УДК 004.056

Д.І. Рабчун

ОЦІНКА ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З УРАХУВАННЯМ ЕКОНОМІЧНИХ ПОКАЗНИКІВ

У роботі розглянуто підходи до управління ресурсами підприємства, котрі виділені на захист. Запропоновано методику багатокритеріальної оптимізації з урахуванням економічних показників на основі математичного моделювання.

Математичні моделі інформаційного протистояння при всій різноманітності їх форм є близькими за своєю сутністю. Цільова функція виражає одну з споріднених величин: частку втраченої інформації, імовірність порушення системи захисту, ризик втрат, який визначається як добуток імовірності реалізації загрози на завданий збиток, тощо. Основна характеристика системи захисту, яка впливає на значення цільової функції — це вразливість, котра в тій чи іншій формі виражається через співвідношення ресурсів нападу і захисту. В цільову функцію входить також імовірність виділення на напад певної кількості ресурсів при заданій кількості ресурсів захисту.

Ключові слова: інформаційна безпека, управління ресурсами, математичне моделювання, оптимізація.

Вступ

Широкомасштабне впровадження автоматизованих систем (АС), побудованих із використанням сучасних інформаційних технологій в структуру бізнес-процесів на всіх рівнях сприяло швидкому переведенню економіки на шлях інновацій.

Проблемою став той факт, що до недавнього часу процес автоматизації проходив без належної уваги до захисту інформації, що призвело до неконтрольованого зростання вразливостей і можливостей несанкціонованого доступу до інформаційних ресурсів.

Поряд з тим, розвиток інформаційної сфери відображається в багатьох показниках: зростають обсяги і вартість інформації, втрати від її витоку, збільшується частота і витонченість нападів, та, відповідно, складність і вартість систем захисту. Як наслідок — зростають вимоги до ефективності використання ресурсів захисту, котра визначається, зрештою, технічними та економічними показниками систем захисту інформації. Оптимізація кількості та розподілу ресурсів захисту являє собою досить серйозну задачу, труднощі рішення котрої пояснюються низкою причин: складність систем захисту, невизначеність умов протистояння, неможливість точного визначення параметрів і функціональних залежностей, котрі характеризують вразливість об’єктів захисту. Невизначеність умов протистояння в економічній сфері полягає в тому, що невідомі наміри, а іноді і дії суперника — націленість атак, кількість його ресурсів і їх розподіл між об’єктами захисту. Розгляд всіх можливих ситуацій при пошуку оптимальної стратегії дії захисту приводить до значного зростання кількості розрахункових варіантів і, зрештою, не дає відповіді на поставлене питання. Часто ці труднощі обходять, оцінюючи імовірності окремих стратегій нападу і переходячи до пошуку рішення в умовах ризику [1]. Суб’єктивізм такого підходу в значній мірі знецінює отримані результати. Бажано знайти таке рішення, котре забезпечує певний результат за будь-яких дій суперника, що особливо важливо в умовах динамічного протистояння, коли умови протистояння змінюються з часом.

Правильне використання інструментів фінансового планування та параметрів оцінки ефективності впроваджуваних проектів дозволяють вибрати найбільш оптимальне рішення й істотно заощадити на фінансових витратах компанії в інформаційну безпеку. У результаті аналізу приведених показників фахівці мають можливість зробити обґрунтований вибір на користь того чи іншого проекту, і так само прогнозувати перспективи своєї діяльності на осяжний термін вперед. Отже, найбільш оптимальним вибором буде проект, в якому присутня комбінація наступних показників:

- Найбільш низький TCO (зниження витрат на зміст проекту системи захисту);
- Збільшення ROI (відсотка повернення фінансових вкладень в проект);
- Зменшення Payback — якомога менший період, бажано, не більше року, тому це дозволить обґрунтувати вкладення в рамках річного бюджету.

Наведені в статті показники і методика розрахунку, безумовно, не є кінцевими, існує ще безліч додаткових критеріїв дозволяють перевірити оптимальність прийнятого рішення і формалізувати ефективність їх експлуатації.

Мета роботи — використання багатокритеріального методу оптимізації ресурсів захисту в умовах динамічного інформаційного протистояння.

Актуальність дослідження систем захисту інформації шляхом використання математичного моделювання з'явилась на початку XXI ст. і знайшла відбиття у низці робіт фахівців різних галузей. Найбільш успішними та результативними виявились праці американських та японських вчених. Перші математичні моделі були побудовані виходячи з логічних міркувань та уявлень про природу інформаційних протиборств.

