компьютерных сетях / Голубенко А. Л., Петров А. С., Хорошко В. А. // Вісник СНУ ім. В. Даля, №15 (204), 2013, ч. 1. – С. 9-14. **7.** *Бурячок В. Л. Основи формування державної системи кібернетичної безпеки / Бурячок В.Л. – К.: Вид. НАУ, 2013. – 432 с.*

Сергій Довбня, Андрій Нікірін, Іван Четверіков
Київський Національний університет імені Тараса Шевченка

УДК 621.321

СТВОРЕННЯ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МАТРИЦ НЕБЕЗПЕЧНИХ ФАКТОРІВ, ЩО ХАРАКТЕРИЗУЮТЬ ТЕХНІЧНІ КАНАЛИ ВИТОКУ

Анотація: **Наведено формальний опис технічних каналів витоку інформації та завдання створення системи технічного захисту інформації. Наведено метод рішення завдання створення системи захисту інформації.**
Summary: **A formal specification over of technical channels of source of information and task of creation of the system of technical defence of information is brought. A method over of decision of task of creation of the system of defence of information is brought.**
Ключові слова: **Технічній канал витоку інформації, технічні засоби розвідки, система технічного захисту.**

Вступ

Забезпечення захисту інформації спрямовується зокрема на те, щоб не допустити збитків від утрати конфіденційної інформації. Відповідно до цього, уже передбачається наявність цінної інформації, в разі втрати якої можуть бути понесені збитки. А якщо є цінна інформація, то звичайно ж є можливість здійснення будь-яких дій, які можуть нанести шкоду цій інформації. Усі шкідливі дії можуть бути здійснені тільки за наявності будь-яких слабких місць (уразливостей) (див. рис. 1).

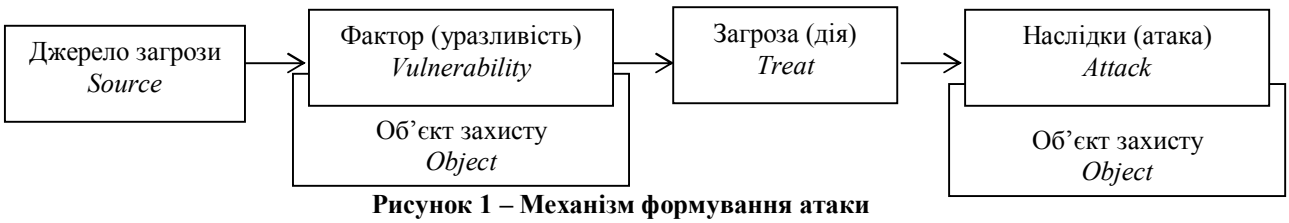

Рисунок 1 – Механізм формування атаки

А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виходити.

Виникає наступний ланцюжок: джерело загрози – фактор (уразливість) – загроза (дія) – наслідки (атака).

Джерело загрози – це потенційні антропогенні, техногенні або стихійні носії загрози безпеці.

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (уразливість) – це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами процесу функціонування об'єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються, програмним забезпеченням і апаратними засобами, умовами експлуатації.

Наслідки (атака) – це завжди пара "джерело-фактор", що реалізує загрозу та приводить до збитків.

Слід зазначити, що захист інформації відповідно до рекомендацій нормативних документів здійснюється за двома основними напрями: захист інформації від її витоку технічними каналами, що виникають в процесі її обробки, і захист інформації від несанкціонованого до неї доступу. У даній публікації мова піде про захист інформації від витоку її технічними каналами. При цьому під технічним каналом витоку інформації розуміється канал витоку інформації, несанкціоноване перенесення інформації в якому від джерела до зловмисника здійснюється з використанням технічних засобів. Основною класифікаційною ознакою технічного каналу витоку інформації є фізична природа носія інформації. За цією ознакою вони поділяються на оптичні, радіоелектронні, акустичні, матеріально-речові.

Інформаційні сигнали можуть бути електричними, електромагнітними, акустичними і ін. Вони мають у більшості випадків коливальний характер, а інформаційними параметрами є амплітуда, фаза, частота, тривалість.

