УДК 621.321

к.військ.н., доц. **Довбня С.Я.** (КНУ)
к.т.н., с.н.с. **Кривцун В.І.** (Академія СВ)
к.т.н., доц. **Четверіков І.О.** (КНУ)
Савран В.О. (ВІКНУ)
Солдатенко О.О. (КНУ)

НАУКОВО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У статті розглянуто підхід до аналізу загроз для інформації, визначення методів та засобів захисту інформації в інформаційно-телекомунікаційних системах із застосуванням логіко-лінгвістичного методу. Засоби технічних розвідок представляється інтегрованим оптимальним приймачем. Загрози та ризики до інформації представляються з використанням теорії нечітких множин. Визначення рівня захищеності інформаційно-телекомунікаційних систем здійснюється шляхом оцінки якості маскуючи акустичних та електромагнітних шумів. Методи визначення ентропійного коефіцієнта якості та коефіцієнту між спектральних зв'язків маскуючого шуму, дозволяють дослідити процеси у ймовірнісній області і оцінити забезпечення інформаційної безпеки. При цьому використовується векторно-матричний підхід до дослідження засобів технічного захисту інформації. Перевагою методу є можливість зручної алгоритмізації процесу дослідження систем інформаційної безпеки.

Ключові слова: аналіз загроз, система інформаційної безпеки, методи теорії нечітких множин.

Нині розвиток сучасних інформаційних технологій, під якими розуміються процеси, методи пошуку, збору, зберігання, обробки, представлення, розповсюдження інформації та способи здійснення таких процесів і методів, є одними з найважливіших складових національних інтересів в інформаційній сфері [1, 2].

Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері [2].

Для забезпечення безпеки інформації необхідно вирішити завдання забезпечення конфіденційності, цілісності та доступності.

Таким чином, в умовах розвитку інформаційного суспільства, існує актуальна проблема.

З одного боку підвищуються обсяги інформації, що обробляється в інформаційних і телекомунікаційних системах. Про це свідчить збільшення частки надання державних послуг в електронному вигляді, розвиток системи ситуаційних центрів, повсюдне запровадження електронного документообігу, використання мережі відеоконференц-зв'язок.

З іншого боку - збільшується і ймовірність ризиків, пов'язаних з існуванням загроз безпеки інформації.

У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах.

Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення.

До таких пристроїв відносяться технічні та криптографічні засоби захисту інформації, засоби захисту від помилок, системи розмежування доступу, а також процеси моделювання засобів та систем захисту інформації. На рис. 1 показані загрози інформаційним і телекомунікаційним системам і системи, що використовують у своїй роботі логічні обчислення.

Роботу сучасних цифрових систем передачі і зберігання інформації неможливо уявити без використання методів завадостійкого кодування. Необхідність їх застосування продиктована тим, що канали зв'язку недосконалі і при передачі і зберіганні інформації можлива поява помилок.

