

В.Б. Дудикевич¹, 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

© Дудикевич В.Б., Прокопишин І.А., Чекурін В.Ф., 2012

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.

Discreet probability model of economical losses 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.

Key words: 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 міри ризику VaR (Value at Risk) та CVaR (Conditional Value at Risk). У пропонуваній роботі цю ідею розвинуто 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 неушкодження 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, \dots, O^N (рис. 1). Вразливості є каналами для реалізації загроз – атак. Об'єкт O^i може бути атакований по K_i каналах $V^{i1}, V^{i2}, \dots, V^{iK_i}$. Припустимо, що всі атаки є незалежними.

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

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).

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

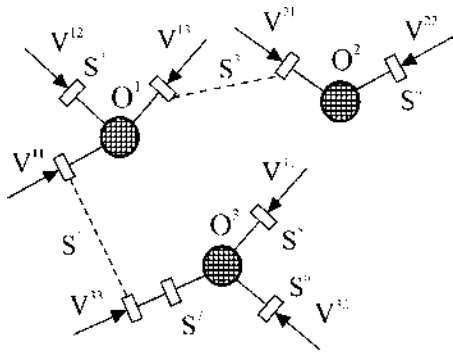


Рис. 1. Структурна схема системи захисту

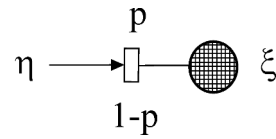


Рис. 2. Випадок одного каналу атаки

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

$$x \sim Bin(n, p), \quad (1)$$

і набуватиме значення $i \in \{0, 1, \dots, n\}$ з ймовірністю $C_n^i p^i (1-p)^{n-i}$, де $C_n^i = \frac{n!}{i!(n-i)!}$ – 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 упродовж вказаного проміжку часу є дискретно розподіленою в. в. h , яка набуває цілих значень $0 \leq n_l$ з ймовірністю $0 < q_l < 1$,

$l = 1, 2, \dots, L$, $L \geq 2$, $\sum_{l=1}^L q_l = 1$. Тоді функція розподілу $F_X(x)$ в. в. кількості ушкоджень об'єкта x визначатиметься ймовірнісною сумішшю розподілів [6]:

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

Математичне сподівання та дисперсія цієї величини відповідно дорівнюють:

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

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

$$p = \prod_{m=1}^M p_m. \quad (4)$$

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 x_i дорівнюватиме сумі відповідних випадкових величин:

$$x_i \sim \sum_{j=1}^{K_i} x_{ij}, \quad (5)$$

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

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

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

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

$$x_i \sim \sum_j^{K_i} \text{Bin}(n_{ij}, p_{ij}). \quad (7)$$

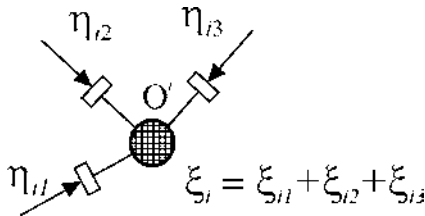


Рис. 3. Випадок кількох каналів атаки

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

Захист зручно описати "тензорним" об'єктом третього рангу \hat{S} з компонентами s_{mij} , що дорівнюють ймовірності злому захисту S^m при захисті каналу V^{ij} , $m=1,2,\dots,M$, $i=1,2,\dots,N$, $j=1,2,\dots,K_i$. 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) дорівнюватиме:

$$p_{ij} = \prod_{m=1}^M s_{mij}. \quad (8)$$

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, дорівнюватиме:

$$\tilde{W} = \sum_{i=1}^N w_i x_i, \quad (9)$$

де в. в. x_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, дорівнюватиме:

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

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

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

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

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

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

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

Вони дають змогу 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]:

$$VaR_a(\tilde{W}) = \sup \{ x \mid P\{\tilde{W} < x\} \leq a \} , \quad (14)$$

$$CVaR_a(\tilde{W}) = E\{\tilde{W} \mid \tilde{W} \geq VaR_a(\tilde{W})\} . \quad (15)$$

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

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

Загальніший 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 потребує 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) дорівнюватиме [10]:

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

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:

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

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

Наведені показники ефективності можна використати як критерії або обмеження при формулюванні задач оптимізації СЗ. Ряд таких формулювань подано у працях [1–5, 8].

Висновки

Проведене дослідження дає змогу сформулювати основні задачі, розв'язання 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 розроблення 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. Венцель Е. С. Теория вероятностей и ее инженерные приложения / Е. С. Венцель, 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.

УДК 538.91;537.32.622;536.51

В.Я. Крайовський, В.А. Ромака

Національний університет “Львівська політехніка”

ПРОГНОЗУВАННЯ ТА РЕАЛІЗАЦІЯ ТЕРМОЕЛЕМЕНТІВ ЕЛЕКТРОРЕЗИСТИВНИХ ТА ТЕРМОЕЛЕКТРИЧНИХ ТЕРМОМЕТРІВ НА ОСНОВІ n -HfNiSn

© Крайовський В.Я., Ромака В.А., 2012

Встановлено закономірності функцій перетворення електрорезистивних та термоелектричних термоелементів на основі термометричного матеріалу n -HfNiSn зі стабільними та відтворюваними характеристиками у температурному діапазоні $4,2 \div 1600$ К.

Ключові слова: температура, електроопір, термо-ЕРС.

Established patterns of transformation functions of electrical resistance and thermoelectric thermoelements based on thermometric material n -HfNiSn with stable and reproducible characteristics in the temperature range $4,2 \div 1600$ K.

Key words: temperature, electric resistivity, thermopower.

Вступ

Цією роботою ми розпочинаємо дослідження нового класу термометричних матеріалів на основі інтерметалічного напівпровідника n -HfNiSn. Напівпровідник n -HfNiSn, поряд з дослідженими нами раніше n -ZrNiSn та n -TiNiSn [1], розглядається як основа для виготовлення термоелементів електрорезистивних та термоелектричних термометрів. Попередні дослідження процесів легування n -ZrNiSn та n -TiNiSn атомами рідкісноземельних металів, перехідних $3d$ - та $4d$ -металів, а також p -елементів, дали змогу встановити у кожному конкретному випадку механізм генерування структурних дефектів донорної, акцепторної або нейтральної природи. Адже концентрація та тип дефектів, у кінцевому результаті, визначають властивості напівпровідника [2]. Виявилося, що