УДК 004.056

к.ф.-м.н., доц. Левченко Є.Г., Рабчун А.О. (ДУІКТ)

ОПТИМІЗАЦІЙНІ ЗАДАЧІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Вступ

Однією з основних складових менеджменту інформаційної безпеки являється пошук розподілу ресурсів, який забезпечує оптимізацію одного з показників – мінімальну кількість вилученої інформації при заданих ресурсах захисту, мінімальну кількість ресурсів захисту, необхідних для додержання певного рівня інформаційної безпеки чи максимальну економічну ефективність системи захисту інформації (СЗІ), котру ми визначаємо як частку двох величин – зменшення втрат інформації в результаті застосування СЗІ і витрат на її захист [1,2]. Можлива також комбінація цих показників, що є предметом багатокритеріальних задач. При цьому через складність ситуації, які можуть виникнути при вирішенні цієї проблеми, математичні моделі відрізняються значною різноманітністю. Тому здається доцільним розглянути типи виникаючих задач і провести їх класифікацію. Основною рисою, яка об'єднує ці задачі і одночасно створює головні труднощі, являється те, що пошук оптимальних рішень ведеться в умовах невизначеності. Ця риса обумовлена самим характером антагоністичного протистояння і тому не може бути усунена.

Постановка задачі

Ключовою проблемою при побудові математичної моделі являється формування цільової функції, яка, частіше за все, визначає кількість вилученої інформації $I(x,y)$. В загальних рисах її можна записати в такому вигляді:

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

де $k = \overline{1,l}$ – номер об'єкта;

g_k – кількість інформації на об'єкті;

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

$q_k(x)$ – імовірність виділення суперником ресурсів x на k-ий об'єкт;

$f_k(x,y)$ – залежність частки вилученої інформації від співвідношення ресурсів x і y, яку можна розглядати як ефективність вкладання ресурсів, або імовірність вилучення інформації при заданих значеннях x і y.

Якщо кількість g_k інформації на об'єкті можна оцінити з певною точністю, то вигляд залежностей $q_k(x)$, $f_k(x,y)$ в умовах відсутності статистичної інформації, (що пов'язане з специфікою проблеми) невідомий і може бути встановлений лише якісно на основі загальних міркувань. В умовах невизначеності вибір цих функцій, як і оцінка g_k, здійснюється на основі експертних оцінок [3].

Мета роботи: розглянути задачі розподілу ресурсів в сфері захисту інформації, а також окреслити проблеми пов'язані з їх вирішенням.

Поставлена проблема виникла при аналізі антагоністичного протистояння у військовій сфері, де в якості залежності $f(x)$ (індекс k поки що опустимо, а також покладемо $y = 1$ – при цьому x визначатиме відносні ресурси нападу) використовувалась функція Гросса [4,5]. В економічних задачах ця функція може знайти застосування лише як апроксимація, постільки вона має кусочно-лінійний характер, а на початковій і кінцевій дільницях $f(x) = const$, що не відповідає реальним ситуаціям. Умовам нашої задачі задовольняють

степеневі функції $f(x) = \frac{ax^n}{bx^n + c}$ і показникові $f(x) = 1 - e^{-mx^n}$, де константи a, b, c, n, m визначають положення і нахил кривих [6]. Запропоновані залежності при різних значеннях констант зображені на рис. 1. Зазначимо, що в моделі Гордона-Лоеба [7], де в якості показника цільової функції виступає вразливість СЗІ, також використовується степенева і показникові функції, причому степенева функція при певному виборі констант співпадає з нашою. В цільовій функції (1) вразливість системи неявно входить як параметр в залежності $f_k(x, y)$, що й спричиняє відмінність цих залежностей для різних об'єктів. В останній час з'явилась низка робіт з дослідження моделі Гордона-Лоеба [8-10], що свідчить про її ґрунтовність і вимушує звернути на неї посилену увагу.

