МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Військовий інститут телекомунікацій та інформатизації
Національного технічного університету України
„Київський політехнічний інститут”

VI-та НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ

„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”

25-26 жовтня 2012 року

(Доповіді та тези доповідей)

Київ – 2012

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів шостої науково-технічної конференції опубліковано доповіді та тези доповідей вчених, науково-педагогічних працівників, ад'юнктів, здобувачів, курсантів і студентів Військового інституту телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут" та інших вищих навчальних закладів, в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення.

ЗМІСТ

(Доповіді)

(Тези доповідей)

Contents

(Reports)

(Tethys)

к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)
к.т.н. Волков О.В. (ВІТІ НТУУ „КПІ”)
Голик О.Л. (ДУІКТ)

АНАЛІЗ ЕНЕРГЕТИЧНОГО ПОТЕНЦІАЛУ АТМОСФЕРНИХ ОПТИЧНИХ СИСТЕМ ПЕРЕДАЧІ

Атмосферні (відкриті) оптичні системи передачі (АОСП) забезпечують передачу даних модульованим випромінюванням в інфрачервоній частині спектра через атмосферу. На сьогоднішньому етапі, застосування зазначених систем отримує все більше поширення в сегменті високошвидкісного безпроводового транспортування даних. Перспективність їх використання ґрунтується на певних особливостях даної технології. Це насамперед використання випромінюючих засобів, що працюють на частотах значно більших від встановленої для радіочастотного діапазону межі (400 ГГц). Отже такі системи не використовують радіодіапазон і не створюють перешкод в радіочастотному спектрі. Крім того, АОСП потребує невеликого часу для розгортання та має мінімальне енергоспоживання (десятки Вт). В результаті вище зазначеного, застосування АОСП може забезпечувати реалізацію ряду технічних переваг, зокрема: відсутність чутливості до радіоперешкод, висока скритність та розвідзахищеність, висока швидкість передачі, прозорий механізм передачі (можливість транспортування потоків створених за різними протоколами *SDH, ATM, Ethernet* і т.д.).

Слід зазначити, що на якість зв’язку в АОСП впливає цілий ряд чинників, які при певних обставинах можуть суттєво знизити позитивний ефект від їх застосування. Найбільше це стосується особливих погодних умов, таких, як дощ, сніг, туман і т. д., що можуть значно погіршити видимість і, таким, чином понизити ефективність використання діапазону інфрачервоного зв’язку [1]. Крім того, в атмосфері спостерігаються турбулентні явища, які приводять до флуктуації показника заломлення середовища, коливанням світла і спотворенням сигналу, що приймається. Деякі з зазначених чинників можуть призводити до збільшення значення показника затухання на десятки дБ. Проте найбільше зростання втрат виникають в умовах щільного туману, коли вони можуть складати до 100 дБ/км і навіть більше. Це безумовно призводить до зменшення рівня сигналу на прийомі, і, як наслідок, до збільшення коефіцієнту помилки. Реальні зразки апаратури, які на сучасному етапі пропонуються для практичного використання, гарантують дальність зв’язку до 4 км (при швидкості передачі 100 Мбіт/с і надійності зв’язку 99,9 %) [2]. Це цілком конкурентоздатні показники, але все ж такі досить скромні, якщо порівнювати їх з сучасними радіорелейними інтервалами або системами безпроводового широкосмугового доступу WiMax. Таким чином, існує завдання по проведенню аналізу параметрів, які визначають значення можливого енергетичного потенціалу АОСП, та відповідної дальності зв’язку, що буде забезпечуватися.

Для збільшення енергетичного потенціалу АОСП і, відповідно, підвищення надійності їх роботи можливе використання наступних шляхів:

– збільшення потужності оптичних випромінювачів (передавачів);

– збільшення чутливості оптичних детекторів (приймачів);

– звуження діаграми спрямованості передавальних антен;

– використання адаптації за довжиною хвилі;

– використання методів рознесеного прийому і ін.

Проаналізуємо кожний з зазначених шляхів. В якості оптичних випромінювачів у АОСП використовують світловипромінюючі або напівпровідникові лазери. Світловипромінюючий діод (СВД) є напівпровідниковим приладом з p-n переходом, протікання електричного струму через який викликає інтенсивне спонтанне випромінювання. Найбільше застосування отримали торцеві або суперлюмінесцентні СВД. У конструкції такого світлодіода передбачено виведення оптичної потужності випромінювання

через один з торців (рис. 1). При цьому інший торець виконаний у вигляді дзеркала, яке відображає фотони в активний шар. У приладі застосовуються додаткові шари напівпровідникового матеріалу GaAlAs, які відрізняються від активного шару показником заломлення і шириною забороненої зони. Робота світлодіодів заснована на випадковій рекомбінаційній люмінесценції надмірних носіїв заряду, які інжектують в активну область світлодіода. В результаті інжекції неосновних носіїв заряду і дрейфу основних в активному шарі відбувається накопичення і рекомбінація цих зарядів з виділенням квантів енергії (фотони світла), які приблизно відповідають ширині забороненої зони активного шару. При цьому фотони, що випадково утворилися, можуть рухатися в будь-якому випадковому напрямі, відбиватися від меж різних шарів напівпровідників, поглинатися кристалами і випромінюватися з торця. Величина випромінюваної потужності СВД приблизно лінійно залежить від величини струму інжекції. СВД називають слабокогерентними джерелами світла.

