УДК 004.681

КОРЕЛЯЦІЯ ВИТРАТ У БАГАТОРУБІЖНИХ СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Є.Г. ЛЕВЧЕНКО, Д.І. РАБЧУН

Оптимізаційні економічні задачі інформаційної безпеки направлено на вирішення двох основних проблем: визначення оптимального розміру інвестицій в захист інформації і оптимізація розподілу ресурсів між об'єктами, котра забезпечує досягнення найкращих економічних показників. Перехід до багаторівневих багаторубіжних систем суттєво розширює проблему і викликає низку питань, обумовлених ускладненням структури і особливостями розташування окремих елементів. Розглянуто послідовно-паралельну схему розташування перешкод, котра містить спільну для всіх об'єктів перешкоду та індивідуальні перешкоди. Проаналізовано доцільність введення спільної перешкоди за незмінного бюджету захисту інформації в залежності від вразливості перешкод і розподілу інформації між об'єктами. Розроблено методику і наведено результати розрахунків оптимального розподілу ресурсів між спільною і індивідуальними перешкодами. Розглянуто умови кореляції між оптимальними розподілами ресурсів, направлених на індивідуальні перешкоди. Наведені результати можуть бути корисними при розробці рекомендацій з управління ресурсами і створенню оптимальних систем захисту інформації.

ВСТУП

Зростання обсягів і вартості інформації призводить до відповідного ускладнення систем захисту — вони стають багаторівневими і багаторубіжними. Подорожчання цих систем робить більш актуальною проблему оптимального використання ресурсів захисту. Оптимізаційні економічні задачі направлено на забезпечення найкращих показників інформаційної безпеки і мають два основних напрямки:

- визначення оптимального розміру інвестицій у захист інформації;
- оптимізація розподілу ресурсів між об'єктами.

У процесі пошуку рішення слід враховувати зміну умов протистояння з часом, пов'язану зі «старінням» інформації та її оновленням, появою нових засобів нападу, модернізацію систем захисту тощо. В результаті приходимо до задачі динамічного управління ресурсами в складних структурах захисту. На рис.1 показано приклад такої структури.

Схема (рис. 1) може представляти як фізичні, так і електронні системи. Прикладом фізичної системи може бути система, в якій спільна перешкода f_0 являє собою захищений периметр території, об'єкти g_1, g_2 — приміщення, а перешкоди f_{ks} — засоби, що захищають ці приміщення (у подвійних індексах перший з них — номер об'єкта, другий — номер перешкоди). Паралельні засоби f_{11}, f_{12}, f_{13} захисту першого об'єкта — це, приміром, заземлення електро- і тепломереж, екранування, зашумлення приміщень. Послідовні засоби f_{21}, f_{22} захисту другого об'єкта розташовані в суміжних

приміщеннях. В електронній системі (рис. 1) об'єкти g_1, g_2 — це комп'ютери, сервери, захищені спільною (firewall) та індивідуальними (антивірусне програмне забезпечення, шифрування даних, антиспамфільтри) перешкодами. Складну схему (рис. 1) можна звести до більш простих схем (рис. 2) з паралельним (рис. 2,*а*) або послідовно-паралельним (рис. 2,*б*) розташуванням елементів захисту.

