УДК 004.681

ОПТИМІЗАЦІЯ РОЗПОДІЛУ РЕСУРСІВ ПРИ ПРОВЕДЕННІ РОЗВІДКИ В ІНФОРМАЦІЙНОМУ ПРОТИСТОЯННІ

М.В. ДЕМЧИШИН, Є.Г. ЛЕВЧЕНКО

Конкурентна боротьба в інформаційній сфері характеризується тим, що кожна зі сторін прагне захистити свою інформацію і здобути інформацію про суперника. В умовах невизначеності, коли дії суперника невідомі й не можуть бути передбачені точно, важливу роль відіграє розвідка, котра може дати відомості про важливість інформації, її розподіл між об'єктами, вразливості та ступені захищеності цих об'єктів. На основі створеної математичної моделі розроблена методика визначення доцільності проведення розвідки в залежності від вразливості об'єктів і кількості ресурсів. Встановлено принципи розподілу ресурсів, які забезпечують максимальну ефективність розвідки. Наведено приклади розрахунків у системі із двох об'єктів із різними вразливостями. Розраховані інтервали значень ресурсів, в яких розвідка доцільна, за різних форм функцій вразливості. Наведено рекомендації по оптимальному розподілу ресурсів на розвідку і на здобуття інформації в залежності від вразливості об'єктів та загальної кількості ресурсів.

ВСТУП

Моделювання протистояння двох сторін в інформаційній сфері має багато спільного з моделюванням військового протистояння. Зокрема це стосується розвідки, яка в умовах невизначеності щодо дій суперника може надати важливі відомості, які сприятимуть прийняттю оптимального рішення. З точки зору захисту це відомості про направленість атак суперника, виділену ним кількість ресурсів нападу, їх розподіл між об'єктами. Мета нападу — одержання відомостей про кількість інформації на кожному з об'єктів, ступінь її захищеності, який залежить від виділених ресурсів захисту і їх розподілу.

Мета роботи — розробка методики пошуку рішень нападу, яка дала б можливість передбачити його дії при побудові оптимальної системи захисту.

МЕТОДИКА РОЗРАХУНКІВ

Цільову функцію, яка визначає кількість вилученої інформації, представимо у вигляді [1]:

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

де x та y — ресурси нападу і, відповідно, захисту; $k=\overline{1,l}$ — номер об'єкта; g_k — відносна кількість інформації на k-му об'єкті; p_k — імовірність нападу на k-й об'єкт; $q_k(x,y)$ — імовірність виділення нападом та захистом

ресурсів x та y, відповідно, на k-й об'єкт; $f_k(x,y)$ — залежність частки вилученої інформації від ресурсів x та y.

Розглянемо спрощений варіант, коли система складається з двох об'єктів, причому $p_k = 1$; $g_1 = g_2 = g/2 = \frac{1}{2}$. Покладемо $y = 1$, $q_k(x,y) = \text{const} = \frac{1}{3}$. Останнє значення знаходимо з умови $\int_0^{x_{\text{гр}}} q(x)dx = 1$, де $x_{\text{гр}} = 3$ — границя можливих, із точки зору нашої експертної оцінки, значень x. Спрощена форма цільової функції, яка визначає відносну кількість вилученої інформації має вигляд:

$$i(x,y) = \frac{1}{2} \cdot \frac{1}{3}\left[f_1(x,y) + f_2(x,y)\right]. \tag{2}$$

В [1] запропоновано два поширених класи функцій, які можуть описувати реальні ситуації: степеневі та показникові. Враховуючи, що криві, які зображують ці залежності, принципово не відрізняються, обмежимось розглядом степеневих функцій $f(x,y) = \frac{a(x/y)^n}{(x/y)^n + c}$ та в (2) будемо використовувати такі форми:

$$f(x,y) = \frac{(x/y)}{(x/y)+4}, \tag{3}$$

$$f(x,y) = \frac{a(x/y)^2}{(x/y)^2 + 16}, \tag{4}$$

$$f(x,y) = \frac{a(x/y)^3}{(x/y)^3 + 32}, \tag{5}$$

$$f(x,y) = \frac{a(x/y)^4}{(x/y)^4 + 64}. \tag{6}$$

Залежності $f(x,y)$ на двох об'єктах можуть виражатись різними парами з набору (3)–(6). Зазначимо, що n в цих виразах впливає, в основному, на кривизну залежності, а c — на її положення відносно осі абсцис. Зокрема, при $n = 1$ опуклість кривої $f(x,y)$ в області $(x/y) \gtrsim 0$ направлена вгору, а при $n > 1$ — вниз.

