Шуми адитивного передавального тракту можуть бути суттєво зменшені при випадковому характері коефіцієнтів модуляції за умови множення кожного відліку сигналу на випадковий коефіцієнт модуляції.

Ширина розподілу коефіцієнта модуляції не повинна перевищувати ширини розподілу для шуму, амплітуда шуму при цих умовах може бути зменшена до 10 разів.

1 Нємкова О.А., Стасевич С.П., Шандра З.А. Дослідження завадостійкості криптографічного захисту інформації на основі інтегральних перетворень // Вісник Східноукраїнського національного університету ім. Володимира Даля. – Луганськ, 2010. – № 9(15). – Ч. 1. – С.39–44.

УДК 621.317

В.Д. Погребенник, Р.В. Політило
Національний університет "Львівська політехніка",
кафедра екологічної безпеки та аудиту

ОЦІНЮВАННЯ ВІРОГІДНОСТІ ВИЯВЛЕННЯ ПОРУШЕННЯ СТАНУ ОБ'ЄКТА

Розглянуто типові параметри сенсорів охоронних систем, які характеризують належну якість виявлення факту проникнення на об'єкт. Оцінено зміни ймовірності виявлення порушення стану об'єкта залежно від кількості спостережень, відстані та різних швидкостей порушника.

Ключові слова: охоронні системи, кількість спостережень.

Typical parameters of sensor of security systems that characterize good quality detection of the penetration of an object. By changing the probability of detecting a violation of the object depending on the number of observations, distances and different speeds of the offender.

Key words: security systems, number of observations.

Вступ

Типовими параметрами сенсорів охоронних систем, які характеризують належну якість виявлення факту проникнення на об'єкт, що охороняється, є ймовірність правильного виявлення, ймовірність помилкового спрацювання та чутливість сенсора [1].

Ймовірність правильного виявлення $P_Д$ – ймовірність того, що сенсор спрацює під час проникнення порушника в охоронну зону. $P_Д$ – величина статистична, оцінюється за результатами серії випробувань і, як наслідок, залежить від прийнятої методики випробувань. Зауважимо, що якщо вказати, наприклад, $P_Д$ =0,9, то воно буде некоректним. У специфікації сенсора повинен бути обумовлений сценарій проникнення, тобто зовнішні умови, модель порушника (який повзе, зі швидкістю 0,5 м/с і т.д.). Крім того, необхідно знати методику оцінювання $P_Д$. Тоді модель виявлення описується двома параметрами: ймовірністю виявлення і довірчим інтервалом C_L, тобто сенсор виявлятиме з ймовірністю $P_Д$ на рівні C_L. Але звичайно така повна інформація недоступна. Здебільшого доводиться задовольнятися значенням $P_Д$, яке слід вважати умовним, бо воно ґрунтується на припущеннях.

Ймовірність хибної тривоги – ймовірність того, що за час t відбудеться хибне спрацювання сенсора. Статистично оцінюється частотою хибних тривог – кількістю хибних тривог за певний інтервал часу. Середній інтервал часу між двома послідовними хибними спрацюваннями називається напрацюванням на помилкове спрацювання $P_{ПС}$.

Тому частота хибних спрацювань є основною характеристикою, за якою можна робити висновки про завадостійкість сенсора. Ідеальний сенсор охоронної сигналізації має ймовірність виявлення, що дорівнює одиниці, і нульову частоту хибних тривог. Проте ідеальних сенсорів не існує, і обидві ці величини насправді часто далекі від ідеалу.

Розглянуті характеристики пов'язані між собою таким параметром, як чутливість сенсора. Чутливість – величина, обернена до порогу. Поріг – деяке значення, нижче від якого сигнали інтерпретуються як шуми. Поріг регулюється під час налаштування сенсора. Чим більша чутливість, тим вища ймовірність виявлення. Але зі збільшенням чутливості зростає й частота хибних тривог.

Налаштовуючи сенсор, доводиться вибирати ці параметри, і при цьому задача полягає у підборі оптимального рівня чутливості $S_{опт}$. Отже, розглядаючи процес виявлення загалом, можна виділити основні показники його якості: достовірність виявлення; стійкість до завад. Ймовірність правильного виявлення є основною характеристикою, яка дозволить оцінити достовірність виявлення. На рис. 1 наведено графік взаємозалежності ймовірності виявлення і помилкового спрацювання.

Частота хибних тривог є основною характеристикою, за якою можна робити висновки про завадостійкість сенсора. Завадостійкість – показник якості сенсора, що характеризує його здатність стабільно працювати в різних умовах.

