УДК 621.311.1
© І. Рудик[1], Ю. Наконечний[1], 2010

РОЗРОБКА ПОКАЗНИКІВ ЗАХИЩЕНОСТІ АДАПТИВНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуто та проаналізовано основні показники захищеності адаптивної системи захисту інформації.

Considering and analizing main demonstrations of the adapted system information security.

1. ВСТУП

Застосування моделі адаптивного захисту, що базується на принципі біологічної аналогії [1] і, зокрема, ієрархічної організації СЗІ, дозволяє [2]:

- забезпечити близьке до оптимального співвідношення "вартість / ефективність" СЗІ за рахунок поступового наповнення багаторівневої моделі ІБ тільки необхідними механізмами захисту;
- у динаміці відстежувати найбільш задіяні механізми захисту при зміні поля загроз;
- формувати специфікацію вимог на відсутні механізми захисту;
- оцінювати захищеність системи ІТ через величини відносного збитку і інтегральні показники активності розподілених по структурі СЗІ механізмів захисту.

2. ПОСТАНОВКА ПРОБЛЕМИ

Рішення про розширення класифікацій атак і механізмів захисту проводиться відповідно до системи оцінок достовірності нейтралізації загроз у розрізі окремих механізмів захисту або окремих ешелонів СЗІ і аналогічних оцінок потенційних збитків, а також співвідносно з окремими механізмами захисту або окремими ешелонами СЗІ. Потенційний збиток будемо розглядати у відносних величинах, наприклад, по відношенню до значення максимально допустимого збитку в інформаційній системі господарюючого суб'єкта.

Можна використовувати розподіл в системі ІТ підмножини механізмів захисту по ешелонах багаторівневої моделі СЗІ, що аналогічний зображеному на рис. 1. [3], враховуючи, що кількість механізмів захисту та вимог безпеки, обумовлених у діючих стандартах інформаційної безпеки, перевищує 250 [4].

[1] Національний університет “Львівська політехніка”

Результати експертних оцінок, а також подальшого навчання нечітких нейронних мереж можуть бути подані у вигляді матриці достовірності «загрози - механізми захисту» ME розмірністю *m*x*n*

$$ME_{m\times n} = \begin{pmatrix} me_{11} & me_{12} & \vdots me_{1n} \\ me_{21} & me_{22} & \vdots me_{2n} \\ \cdots & \cdots & \cdots \\ me_{m1} & me_{m2} & \vdots me_{mn} \end{pmatrix},$$

де *m* – число механізмів захисту, *n* – число ешелонів СЗІ.