Доцільність проведення розвідки і корисність одержаних від неї результатів залежить від двох основних факторів:

- вразливості об'єктів;
- кількості виділених на розвідку ресурсів.

Вразливість будемо поділяти на статичну і динамічну. Статична, або початкова вразливість визначається рівнем природної й технічної захищеност-

ті у відсутності додаткових ресурсів захисту, тобто при $y = 0$. Динамічна вразливість залежить від співвідношення x та y та виражається функціями $f(x, y)$. При використанні степеневих функцій та $y \to 0$ маємо $f(x, y) \to$ $\to a$, що виражає статичну вразливість.

Показники розподілу ресурсів, які підлягають оптимізації, можна поділити на три групи:

- загальна кількість ресурсів X;
- кількість ресурсів, виділених на розвідку — $X^{(1)}$ й на витік — $X^{(2)}$, де $X^{(1)} + X^{(2)} = X$;
- розподіл ресурсів між об'єктами: $x_1^{(1)} / x_2^{(1)}$, $x_1^{(2)} / x_2^{(2)}$, $x_1{}^{(1)} + x_2{}^{(1)} =$ $= X^{(1)}$, $x_1{}^{(2)} + x_2{}^{(2)} = X^{(2)}$.

РЕЗУЛЬТАТИ РОЗРАХУНКІВ

На рис. 1–6 наведено результати розрахунків, виконаних з використанням пакету Optimization Toolbox програмного комплексу Matlab. На лівих частинах рисунків зображені залежності $i(x, y)$, які розраховано на базі функцій (3)–(6) та їх похідні. На правих — втрати інформації з двох об'єктів під час розвідки, під час витоку і сумарні. По осі абсцис на лівих частинах відкладено загальні ресурси, на правих — ресурси, виділені на кожний об'єкт під час розвідки. Вважаючи, що протистояння здійснюється в умовах повної невизначеності, ресурси розвідки поділяємо між об'єктами порівну: $x_1^{(1)} = x_2^{(1)}$, тому максимальні значення на осі абсцис правих рисунків вдвічі менші, ніж на лівих.

Метою нападу є визначення розподілу ресурсів, який забезпечує досягнення оптимальних значень обраних показників ефективності. В нашому розгляді таким показником є сумарна кількість вилученої інформації $I(x, y)$ під час розвідки і під час витоку. Першим кроком є визначення доцільності проведення розвідки, яка встановлюється в результаті порівняння значень $I(x, y)$ із застосуванням розвідки та без неї. Означення цих величин потребує деякого уточнення.

- Вважатимемо, що після проведення розвідки напад робить правильний вибір об'єкта, на котрий направляється залишок ресурсів $x_2 = X - x_1$, й кількість вилученої інформації на кожному інтервалі Δx визначається верхньою з двох кривих, які зображають сумарний витік.
- Кількість $i(x, y)$ при відсутності розвідки будемо визначати при двох варіантах розподілу ресурсів:

– усі ресурси діляться порівну між об'єктами — це крайня права точка $x_1 = x_2 = x_{\Pi} = \dfrac{x}{2}$ (вона визначає положення суцільної горизонтальної лінії $i_{\Pi} = \text{const}$ на правих частинах рисунків); в цій точці вилучення інформації

відбувається в результаті одного етапу, в якому розвідка повністю переходить у витік;

– усі ресурси направляються на один із об'єктів (крайні ліві точки); невизначеність у виборі об'єкта може бути врахована шляхом усереднення $i(x,y)=\dfrac{i_1(x,y)+i_2(x,y)}{2}$ (штрихова горизонтальна лінія).

Будемо називати ці варіанти першим і другим критеріями порівняння.

Перша задача в розв'язанні поставленої проблеми — визначення впливу основних факторів (вразливості об'єктів $f(x,y)$ і кількості ресурсів X) на значення цільової функції. На рис. 1–6 наведено результати розрахунків у різних діапазонах Δx для двох варіантів комбінацій функцій $f(x,y)$: дробно-лінійної для першого об'єкта та дробно-нелінійної для другого (рис. 1–3) і двох дробно-нелінійних (рис. 4–6).

