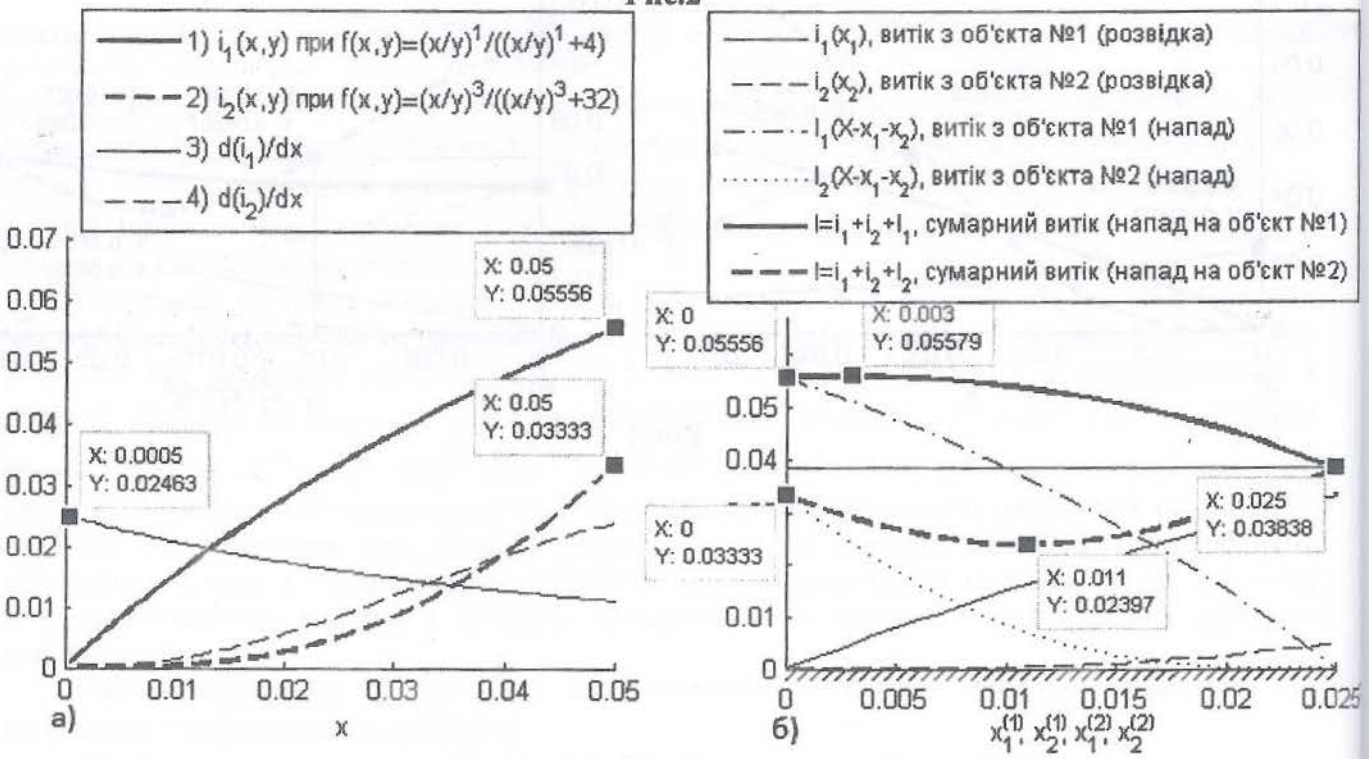

Рис.3

З врахуванням приведених міркувань на рисунках вся шкала x поділена на дві дільниці: перша (позначається лівосторонньою штриховкою) – це зона, в якій розвідка доцільна (штрихова жирна лінія на рис.1а лежить вище горизонтальної лінії, проведеної на рівні $x_{\Pi} = 0{,}06667$) і друга, в якій розвідка недоцільна (правостороння штриховка). На рис.1,2 зона доцільності розташована в лівій частині інтервалу зміни x, на рис.4 – всередині, на рис.5 – в правій частині, на рис.3 вона займає всю шкалу, а на рис.6 – взагалі відсутня.