Зумовлено це, передовсім, тим, що будь-який сенсор зазнає дії великої кількості інтенсивних завад різноманітного походження, і в цих умовах абсолютно достовірно розрізнити дію завад від вторгнення порушника неможливо [2].

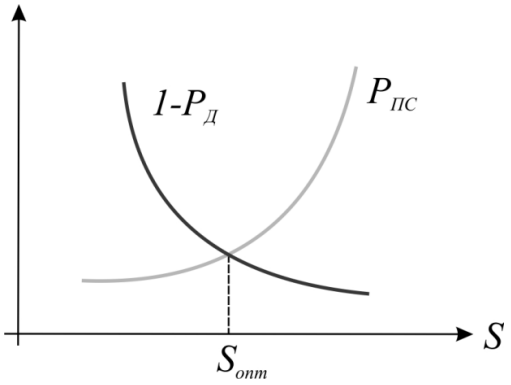

Рис. 1. Взаємозалежність ймовірності виявлення $P_Д$ та ймовірності помилкового спрацювання $P_{ПС}$: $P_Д$ – ймовірність правильного виявлення; $P_{ПС}$ – ймовірність помилкового спрацювання; S – чутливість сенсора; $S_{опт}$ – оптимальне значення чутливості сенсора

Величина ймовірності виявлення порушника ($P_Д$) та величина середнього напрацювання на помилкову тривогу ($t_{пт}$) є основними тактико-технічними характеристиками порушника, які характеризують його сигналізаційну надійність – можливість виявлення і завадостійкість.

$P_Д$ можна розрахувати за формулою:

$$P_Д = \frac{N_в - M - 1}{N_в}, \quad (1)$$

де $N_в$ – кількість випробувань із подолання зони виявлення (ЗВ); M – кількість пропусків порушника (експериментів, в яких не спрацювала ЗВ).

Також важливим параметром ЗВ є частота помилкових спрацювань $N_{пс}$, яка обчислюється так:

$$N_{пс} = \frac{1}{t_{пт}}. \quad (2)$$

Причини помилкових тривог можуть бути різними. Зокрема, помилкова тривога може виникнути через «технологічні» причини: неграмотний монтаж сенсорів, неправильне налаштування електронних блоків або просто незадовільний інженерний стан об'єкта.

Для аналізу показників вірогідності контролю використовують ймовірність помилкових рішень $P_{ПОМ}$, що визначається як різниця

$$P_{ПОМ} = 1 - P_{Д}. \quad (3)$$

Помилкові рішення при виявленні мають дві складові, які отримали назву *хибна відмова* та *невизначена відмова.* В теорії виявлення для цих подій існують відповідно такі назви: помилка першого роду, або ризик виробника, і помилка другого роду, або помилка споживача.

Ймовірність помилковості рішень подамо так

$$P_{ПОМ} = P_X + P_H, \quad (4)$$

де P_X – ймовірність того, що об'єкт С справний, а результат виявлення негативний (стан об'єкта порушений П); P_H – ймовірність того, що об'єкт С несправний, а результат виявлення позитивний (стан об'єкта не порушений П).

Розглянемо ймовірність виявлення нерухомих об'єктів. Важливим критерієм оцінки системи є *миттєва* ймовірність p виявлення об'єкта за один цикл.

Допустимо, що миттєві спостереження виконуються за незмінних умов і що ймовірність виявлення при кожному з них – величина незалежна. Ймовірність виявлення при m миттєвих спостереженнях визначають відповідно до теореми про повторення незалежних подій за формулою [3]

$$P_C(m) = 1 - (1 - p)^m. \quad (5)$$

Значення $P_C(m)$ – це накопичена ймовірність виявлення.

На рис. 2 подано криві, які дають змогу знайти кількість спостережень m, за якої на певній відстані реалізується потрібна ймовірність виявлення P_C. Очевидно, що навіть за малого значеннння ймовірності правильного виявлення за одне спостереження p можна одержати прийнятні значення $P_C > 0{,}9$. Але при дуже малих значеннях p для отримання $P_C > 0{,}9$ потрібна досить велика кількість m спостережень.

