КОМП`ЮТЕРНІ СИСТЕМИ ТА КОМПОНЕНТИ

УДК 681.3

О. П. ВОЙТОВИЧ

Вінницький національний технічний університет, м. Вінниця

ДОСТОВІРНІСТЬ ПРИЙНЯТТЯ РІШЕННЯ В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація. В статті розглянуті питання визначення достовірності прийняття рішення в ситсетмах технічного захисту інформації, які використовують для отримання первинної інофрмації сенсорні мережі. Досліджено особливості розрахунку ризиків першого та другого роду при одному параметрі. Отримано аналітичні співвідношення достовірності прийняття рішення, які є загальними для різних комбінацій законів розподілу ймовірностей параметрів і розподілу ймовірностей їх випадкових похибок вимірювання у системах технічного захисту інформації.

Ключові слова: системи технічного захисту інформації, сенсорні мережі, достовірність прийняття ріщень, ризики першого та другого роду

Аннотация. В статье рассмотрены вопросы определения достоверности принятия решения в системах технической защиты информации, использующие сенсорные сети для получения первичной информации. Исследовано особенности расчетов рисков первого и второго рода при одном параметре. Получены аналитические соотношения достоверности принятия решения, которые являются общими для разных комбинаций законов распределения вероятностей параметров и распределения вероятностей их случайных погрешностей в системах технической защиты информации.

Ключевые слова: системы технической защиты информации, сеснорные сети, достоверность принятия решения, риски первого и второго рода

Abstract. The questions of decision certainty of the technical information protection systems which use sensor networks to obtain primary information are considered. The estimate features of the false alarm ratio and false positive rate with a single parameter were reseached. The analytical relations of the decision certainty that are common to different combinations of the probability distribution parameters and the probability distribution of random errors at the technical information protection systems are obtained.

Key words: technical information protection systems, sensor networks, decision certainty, false alarm ratio, false positive rate

Вступ

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 технічного захисту інформації (СТЗІ), які включають блоки спостереження, аналізу, прийняття рішень, виконання певних дій, у відповідності до прийнятого рішення.

Актуальність

Перспективним напрямком побудови СТЗІ є сенсорні мережі [1].

Сенсорні мережі – це мережі, що утворюються з сенсорів, які обмінюються інформацією один з одним за допомогою безконтактних технологій. Особливістю таких мереж є відсутність єдиного центру, відповідального за обмін інформацією та прийняття рішення. Кожен сенсор в мережі має можливість приймати рішення базуючись на інформації отриманій від сусідніх сенсорів [2].

Застосування сенсорних мереж в системах захисту інформації [3]:

- системи оборони і забезпечення безпеки;
- охоронні системи;
- пожежна сигналізація;
- системи автентифікації (біометричної);
- контроль персоналу.

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, як це пропонується в сенсорних мережах.

Мета

В СТЗІ постає питання забезпечення необхідної достовірності прийняття рішення щодо реакції на появу загрози. Визначальним при цьому є правильність та точність отриманих від сенсорів вимірювальних даних. Достовірність прийняття рішення залежить від ризиків першого та другого роду (α та β відповідно). Метою даної статті є розробка та дослідження методів, що дозволяють підвищити достовірність прийняття рішення в СТЗІ.

Аналіз сенсорних мереж як СТЗІ

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.

Переваги сенсорних мереж: участь людини в роботі даної системи мінімальна; відсутність єдиного центру прийняття рішень; блок сенсору збирає інформацію про оточуюче середовище та, в разі необхідності, може приймати рішення; здатність до самонавчання.

На основі даних отриманих і з інших сенсорів формується рішення щодо подальших дій: ігнорування; генерація тривожного сигналу; виконання певних дій.

Кожен сенсор (мот) мережі складається з таких частин (рис. 1) [1,2]:

- первинний перетворювач;
- мікропроцесорний пристрій;
- пристрій бездротового зв'язку;
- батарея.

