УДК 004.681

В.Б. Дудикевич[1], І.А. Прокопишин[1,2], В.Ф. Чекурін[1,3],
[1] Національний університет "Львівська політехніка",
[2] Львівський національний університет імені Івана Франка,
[3] Інститут прикладних проблем механіки та математики ім. Я.С. Підстригача НАН України

ПРОБЛЕМИ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ

Для консервативних систем захисту розроблено дискретну ймовірнісну модель економічних втрат. На її основі сформульовано ймовірнісні та економічні показники ефективності систем захисту та розглянуто основні проблеми їх розрахунку.

Ключові слова: системи захисту, оцінка ризику, ефективність.

PROBLEMS OF EFFICIENCY ESTIMATION OF SECURITY SYSTEMS

Discreet probability model of economical looses for conservative security systems are developed. On the base probability and economics efficiency indexes for security systems are formulated and main problems of estimating of the indexes are discussed.

Keywords: security systems, risk estimation, efficiency.

Вступ

Оцінка ефективності систем захисту (СЗ) актуальна для порівняльного аналізу та оптимізації цих систем. Серед показників ефективності СЗ, насамперед, виділяють ймовірнісні показники, які описують надійність, та економічні, що оцінюють можливі економічні збитки та витрати [1-5].

Такі класичні міри ризику, як математичне сподівання та середньоквадратичне відхилення втрат, для оцінки ефективності та оптимізації систем захисту інформації використано у роботах [1-4].

У праці [5] запропонована методика оцінки ризику для систем захисту інформації з використанням мір ризику VaR (Value at Risk). та CVaR (Conditional Value at Risk). У пропонованій роботі ця ідея отримала дальший розвиток для консервативних СЗ, структура та складові частини яких не змінюються протягом тривалого проміжку часу. На основі запропонованого структурно-логічного опису таких систем розроблено дискретну ймовірнісну модель економічних втрат зумовлених можливими атаками. Для цієї моделі записано формулу для ймовірності не ушкодження жодного з об'єктів захисту. З використанням вартісних мір ризику VaR та CVaR також сформульовано економічні показники ефективності СЗ та розглянуто проблеми їх розрахунку.

Дискретна ймовірнісна модель втрат, зумовлених атаками

Розглянемо деяку консервативну СЗ, структура та складові якої є незмінними протягом фіксованого проміжку часу.

Система складається з N об'єктів захисту $O^1, O^2, \ldots, O^N$ (Рис. 1). Вразливості є каналами для реалізації загроз – атак. Об'єкт O^i може бути атакований по K_i каналах $V^{i1}, V^{i2}, \ldots, V^{iK_i}$. Припустимо, що всі атаки є незалежними.

Розгляд розпочнемо з найпростіших випадків, які виникають при захисті одного об'єкта, поступово ускладнюючи структуру системи захисту.

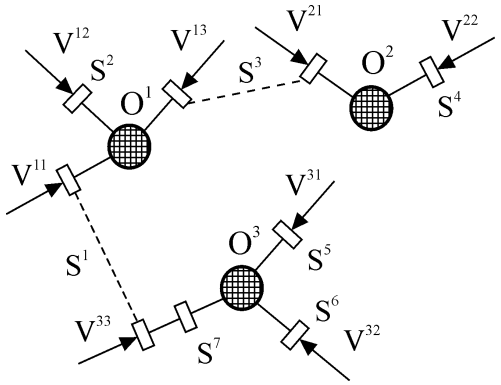

Рис. 1. Структурна схема системи захисту

Один канал для атак з одним пристроєм захисту. Об'єкт захисту має лише один канал для атак, який захищено одним пристроєм захисту з ймовірністю злому $0 < p < 1$ (Рис. 2).

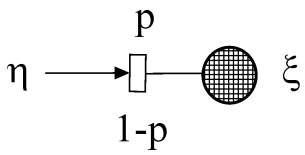

Рис. 2.Випадок одного каналу атаки.

Спочатку припустимо, що на протязі визначеного проміжку часу передбачається лише одна атака. Введемо бінарну випадкову величину (в. в.) ξ, яка приймає значення "1", коли об'єкт ушкоджено, і значення "0" – у протилежному випадку. Очевидно, що вона описується так: $P\{\xi = 0\} = 1 - p$; $P\{\xi = 1\} = p$.

Далі припустимо, що за фіксований проміжок часу на об'єкт здійснюється n послідовних атак. Тоді в. в. кількості ушкоджень об'єкта ξ буде дорівнювати сумі бінарних величин описаних вище. Вона матиме біноміальний розподіл [6]:

$$\xi \sim Bin(n, p), \tag{1}$$

і прийматиме значення $i \in \{0,1,\ldots,n\}$ з ймовірністю $C_n^i p^i (1-p)^{n-i}$, де $C_n^i = \dfrac{n!}{i!(n-i)!}$ – біноміальні коефіцієнти.

Позначимо функцію розподілу в. в. (1) через $F_{Bin(n,p)}(x)$. Додатково означимо, що величина $Bin(0, p)$ є детермінованою величиною, яка з ймовірністю один дорівнює нулю.