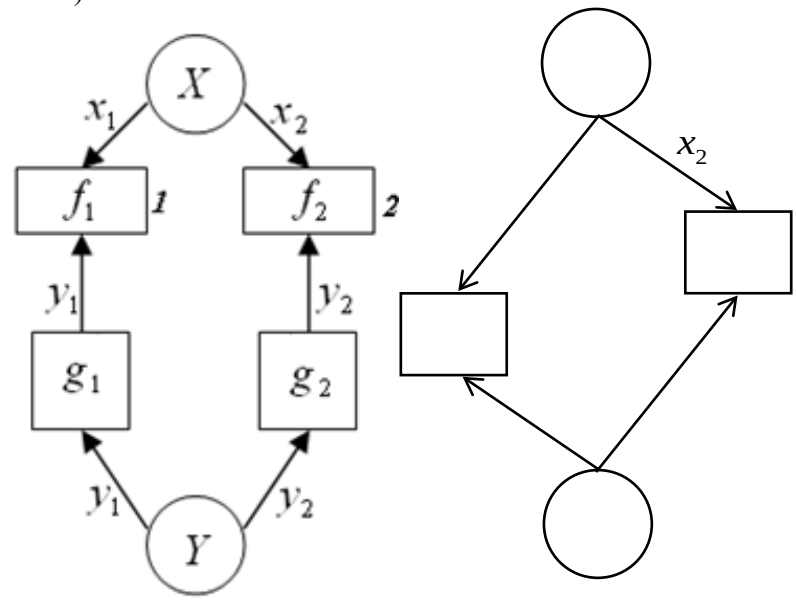
З розвитком інформаційних технологій в Україні і зростанням інтеграції економіки в глобальну інформаційну інфраструктуру питання інформаційної безпеки набрало актуальності і в нашій державі. Відповідною реакцією стала поява низки робіт по економіці ІБ. При детальному аналізі вітчизняних моделей виявлено: при певному наборі вихідних параметрів результати отримані за допомогою математичної моделі [2] співпадають з результатами в [3]. Враховуючи виявленні при порівняльному аналізі переваги можна стверджувати про високий рівень достовірності та адекватності отримуваних результатів, а отже і вагомість їх впливу на прийняття рішення по менеджменту ІБ.

Аналіз існуючих моделей систем захисту інформації було проведено з метою вибору математичного апарату для досягнення основної мети роботи, а саме, створення методики для оцінки ефективності СЗІ з урахуванням економічних показників. В результаті, за рядом показників, було обрано модель, описану в [4].

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

Методика розрахунків і результати

Для ілюстрації методики використано найпростішу структуру інформаційної системи (рис.1), котра містить два об'єкти g_1, g_2, захищені індивідуальними перешкодами f_1 та f_2 (назви об'єктів одночасно визначають кількість інформації на них, а назви перешкод — вразливості об'єктів).



а) б)

Рис.1. Схеми різних форм протистояння:
а) однонаправленого; б) різнонаправленого

Також під час більш детального аналізу цільової функції були виявлені можливості для

збільшення відповідності даної моделі реальним системам та врахування більшого спектру параметрів, що дозволило збільшити її адекватність та точність отримуваних результатів

1) Варто відмітити важливість обґрунтування параметрів, змінних, констант та залежностей, котрі входять до цільової функції.

Так, вибір залежності функції вразливості $f(x,y)$ залишився на дробово-степеневій функції:

$$f(x,y)=\frac{\left(x/y\right)^n}{\left(x/y\right)^n+c}$$

вигляд цієї функції відповідає природі об'єкта, який описується, легко піддається аналізу, приймає значення у діапазоні від 0 до 1, при $x/y \to 0$ $f_k(x,y)\to 0$, при $x/y \to \infty$ $f_k(x,y)\to 1$.

2) Визначено роль параметрів n, c. Відповідно до діапазону значень, які можуть приймати параметри n, c функція $f(x,y)$ буде описувати різні системи.

