ВАРІАНТ ОПТИМІЗАЦІЇ ВИТРАТ НА СИСТЕМУ ЗАХИСТУ ІНФОРМАЦІЇ

Заболотний В.І., Петросян К.С.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Леніна, 14, каф. безпеки інформаційних технологій),
тел./факс (057)-702-14-25; E-mail: bit@kture.kharkov.ua

Summary: Organization of restricted access information during the information activity starts from problem definition of information security. There are three variants of problem definition. It is recommended to provide information security by one of variants depending on information owner. One of the variants is based on conscious allowance such level of information security which causes loses of unprotected data not more than all enterprise income.

Вступ

Організація захисту інформації з обмеженим доступом (ІзОД) в процесі інформаційної діяльності (ІД), як передбачено державним стандартом України у галузі технічного захисту інформації (ТЗІ) [1], розпочинається з постановки задач захисту інформації. Вказаним ДСТУ 3396.1-96 визначено три можливих варіанти постановки задач захисту інформації:

- досягнення необхідного рівня захисту ІзОД за мінімальних затрат і допустимого рівня обмежень видів ІД;
- досягнення найбільш можливого рівня захисту ІзОД за допустимих затрат і заданого рівня обмежень видів ІД;
- досягнення максимального рівня захисту ІзОД за необхідних затрат і мінімального рівня обмежень видів ІД.

Захист інформації рекомендовано [1] забезпечувати застосуванням одного із варіантів. Захист інформації, яка становить державну таємницю, забезпечується, як правило, застосування третього варіанту. Захист інформації, яка не є державною таємницею, забезпечується, як правило, застосуванням першого чи другого варіанту.

Проте при виборі варіанту захисту інформації можливий ще один варіант, заснований на свідомому допущенні такого рівня захисту інформації при якому різниця між доходом підприємства і втратами від незахисту інформації й від затрат на захист інформації максимальна. Тобто підприємство у ринкових умовах дає максимальний прибуток в умовах реалізації загроз інформації.

Надалі у роботі буде сформульована математична постановка і запропоноване рішення задачі обґрунтування таких затрат на захист інформації на підприємстві, що забезпечують максимальний прибуток загальної діяльності підприємства ІД.

Формулювання математичної моделі прибуткового варіанту захисту інформації

Аналіз змісту [1], у частині постановки задач захисту інформації дозволяє формалізувати наступні положення, які можуть бути основою для розробки математичної моделі з метою дослідження впливу затрат на захист інформації на прибуток підприємства. Надалі мова буде йти про витрати, прибутки, доходи віднесені на якийсь визначений термін, наприклад, на звітний період – місяць, квартал або рік. Рівень захисту інформації $P_d(z)$ - імовірність того, що задача захисту інформації буде досягнута. Величина $P_d(z)$ залежить від затрат на захист інформації – z. Природно припустити, виходячи із принципу доцільності, що із ростом затрат z рівень захисту інформації не зменшується, а зростає. Значення функції $P_d(z)$ позитивне і не перевищує 1. Таким чином, функція $P_d(z)$ відповідає вимогам які пред'являються до інтегральних функцій розподілу [2]. Доречи, похідна функції $P_d(z)$ по z є густиною імовірності $w_d(z)$. Графіки функцій $P_d(z)$, $w_d(z)$ наведені на рисунку.