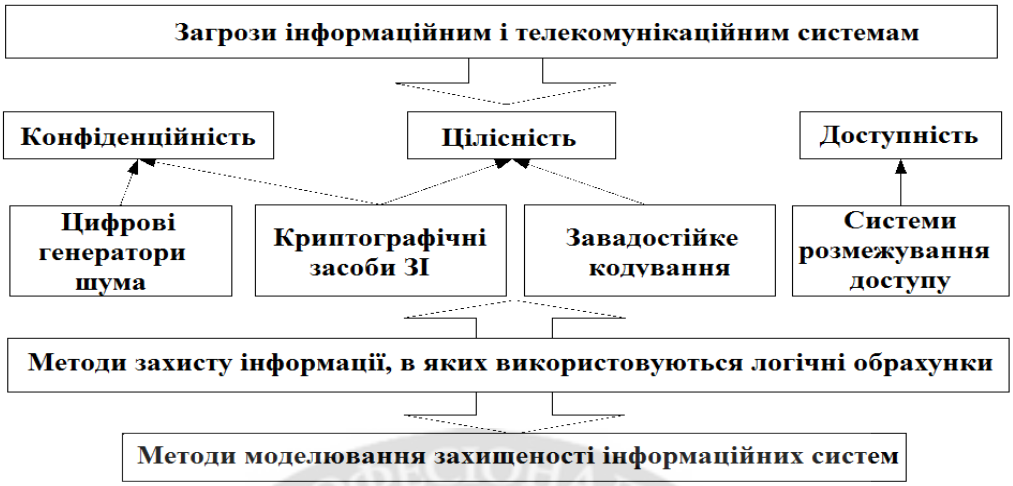

Рис. 1. Взаємозв'язок загроз, методів захисту інформації та моделювання захищеності інформаційних систем

Можна навести приклади систем, що використовують методи завадостійкого кодування, це: системи стільникового, транкінгового, супутникового зв'язку, системи цифрового телебачення, бездротові мережі, системи запису інформації на оптичні диски та ін. [3]

Завадостійкі коди діляться на два класи: блокові коди та згорткові [3]. В реально діючих системах для виявлення та виправлення помилок в основному використовуються коди лінійні блокові коди двох типів: циклічні і ітеративні (матричні), що обумовлено простотою апаратурною або програмною реалізацією кодування та декодування.

Серед лінійних блокових кодів найбільше значення мають коди з однією перевіркою на парність, Хеммінга, Голея, Боуза-Чоудхурі - Хоквінгема, CRC-коди, Ріда-Маллера і ін.

Але засоби технічних розвідок переважно будують з використаних теорії оптимального приймача Котельникова та квазіоптимального приймача з використаних методів адаптації та авто компенсації завад. Цей алгоритм реалізується у загальному вигляді інтегрального приймача-перемножувача m прийнятого $S_{пр}$ сигналу на опорний (еталонний) сигнал $S_{опорн}$ зі схемою прийняття рішень (РС) на виході, де встановлюється відповідній поріг (рис. 2), і має вигляд:

$$R = \frac{1}{T}\int_0^T S_{пр} S_{опорн} dt \begin{cases} \le 0 \\ > 1 \end{cases} \qquad (1)$$

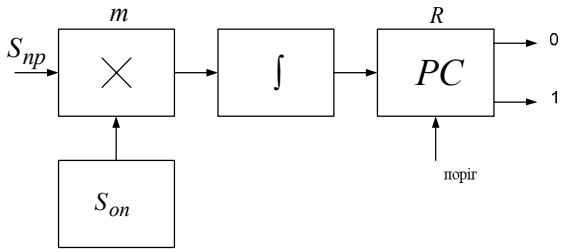

Рис. 2. Структурна схема оптимального інтегрального приймача

Крім того використовують і оптимальні властивості приймача з узгодженим фільтром, частотна характеристика якого $S_ф(f)$ комплексно спряжена з частотною характеристикою

сигналу $S_{\text{пр}}(f)$. Рішення R для приймача з узгодженим фільтром приймається згідно з алгоритмом:

$$R = S_{\text{пр}}(f) \cdot S_{\text{ф}}^{(*)}(f) \begin{cases} \geq 1 \\ < 0 \end{cases}; \quad (2)$$

$$R = S_{\text{пр}}(f) \cdot S_{\text{ф}}(\tau - t) \ . \quad (3)$$

Аналогічне рішення може бути прийняте і щодо перехідних характеристик фільтра $S_{\text{ф}}(\tau - t)$, коли відома перехідна характеристика сигналу $S_{\text{пр}}(f)$.

Тому виникають питання розробки сучасних методів технічного захисту інформації в інформаційно-телекомунікаційних системах.

Розробка моделі загроз, критеріїв та показників оцінки уразливості інформаційних систем і мереж. Аналіз іноземної та вітчизняної літератури з питань захисту інформації та накопичений позитивний досвід побудови моделей загроз для державних об'єктів, дозволяють констатувати, що на сьогодні існує декілька методів оцінки можливих загроз, які варіюються від простих кількісних систем (емпіричних формул) до систем, в основі яких складні математичні викладки [4,5]. Враховуючи це, на рис. 3 представлені основні методи оцінки можливих загроз. Розглянемо ці методи більш докладно.