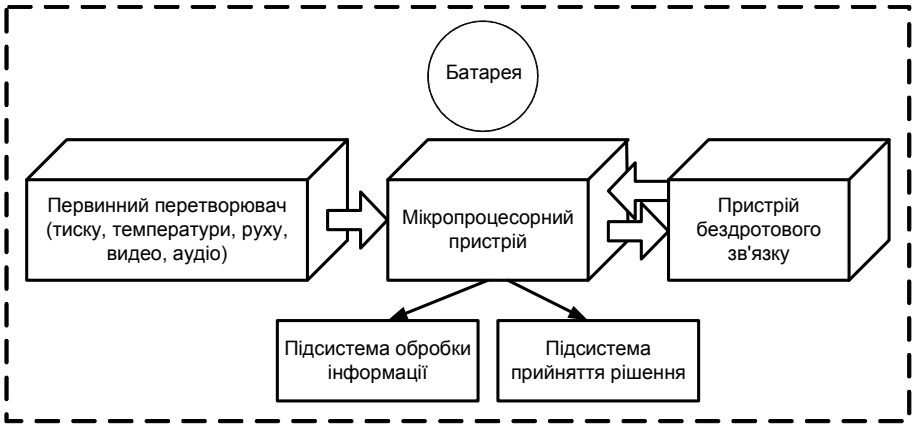

Рисунок 1 – Структура сенсору (моту)

Як первинний перетворювач можуть бути перетворювачі тиску, руху, температури, відео- або аудіо-сигналу тощо. Мікропроцесорний пристій містить дві основі підсистеми, які призначені для обробки вимірювальної інформації та прийняття рішення на її основі, а також керування пристроєм бездротового зв'язку. Живлення сенсора відбувається за допомогою батареї.

Достовірність прийняття рішень

Параметри виміряні первинними перетворювачами 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 однієї 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, FAR), а ймовірність $P(Г) = \beta$ - величину ризику другого роду (пропущеної атаки, FPR). Тоді інструментальна метрологічна достовірність прийняття рішення системою визначається

$$Д = 1 - \alpha - \beta. \quad (1)$$

Щоб визначити необхідну точність вимірювання по і-му параметру, необхідно визначити допустиму величину ризику I роду α або II роду β через величини α_i та β_i за цим параметром. Характеристики достовірності прийняття рішення α і β через величини α_i та β_i виражаються [4]:

$$\alpha = \prod_{i=1}^{n}(1-p_i) - \prod_{i=1}^{n}(1-p_i-\alpha_i);\ \beta = \prod_{i=1}^{n}(1-p_i-\alpha_i+\beta_i) - \prod_{i=1}^{n}(1-p_i-\alpha_i). \quad (2)$$

Тоді з виразів (1-2) отримаємо

$$Д = P + 2 \cdot \prod_{i=1}^{n}(1 - p_i - \alpha_i) - \prod_{i=1}^{n}(1 - p_i - \alpha_i + \beta_i) \quad (3)$$

Достовірність прийняття рішення в СТЗІ явно виражається не через інструментальну складову достовірності окремих параметрів $Д_i = 1 - \alpha_i - \beta_i$, а через їх характеристики α_i та β_i.

В загальному випадку, рівняння для ризиків І та ІІ роду по кожному параметру виразяться [4]:

$$\alpha_i = \int_{-kd}^{d} f(x)\left(\int_{-\infty}^{-kd-\overline{c2^1}+\overline{c1}-x} \varphi(\Delta)d\Delta + \int_{d+\overline{c2^1}+\overline{c1}-x}^{\infty} \varphi(\Delta)d\Delta\right)dx, \quad (4)$$

$$\beta_i = \int_{-\infty}^{-kd} f(x) \int_{-kd-\overline{c2^{11}}-\overline{c1}-x}^{d+\overline{c2^{11}}+\overline{c1}-x} \varphi(\Delta)d\Delta dx + \int_{d}^{\infty} f(x) \int_{-kd-\overline{c2^1}-\overline{c1}-x}^{d+\overline{c2^{11}}+\overline{c1}-x} \varphi(\Delta)d\Delta dx, \quad (5)$$

де $f(x)$ - густина розподілу ймовірностей параметра; $\varphi(\Delta)$ - густина розподілу ймовірностей випадкових похибок вимірювання; $-kd$ - задане, гарантоване поле допуску; k - коефіцієнт асиметрії поля допуску; $\overline{c2^1}$, $\overline{c2^{11}}$ - контрольні прирости поля допуску по нижній та верхній межі; $\overline{c1}$ - систематична похибка вимірювання.

