View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №1, 2011

УДК 004.681

Вербовська Г.В., Левченко Є.Г.

ДИНАМІЧНЕ УПРАВЛІННЯ РЕСУРСАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуто принципи динамічного управління ресурсами захисту інформації, метою якого є досягнення оптимального розміру інвестицій в інформаційну безпеку і оптимального моменту інвестування. Приведено приклад, в якому порівнюються результати попереднього розподілу ресурсів між об'єктами захисту інформації і адаптивного розподілу, коли ресурси вносяться після першого нападу. Проаналізовано умови, при яких доцільно застосовувати адаптивне управління, і ситуації, в яких воно дає найкращі результати.

Вступ. Важливим завданням економічного менеджменту інформаційної безпеки є визначення двох пов'язаних між собою величин: оптимального розміру і розподілу інвестицій y^0 в інформаційній системі і оптимального моменту t^0 інвестування. Існування оптимуму відносно моменту внесення можна пояснити наступними міркуваннями. Затримка в інвестуванні в умовах послідовних атак, звичайно, приведе до певних втрат. Проте попередній розподіл ресурсів, коли ще не проявилась націленість суперника, може виявитись неефективним і привести до ще більших втрат. Тому настає момент t^0, який визначається пороговим значенням i^0 кількості вилученої інформації, при настанні якого стає доцільним виділення певної кількості ресурсів захисту y^0 і певного розподілу $\{y_k^0\}$ їх між об'єктами.

Шукані значення y^0 і t^0 можна знайти з умови досягнення максимуму цільової функції, яка визначає прибуток від внесення інвестицій. Ця величина дорівнює вартості захищеної в результаті внесення інвестицій інформації за відрахуванням втрат на її захист.

Необхідність динамічного (або адаптивного) управління ресурсами інформаційної безпеки обумовлена двома основними причинами:

1) невизначеністю відносно дій суперника, а саме направленістю його зусиль по вилученню інформації і масштабом цих зусиль;

2) зміною з часом як внутрішніх, так і зовнішніх умов протистояння – стану інформаційної системи (вартості інформації і її розподілу між об'єктами),направленості атак суперника, появою нових суперників тощо.

Аналіз джерел. Аналізу поставленої задачі присвячена низка робіт[1-3]. В [1] розглядається антагоністичне протистояння двох сторін у сфері інформаційної безпеки: захисту, який знаходиться у невизначеності щодо дій суперника, і нападу, котрий має певне уявлення про структуру системи захисту і направляє свої зусилля в найслабшу ланку системи безпеки. Розподіл ресурсів захисту на блокування різного типу загроз може вестись як в активному режимі – випереджаючи дії суперника, так і реактивному (адаптивному), з затримкою інвестування, коли захист визначає напрямок атак. Ця модель призначена для ситуації , коли відбуваються численні атаки суперника, причому в результаті кожної атаки вилучається незначна кількість активів. Динаміка протистояння проявляється в тому, що захист, зафіксувавши направленість дій суперника, прагне заблокувати їх.

В [2] використовується модель Гордона-Лоеба [4] і послідовні атаки розглядаються як гаусівський випадковий процес. Розглядають 25 типів загроз, і метою аналізу є визначення оптимальної кількості загроз, на які слід направляти ресурси захисту. Ця величина визначається в динаміці в залежності від параметрів, які характеризують: σ – рівень невизначеності, λ – безповоротні витрати, які знаходяться нижче допустимого рівня i^0; ρ – коефіцієнт кореляції захисту від різних загроз.

В цільову функцію входять параметри, які визначають шукані величини y^0 і t^0: σ – рівень невизначеності, μ – очікуваний темп зростання потенціальних втрат, υ – вразливість інформаційної системи, α – продуктивність інвестицій.

Постановка задачі. Метою дослідження є визначення доцільності застосування динамічного управління ресурсами захисту інформації в інформаційних системах в умовах, які відрізняються загальною кількістю об'єктів і об'єктів, на які здійснюється напад, кількістю атак і розподілом інформації на об'єктах.