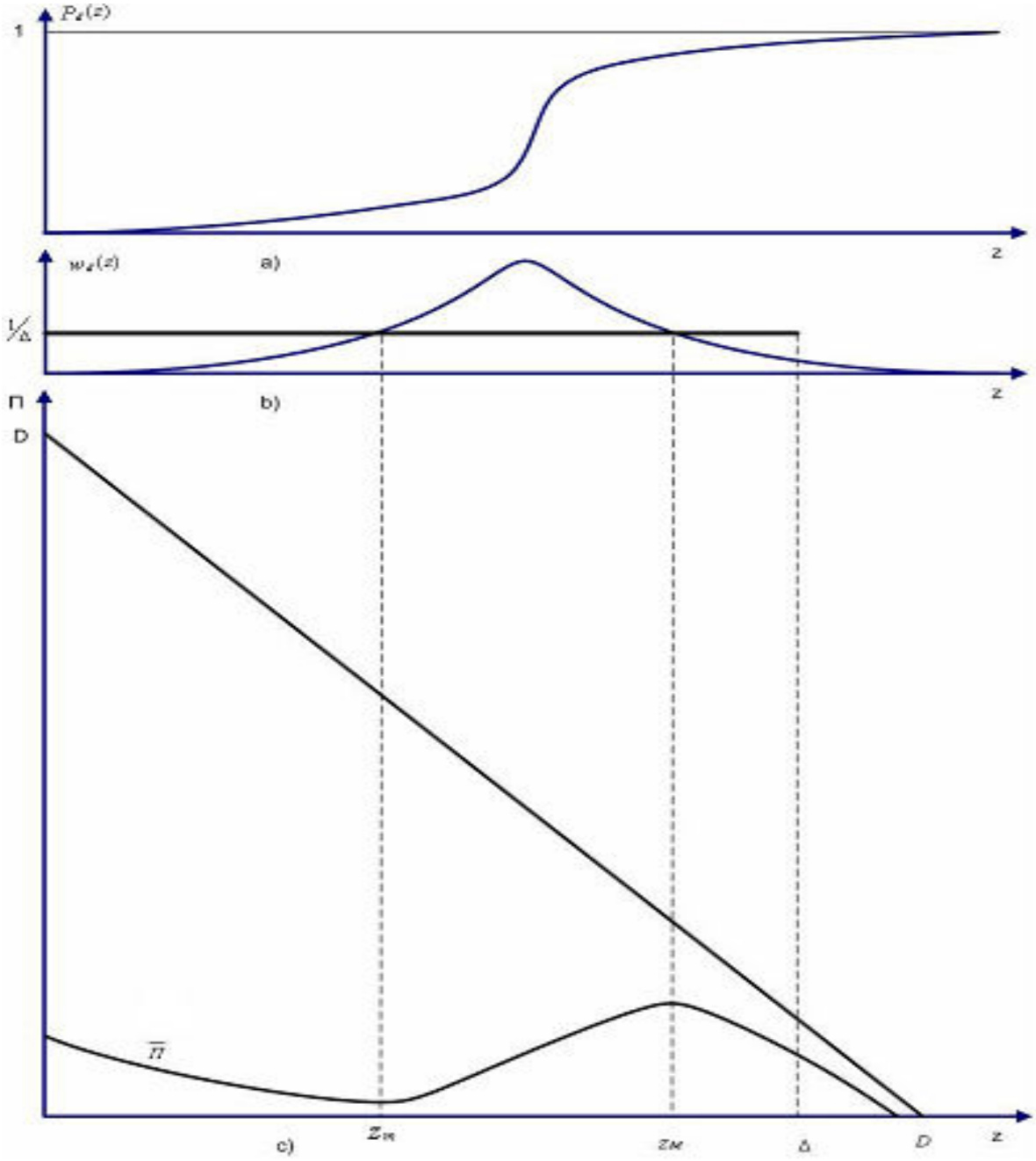

Рисунок 1 – Графік залежності прибутку підприємства та рівню захисту інформації від затрат *z*

Прибуток *П* підприємства, у спрощеному вигляді, можна представити як різницю між доходом D, збитками від незахисту інформації – *Δ* та затратами на захист інформації z. Інші складові витрат у даній роботі не розглядаються, але вони можуть бути певним чином враховані. У затрати на захист інформації z входять амортизаційні, експлуатаційні затрати тощо віднесені, як було визначено вище, до звітного періоду.

Прибуток *П* підприємства у разі забезпечення безпеки інформації становитиме величину $D - z$. Імовірність такої ситуації – $P_d(z)$.

Прибуток у разі незахисту інформації буде $D-\Delta-z$. Імовірність даної ситуації буде $1-P_d(z)$.

Середнє очікуване значення прибутку $\overline{\Pi}$ становитиме, як легко показати, величину

$$\overline{\Pi} = D - \Delta\left(1 - P_d(z)\right) - z\,. \tag{1}$$

Доданок $\Delta P_d(z)$ у (1) зростає, а $-z$ - зменшується із зростанням z. А раз так, то $\overline{\Pi}$ може мати екстремуми.

У подальшому наведений вираз відкриває шлях до обґрунтування варіанту захисту інформації, який дозволяє підприємству одержувати в оцих умовах максимальний прибуток.

Оптимізація витрат на захист інформації

З метою проведення кількісного аналізу впливу на прибуток підприємства затрат на захист інформації необхідно провести дослідження функції (1) на екстремуми по області визначення z. Класичний шлях – вираз та дослідження похідної (1). Після нескладних спрощень і реалізації зауваження щодо густини розподілу $w_d(z)$ похідна від (1) буде: $\dfrac{d\overline{\Pi}}{dz} = \Delta \cdot w_d(z) - 1$.

Екстремуми (1) знаходять як корені рівняння $\dfrac{d\overline{\Pi}}{dz} = 0$, тобто

$$w_d(z_i) = 1/\Delta\,, \tag{2}$$

де - z_i корені рівняння.

Максимуми (1) з числа екстремумів можна знайти аналітичним шляхом по значенням другої похідної для визначених коренів. Так $\dfrac{d^2\overline{\Pi}}{dz^2} > 0$ для кореня (2) дає мінімум функції (1), а $\dfrac{d^2\overline{\Pi}}{dz^2} < 0$ – максимум. Лівий схил $w_d(z)$ має позитивна значення другої похідної, а правий – від'ємну. Тобто перший перетин $w_d(z)$ з $1/\Delta$ дає мінімальне значення $\overline{\Pi}$, а другий – максимальне, що відшукується.