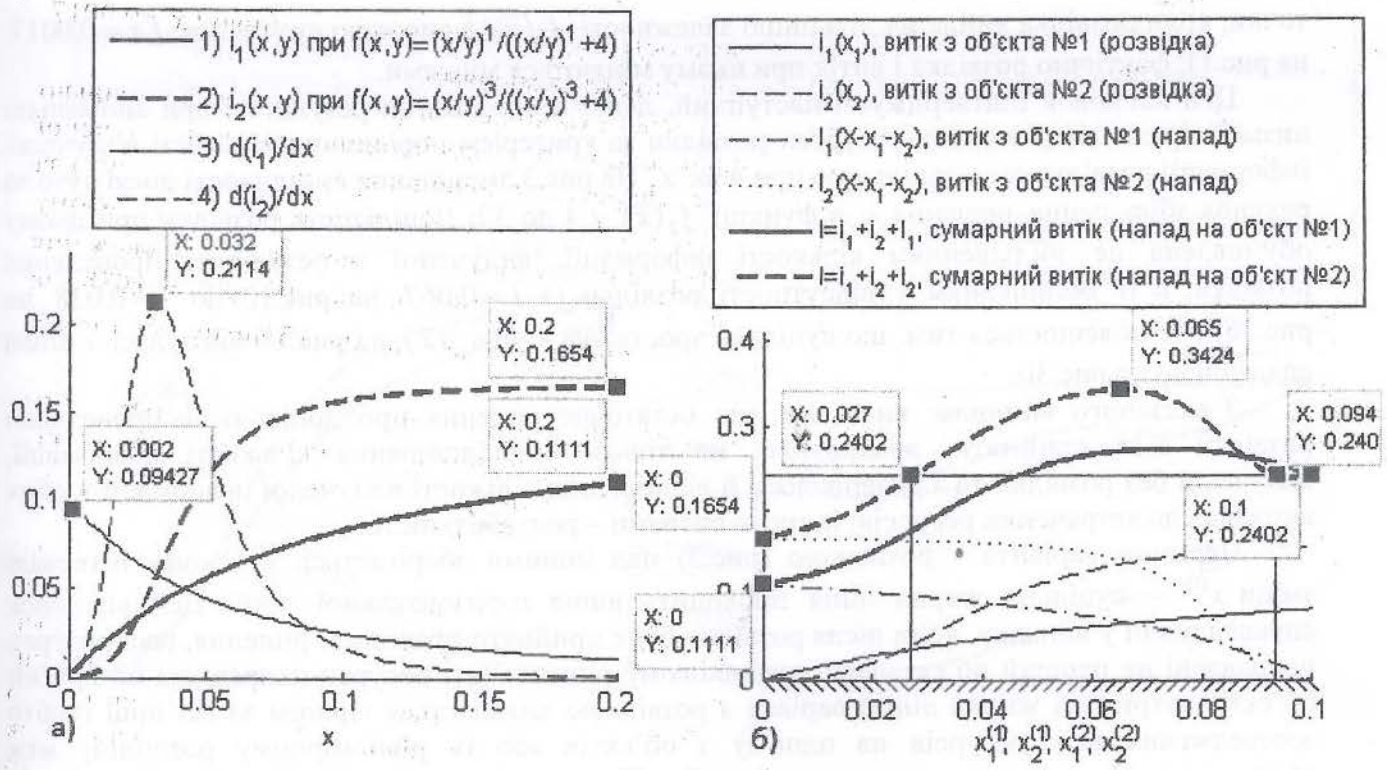

Рис.4

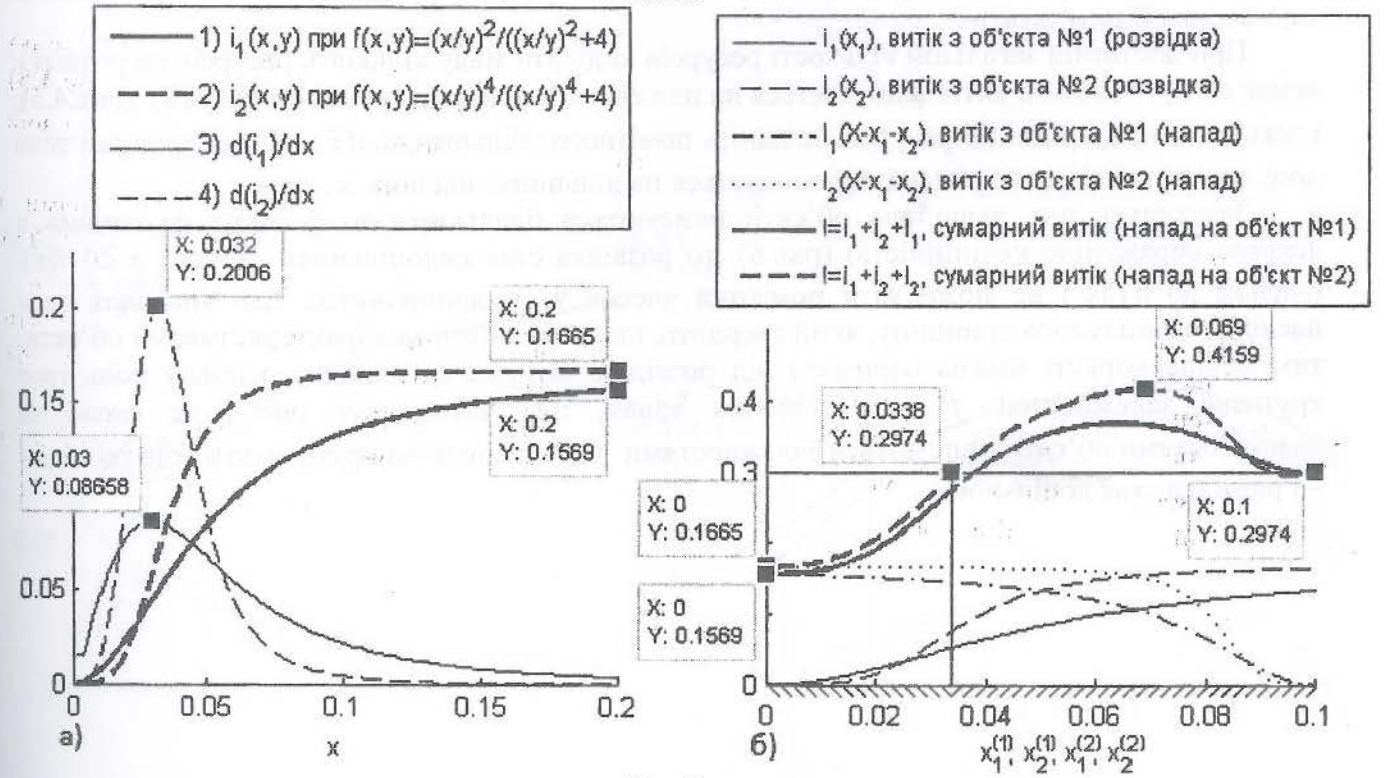

Рис.5

Одержані результати можна пояснити наступним чином.