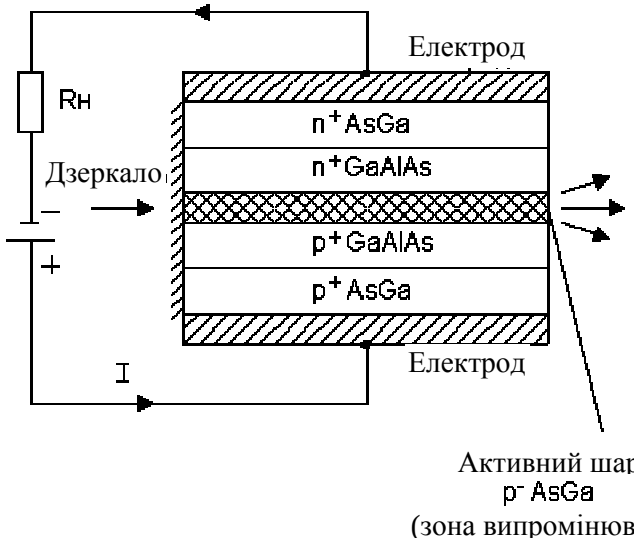


Рис. 1. Конструкція торцевого світловипромінюючого діода

Сучасні світловипромінюючі діоди здатні забезпечувати випромінювання з потужністю декілька одиниць мВт, з кутом розходження порядку до 30˚ (у вертикальній площин) і до 60˚ (у горизонтальній) та шириною спектра випромінювання 50 нм.

Лазер – прилад, що генерує оптичне когерентне випромінювання на основі ефекту вимушеного, стимульованого випромінювання. Принцип роботи лазера заснований на створенні активного середовища, в якому під впливом зовнішнього поля створюються електрони, що перебувають у збудженому стані. Так же саме, як і в СВД під впливом модулюючого струму, створюється спонтанне випромінюється. Утворений фотон потрапляє у резонансну систему, яке представляє собою двох-дзеркальну систему, що охоплює активне середовище з двох боків (рис. 2). Відстань між дзеркалами та їх прозорість обирають таким чином, щоб забезпечити когерентне випромінювання лазера.

Електромагнітна хвиля, яка випромінюється лазером вважається когерентною, оскільки її амплітуда, частота, фаза, напрям поширення і поляризація постійні або змінюються впорядковано. Сучасні напівпровідникові лазери здатні забезпечити випромінювання з потужністю декілька сотень Вт, з кутом розходження порядку до 5˚ (у вертикальній площин) і до 15˚ (у горизонтальній) та шириною спектра випромінювання до 3 нм.

Очевидні висновки, що з точки зору застосування більш дешевої оптики доцільне використання СВД. Однак для роботи на великі відстані, де важливо забезпечити високу потужність випромінювання та зменшити втрати пов’язані із великим кутом розходження,

що призводить до невлучення частини випромінювання у приймальну антену, перевагу має застосування лазерів. Отже потенційно можливе використання, оптичного

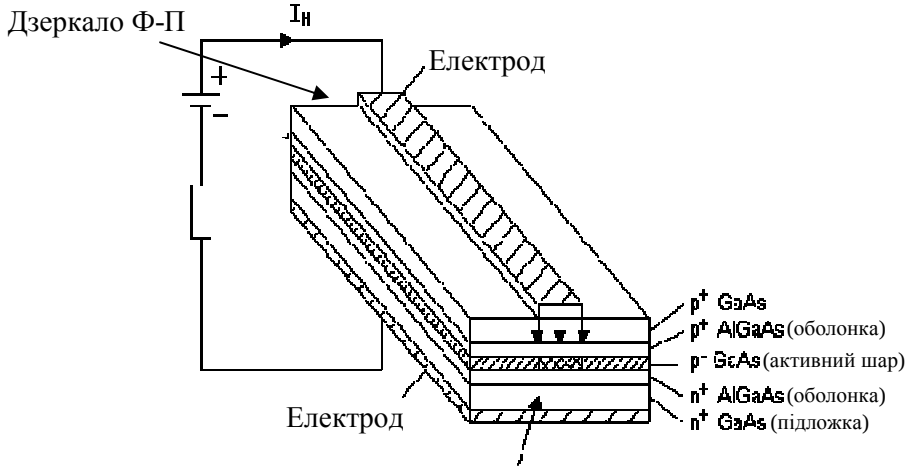


Рис. 2. Конструкція смужкового лазера Фарбі-Перо (Ф-П)

випромінювача (лазера) з потужністю до 100 Вт (зразки, що випускають серійно). Проте треба зазначити, що існують також обмеження щодо використання високопотужних оптичних джерел випромінювання, які пов'язані із встановленими вимогами до безпеки персоналу. Максимальне допустиме лазерне випромінювання залежить від типу використовуваного лазерного діода (довжини хвилі). Міжнародний стандарт IEC.825 визначає максимальний рівень лазерного випромінювання для кожного лазерного класу відповідно до довжини хвилі (у класи входять лазерні діоди і оптичні підсилювачі).