Математичне очікування, дисперсія та середньоквадратичне відхилення кількості миттєвих спостережень, необхідних для виявлення об'єкта, можна визначити за виразами

$$M(m) = \sum_{k=1}^{\infty} k(1-p)^{k-1} p.(m = k), \quad (6)$$

$$D(m) = M(m^2) - \left[M(m)\right]^2 = (1-p)/p^2, \quad (7)$$

$$s(m) = \sqrt{L(m)} = \sqrt{1-p}/p. \quad (8)$$

Якщо хоча би одного виявлення в m спостереженнях недостатньо, то тоді потрібно не менше за k правильних рішень і ймовірність визначають з рівності

$$P_{k,m} = \sum_{i=k}^{m} C_m^i p)^{k-1} p^i (1-p)^{m-i}, \quad (9)$$

де $C_m^i = \dfrac{m(m-1)...(m-i+1)}{1 \cdot 2 \cdot 3...i}$.

Як видно з рис. 3, за одного й того самого значення p ймовірність $P_{2,3}$ менша від ймовірності $P_{2,5}$, тобто при трьох спостереженнях важче забезпечити не менше від двох правильних виявлень, ніж в п'яти.

Враховуючи, що величина p пов'язана з відстанню L, тобто $p=f(L)$, то й $P(m)$ залежатиме від L. Використовуючи формулу (5) для різних m, можна розрахувати криві $P(L)$, які подано на рис. 4. Їх можна використати для визначення ймовірності виявлення на відповідній відстані до нерухомих об'єктів залежно від кількості спостережень.

Вище ми приймали, що спостереження проводились за незмінних умов, тобто p=const. У загальному випадку в разі зміни умов спостереження маємо

$$P_C = 1 - \prod_{i=1}^{m} (1 - p_i), \quad (10)$$

де p_i – ймовірність виявлення об'єкта при i-му спостереженні.

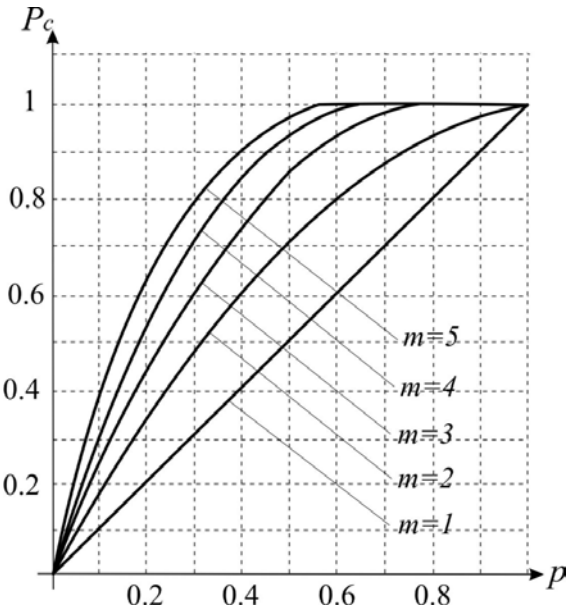

Рис. 2. Залежність накопиченої ймовірності P_C від ймовірності правильного виявлення в одному циклі p за різної кількості спостережень m

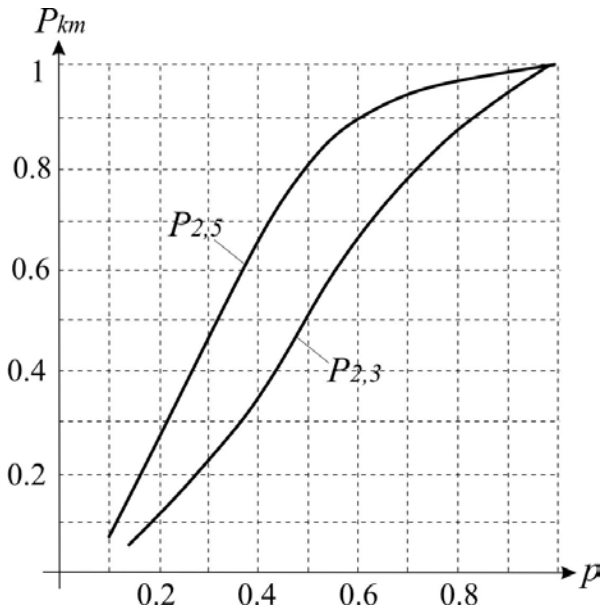

Рис. 3. Залежність накопиченої ймовірності від ймовірності правильного виявлення в одному циклі за заданої кількості виявлень