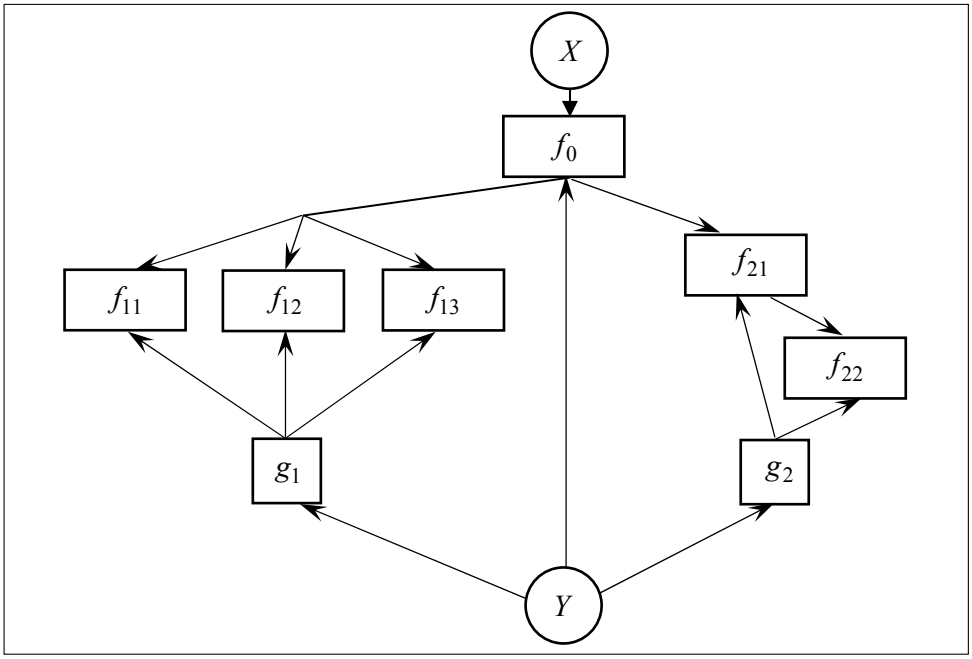

Рис. 1. Структура системи захисту інформації

Розгляду зазначених задач присвячено низку робіт, в якій аналізується як перша із сформульованих проблем [1–3], так і друга [4–6], причому в перших роботах структура інформаційної системи не конкретизувалась, а в інших розглядались лише найпростіші однорівневі системи. В [7] розглянуто деякі загальні аспекти аналізу багаторубіжних структур та наведено вирази для розрахунку їх показників. Слід зазначити, що перехід до багаторубіжних систем суттєво розширює проблему і викликає низку питань, обумовлених ускладненням структури і особливостями розташування окремих елементів.

Мета роботи — дослідження кореляції між оптимальними значеннями кількості ресурсів у багаторівневих багаторубіжних системах і розробка рекомендацій з управлінню розподілом ресурсів при зміні кількості об'єктів і введенні нових перешкод.

ПОСТАНОВКА ЗАДАЧІ

Маючи на меті виявлення основних закономірностей розподілу ресурсів захисту інформації в багаторубіжних системах, обмежимось розглядом спрощених структур (рис. 2). Аналізуючи послідовно-паралельну схему розташування перешкод (рис. 2,*б*), розглянемо такі задачі:

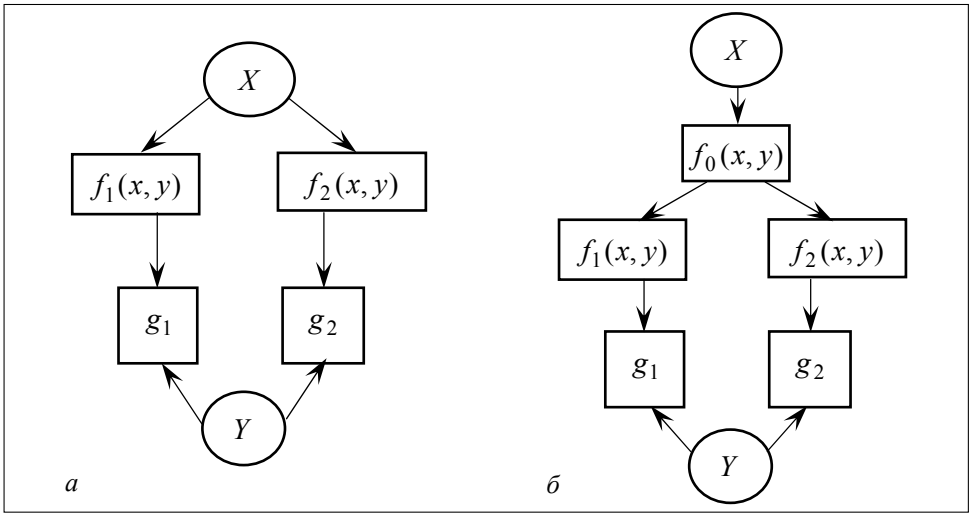

Рис. 2. Спрощені схеми систем захисту інформації, де: *а* — однорівнева система; *б* — дворівнева

- порівняння схеми (рис. 2,*б*) зі схемою (рис. 2,*а*) і визначення доцільності введення додаткової перешкоди при незмінному бюджеті захисту інформації;
- визначення оптимального розподілу ресурсів між спільною та індивідуальними перешкодами;
- встановлення кореляції між оптимальними розподілами ресурсів, направлених на індивідуальні перешкоди, для заданих схем;
- розробка рекомендацій по управлінню ресурсами в багаторубіжних системах.

