УДК 004.681
© В. Дудикевич[1], В. Іванюк[1], І. Прокопишин[1,2] , 2014

ЕФЕКТИВНІСТЬ ІНВЕСТИЦІЙ У СИСТЕМИ ЗАХИСТУ ПРИМІЩЕНЬ ВІД ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ

Розглянуто дискретну ймовірнісну модель економічних втрат для консервативних систем захисту. На основі нерівності Чебишова сформульовано показник ризику та загальний показник економічної ефективності інвестицій у системи захисту. Практичні розрахунки проведено для системи захисту приміщень від витоку мовної інформації.

Discreet probability model of economical looses for conservative security systems are developed. On the base of Chebyshev's inequality risk index and general investment efficiency index are formulated for security systems. Practical calculations are implemented for verbal information leakage protection.

1. ВСТУП

Системи захисту інформації є складними ієрархічними системами, функціонування яких вимагає значних фінансових затрат. Природними критеріями ефективності таких систем є економічні показники, а математичною моделлю ризику – випадкова величина втрат [1-7]. Однак, при цьому виникає проблема вибору адекватної міри ризику, яка була б достатньо повною і одночасно – простою [5-7,12].

У пропонованій роботі, на основі загального підходу до оцінки економічної ефективності консервативних систем захисту [7], розглядається проблема ефективності інвестицій у системи захисту службових приміщень від витоку мовної інформації. Застосовано просту оцінку ризику, побудовану на нерівності Чебишова П. Л., що дозволило провести практичні розрахунки засобами електронних таблиць.

2. ДИСКРЕТНА ЙМОВІРНІСНА МОДЕЛЬ ВТРАТ

Розглянемо структурно-логічну модель консервативної системи захисту, структура та складові якої є незмінними протягом деякого проміжку часу [7].

Система складається з N об’єктів захисту O^1, O^2, K, O^N .

[1] Національний університет "Львівська політехніка",

[2] Львівський національний університет імені Івана Франка

Вразливості є каналами для реалізації загроз – атак. Об'єкт O^i може бути атакований по K_i каналах $V^{i1}, V^{i2}, \text{K}, V^{iK_i}$. Усі атаки є незалежними, відома кількість атак n_{ij} за фіксований проміжок часу. Система захищена M пристроями захисту S^1, S^2, K, S^M. Захист в цілому означимо як об'єкт $\hat{S}$, який описується компонентами s_{mij}, рівними ймовірності злому пристрою захисту S^m при захисті каналу V^{ij}, $m = 1,2,...,M$, $i = 1,2,...,N$, $j = 1,2,..., K_i$. Якщо пристрій S^m не захищає канал V^{ij}, тоді $s_{mij} = 1$.

Економічні збитки від вдалої атаки на об'єкт O^i по каналу V^{ij} позначимо w_{ij}. Припустимо, що втрати від можливого ушкодження засобів захисту – незначні. Тоді випадкова величина (в.в.) економічних втрат, зумовлених атаками, буде дорівнювати [7]:

$$\widetilde{W} = \sum_{i=1}^{N} \sum_{j=1}^{K_i} w_{ij} Bin(n_{ij}, r_{ij}), \qquad (1)$$

де $r_{ij} = \prod_{m=1}^{M} s_{mij}$ – ймовірність злому по каналу V^{ij}, n_{ij} – кількість можливих атак по цьому каналу, $Bin(n_{ij}, r_{ij})$ – випадкова величина, яка має біноміальний розподіл [8].