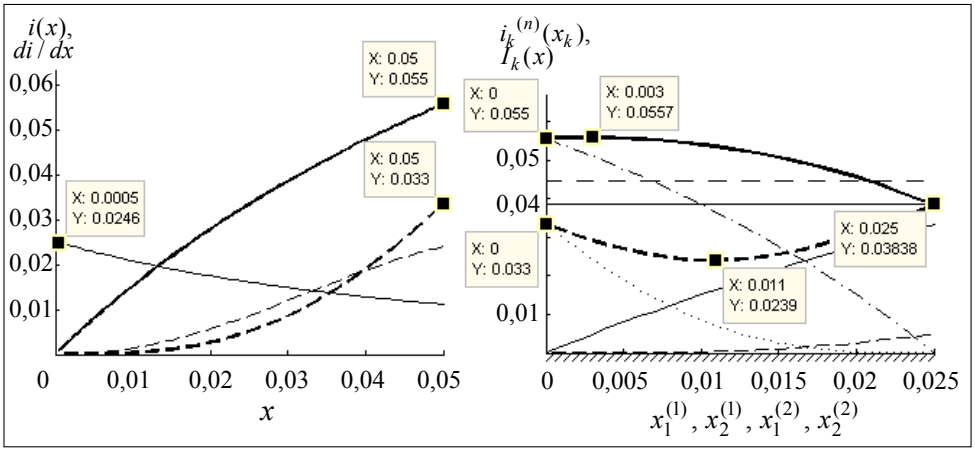

Рис. 1. Втрати інформації при використанні функцій вразливості $f_1(x,y)=\dfrac{x/y}{x/y+4}$, $f_2(x,y)=\dfrac{(x/y)^3}{(x/y)^3+32}$ та $Y=0{,}05$, $x_{\max}=0{,}05$

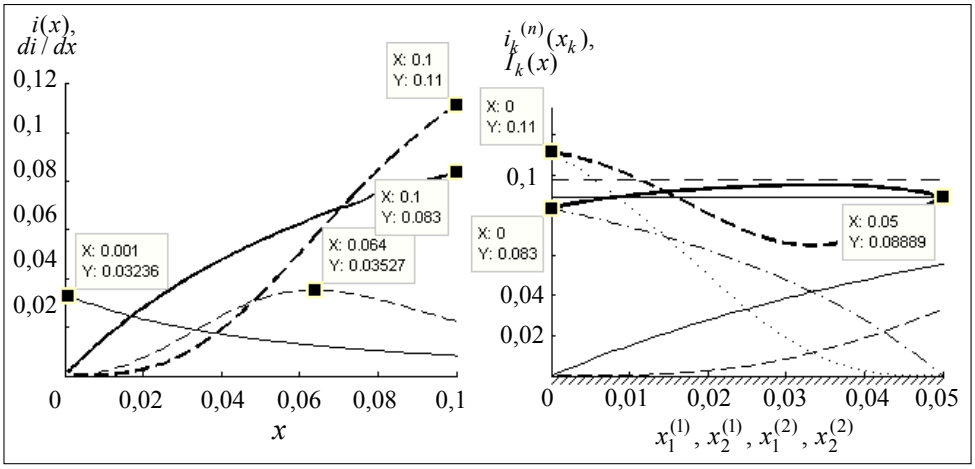

Рис. 2. Втрати інформації при використанні функцій вразливості (рис. 1) та $x_{\max}=0{,}1$