Друга серйозна задача – це визначення виду функції $q(x)$. Найпростіший варіант дає лапласівський підхід, відповідно до якого всі можливі рішення суперника в умовах невизначеності вважаються рівноімовірними, тобто $q(x) = const$. Звичайно, такий підхід потребує серйозного коригування, оскільки, вимагає визначення інтервалу Δx, в якому знаходяться можливі значення x, а головне – зрозуміло, що в реальних умовах $q(x) \neq const$. Таким чином, виникають два питання: 1) визначення виду залежності $q(x)$; 2) встановлення значення x_m, при якому залежність $q(x)$ досягає максимума. За нашою думкою, ця залежність має більшу крутизну на ділянці $x = 0..x_m$, поступово спадаючи при зростанні x і прямуючи до нуля при $x \gg 1$. Цим умовам задовольняють залежності виду $f(x) = Nx^n e^{-h^2x^2}$, зокрема розподіл Максвела $q_M(x) = Nx^2 e^{-h^2x^2}$ і розподіл Релея $q_p(x) = Nxe^{-h^2x^2}$, де N – нормовочний коефіцієнт, а константи n, h визначають положення максимума залежності (для розподілу Максвела $x_m = \frac{1}{h}$, Релея $x_m = \frac{1}{\sqrt{2}h}$) і ступінь її асиметрії. На рис. 2. приведені максвелівські розподіли для трьох значень x_m, а також лінія $q(x) = q = const$, проведена при умові, що значення x лежать в межах $x = 0 \ldots 3$, а величина q визначається умовою, що повна імовірність події, тобто площа під відповідними залежностями, дорівнює 1. Штриховими лініями зображені релеєвські розподіли. Зазначимо, що основна відмінність форм розподілів Максвела і Релея, суттєва для наших задач, полягає в тому, що в початковій області (при $x \gtrsim 0$) опуклість в розподілі Максвела направлена вниз, а в розподілі Релея – вгору (рис. 2). Зрозуміло, що комбінація можливих залежностей $f(x)$ і $q(x)$ утворює значну кількість варіантів, яку бажано обмежити. Це, очевидно, можна зробити, враховуючи специфіку кожної системи захисту інформації і спираючись на оцінку експертів.

Коефіцієнти h обрані таким чином, що максимуми функцій розподілу знаходяться в точках $x = 1$ (криві 1, 4); $x = 1{,}5$ (криві 2, 5); $x = 2$ (криві 3, 6). Коефіцієнти N нормують інтеграл функції в межах [0;3] до одиниці.

Розглянемо тепер окремі системи захисту інформації, відповідні математичні моделі і проблеми, які виникають при пошуку оптимальних рішень для цих моделей.