Методика розрахунків. Використовуючи математичну модель [8], сформуємо цільову функцію, яка визначає відносну вартість втраченої інформації, у вигляді:

$$i(x,y)=\sum_{k=1}^{l} i_k(x,y)=\sum_{k=1}^{l} g_k p_k q_k(x,y) f^{(k)}(x,y),$$

де

x та y — ресурси нападу і, відповідно, захисту;

$k=\overline{1,l}$ — номер об'єкта;

g_k — відносна вартість інформації на об'єкті, $\sum_{k=1}^{l} g_k = 1$;

p_k — імовірність нападу на об'єкт;

$q_k(x,y)$ — щільність двомірного розподілу імовірності виділення ресурсів x, y;

$f^{(k)}(x,y)$ — частка втраченої інформації на об'єкті, котра визначає вразливість об'єкта.

Величини $i(x,y)$, $i_k(x,y)$ та g_k віднесені до загальної вартості інформації, $f^{(k)}(x,y)$ — до вартості інформації на об'єкті.

Зосередимось на впливі вразливостей об'єктів. З цією метою покладемо $p_k = 1$ і задамо $q(x, y) = \text{const} = 1$ в інтервалі значень x, y, котрий вважатимемо реальним.

З урахуванням наведених припущень цільова функція для структури (рис. 1,*б*) має вигляд:

$$i(x, y) = g_1 f^{(1)}(x, y) + g_2 f^{(2)}(x, y) = f_0(x, y)\left[g_1 f_1(x, y) + g_2 f_2(x, y)\right]. \quad (1)$$

Верхній індекс у виразах $f(x, y)$ — номер об'єкта, нижній — номер перешкоди. Вразливості об'єктів визначаються вразливостями перешкод:

$$f^{(1)}(x, y) = f_0(x, y) f_1(x, y), \quad f^{(2)}(x, y) = f_0(x, y) f_2(x, y).$$

Функції $f_k(x, y)$ виражають динамічну вразливість перешкод. Наслідуючи [8], приймемо, що змінні x, y входять у функції $q_k(x, y)$, $f^{(k)}(x, y)$ у вигляді відношення $\dfrac{x}{y}$. Величини $f_k(x, y)$ визначаються властивостями перешкод і мають задовольняти умовам: при $x/y \to 0$ $f_k(x, y) \to 0$, при $x/y \to \infty$ $f_k(x, y) \to 1$. Найпростішою формою функцій, які задовольняють зазначеним умовам, є дробово-степенева:

$$f_k(x, y) = \frac{\left(x/y\right)^{n_k}}{\left(x/y\right)^{n_k} + c_k} = \frac{1}{1 + c_k \left(y/x\right)^{n_k}} \quad (2)$$

При $n_k = 1$ (2) виражає дробово-лінійну залежність, при $n_k > 1$ — дробово-нелінійну. Параметри n_k та c_k мають смисл продуктивностей витрат на захист інформації [9]. При графічному зображенні вони впливають на форму залежностей $f_k(x, y)$.

У подальшому для спрощення запису введемо позначення: $\dfrac{x}{y} = \tilde{x}$, $\dfrac{y}{x} = \tilde{y}$. Тоді цільова функція (1) для служби захисту матиме вигляд:

$$i(\tilde{y}) = \frac{1}{1 + c_0 \tilde{y}_0^{n_0}} \left(\frac{g_1}{1 + c_1 \tilde{y}_1^{n_1}} + \frac{g_2}{1 + c_2 \tilde{y}_2^{n_2}} \right). \quad (3)$$

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Метою наших розрахунків є знаходження оптимального розподілу $\{y_k^0\}$, який мінімізує $i(\tilde{y})$. Структуру (рис. 2,*а*) вважаємо базовою, з якою порівнюємо структуру (рис. 2,*б*) при різних варіантах параметрів $G = g_1/g_2$, n_k, c_k.