Для математичного сподівання та дисперсії в.в. втрат отримаємо:

$$M(\widetilde{W}) = \sum_{i=1}^{N} \sum_{j=1}^{K_i} w_{ij} r_{ij} n_{ij} \ , \qquad (2)$$

$$D(\widetilde{W}) = \sigma^2(\widetilde{W}) = \sum_{i=1}^{N} \sum_{j=1}^{K_i} w_{ij}^2 r_{ij} (1 - r_{ij}) n_{ij} < +\infty \qquad (3)$$

3. ПОКАЗНИК ЕФЕКТИВНОСТІ ІНВЕСТИЦІЙ

Для описаної в.в. втрат $\widetilde{W}$ виконується нерівність Чебишова П. Л. [8]:

$$\forall\ z > 0\ P\{|\widetilde{W} - M(\widetilde{W})| \geq z\} \leq D(\widetilde{W}) / z^2, \qquad (4)$$

з якої отримуємо таку нерівність:

$$\forall\ k>0\ P\{\widetilde{W} < M(\widetilde{W}) + k\sigma(\widetilde{W})\} \geq 1 - 1/k^2 . \quad (5)$$

Величину

$$VaR_{k\sigma} = M(\widetilde{W}) + k\sigma(\widetilde{W}), \quad (6)$$

яка визначає максимальні втрати з надійністю $1-1/k^2$, називають $k\sigma$-вартістю ризику. Вона задовольняє аксіоми позитивної однорідності; інваріантності відносно зсуву та субадитивності, які характеризують когерентні міри ризику [12].

Впровадження чи модернізацію системи захисту будемо розглядати як інвестиційний проект на T років. Впровадження засобу захисту S^m потребує капіталовкладень у розмірі P_m та річних витрат на обслуговування у розмірі C_m. Витрати на обслуговування та випадкові втрати від можливих атак віднесемо на кінець року $\widetilde{\mathrm{W}}(\hat{S})$. Тоді в.в. чистої теперішньої вартості (ЧТВ) сумарних витрат дорівнює:

$$NPV(\hat{S}) = \sum_{m=1}^{M} P_m(S^m) + \frac{1-(1+r)^{-T}}{r} \sum_{m=1}^{M} C_m(S^m) + \sum_{t=1}^{T} \frac{\widetilde{\mathrm{W}}(\hat{S})}{(1+r)^t}, \quad (7)$$

де r – необхідна процентна ставка.

У формулі (7) перший доданок – сумарні капітальні затрати на систему захисту, другий доданок – теперішня вартість обслуговування, а третій доданок – теперішня вартість в.в. втрат.

За показник ефективності візьмемо $k\sigma$-вартість ризику (6):

$$VaR_{k\sigma}(NPV) = \sum_{m=1}^{M} P_m + \frac{1-(1+r)^{-T}}{r}\left(\sum_{m=1}^{M} C_m + M(\widetilde{\mathrm{W}})\right) + k\left(\frac{1-(1+2r+r^2)^{-T}}{2r+r^2} D(\widetilde{\mathrm{W}})\right)^{\frac{1}{2}}.$$

4. РОЗРАХУНОК ЕФЕКТИВНОСТІ ЗАХИСТУ ВІД ВИТОКУ МОВНОЇ ІНФОРМАЦІЇ

Витік мовної інформації з службових приміщень здійснюється головним чином по аудіоканалу та провідними лініями телефонного зв'язку або інших комунікацій [9-11].

Виділимо такі об'єкти захисту:

O^1 – мовна інформація, відмінна від телефонних розмов (ВІ);

O^2 – телефонні розмови (ТР).

Вкажемо основні канали можливого витоку аудіоінформації:

V^{11} – радіомікрофони;

V^{12} – будівельні конструкції – стіни, підлога, стеля, вікна, система опалення.

V^{13} – електромережа;

V^{14} – охоронно-пожежна сигналізація;

V^{15} – телефонна лінія – виносний мікрофон;

V^{16} – телефонна лінія – мікрофонний ефект та високочастотне нав'язування.