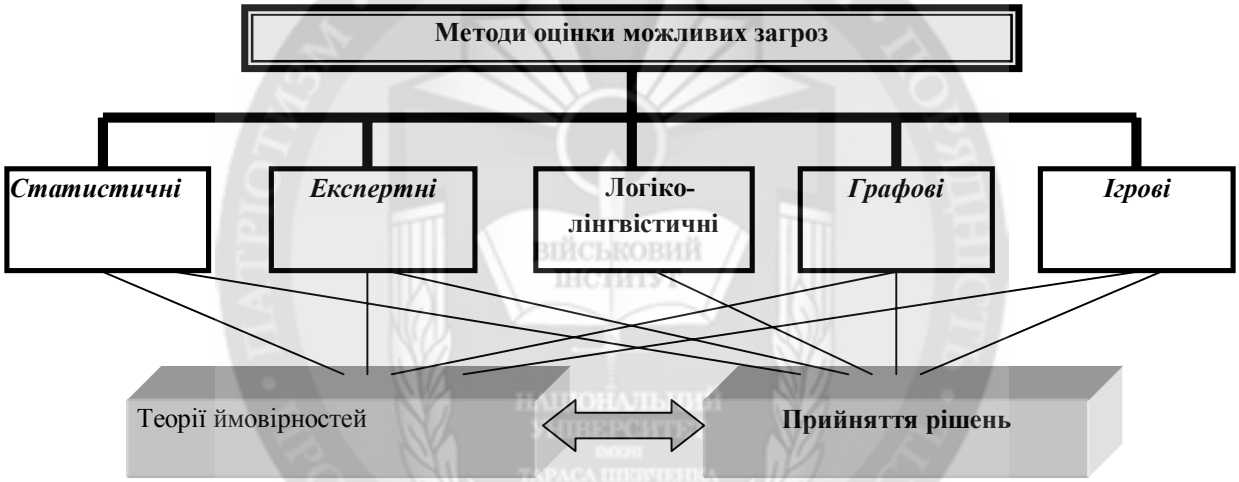

Рис. 3. Основні методи оцінки можливих загроз

Корисність цих методів для оцінки можливих загроз важко переоцінити. Однак, на практиці існують чисельні випадки, коли експерти утрудняються (через високий рівень невизначеності) кількісно оцінити значення параметрів, або зовсім не вдається (наприклад, через новизну проблеми, що вивчається) сформувати групу компетентних спеціалістів достатній чисельності. Проблеми оцінки загроз в галузі технічного захисту інформації відносяться до проблем саме такого типу [4,5,6]. У таких ситуаціях для проведення оцінки загроз доцільно використовувати логіко-лінгвістичні методи (ЛЛМ). Обґрунтованість застосування ЛЛМ полягає в тому, що використання тільки кількісних методів у чисельних випадках приводить до "вихолощування" сутності задач, що вирішуються, втраті їх важливих аспектів, які не підлягають формалізації [7]. Слід відзначити, що поряд із промисловою та комерційною сферами логіко-лінгвістичні методи знайшли широке застосування для підвищення ефективності військових систем, в основі яких лежать принципи ситуаційного управління.

Актуальність використання логіко-лінгвістичного підходу для формалізованого опису задач оцінки можливих загроз в галузі ТЗІ, обумовлена їх особливостями, до яких слід віднести:

- багатокритеріальний характер більшості цих задач та наявністю поряд із кількісними якісних показників [8], необхідних для оцінки загроз;

• необхідністю врахування великої кількості різноманітних характеристик об’єкта, які обумовлюють небезпечні фактори, під час проведення оцінки;

• високим рівнем невизначеності вихідних даних для рішення задач оцінки, особливо, на початковому етапі проектування заходів із ТЗІ;

• будь-яку оцінку можливих загроз здійснюють спеціалісти-експерти з питань ТЗІ, рішення яких мають високий рівень суб’єктивізму (власних переваг).