Якщо розвідка проводиться в зоні низької динамічної вразливості (при $y \gtrsim 0$), то збільшення ресурсів розвідки не приносить бажаного результату, оскільки збільшення кількості вилученої інформації під час розвідки не може компенсувати її зменшення під час витоку (крутизна кривої $f_2(\tilde{x})$ на рис.1,2 в зоні витоку при значних x значно більша, ніж в зоні розвідки при $x \gtrsim 0$). В результаті сумарний витік зі зростанням x зменшується – аж до

точки, коли розвідка вийде на ділянку залежності $f_2(\tilde{x})$ з високою крутизною ($x = 0{,}0017$ на рис.1); фактично розвідка і витік при цьому міняються місцями.

Цей висновок підтверджує і наступний, дещо несподіваний результат: при аномально низькій вразливості і малих ресурсах розвідки за критерієм порівняння кількості вилученої інформації розвідка стає доцільною при всіх x. На рис.3 зменшення вразливості досягнуто за рахунок збільшення значення c в функції $f_2(\tilde{x})$ з 4 до 32. Доцільність розвідки при цьому обумовлена не збільшенням кількості інформації, вилученої в результаті проведення розвідки, а її зменшенням у відсутності розвідки (з $i = 0{,}067$ на рис.1б до $i = 0{,}038$ на рис.3б). Це пояснюється тим, що суцільна зростаюча крива $i(\tilde{x})$ на рис.1б вигнулась і стала спадаючою на рис.3б.

З сказаного випливає висновок, що остаточне рішення про доцільність проведення розвідки слід приймати, враховуючи не тільки співвідношення кількості інформації, вилученої без розвідки та з розвідкою, а й відношення кількості вилученої інформації в обох випадках до затрачених ресурсів, іншими словами – рентабельність.

Перевага варіанта з розвідкою (рис.3) над іншими зберігається у всьому інтервалі зміни $x^{(1)}$ – суцільна жирна лінія проходить вище горизонтальної лінії. Цей висновок справедливий у випадку, коли після розвідки буде прийнято правильне рішення, і всі ресурси направлені на перший об'єкт. При помилковому рішенні (всі ресурси направлені на другий об'єкт – штрихова жирна лінія) варіант з розвідкою виявляється гіршим за всі інші (тобто зосередження всіх ресурсів на одному з об'єктів або їх рівномірному розподілу між об'єктами). Це свідчить про важливість як проведення розвідки, так і правильного тлумачення її результатів.

При достатній загальній кількості ресурсів виділяти малу кількість ресурсів на розвідку немає сенсу, оскільки витік відбувається на положистій дільниці залежностей $f(\tilde{x})$ (рис.4,5), і зекономлені на розвідці ресурси не дають помітного збільшення $i(\tilde{x})$. З цієї причини зона доцільності розвідки на рис.4,5 переміщується на дільницю значних x.

Зазначимо, що, якщо два об'єкти описуються близькими зо формою функціями з яскраво вираженою нелінійністю (рис.6), то розвідка стає недоцільною – в зоні $x \gtrsim 0$ $i(x)$ близька до нуля і не може дати помітний внесок у сумарний витік. Цей висновок не є наслідком загального принципу, який твердить, що чим ближчі за характеристиками об'єкти, тим менше користі можна отримати від розвідки. В нашому випадку основну роль грає крутизна залежностей $f(\tilde{x})$ в робочих зонах. Це підтверджує рис.7, де схожі за властивостями об'єкти описуються залежностями $f(\tilde{x})$ з високою крутизною в зоні розвідки – і розвідка стає доцільною.