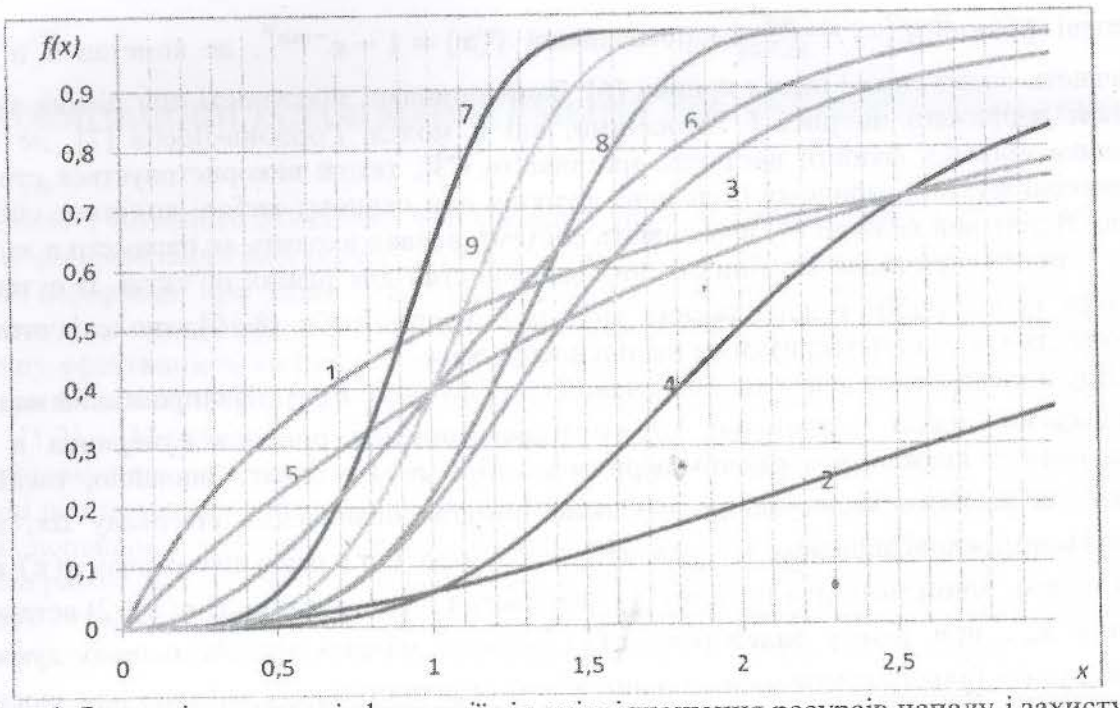

Рис. 1. Залежність втрат інформації від співвідношення ресурсів нападу і захисту.

1. $f(x)=\frac{x}{x+1}$ 2. $f(x)=\frac{x^2}{x^2+4^2}$ 3. $f(x)=\frac{x^4}{x^4+4}$

4. $f(x)=\frac{x^4}{x^4+2^4}$ 5. $f(x)=1-e^{-\frac{1}{2}x}$ 6. $f(x)=1-e^{-\frac{1}{2}x^2}$

7. $f(x)=1-e^{-x^2}$ 8. $f(x)=1-e^{-\frac{1}{4}x^4}$ 9. $f(x)=1-e^{-\frac{1}{2}x^4}$