Зазначені особливості обумовлюють перспективність та доцільність використання поряд із традиційними математичними методами (математичної статистики, експертного оцінювання, теорії ймовірностей) логіко-лінгвістичного підходу на основі теорії нечітких множин (ТНМ), яка дозволяє формалізувати словесний опис, який отримується від експертів, у вигляді математичних виразів, і врахувати їх нечіткість через оцінки істинностей (приналежностей) та переваг. Математичний та логічний апарат нечітких множин спрямований на пошук й оцінку переваг під час вибору рішення $\boldsymbol{A}$ на базовій множині альтернатив $\boldsymbol{X}$. Це відповідає тому психологічному факту, що експерт (особа, що приймає рішення (ОПР) завжди спирається на деяку структуру переваг [6-8].

Крім того, якісний, а саме лінгвістичний характер оцінок загроз (ризиків) під час вирішення конкретних задач ТЗІ має місце у міжнародній практиці визначення рівня загроз та очікуваної шкоди від їх реалізації.

При цьому кожен з експертів спроможний дати власні оцінки граничних ймовірностей прояву загроз або використати типову шкалу, яка пропонується керівником експертного опитування. Наприклад, в автоматизованій системі аналізу ризиків CRAMM (розробник – компанія Logica, Великобритания) на основі результатів експертного оцінювання вибираються значення наступних лінгвістичних змінних: «рівень загроз»={“дуже високий”, “високий”, “середній”, “низький”, “дуже низький”}та «рівень вразливості інформації»={“високий”, “середній”, “низький”} [7].

У [12] доведено, що значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо. При цьому оцінка може мати числове або лінгвістичне значення (наприклад, «ймовірність реалізації загрози» = {незначна, низька, висока, неприпустимо висока}).

Рівні захищеності інформаційних систем. Для забезпечення безпеки інформації, при її обробки в інформаційних системах, розробляють і використовують політику безпеки, під якою розуміється сукупність норм і правил,що регламентують процес обробки інформації, виконання яких забезпечує захист від певної множини загроз і становить необхідну (а іноді і достатню) умову безпеки системи. Формальний вираз політики безпеки називається моделлю політики безпеки. Основні моделі політик безпеки можуть бути наступні: дискреціонна, мандатна, рольова, безпеки інформаційних потоків, ізольованої програмного середовища.

В дискреціонній моделі розмежування доступу основою є матриця доступу, визначальна наявність того чи іншого права суб'єкта по відношенню до об'єкта інформаційної системи. Визначення прав в відповідності з матрицею доступу можна звести до обрахунку системи бульових функцій. Політика рольового розмежування доступу є розвитком політики дискреційного розмежування доступу, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх застосування, утворюючи ролі.

В даний час розроблено цілий ряд методів захисту інформації в інформаційних системах, для реалізації яких існує безліч засобів захисту, що постійно оновлюються. Кожна конкретна захищена інформаційна система має свої особливості (важливість оброблюваної і збереженої інформації, умови функціонування і т. п.), які визначають вимоги до системи захисту інформації. У цих умовах практично важливим є отримання оцінок ефективності різних варіантів реалізації системи захисту інформації, що згодом може бути використано

для вибору оптимального з точки зору пропонованих вимог комплексу захисних методів і засобів, необхідних для її створення [11, 13].

Збиток, що наноситься захищеній інформаційній системі загрозами, часто реалізується досить швидко, тому для коректної оцінки ефективності системи захисту інформації необхідно враховувати динаміку функціонування даної системи. Отримання оцінок ефективності системи захисту інформації з урахуванням динаміки, можливо на основі математичного моделювання процесу функціонування захищеної інформаційної системи в умовах впливу загроз, яке, здійснюється з використанням теорії автоматів [13].

Але для визначення рівня захищеності інформаційно-телекомунікаційних систем в першу чергу необхідно вирішити завдання визначення сучасних вимог до засобів (комплексів) захисту інформації та оцінка їх реалізації [10, 11].