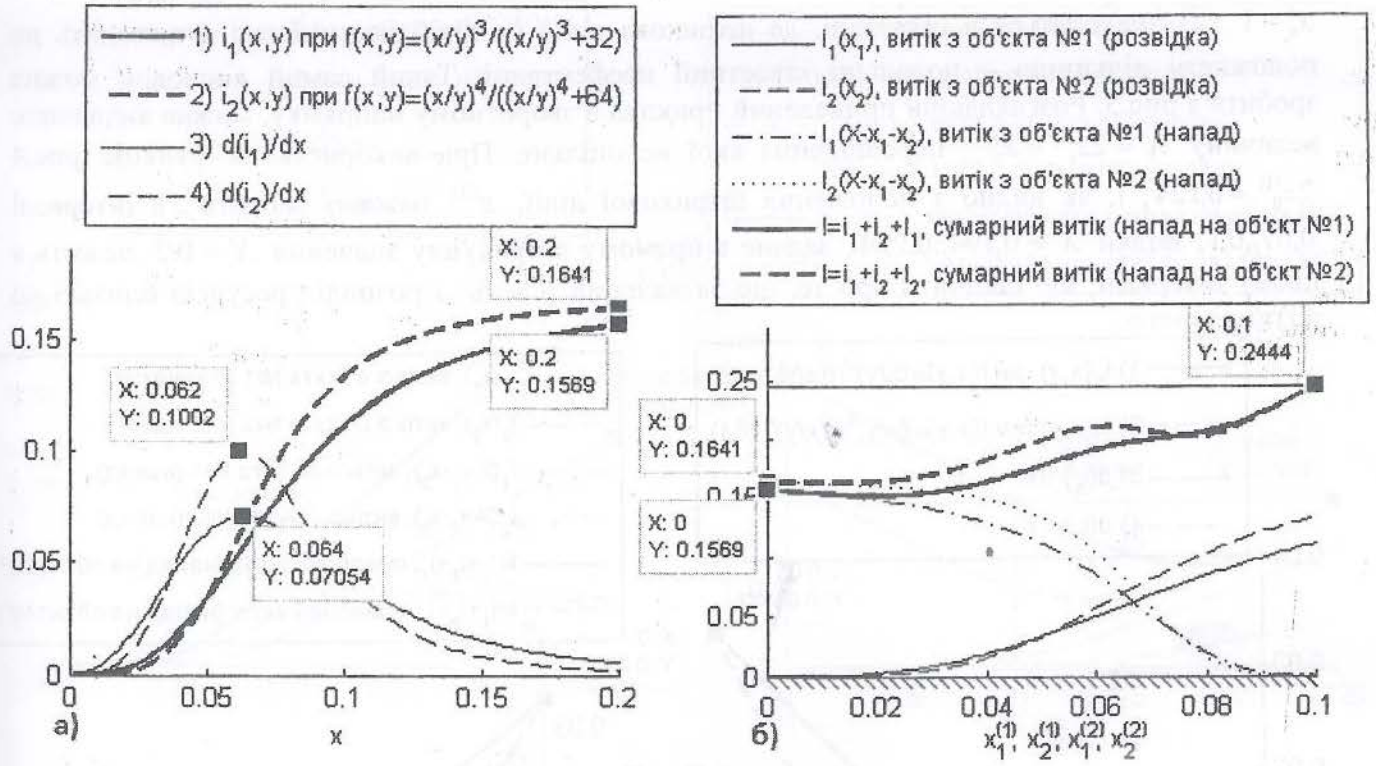

Рис.6

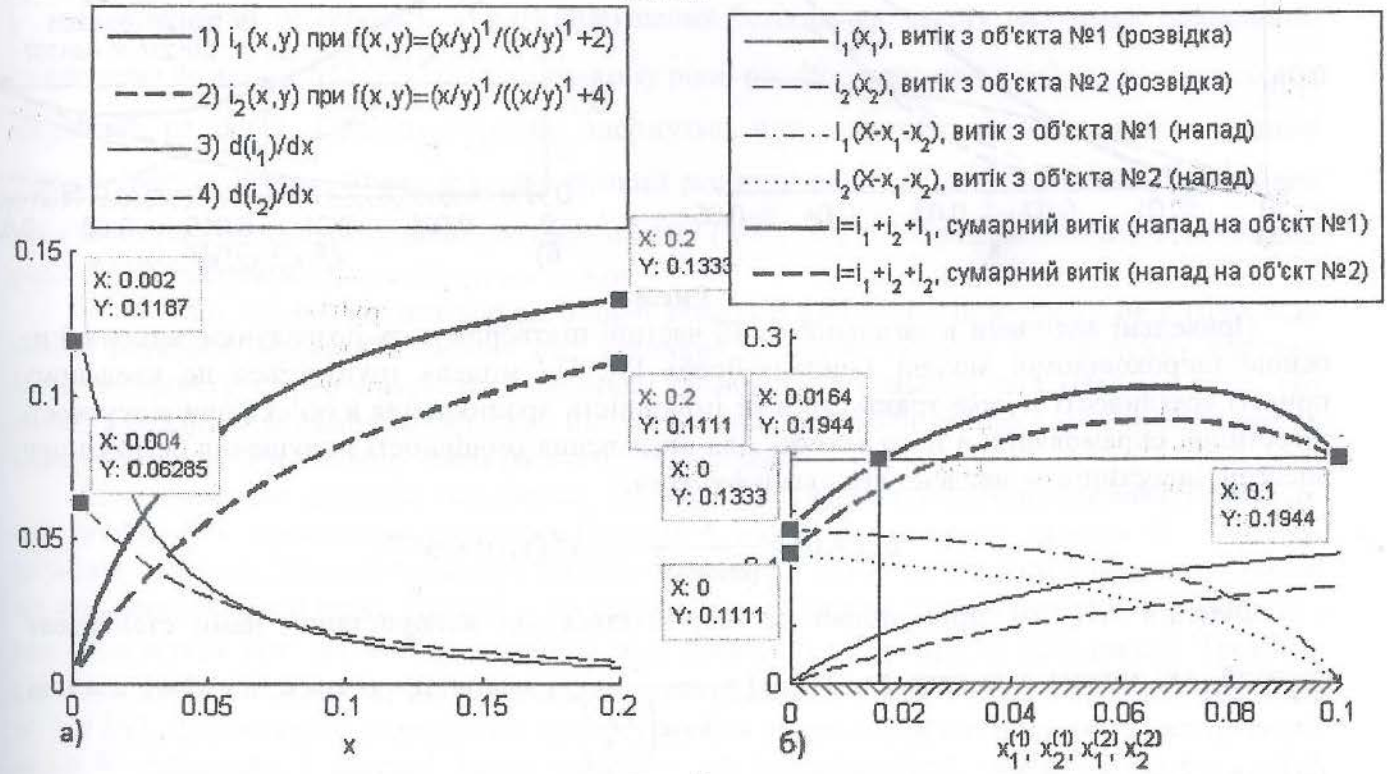

Рис.7

Оптимальні значення ресурсів, які необхідно виділяти на розвідку – $x_0^{(1)}$ і на витік інформації – $x_0^{(2)}$, досягаються в інтервалі значень x, де зростання функції $f(\tilde{x})$ уповільнюється (похідна $f'(\tilde{x})$ зменшується і згодом прямує до нуля). На рис.4 максимальне значення $i_{2\max}(\tilde{x}) = 0{,}3424$ для залежності $f_2(\tilde{x})$ (штрихова лінія) досягається при $x_0^{(1)} = 0{,}065$, що визначає величину $x_0^{(2)} = X - 2x_0^{(1)} = 0{,}2 - 0{,}124 = 0{,}076$. Ці обидва значення

$x_0^{(1)}$ і $x_0^{(2)}$ знаходяться в інтервалі, де штрихова лінія на лівій частині рис. 4 виходить на положисту дільницю – подальші інвестиції неефективні. Такий самий висновок можна зробити з рис.5. Розглядаючи приведений приклад в зворотному напрямку, можна визначити величину $X = 2x_1^{(1)} + x_0^{(2)}$, перевищення якої недоцільне. При використання функцій рис.4 $2x_0^{(1)} = 0{,}124$, і, як видно з положення штрихової лінії, $x^{(2)}$ бажано вибрати в інтервалі 0,07..0,1, звідки $X = 0{,}194..0{,}224$. Задане в прямому розрахунку значення $X = 0{,}2$ лежить в цьому інтервалі, що свідчить про те, що зазначений рівень і розподіл ресурсів близькі до оптимального.