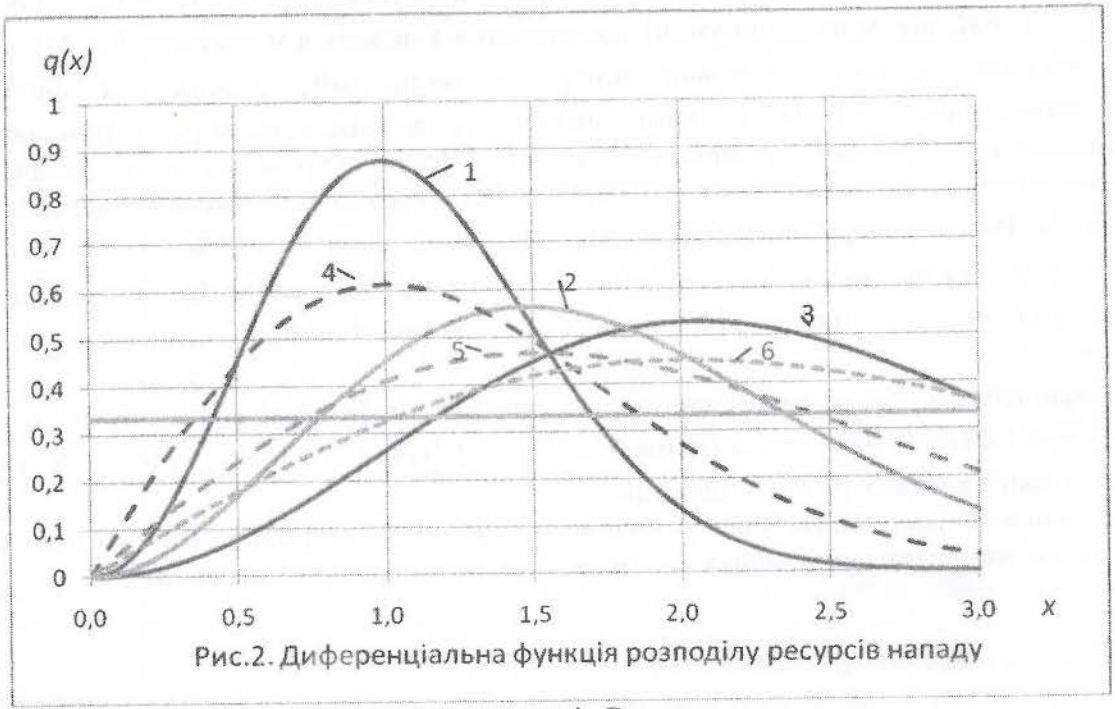

Рис.2. Диференціальна функція розподілу ресурсів нападу

1,2,3 – розподіл Максвела, 4,5,6 – розподіл Релея.

1) $h=1;\ N=2{,}257;$
2) $h=0{,}66;\ N=0{,}682;$
3) $h=0{,}5;\ N=0{,}358;$
4) $h=0{,}7071;\ N=1{,}011;$
5) $h=0{,}471;\ N=0{,}513;$
6) $h=0{,}3536;\ N=0{,}37;$

1. Оптимальний розподіл ресурсів між об'єктами захисту інформації

Графічно модель цієї задачі представлена на рис. 3. Система складається з кількох об'єктів, і задача полягає в пошуку оптимального розподілу ресурсів $\{y_k^o\}$ між об'єктами (на нашій моделі для конкретності зображено 3 об'єкти).

Задано: 1) розподіл об'ємів інформації $\{g_k\}$;

2) ресурс захисту $Y = \sum_k y_k$ (ми покладаємо $Y = 1$).

Знайти: розподіл $\{y_k^o\}$ при умові, що $X = \sum_k x_k$ і $\{x_k\}$ невідомі.

Ця задача розподіляється на дві частини, в залежності від того, на яку кількість об'єктів здійснюється напад.

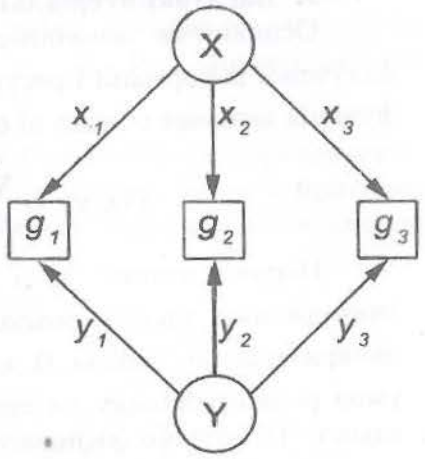

Рис. 3.

1а. Напад здійснюється на один з об'єктів

Цей варіант реалізується при виконанні принаймні однієї з таких умов:

а) ресурси нападу обмежені, і він вважає недоцільним розпорошувати їх між об'єктами;

б) супернику відомий розподіл інформації $\{g_k\}$, і він спрямовує свої зусилля на найважливіший об'єкт;

в) суперника цікавить, в першу чергу, інформація на якомусь певному об'єкті, куди він і направляє свої ресурси.

В таких задачах використовується, зазвичай, один з критеріїв пошуку оптимальних рішень в умовах невизначеності [11,12]. Вибір критерію визначається схильністю до ризику. Нам здається доцільним використати критерій Севіджа, який при розгляді можливих варіантів розподілу $\{x_k\}$ дозволяє знайти розподіл $\{y_k\}$, котрий мінімізує максимальний ризик [1].

1б. Напад здійснюється на всі об'єкти

Цей варіант реалізується при виконанні однієї або декількох з таких умов:

а) ресурси нападу достатні для того, щоб розподілити їх між об'єктами;

б) супернику невідомий розподіл ресурсів $\{g_k\}$;

в) суперник виділяє частину ресурсів на розвідку розподілу $\{g_k\}$.