Розглянемо ці питання на прикладі створення та випробувань засобів активного захисту інформації від витоку акустичними та віброакустичними каналами, за рахунок використання лазерних засобів знімання інформації та витоку каналами побічних електромагнітних випромінювань та наведень (далі – ПЕМВН). При цьому за основний параметр оберемо якість маскуючого шуму.

Оцінка якості акустичного маскуючого шуму. У відомих способах для оцінки якості маскуючого шуму визначають еталонні статистичні характеристики миттєвих значень маскуючого шуму (нормальний закон розподілу), при яких досягається максимальний маскувальний ефект. Потім визначають ентропійний коефіцієнт якості для реального випромінюваного маскуючого шуму, статистичні характеристики якого відхиляються від еталонних. Використовують отримане значення ентропійного коефіцієнта для оцінки якості маскуючого шуму [11]. Але, описаний спосіб має істотний недолік. При наявності спектральних складових в маскуючому шумі має місце велика похибка визначення ентропійного коефіцієнта якості маскуючого шуму, оскільки в цьому випадку закон розподілу миттєвих значень напруг електричного сигналу буде мало відрізняться від нормального закону розподілу. У той же час наявність спектральних складових в маскуючому шумі різко знижує його якість, оскільки значна частина енергії маскуючого шуму буде зосереджена в спектральних складових, які не володіють маскуючими властивостями і які можуть бути видалені при прийомі акустичного мовного сигналу режекторними фільтрами.

Для усунення даного недоліку, пропонується обчислити ентропійний коефіцієнт якості η^0 обвідної електричного сигналу по формулі

$$\eta^0 = \frac{e^{\mathrm{H}^0}}{e^{\mathrm{H}^{\mathrm{p}}}} = e^{\left(H^0 + m - 2\ln k - \frac{\sigma_0^2}{2k^2}\right)}.$$

А також обчислити ентропійний коефіцієнт якості η маскуючого акустичного (віброакустичного) шуму за формулою $\eta = \eta^{\mathrm{M}}\eta^0$, використовуючи отримане значення η ентропійного коефіцієнта якості для оцінки якості маскуючого акустичного (віброакустичного) шуму.

В даному випадку закон розподілу обвідної маскуючого сигналу має жорсткий функціональний зв'язок з енергетичним спектром цього сигналу, то поява в ньому гармонійних складових, а також найменше відхилення спектра маскуючого сигналу від еталонного призводить до зміни закону розподілу обвідної цього сигналу. Еталонний закон розподілу обвідної є релеєвським законом. Оскільки спектр мовної інформації також апроксимується релеєвським законом, то в цьому випадку буде досягатися максимальний маскувальний ефект. Цей максимальний маскувальний ефект відповідає стаціонарному випадковому процесу, у якого миттєві значення випадкової величини підпорядковані нормальному закону розподілу, а значення обвідної випадкової величини підпорядковані релеєвскому закону розподілу.

Еталонний закон розподілу миттєвих значень маскуючого сигналу є нормальним, то в якості обмеження для порівнюваних законів розподілу розглядають тільки дисперсію. В цьому випадку максимальною ентропією володітиме нормальний закон розподілу по відношенню до всіх інших законів розподілу, але оскільки еталонний закон розподілу обвідної маскуючого сигналу є релеєвським, то в цьому випадку в якості обмеження для порівнюваних законів розподілу розглядають другий момент закону розподілу і математичне сподівання логарифма випадкової величини, так як в цьому випадку максимальною ентропією володітиме релеєвський закон розподілу по відношенню до всіх інших законів розподілу, в тому числі і по відношенню до нормального закону розподілу [11].

Оцінка якості електромагнитного маскуючого шуму. Для дослідження якості електромагнітного маскуючого шуму пропонується застосування високошвидкісного реєстратору сигналів – цифрового осцилографу, який має функцію накопичення та запису оцифрованих даних (далі – реєстратор). Характеристики реєстратора, такі як частота дискретизації, робоча смуга частот, граничний розмір масивів накопичення даних, приведена до входу чутливість і вхідний опір, мають відповідати характеристикам вимірювальних антен та датчиків сигналів, що застосовуються при проведенні вимірювань. Процедури обчислення, які проводяться відповідно до викладеної методики, забезпечують нормування виміряних величин та їх відносне оцінювання.