Таблиця 1

Класи лазерних пристроїв за міжнародним стандартом IEC 825

Клас лазера	Довжина хвилі випромінювання, нм	Максимальна потужність лазерного випромінювання, мВт
1	810	25
	830	35
	910	25
	1300	8.85
	1550	10
2	910	100
3A	1300	31
	1550	50
3A*	1300	81
3B	1300	500
	1550	500

В якості приймачів АОСП використовують, як правило, фотодіоди *p*-*i*-*n* або лавинні фотодіоди (ЛФД). Фотодіоди *p*-*i*-*n* відрізняються простотою конструкції, високою надійністю, низкою вартістю. На рис. 3 наведений приклад конструкції *p*-*i*-*n* фотодіода. В ньому між областями з провідністю p^+ (база) и n^+ (колектор) розміщений шар *i* (шар поглинання фотонів). При подаче зворотної напруги зміщення $E_{ЗМ}$ в базі та колекторі створюється підвищена концентрація носіїв заряду. При надходженні до *i*-шару випромінювання певної довжини хвилі утворюються пари „електрон-дірка". На них впливає поле, яке створене напругою $E_{ЗМ}$ та зосереджене в *i*-шарі, воно примушує заряди дрейфувати. Створюється фотострум дрейфу, величина якого прямо пропорційна величині потужності прийнятого оптичного випромінювання

$$I_{\text{ф}} = \frac{P \cdot \text{л} \cdot e}{h \cdot c} \text{з}\ , \tag{1}$$

де P – потужність оптичного випромінювання, λ – довжина хвилі оптичного випромінювання, e – заряд електрона, h – постійна Планка, c – швидкість світла та η – квантова ефективність фотодіода.

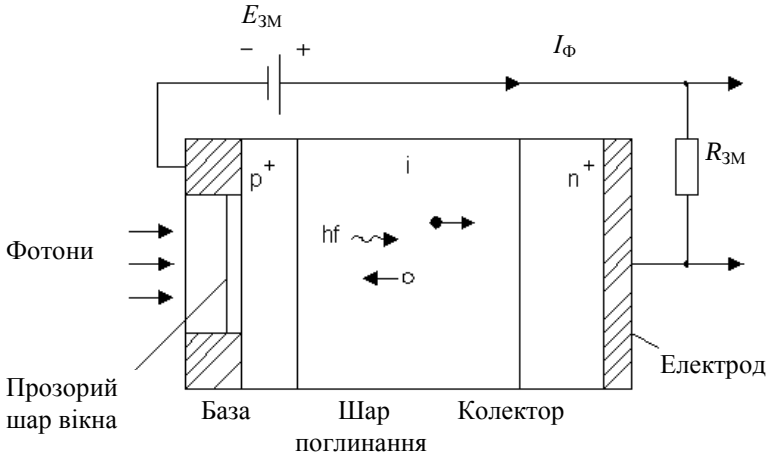


Рис. 3. Конструкція *p-i-n* фотодіода

Чутливість фотодіода оцінюється відношенням утвореного фотоструму до потужності оптичного випромінювання, що його обумовило

$$S = \frac{I_{\text{ф}}}{P} = \frac{\text{л} \cdot e}{h \cdot c} \text{з}\ . \tag{2}$$

Реальні приймальні оптичні модулі обладнані *p-i-n* фотодіодами мають чутливість порядку –20 дБм [4] (для швидкості передачі сигналу 10 Гбіт/с).

У лавинному фотодіоді досягається посилення первинного фотоструму за рахунок керованого лавинного множення числа носіїв заряду. Цьому сприяє конструкція ЛФД. Лавинне множення виникає у шарі множення (рис. 4).

Лавинне множення досягається за рахунок збільшення напруги $E_{\text{ЗМ}}$ до величини, близької до пробійної.

При цьому на *p-n* переході встановлюється дуже сильне електричне поле причому у вузькій області. Висока швидкодія приладу буде досягнута, якщо основна частина фотонів поглинається в шарі, де існує сильне електричне поле. Фотони пролітають шар множення і не встигають взаємодіяти з кристалами.

Носії зарядів утворюються в шарі поглинання і дрейфують до відповідних потенціалів. Рухаючись в сильному полі, носії набувають великої кінетичної енергії і, віддаючи частину її іншим носіям, звільняють нові носії (електрони і дірки).

