УДК 681.3

ДОСТОВІРНІСТЬ ПРИЙНЯТТЯ РІШЕННЯ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

О.П. Войтович, к.т.н., доцент
Вінницький національний технічний університет
o_voytovych@mail.ru

Для забезпечення конфіденційності та цілісності інформації, що представлена у вигляді предметів, нанесена на папері або збережена в електронному вигляді і знаходиться на території певного об'єкту застосовують комплексні системи захисту, які включають блоки спостереження, аналізу, прийняття рішень, виконання певних дій, у відповідності до прийнятого рішення.

Зазвичай блок спостереження – це сенсор. Блоки аналізу, прийняття рішень та виконання певних дій найчастіше представлені певною групою осіб або однією особою, тобто надійність такої системи залежить від людського фактору, і є набагато нижчою в порівнянні із такою, в якій усі блоки реалізовані автоматично.

Для реалізації систем аналізу та прийняття рішень, мережа, що утворюється системою сенсорів працює за принципом нейронної мережі. Кожен сенсор системи представлений нейроном віртуальної нейронної мережі, яка і виконує роль аналізатора та системи прийняття рішень.

Сенсор фіксує певний параметр(и) и зберігає поточні дані. У випадку зміни параметру та перевищення ним порогового значення, генерується тривожний сигнал до інших сенсорів, які в цей час можуть знаходитись в пасивному режимі. Сусідні сенсори активуються та генерують відповідний сигнал, передають дані щодо ситуації навколо них.

Параметри виміряні сенсорами використовуються для ухвалення рішень про подію, що відбувається, і лише їх точність забезпечує правильність на всіх рівнях управління, а недостовірність – призводить до прийняття неправильних рішень, що в свою чергу може спричинити значні втрати. В більшості випадків методика визначення необхідної точності вимірювань в різноманітних технічних системах проходять за однією методикою. Відмінність є лише у способах знаходження тієї чи іншої величини.

В результаті прийняття рішення при наявності похибок вимірювань є повна група несумісних подій: А – система визначила атаку, що відбулася; Б – система не визначає атаки, атаки немає; В – атаки немає, система генерує тривожний сигнал; Г – атака відбулась, система її не визначила.

Ймовірність $P(B) = \alpha$ визначає величину ризику першого роду (хибної тривоги), а ймовірність $P(Г) = \beta$ - величину ризику другого роду (пропущеної атаки). Тоді інструментальна метрологічна достовірність прийняття рішення системою визначається $Д = 1 - \alpha - \beta$.

Щоб визначити необхідну точність вимірювання по і-му параметру, необхідно визначити допустиму величину ризику хибної тривоги α або пропущеної атаки β через величини α_i та β_i за цим параметром.

В задачах захисту інформації ризики хибної тривоги та пропущеної атаки оцінюються для таких систем: системи автентифікації (в тому числі біометричної), фільтрація спаму, антивірусні системи, системи виявлення вразливостей, запобігання вторгнень, системи пожежної та охоронної сигналізації.

В даній роботі пропонується методика визначення ризику хибної тривоги α, пропущеної атаки β та достовірності Д, в системах прийняття рішення при технічному захисті інформації.