ЗАЩИТА ИНФОРМАЦИИ В РАДИОТЕХНИЧЕСКИХ И ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

УДК: 621.391.28, 621.391.7

Л. Б. МАКАРОВ, канд. техн. наук, О. М. БІТЧЕНКО, канд. техн. наук,
О. І. ЦОПА, д-р. техн. наук, О. О. КУЗНЕЦОВ

ЕНТРОПІЙНА ОЦІНКА ХАРАКТЕРИСТИК ЗАХИЩЕНОСТІ СИСТЕМ ПЕРЕДАЧІ ІНФОРМАЦІЇ

Вступ

Поняття ентропії було вперше введено в науку для визначення теплового стану речовини у термодинамічних системах, де вона характеризує імовірність певного стану будь-якої фізичної системи серед безлічі можливих її станів. Разом з тим ентропія стала дуже вдалою конструктивною категорією для використання в теорії зв'язку, телекомунікаційних мережах і системах передачі інформації (СПІ), а також для вирішення ряду важливих специфічних завдань в різних області техніки, біології і навіть у гуманітарній сфері. За її допомогою введена статистична міра кількості інформації, проводяться розрахунки і основних інформаційних характеристик СПІ, щоправда, лише на суто технічному, структурно-синтаксичному рівні [1, 2].

У теорії прикладної інформації ентропія розглядається як міра невизначеності (неймовірності), в інших областях ентропію розглядають як міру складності об'єкта, або міру різноманіття, або як характеристику невпорядкованості та інше [3]. У системах зв’язку на базі прикладної теорії інформації розроблені та запропоновані ідеї статистичного кодування джерела, завдяки реалізації яких спрощуються і стають більш високошвидкісними канали передачі інформації. Теоретико-інформаційний підхід дозволив отримати також ряд важливих наукових результатів в області автоматичного управління, ЕОМ, вимірювальної техніки, планування експериментів і системотехніки, а також у галузі захисту інформації [4].

Наприклад, у роботі [5] розглядається ефективне застосування ентропії для кількісних оцінок різних видів скритності передачі інформації і в цілому завадозахищеності СПІ. Скритність пов'язують з труднощами досить швидкого визначення великого числа робочих параметрів сигналу з метою створення ефективних перешкод. Такими параметрами можуть бути бітові елементи псевдовипадкових послідовностей (ПВП) в завадозахищеному радіозв'язку з використанням широкосмугових шумоподібних сигналів (ШШС), параметри робочих каналів в завадозахищених радіосистемах з псевдовипадковим переналаштуванням робочої частоти (ППРЧ), параметри ортогональних частот у системах зв’язку з модуляцією *OFDM*, характеристики і кількість антен при застосуванні *MIMO* технологій [6].

Мета роботи – розгляд області застосування інформаційної ентропії при вирішенні задач з моделювання та забезпечення захисту інформації у СПІ згідно існуючих критеріїв захищеності інформації, а також для пошукових задач в техніці зв'язку.

Основна частина

При створенні сучасних інформаційно-коммунікаційних систем (ІКС) постає проблема вибору та оцінки ефективності систем захисту інформації (СЗІ). Для вирішення цієї проблеми використовують різноманітні моделі системи захисту, які відображають різні аспекти захисту інформації і дають можливість оцінити основні параметри СЗІ. Відповідно до нормативного документу з технічного захисту інформації [7] в Україні існують п’ять основних критеріїв захищеності інформації в комп’ютерних системах, які використовуються для обробки (в тому числі збирання, зберігання, передачі та ін.) критичної інформації. Ці критерії є методологічною базою для визначення вимог з захисту інформації від несанкціонованого доступу, які можуть застосовуватися до всього спектра комп'ютерних систем, включаючи

однорідні системи, багатопроцесорні системи, бази даних, вбудовані системи, розподілені системи, об'єктно-орієнтовані системи, комп'ютерні мережі та ін. По аналогії з комп'ютерними мережами ці критерії можна також віднести до функціональних критеріїв захищеності інформації у СПІ: конфіденційності, цілісності, доступності та спостережності.