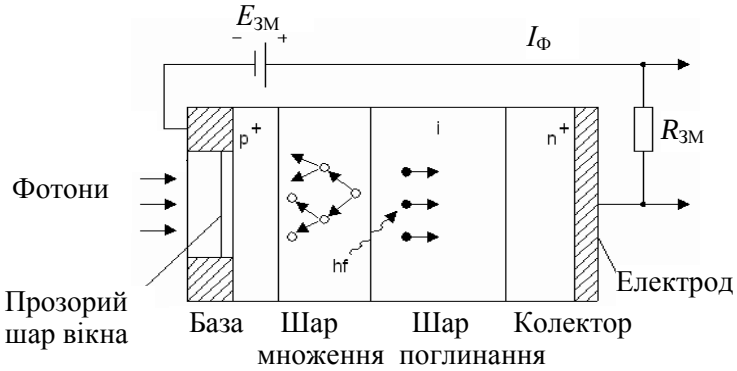


Рис.4. Конструкція ЛФД

Процес збільшення числа носіїв зарядів розвивається лавиноподібно і характеризується відповідним коефіцієнтом, який залежить від матеріалу виготовлення і може складати від 2 (для германієвих ЛФД) до 100 (для кремнієвих ЛФД). Відповідно до (2) цей процес призводить до аналогічного збільшення чутливості. Таким чином практична чутливість ЛФД може складати до –40 дБм [4] (для швидкості передачі сигналу 10 Гбіт/с). Крім того, приймачі обладнані ЛФД мають значну швидкодію, що дозволяє їхнє використання на швидкостях передачі даних вище 10 Гбіт/с.

Недоліками ЛФД прийнято вважати високу напругу зсуву (до 400 В) і складність схеми управління регульованим джерелом $E_{ЗМ}$.

Третій з факторів, що впливають на енергетичний потенціал АОСП є діаграма спрямованості або апертура передавача. Дійсно, якщо розглянути спрощену схему розповсюдження оптичного променя (рис. 5), то стає очевидним, що лише частина випромінюваної потужності буде потрапляти в лінзу приймальної частини.

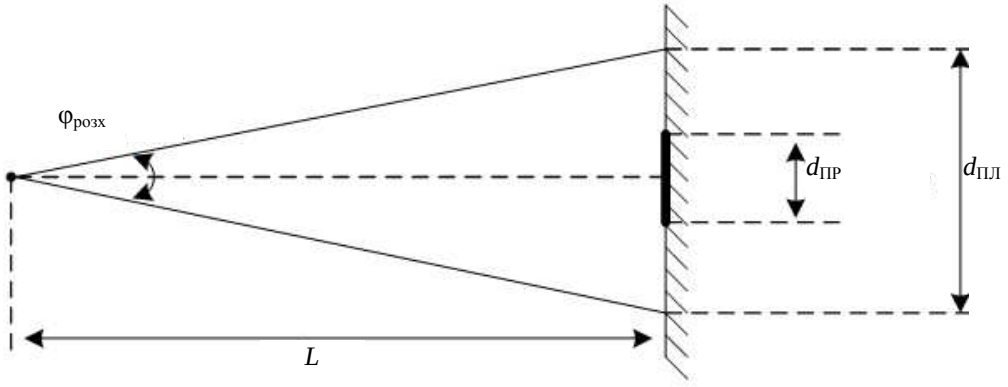


Рис. 5

Відповідно до рис. 5 втрати за рахунок розходження променя можна оцінити за формулою

$$W_{\text{розх}} = 20\log\left(\frac{L\varphi_{\text{розх}}}{d_{\text{ПР}}}\right). \tag{3}$$

При чому потужність, що зосереджена у пучку, що влучає в отвір $d_{\text{ПР}}$ може бути розрахована за виразом [5]

$$P = 1 - \exp\left[-2\left(\frac{d_{\text{ПР}}/2}{\text{в}L}\right)^2\right], \tag{4}$$

де $\text{в} = \dfrac{2\lambda}{\text{р}\omega_0}$, λ – довжина хвилі, ω_0 – радіус променя в найвужчому місці.

Типове значення розходження оптичного променя без застосування систем наведення відносно велике – 2…10 мрад, що еквівалентно діаметру пучка ($d_{\text{ПЛ}}$) 2…10 м на відстані 1 км). За наявності системи наведення розбіжність променя може бути істотно знижена (зазвичай до 0,05…1 мрад, що еквівалентно розміру пучка 5…100 см на відстані 1 км) для збільшення доступності зв'язку, в тому числі і за погодними умовами. Слід мати на увазі, що вартість системи наведення досить велика. Крім того, в процесі експлуатації виникають ситуації неузгодженості (порушення юстировки) оптичних осей передавача та приймача. Такі неузгодженості пов'язані, наприклад з температурними коливаннями опор, на яких закріплюється обладнання. Отже можуть виникати випадки, коли потрібно адаптивно змінювати діаграму спрямованості передавача для забезпечення потрапляння променя у

лінзу приймальної частини. Зрозуміло, що така адаптація буде призводити до зменшення потужності P, що визначається виразом (4).

Механізм реалізації алгоритму зазначеної адаптації може бути досить складним, оскільки єдиним адекватним її критерієм є значення потужності (4). Але на цю величину впливає надто багато факторів, які мають різну природу походження, що фактично унеможливлює здійснення адаптації лише за рівнем потужності прийнятого сигналу. Введення ж інших параметрів адаптації суттєво ускладнює систему.