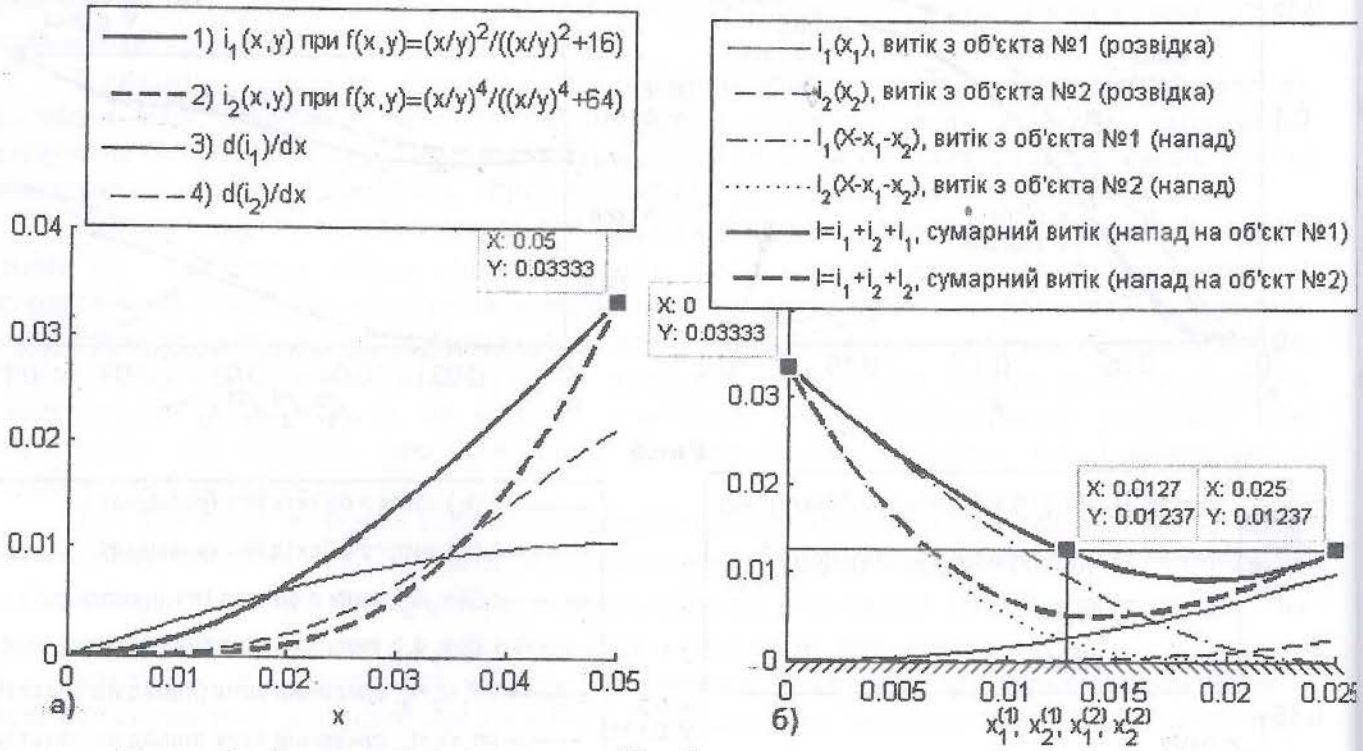

Рис.8

Приведені висновки в загальній своїй частині підтверджують розрахунки, виконані на основі широковідомої моделі Гордона-Лоеба [3]. Ця модель ґрунтується на введеному понятті вразливості υ, яка трактується як імовірність проникнення в об'єкт при відсутності інвестицій, спрямованих в його захист. Для визначення імовірності порушення безпеки при внесенні інвестицій y введено два класи функцій:

$$S^{I}(y,\upsilon) = \frac{\upsilon}{(\alpha y + 1)^{\beta}} \text{ та } S^{II}(y,\upsilon) = \upsilon^{\alpha y + 1}.$$

Функція $S^{I}(y,\upsilon)$ принципово не відрізняється від використаних нами степеневих функцій, які можна записати як $f(x,y) = \dfrac{a}{1 + c\left(y/x\right)^{n}}$, а при $a = \upsilon, c = \alpha, n = \beta = 1, x = 1$ ці функції повністю співпадають.

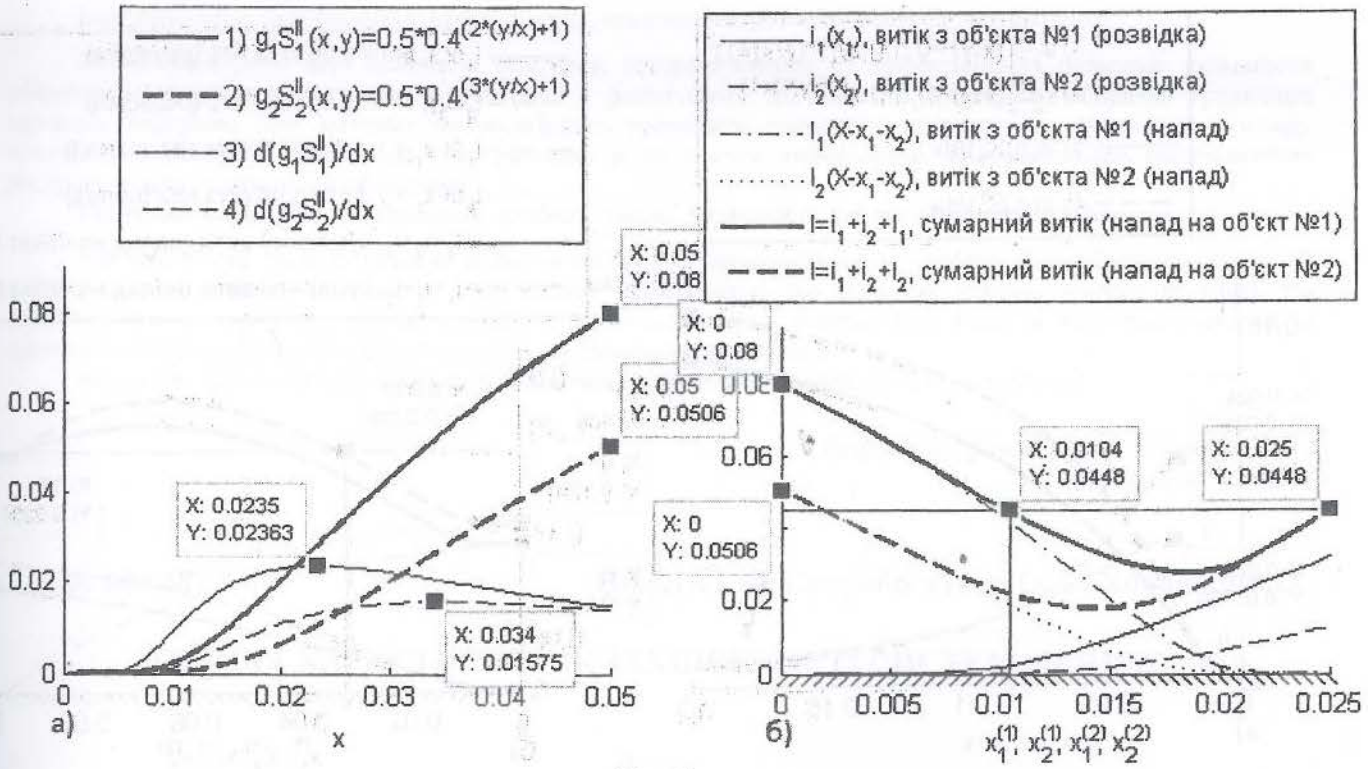

Рис.9

Розглядаючи імовірність $S(y,\upsilon)$ порушення безпеки як частку вилученої інформації, розрахуємо функцію $S^{II}(y/x,\upsilon)$ при низькому рівні ресурсів нападу ($x = 0..0{,}05$). Результати зображені на рис.9. Подібну картину одержуємо при використанні степеневих функцій $f(x,y)$ (рис.2). На рис.10 використані функції різних класів – $S^{I}(y/x,\upsilon)$ та $S^{II}(y/x,\upsilon)$, для двох об'єктів при високому рівні ресурсів нападу ($x = 0..0{,}2$). Зображені залежності схожі на рис.4-5 і підтверджують приведені висновки.