У ході вирішення першої з поставлених задач необхідно визначити умови, за яких введення додаткової перешкоди при незмінному бюджеті захисту інформації є доцільним. Критерієм доцільності є зменшення можливого обсягу втраченої інформації при забезпеченні оптимального розподілу ресурсів захисту між об'єктами.

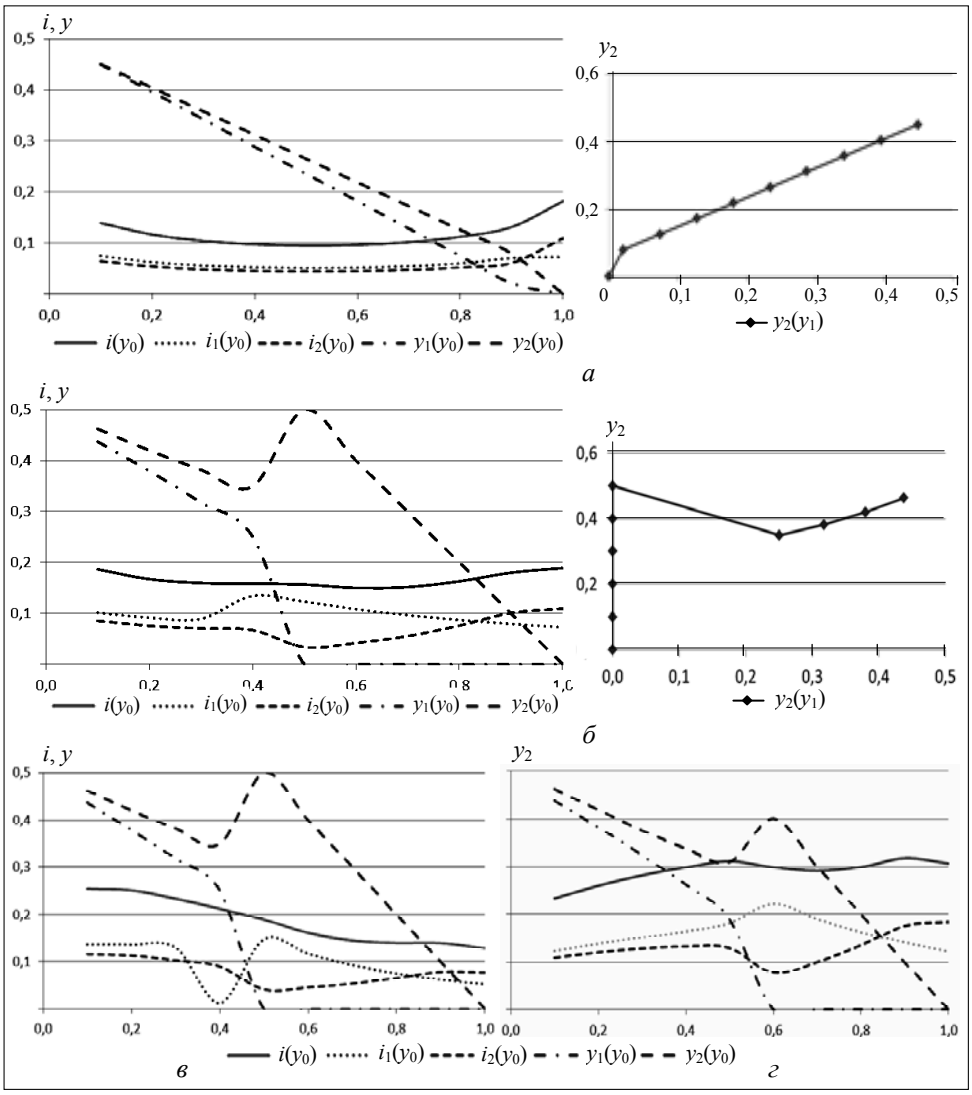

Рис. 3. Залежності $y_k^0(y_0)$, $i_k(y_0)$, та $i(y_0)$ для системи (рис. 2,*б*,*г*) при $Y=1$ $X=2$, $g_1=0{,}4$, $g_2=0{,}6$ та різних значеннях параметрів n_k, c_k: *а* — $n_0=n_1=n_2=1$; *б* — $n_0=1$, $n_1=n_2=2$; *в* — $n_0=n_1=n_2=2$, (для *а*, *б*, *в* — $c_0=3$, $c_1=4$, $c_2=8$); *г* — $n_0=n_1=n_2=2$, ($c_0=1$, $c_1=5$, $c_2=9$)