На рисунку *b)* зображені: горизонтальною лінією величина $1/\Delta$ і кривою – графік $w_d(z)$. Точки перетинання дають корені z_m і z_M, відповідно мінімального і максимального значень (1).

Можна застосувати чисельний метод знаходження максимуму шляхом підстановки коренів, обчислення та порівняння ординат (1).

Також необхідне чисельне порівняння величини ординати функції (1) для значення $z = 0$ із знайденими максимумами для прийняття взагалі рішення на захист інформації. Може статися так, що (1) від $z=0$ буде більше ніж від z_M. У цьому випадку витрати на захист інформації не покриваються одержаним доходом від діяльності підприємства.

Якщо $w_d(z)$ унімодальна, тобто $P_d(z)$ функція яка суворо зростає, то коренів буде не більше 2-х. Для полімодальної функції $w_d(z)$ кількість коренів може бути більше. Тоді буде необхідність порівняти величини усіх максимумів (1) і вибрати відповідний корінь – затрати z на захист інформації.

Вихідні дані для застосування методики

Варіант постановки задачі захисту інформації для одержання максимального прибутку підприємства потребує певних вихідних даних. ДСТУ 3396.1-96 [1] не дає відповіді щодо

методики формування вихідних даних для постановки задач захисту інформації. Виходячи із змісту показника $P_d(z)$ може бути наступний порядок його одержання.

Побічні електромагнітні випромінюванням і наводки формують технічний канал витоку інформації. Показник „небезпечний інформаційний сигнал/шум" на межі контрольованої території [3], може лежати в основі визначення $P_d(z)$. Співвідношення показника „небезпечний інформаційний сигнал/шум" з нормою захисту згідно з теорією виявлення сигналів дає змогу визначити ймовірність визначення засобами розвідки небезпечного сигналу на межі контрольованої території. Так, засоби технічного захисту інформації: екрани, екрановані приміщення, фільтри, генератори перешкод, заземлення приводять до зменшення величини „небезпечний інформаційний сигнал/шум". Збільшення відстані до межі контрольованої території потребує більше витрат на огорожу, охорону, плату за землю, обслуговування технічних засобів охорони тощо. Для кожного із конкретних засобів враховують їх власну ціну, затрати на експлуатацію, амортизацію тощо.

У випадках невизначеності факторів, які лежать у основі показника „небезпечний інформаційний сигнал/шум" на межі контрольованої території, може застосовуватися підхід викладений у [4]. Суть підходу лежить у аналітичному розрахунку характеристик розподілу ймовірності випадкової величини „небезпечний інформаційний сигнал/шум" і обчислення його перевищення порогу-норми на межі контрольованої території.

Хід залежності $P_d(z)$ може бути визначений також експертним шляхом на основі досвіду діяльності фахівців даної галузі. Методика створення і роботи експертної групи викладена, наприклад, у [5].

Збитки підприємства за рахунок незахисту інформації Δ можуть виникати за рахунок зменшення конкурентноздатності продукції, зменшення фактору раптовості розробки й впровадження продукції, технологій, відмови замовників і партнерів підприємства від співробітництва тощо. Дані збитки доцільно оцінювати або на базі статистичних досліджень, або експертним шляхом, як вже було вказано вище.

Взагалі слід зазначити, що формування вихідних даних є темою окремих досліджень на які повинні бути у подальшому зосереджені певні зусилля.

Висновки

Вираз для середнього очікуваного значення прибутку підприємства ІД дозволяє оптимізувати затрати на захист інформації так, що за звітний період загальний прибуток підприємства буде мати у середньому максимальну величину.

Запропонований підхід до постановки задачі захисту інформації має деякі особливості.

По-перше, керівництво підприємства ІД повинно усвідомлювати наявність існування певного рівня незахисту інформації з витікаючими з цього наслідками.

По-друге, для одержання обґрунтованих рекомендацій щодо необхідних затрат на захист інформації потрібні вихідні дані:

- по рівню захисту інформації в залежності від затрат;
- по величині збитків підприємства від незахисту інформації.

Література: 1. ДСТУ3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. 2. Д. Дюге. Теоретическая и прикладная статистика. Главная редакция физико-математической литературы, изд. «Наука», 1972. – 384 с. 3. Тимчасові рекомендації з технічного захисту інформаці у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ – 95) ДСТЗІ Київ. Затверджено наказом Державної служби України з питань технічного захисту інформації від 09 червня 1995 р.N 25. 4. В.І. Заболотний, О.Г. Лебедєв, О.П. Метелев. Забезпечення достовірності оцінки далекості виявлення випромінювань технічних засобів передачі інформації. 5. Саркисян С.А. и др. Анализ и прогноз развития больших технических систем. М.: Наука, 1983. –280 с.