Застосуємо інформаційно-теоретичній підхід для моделювання і оцінки характеристик захищеності СПІ, використовуючи поняття ентропії. В якості базової моделі розглянемо модель СПІ по каналу зв'язку з відводом (*wiretap channel*) запропоновану Вайнером А. [8].

Схема (рис. 1) представляє собою так званий погіршений широкомовний канал (ШК) з одним входом і двома виходами. Проте на відміну від звичайного завдання максимізації швидкості передачі до обох одержувачів, традиційної для ШК, тут ставиться завдання мінімізації кількості інформації, що отримується незаконним користувачем, при збереженні максимально можливої швидкості передачі інформації законному користувачеві тобто забезпечення *конфіденційності* передачі інформації. З цією метою застосовується випадкове кодування на передачі і відповідне (невипадкове) декодування на прийомі.

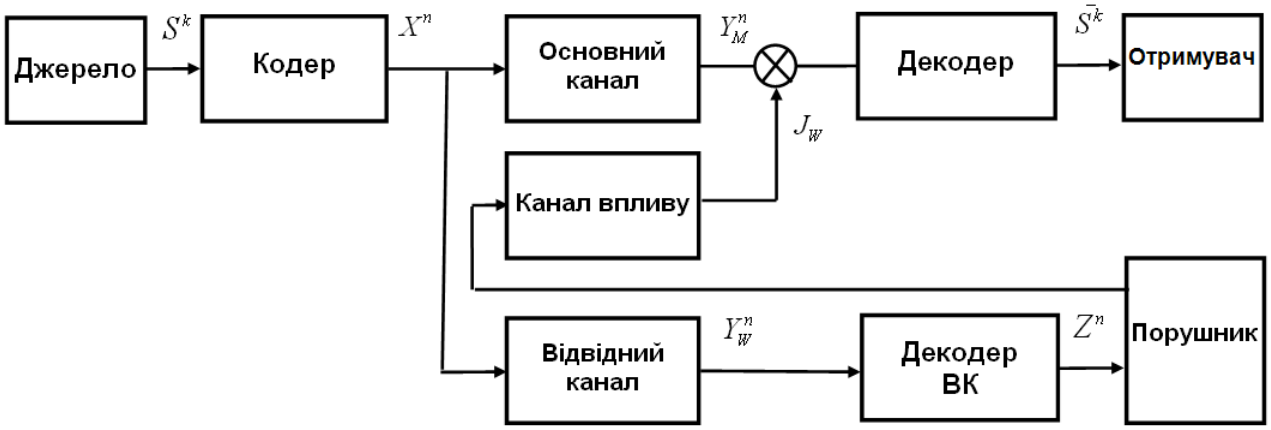

Рис. 1

Канал передачі інформації від джерела до одержувача називається основним каналом *(main channel)*, канал відведення до незаконного користувача (порушника) – відвідним каналом *(wiretap channel)*. Порушник через канал впливу може встановлювати завади (*jammer*).

Джерело – пристрій, який виробляє послідовності незалежних, однаково розподілених випадкових величин. В кожну джерело одиницю часу формує один з двійкових символів $S_1, S_2 ... S_i$, що належать дискретній множині S. Позначимо ентропію джерела через H_S.

Кодер об'єднує вхідні символи в блоки по *k*-символів $S^k = (S_1, S_2, ..., S_k)$ та кодує кожний блок в двійковий *n*-мірний вектор $X^n = (X_1, X_2, ..., X_n)$. Випадковий кодер має функцію кодування $x = G(s,t)$, де t – випадкове число.

Основний канал – дискретний канал без пам'яті $\left\{X^n, p_м(y/x), Y_м^n\right\}$ з вхідним алфавітом X^n, вихідним алфавітом Y_M^n і матрицею перехідної імовірності $\left|p_м(y/x)\right|$. Якщо основний канал не має шумів і завад, то $Y_M^n = X^n$. При дії навмисних завад $Y_W^n = X^n \oplus J_W^n$, де $\oplus$ – покомпонентне сумування за модулем два, J_W^n – двійковий вектор помилок у каналі впливу.

Декодер в основному каналі є невипадкове відображення *n*-блоків y в *k*-блоки s', $s' = G'(y)$, де G' – функція декодування.