На рис. 3 показано оптимальний розподіл ресурсів захисту $y_1^0(y_0)$, $y_2^0(y_0)$ між індивідуальними перешкодами і відповідну частку втраченої інформації $i_1(y_0)$, $i_2(y_0)$ на кожному з об'єктів, а також сумарні втрати $i(y_0)=i^{(1)}(y_0)+i^{(2)}(y_0)$ — залежно від кількості ресурсів y_0 на спільній

перешкоді. Нижній нулик у позначенні змінних відноситься до спільної перешкоди, верхній — до оптимальних значень. Розподіл ресурсів нападу між перешкодами вважаємо рівномірним: $x_k = \frac{X}{l}$. Рис. 3,*а,б* відображають ситуацію, коли вразливість спільної перешкоди описується дробово-лінійною залежністю ($(n_0 = 1)$, рис. 3,*в,г* — коли дробово-квадратичною $(n_0 = 2)$. Для індивідуальних перешкод розглянуто різні варіанти функцій — як дробово-лінійних (рис. 3,*а*), так і дробово-квадратичних (рис. 3,*б–г*). На правих частинах рис. 3,*а,б* показано лінії регресії $y_2^0(y_1^0)$.

Аналізуючи результати розрахунків, звернемо увагу на форми залежностей $i(y_0)$ та $y_2(y_1)$. Перша з них визначає доцільність введення спільної перешкоди і дозволяє встановити оптимальну кількість y_0^0 ресурсів, які слід виділяти на цю перешкоду. Можливі такі варіанти:

- $0 < y_0^0 < 1$ (рис. 3,*а,б*) — існує оптимальне значення y_0^0;
- $y_0^0 = 1$ (рис. 3,*в*) — на спільну перешкоду слід направити всі ресурси;
- $y_0^0 = 0$ (рис. 3,*г*) — вводити спільну перешкоду недоцільно.

Шуканий розподіл $\{y_k^0\}$ знаходимо як оптимум функції трьох змінних $i(y_0, y_1, y_2)$. Точка оптимуму (y_0^0, y_1^0, y_2^0) визначається методом перебору всіх можливих комбінацій (y_0, y_1, y_2), обмежених умовою $\sum_{k=1}^{3} y_k = Y$. Ця процедура здійснюється за допомогою програмного комплексу Matlab.

На рис. *3,а–г* фіксується величина y_0 в інтервалі від 0 до 1 й для кожного з цих значень наведено оптимальні величині y_1^0, y_2^0. Шуканий розподіл $\{y_0^0, y_1^0, y_2^0\}$ визначається точкою y_0^0, яка відповідає найменшому значенню $i(y_0)$ (ця точка позначається вертикальною штриховою лінією).

Точка (y_0^0, y_1^0, y_2^0) характеризує ситуацію, коли збільшення будь-якої з цих величин (за рахунок інших) призводить лише до погіршення ситуації, тобто збільшення величини $i(y)$. Значення кожної з величин y_0^0, y_1^0, y_2^0 залежить від вразливості перешкод і продуктивності відповідних витрат. На продуктивність витрат впливають величини похідних $\frac{di}{dy_k}(y_k)$. Співвідношення похідних з врахуванням вагових коефіцієнтів g_k при всіх можливих значеннях y_k визначає напрямок найбільш ефективного внесення ресурсів. Вразливості перешкод, тобто значення функцій $f(y)$ (2) (де покладено $x = 1)$, та величини похідних $\frac{df}{dy}$, тобто продуктивності витрат за однакових значень g_k, зображено на рис. 4 та 5.