Залежно від фізичної природи сигнали поширюються у визначених фізичних середовищах. Середовищем поширення може бути газове (повітряне), рідинне (водне) і тверде. До таких середовищ відносяться повітряний простір, конструкції будівель, сполучні лінії і струмопровідні елементи, ґрунти і тому подібне.

Формальний опис технічних каналів витоку інформації

Один об'єкт може мати декілька можливих технічних каналів витоку інформації (ТКВІ). Тому на вірогідність такого витоку в цілому впливає вірогідність витоку по кожному каналу. Загальним критерієм для усіх типів каналів є рівень загрози застосування технічних засобів розвідки (ТЗР). Якщо просочування інформації може завдати збитку – прямо або за рахунок зниження конкурентоспроможності, – захист необхідно проводити.

Методи отримання інформації за можливістю застосування технічних засобів розвідки і інформативності каналів витоку інформації можливо розподілити за чотирма напрямками.

Перший напрямок. Дистанційний пасивний безконтактний. Використовуються технічні канали витоку інформації без контакту з комунікаціями і елементами конструкції об'єкту. Характеризується високою скритністю застосування і мінімальним ризиком для зловмисника. Проте інформативність каналів цього типу невисока, оскільки умови їх виникнення випадкові і недостатні для упевненого відновлення інформації. Вірогідність використання цього методу мало залежить від загального рівня загрози застосування технічних засобів розвідки.

Другий напрямок. Дистанційний контактний (пасивний). Використовуються технічні канали витоку інформації з установкою розвідзасобів в різних комунікаціях без застосування активної дії. Досить висока скритність застосування, але є ризик їх виявлення, особливо, якщо комунікації, якими поширюється сигнал, загальнодоступні. Інформативність дещо вища, оскільки використовуються фізичні принципи, що формують стійкіші канали передачі інформації. Вірогідність використання цього методу зростає залежно від загального рівня загрози застосування ТЗР.

Третий напрямок. Дистанційний активний. Метод грунтований на формуванні навмисного каналу витоку інформації. Джерело випромінювання і приймальна апаратура розташовані за межами контрольованої території. У каналах цього типу використовується високочастотне електромагнітне поле, у тому числі в оптичному діапазоні (високочастотне "накачування", лазерне знімання мовної інформації і т. п.). Така дія легко може бути виявлена при застосуванні в системі захисту відповідних індикаторів. Досить висока інформативність. Вірогідність використання цього методу істотно зростає залежно від загального рівня загрози застосування ТЗР. Вона буде істотно нижча, якщо "зловмиснику" відомо про наявність ефективної системи захисту інформації.

Четвертий напрямок. Впроваджені пристрої. Інформативність впроваджених засобів (закладних пристроїв) дуже висока - для цієї мети вони і розробляються. Також високий ризик їх застосування для "зловмисника". З одного боку він пов'язаний з необхідністю проникнути в приміщення і, чим надійніше вимагається встановити пристрій, тим більше потрібно на це часу. З іншого боку, професійне виявлення і використання закладного пристрою дозволить керівництву фірми однозначно встановити факт застосування ТСР, передавати "достовірну" дезинформацію, встановити сторону, що виявляє цікавість до фірми.

Ризик застосування закладних пристроїв значно зростає з підвищенням загального рівня загрози застосування ТЗР. При цьому підвищується вірогідність використання сучасних високопрофесійних засобів.

Захист інформації не існує сам по собі, у відриві від людини. Він забезпечується для людини і ними же оцінюється. Тому, поняття технічного захисту інформації має не лише об'єктивну, але і суб'єктивну сторону, оскільки оцінка його рівня проводиться людиною. При цьому оцінка рівня захищеності інформації завжди відносна. Спроби безпосередньо надати цій оцінці чисельне значення у більшості випадків безперспективні в плані подальшої інтерпретації результатів.