Вкажемо основні засоби захисту для захисту витоку інформації по аудіоканалу:

S^1 – пристрій виявлення радіомікрофонів, здійснює захист по каналу 1-1, 2-8;

S^2 – захист витоку аудіоінформації через будівельні конструкції, канал 1-2;

S^3 – фільтр для електромережі, канал 1-3;

S^4 – фільтр для охоронно-пожежної сигналізації, канал 1-4;

S^5 – пасивний фільтр, канал 1-5;

S^6 – активний фільтр, канал 1-6;

S^7 – акустичний зашумлювач, канали 1-1 – 1-6, 2-7, 2-8, 2-9;

S^8 – електромагнітний зашумлювач, канали 1-1, 1-3, 1-4, 1-5, 1-6, 2-8.

Зауважимо, що по аудіоканалу також можна прослуховувати телефонні розмови. В цьому випадку ми отримуємо лише половину інформації. Тому, перераховані нижче канали можливого витоку аудіоінформації та засоби їх захисту, стосуються також телефонних розмов (O^2).

Для другого об'єкта захисту (ТР) вкажемо основні канали можливого витоку інформації:

V^{21}–V^{26} – ідентичні каналам V^{11}–V^{16} ,

та додаткові:

V^{27} – підключення пряме або за допомогою адаптера;

V^{28} – радіозакладки;

V^{29} – витік інформації поза периметром захисту.

Перерахуємо можливі засоби захисту по цих каналах:

S^{11} – пристрій виявлення закладок та під'єднань, здійснює захист по каналах 2-7 та 2-8;

S^{12} – активний зашумлювач, канали 2-7, 2-8, 2-9;

S^{13} – засоби одностороннього зашумлення, канали 2-7, 2-8;

S^{14} – скремблери, канали 2-7, 2-8, 2-9;

S^{15} – шифратори, канали 2-7, 2-8, 2-9;

S^{16} – універсальні пристрої, які можуть також забезпечувати захист по аудіоканалу.

Задамо необхідні вхідні дані. Будемо виходити з того, що вартість повної інформації службового приміщення за рік складає 6 млн. грн. На протязі року у цьому приміщенні відбувається 20 нарад, 10 переговорів та укладається 6 угод.

Припускаємо, що одна атака – це не виявлене прослуховування протягом одного тижня.

Необхідні дані, які отримали з джерел [9-11], мережі Internet та шляхом експертних оцінок, подано у наступних таблицях.

Об'єкти захисту та канали захисту, в цілому, описано вище. Для кожного каналу V^{ij} необхідно задати кількість можливих атак n_{ij} та вартість втрат w_{ij} при його зломі. Ці величини подано у таблиці 1.

Засоби захисту описуються капітальними та поточними річними затратами, номерами каналів, які вони захищають, та ймовірністю їх злому. Відповідні величини для ряду засобів захисту подано нижче у таблиці 2.

Таблиця 1

Опис загроз для об'єктів захисту O^1 (ВІ) та O^2 (ТР)

Номер об'єкта захисту *i*	Номер каналу *j*	Позначення каналу *i-j*	Кількість можливих атак по каналу за рік n_{ij}	Можливі втрати від однієї вдалої атаки w_{ij}, тис. грн.
1	1	1-1	5	200
1	2	1-2	10	200
1	3	1-3	5	200
1	4	1-4	3	200
1	5	1-5	3	200
1	6	1-6	5	200
2	1	2-1	5	40
2	2	2-2	10	40
2	3	2-3	5	40
2	4	2-4	3	40
2	5	2-5	3	40
2	6	2-6	5	40
2	7	2-7	5	20
2	8	2-8	5	20
2	9	2-9	20	20