Положення точки y_0^0 на шкалі y_0 визначається параметрами n_k, c_k. Слід врахувати, що, відповідно до (2), у ході зростання c_k вразливість $f(x,y)$ зменшується (рис. 4), а у ході зростання n_k — збільшується (оскільки вартість ресурсів захисту має бути меншою, ніж вартість інформації — $y_k < 1$). Тому значення $y_0^0 = 0$ досягається в системі, де c_0 приймає мінімальне значення $c_0 = 1$, а $n_0 = 2$ (рис. 3,*г*). При цих значеннях n_0, c_0 вразливість $f(y)$ спільної перешкоди висока, а продуктивність $|f'(y)|$ інвестицій низька (рис. 4,*б*, 5,*б* криві 4), і їх доцільно розподілити між індивідуальними перешкодами. При зростанні c_0 вразливість зменшується, а продуктивність зростає в основному інтервалі зміни y (рис. 4,*а*, 5,*а* криві 4). Точка y_0^0 зміщується вправо і зрештою досягає значення $y_0 = 1$ (рис. 3,*в*).

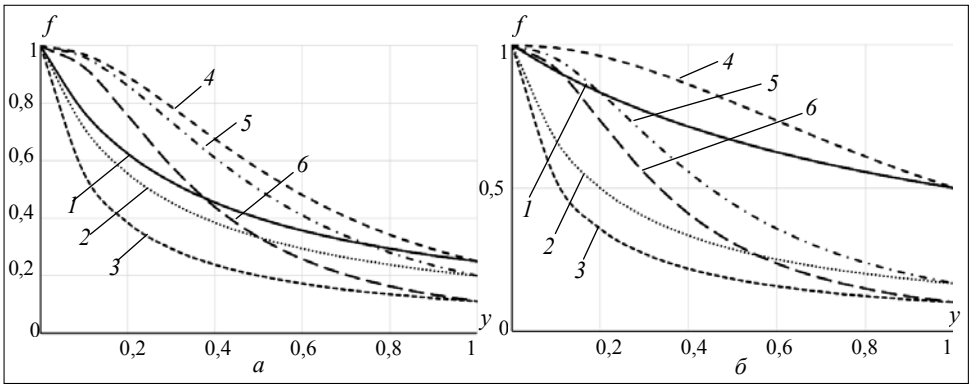

Рис. 4. Вразливості перешкод при різних значеннях n та c:
криві *1–3* — $n = 1$, криві *4–6* — $n = 2$;
а — криві *1*, *4* — $c = 3$; *2*, *5* — $c = 4$; 3, 6 — $c = 8$;
б — криві *1*, *4* — $c = 1$; *2*, *5* — $c = 5$; 3, 6 — $c = 9$

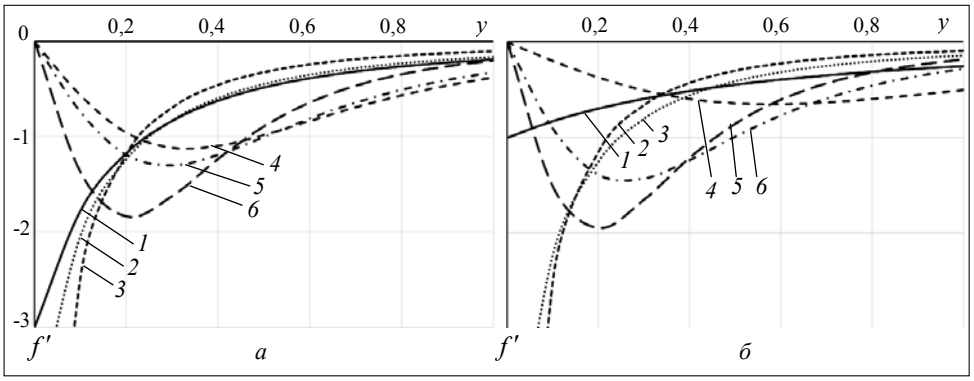

Рис. 5. Продуктивності витрат на захист інформації при різних значеннях n та c:
криві *1–3* — $n = 1$; *4–6* — $n = 2$;
а — криві *1*, *4* — $c = 3$; *2*, *5* — $c = 4$; *3*, *6* — $c = 8$;
б — криві *1*, *4* — $c = 1$; *2*, *5* — $c = 5$; *3*, *6* — $c = 9$

При зміні обох типів показників — n_k й c_k — необхідно врахувати вплив кожного з них. Порівнюючи показники різних перешкод, слід

пам'ятати, що показники спільної перешкоди грають більшу роль, оскільки вона захищає обидва об'єкти. При певних співвідношеннях значень n_k, c_k введення спільної перешкоди є доцільним і значення y_0 знаходиться в інтервалі $0 < y_0 < 1$ (рис. 3,*а*,*б*).