Проте можливий інший варіант збільшення енергетичного потенціалу АОСП – шляхом використання декількох передавачів і декількох приймачів. Таке рішення дозволяє реалізувати схему рознесеної передачі, що є фактично безальтернативним заходом для боротьби із впливом турбулентності атмосфери та іншими явищами, що носять випадковий характер впливу. Одночасно збільшується сумарна площина приймальної поверхні, без збільшення апертури приймача, що дозволяє компенсувати порушення юстировки і при цьому уникнути збільшення ймовірності потрапляння до приймальної лінзи стороннього випромінювання (наприклад, сонячного світла). При певної реалізації, заходів адаптації діаграми спрямованості та рознесеної передачі можливо повністю мінімізувати втрати за рахунок неузгодженості.

Таким чином, враховуючі все вище зазначене можна порівняти характеристики типового існуючого обладнання АОСП та перспективного. Результати порівняння, які були зроблені для випадку найгірших умов передачі (щільний туман), коли втрати будуть складати порядку 100 дБ/км, наведені у табл. 2.

Таблиця 2

Порівнювальний аналіз енергетичного потенціалу АОСП

№ з/п	Назва параметру	Значення параметру для	
		існуючих АОСП	перспективних АОСП
1.	Потужність випромінювання	50 мВт (17 дБм)	100 Вт (50 дБм)
2.	Чутливість приймача	10 нВт (–50 дБ)	10 пВт (–80 дБ)
3.	Втрати юстировки	3 дБ	0 дБ
4.	Енергетичний потенціал	64 дБ	130 дБ
5.	Дальність зв’язку в ясну погоду/в туман	21 км / 0,64 км	43 км /1,3 км

ЛІТЕРАТУРА

1. Яременко, Ю.И. Применение открытых оптических систем передачи в сетях связи [Текст] / Яременко Ю.И. – Радиоэлектроника и телекоммуникации № 1 (37), 2005. – С. 35 – 42.

2. Каталог. Атмосферные оптические системы передачи [Електронний ресурс]. – Режим доступу: http://www.micromax.ru/catalog/comparePAV.shtml.

3. Конспект лекцій. Волоконно-оптические системы передачи (ВОСП) [Електронний ресурс]. – Режим доступу: /http:// ndo.sibsutis.ru /magistr /courses_work /vosp_work/ lectures_ index.htm.

4. Корнійчук, В.І. Аналіз чутливості приймальних пристроїв ВОСП-СРК [Текст] / Корнійчук В.І., Барба І.Б., Дойжа Г.І. – Збірник наукових праць ОНАЗ ім. О.С. Попова. – № 2 / 2010.

5. Scott, Bloom. Принципы работы FSO – систем (перевод ООО „МОСТКОМ”) [Текст] / Scott Bloom, Eric Korevaar, John Schuster, Heinz Willebrand // JOURNAL OF OPTICAL NETWORKING. – June 2003, Vol. 2, No. 6.

д.т.н. Міночкін А. І. (ВІТІ НТУУ „КПІ”)
д.т.н. Кувшинов О. В. (ВІТІ НТУУ „КПІ”)

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ СИЛ І ЗАСОБІВ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ

Характер збройної боротьби у війнах і збройних конфліктах XXI ст. зумовлює виникнення і розвиток фундаментальних змін в основних положеннях воєнної стратегії й оперативного мистецтва. Зокрема, війна доповнюється новою складовою – інформаційною. Досягнення інформаційної переваги представляється як об’єктивна необхідність успішного ходу бою (операції) [1, 2].

Військові фахівці розвинутих країн світу наполегливо працюють над розробкою та впровадженням нових концепцій ведення операцій. Застосування сучасних інформаційних технологій (ІТ) дозволяє суттєво поширити можливості з розробки таких концепцій [3, 4].

Серед концепцій, що засновані на застосуванні „жорсткої сили”, найбільш показовими є так звана „мережецентрична концепція ведення бойових дій”, що розроблена американськими фахівцями, та „концепція інтегрованого бойового простору”, що запропонована військовими фахівцями Великої Британії [5 – 7].

Згідно [8], мережецентрична війна – це орієнтована на досягнення інформаційної переваги концепція проведення воєнних операцій, що передбачає збільшення бойової міцності угруповання об’єднаних сил за рахунок створення єдиної інформаційно-комунікаційної мережі, що пов’язує джерела даних, осіб, які приймають рішення, і виконавців, що забезпечує доведення до учасників операцій інформації про обстановку, прискорення процесу управління силами і засобами, а також підвищення темпу операцій, ефективність поразки сил супротивника, живучість своїх військ і рівень самосинхронізації бойових дій.

Основна перевага мережоцентричної концепції ведення бойових дій проявляється у високій маневреності частин і з’єднань, здатних у ході операції оперативно планувати свої наступні дії, постійно отримуючи свіжі дані розвідки, та вступати в бій, не піклуючись про тилове постачання, яке прийде в потрібний час і точно за призначенням.

Ця концепція управління збройними силами дає змогу прискорити процеси прийняття оперативних (бойових) рішень і планування операції (бою), підвищити маневреність збройних сил, їх ситуаційну боєздатність і в підсумку – бойові можливості.