Відвідний канал – дискретний канал без пам'яті $\left\{X^n, p_w(y/x), Y_W^n\right\}$ з вхідним алфавітом X^n, вихідним алфавітом Y_W^n і матрицею перехідної імовірності $\left|p_W(y/x)\right|$. Якщо у відвідному каналі є шуми то $Y_W^n = X^n \oplus E^n$, де $\oplus$ – по компонентне сумування за модулем два, E^n – двійковий вектор помилок у відвідному каналі.

Декодер у відвідному каналі реалізує функцію оптимального декодера G_{opt}.

Основними параметрами передачі в даній моделі є:

– швидкість передачі інформації – $R = k/n$;

– ймовірність помилки на символ P_e в основному каналі

$$P_e = \frac{1}{k} \cdot \sum_{i=1}^{k} p(s_i \neq s_{i'}) \tag{1}$$

– невизначеність інформації Δ, яка характеризує захищеність інформації відносно каналу відведення

$$\Delta = 1/k \cdot H(S^k \left| Z^n \right.), \tag{2}$$

де $H(S^k \left| Z^n \right.)$ – умовна ентропія джерела при відомих *n*-блоках на виході каналу.

– імовірність правильного декодування повідомлень у відвідному каналі за допомогою оптимального декодера

$$P(G) = P\left\{G_{opt}(Y_W^n) = S^k\right\}. \tag{3}$$

Використовуючи відоме співвідношення для кількості інформації, що передається по каналу, можна записати

$$I(S^k; Z^n) = H(S^k) - H(S^k \left| Z^n \right.), \tag{4}$$

де $I(S^k; Z^n)$ – середня взаємна інформація між *k*-блоками на вході і *n*-блоками на виході каналу; $H(S^k)$ – ентропія *k*-блоків джерела.

З виразу (3) видно, що якщо $H(S^k \left| Z^n \right.) = H(S^k)$, то $I(S^k; Z^n) = 0$ і інформація незаконному користувачеві не передається. Якщо $H(S^k \left| Z^n \right.) = 0$, то $I(S^k; Z^n) = H(S^k)$ і незаконний користувач отримує повну інформацію про джерело [8]. У проміжному випадку незаконний користувач отримує деяку кількість інформації, що відрізняється від нульового, але неповне.

При використанні асимптотично довгих кодів, тобто кодів, в яких $n \to \infty$, між параметрами системи передавання інформації з імовірнісним кодуванням є взаємозв'язок і існує область *D* досяжних швидкостей та невизначеності, яка відображена на рис. 2.

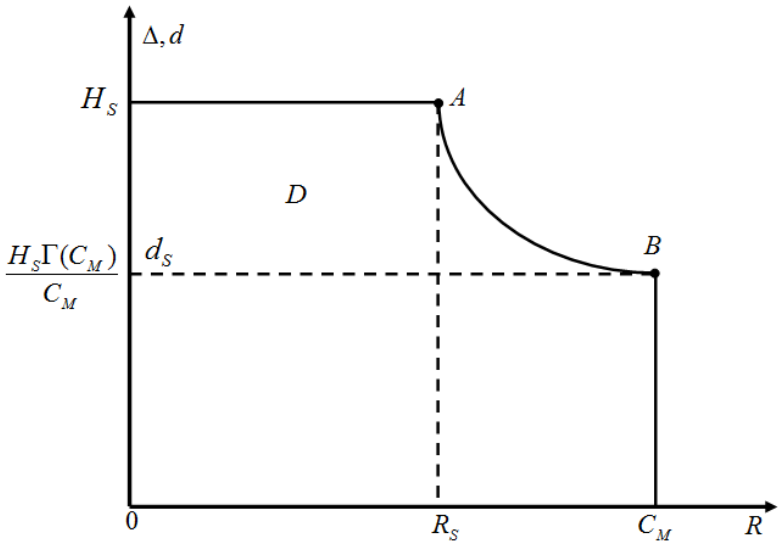

Рис. 2

Пара чисел (R,d) називається досяжною для швидкості і невизначеності, якщо для будь-якого $\varepsilon \to 0$ існують кодер і декодер G, для яких