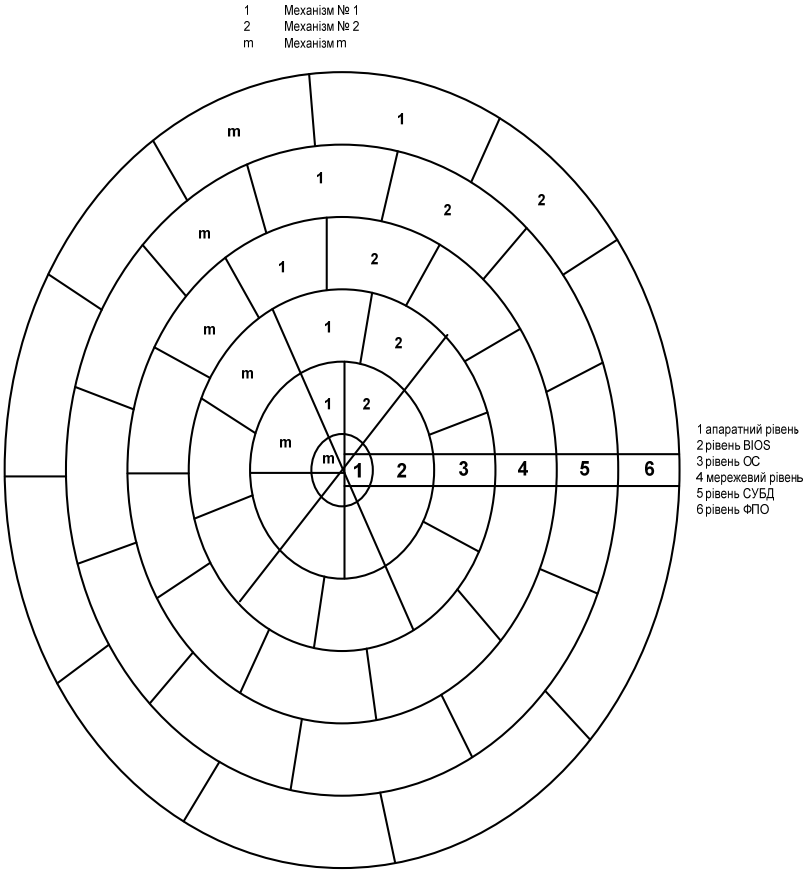

Рис. 1. Розподіл механізмів захисту за ешелонами СЗІ

Активність ешелону СЗІ за нейтралізацією загроз, що входять в систему предикатних правил, як посилань, визначається рядком інтег-

ральних показників, поданих, наприклад, рядком показників значущості [4] ешелону в багаторівневій СЗІ

$$x_j = \sqrt{\sum_{k=1}^{m} me_{kj}^2}, j = 1,...,n, \quad (1)$$

нормованих, наприклад, за значенням максимального із $x_j, j = 1,...,n$ або за значенням суми елементів рядка показників значущості $\sum_{j=1}^{m} x_j, j = 1,...,n$. Співставлення інтегральних показників у межах рядка дозволяє виявити найбільш задіяні ешелони у багаторівневій моделі СЗІ за нейтралізацією поля діючих на систему ІТ загроз.

Аналогічно за матрицею достовірності використання механізмів захисту для нейтралізації загроз можна отримати стовпець інтегральних показників активності використання окремого механізму захисту в усіх ешелонах багаторівневої СЗІ для нейтралізації наслідків чинного поля загроз

$$x_i = \sqrt{\sum_{k=1}^{n} me_{ik}^2}, i = 1,...,m. \quad (2)$$

Зіставлення інтегральних показників у межах стовпця дозволяє виявити найбільш задіяні механізми захисту у багаторівневій СЗІ.

Аналіз інтегральних показників матриці достовірності «загрози - механізми захисту» дає можливість обгрунтувати доцільність використання механізму захисту у складі відповідного ешелону багаторівневої СЗІ.

Використання експертних оцінок і подальше відображення у структурі нейро-нечіткої мережі апріорного досвіду експертів ІБ супроводжується перевіркою на несуперечність результатів опитування експертів. Несуперечливість оцінок експертів ІБ може бути забезпечена застосуванням, наприклад, методу експертних оцінок матриці нечітких співвідношень [3] або методу на основі розрахунку максимального власного значення матриці парних порівнянь [4].

3. ВИСНОВКИ

Наведені вище показники будуть більш інформативними, якщо враховувати не тільки достовірність використання механізмів захисту в структурі СЗІ, але й показники потенційного збитку, що виникають в результаті реалізації атак на систему ІТ і яким можна запобігти системою інформаційної безпеки. З цією метою за аналогією з [4] оцінку захищеності можна опосередковано пов'язати із запобіганням шкоди

системі ІТ, і, крім того, використовувати експертні оцінки для зіставлення, з одного боку, поля загроз ІБ з потенційним збитком від їх реалізації, з іншого боку, розміру потенційного збитку з місцем реалізації загрози в структурі ІТ.

1. Golub G., Van Loan C Matrix Computations. N.Y.: Academy Puss, 2002. – С. 38-42. 2. Роберт Коллан Основные концепции нейронных сетей ─ М., 2005.– С. 44-53. 3. Галушкин А. Теория нейронных сетей. ─ М., 2006. – С. 82-85. 4. Терехов В., Ефимов Д., Тюнин И. Нейросетевые системы управление. ─ М., 2006. – 72 с.