Стосовно мережоцентричної концепції передбачаються чотири основні фази ведення бойових дій [5]:

1) досягнення інформаційної переваги внаслідок випереджального знищення (виведення з ладу, подавлення) системи розвідувально-інформаційного забезпечення супротивника (сенсорів, мережоутворюючих вузлів, центрів обробки інформації та управління);

2) завоювання переваги в повітрі шляхом подавлення (знищення) системи ППО супротивника;

3) послідовне знищення залишених без управління й інформації засобів ураження супротивника, насамперед ракетних комплексів, авіації, артилерії, бронетехніки;

4) остаточне подавлення або знищення осередків опору супротивника.

Виходячи з цього в розвинутих країнах світу здійснюється цілеспрямоване реформування збройних сил, спрямоване в тому числі на здійснення структурних і функціональних змін у системі їх управління. Основним змістом цього процесу є трансформація сукупності різнорідних сил і засобів, в об’єднані збройні сили інформаційного століття – більш гнучкі та мобільні, здатні, використовуючи сучасні системи зв’язку і автоматизовані інформаційно-управлінські системи, удосконалені засоби розвідки та високоточну зброю, у стислий термін і при мінімальних втратах забезпечити ефективне

досягнення військово-політичних або інших цілей держави (коаліції держав) у ході протиборства з будь-яким супротивником [9, 10].

Інформаційні технології природно призвели до виникнення нової оперативно-стратегічної категорії, що одержала назва „інформаційна перевага", а вона, у свою чергу, чітко позначила необхідність зсуву акценту на розробку нових оперативно-концептуальних установок, процесів і процедур для системи управління військами й зброєю.

Як свідчить досвід бойових дій і локальних конфліктів останніх років провідне місце в управлінні військами (силами) посідає радіоелектронна боротьба (РЕБ), яка трансформується в один з основних елементів сучасних війн і найбільш значну силу інформаційних операцій. РЕБ, как основа протиборства с системами бойового управління супротивника, стає невід'ємною частиною військового протистояння будь-якого масштабу [11, 12].

Об'єктами першочергового впливу системи РЕБ в ході воєнних операцій є елементи систем управління військами (силами) і зброєю, засоби розвідки та системи зберігання, обробки і розподілу інформації, радіоелектронні засоби (РЭЗ), автоматизовані системи, бази даних і мережі ЕОМ, особовий склад, що бере участь у підготовці й прийнятті рішень.

Радіоелектронна боротьба стала ключовим елементом інформаційної війни внаслідок двох основних факторів.

По-перше, підвищення маневреності збройних сил (ЗС), збільшення масштабу глибини проведення операцій, автоматизація всіх процесів управління (військами, бойовою технікою і зброєю), створення функціональних інтегрованих систем управління, розвідувального забезпечення. Широке застосування РЕБ та високоточної зброї призвело до кількісного перерозподілу в операції ударних сил і сил забезпечення. Так, за поглядами командування ЗС США та об'єднаних ЗС НАТО, в операціях початку XXI століття більше ніж 60-70 % задіяних сил будуть вирішувати завдання забезпечення розвідки, РЕБ, зв'язку та автоматизації [7, 9].

По-друге, за час еволюційного розвитку радіоелектронної боротьби різко змінився її зміст, складові елементи, характер, використовувані засоби, об'єкти розвідки, впливу і захисту. Крім того, сили і засоби РЕБ стали більш універсальними стосовно засобів системи бойового управління супротивника. Вони можуть діяти на всю глибину не тільки театру військових дій, але й театру війни в цілому, дозволяють здійснювати розвідувально-інформаційне забезпечення операції, використати нелетальні і летальні (вражаючі) засоби, впливати в будь-який час доби на об'єкти, бойову техніку і зброю, а також забезпечувати всебічний захист своїх ЗС. Засоби РЕБ можуть застосовуватися приховано і відкрито, входити до складу різних багатоцільових функціональних і автоматизованих інтегрованих систем: багатосферного базування, бойового управління, зв'язку, комп'ютерного забезпечення розвідки, вогневого ураження, боротьби з системами бойового управління супротивника та захисту своїх систем, використовувати у своїх інтересах мережі ЕОМ протиборчої сторони та впливати на них.

Основними завданнями, які вирішує система РЕБ, є:

зрив і дезорганізація управління військами і зброєю супротивника;

зниження ефективності розвідки і застосування зброї та бойової техніки;

забезпечення стійкої роботи систем і засобів управління своїми військами і зброєю.

У такий спосіб РЕБ – це сукупність взаємозалежних за метою, завданнями, місцем і часом заходів і дій військ по виявленню систем і засобів управління військами і зброєю супротивника, їх ядерному та вогневому ураження, виявленню та радіоелектронному подавленню, а також по радіоелектронному захисту своїх систем і засобів управління військами і зброєю та протидії технічним засобам розвідки супротивника.

Основними тенденціями розвитку сучасних систем РЕБ є [11]:

часткова втрата самостійної ролі РЕБ, що стає одним з основних елементів систем бойового управління при проведенні інформаційних операцій.