Тепер розглянемо найскладніший випадок, коли кількість атак на протязі вказаного проміжку часу є дискретно розподіленою в. в η, яка приймає цілі значення $0 \le n_l$ з ймовірністю $0 < q_l < 1$, $l = 1,2,...,L$, $L \ge 2$, $\sum_{l=1}^{L} q_l = 1$. Тоді, функція розподілу $F_\xi(x)$ в. в. кількості ушкоджень об'єкта ξ буде визначатися ймовірнісною сумішшю розподілів [6]:

$$F_\xi(x) = \sum_{l=1}^{L} q_l F_{Bin(n_l,p)}(x). \tag{2}$$

Математичне сподівання та дисперсія цієї величини відповідно дорівнюють:

$$M(\xi) = p\sum_{l=1}^{L} q_l n_l,\ D(\xi) = \sum_{l=1}^{L} q_l [n_l(n_l - 1)p^2 + n_l p] - M^2(\xi). \tag{3}$$

Один канал для атак з кількома пристроями захисту. Послідовно встановлені M пристроїв захисту з ймовірністю злому p_m, за ряду спрощуючих припущень, можна розглядати як один пристрій з ймовірністю злому:

$$p = \prod_{m=1}^{M} p_m \,. \tag{4}$$

Кілька каналів для атак. Об'єкт O^i може бути атакований по K^i каналах (Рис. 3). У загальному випадку в. в. кількості ушкоджень об'єкта ξ_i буде дорівнювати сумі відповідних випадкових величин:

$$\xi_i \sim \sum_{j=1}^{K_i} \xi_{ij} \,, \tag{5}$$

функції розподілу яких визначаються відповідно до формули (2) так:

$$F_{\xi_{ij}}(x) = \sum_{l=1}^{L_{ij}} q_{ijl} F_{Bin(n_{ijl}, p_{ij})}(x) \,, \tag{6}$$

де параметри $0 \le n_{ijl}$ та $0 < q_{ijl} < 1$ ($l = 1,2,...,L_{ij}$, $\sum_{l=1}^{L_{ij}} q_{ijl} = 1$) описують дискретно розподілені в. в. кількості атак на об'єкт O^i по каналу $V^{ij} - \eta_{ij}$.

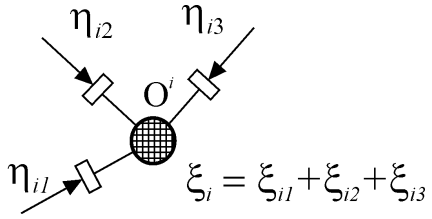

Рис. 3. Випадок кількох каналів атаки.

У спрощеному випадку, коли відома можлива кількість атак n_{ij} по каналу V^{ij}, отримаємо:

$$\xi_i \sim \sum_{j}^{K_i} Bin\,(n_{ij}, p_{ij}) \,. \tag{7}$$

Загальна система захисту. Повернемось до розгляду СЗ у цілому. Нехай ця система складається з N об'єктів захисту та має M пристроїв захисту $S^1, S^2, \ldots, S^M$ (рис.1).

Захист зручно описати "тензорним" об'єктом третього рангу $\hat{S}$ з компонентами s_{mij}, рівними ймовірності злому захисту S^m при захисті каналу V^{ij}, $m = 1,2,...,M$, $i = 1,2,...,N$, $j = 1,2,..., K_i$. Зрозуміло, що коли захист S^m не захищає канал V^{ij}, тоді $s_{mij} = 1$. Ймовірність злому по каналу V^{ij} відповідно до формули (4) буде дорівнювати:

$$p_{ij} = \prod_{m=1}^{M} s_{mij} \,. \tag{8}$$

Нехай w_i – величина можливих економічних збитків від вдалої атаки на об'єкт O^i. Припустимо, що втрати від можливого ушкодження засобів захисту – незначні. Тоді в.в. економічних втрат зумовлених атаками буде дорівнювати:

$$\tilde{W} = \sum_{i=1}^{N} w_i \xi_i \ , \tag{9}$$

де в. в. ξ_i кількість ушкоджень об'єкта O^i, яка визначається формулою (5).

Оцінка ефективності системи захисту

Розглянута дискретна ймовірнісна модель атак і зумовлених ними втрат є основою для побудови показників ефективності СЗ. Для спрощення викладу припустимо, що кількість можливих атак n_{ij} по каналу V^{ij} – відома. Тоді в. в. економічних втрат, зумовлених атаками, буде дорівнювати:

$$\tilde{W} = \sum_{i=1}^{N} w_i \sum_{j=1}^{K_i} Bin(p_{ij}, n_{ij}) \, . \tag{10}$$

Насамперед зазначимо, що ймовірність ситуації, коли жодний з об'єктів захисту не буде ушкоджений, дорівнює:

$$Q(\tilde{W}) = P\{\tilde{W} = 0\} = \prod_{i=1}^{N} \prod_{j=1}^{K_i} \left(1 - p_{ij}\right)^{n_{ij}} \ . \tag{11}$$

Ця величина характеризує абсолютну надійність СЗ і є одним з показників її ефективності [4].