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

В роботі [5] пропонується методика визначення ризику І роду α, ризику ІІ роду β та достовірності Д, при контролі одного параметра та симетричному двосторонньому допуску. При цьому вважається відомим: границі допуску на параметр А, В; Δ- границя допустимої похибки вимірювання; густина розподілу ймовірностей параметра f(x); густина розподілу ймовірностей похибок вимірювання $\varphi(\Delta)$.

Нехай дійсного значення х отримано значення $x_{вим} = x \pm \Delta$. При цьому можливі такі події (рис. 2).

Подія Н1 – дійсне значення та його виміряне значення в межах допуску $A \le x_1 \le B$ та $A \le x_{1вим} \le B$. Подія Н2 – дійсне значення та його виміряне значення поза межами допуску $x_2 < A$ або $x_2 > B$ та $x_{2вим} < A$ або $x_{2вим} > B$.

Подія Н3 – дійсне значення в межах допуску проте його виміряне значення поза межами допуску $A \le x_3 \le B$ та $x_{3вим} < A$ або $x_{3вим} > B$, тобто нормальний сигнал визнано анормальним. Ймовірність $P(H3) = \alpha$ визначає величину хибної тривоги.

Подія Н4 – дійсне значення поза межами допуску, проте його виміряне значення в межах допуску $x_4 < A$ або $x_4 > B$ та та $A \le x_{4вим} \le B$, тобто анормальний сигнал визнано нормальним. Ймовірність $P(H4) = \beta$ - величина пропущеної атаки.

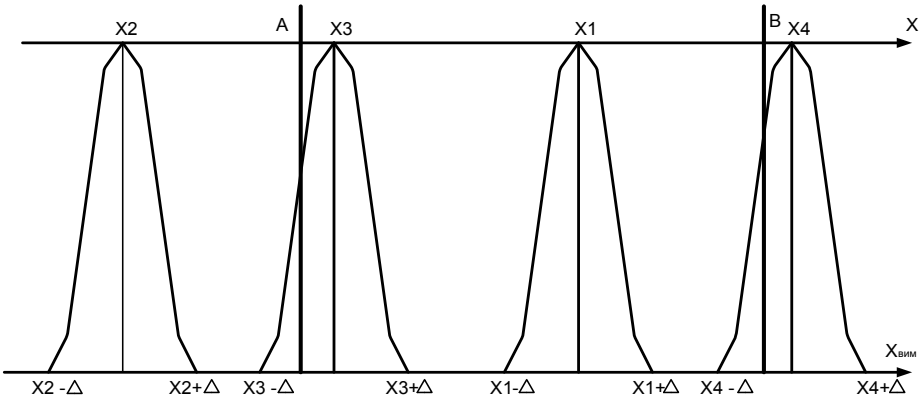

Рисунок 2 – До визначення ризиків І та ІІ роду

Для оцінки значень ризиків І та ІІ роду розглянемо розподіл параметра в межах впливу на результат прийняття рішення похибки вимірювання., тобто на проміжках А±Δ та В±Δ. Очевидно, що при отриман-

ні значень Хвим< А-Δ та Хвим > В+Δ буде фіксуватися атака, а у випадку А+Δ < Хвим< В-Δ - завжди буде визначено нормальну роботу системи.

Тоді ризики I та II роду [6]:

$$\alpha = \int_{A}^{B} f(x)\left[\int_{A-\Delta}^{A} \varphi(\Delta)d\Delta + \int_{B}^{B+\Delta} \varphi(\Delta)d\Delta\right]dx, \quad (6)$$

$$\beta = \int_{B}^{B+\Delta} f(x)\left[\int_{B-\Delta}^{B} \varphi(\Delta)d\Delta\right]dx + \int_{A-\Delta}^{A} f(x)\left[\int_{A}^{A+\Delta} \varphi(\Delta)d\Delta\right]dx, \quad (7)$$

Загальна кількість законів, яким підпорядковуються розподіли f(x) та φ(Δ), порівняно велика. Для їх опису допускається використання нормального зрізаного, трикутного, рівномірного, трапецевидного, Релея зрізаного, антимодального I і II законів розподілу.