корінна поетапна зміна характеру, змісту і ролі РЕБ і операції (бою). Так, на сучасному етапі розвитку збройних сил РЭБ стала компонентом синергетической системи інформаційної війни – однією зі складових військового потенціалу;,

використання для ведення РЕБ нових видів спрямованої зброї, а також створення летальної і нелетальної зброї, яка діє на нових фізичних принципах;

перехід від подавлюючого впливу і захисту радіоелектронних засобів (РЕЗ) до комплексного вражаючого і подавляючому впливу і захисту не тільки РЕЗ, але й бойової техніки, об'єктів збройних сил, систем зброї і особового складу збройних сил і органів державного управління;

повна інформатизація і автоматизація процесу РЕБ. Зсув акценту протиборства в інформаційно-інтелектуальну область, сферу підготовки і прийняття рішень, планування і керівництва операцією (боєм). Становлення РЕБ як основи інформаційних операцій.

Цілями радіоелектронної боротьби в операціях збройних сил нового типу поряд з дезорганізацією систем бойового управління супротивника стануть позбавлення його можливості використовувати інформацію про свої війська та дії конфронтуючої сторони, забезпечення попередження супротивника в прийнятті оперативних (бойових) рішень і підвищення ефективності ведення бойових дій збройних сил, зниження людських і матеріальних втрат та успішне завершення операції в найкоротший термін.

Структура РЕБ за сучасними поглядами зображена на рис. 1.

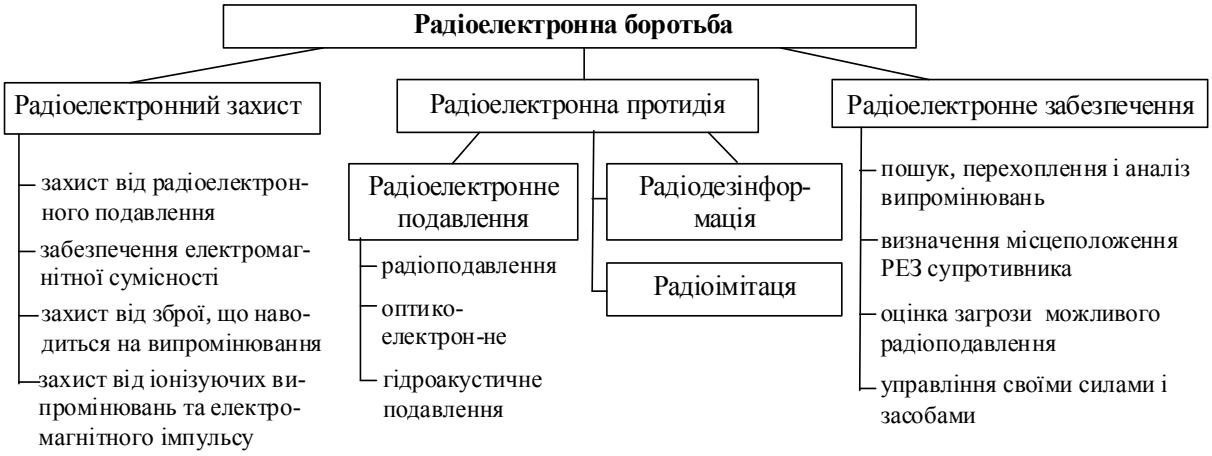


Рис. 1. Структура радіоелектронної боротьби

Найбільш важливим елементом РЕБ є радіоелектронна атака з використанням засобів наземного і повітряного базування (пілотованих і безпілотних), переносних і, що закидають на територію супротивника (авіацією, артилерією, разведгрупами).

Засоби радіоелектронної атаки можна поділити на два типи: неруйнуючого й руйнуючого впливу. До неруйнуючих (нелетальних) засобам впливу відносяться засоби радіоелектронних завад і радіоелектронної дезінформації. Засобами РЕБ неруйнуючого впливу є засоби спрямованої енергії, високоточної зброї та боєприпаси з голівками радіоелектронного самонаведення. Необхідно відмітити, що засоби спрямованої енергії на великих площах можуть діяти як засоби завад, не завдаючи летального впливу.

З визначення, даного фахівцями США радіоелектронним силам, і аналізу засобів, які можуть бути використані для проведення радіоелектронної атаки, можна визначити наступні їх завдання: зрив, подавлення або виведення з ладу радіоелектронних і оптикоелектронних систем, а також засобів розвідки, спостереження, наведення, зв'язку, навігації, управління військами і зброєю; зміна режиму випромінюванні РЕЗ; імітація роботи РЕЗ, об'єктів і зброї своїх військ і військ супротивника; імітація демонстративних дій військ; перевантаження систем зв'язку і управління супротивника; введення супротивника в оману щодо намірів своїх військ; вплив на особовий склад що обслуговують РЕЗ, системи розвідки,

спостереження, засоби зв'язку, навігації та управління військами і зброєю, а також на особовий склад, що бере участь в аналізі добутої розвідкою інформації, підготовці й прийнятті рішень, плануванні операції й бою.