В цьому випадку ми приходимо до задачі лінійного програмування, і застосування симплекс-метода приводить до одного з двох варіантів:

1) розв'язок має сідлову точку, тобто існує в чистих стратегіях; застосовуючи стратегії, кожна сторона одержує найкращий результат, і відхилення від неї може привести до його погіршення;

2) розв'язок існує лише в змішаних стратегіях, які і формують оптимальні рішення.

У випадку двох змінних (тобто двох об'єктів) розв'язок можна одержати графічно, що дає можливість наочно продемонструвати формування оптимального результату. При цьому ми можемо застосувати один з методів умовної оптимізації – метод Лагранжа або метод Якобі [9] і розв'язок одержати аналітично. Якщо кількість змінних перевищує 2, можна застосувати метод оптимізації Белмана [13], який забезпечує найшвидший шлях одержання результату.

В приведених прикладах ми розглядали пряму задачу: задано ресурс захисту Y, і необхідно визначити, яким може бути при цьому витік інформації I. Може бути сформульована і зворотна задача: задано I_m, і необхідно визначити, яким повинен бути

ресурс захисту Y, котрий забезпечить $I < I_m$. Розв'язок зворотної задачі утруднений, і тому вона зводиться зазвичай до прямої, а рішення знаходиться методом перебору.

2. Багатокритеріальна задача

Основними показниками ефективності системи захисту інформації є кількість I вилученої інформації і ресурс Y, витрачений на її захист. Розглянемо випадок, коли цільова функція включає обидва ці показники з ваговими коефіцієнтами λ і $1-\lambda$:

$$S(x,y)=\sum_{k=1}^{l}[\lambda I_k(x,y)+(1-\lambda)y_k],\quad \sum_{k=1}^{l} I_k = I,\quad \sum_{k=1}^{l} y_k = Y. \quad (2)$$

Нашою метою, як і раніше, являється мінімізація цільової функції по y, тобто знаходження такого розподілу $\{y_k\}$, при якому досягається мінімум функції (2). Це двокритеріальна задача. В даному випадку крім g_k задаються значення λ, які можна знайти з умов рівності впливу на економічну безпеку підприємства втрат інформації і витрат на її захист. Необхідно визначити $S_{min}(x,y)$ і відповідний розподіл $\{y_k^o\}$. Можливо залучити третій показник – економічну ефективність $E=\frac{\Delta I}{\Delta Y}$, де ΔI – зменшення втрат інформації при збільшенні витрат ΔY на її захист.

3. Багаторубіжний захист

Комплексні системи захисту інформації (КСЗІ) являються багаторубіжними, або багатоступінчастими [2,14]. Складність цих систем створює додаткові труднощі як при розрахунку їх показників [8], так і при визначенні оптимального розподілу ресурсів між окремими рубежами захисту. Спрощена модель багаторубіжної СЗІ показана на рис. 4.

Слід зазначити, що ресурси захисту розподіляються автономно, тобто ресурси спрямовують на об'єкти g_1, g_2 і перешкоди 1, 2, 3 паралельно і одночасно. В той же час ресурси нападу направляються на подолання перешкод послідовно, після подолання чергової перешкоди (рис 4). Таким чином, розподіл ресурсів захисту встановлюється заздалегідь, а ресурси нападу розподіляються в динамічному режимі. Послідовний характер подолання перешкод приводить до того, що аналіз протистояння на кожній перешкоді необхідно проводити з врахуванням імовірності подолання попередньої перешкоди. Таким чином, ми одержали стохастичну задачу, в якій повинні бути враховані дві імовірності: імовірність $q(x)$ виділення нападом певних ресурсів x для подолання цієї перешкоди і імовірність $p(x,y)$ подолання перешкоди при певному співвідношенні x і y. Маємо умовну імовірність, яка входить в вираз (1) і визначається добутком цих величин:

