

**ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

Одним із найпоширеніших підходів до оцінки якості захисту інформації є визначений поділ реалізованих функцій і завдань, експлуатаційних характеристик і вимог у відповідність технічним завданням на створення системи захисту. Інший спосіб, який використовується у вітчизняній та закордонній практиці – це аналіз функціональної надійності системи, яка також характеризує якісний рівень системи інформаційної безпеки (СІБ).

Існують наступні методи та засоби оцінки ефективності СЗІ:

1. Метод порівняльного багатовимірного аналізу. Цей метод створений для визначення ступеня взаємного впливу загроз та причин їх виникнення. Суть методу можна звести до такого узагальненого алгоритму:

– складатися перелік об'єктів, що оцінюються, і вибираються ознаки, за якими буде проводитись оцінка. В даному випадку під об'єктами оцінки будемо розуміти показники захищеності обчислювальної системи, а під ознаками – сукупність параметрів, що характеризують ці показники;

– цей перелік слугує основою для формування матриці ознак  $X(n,w)$ , де  $n$  – кількість ознак, а  $w$  – кількість об'єктів, що оцінюються. Кожному об'єкту ставиться у відповідність рядок матриці із  $n$  ознак;

– через те, що дані, які зведені в матрицю, описують різні властивості об'єктів і мають різні одиниці виміру, вихідна матриця нормалізується відповідно до формули

$$Z_{ik} = \frac{x_{ik} - \bar{x}_k}{S_k}$$

де

$$\bar{x}_k = \frac{1}{w} \sum_{i=1}^w x_{ik}$$

– середнє арифметичне ознаки  $k$  по усіх об'єктах,

$$S_k = \left[ \frac{1}{w} \sum_{i=1}^w (x_{ik} - \bar{x}_k)^2 \right]^{\frac{1}{2}}$$

– стандартне відхилення ознаки  $k$

$Z_{ik}$  – нормалізоване значення ознаки  $k$  для одиниці об'єкта  $i$ ;

– проводиться розрахунок елементів матриці відстаней між показниками захищеності з урахуванням усіх елементів матриці ознак

$$W_{rs} = \frac{1}{n} \sum_{k=1}^n |z_{rk} - z_{sk}|, \quad (r,s=1,2,3,\dots,w).$$

2 Методи аналізу ризиків інформаційних систем (ІС). На даний час при побудові СЗІ АС особливого значення набуває завдання побудови моделей загроз

інформації. Існує чимало алгоритмів, які здійснюють аналіз ризиків ІС. До найбільш відомих алгоритмів належать CRAMM і RiskWatch. Зазначені алгоритми мають ряд переваг та набули широкого поширення.

Версії програмного забезпечення CRAMM, орієнтовані на різні типи організацій, відрізняються один від одного своїми базами знань.

*Науковий керівник – доц., В.В. Литвин*