$$kH_S / n \geq R - \varepsilon, \tag{5}$$

$$\Delta \geq d - \varepsilon, \tag{6}$$

$$P_e \leq \varepsilon. \tag{7}$$

У роботі [9] показано, що область *D* досяжна тоді і лише тоді, коли

$$R \leq C_M, \qquad d \leq H_S, \qquad Rd \leq \Gamma(R), \tag{8}$$

$$\Gamma(R) = \max_{p(x)\in p} I(X,Y\,|Z), \tag{9}$$

де p – множина розподілів вірогідності $p(x)$ на вході каналу, для яких $I(X;Y) \geq R$; C_M – пропускна спроможність основного каналу.

На рис. 2 найбільший інтерес для аналізу представляють дві області: *A* – (R_S, H_S) і *B* – (C_M, d_S). Швидкість R_S є максимальною швидкістю передачі по основному каналу, при якій по каналу перехоплення інформація взагалі не передається, тобто $H(S^k\,|Z^n) = H(S^k)$. Ця швидкість називається таємною пропускною спроможністю [9].

Область *B*, для якої $R_S = C_M$ відповідає швидкості передачі, рівній пропускній спроможності основного каналу. Це максимальна швидкість, при якій можлива надійна передача по цьому каналу ($P_e \to 0.$, при $n \to \infty$). На цій швидкості передачі досяжна невизначеність $d_в = H_S\Gamma(C_M)/C_M$. Тобто, якщо вибрати $k/n > R_S$, то при $n \to \infty$ кількість інформації у відводі відносно повідомлення $I(S^k;Z^n)$ убуває до нуля.

При побудові області *D* важко визначити функцію *Γ(R)*. Для деяких випадків вона може буде константою. Умовою для цього є той факт, що випадкові величини *X, Y, Z* утворюють марківську послідовність [9]:

$$I(Y,X\,|Z) = H(X\,|Z) - H(X\,|Y,Z) = H(X\,|Z) - H(X\,|Y) = H(X;Y) - H(X;Z), \tag{10}$$

Якщо $I(X;Y)$ і $I(X;Z)$ одночасно максимізовувати при деякому розподілі $p(x)$ тоді *Г(R)* – константа, а таємна пропускна спроможність

$$R_S = C_M - C_W, \tag{11}$$

де C_W – пропускна спроможність відвідного каналу.

Вираз (10) показує, що при фіксованій якості основного каналу збільшення R_S можливо лише за рахунок погіршення якості каналу перехоплення.

Для випадку, коли основний і відвідний канали є двійковими симетричними каналами (ДСК), імовірність помилки в каналі витоку рівна p_W, а в основному каналі $p_M = 0$, якщо джерело інформації безнадмірне ($H_S = 1$), то область *D* досяжна тоді і лише тоді, коли

$$0 \le R \le 1, \qquad 0 \le d \le 1, \qquad Rd \le h(p_W), \tag{12}$$

де $k/n \ge R - \varepsilon$, $\Delta \ge d - \varepsilon$, для усіх $\varepsilon > 0$;

$h(p_W)$ – функція ентропії: $h(p_w) = -p_w \cdot \log p_w - (1 - p_w)\log(1 - p_w)$.

З урахуванням виразу (8) і при $C_M = 1$ маємо:

$$C_W = 1 - h(p_W). \tag{13}$$

У роботі [10] отримані асимптотичні значення невизначеності у відвідному каналі при деяких спрощеннях

$$\Delta \le 1 - (1 - p_w)^n. \tag{14}$$

Сенс спрощеного виразу (14) полягає у тому, що якщо p_W у відвідному каналі мало, а довжина кодового блоку n недостатньо велика, то ефективний захист інформації неможливий, оскільки імовірність прийому кодового блоку у відводі без помилок (а отже, і правильне виділення повідомлення) буде значно відрізнятися від нуля.

Основний висновок розглянутого ентропійного підходу в оцінці захищеності полягає в підтвердженні існування способу кодування-декодування G для області кінцевих швидкостей передачі $0 \le R \le R_S$, при якому в відвідному каналі може бути забезпечена висока захищеність від перехоплення $\Delta \to H_S \to 1$ (висока невизначеність в каналі порушника), якщо $n \to \infty$.