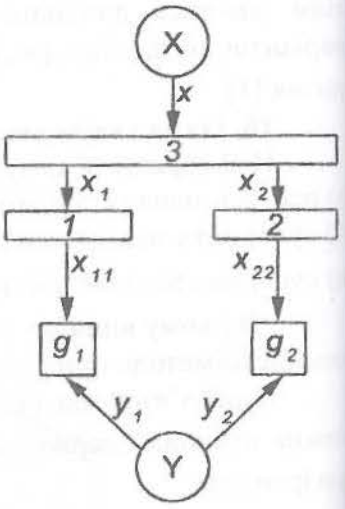

Рис. 4.

$$F_k(x,y)=q_k(x)\cdot p_k(x,y)$$

Враховуючи рекурентний характер задачі, одержуємо повну імовірність P_i подолання i-ої перешкоди, з врахуванням ймовірностей p_j подолання всіх попередніх перешкод:

$$P_i(x,y)=\prod_{j=1}^{i} p_j(x,y)$$

При цьому кількість величин, які потребують визначення за допомогою експертної оцінки, зростає, що створює додаткові труднощі, проте є особливістю задач пошуку оптимальних рішень в умовах невизначеності.

Зазначимо, що розподіл ресурсів в багаторубіжних системах може бути централізованим – коли кількість об'єктів (і кількість перешкод) невелика, і управління ресурсами ведеться з єдиного центру, і децентралізованим – коли об'єктами являються окремі підприємства, і центр проводить розподіл ресурсів між ними, а подальше управління ресурсами виконується на місцях: $\{y_k\} = \{y_{k,j}\}$, $\sum_j y_{k,j} = y_k$ де k – номер об'єкта (підприємства), j – номер перешкоди.

Ступінь децентралізації визначається складністю системи, При цьому слід враховувати, що центр має більш повну інформацію, проте окремі підприємства можуть більш оперативно реагувати на дії суперника, хоча з удосконаленням електронних інформаційних систем останнє твердження стає менш значущим.

4. Вплив розвідки на розподіл ресурсів

При наявності достатніх ресурсів напад може свої дії поділити на два етапи – розвідку і здобуття інформації. Схема такого протистояння зображена на рис. 5.

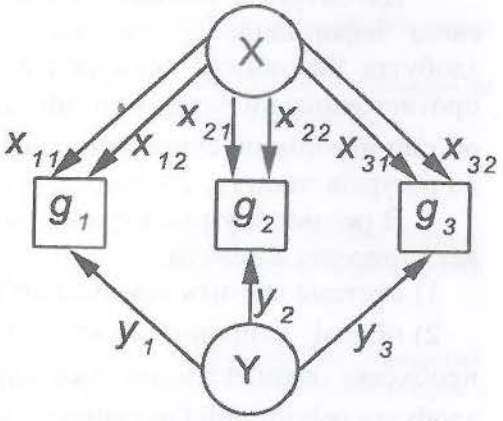

Рис. 5.

Перший індекс в позначенні ресурсів нападу x_{ks} - це номер об'єкта, а другий приймає два значення: $s = 1$ відноситься до розвідки, $s = 2$ - до здобуття інформації.

Ця задача відрізняється від задачі 1 більшою кількістю варіантів можливого розподілу ресурсів нападу і тим, що на другому етапі напад діє в умовах певної інформованості, що, звичайно, необхідно враховувати при розподілі ресурсів захисту (цим самим ми переходимо від задачі в умовах невизначеності до стохастичної задачі).

Розглянутий варіант можна вважати першим кроком до динамічного управління ресурсами, коли після перших спроб вилучення інформації обидві сторони можуть внести корективи в розподіл своїх ресурсів (для нападу така можливість виникає, якщо спроби виявились вдалими, а для захисту – у випадку, коли спроби суперника зафіксовані).

5. Управління ресурсами

Процес динамічного управління ресурсами захисту і нападу схематично показано на рис. 6, де для цього використовують сигнали зворотного зв'язку G_k і D_k. Приведена схема ілюструє застосування динамічного програмування, яке дає можливість здійснювати оптимальний розподіл ресурсів в динамічному режимі: $x_k = x_k(t)$, $y_k = y_k(t)$. З точки зору теорії ігор це позиційна гра.