Методика розрахунку і результати. В нашому аналізі будемо використовувати введену в [3] цільову функцію, яка визначає кількість вилученої інформації:

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

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

l – кількість об'єктів;

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

$p_k(x,y)$ – імовірність нападу на k -ий об'єкт;

$q_k(x,y)$ - імовірність виділення ресурсів x при нападі на k -ий об'єкт;

$f_k(x,y)$ – частка вилученої інформації з k -го об'єкта.

Залежності $f_k(x,y)$ оберемо у вигляді [3]:

$$f_k(x,y) = \frac{(x/y)^{n_k}}{a_k(x/y)^{n_k} + c_k}.$$

Ці залежності задовольняють двом необхідним умовам: при $x/y \to 0$ $f_k(x,y) \to 0$; при $x/y \to \infty$ $f_k(x,y) \to 1$. Параметри a_k, c_k, n_k, визначають форму залежності для кожного об'єкта.

Розглянемо приклад: кількість об'єктів $l = 20$, напад здійснюється на 2 об'єкти, кількість атак дорівнює 3. Розглядаємо спрощений варіант, коли $p_k(x,y) = 1$ і $p_k(x,y) = 1$. Тоді в силу однаковості об'єктів:

$$I = \sum_{k=1}^{2} g_k * f_k(x,y) = 2g * f(x,y).$$

Залежність $f(x,y)$ оберемо у вигляді:

$$f(x,y) = \frac{x/y}{2(x/y) + 8}.$$

Форма цієї функції залежить від вразливості об'єкта. Параметри в даному випадку вибрані такими, що при $x/y \to 1$ $f(x,y) = 0{,}10$ – це значення вважаємо близьким до реальності, а при $x/y \to \infty$ $f(x,y) \to 0{,}5$, що визначається початковою вразливістю об'єкта. Покладемо Y=1 і Z=$\frac{x}{y}$=2.

Порівняємо два види розподілу: попередній і динамічний.

Попередній:

Ресурси розподіляються порівну між всіма об'єктами, такий розподіл залишається стабільним на протязі всіх трьох атак.

$$y_k = y = \frac{Y}{l} = \frac{1}{20} = 0{,}05; \quad x_k = x = \frac{X}{2} = 1;$$

Втрачена інформація на об'єкті кожен раз поповнюється:

$$I_1 = I_2 = I_3 = 2g * \frac{1/0{,}05}{2/0{,}05 + 8} = 0{,}833g$$

Після трьох атак втрачається інформація:

$$I\ пол = 2{,}49\text{g}$$

Динамічний:

В цьому варіанті ми не встановлюємо захист взагалі перед першою атакою, використовуючи природну захищеність.

1) перша атака:

$x / y \to \infty \quad f(x, y) \to 0{,}5$

$$I_1 = 2g * 0{,}5 = g$$

2) друга атака: $I_2 = 2g * \dfrac{1/0{,}5}{2/0{,}5 + 8} = 2g * 0{,}167 = 0{,}333g$.

3) третя атака: $I_3 = I_2 = 2g * 0{,}167 = 0{,}333g$.

Після трьох нападів втрата інформації становить:

$$I_{дин} = (1 + 0{,}333 + 0{,}333)\text{g} = 1{,}67g$$

Перевага динамічного режиму:

$$I\ пол = 2{,}49g,\ \ I_{дин} = 1{,}67g.$$

Введемо показник ефективності застосування динамічного підходу $E = \dfrac{I_{пол}}{I_{дин}}$.

Одержимо:

$$E = \frac{2{,}49}{1{,}67} = 1{,}491$$

В таблиці 1-6 приведені результати розрахунків ефективності застосування динамічного підходу для чотирьох функцій в умовах, які відрізняються загальною кількістю об'єктів і кількістю атакованих об'єктів, а також кількістю атак.