Це дуже важливий аспект, який призводить до слабкої формалізованості завдання оцінки технічної захищеності інформації і до необхідності оперування лінгвістичними змінними (основними структурними одиницями в мові людей) і, як наслідок, до застосування апарату нечіткої логіки [1 – 3].

Для вирішення широкого кола завдань, пов'язаних з моделюванням нечітко формалізованих процесів, їх прогнозуванням і підтримкою ухвалення рішень, часто використовуються нечітки когнітивні моделі. Безумовними їх перевагами порівнянно з іншими методами є можливість формалізації чисельно незмірних чинників, використання неповної, нечіткої і навіть суперечливої інформації [4, 5].

При побудові нечіткої когнітивної моделі (НКМ) об'єкт дослідження зазвичай представляють у вигляді знакового орієнтованого графа. За таку модель при оцінці ТКВІ (TKUI) може бути прийнятий кортеж:

(1) $TKUI=<G, L, E>$.

G - орієнтований граф, що має одну кореневу вершину і не містить петель і горизонтальних ребер в межах одного рівня ієрархії :

(2) $G=<\{F\}; (Д_у\}>$,

де $\{F\}$ - безліч вершин графа (чинників або концептів в термінології НКМ); $\{D_i]\}$ - безліч дуг, що сполучають i-ую і j-ую вершини (безліч причинно-наслідкових зв'язків між концептами);

$F_0 = K$ - коренева вершина, що відповідає рівню захисту інформації від витоку по ТКВІ в цілому (інтегральному критерію захисту інформації - цільовому концепту);

L - набір якісних оцінок рівнів кожного чинника в ієрархії:

L ={Низький, Нижче середнього, Середній, Вище за середній, Високий};

E - система стосунків, переваги одних чинників перед іншими в міру їх впливу на заданий елемент наступного рівня ієрархії :

(3) $E=\{F(e) F_j \mid e\ E(>;\sim)\}$,

де F_i і F_j - чинники одного рівня ієрархії;

$>$ - відношення переваги;

$\sim$ - відношення байдужості.

Така система може бути отримана, наприклад, викладеним в [1] модифікованим методом нестрогого ранжування. Цей метод дозволяє визначити узагальнені ваги Фишберна для кожної дуги D_{ij} (ваги зв'язків) (на випадок переваги/байдужості чинників по відношенню один до одного).

Веса Фишберна відображають той факт, що системі спадаючої переваги N альтернатив якнайкраще відповідає система вагів, що знижуються за правилом арифметичної прогресії.

Тому ці ваги є раціональними дробами, в знаменнику яких стоїть сума N перших членів натурального ряду (арифметичній прогресії з кроком 1), а в чисельнику - елементи натурального ряду, що убувають на одиницю, від N до 1 (наприклад, 3/6, 2/6, 1/6). Таким чином, перевага по Фишберну виражається в спаданні на одиницю чисельника рационального дробу вагового коефіцієнта слабкішої альтернативи.

Приклад системи стосунків переваги типу

E ={$U > U_2$; $U_2 > U_3 \sim U_4$; $U_4 \sim U_5$} на фрагмент графа показаний на рис. 2.