Конфіденційність при передачі інформації також пов'язана з характеристиками скритності СПІ. У роботі (4), наприклад, запропоновано таємність S_A арсеналу суміжних параметрів передачі системи зв'язку визначати через ентропію по формулі Шеннона [2]

$$S_A = H(A) = -\sum_{i=1}^{A} p(a_i)\log_2 p(a_i), \tag{15}$$

де $p(a_i)$ – ймовірність вибору для даної передачі деякого значення параметру a_i з повної безлічі $\{a_i\}$, $i = \overline{1.A}$; $\sum_i p(a_i) = 1$.

Величина S_A може розглядатися як мінімально необхідне (оцінка знизу) середнє число двійкових вимірювань (проб) з рівноімовірними наслідками типу так-ні для розкриття невизначеності (15). Оскільки на практиці змінні параметри зазвичай мають рівнощільний закон розподілу ймовірності, ентропія такого ансамблю максимальна і визначається формулою Хартлі

$$S_{A\max} = \log_2 A \text{ [дв. вим.] при } p(a_i) = 1/A. \tag{16}$$

Максимально необхідний час $T_{A\min}$ для розкриття невизначеності (16) при байдужих переборних в часі бінарних вимірах дорівнює

$$T_{A\min} = S_A \cdot \tau, \tag{17}$$

де τ – час одного двійкового виміру.

Подібним, але трохи більш складним чином можна оцінити часову, енергетичну, маскувальну, комбіновану, структурну та інші види скритності [5].

Характеристика *цілісності* інформації відображає можливості СПІ забезпечувати необхідну якість передачі інформації в каналу зв'язку при впливі шумів та завад, в тому числі завад, які встановлює порушник щоб зруйнувати легітимний канал зв'язку.

Процес передачі інформації в каналі зв'язку с завадами можна представити графічно, як показано на рис. 3.

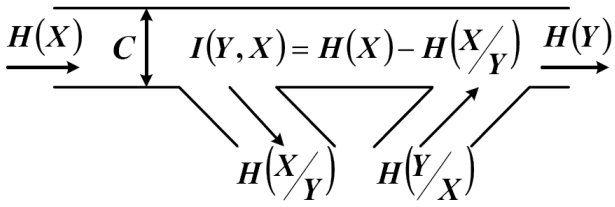

Рис. 3

На рис. 3 умовна ентропія $H(X|Y)$ характеризує виток інформації з каналу зв'язку, а $H(Y|X)$ – середню ступінь невизначеності сигналів, що приймаються, при дії завад.

В загальному випадку для *m*-марного дискретного каналу «шумову» ентропію можна представити виразом [11]

$$H(Y|X) = \sum_{i=1}^{m} p(x_i) \cdot \sum_{j=1}^{m} p(y_j / x_i) \cdot \log_2 \frac{1}{p(y_j / x_i)} = \\ = -(1 - p_{\Pi}) \cdot \log_2 (1 - p_{\Pi}) - p_{\Pi} \cdot \log_2 \frac{p_{\Pi}}{m-1}, \tag{18}$$

де $p_{\Pi} = p(y_1 / x_2) = p(y_2 / x_1)$ – імовірність помилки при передачі будь-якого символу.

Цей вираз показує, що ентропія, яка визначається тільки завадами, не залежить від імовірності появи символів на вході каналу. Якщо символи на вході каналу беруться незалежно від попередніх символів і з однаковими ймовірностями, то ентропія вихідних символів досягає свого максимального значення $H(Y) = \log_2 m$.