Таблиця 1. 20 однакових об'єктів, 3 атаки, напад на k об'єктів

$E = \dfrac{I_{пол}}{I_{дин}}$										
№	k / $f(x,y)$	2	3	5	6	8	9	10	14	15
1.	$\dfrac{x/y}{2(x/y)+8}$	1,491	1,381	1,199	1,125	1	0,947	0,9	0,75	0,72
2.	$\dfrac{x/y}{2(x/y)+16}$	1,530	1,337	1,071	0,974	0,824	0,765	0,714	0,564	0,536
3.	$\dfrac{x/y}{3(x/y)+8}$	1,432	1,34	1,212	1,154	1,054	1,01	0,969	0,836	0,808
4.	$\dfrac{(x/y)^2}{2(x/y)^2+8}$	1,485	1,76	1,412	1,376	1,293	1,247	1,2	1,007	0,96

Затінені клітинки відносяться до ситуацій, коли динамічний підхід недоцільний ($E < 1$).

Таблиця 2. 20 однакових об'єктів, 2 атаки, напад на k об'єктів

$E = \frac{I_{non}}{I_{дин}}$										
№	$f(x,y)$ \ k	2	3	4	5	6	10	11	12	15
1.	$\frac{x/y}{2(x/y)+8}$	1,25	1,154	1,071	1	0,938	0,75	0.714	0.682	0,6
2.	$\frac{x/y}{2(x/y)+16}$	1,19	1,042	0,926	0,833	0,758	0,556	0.521	0.49	0,417
3.	$\frac{x/y}{3(x/y)+8}$	1,235	1,167	1,105	1,05	1	0,84	0.808	0.778	0,7
4.	$\frac{(x/y)^2}{2(x/y)^2+8}$	1,32	1,304	2,564	1,255	1,223	1,067	1,024	0,98	0,853

Таблиця 3. 10 однакових об’єктів, 3 атаки, напад на k об’єктів

$E = \frac{I_{non}}{I_{дин}}$						
№	$f(x,y)$ \ k	2	3	4	5	7
1.	$\frac{x/y}{2(x/y)+8}$	1,286	1,125	1	0,9	0,75
2.	$\frac{x/y}{2(x/y)+16}$	1,19	0,974	0,824	0,714	0.564
3.	$\frac{x/y}{3(x/y)+8}$	1,275	1.154	1,054	0,969	0.836
4.	$\frac{(x/y)^2}{2(x/y)^2+8}$	1,442	1,376	1,293	1,2	1,007

Таблиця 4. 5 однакових об’єктів, 3 атаки, напад на k об’єктів

$E = \frac{I_{non}}{I_{дин}}$				
№	$f(x,y)$ \ k	2	3	4
1.	$\frac{x/y}{2(x/y)+8}$	1	0,818	0.692
2.	$\frac{x/y}{2(x/y)+16}$	0,824	0,63	0.51
3.	$\frac{x/y}{3(x/y)+8}$	1,05	0,897	0.782
4.	$\frac{(x/y)^2}{2(x/y)^2+8}$	1,293	1,103	0,915

В таблицях 2-4 представлені результати розрахунків при зміні загальної кількості об’єктів і кількості атак. З приведених результатів можна зробити наступні висновки: при збільшенні кількості атак динамічний підхід є більш ефективним, про що свідчить збільшення граничної кількості об’єктів, при яких доцільно використовувати динамічний підхід. При зменшенні загальної кількості об’єктів ефективність динамічного підходу

зменшується, що проявляється у зменшенні граничної кількості об'єктів – в нашому випадку: з 8 до 4 для функції 1, з 5 до 2 для функції 2, з 9 до 4 для функції 3, з 14 до 7 для функції 7 (при загальній кількості об'єктів 20 і 10 відповідно). В системі з 5 об'єктів динамічний підхід доцільно використовувати тільки у випадку функції 4.

Ми розраховували варіанти протистояння при умові наявності на всіх об'єктах однакової кількості інформації. Тому для зловмисника всі цілі були рівнозначні. Розглянемо тепер випадок, коли система має різні об'єкти.

