ПОКАЗНИК ЯКОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Сташевський З. П.; Грицюк Ю. І., д.т.н., проф.
Львівський ДУ БЖД, м. Львів, Україна

Відповідно до чинного законодавства, наявність конфіденційної та таємної інформації змушує структурні підрозділи Державної служби України з надзвичайних ситуацій розробляти та впроваджувати СЗІ та постійно стежити за її якісною роботою. Для розв'язання однієї з цих задач необхідно передусім обґрунтувати математично показник якості функціонування СЗІ [3].

Встановлено, що інформаційна система (ІС) будь-якого структурного підрозділу може піддаватися різним загрозам, кількість буде обмежена $\tilde{Z}^{дз} = f(\tilde{P}^{заг}, \Delta\tilde{Q}^{заг})$, де: $\tilde{P}^{заг} = \{p_i^{заг}, i = \overline{1,m}\}$ — ймовірністю появи *i*-ої загрози; $\Delta\tilde{Q}^{заг} = \{\Delta q_i^{заг}, i = \overline{1,m}\}$ — обсяг збитку ІС, який наноситься *i*-ою загрозою. СЗІ виконує функцію повної або часткової ліквідації загроз для ІС, основною характеристикою якої є ймовірність усунення дії *i*-ої загрози з наявної множини $\tilde{P}^{усун} = \{p_i^{усун}, i = \overline{1,m}\}$.

Нехай ΣW — загальний попереджений збиток ІС, а $\tilde{W} = \{\omega_i, i = \overline{1,m}\}$ — попереджений збиток за рахунок ліквідації дії *i*-ої загрози. Тоді задача якісної роботи СЗІ має такий вигляд: необхідно вибрати такий варіант її реалізації, який забезпечить максимальне попередження збитку, що може виникнути під впливом різних загроз, при обмежених витратах на її функціонування. Формальний запис цієї задачі має такий вигляд:

Знайти $$\tilde{T}^0 = \arg\tilde{W}(\tilde{T}) \to \max : \tilde{T}^0 \in \tilde{T}^+, \quad (1)$$

при обмеженні $$C(\tilde{T}^0) \le C^{доп}, \quad (2)$$

де: $\tilde{T} = \{t_j, j = \overline{1,n}\}$ — множина параметрів технічної реалізації КСЗІ; $\tilde{T}^+ = \{t_j^+, j = \overline{1,n}\}$, $\tilde{T}^0 = \{t_j^0, j = \overline{1,n}\}$ — множина допустимих і оптимальних значень параметрів технічної реалізації СЗІ; $C^{доп}$ — сума допустимих витрати на функціонування СЗІ [1].

Для розв'язання цієї задачі необхідно насамперед сформулювати показник якості функціонування СЗІ, тобто $\tilde{W}(\tilde{T})$. Очевидно, попереджений збиток у загальному вигляді виражатиметься таким співвідношенням:

$$\tilde{W} = F\left(\tilde{P}^{заг}, \Delta\tilde{Q}^{заг}, \tilde{P}^{усун}\right) \to F\left(p_i^{заг}, \Delta q_i^{заг}, p_i^{усун}, i=\overline{1,m}\right). \quad (3)$$

За умови незалежності загроз і адитивності їх наслідків отримуємо

$$\Sigma W = \sum_{i=1}^{n} \omega_i = \sum_{i=1}^{m} p_i^{заг} \cdot \Delta q_i^{заг} \cdot p_i^{усун}. \quad (4)$$

Ймовірність появи *i*-ої загрози ($p_i^{заг}$) визначається статистично і відповідає відносній частоті її появи.

Збиток ($\Delta q_i^{заг}$), що виникає від впливу *i*-ої загрози, може визначатися в абсолютних одиницях: фінансових чи матеріальних втратах на відновлення СЗІ, тимчасових витратах, обсязі знищеної або «зіпсованої» інформації і т.д. Проте, практично це зробити дуже складно, особливо на ранніх етапах функціонування СЗІ. Тому доцільно замість абсолютного збитку використовувати відносний збиток, який, по суті, є ступенем небезпеки появи *i*-ої загрози для ІС. Ступінь небезпеки здебільшого визначаються експертно у припущенні, що усі загрози становлять групу подій [2], тобто:

$$0 \le \Delta Q^{заг} \le 1 \to \left\{ 0 \le \Delta q_i^{заг} \le 1,\ i = \overline{1,m} \right\};\ \sum_{i=1}^{m} \Delta q_i^{заг} = 1.$$

Найбільш складним питанням є визначення ймовірності усунення *i*-ої загрози $p_i^{усун}$ при функціонуванні СЗІ. Зробимо звичайне припущення, що ця ймовірність визначається тим, наскільки повно враховані кількісні та якісні вимоги до СЗІ при її проектуванні, тобто:

$$\tilde{P}^{усун} = \left\{ p_i^{усун} = f_i(\tilde{X}_i),\ i = \overline{1,m} \right\}, \qquad (6)$$

де $\tilde{\tilde{X}} = \left\{ \tilde{X}_i = \{x_{ij},\ j = \overline{1,n}\},\ i = \overline{1,m} \right\}$ — ступінь виконання *j*-ої вимоги до СЗІ для усунення *i*-ої загрози.

Отож, задача проектування СЗІ у вигляді (1) і (2) зводиться до оптимального обґрунтування кількісних і якісних вимог до неї при допустимих витратах на її функціонування, тобто має такий вигляд:
знайти

$$\tilde{W}\left(\tilde{\tilde{X}}' \right) \to \max, \qquad (7)$$

при обмеженні $C(\tilde{\tilde{X}}') \le C^{доп}$.

Отже, ефективний захист інформації є однією з найголовніших проблем при побудові надійної ІС будь-яких структурних підрозділів ДСНС України. Наведена математична модель показника якості функціонування СЗІ в ІС структурного підрозділу рятувальної служби дає змогу вибрати такий її варіант реалізації, який може забезпечити максимум попередженого збитку, отриманого внаслідок дії загроз при доступних витратах на функціонування цієї системи.

Література

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. — К. : Вид. група BHV, 2009. — 608 с.

2. Комплексна система захисту інформації. [Електронний ресурс]. — Доступний з http://uk.wikipedia.org/wiki/Комплексна_система_захисту_інформації.

3. Сташевський З. П. Особливості проблеми синтезу систем захисту інформації у структурних підрозділах МНС України / З. П. Сташевський, Ю. І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. — Львів : РВВ НЛТУ України. — 2012. — Вип. 22.10. — С. 79 — 96.