В реальних системах розподіл інформації на об'єктах може бути нерівномірним $(g_1 \neq g_2)$, що також буде впливати на оптимальний розподіл ресурсів.

Залежності $y_1(y_0)$ й $y_2(y_0)$ і, відповідно, лінії регресії $y_2(y_1)$ можуть приймати дві принципово відмінні форми. Перша з них відтворює узгоджену зміну величин y_1 й y_2 та близьку до лінійної залежність $y_2(y_1)$ (рис. 3,*а*). Така ситуація спостерігається, коли вразливості перешкод описуються дробово-лінійними функціями (рис. 3,*а*). Цей висновок справедливий також для однорівневих систем з більшою кількістю об'єктів. Привабливість цієї форми обумовлена тим, що за умови введення додаткової перешкоди співвідношення між необхідними ресурсами y_1, y_2 не змінюється суттєво і не потребує значної перебудови системи захисту інформації. Друга форма характеризує ситуацію, коли при досягненні певного значення y_0 узгоджена зміна величин y_1, y_2 переходить в кардинальний перерозподіл ресурсів — всі ресурси зосереджуються на одному з об'єктів. Цю ситуацію ілюструють рис. 3,*б–г*, де, починаючи зі значення $y_0 = 0{,}5$, величина y_1 зменшується до нуля, а y_2 зростає до максимально можливого значення $y_2 = 0{,}5$. На рис. 3,*г* y_2 зростає до значення $y_2 = 0{,}4$, оскільки перерозподіл відбувається при $y_0 = 0{,}6$. Причину таких «стрибків» проаналізовано в [10].

Весь інтервал зміни y_0 можна поділити на 3 зони (рис. 3,*б*):

- зона 1 — при зростанні y_0 величини y_1, y_2 монотонно і узгоджено зменшуються. При цьому зростають вразливості індивідуальних перешкод, проте одночасно зростає захисна дія спільної перешкоди — відбувається часткова компенсація, в результаті $i_1(y_0)$, $i_2(y_0)$ та $i(y_0)$ змінюються слабо.
- зона 2 — y_1 зменшується до нуля, y_2 зростає до максимально можливого (при даному y_0) значення, відповідно, $i_1(y_0)$, зростає, а $i_2(y_0)$ зменшується.
- зона 3 — $y_1 = 0$, y_2 поступово зменшується (через зростання y_0), $i_1(y_0)$ спадає (з тієї ж причини), $i_2(y_0)$ зростає через спадання y_2.

Оптимізацію розподілу ресурсів направлено на досягнення мінімального значення $i(x, y)$. Розглянемо, при яких комбінаціях $\{n_k\}$, $\{c_k\}$ величина $i_{\min}(y_0)$ досягає найменшого значення. Будемо звертати увагу також на інтервал Δi зміни величини $i(x, y)$ при зростанні y_0 від 0 до 1. Як видно з рис. 3, найкращі результати за цими показниками досягаються при $n_0 = n_1 = n_2 = 1$: на рис. 3,*а* $i_{\min}(y_0) = 0{,}09$, причому в значній частині інтер-

валу зміни y_0 значення $i(y_0)$ не перевищують 0,1. Це й зрозуміло: найменші значення n_k виражають найменшу вразливість перешкод. При переході до значень $n_1 = n_2 = 2$ (рис. 3,*б*) $i_{\min}(y_0)$ зростає до 0,15, залишаючись у всьому інтервалі зміни y_0 близьким до цього значення (на границях інтервалу $i(y_0) = 0{,}19$). При повністю нелінійних функціях вразливості $n_0 = n_1 = n_2 = 2$ значення $i(y_0)$ зростають, а сама залежність при заданих на рис. 3,*в*,*г* значеннях c_k стає відчутно нерівномірною. Наведені дані свідчать про те, що фізичні системи простіше піддаються захисту, ніж електронні. Порівняння залежностей $i(y_0)$ показує також, що при певних наборах параметрів n_k й c_k можна досягти значної компенсації зміни вразливостей спільної та індивідуальних перешкод і досягти досить рівномірного характеру залежності $i(y_0)$ (рис. 3,*б*).