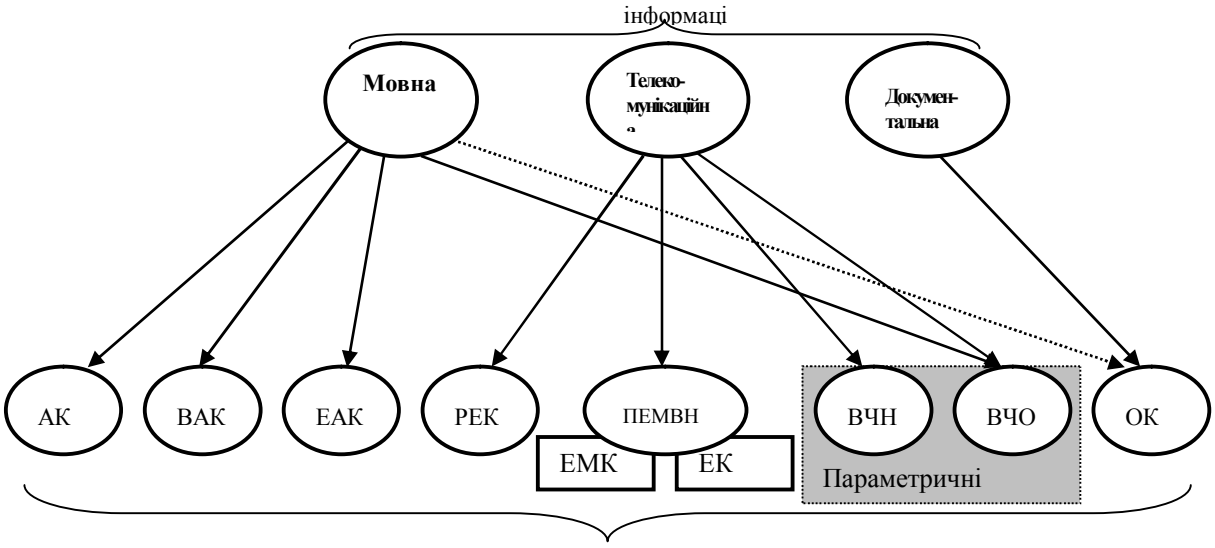

Рисунок 2 – Граф зв'язності

де АК – акустичний канал, ВАК – віброакустичний канал, ЕАК – електроакустичний канал, РЕК – радіоелектронний канал, ЕМК – електромагнітний канал, ЕК – електроакустичний канал, ВЧО – канал високочастотного опромінювання; ВЧН – канал високочастотного нав'язування; ОК – оптичний канал.

Зв'язок між будь-якими двома вершинами (концептами) при необхідності можна також представити у вигляді нечіткої когнитивной моделі нижчого рівня. При цьому на верхній рівень передаватиметься максимальне значення зв'язку, виявлене в ході аналізу НКМ нижнього рівня. Такий ієрархичний спосіб дозволяє спростити побудову НКМ для систем високої міри складності.

Рішення задачи створення системи технічного захисту інформації

Рішення такої задачі необхідно проводити з урахуванням інформації, яка циркулює на об'єкті та її співвідношення з типом технічного каналу [6 - 10]. Цей зв'язок можливо представити графом (рис. 2).

Зазначена таблиця повинна враховувати всі можливі небезпечні фактори, шляхом формування списку всіх відповідних технічних каналів, наприклад: небезпечний фактор – "наявність на ОІД вікон "→" можливість створення ***акустичного, віброакустичного та оптичного каналів*** витоку інформації (мовної та документальної)".

Для отримання множини небезпечних факторів на основі зазначеної таблиці $\{X_j\}_{\text{НФ}}$ необхідно сформувати алгоритм оцінки захищеності. Алгоритм являє собою сукупність послідовних "тестових" дій спеціаліста в галузі ТЗІ щодо об'єкта та формування для кожного можливого технічного каналу однорозмірної матриці небезпечних факторів. Наприклад, зазначені матриці можуть мати такий вигляд:

$$
\begin{aligned}
A_{\text{РЕК}} &= \left|X_4 \quad X_5 \quad X_6 \quad X_7 \quad X_9\right|;\\
A_{\text{ЕАК}} &= \left|X_{19} \quad X_{20} \quad X_{21} \quad X_{22} \quad X_{23} \quad X_{24} \quad X_{25} \quad X_{26} \quad X_{27}\right|;\\
A_{\text{АК}} &= \left|X_{28} \quad X_{29} \quad X_{35}\right|;\\
A_{\text{ВАК}} &= \left|X_{28} \quad X_{29} \quad X_{30} \quad X_{31} \quad X_{32} \quad X_{33} \quad X_{34} \quad X_{35} \quad X_{36} \quad X_{37} \quad X_{38}\right|;\\
A_{\text{ПЕМВН}} &= \left|X_1 \quad X_2 \quad X_3 \quad X_8 \quad X_{11} \quad X_{12} \quad X_{13} \quad X_{14} \quad X_{15} \quad X_{16} \quad X_{17} \quad X_{18}\right|;\\
A_{\text{ВЧН}} &= \left|X_{11} \quad X_{12} \quad X_{13} \quad X_{19} \quad X_{20} \quad X_{21} \quad X_{22} \quad X_{23} \quad X_{24} \quad X_{25} \quad X_{26} \quad X_{27} \quad X_{30} \quad X_{31} \quad X_{32}\right|;\\
A_{\text{ВЧО}} &= \left|X_1 \quad X_2 \quad X_{10} \quad X_{11} \quad X_{12} \quad X_{13} \quad X_{14} \quad X_{24}\right|;\\
A_{\text{ОК}} &= \left|X_{35}\right|.
\end{aligned}
\qquad (1)
$$