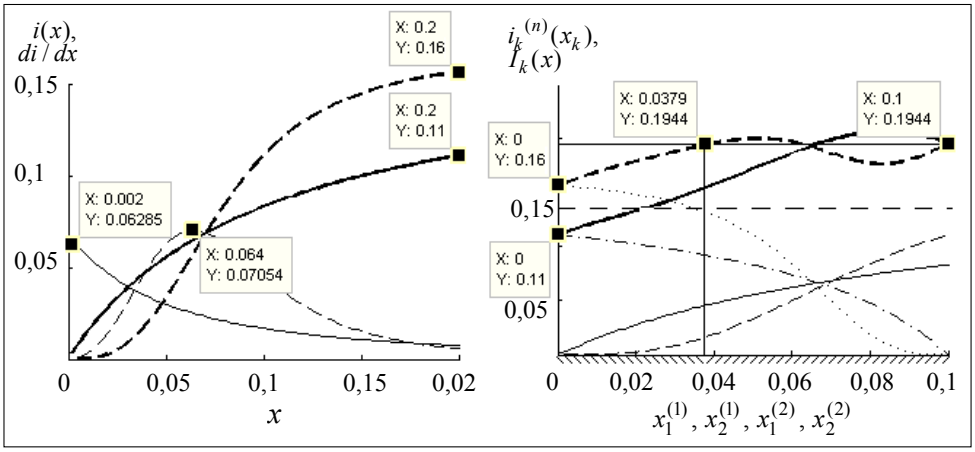

Рис. 3. Втрати інформації при використанні функцій вразливості (рис. 1) та $x_{\max} = 0{,}2$

На рис. 1–3 використано функції $f_1(x,y) = \dfrac{x/y}{x/y+4}$, $f_2(x,y) = \dfrac{(x/y)^3}{(x/y)^3+32}$ у різних діапазонах Δx: на рис. 1 — $\Delta x = 0...0{,}05$, на рис. 2 — $\Delta x = 0...0{,}1$, на рис. 3 — $\Delta x = 0...0{,}2$. На лівих частинах рисунків суцільними жирними лініями зображено залежності $i_1(x)$, жирними штриховими — $i_2(x)$, суцільними тонкими — di_1/dx, тонкими штриховими — di_2/dx. На правих частинах рисунків: суцільні тонкі лінії — $i_1^{(1)}(x_1^{(1)})$, тонкі штрихові — $i_2^{(1)}(x_2^{(1)})$, штрихові пунктирні — $i_1^{(2)}(x_1^{(2)})$, точки — $i_2^{(2)}(x_2^{(2)})$, суцільні жирні лінії — $I_1(x) = i_1(x_1^{(1)}) + i_2(x_2^{(1)}) + i_1(x_1^{(2)})$, жирний штрих — $I_2(x) = i_1(x_1^{(1)}) + i_2(x_2^{(1)}) + i_2(x_2^{(2)})$. Значення y в наведених залежностях виступає як параметр: $y = \dfrac{Y}{2} = 0{,}025$.

При використанні двох типів функцій (рис. 1–3) порівняння наведених результатів приводить до наступних висновків.

За першим критерієм. У першому діапазоні ($x = 0..0{,}05$ — рис. 1) розвідка доцільна при всіх x (суцільна крива лежить вище суцільної горизонтальної лінії) з концентрацією ресурсів витоку на першому об'єкті; в другому діапазоні ($x = 0..0{,}1$ — рис. 2) розвідка доцільна теж у всьому діапазоні, проте ресурси витоку в початковій області $x^{(1)}$ ($x^{(1)} = 0..0{,}015$) концентруються на другому об'єкті, а в кінцевій ($x^{(1)} = 0{,}015..0{,}05$) — на першому; в третьому діапазоні ($x = 0..0{,}2$ — рис. 3) розвідка доцільна лише в кінцевій області — при $x^{(1)} = 0{,}038..0{,}065$ — з зосередженням ресурсів витоку на другому об'єкті, а при $x^{(1)} = 0{,}065..0{,}1$ — на першому.

За другим критерієм. У першому діапазоні (рис. 1) розвідка доцільна в початковій області, яка займає майже весь діапазон ($x^{(1)} = 0..0{,}022$).

У другому діапазоні (рис. 2) розвідка доцільна теж у початковій області, проте в звуженому інтервалі ($x^{(1)} = 0..0{,}012$). У третьому діапазоні (рис. 3) розвідка доцільна у всій області.

Зміна інтервалів доцільності викликана зміщенням крайніх точок $x^{(1)} = 0$ та $x^{(1)} = x_{\Pi}$, причому темп зміщення цих точок різний: він визначається кривизною ліній $f_k(x, y)$ у відповідних діапазонах. Проте слід звернути увагу на такий результат: розвідка доцільна у всій області — за першим критерієм у першому діапазоні, за другим критерієм — у третьому діапазоні. Таким чином, вибір критерію може суттєво вплинути на прийняття рішення. Зазначимо, що перший критерій застосовується в умовах повної невизначеності, в той час, як при певній обізнаності про вразливість об'єктів має сенс застосування другого критерію.