Таким чином, кількість інформації, яка передається по каналу, можна визначити як різницю між ентропією на виході та ентропією шуму:

$$I(Y, X) = H(Y) - H(Y|X) == \log_2 m + (1 - p_{\Pi}) \cdot \log_2 (1 - p_{\Pi}) + p_{\Pi} \cdot \log_2 \frac{p_{\Pi}}{m-1}. \tag{19}$$

Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози *доступності*. Інформація в системі повинна бути доступна для легітимних користувачів «у потрібному місті – у потрібний час». При цьому забезпечення відповідних параметрів у СПІ вимагають розв'язання різноманітних пошукових задач [12, 13], зокрема:

– параметричний пошук складних складових сигналів типу ШШС в площині «частота-затримка» в системах завадозахищеного радіозв'язку;

– пошук «стрибаючих» частот в радіомережах з ППЧР;

– взаємний просторовий пошук кореспондентів – повітряно-космічних об'єктів в їх зонах невизначеності бортовими зв'язковими квантово-оптичними приймально-передаючими модулями [14, 15];

– переборний або словниковий методи пошуку і розкриття паролів різної структури та довжини в задачах атаки або захисту паролів в галузі забезпечення інформаційної безпеки.

Існує розвинута класифікація видів пошуку і велика кількість пошукових процедур і алгоритмів. Традиційними критеріями, використовуваними при пошуку об'єкта, є ймовірність, точність і час його виявлення [13].

Найбільш легко піддається ентропійним розрахункам так званий дихотомічний пошук, процедура якого зводиться до послідовного зменшення вдвічі зони пошуку на кожному кроці з визначенням в одній з половинок наявності об'єкта до визначення його місця розташування з необхідною точністю [15].

Ентропія невизначеності зони такого пошуку визначається за аналогією з виразом (16)

$$H(M)_{\partial n} = \log_2 M \text{ ,[дв. вим./комірку з об'єктом],} \qquad (20)$$

де M – кількість елементарних комірок в зоні пошуку, розмір яких визначається.

Узагальненням дихотомічного пошуку є поліхотомічний, при якому зона пошуку ділиться не на *2*, а на μ частин на кожному його кроці.

Ентропійна оцінка поліхотомічного пошуку відрізняється від виразу (20) лише підставою логарифма μ

$$H(M)_{nn} = \log_{\mu} \mathrm{M} \text{ , [μ – ічн. вим./комірку з об'єктом].} \qquad (21)$$

Так, наприклад, при $M = 64$ комірки дихотомічний пошук ($\mu = 2$) буде складатися з 6 кроків, а поліхотомічний зі значенням $\mu = 4$ – з трьох кроків.

Величини $H(M)_{\partial n}$ і $H(M)_{nn}$ також є оцінкою знизу процедур дихотомічного та поліхотомічого пошуків. Їх часові характеристики визначаються виразами

$$T_{\partial n} = \tau H(M)_{\partial n} = \tau \log_2 M, \text{ [с];} \qquad (22)$$
$$T_{nn} = \tau H(M)_{nn} = \tau \log_{\mu} M \text{ , [с].}$$

Подібні види пошуку використовуються при застосуванні в радіозв'язку з ШШС, побудованих на основі функцій Радемахера і Уолша, а також у підсистемах кутового пошуку-наведення-автосупроводження лазерних космічних систем передачі інформації, де дихотомічний пошук забезпечує виграш у порівнянні з переборним послідовним у $M / \log_2 M$ раз, а поліхотомічний – в $M / \log_{\mu} M$ раз.

Зазначимо, що дихотомічний пошук по своїй суті є одночасно відмінним навчальним прикладом для демонстрації і розуміння сенсу ентропії ансамблю рівноймовірних об'єктів (осередків, символів, сигналів).

Для паралельного пошуку число кроків через ентропію може бути записано у вигляді

$$H(M)_{пар.п} = \log_{\mu} M = 1, [\,\mu\text{– ічн. вим./комірку з об'єктом];} \qquad (23)$$
$$T_{пар.п.} = \tau \log_{\mu} M = \tau \text{ , [с],}$$

а для послідовного пошуку наступним чином

$$H(M)_{посл.п} = \log_2 2^M = M \log_2 2 = M \text{ , [вим./комірку з об'єктом]} \qquad (24)$$
$$T_{посл.п.} = \tau M \text{ ,[с];} \qquad \overline{T} = 0{,}5\tau M \text{ , [с].}$$

Розглянемо характерний для завадостійкого супутникового радіозв'язку із застосуванням ШШС двовимірний послідовний пошук у площині частота f затримки T. Такий пошук проводиться незалежно по двом параметрам і може бути оцінений через ентропію складних подій, яка формально записується у вигляді

$$H(X,Y) = -\sum_{i=1}^{n} \sum_{j=1}^{m} P(x_i; y_j) \log_2 P(x_i; y_j), \qquad (25)$$

де $P(x_i; y_j)$ – імовірність спільного появу символів x_i і y_j.