Обчислення здійснюються окремо для кожного типу застосованої вимірювальної антени, а також типу і способу підключення датчиків сигналів. При проведенні розрахунків пропонується використання вбудованих у зазначені засоби обчислень операторів і функцій.

При проведенні робіт з оцінювання коефіцієнтів кореляції захисних сигналів просторового зашумлення, слід встановити на аналізаторі спектру оглядовий діапазон частот, що перекриває робочий діапазон частот вимірювальної антени, смугу пропускання аналізатору, в межах від $0{,}001\cdot\Delta F$ до $0{,}03\cdot\Delta F$, та, при включеному генераторі, обрати і зафіксувати положення вимірювальної антени, при якому спостерігається найменша нерівномірність спектральної характеристики шумового сигналу.

Параметри розгортки та накопичення даних реєстратора слід встановити такими, що забезпечити час накопичення даних більший ніж T та частоту дискретизації більшу ніж Fc.

Підключити вимірювальну антену, або датчик сигналу до високошвидкісного реєстратора та, при включеному генераторі захисних завад, встановити коефіцієнт канальної атен'юації (підсилення) та рівень канального зсуву, за яких мінімальні та максимальні відліки амплітуд шумового сигналу знаходяться в межах від 0% до 10% та від 90% до 100% шкали оцифрування, відповідно. Не змінюючи положень і настроювань складових частин засобів вимірювальної техніки та генератору захисних завад, послідовно, з інтервалом 5 – 10 секунд, здійснити накопичення та запис на носій інформації десяти масивів даних аналогово-цифрового перетворення, що виконуються реєстратором при включеному генераторі захисних завад.

Сформувати масив AT, що складається з векторів значень відліків амплітуд лінійної передискретизації сигналів $AT^{<0>}$, $AT^{<1>}$.. $AT^{<9>}$ за формулами:

$$mn = floor\,(TNn \cdot Fo) \qquad an,\,k = (AMmn + 1,\,k - AMmn,\,k) \,/\, (TMmn + 1 - TMmn)$$

$$an,k = (AMmn,k \cdot TMmn + 1 - AMmn + 1,k \cdot TMmn) \,/\, (TMmn + 1 - TMmn)$$

$$ATn,k = an,k \cdot TNn + an,k,$$

де k – порядковий номер векторів $AM^{<k>}$ та $AT^{<k>}$, що змінюється від 0 до 9.

Обчисливши масив AF, що складається з векторів комплексних значень односторонніх спектрів сигналів завад $AF^{<0>}$, $AF^{<1>}$.. $AF^{<9>}$ за формулою:

$$AF_{i,k} = \frac{1}{N} \cdot \sum_{n=0}^{N-1} AT_{n,k} \cdot \exp(-j \cdot 2 \cdot \pi \cdot n \cdot i \cdot N^{-1})$$

де: j – символ комплексної одиниці; k – порядковий номер векторів AF<k> та AT<k>, що змінюється від 0 до 9; i – порядковий номер спектральних складових, що змінюється від 0 до N/2.

Визначаються значення вектору лінійної інтерполяції коефіцієнтів передачі вимірювальної антени або датчика сигналу AD_i за формулою:

$$s_i = \text{numvec}(FP, FI_i)$$

$$yi = (KP_{si+1} - KP_{si}) / (FP_{si+1} - FP_{si})$$

$$\eta i = (KP_{si} \cdot FP_{si+1} - KP_{si+1} \cdot FP_{si}) / (FP_{si+1} - FP_{si})$$

$$AD_i = y_i \cdot FI_i + \eta_i$$

де: numvec – оператор відбору номеру найближчого меншого по відношенню до величини Fii значення частоти серед всіх значень вектору частот таблиці коефіцієнтів передачі; FP – вектор частот таблиці коефіцієнтів передачі; KP – вектор коефіцієнтів передачі.