Зазначимо, що одержання максимальної кількості вилученої інформації не є головною метою розвідки. Проте збільшення цієї величини дозволяє скласти більш повну картину системи захисту і тому покращує показники розвідки. При цьому слід мати на увазі, що низькі значення вилучення інформації під час розвідки не обов'язково спричиняють такі ж низькі величини під час вилучення (може бути навпаки).

Відзначимо ще декілька показників, які необхідно враховувати при прийнятті рішення про доцільність проведення розвідки. Перший з них – це інтервал значень x, в якому розвідка доцільна. Збільшення цього інтервалу зменшує ризик непродуктивних витрат, коли ми виходимо за його межі. Другий – це ступінь перевищення оптимального значення $i(\tilde{x})$, яке досягається при проведенні розвідки над значенням $i(\tilde{x})$ при її відсутності. Третій – ступінь близькості кривих, які зображають сумарний витік при нападі на об'єкт №1 і на об'єкт №2. Два останніх відношення характеризують рівень стійкості прийнятої методики до зміни її складових. І нарешті такий показник, як рентабельність загальних витрат, котрі можуть вирости внаслідок потреб на розвідку.

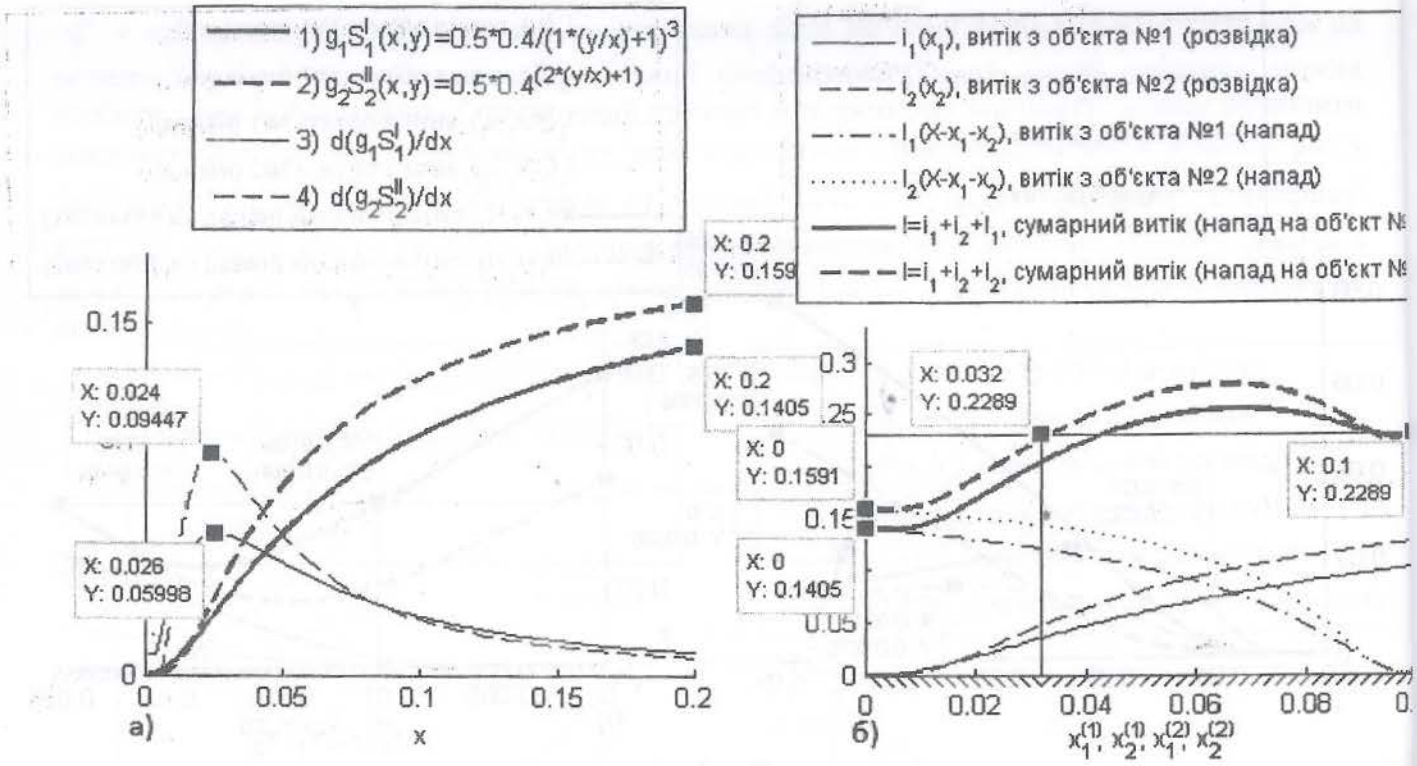

Рис.10

Відзначимо ще одну деталь, яку необхідно враховувати при проведенні розвідки: одна точка $f(\tilde{x})$, яку ми одержуємо в результаті розвідки не дає можливості передбачити форму всієї залежності. Для цього необхідно мати принаймні дві точки. Друга спроба може дати ще й побічний позитивний ефект: розподіл ресурсів на декілька спроб може пересунути робочу точку на дільницю залежності $f(\tilde{x})$ з великою крутизною, що збільшує сумарний результат. Ця можливість обумовлена тим, що зі зростанням x $f(\tilde{x})$ зменшує свою крутизну, що є відбитком відомого економічного закону про зменшення граничної норми прибутку.