Тому для опису функції густини законів розподілу запропоновано використати функцію Іордана [6, 7]. При зміні параметра ε форма функції змінюється від прямокутної до функції Лапласа.

$$\phi_{\varepsilon,c}(y) = \frac{k \cdot \cos(cy)}{\sqrt{1 + \varepsilon \cdot \sin^2(cy)}}, \quad (8)$$

де $k = \begin{cases} c\sqrt{|\varepsilon|}/2\arcsin(\sqrt{|\varepsilon|}) & \text{при} \quad 1 \le \varepsilon < 0; \\ c/2 & \text{при} \quad \varepsilon = 0; \\ c\sqrt{|\varepsilon|}/2\ln(\sqrt{\varepsilon} + \sqrt{1+\varepsilon}) & \text{при} \quad \varepsilon > 0, \end{cases}$

$c = \sigma(\varepsilon)/\sigma$;

$$\sigma(\varepsilon) = \sqrt{\int_{-\pi/2}^{+\pi/2} x^2 \varphi_\varepsilon(x)dx};$$

$\varphi_\varepsilon(y) = \varphi_{\varepsilon,c}(y)$ при c=1; σ - реальне СКВ похибки при будь-якому даному виді закону розподілу. Вид закону розподілу визначається значенням ε.

Графік функції Іордана показано на рис. 3. Як видно при зміні параметра ε форма функції змінюється від прямокутної до функції Лапласа.

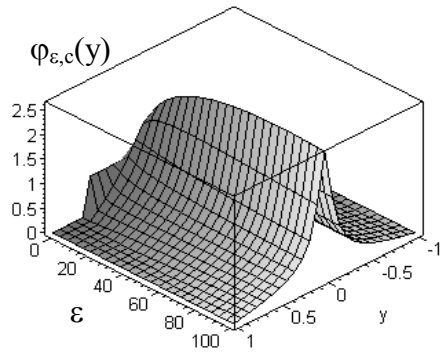

Рисунок 3 – Вигляд функції Іордана

В результаті проведених досліджень отримані залежності значення ε від реального СКВ σ заданих функцій розподілу густини ймовірності, а також залежності похибки апроксимації від σ. З використанням пакету прикладних програм Maple отримано аналітичні залежності для ризиків I та II роду при підстановці в них функцій Іордана.

Залежність значення достовірності від максимально допустимої похибки та виду закону розподілу, що у свою чергу виражається через коефіцієнти ε1, ε2, показана на рис.3. Як видно, достовірність прийняття рішень в СТЗІ залежить не тільки від допустимих похибок, але й від параметрів ε, які характеризують вид закону розподілу.

Опишемо густину розподілу ймовірностей контрольованих параметрів f(x) та густину розподілу ймовірностей випадкових похибок вимірювання φ(Δ) за допомогою функції Іордана (8):

$$f(x)=\frac{k_1\cdot\cos(c_1x)}{\sqrt{1+\varepsilon_1\sin^2(c_1x)}};\ \varphi(\Delta)=\frac{k_2\cdot\cos(c_2\Delta)}{\sqrt{1+\varepsilon_2\sin^2(c_2\Delta)}}, \qquad (9)$$

де k1, k2, c1, c2 - коефіцієнти k і c для густин розподілу f(x) і φ(Δ) відповідно.

З використанням пакету прикладних програм Maple отримано аналітичні залежності для ризиків α (6) і β (7) при підстановці в них функцій Іордана (8) [6].

Виходячи з вище вказаного, за допомогою пакету прикладних програм Maple, було отримано аналітичні та графічні залежності ризиків α та β від величини максимально допустимої похибки Δ в залежності від виду закону розподілу вимірювальної величини та закону розподілу її похибки, коефіцієнти функції Іордана ε_1, ε_2 відповідні для даного виду розподілу.