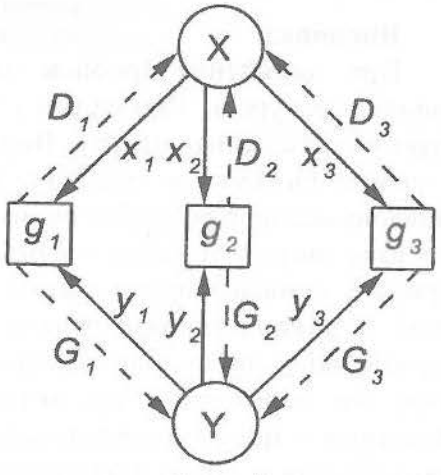

Рис. 6.

6. Визначення станів інформаційної безпеки

В попередніх прикладах ми розглядали результат протистояння двох сторін при спробі вилучення інформації. Не в меншій мірі нас цікавить питання: яким буде стан інформаційної безпеки після низки таких спроб, котрі можуть відрізнятися як параметрами, так і результатом протистояння. Відповідь на це питання може дати використання теорії випадкових процесів, зокрема марковських ланцюгів [11]. При цьому виникає ряд додаткових обчислювальних труднощів, пов'язаних з недостатністю відомостей про характеристики цього випадкового процесу. Зокрема, в розрахунок перехідних ймовірностей, а потім і ймовірностей станів ми повинні закласти:

1) частість спроб;

2) залежність $q_{kn}(x)$ для n-ої спроби;

3) залежність $x_k(n)$;

4) величину g_k, яка тепер через зменшення кількості інформації з кожною спробою стає залежною від часу: $g_k = g_k(t)$, в результаті чого ланцюги стають неоднорідними.

При розгляді дискретних марковських ланцюгів задача зводиться до розв'язку системи лінійних диференціальних рівнянь. Більш повну інформацію можна одержати, розглядаючи неперервні марковські ланцюги, які приводять до необхідності розв'язання системи диференціальних рівнянь Колмогорова.

7. Комплексне протистояння

Ця ситуація виникає, коли кожна сторона захищає свою інформацію і одночасно спрямовує зусилля на здобуття інформації конкурента. Спрощена схема такого протистояння зображена на рис. 7, де через g і d позначені об'єми інформації суперників, верхній індекс 1 відноситься до ресурсів захисту, 2 – до ресурсів нападу.

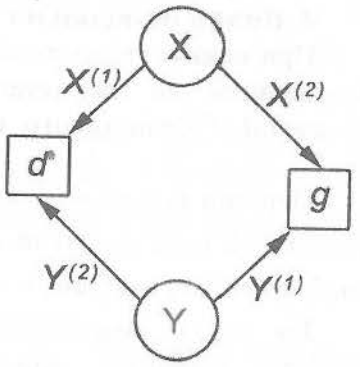

Рис. 7.

В реальних умовах схема рис. 7, може узагальнювати всі попередні варіанти:

1) система містить декілька об'єктів;

2) обидві сторони можуть проводити розвідку – і необхідно визначити оптимальну частку ресурсів, які направляються на розвідку і на здобуття інформації (звичайно, з врахуванням можливих дій суперника);

3) система захисту кожного об'єкта є багаторубіжною – отже, нам необхідно визначити оптимальний розподіл ресурсів між окремими перешкодами, сформованими по послідовно-паралельній схемі;

4) оптимізація ресурсів ведеться в динамічному режимі;

5) оптимізація може вестись по декількох критеріях;

6) результатом являється визначення станів системи в неперервному режимі.