Значення кожного небезпечного фактора (НФ) визначається на бінарній шкалі, тобто:

$$
X_i = \begin{cases} 1, & \text{якшо НФ є;} \\ 0, & \text{якщо НФ немає,} \end{cases} \quad i = \overline{1, M}, \quad M = 38. \qquad (2)
$$

За результатом проведення обстеження та первинної інструментальної (розрахункової) оцінки захищеності для кожного можливого технічного каналу маємо бінарні матриці розміром $N_{\text{експ}} \times M_l$, де M_l – кількість НФ, що характеризують l-й технічний канал.

Для отримання одномірної матриці необхідно застосувати процедуру згортання значень отриманих оцінок для кожного НФ на "найгірший" випадок:

$$
X_i^l = X_{i,1} \vee X_{i,2} \vee \ldots \vee X_{i,N_{\text{експ}}},\ i = \overline{1, M_l};\ j = \overline{1, N_{\text{експ}}};\ l = \overline{1, L}, \qquad (3)
$$

де L – кількість можливих технічних каналів витоку інформації на конкретному об'єкті за результатами проведеної оцінки;

M_l – кількість небезпечних факторів, що характеризують l-й технічний канал;

$N_{\text{експ}}$ – кількість варіантів оцінки захищеності (атестації, експертизи отриманих результатів).

В результаті маємо сукупність матриць $A^*_{\text{РЕК}}$; $A^*_{\text{ЕАК}}$; $A^*_{\text{АК}}$; $A^*_{\text{ВАК}}$; $A^*_{\text{ПЕМВН}}$; $A^*_{\text{ВЧН}}$; $A^*_{\text{ВЧО}}$; $A^*_{\text{ОК}}$, які фактично визначають формальний опис **о**б'єкту **і**нформаційної **д**іяльності (ОІД).

За отриманими попередніми даними оцінки захищеності інформації від витоку технічними каналами необхідно провести інструментальний контроль (випробування) та визначити остаточний список можливих технічних каналів витоку інформації на об'єкті. Для цього здійснюється аналіз матриц за правилом:

$$
K_l = \begin{cases} \text{є}, & \text{якщо} \quad X_1 \vee X_2 \vee \ldots \vee X_i = 1, i = \overline{1, M_l}; \\ \text{ні}, & \text{якщо} \quad X_1 \vee X_2 \vee \ldots \vee X_i = 0, \end{cases} \qquad (4)
$$

де M_l – кількість НФ, що характеризують l-й технічний канал.

За результатами цього кроку маємо множину $\{K_l\}_{\text{ТКВІ}}$, $l = \overline{1, L}$, де $L \le 8$.

Для кожного технічного каналу із множини $\{K_l\}_{\text{ТКВІ}}$ визначається його важливість.

Незважаючи на різницю у кількості небезпечних факторів (4), які визначають кожен можливий технічний канал, ця кількість не визначає ступінь небезпеки самого технічного каналу.