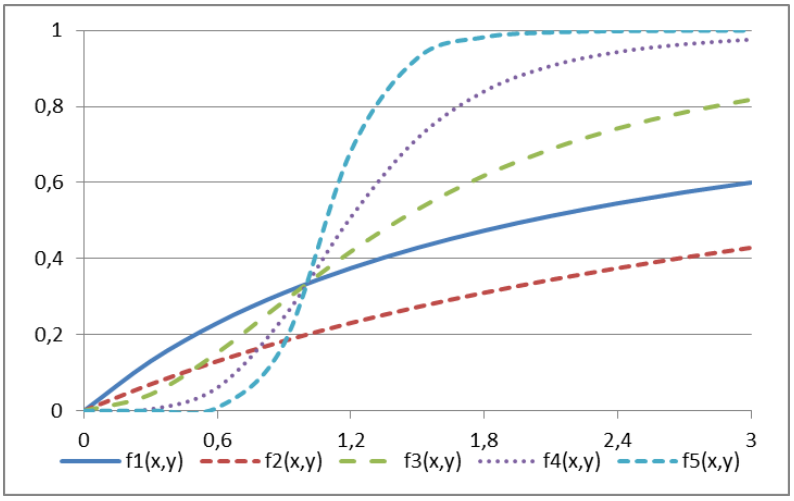


Рис.2. Вигляд функції вразливості при різних значеннях c, n

Дробово-лінійним функціям вразливості при $n=1$ відповідають системи захисту інформації, для яких внесення інвестицій навіть на початкових етапах ($x/y<1$) дає певні результати. Наприклад: охорона периметру, захист від витоку каналами ПЕМВН, тощо.

Дробово-нелінійні функції при $n>1$ описують вразливість, наприклад, криптографічних систем: внесення інвестицій не приносить результату до моменту коли з'ясований ключ або виявлена уразливість криптоалгоритму, після цього моменту вразливість криптосистеми різко збільшується.

Чим більше n, тим більшим є порогове значення при якому перешкода є маловразливою до атак і тим стрімкішою є зона росту при перевищенні порогового значення співвідношення ресурсів нападу та захисту.

Коефіцієнт c можна інтерпретувати як природну захищеність, наприклад: рекомендується облаштовувати серверні приміщення невеликих мереж в окремих кімнатах, які не мають суміжних дверей з іншими приміщеннями і знаходяться якомога далі від сходів і виходів.

3) Визначення меж та допустимих значень, котрі може приймати цільова функція і змінні. Для вирішення цього питання будо зібрано та консолідовано інформацію із періодичних звітів у сфері інформаційної безпеки, як України, так і інших держав.

Встановлено, що на захист інформації, в залежності від масштабів компанії витрачається від 1% до 30% бюджету IT, а втрати інформації вважаються прийнятними у

діапазоні від 0 до 4%, на додачу до цього втрата більш ніж 20% інформаційних активів в 60% призводить до краху і банкротства компанії.

Застосування вищезгаданих пропозицій до моделі [2] дозволяє стверджувати про збільшення її адекватності, пригодності та достовірності отриманих результатів при моделюванні систем захисту. Якщо раніше використання даної моделі давало якісну оцінку СЗІ та описувало природу залежності цільової функції від ресурсів виділених на захист, після врахування описаних зауважень отримано кількісні результати, котрі можуть бути використані при проектуванні систем захисту.

Для прикладу параметри системи вважаємо відомими. Вразливості об'єктів на першому етапі описуються дробово-лінійними функціями: $n_1 = n_2 = 1$. Параметри c_k становлять: $c_1 = 32$, $c_2 = 128$. Розподіл інформації по об'єктах: $g_1 = 0.4$, $g_2 = 0.6$, що відповідає логічному рішенню — більша частина інформації розташована на об'єкті з меншою вразливістю. Загальну кількість ресурсів нападу вважаємо сталою і задаємо рівною $X = 0.1$ (10% від вартості інформації).

Умову сформулюємо наступним чином. Втрати інформації не повинні перевищувати $i_{гр} = 0.05$, загальні втрати — $S_{гр} = (i + Y)_{гр} = 0.09$. Необхідно знайти кількість ресурсів захисту Y і їх оптимальний розподіл $\{y_k^0\}$ по об'єктах, котрий забезпечує досягнення мінімального значення $S_{\min}$ при виконанні заданих обмежень і відповідає сідловій точці.