Висновки. Як зазначено вище, оптимальні з точки зору одержання i_{max} значення ресурсів, які слід направляти на розвідку і на вилучення інформації, знаходяться на дільниці залежності $f(\tilde{x})$, де її зростання уповільнене, і $f'(\tilde{x})$ починає різко зменшуватись. Ця умова, з одного боку, підкреслює значення виду функції $f(\tilde{x})$, що характеризує динамічну вразливість об'єкта, з другого боку – ставить вимоги до необхідної кількості ресурсів нападу. При зміні одного з цих показників розвідка з недоцільної може переходити в доцільну і навпаки. Таким чином, питання про доцільність розвідки зводиться до одного з основних питань, які виникають при побудові математичної моделі – визначення складових і параметрів цільової функції, які в максимальній степені відповідають характеристикам реальних об'єктів. Це питання потребує свого дослідження та розв'язання.

Список використаних джерел

1. Рачко П. Эффективность разведки в задаче Гросса. В сб. "Исследование операций", под ред. Ю.Б. Гермейера. М.: Наука. – 1971. – №2. – С.58-71.

2. Левченко Є.Г., Рабчун А.О., Оптимізаційні задачі менеджменту інформаційної безпеки, НТЖ «Сучасний захист інформації», – 2010, – №1. – С.16-23.

3. 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.

Розглянуто роль двох основних факторів, які впливають на ефективність розвідки: вразливості об'єктів і кількості ресурсів нападу. В системах з різними значеннями вразливості визначені граничні значення ресурсів, при яких доцільно проводити розвідку, оптимальні співвідношення між кількістю ресурсів, виділених на розвідку і на витік інформації, і оптимальний розподіл ресурсів між окремими об'єктами.

Ключові слова: інформаційне протистояння, вразливість, розподіл ресурсів, оптимізація.

Рассмотрена роль двух основных факторов, которые влияют на эффективность разведки: уязвимости объектов и количества ресурсов. В системах с различными значениями уязвимости определи граничные значения ресурсов, при которых целесообразно проводить разведку, оптимальное соотношения между количеством ресурсов, выделяемых на разведку и на утечку информации, и оптимальное распределение ресурсов между отдельными объектами.

Ключевые слова: информационное противостояние, уязвимость, распределение, оптимизация.

The role of two basic factors that influence on reconnaissance efficiency – objects vulnerability and resources number – is considered. In systems with various vulnerabilities the resources extreme number at which the reconnaissance is expedient, optimal correlation between resources number that direct at reconnaissance and at extraction and optimal resources distribution among objects are determined.

Keywords: Information Confrontation, Vulnerability, Resources Distribution, Optimization.

Рецензент:д.т.н., проф Хорошко В.О..
Надійшла:11.01.2011

УДК 004.681.5

Пискун І.В., Скоробогатько О.А., Хорошко В.О.

ОЦІНКА ХАРАКТЕРИСТИК ЗАХИЩЕНОСТІ СИСТЕМ ЗВ'ЯЗКУ

Вступ

Сучасне суспільство не може існувати без інформації. А наявність інформації потребує її захисту. Тому основними задачами забезпечення інформаційної безпеки є:

- виявлення, оцінка та прогнозування джерел загроз інформаційній безпеці;
- розробка державної політики забезпечення інформаційної безпеки та комплексу заходів і механізмів її реалізації;
- створення нормативно-правових засад забезпечення інформаційної безпеки;
- розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання загрозам інформаційній безпеці та ліквідації наслідків її порушення.

Основна частина

При розробці систем зв'язку, які забезпечують інформацією різні системи, слід визначити функціональні вимоги до захисту інформації в ній, вимоги щодо гарантування безпеки інформації. При вирішені цих задач дуже важливою є розробка методології оцінки рівня захищеності системи зв'язку з використанням існуючих вимог стандартизації.

Створення та використання за призначенням систем зв'язку(СЗ) передбачає реалізацію ряду організаційних, математичних та інженерних методів забезпечення необхідною рівня безпеки інформації.[1].

СЗ може мати **m** вразливостей, кожна з яких характеризується певною ймовірністю існування $P_{враз/i}$, **i** $\in$ **m**. Реалізація заходів захисту інформації(ЗІ) дозволяє зменшити цю ймовірність до значення:

$$P_{враз\ i}^{(1)}:P_{враз\ i}^{(1)}=P_{враз\ i}(1-P_{зах\ i}), \quad (1)$$

де $P_{зах\ i}$ – імовірність реалізації заходу щодо ЗІ щодо імовірнісної вразливості.

Ризик отримати певні наслідки від впливу імовірнісної загрози на частково захищену систему становить (рис. 1)