При використанні двох дробно-нелінійних функцій отримуємо суттєво відмінний результат. У цьому випадку існують області, в яких розвідка недоцільна при всіх x — за першим критерієм у третьому діапазоні (рис. 6), за другим критерієм — у першому (рис. 4). Іншими словами, за малої кількості ресурсів їх слід вкладати в один із об'єктів, а за великої — ділити нарівно між об'єктами. Таким чином, при використанні двох дробно-нелінійних функцій розвідка частіше є недоцільною.

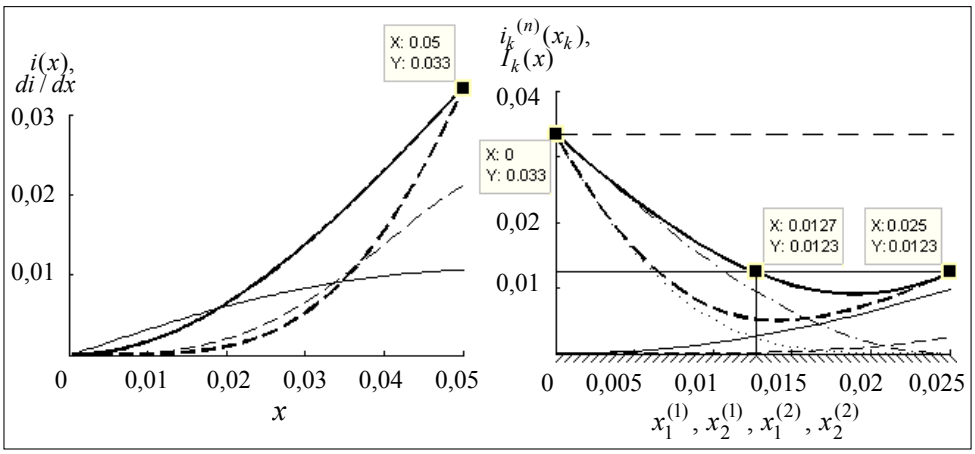

Рис. 4. Втрати інформації при використанні функцій вразливості $f_1(x, y) = \frac{(x/y)^2}{(x/y)^2 + 16}$, $f_2(x, y) = \frac{(x/y)^4}{(x/y)^4 + 64}$ та $x_{\max} = 0{,}05$

Спробуємо пов'язати питання про доцільність розвідки з формою кривих $f(x, y)$. Зауважимо, що положення крайніх правих точок (при $Y = 0{,}05$ та $x = x_{\max} = 0{,}05$) на лівих рисунках визначає положення крайніх лівих точок на правих рисунках. Вирішальну роль при цьому грає положення крайньої правої точки на правих рисунках відносно крайніх лівих. Якщо права точка розташована нижче однієї з лівих і відповідна крива має опуклість, направлену вгору у всьому діапазоні (функція $f(x, y)$ має дробно-лінійний характер), то розвідка по першому критерію доцільна у всьому діапазоні

(рис. 1). Якщо крива має змінний напрямок опуклості (дробно-нелінійна функція), то інтервал доцільності, який визначається цією кривою, звужується (рис. 2). В обох випадках існує певний інтервал доцільності по другому критерію. Якщо опуклість направлена донизу (рис. 4), то розвідка за другим критерієм недоцільна у всьому діапазоні, а за першим — в кінцевому інтервалі. Якщо ж права точка лежить вище обох лівих (рис. 3, 6), то можливі різні варіанти, в тому числі такий, при якому у всьому діапазоні розвідка недоцільна по першому критерію (рис. 6) і доцільна по другому (рис. 3, 6). Таким чином, аналіз напрямку опуклості кривих $f(x, y)$ може дати рекомендації з вибору принципу розподілу ресурсів за недоцільності розвідки — на один, більш привабливий об'єкт чи на два об'єкти.