Маючи на меті пошук сідлової точки, зосереджуємо увагу на таких складових цільової функції, як вразливість об'єктів $f_k(x, y)$ і розподіл інформації $\{g_k\}$. Для цього покладемо $p_k = 1$, $q_k(x, y) = 1$. Цільова функція при сформульованих умовах приймає вигляд:

$$i(x, y) = i_1(x, y) + i_2(x, y) = 0.4\frac{x_1 / y_1}{x_1 / y_1 + 32} + 0.6\frac{x_2 / y_2}{x_2 / y_2 + 128} \qquad (1)$$

Пошук сідлової точки ведеться з допомогою програмного комплексу MatLab шляхом почергової оптимізації ресурсів нападу і захисту [5]. Розподіл ресурсів протилежної сторони, досягнутий на попередньому кроці, вважається відомим. На першому кроці покладаємо розподіл $\{y_k\}$ ресурсів захисту на об'єктах пропорційним розподілу інформації $\{g_k\}$ і знаходимо розподіл $\{x_k\}$ ресурсів нападу, котрий забезпечує досягнення $\max_x i(x, y)$ в межах заданої кількості ресурсів $\sum_{k=1}^{l} x_k = X$. На другому кроці, виходячи з одержаного розподілу $\{x_k\}$, знаходимо оптимальний для захисту розподіл $\{y_k\}$, котрий забезпечує досягнення $\min_y i(x, y)$ в межах заданого значення $\sum_{k=1}^{l} y_k = Y$. Якщо сідлова точка для функції $i(x, y)$ існує, то цей процес є збіжним, і ми продовжуємо його до досягнення рівності $\max_x i(x, y) = \min_y i(x, y)$. Ця точка і визначає оптимальні розподіли $\{x_k^0\}$, $\{y_k^0\}$. Якщо сідлова точка відсутня, то після певної кількості кроків процес буде циклічно повторюватись необмежене число разів, показуючи, що стаціонарного стану не існує.

Оптимальний розподіл ресурсів захисту при фіксованому розподілі ресурсів нападу $X = 0.1$ знаходимо з умови $S(y_1, y_2) \to \min$ при виконанні введених граничних обмежень на величини i, S.На рис.3 представлено результати при дробово-лінійних функціях вразливості і цільовій функції у формі (1).

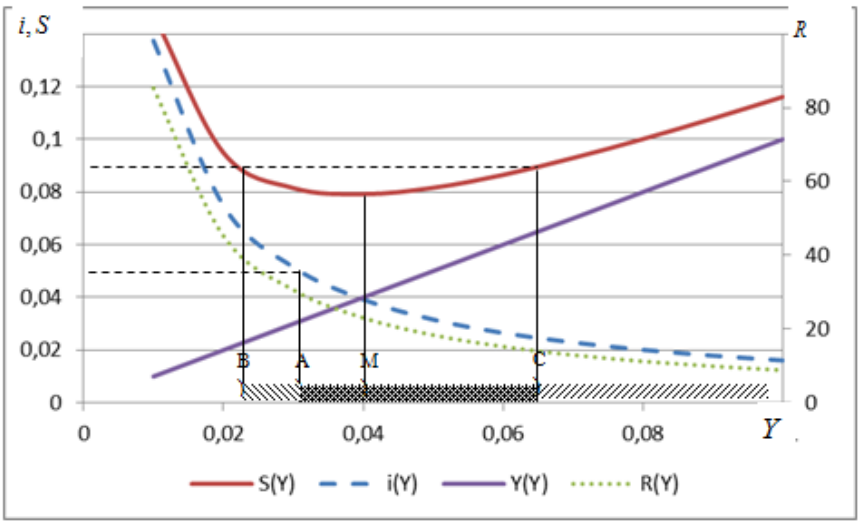


Рис.3. Показники системи (рис.1,а) в сідлових точках при $g_1 = 0.4$, $g_2 = 0.6$, $n_1 = n_2 = 1$; $c_1 = 32$, $c_2 = 128$;

Наступним важливим фактором при переході до дробово-нелінійних функцій виявилось зміщення оптимального значення: якщо при $n = 1$ оптимальне значення цільової функції забезпечувалося екстремальною точкою, то при $n > 1$ мінімум знаходиться на межі інтервалу допустимих значень і являє собою інфімум. Таким чином можна стверджувати про явище міграції оптимуму в залежності від значень параметрів функцій вразливості.

При побудові систем захисту та плануванні стратегії та політики інформаційної безпеки виявлене явище має суттєве значення. Помилка при оцінці вихідних параметрів на етапі проектування або розподілу ресурсів захисту призведе до значних втрат інформаційних активів.

Також слід зазначити, що отримане значення не може гарантувати мінімального результату за тієї причини, що границя допустимих значень визначається межами існування сідлової точки і відхилення від заданої точки рівноваги «вліво» призведе до нескінченного циклічного процесу при якому ні одна із стратегій захисту не буде гарантувати стабільного результату.