Таблиця 2

Опис засобів захисту

Номер захисту m	Ціна P_m, тис. грн.	Річна вартість обслуговування C_m, тис. грн.	Канал захисту ij – ймовірність відмови s_{mij}
1	18,0	0,5	11 – 0,005; 28 –0,01
2	300,0	5,0	11 – 0,005; 13 – 0,01; 14– 0,01; 15 – 0,01; 16– 0,01; 27 – 0,01; 28 – 0,01
3	9,0	0,5	11 – 0,01; 28 –0,015
4	3,5	0,5	12 – 0,02
5	8,5	0,5	12 – 0,01
6	3,3	0,1	13 – 0,02
7	1,9	0,1	14 – 0,01
8	0,4	0,1	15 – 0,01
9	4,0	0,2	16 – 0,01; 27 – 0,01
10	4,0	0,4	11 – 0,1; 12 – 0,1; 13 – 0,1; 14 – 0,1; 15 – 0,1;16 – 0,1
11	4,5	0,4	11 – 0,1; 13 – 0,1; 14 – 0,1; 16 – 0,1; 28 – 0,1
12	5,0	0,4	11 – 0,1; 13 – 0,1; 14 – 0,1; 16 – 0,1; 28 – 0,1
13	19,0	5,0	13 – 0,05; 14 – 0,05; 15 – 0,05; 16 – 0,05; 27 – 0,05; 28 – 0,05
14	144,0	5,0	13 – 0,01; 14 – 0,01; 15 – 0,01; 16 – 0,01; 27 – 0,01; 28 – 0,01
15	1,8	0,1	27 – 0,1; 28 – 0,1
16	7,0	0,1	27 – 0,1; 28 – 0,1
17	1,5	0,1	27 – 0,1; 28 – 0,1;29 – 0,1
18	0,55	0,1	27 – 0,1; 28 – 0,1; 29 – 0,1
19	2,5	0,2	16 – 0,05; 27 – 0,05; 28 – 0,05; 29 – 0,05

За допомогою електронних таблиць проведено розрахунки для трьох профілів захисту (ПЗ):
ПЗ 1: засоби захисту 1, 4, 6, 7, 8, 9, 10, 11, 13, 19; ПЗ 2: засоби захисту 1, 4, 6, 7, 8, 9, 10, 13, 17; ПЗ 3: засоби захисту 2, 5, 6, 7, 8, 9, 10, 13, 18.

Топологію захисту задавали матрицями ймовірностей злому захисту для кожного об'єкта захисту. Для профілю захисту ПЗ 1, у таблиці 3 наведено таку матрицю з елементами s_{m1j}.

Такий підхід хоча і дещо громіздкий, але не потребує графічного зображення системи захисту. За допомогою матриць ймовірностей легко встановити, які канали є незахищеними або захищені надмірно, які засоби захисту – не задіяні.

Таблиця 3

Матриця ймовірностей злому засобів захисту для об'єкта захисту O^1 (BI)

Номер захисту, *m*	Номер каналу атаки, *ij*					
	11	12	13	14	15	16
1	0,005	1,000	1,000	1,000	1,000	1,000
2	1,000	1,000	1,000	1,000	1,000	1,000
3	1,000	1,000	1,000	1,000	1,000	1,000
4	1,000	0,020	1,000	1,000	1,000	1,000
5	1,000	1,000	1,000	1,000	1,000	1,000
6	1,000	1,000	0,020	1,000	1,000	0,010
7	1,000	1,000	1,000	0,010	1,000	1,000
8	1,000	1,000	1,000	1,000	0,010	1,000
9	1,000	1,000	1,000	1,000	1,000	0,010
10	0,100	0,100	0,100	0,100	0,100	0,100
11	0,100	1,000	0,100	0,100	1,000	0,100
12	1,000	1,000	1,000	1,000	1,000	1,000
13	1,000	1,000	0,050	0,050	0,050	0,050
14	1,000	1,000	1,000	1,000	1,000	1,000
15	1,000	1,000	1,000	1,000	1,000	1,000
16	1,000	1,000	1,000	1,000	1,000	1,000
17	1,000	1,000	1,000	1,000	1,000	1,000
18	1,000	1,000	1,000	1,000	1,000	1,000
19	1,000	1,000	1,000	1,000	1,000	0,050

У таблиці 4 для трьох профілів захисту наведено результати розрахунку чотирьох показників:

1) ЧТВ загальних інвестиційних витрат – $NPV(\overline{P}) + NPV(\overline{C})$;

2) Математичне сподівання ЧТВ випадкових втрат – $M(NPV(\widetilde{W}))$;

3) Середньо квадратичне відхилення (с.к.в.) ЧТВ випадкових втрат – $\sigma(NPV(\widetilde{W}))$;

4) Показник ризику "три сигма" (6) – $VaR_{3\sigma}(NPV)$.