Обчислити значення елементів масиву CORR, що складається з Q векторів взаємної кореляції $CORR^{<0>}$, $CORR^{<1>}$ .. $CORR^{<Q-1>}$, по N елементів кожний, за формулою:

$$CORR_{c,q} = \sum_{n=0}^{N-1} AFM_{n,q} \cdot \exp(j \cdot 2 \cdot \pi \cdot n \cdot c \cdot N^{-1})$$

де: c – порядковий номер елемента окремого вектора $CORR^{<q>}$, що змінюється в межах від 0 до N-1.

Обчислити вектор максимальних значень викидів векторів кореляції MC за формулою:

$$MC\,q = \max(\max(CORR < q >) - \min(CORR < q >))$$

де: max – оператор відбору максимальних величин серед всіх значень вектору; min – оператор відбору мінімальних величин серед всіх значень вектору.

Наведена методика дозволяє визначати коефіцієнт міжспектральних зв'язків в відносних значеннях від 0 до 1, що є відміною від інших де даний коефіцієнт розраховується в разах, або децибелах.

Висновки.

1. Таким чином вирішення проблеми забезпечення безпеки інформації в умовах значного росту її об'ємів, що обробляється інформаційно-телекомунікаційними системами та збільшення ймовірності ризиків, загроз до неї, можливо шляхом розробки сучасних методів та систем захисту інформації.

2. Аналіз можливих методів оцінки можливих загроз для інформації, яка циркулює на об'єкті інформаційної діяльності, свідчить проте, що жоден із цих методів не може забезпечити повну і адекватну оцінку. Найбільш раціональним є поєднання декількох методів з урахуванням їх особливостей, тобто - застосування інтегрованого підходу до розробки математичних моделей оцінки загроз з урахуванням декількох методів. При цьому маємо ефект «складання» потужності цих методів та подолання проблем невизначеності вихідної інформації та адекватності розроблених моделей.

3. Серед найбільш прийнятних методів слід виділити наступні: експертні методи (метод безпосередньої оцінки, метод Акоффа-Черчмена); графові методи та відповідні матриці, які відображають причинно-слідчі відносини між всіма елементами (параметрами) оціночної моделі; методи теорії нечітких множин для усунення невизначеності вихідних даних для рішення задач оцінки, формалізації та врахування суб'єктивізму (власних переваг) ОПР; методи теорії ймовірностей, якщо відомі або визначені закони розподілення випадкових величин, що використовуються в оціночної моделі, а також методи теорії прийняття рішень.

4. Розвиток теорії та практики побудови оптимальних (квазіоптимальних) приймачів сигналів та методів цифрової обробки суміші сигналів та завад потребує розроблення та удосконалення методів (засобів) побудови та використання технічних засобів захисту інформації.

5. Одним із важливих напрямків забезпечення процесу створення систем захисту інформації є проведення досліджень методів оцінки якості маскуючих шумів та розробка

сучасних норм, методик та рекомендацій щодо побудови та використання технічних засобів захисту інформації.

6. При цьому виникають питання скорочення часу на проведення різних досліджень під час розробки, створення, державної експертизи та оцінки захищеності інформації засобів та систем захисту інформації, що використовуються в інформаційно-телекомунікаційних системах держави.

7. Одним із напрямків підвищення швидкості логічних обчислень є вибір форми представлення, реалізація якої засобами вимірювально-обчислювальної техніки було би найбільш оптимальним.

ЛІТЕРАТУРА:

1. Додонов О.Г. Глобалізація інформаційних систем та безпека / О.Г.Додонов, О.С. Горбачик, М.Г. Кузнєцова // Інформаційні технології та безпека. Зб. наук. праць. - К.: ІПРІ НАН України, 2002. – С.49–53.

2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення. Затверджено наказом Держстандарту України від 11.04.97 р. № 200.

3. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн.: Кн.1. - М.: Энергоатомиздат, 1994. – 400 с.

4. Куршев М.А. Оценка и предотвращение рисков (по материалам зарубежной печати) / М.А. Куршев // Мир безопасности. – 2003.– №7/8. – С.27–29.