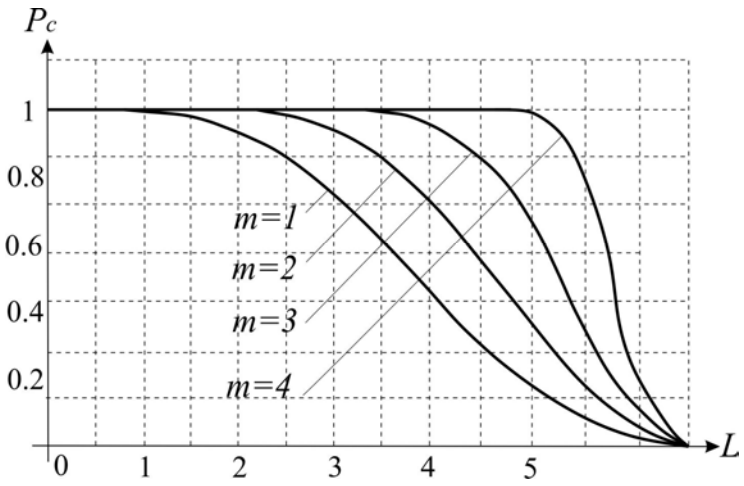

Рис. 4. Зміна накопиченої ймовірності залежно від відстані L для різних значень m

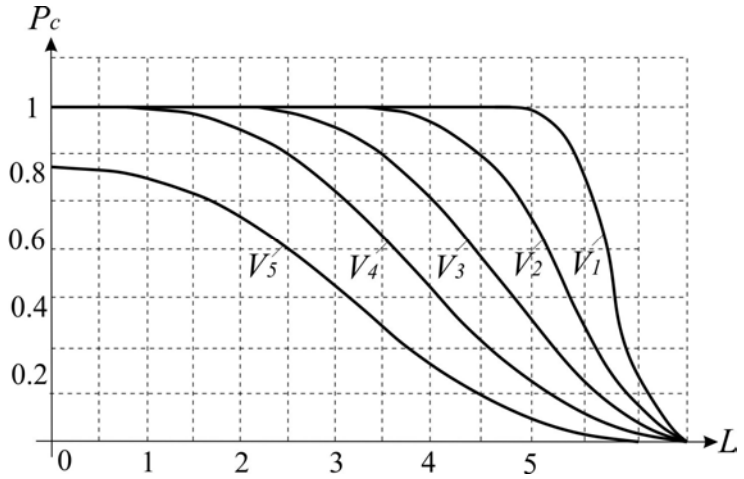

Рис. 5. Зміна накопиченої ймовірності залежно від дальності для різних швидкостей порушника ($v_5>v_4>v_3>v_2>v_1$)

Розглянемо випадок, коли порушник рухається з постійною швидкістю *v*. Для встановлення залежності P_C від відстані до об'єкта *L* слід використати формулу (10), оскільки у цьому випадку за рахунок руху порушника весь час відбувається зміна миттєвої ймовірності *p*. Якщо відома швидкість *v*, можна визначити зміну дальності при послідовних спостереженнях, а за залежністю *P*(*L*) знайти p_i для *i*-го спостереження. Тоді, користуючись (10), можна побудувати графіки зміни P_C від *L* для характерних значень *v* (рис. 5).

Знання залежності *P*(*L*) дає змогу визначити $L_{\max}$ і $L_{\min}$ і тим самим окреслити зону дії системи, яка містить зону ймовірного та достовірного виявлення.

Складніше розв'язується задача оцінювання P_C, якщо порушник рухається відносно системи виявлення під будь-яким кутом. Показано, що на заданій траєкторії переміщення порушника зона дії системи обмежена максимально можливою відстанню виявлення $L_{\max}$. Порушник при цьому рухається паралельно до осі *y* на віддалі X_i, яка може бути в межах від 0 до $\pm L_{\max}$.

За формулою (10) для кожного і-го спостереження довжиною $2X_i$ можна розрахувати значення $P_C(m)$. Весь інтервал параметра X_i можна охарактеризувати розподілом $P_C(X)$. Тоді можна побудувати залежності $P_C(X)$ для кожного типу об'єкта та для різних умов. У теорії пошуку та виявлення об'єктів введено поняття ефективної ширини смуги виявлення об'єкта, яку визначають як основу прямокутника, площа якого дорівнює площі під кривою $P_C(X)$:

$$B_E = \frac{1}{P_Z}\int_{-\infty}^{+\infty} P_C(X)dX, \tag{11}$$

де P_Z – задана ймовірність виявлення об'єкта.

У загальному випадку закон розподілу $P_C(X)$ може бути різним.