Тому для визначення коефіцієнтів важливості раціонально використати співвідношення між загальною кількістю НФ конкретного каналу та кількістю НФ, які прийняли значення "1" за результатами попередньої оцінки захищеності інформації. Тоді формула для визначення коефіцієнтів важливості кожного технічного каналу у списку має такий вид:

$$\lambda_l = \frac{M_l^1}{M_l}, \quad l = \overline{1, L}, \tag{5}$$

де M_l^1 - кількість небезпечних факторів *l*-го технічного каналу, які прийняли значення "1" за результатами експертного опитування;

M_l – загальна кількість НФ, що характеризують *l*-й технічний канал.

Таким чином формується множина значень важливості для кожного технічного каналу витоку інформації - $\{\lambda_l\}_{\text{ТКВІ}}$, $l = \overline{1, L}$.

За результатами виконання попередніх етапів можливо провести ранжування технічних каналів за важливістю та сформувати остаточний перелік технічних каналів витоку інформації на ОІД: $\{K_l\}^*_{\text{ТКВІ}}$, $l = \overline{1, L}$, де $L \le 8$.

На підставі вищевикладеного загальне завдання створення системи ТЗІ на основі нечіткого когнітивного моделювання можна представити в наступному виді:

1. Збір інформації про об'єкт захисту, вибір критеріїв, що характеризують стан різних ТКВІ, визначення їх прийнятного рівня (можливо у вигляді інтервальних оцінок або лінгвістичних термінів).
2. Побудова когнітивної моделі у вигляді знакового орієнтованого графа з накладеною системою стосунків переваги типу (3).
3. Обчислення вагів Фішберна на підставі модифікованого методу нестрого ранжування.
4. Аналіз рівня захисту інформації (РЗІ).

Якщо РЗІ не знаходиться в прийнятному діапазоні значень, то робляться зміни у складі концептів, які приймають участь в побудові когнітивної моделі, у складі зв'язків між концептами, змінюються їх ваги за допомогою введення захисних заходів, впливи яких відбиваються МПМ і МЛП. Ці зміни відповідають різним стратегіям побудови системи ТЗІ: зменшення ризиків, ухилення від ризиків, прийняття ризиків [7].

Таким чином, процес створення системи ТЗІ має на увазі рішення двох взаємозв'язаних завдань: прямого (аналіз стану системи) і зворотного завдання управління (дія на систему).

При рішенні першої задачі вимагається визначити значення критеріїв просочування інформації K_i і інтегрального критерію K при заданих значеннях усіх концептів, що впливають на них. Якщо отримані значення знаходяться поза діапазоном прийнятності, то при рішенні зворотної задачі необхідно підібрати такі дії Z_i і L, що управляють, які забезпечать повернення цільових критеріїв у безпечний діапазон.

Якщо існує не єдиний набір необхідних управляючих дій, то на цьому етапі може виникнути завдання оптимізації, що полягає в знаходженні такої комбінації *Zi* і *L*, яка забезпечує максимальну дію на негативні чинники при заданих або мінімальних витратах на реалізацію способів і засобів захисту.

Висновки

1. Запропонована методика має узагальнений характер, відповідає висунутим до неї вимогам та враховує положення чинних нормативно-методичних документів з питань протидії технічним розвідкам.
2. За результатами її застосування маємо кінцеву множину значень показників оцінки за кожним типом засобів технічних розвідок та остаточний список небезпечних засобів, які забезпечують прийняття технічно обґрунтованих рішень щодо протидії на об'єкті.
3. Методика має завершену логічну структуру та упорядковує складний процес формалізованого опису об'єкта, умов ведення розвідки та засобів технічних розвідок.
4. Можливість автоматизації розглянутих у методиці алгоритмів, побудова спеціалізованих баз даних та спеціального програмного забезпечення робить процес оцінки можливостей технічних розвідок доступним для звичайного фахівця, який відповідає за проектування та впровадження заходів ТЗІ на ОІД.
5. Нормальне життя суспільства все більше залежить від правильності функціонування інформаційних систем. Вони стають найважливішим об'єктом для атаки з боку сил, ворожих для суспільства (або окремої держави). Інформаційна сфера стає не тільки однією з найважливіших сфер міжнародного співробітництва, але і об'єктом суперництва.