5. Висоцкая Е. Современное состояние методологии анализа рисков при обеспечении информационной безопасности компьютерной системы / Е. Висоцкая, А.Давиденко // Правове. нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2002. – вип.4. – С.43–49.

6. Анохин А.М. Методи определения важности критериев / А.М. Анохин // Автоматика и телемеханика. – 1997. – № 8. – С.3–35.

7. Логико-лингвистические модели в военных системных исследованиях. – М.: Воениздат. 1988.

8. Довбня С.Я. Особливості та методика створення експертної системи підтримки прийняття рішення щодо управління комплексною безпекою інформації в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності / С.Я. Довбня, С.В. Биков, Ю.І. Хлапонін, І.О. Четверіков // Збірник наукових праць "Сучасний захист інформації". – 2013. – Вип. № 1. – С. 16–25.

9. Adaptive filters. Editet by C. F. N. Cowan and P.M. Grand. – Prentice-Hall. Inc., Englewood Cliffs, 1985. - 392

10. Довбня С.Я. Методичні підходи щодо організації захисту інформації та раціонального вибору технічних засобів інформації / С.Я.Довбня, А.В.Нікірін, І.О. Четверіков // Бізнес і безпека. – 2013. – № 6. – С . 78–80.

11. Хорев А.А. Системы виброакустической маскировки. - М.: Специальная техника, 2003, № 6. – 12 с.

12. Довбня С.Я. Методологічні та організаційно-технічні основи створення систем та методів захисту інформації від витоку технічними каналами / С.Я.Довбня, Д.А.Алексєєв // Збірник наукових праць СТСЗІ Держспецзв'язку. – 2011. – Вип. №1 (19). – С. 58–77.

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

к.воен.н., доц. Довбня С.Я., к.т.н., с.н.с. Кривцун В.И.,
к.т.н., доц. Четвериков И.А., Савран В.О., Солдатенко О.А.

НАУКОВО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ СТВОРЕННЯ ТА ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

У статті розглянуто підхід до аналізу загроз для інформації, визначення методів та засобів захисту інформації в інформаційно-телекомунікаційних системах із застосуванням логіко-лінгвістичного методу. Засоби технічних розвідок представляється інтегрованим оптимальним приймачем. Загрози та ризики до інформації представляються з використанням теорії нечітких множин. Визначення рівня захищеності інформаційно-телекомунікаційних систем здійснюється шляхом оцінки якості маскуючи акустичних та електромагнітних шумів.

Методи визначення ентропійного коефіцієнта якості та коефіцієнту між спектральних зв'язків маскуючого шуму, дозволяють дослідити процеси у ймовірнісній області і оцінити забезпечення інформаційної безпеки. При цьому використовується векторно-матричний підхід до дослідження засобів технічного захисту інформації. Перевагою методу є можливість зручної алгоритмізації процесу дослідження систем інформаційної безпеки.

Ключові слова: аналіз загроз, система інформаційної безпеки, методи теорії нечітких множин.

Ph.D. Dovbnya S.J., Ph.D. Kryvtsun V.I.,
Ph.D. Chetverikov I.A., Savran V.A., Soldatenko O.A.

SCIENTIFIC-METHODOLOGICAL SUPPORT ESTABLISHMENT AND FUNCTIONING OF STATE INFORMATION SECURITY

The article deals with an approach to the analysis of threats to information, determine the methods and means of information protection in information and telecommunication systems with the use of logical and linguistic methods. Of technical studies submitted optimal integrated receiver. Threats and risks to information submitted using the theory of fuzzy sets. Determining the level of security of information and telecommunication systems is carried out by assessing the quality masking acoustic and electromagnetic noise. Methods for determining the entropic factor quality factor and spectral relationships between the masking noise, can explore the probabilistic processes in the region and to assess information security. It uses vector-matrix approach to the study of technical protection of information. The advantage of the method is the possibility of convenient algorithmic process research of information security.

Keywords: analysis of the threats of information security, methods of fuzzy sets.