Залежність значення достовірності Д від максимально допустимої похибки Δ та виду закону розподілу, що у свою чергу виражається через коефіцієнти ε_1, ε_2 (відповідно для закону розподілу контрольованого параметра та закону розподілу похибки) показана на рис. 4.

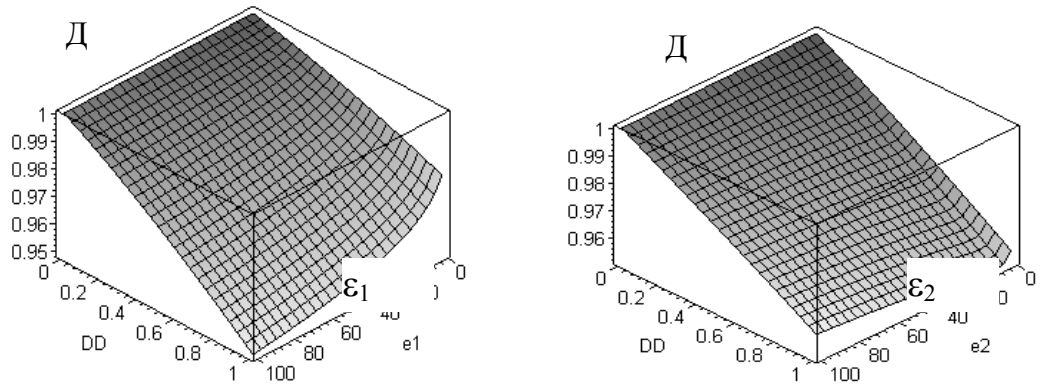

Рисунок 4 – Залежність достовірності Д від похибки Δ та коефіцієнтів ε1, ε2

Як видно з наведених на рис. 4 залежностей, достовірність прийняття рішення в СТЗІ залежить не тільки від допустимих похибок, але й від виду закону розподілу.

Висновки

Для визначення ризиків α та β у СТЗІ, які будуються на основі сенсорних мережа, запропоновано використати функцію Іордана. Використання функції Іордана дозволяє узагальнити методику отримання необхідної точності вимірювань контрольованих параметрів в сенсорних мережах СТЗІ.

Отримано аналітичні співвідношення для α та β, які є загальними для різних комбінацій законів розподілу ймовірностей контрольованих параметрів і розподілу ймовірностей їх випадкових похибок вимірювання мотів СТЗІ.

Список літератури

1. Кучерявый А. Е. Самоорганизующиеся сети и новые услуги / / Электросвязь. – 2009. – № 1. – С. 14-19.

2. Рагозин Д. В. Моделирование синхронизированных сенсорных сетей / / Проблеми програмування – 2008 – № 2-3 – С. 721-729 с.

3. Williams, G.O. (1996). "Iris Recognition Technology". p. 56. http://debut.cis.nctu.edu.tw/~ching/Face /Articles/Biometric%20Identification/00551842.pdf. Retrieved 2010-05-23

4. Новицкий П. В. Оценка погрешностей результатов измерений / П. В. Новицкий, И. А. Зограф. – Л. : Энергоатомиздат. Ленингр. отд-ние, 1991. – 304 с.

5. Визначення вимог до точності вимірювань в системах технічної діагностики / О. В. Поджаренко [та ін.] / / Вимірювальна техніка та метрологія. – 2001. – №58. – С. 138-142.

6. Оцінка достовірності моделі системи для повірки тахометрів / О. В. Поджаренко [та ін.] / / Вісник Державного університету „Львівська політехніка". – 2005 – № 530. – С. 110-115.

7. Земельман И. А. О классификации погрешностей измерений / Измерительная техника. – 1985. – №6. – С. 3-5.

Стаття надійшла: 29.06.2010.

Відомості про авторів

Войтович Олеся Петрівна – к.т.н., доцент, доцент кафедри захисту інформації, Вінницького національного технічного університету.