Для порівняння систем введемо величину $K = i_{\min}(y_0) \times \Delta i$, яка враховує обидва зазначені показники. Для системи (рис. 3,*в*) маємо $K = 0{,}13 \times \times 0{,}12 = 0{,}016$, для системи (рис. 3,*г*) $K = 0{,}23 \times 0{,}09 = 0{,}018$. Найкращий результат у системі з $n_0 = n_1 = n_2 = 2$ досягається при $c_0 = 2$, $c_0 = 4$, $c_0 = 9$ і становить $K = 0{,}18 \times 0{,}08 = 0{,}014$.

Зауважимо, що кореляція величин y_1 та y_2 визначається, в основному, значенням n_0: при $n_0 = 1$ ці величини корелюють у всьому інтервалі зміни y_0, а при $n_0 = 2$ коефіцієнт кореляції при певному значенні y_0 різко змінює знак з позитивного на негативний.

На завершення зазначимо, що обґрунтуванням застосування наведеної методики можна вважати те, що вона дає якісно схожі, а при певному виборі параметрів — співпадаючі результати [11] з широко відомою методикою Гордона-Лоеба [1], яка знайшла своє емпіричне підтвердження [12–13].

ВИСНОВКИ

Введення спільної перешкоди на додаток до індивідуальних змінює співвідношення між надійністю об’єктів і потребує коригування розподілу ресурсів в рамках незмінного бюджету. Доцільність введення спільної перешкоди та оптимальний розподіл ресурсів між перешкодами залежить від їх динамічних вразливостей $f_k(y)$ і розподілу інформації між об’єктами. Ці фактори впливають на ступінь коригування розподілу ресурсів, яке може бути узгодженим для окремих об’єктів, але й також може переходити у кардинальний перерозподіл ресурсів. Визначення форми залежностей $f_k(y)$, точніше кажучи — параметрів n_k, c_k — при використанні наведеної методики дозволить надати рекомендації з оптимізації багаторубіжних систем захисту інформації, а в перспективі — до їх синтезу.

ЛІТЕРАТУРА

1. *Gordon L.A., Loeb M.P.* The Economics of Information Security Investment // ACM Transactions on Information and System Security. — 2002. — **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. *Рабчун А.О.* Оптимізація сумарних втрат в сфері захисту інформації // Безпека інформації. — 2012. — № 1. — С. 32–36.
4. *Левченко Є.Г.* Оптимізація розподілу ресурсів між об'єктами захисту інформації // НТЖ «Захист інформації». — 2007. — № 1. — С. 33–38.
5. *Прус Р.Б.* Оптимізація розподілу ресурсів захисту інформації в динамічному режимі // Безпека інформації. — 2012. — № 1. — С. 26–32.
6. *Демчишин М.В., Левченко Є.Г.* Оптимізація розподілу ресурсів при проведенні розвідки в інформаційному протистоянні // Системні дослідження та інформаційні технології. — 2012. — № 4. — С. 56 – 63.
7. *Левченко Є.Г., Прус Р.Б., Рабчун А.О.* Показники багатоступінчастих систем захисту інформації // Вісник Інженерної академії України. — 2009. — № 1. — С. 61–65.
8. *Левченко Є.Г., Рабчун А.О.* Оптимізаційні задачі менеджменту інформаційної безпеки // Сучасний захист інформації. — 2010. — № 1. — С. 16–23.
9. *Левченко Є.Г., Прус Р.Б., Рабчун Д.І.* Показники продуктивності витрат на захист інформації // Безпека інформації. — 2012. — № 2. — С. 6–11.
10. *Демчишин М.В., Левченко Є.Г.* Вплив вразливості об'єктів на розв'язок прямої та зворотної задач менеджменту інформаційної безпеки // Системні дослідження та інформаційні технології. — 2012. — № 3. — С. 43–57.
11. *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.
12. *Matsuura K.* Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model // The Seventh Workshop on the Economics ofInformation Security. June 25–28, Hanover, USA. — 2008.
13. *Lui W., Tanaka H., Matsuura K.* Empirical – Analysis Methodology for Information – Security Investment and its Application to a Reliable Survey ofJapanese Firms // Information Proceeding of Japan Digital Courier. — 2007. — **3**. — P. 585–599.

Надійшла 21.05.2013