Проте завдання можна спростити. Нехай пошук по затримці оцінюється зрушенням ПВП довжиною *M* біт. Тоді число різних зсувних комбінацій ПВП за фіксований період визначиться як 2^M. Нехай кількість елементарних частотних інтервалів ΔF в діапазоні Δf розладу частоти по Доплеру дорівнює $N=\Delta f/\Delta F$. Тоді загальне число кроків по виявленню об'єкта (сигналу), очевидно, буде дорівнює $(2^M)^N$. А ентропія такого пошуку буде мати вигляд

$$H(M,N)_{f-\tau} = \log_2(2^M)^N = MN\log_2 2 = MN\text{, [вим./об'єкт]} \qquad (26)$$

а середній час пошуку $\overline{T}_{f-\tau} = \frac{\tau}{2}MNc$. Це відповідає відомим виразам, отриманим іншим шляхом [12].

Розглянемо ще одне пошукове завдання в галузі парольного захисту інформації при доступі к системі обробки інформації.

Нехай А – число символів в алфавіті, що використовується для набору пароля, S – довжина пароля в символах, включаючи пробіли та інші службові символи; $t_П$ – час введення пароля в секундах з урахуванням часу затримки між дозволеними спробами введення неправильного пароля.

У цьому випадку ентропія ансамблю паролів (АП) може бути записана у вигляді

$$H(АП) = \log_2 2^{A^S} = A^S\text{, [вим./пароль].} \qquad (27)$$

Середній час розкриття пароля можна записати як

$$\overline{T} = \frac{A^S \cdot t_П}{2}. \qquad (28)$$

Так, наприклад, якщо $A = 26$ символів (літери англійського алфавіту), $t_П=2c$, $S=6$ символів, середній час розкриття пароля становить близько одного року.

Для ряду пошукових задач можна запропонувати новий ефективний критерій на базі середньої кількості інформації, яка отримана в результаті пошуку, який також виражається через ентропію [13].

Дійсно, точність визначення координат об'єкта тим вища, чим менша ентропія положення об'єкта, а усереднення кількості інформації з усіх результатів пошуку враховує ймовірність зміни ентропії положення об'єкта в результаті пошуку. Кількість інформації, що отримується в результаті пошуку, дорівнює різниці ентропій безперервних повідомлень про становище об'єкта до і після пошуку (H_1 и H_2 відповідно) і визначається формулою

$$I = H_1 - H_2 = -\iint_S \omega_1(x,y)\log_2\omega(x,y)dxdy + \int_\Omega\left[\iint_S \omega_2^z(x,y)\log_2\omega_2^z(x,y)dxdy\right], \qquad (29)$$

де $\omega_1(x, y)$ и $\omega_2^Z(x, y)$ – щільності розподілу положення об'єкта до пошуку і при *z*-му результаті пошуку.

Очевидно, галузь застосування ентропії може бути розширена на оцінку і розрахунок покрокових і часових характеристик більш складних видів пошуку: двоетапного, багатоетапного, комбінованого, взаємного та ін.

Згідно [16] загроза інформаційної безпеки у СЗІ визначається, як «причина або подія, які можуть чинити негативний вплив на інформаційний актив і призводити до втрати конфіденційності, цілісності або доступності активу». Тобто загроза включає в себе два фактори: «причину» і «можливі наслідки». Іншими словами, загроза являє собою пару {джерело, вразливість}, кожен з компонентів якої можна характеризувати своїми частотними, часовими та іншими показниками.