Нехай система складається з 10 об'єктів, причому інформація розподіляється таким чином: $g_1 = 0{,}3,\ g_2 = 0{,}2,\ g_k = 0{,}0625$ ($k = \overline{3{,}10}$), вся інформація $g = 1$. Напад здійснюється на 2 об'єкти. Вибираємо варіант, найгірший для захисту – коли зловмисник нападе на об'єкти g_1 та g_2, де міститься половина всієї інформації. Порівнюємо два види розподілу. Умови попереднього розподілу залишаються незмінними – порівну між всіма об'єктами на протязі всіх трьох атак. Динамічний розподіл має декілька варіантів, в яких перед першою атакою вносимо інвестиції в розмірі: 1) 0%; 2) 50%; 3) 30%; 4) 20%. Іншу частину коштів вносимо після першої атаки і розподіляємо між двома об'єктами пропорційно кількості інформації. Результати показані в таблиці 5.

Таблиця 5. 10 різних об'єктів, 3 атаки, напад на 2 об'єкти

$E = \frac{I_{non}}{I_{дин}}$					
№	$f(x,y)$ \ k	Варіант 1	Варіант 2	Варіант 3	Варіант 4
1.	$\frac{x/y}{2(x/y)+8}$	1,29	1,175	1,247	1,27
2.	$\frac{x/y}{2(x/y)+16}$	1,193	1,212	1,254	1,249
3.	$\frac{x/y}{3(x/y)+8}$	1,281	1,144	1,215	1,242
4.	$\frac{(x/y)^2}{2(x/y)^2+8}$	1,457	1,126	1,249	1,317

Таблиця 6. 10 різних об'єктів, 2 атаки, напад на 2 об'єкти

$E = \frac{I_{non}}{I_{дин}}$					
№	$f(x,y)$ \ k	Варіант 1	Варіант 2	Варіант 3	Варіант 4
1.	$\frac{x/y}{2(x/y)+8}$	1.074	1.076	1.094	1.093
2.	$\frac{x/y}{2(x/y)+16}$	0.927	1.064	1.041	1.012
3.	$\frac{x/y}{3(x/y)+8}$	1.109	1.069	1.098	1.105
4.	$\frac{(x/y)^2}{2(x/y)^2+8}$	1.291	1.083	1.164	1.206

З таблиць 5 та 6 робимо висновки:

- При наявності різних об'єктів і здійсненні трьох атак динамічний підхід доцільно використовувати. Коли вразливість системи описується функціями 1,3,4

раціональніше застосовувати перший варіант динамічного підходу. У випадку другої функції найкращий результат дає третій варіант.

- Таблиця 6 підтверджує той факт, що при невеликій кількості атак (в нашому випадку 2) динамічний підхід не є доцільним (затінена клітинка в таблиці) або дає результати, що відповідають попередньому розподілу.

Висновки. Проведені розрахунки дозволяють зробити висновки щодо доцільності використання кожного з двох варіантів розподілу ресурсів – попереднього і динамічного та безпосередньо варіацій розподілу при динамічному підході. Динамічний розподіл має сенс використовувати при виконанні наступних умов:

1) наявність великої кількості об’єктів;
2) невизначеність відносно націленості атак суперника;
3) достатній рівень природної захищеності об’єктів (невелика початкова вразливість);
4) повторюваність атак.

Література

1. Tatsumi Ken-ichi, Goto Makoto, Optimal timing of information security investment: A real options approach. – WEIS July 21, 2009.

2. Böhme, Moor, The iterated weakest link: A model of adaptive security investment. — WEIS, London, 24 June 2009.

3. Левченко Є.Г., Рабчун А.О., Оптимізаційні задачі менеджменту інформаційної безпеки. — НТЖ "Сучасний захист інформації», №1, 2010, с.16-23.

4. Gordon L.A., Loeb M.P., The economics of information security investment. – ACM transactions on information and system security, 5(2002), p.438-457.

Надійшла: 10.03.11

Рецензент: д.т.н., проф. Дудикевич В.Б.