Висновки

При вирішенні проблем захисту інформації виникають різноманітні задачі щодо розподілу ресурсів. Такі задачі є багатогранними, та їх розв'язок не являється очевидним і потребує детального аналізу. Вирішення цих задач дозволяє раціонально витрачати ресурси на захист, що суттєво збільшує конкурентоздатність підприємства. При проектуванні СЗІ кінцевою метою є розробка оптимальної системи. Тим самим ми приходимо до необхідності розв'язку зворотної задачі – формування системи по заданих параметрах і характеристиках. В умовах невизначеності синтез СЗІ можливий шляхом переходу до прямої стохастичної задачі з використанням певних критеріїв. При цьому можуть виникнути нестандартні ситуації, які лишились поза нашою увагою. Прикладами таких ситуацій є недбальство – при цьому ми переходимо від антагоністичної гри до гри з природою, випадок декількох нападників – це гра з ненульовою сумою і т.ін. Всі ці ситуації і математичні моделі систем мають бути розглянуті в майбутньому.

Список літератури

1. Левченко Є.Г. Оптимізація розподілу ресурсів між об'єктами захисту інформації. – К.: НТЖ «Захист інформації», №1, 2007. С. 34-38.

2. Левченко Є.Г., Прус Р.Б., Рабчун А.О. Показники багатоступінчастих систем захисту інформації. «Вісник інженерної академії України», №1, 2009.

3. Левченко Є.Г., Рабчун А.О. Експертні оцінки в економічних задачах інформаційної безпеки. – К.: НТЖ «Захист інформації», №3, 2009. С.81-85.

4. Применение теории игр в военном деле/ Под ред. В.О. Ашкеназы. – М.: Сов. радио, 1961 – 360 с.

5. Гермейер Ю.Б. Введение в теорію исследования операцій. – М.: Наука, 1971. – 383с.

6. Левченко Є.Г., Рабчун А.О. Модель Гросса в протистоянні двох сторін у сфері захисту інформації. – К.: НПЖ «Сучасна спеціальна техніка», №3 (18), 2009. С. 75-81.

7. Gordon L., Loeb M. The Economics of Information Security Investment. ACM Transactions of Information and System Security, November 2002. – Vol.5, No. 4. – P. 438-457.

8. Задірака В.К., Олеснюк О.С., Смоленюк Р.П., Штабалюк П.І. Фінансування витрат на захист інформації в економічній діяльності. Університетські наукові записки, №3-4 (19-20), 2006 – С. 479-490.

9. W. Liu, H. Tanaka, K. Matsuura. Empirical – Analysis Methodology for Information-Security Investment and Its Application to Reliable Survey of Japanese Firms. IPSJ Digital Courier, 3, 2007, p. 585-599.

10. K. Matsuura. Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model. M.E. Johnson (ed.) Managing Information Risk and the Economics of Security. Springer, USA, 2009.

11. Вентцель Е.С. Исследование операций. – М.: Сов. радио, 1972. – 552с.

12. Таха Х., Исследование операций. – М.: Вильямс, 2005. – 912 с.

13. Беллман Р. Динамическое программирование. – М.: Наука, 1960.

14. Хорошко В.О., Ковальова Ю.Є., Плус Д.В. Розподіл ресурсів у багаторубіжній системі захисту. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 8, 2004. С. 39-43.

Розглянуто широке коло задач, які виникають при протистоянні двох сторін у сфері захисту інформації. Побудовано математичні моделі, обговорюбться проблеми, які виникають при пошуку оптимальних рішень в умовах невизначеності, намічено шляхи їх подолання.

Ключові слова: оптимальний розподіл ресурсів, математична модель, цільова функція.

Рассмотрен широкий круг задач, которые появляются при противоборстве двух тсорон в сфере защиты информации. Построены математические задачи, обсуждаются проблемы, которые возникают при поиске оптимальных решений в условиях неопределенности, предложены пути их решения.

Ключевые слова: оптимальное распределение ресурсов, мтаематическая модель, целевая функция.

Various tasks that arise up in investigation of opposition between two sides in the field of information security are considered in the paper. Mathematical models are built, problems at the search of optimum decisions in the conditions of indefinite come into question are arised, the ways of their overcoming are set.

Key words: optimum resource allocation, mathematical model, objective function.

Надійшла 17.12.2009