Важливими показниками є математичне сподівання та дисперсія в. в. втрат :

$$E(\tilde{W}) = \sum_{i=1}^{N} w_i \sum_{j=1}^{K_i} p_{ij} n_{ij} \ , \tag{12}$$

$$D(\tilde{W}) = \sum_{i=1}^{N} w_i \sum_{j=1}^{K_i} p_{ij}(1 - p_{ij}) n_{ij} \ . \tag{13}$$

Вони дозволяють оцінити середні економічні втрати та можливе відхилення від них.

У сучасному фінансовому ризик-менеджменті ефективно використовують міри ризику Value at Risk (VaR) та Conditional Value at Risk (CVaR) [7]:

$$VaR_\alpha(\tilde{W}) = \sup\left\{x \,|\, P\{\tilde{W} < x\} \le \alpha\right\}, \tag{14}$$

$$CVaR_\alpha(\tilde{W}) = E\left\{\tilde{W} \,|\, \tilde{W} \ge VaR_\alpha(\tilde{W})\right\}. \tag{15}$$

Перша з них описує втрати, які не будуть перевищені з ймовірністю α, а друга – математичне сподівання втрат, якщо вони будуть більші попередньої величини.

Якщо абстрагуватися від вартості засобів захисту, то величини (12), (14), (15) будуть абсолютними показниками економічної ефективності СЗ.

Більш загальний підхід, який враховує капіталовкладення та вартість обслуговування СЗ запропоновано у працях [2,5,8].

У цьому випадку впровадження чи модернізація системи захисту розглядається як інвестиційний проект на T років. Припускається, що впровадження захисту S^m вимагає капіталовкладень у розмірі P_m та річних витрат на обслуговування у розмірі C_m. Річні витрати на обслуговування та випадкові втрати зумовлені атаками віднесено на кінець року. Тоді, в. в. чистої теперішньої вартості сумарних затрат (Net Present Value – NPV) буде дорівнювати [10]:

$$NPV(\hat{S}) = \sum_{m=1}^{M} P_m(S^m) + PVIFA_{i_0,T}\left(\sum_{m=1}^{M} C_m(S^m) + \tilde{W}(\hat{S})\right), \tag{16}$$

де $PVIFA_{i_0,T} = (1-(1+i_0)^{-T})/i_0$ – процентний фактор теперішньої вартості ренти постнумерандо, i_0 – необхідна процентна ставка. На її основі легко розрахувати показники ефективності (12), (14), (15).

Методика розрахунку величин VaR та CVaR для дискретно розподілених в. в. описана у роботах [8,9]. Такий розрахунок може мати значну обчислювальну складність, оскільки кількість станів L в. в. втрат (10) оцінюється величиною:

$$L \sim \prod_{i=1}^{N} \prod_{j=1}^{K_i} \left(n_{ij}+1\right). \qquad (17)$$

У праці [9] з використанням спрощеної моделі наведено результати практичних розрахунків для системи захисту корпоративної інформаційної системи, яка використовує 15 засобів захисту.

Приведені показники ефективності можуть бути використані як критерії або обмеження при формулюванні задач оптимізації СЗ, ряд таких формулювань дано у працях [1-5,8].

Висновки

Проведене дослідження дозволяє сформулювати основні задачі, вирішення яких необхідне для оцінки ефективності систем захисту:

1) Загальний структурно-логічний опис системи захисту, який включає об’єкти захисту, вразливості – канали атак, засоби захисту.

2) Оцінка економічних втрат від злому засобів захисту та ушкодження об’єктів захисту.

3) Статистичний опис можливих атак.

4) Оцінка вартісних параметрів засобів захисту, статистична оцінка їх надійності.

5) Побудова ймовірнісної моделі втрат, зумовлених атаками, а також загальної моделі витрат.

6) Вибір показників ефективності та розробка методів їх розрахунку.

1. 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. 2. Петренко С. А. Обоснование инвестиций в безопасность / С. А. Петренко, Е. М. Терехова // Научно-технический журнал "Защита информации. INSIDE". – 2005. – № 1. – С.49-53. 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. – С. 80-84. 6. Вентцель Е. С. Теория вероятностей и ее инженерные приложения / Е. С. Вентцель, Л. А. Овчаров. – М.: Высш. шк., 2000. – 480 с. 7. Энциклопедия финансового риск-менеджмента / Под ред. А.А.Лобанова и А.В.Чугунова. – 3-е изд. – М.: Альпина Бизнес Букс, 2007. – 878 с. 8. Дудикевич Я. В. Вартісні міри ризику та їх застосування до оптимізації інвестицій у системи захисту / Я. В. Дудикевич, І. А. Прокопишин // Системи обробки інформації. – 2010. – Вип. 3(84). – С.24-27. 9. 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. 10. Четыркин Е.М. Финансовая математика / Е. М. Четыркин. – М.: Дело, 2004. – 400 с.