Беручи до уваги все різноманіття факторів, які потрібно враховувати при оцінці інформаційного ризику, слід визнати, що невизначеності в цих факторах більше ніж статистичної

виразності. У зв'язку з цим можна припустити, що оцінки невизначеності ризиків є більш коректними, ніж оцінки ймовірності реалізації загрози. Враховуючи те, що мірою невизначеності є ентропія, то слід чекати більш широкого використовування ентропійного підходу для оцінки інформаційних ризиків при вирішенні задач оцінки ризиків інформаційної безпеки при моделюванні і створенні ефективних СЗІ [17].

Висновок

1. Показано можливості застосування інформаційно-теоретичного підходу для оцінки параметрів захищеності систем передачі інформації на канальному та фізичному рівнях взаємодії систем зв'язку.

2. Показано, що за допомогою поняття і аналітичного вираження ентропії можна оцінити параметри СПІ згідно з функціональними критеріями захищеності. Розглянуті приклади такої оцінки демонструють свою універсальність і показують ефективність застосування ентропійного підходу.

3. Галузь використання ентропії може бути розширена на розрахункові задачі оцінки покрокових і часових характеристик різних видів пошуку об'єктів: поліхотомічного, двоетапного, багатоетапного, комбінованого, взаємного та ін. Новий ефективний критерій середньої кількості інформації, отриманої в результаті пошуку, також виражається через ентропію.

Список літератури: 1. *Лидовский В. В.* Теория информации : учеб. пособие. – М. : Компания Спутник, 2004. – 111 с. 2. *Shannon C. E.* A mathematical theory of communication. // Bell System Technical Journal. – 1948. – Vol. 27. – pp. 379-423. 3. *Каган И.М.* Прикладная теория информации. – М. : Радио и связь, 1981. – 216 с. 4. *Вилсон А. Дж.* Энтропийные методы моделирования сложных систем. – М. : Наука, 1978. – 248 с. 5. *Каневский М.* Энтропийная оценка скрытности радиопередачи. – Радиотехника. – 1980. – Т.35, №4. 6. *Методы* прогнозирования защищенности ведомственных систем связи на основе концепции отводного канала / Под ред. А. И. Цопы, В. М. Шокало. – Харьков : КП «Городская типография», 2011. – 502 с. 7. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. – К. : Департамент спеціальних телекомунікаційних систем та захисту інформації СБУ, 1999. – 57 с. 8. *Wyner A.D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355-1387. 9. *Csisz´ar I., K¨orner J.* Broadcast Channels with Confidential Messages // IEEE Trans. Inform. Theory. –1978. –Vol. 24, № 3. – pp. 339–348, May 1978. 10. *Коржик В. И., Яковлев В. А.* Неасимптотические оценки эффективности кодового зашумления одного канала // *Проблемы передачи информации*. – 1981. – Т. 17, Вып. 4. – С. 11–18. 11. *Борисов В.А., Калмыков В.В., Ковальчук Я.М.* и др. Радиотехнические системы передачи информации / Под ред. В.В. Калмыкова. – М. : Радио и связь, 1990. – 304 с. 12. *Хеллман О.* Введение в теорию оптимально поиска. – Пер. с англ. ; под ред. Н.Н. Моисеева. – М. : Наука. Гл. ред. физ.-мат. литературы, 1985. – 248с. 13. *Головинский О. Б., Лавинский Г. В.* Поисковые системы. – К. : Техніка, 1979. – 104с. 14. *Минаев И.В., Мордовин А. А., Шереметьев А. Г.* Лазерные информационные системы космических аппаратов. – М. : Машиностроение, 1981. – 272. 15. *Авт. свид.* СССР №1297698 по заявке на изобретение «Способ взаимного вхождения в связь двух удаленных объектов» / Макаров Л. Б., Брезгунов А. В. Зарегистрировано в Гос. реестре изобретений СССР 15.11.1986г. 16. *ДСТУ 13335-1:2003.* Інформаційні технології. Настанови з керування безпекою інформаційних технологій (ІТ). Ч. 1. Концепції та моделі безпеки ІТ. 17. *Прангишвили И.В.* Энтропийные и другие системные закономерности: Вопросы управления сложными системами / Ин-т проблем управления им. В.А. Трапезникова. – М. : Наука, 2003. – 418 с.

Харківський національний
університет радіоелектроніки

Надійшла до редколегії 08.07.2013