При дослідженні впливу параметра c на оптимум цільової функції було виявлено наступні закономірності:

1) параметри c_k пов'язані із значеннями g_k. А саме: раціональний розподіл інформації по об'єктам, коли більш захищені об'єкти містять більшу кількість інформації показують найбільшу ефективність при однаковій кількості ресурсів на захист Y.

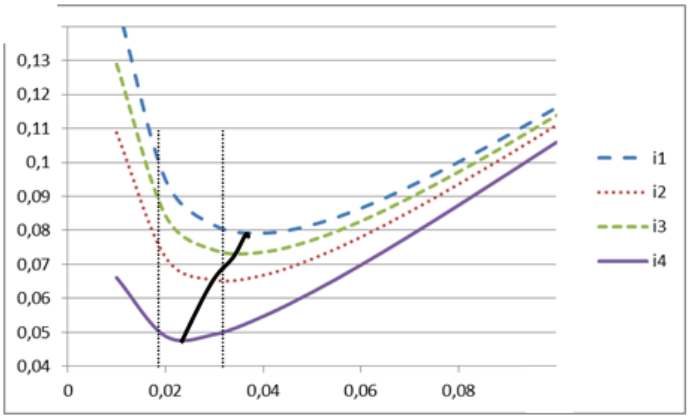


Рис.4. Міграція оптимальних значень в значень параметра c та розподілу інформації по об'єктам g_1 / g_2

Рис.4 ілюструє описану вище закономірність. Розподіляючи раціональним чином інформацію по захищеним об'єктам керівництво може досягти значного зменшення загальних втрат інформації.

Точки А і В відображають індиферентну зону (+-10% від оптимальної точки) для і4. Крива CDвідображає шлях оптимуму під час зміни параметрів. Варто зазначити, що частина кривої потрапляє в індиферентну зону і це означає невисоку чутливість модельованої системи як до змін ресурсів, так і до вихідних параметрів. Така властивість СЗІ не тільки збільшує кількість прийнятних стратегій при побудові систем захисту, але і дає керівництву невеликий простір для прийняття помилкових рішень без критичних наслідків.

При пошуку оптимального рішення на етапі побудови СЗІ слід зважати на те, що режим сідлової точки, котрий забезпечує деякий гарантований результат при будь-яких діях суперника, існує лише для певних структур і при певних умовах протистояння. Забезпечення існування цього режиму досягається шляхом вибору значень параметрів, котрі визначають вразливість об'єктів. Критерієм вибору робочої точки, котра визначає необхідну кількість ресурсів та їх розподіл між об'єктами, є забезпечення наступних показників: для одностороннього протистояння — мінімум загальних втрат, котрі об'єднують втрати інформації і витрати на її захист, при двосторонньому — максимум загального прибутку, який є сумою прибутку від внесення інвестицій в захист і прибутку від здобуття інформації суперника. Надійність реалізації оптимальної стратегії досягається за рахунок дотримання додаткових вимог: робоча точка повинна знаходитись на деякому віддаленні від межі інтервалу, в якому виконуються зазначені умови, і, крім того, в околі робочої точки не повинні спостерігатись значні зміни оптимального співвідношення ресурсів на об'єктах. Забезпечення наведених умов дозволяє визначити необхідні ресурси, а, зрештою, засоби захисту, що відкриває шлях до побудови оптимальних систем захисту інформації.

Література

1. Лабскер Л.Г. Игровые методы в управлении экономикой и бизнесом /Л.Г. Лабскер, Л.О. Бабешко - М.: Дело, 2001. – 46с.

2. Прус Р.Б. Вибір цільової функції та її вплив на розподіл ресурсів захисту інформації/ Р. Прус// Защита информации. Сборник научных трудов НАУ. – К.: НАУ. – 2009. – №16. – С. 172-175.

3. GordonL.A., LoebM.P., ReturnonInformationSecurityInvestments: Mythsvs. Reality // StrategicFinance. - Nov. 2002, pp. 26-31.

4. ЛевченкоЄ.Г. Умовиіснуваннясідловоїточкивбагаторубіжнихсистемахзахистуінформації/ Є. Левченко, Р. Прус, Д. Рабчун// Безпекаінформації: наук.-практ. журнал, 2013. — №1. — С. 70-76.

5. Шевченко В.Л. Оптимізаційне моделювання в стратегічному плануванні/ В. Шевченко. - К.: ЦВСД НУОУ, 2011.- 283с

Надійшла 21.11.2015 р. Рецензент: д.т.н., проф. Шевченко В.Л.