Таблиця 4

Економічні показники профілів захисту (тис. грн.).

Про-філь	$NPV(\overline{P}) + NPV(\overline{C})$	$M(NPV(\widetilde{W}))$	$\sigma(NPV(\widetilde{W}))$	$VaR_{3\sigma}$
1	89,531	94,423	59,943	363,782
2	82,136	172,866	69,941	464,825
3	400,360	163,03	60,230	744,072

З наведеної таблиці видно, що профіль захисту ПЗ 2 є дешевшим у порівнянні з профілем ПЗ 1, але має більші математичне сподівання та с.к.в. втрат, тому – у результаті – більше значення показника ризику "три сигми". Профіль ПЗ 3 забезпечує менші випадкові втрати, але за рахунок великих капіталовкладень має значний результуючий показник.

5. ВИСНОВКИ

Розвинуто дискретну ймовірнісну модель втрат для консервативних систем захисту. На основі нерівності Чебишова сформульовано простий показник ризику та загальний показник економічної ефективності інвестицій у системи захисту, що дозволяє проводити практичні розрахунки засобами електронних таблиць. Практичні розрахунки, проведені для системи захисту службових приміщень від витоку мовної інформації, показали ефективність запропонованої методики для вибору оптимального профілю захисту.

1. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / С.А. Петренко, С.В. Симонов. – М.: Компания АйТи; ДМК Пресс, 2004. – 384 с. 2. Антонюк А. А. Задача оптимального выбора функционального профиля защищенности / А. А. Антонюк, Д. С. Берестов, С. Н. Пустовит, В. П. Шилин // Захист інформації. – 2005. –

Спец. вип. – С. 11-14. 3. Степанов А.В. Характерные особенности задачи построения комплексной системы защиты информации распределенных корпоративных ресурсов / А.В. Степанов // Захист інформації. – 2007. – Спец. вип. – С. 131-134. 4. Егоров Ф. И. Задачи защиты информации / Ф. И. Егоров, Е. О. Тискина, В. А. Хорошко // Захист інформації. – 2009. – № 1. – С. 5-12. 5. Дудикевич Я. В. Економічна ефективність та оптимізація систем захисту інформації з урахуванням вартості ризику втрати інформації / Я. В. Дудикевич, І. А. Прокопишин // Інформаційна безпека / Матеріали науково-практичної конференції, Київ, 26-27 березня 2009 р. – Київ, ДУІКТ, 2009. 6. Дудикевич В. Б. Оцінка вартості ризику для систем захисту інформації / В. Б. Дудикевич, Ю. В. Лах, І. А. Прокопишин // Інформаційна безпека. – 2011, № 1(5). – С. 44-49. 7. Дудикевич В. Б. Проблеми оцінки ефективності систем захисту / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник НУ "Львівська політехніка". – 2012 – № 741. Автоматика, вимірювання та керування. – С. 118-122. 8. Вентцель Е. С. Теория вероятности и ее инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – Л.: Наука, 1988. – 480 с. 9. Дудикевич В. Б. Захист засобів і каналів телефонного зв'язку / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Львів: Вид-во Львів. політехніки, 2012. – 212 с. 10. Защита информации техническими средствами: Учебное пособие / Под ред. Ю. Ф. Каторина – СПб: НИУ ИТМО, 2012. – 416 с. 11. Методы и средства защиты информации: В 2-х т. / Под ред. В.А. Хорошко. – Т.2. Информационная безопасность. – К.: Арий, 2008. – 344 с. 12. Artzner P. Coherent measures of risk / P. Artzner, F. Delbaen, J.-M. Eber, D. Heath // Mathematical Finance. – 1999. – V.9, N 3. – P.203–227.