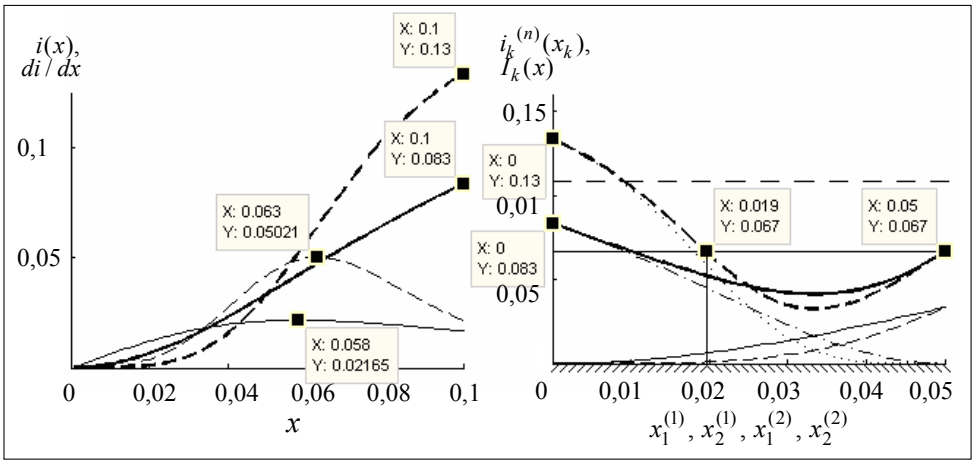

Рис. 5. Втрати інформації при використанні функцій вразливості (рис. 4) та $x_{\max} = 0{,}1$

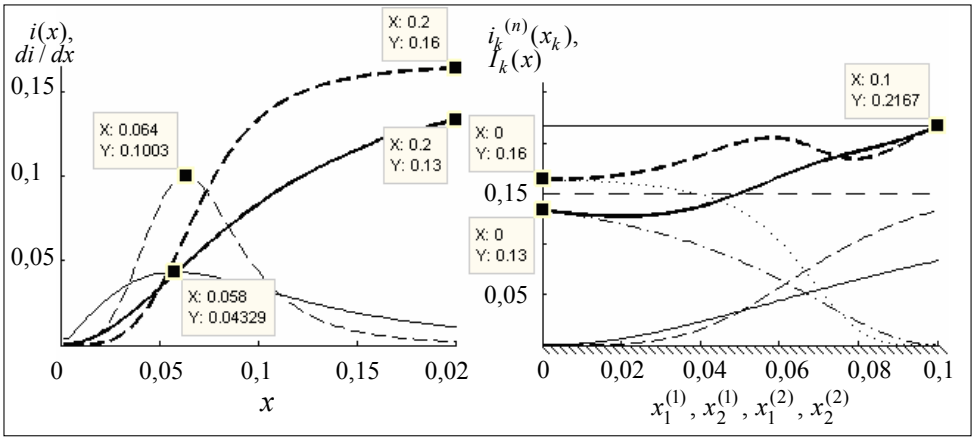

Рис. 6. Втрати інформації при використанні функцій вразливості (рис. 4) та $x_{\max} = 0{,}2$

Зауважимо, що напрямок опуклості кривих на правих рисунках визначається їх формою на лівих рисунках. Прослідкуємо це на прикладі рис. 1, 4. На правій частині рис. 1 ліва верхня точка $Y = 0{,}0558$ визначається правою верхньою точкою лівої частини. Крайня права точка $Y = 0{,}0383$ є сума ординат кривих $f(x, y)$ лівої частини в точці $x = 0{,}025$. Форма кривої, яка

з'єднує крайні точки на кожній частині, є в значній мірі дзеркальним відображенням кривої $f_1(x, y)$ між точками $x = 0{,}05$ і $x = 0{,}025$ відносно вертикальної прямої, що проходить через точку $x = 0{,}025$. При цьому зберігається і напрямок опуклості. З тих же причин суцільна крива на правій частині рис. 4 має опуклість, направлену вниз — так само, як відповідна крива на лівій частині рисунка. Додаткові відомості з розглянутого питання містяться в [3].

ВИСНОВКИ

Питання про доцільність проведення розвідки можна вирішити шляхом встановлення форми залежності динамічної вразливості об'єктів від ресурсів захисту і нападу. У випадку, коли розвідка недоцільна, проведений аналіз дозволяє надати рекомендації відносно вибору принципу розподілу ресурсів між об'єктами.

ЛІТЕРАТУРА

1. *Левченко Є.Г., Рабчун А.О.* Оптимізаційні задачі менеджменту інформаційної безпеки // Сучасний захист інформації. — 2010. — № 1. — С. 16–23.
2. *Gordon L.A.*, *Loeb M.P.* The Economics of Information Security Investment // Transactions on Information and System Security. — 2002. — **5**, № 4. — P. 438–457.
3. *Демчишин М.В.*, *Левченко Є.Г.* Ефективність розвідки при протистоянні двох сторін в інформаційній сфері // Сучасний захист інформації. — 2011. — № 2. — С. 5–15.

Поступила 17.03.2011