Розглянемо, як впливає спосіб пошуку на значення накопиченої ймовірності виявлення. Подамо пошук як випадковий марковський процес, в якому кількість виявлень за певний відрізок часу не залежить від результатів попереднього [4]. Такий найпростіший потік характеризують розподілом Пуассона, а накопичену ймовірність виявлення об'єкта системою визначають для стаціонарного пуассонівського потоку за формулою

$$P_C(t) = 1 - \exp\left[-U(t)\right], \tag{12}$$

де *U*(*t*) – потенціал пошуку:

$$U(t) = \gamma t_p \tag{13}$$

і для нестаціонарного:

$$U(t) = \int_{-t_0}^{+t_0+t_p} P_C(X)dX, \tag{14}$$

де γ – густина (інтенсивність) потоку подій, тобто середня кількість виявлень за одиницю часу; t_p – час пошуку, t_0 – початок відліку часу пошуку.

Отже, потенціал пошуку характеризує накопичення ймовірності з наростанням циклів спостережень, тобто протягом часу. З (13) та (14) після перетворень отримаємо

$$U(t) = -m\ln(1-p) \tag{15}$$

і

$$p = 1 - \exp(-\gamma t_p). \tag{16}$$

Ці формули справедливі для віддалі L_0. Для довільної віддалі *L* отримаємо

$$g(t) = -\frac{1}{t_p}\ln\left[1 - p(L)\right]; \tag{17}$$

$$p(D) = 1 - \exp\left[-g(L)t_p\right]. \tag{18}$$

Отже, за допомогою наведених формул можна еквівалентно замінювати задані ймовірнісні характеристики. Тому розрахунок накопиченої ймовірності зводиться до визначення потенціалу виявлення або інтенсивності пошуку.

Висновки

Оцінено зміни ймовірності виявлення порушення стану об'єкта залежно від кількості спостережень, відстані та різних швидкостей порушника.

1. Політило Р. В. Підвищення надійності ультразвукових систем охоронної сигналізації / Погребенник В. Д., Політило Р. В. // Збірник тез доповідей VII Міжнародної науково-технічної конференції «Приладобудування 2008: стан і перспективи». – К.: НТУ «Київський політехнічний інститут», 2008. – С. 105–106. 2. Політило Р. В. Вибір параметрів первинних вимірювальних перетворювачів ультразвукових засобів охоронної сигналізації / Погребенник В. Д., Політило Р. В. // Збірник матеріалів IУ Міжвузівської науково-технічної конференції науково-педагогічних працівників «Проблеми та перспективи розвитку економіки і підприємництва та комп'ютерних технологій в Україні». – Львів: ІППТ, 2009. – С. 48–49. 109. 3. Абчук В.А. Поиск объектов / Абчук В.А., Суздаль В.Г. – М.: Сов. радио, 1977. – 336 с. 110. 4. Бакут П.А. Обнаружение движущихся объектов / Бакут П.А., Жулина Ю.В., Иванчук Н.А. – М.: Сов. радио, 1980. – 288 с.

УДК 004.4

В.Д. Погребенник, П.Т. Хромчак
Національний університет "Львівська політехніка",
кафедра захисту інформації

ПАСИВНІ МЕТОДИ ВИЯВЛЕННЯ БОТНЕТ-МЕРЕЖ

Підсумовано та описано групи пасивних методів виявлення ботнет-мереж. Наведено основні недоліки та переваги роботи кожного з них.

Ключові слова: ботнет-мережі, пасивні методи.

Groups of passive techniques of botnet detection mechanisms are described and summarized in this article. Base advantages and disadvantages of each of them are also shortly noted.

Key words: botnet detection mechanisms, passive techniques.

Вступ

Група пасивних методів виявлення ботнет-мереж ґрунтується на методах, які отримують дані виключно за допомогою спостереження за роботою мережі. Такий підхід уникає прямої взаємодії з середовищем передавання даних, що дає змогу залишатись анонімним та непоміченим як для програм, так і для аналітика. Проте пасивні методи мають ряд обмежень, які стосуються даних, отриманих для аналізу.

У цій роботі наведено різноманітні підходи для здійснення вимірювань показників активності ботнету та його виявлення. Методи, що застосовують для аналізу мережевих даних, застосовують техніки, які фокусуються на певній абстракції даних та протоколах, що використовуються в галузі ботнетів. Ці методи не обмежуються архітектурою мережі та можуть застосовуватись до будь-якої з них.

Мета роботи – підвести підсумки щодо використання та групування пасивних методів виявлення ботнет- мереж, а також висвітлити основні недоліки та переваги роботи кожного з них в умовах роботи в інформаційній мережі контрольованої зони.