

АДАПТИВНИЙ МЕТОД ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ НЕВИЗНАЧЕНОСТІ

**А.В. Дудатьєв, к.т.н., доцент,
Ю.В. Баришев, студент
Вінницький національний технічний університет
e-mail: andreysaf60@mail.ru**

Оцінка інформаційної безпеки є надзвичайно актуальною і складною, в той же час, задачею, оскільки її розв'язок потребує значних ресурсів. Але рішення задачі оцінки інформаційної безпеки і прийняття відповідних рішень щодо її захисту, як правило, виправдовує всі витрати. Знаходження відповідей на дані питання можливо отримати за допомогою математичного моделювання.

У відомих програмних продуктах @RISK, ALRAM, BDSS, LRAM для оцінювання ризику використовують традиційні кількісні методи. Засоби аналізу ризику BUDDY SYSTEM, CONTROL-IT, CRAMM, базуються на якісному підході і ймовірні втрати виражаються у лінгвістичній формі, наприклад, «ризик відсутній», «ризик середній» і т.п. Ці засоби вимірюють можливі втрати на базі метода послідовних наближень, метода дерева подій, метода нечіткої логіки. Проте вони не дозволяють враховувати фактор часу.

Для розв'язку задачі пропонується використовувати побудову нейро-нечіткої мережі, яка визначає оцінку захищеності об'єкту на основі нечітких експертних оцінок факторів, які впливають на ту, чи іншу складову безпеки, в тому числі й на інформаційну безпеку. Для опису оцінки

даних факторів пропонується використовувати функції належності у вигляді трикутників.

Оскільки пропонується враховувати всі фактори, які впливають на безпеку об'єкта, то пропонується ваги персептронів вхідного шару нейромережі змінювати в діапазоні всіх дійсних чисел, тобто, чим більше модуль ваги персептрона, тим більше значення даний фактор має на складову захищеності. Від'ємними коефіцієнтами будуть позначатися протидії загрозам, а додатними – загрози.

Наступні шари нейромережі будуть мати тільки додатні значення, оскільки виходи вхідного шару нейромережі можуть бути як додатними, так і від'ємними.

Оптимальною системою захисту авторами пропонується визначати ту, значення виходу нейромережі якої прямує до нуля зліва.

Важливою характеристикою нейромережі є її здатність навчатися, що дозволяє їй адекватно оцінювати захищеність об'єкту, за умови коректної оцінки факторів. Крім того, якщо на окремий тип захисту певний фактор почне впливати, то його вага зміниться і стане відмінною від нуля. Тобто даний метод дозволить враховувати вплив нових загроз або появу нових методів протидії ним.

Отже нейро-нечіткий підхід до оцінювання інформаційної безпеки враховує фактор часу, пристосовується до зміни характеру впливу факторів, дія яких буває як негативна, так і позитивна з точки зору захищеності об'єкту. Нейро-нечіткий метод оцінювання захисту інформації є ефективнішим за існуючі методи, оскільки зберігаючи їх позитивні сторони – можливість оцінити захист інформації за відсутності чітких вхідних даних, дозволяє без побудови нової математичної моделі врахувати дію нових факторів впливу на стан загальної захищеності об'єкту.