Список використаної літератури: ***1****. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн.1. М.: Энергоатомиздат, 1994. 400 с.* ***2****. Антонов А. В. Системный анализ. Методология. Построение моделей: Учебное пособие. Обнинск: ИАТЭ. 2001. 272 с.* ***3.*** *Домарев В. В. Безопасность информационных технологий: Методология создания систем защиты. К.: ООО "Тид "ДС". 2001. 688 с.* ***4.*** *Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. М.: Изд-во МГУ, 1982. 120 с.* ***5****. Хорев А. А. Способы и средства защиты информации: Учебное пособие. М.: МО РФ, 1998. 315 с.* ***6.*** *ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.* ***7.*** *Богуш В. М., Кудін А. М. Інформаційна безпека від А до Я. 3000 термінів і понять – К.: МОУ, 1999. – 456 с.* ***8.*** *Технические средства и методы защиты информации. Учебное пособие для вузов/ А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия-Телеком, 2012. – 616 с: ил.* ***9.*** *Богуш В. М., Юдін О. К. Інформаційна безпека держави. – К.: "МК-Прес", 2005. – 432 с., іл.* ***10.*** *Богуш В. М. Розвідка в інформаційному суспільстві: Довідник-словник. – К.: МОУ, 2000. – 768 с.*

Михаил Прокофьев, Василий Стеченко
НДЦ «ТЕЗИС» НТУУ КПИ

УДК 621.372

ОЦЕНКА ВЕРОЯТНОСТИ ПРАВИЛЬНОГО РАСПОЗНАВАНИЯ ИНФОРМАЦИИ ПРИ ПРИЕМЕ ПОБОЧНОГО ИЗЛУЧЕНИЯ ОТ ПАРАЛЛЕЛЬНО ПЕРЕДАВАЕМЫХ СИГНАЛОВ

Анотація: ***Показано шлях розрахунку ймовірності правильного прийому одиниці інформації залежно від відношення сигнал/шум для сигналів з паралельним кодуванням інформації.***
Summary: ***Shows the calculation of the probability of correct reception of units of information, depending on the signal / noise ratio for signals with parallel coding information***
Ключевые слова: ***Защита информации, параллельное кодирование информации.***

I Введение

В средствах вычислительной техники часто применяется параллельная передача информационных сигналов по многопроводному кабелю. Информация передается с помощью электрических сигналов, поэтому в окружающее пространство излучается электромагнитное поле, которое может быть перехвачено средствами технической разведки.

В многопроводном кабеле по n линиям синхронно передаются n двоичных сигналов с потенциальным кодированием информации. Обычно высоким уровнем сигнала кодируется «1», а низким - «0». Средства технической разведки принимают сигнал побочного излучения от всех проводов кабеля, что затрудняет задачу идентификации сигналов в каждом проводе кабеля. О большей защищенности информации при параллельной ее передачи указывается в работах [1, 2], однако численные сравнения отсутствуют. Оценке вероятности правильного приема бита информации при параллельной передаче сигналов и посвящена настоящая статья.

II Основная часть

Количественной характеристикой качества передачи информации является вероятность ее правильного приема, например, вероятность правильного приема одного бита информации. Такая оценка определяет среднее число правильно расшифрованных битов при распознавании принятого сигнала.

Информационные сигналы побочного излучения принимаются на некотором расстоянии без прямого подключения к проводам многопроводной линии. В результате на вход приемного устройства поступает суммарный сигнал, излученный всеми проводами многопроводной линии. По результатам измерения этого суммарного сигнала необходимо определить значение переданных символов в каждой линии.

За один такт количество передаваемых многопроводной линией информационных битов совпадает с количеством сигнальных проводов в линии n. В зависимости от номера линии и уровня передаваемого сигнала (высокий – «1», низкий – «0») общее количество возможных вариантов комбинаций символов, которое одновременно передается многопроводным кабелем, равно 2^n. При передаче электрического сигнала в пространство излучается электромагнитное поле и уровень излученного сигнала может изменяться в больших пределах. Минимальный уровень излучения будет при передаче по всем линиям «0», а