Завданнями руйнуючих засобів радіоелектронного подавлення при проведенні операцій збройних сил можуть бути: наведення на ціль високоточної зброї і зброї спрямованої енергії; ураження, подавлення, знищення, руйнування і виведення з ладу засобів розвідки, навігації та спостереження; ураження, подавлення, знищення, руйнування і виведення з ладу засобів, вузлів, центрів і органів зв'язку управління військами і зброєю, а також об'єктів, бойової техніки і систем озброєння; ураження і виведення з ладу особового складу, що приймає участь у підготовці, прийнятті оперативних (бойових) рішень і плануванні операції (бою).

Приклад бойового застосування систем радіоелектронного подавлення мереж радіозвязку подано на рис. 2.

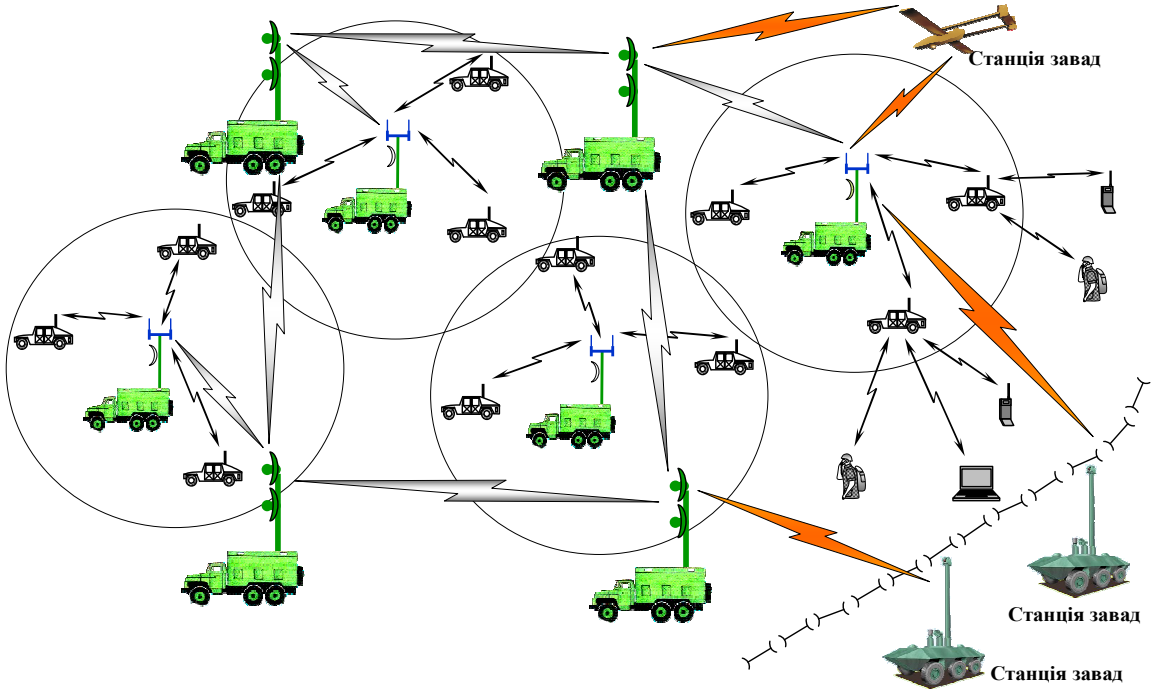


Рис. 2. Бойове застосування засобів радіоелектронного подавлення

Сили і засоби радіоелектронного захисту можна умовно поділити на три типи: безпосереднього захисту РЕЗ; забезпечення електромагнітної сумісності РЕЗ на пунктах управління та у бойових порядках військ; радіоелектронного захисту при проведенні інформаційних операцій. Завданнями сил і засобів радіоелектронного захисту радіоелектронних засобів в операції можуть бути: захист РЕЗ своїх військ від навмисних радіоелектронних і оптикоелектронних завад супротивника; захист РЕЗ своїх військ від випадкових атмосферних, промислових завад, ненавмисних завад від РЕЗ цивільних відомств і союзних військ; захист РЕЗ, бойової техніки, систем зброї і особового складу своїх військ від радіоелектронної дезінформації супротивника, захист бойової техніки, об'єктів, пунктів управління, РЕЗ, систем озброєння, боєприпасів від самонавідної на радіоелектронне випромінювання зброї супротивника; захист об'єктів, пунктів управління, РЕЗ і військ від летальних і нелетальних засобів спрямованої енергії. Крім того, до завдань сил і засобів радіоелектронного захисту при проведенні інформаційних операцій варто віднести: інформаційний захист засобів розвідки, засобів радіоелектронної атаки і радіоелектронного захисту підрозділів і засобів РЕБ; інформаційний захист сил і засобів психологічних операцій; інформаційний захист сил і засобів власної інформації.

Аналіз цілей і завдань сил і засобів РЕБ збройних сил США, що застосовувалися в ході бойових дій в Афганістані та Іраку, дає можливість сформулювати основні тенденції в організації і веденні РЕБ: застосування сил і засобів РЕБ з іншими силами систем бойового управління в інформаційних операціях; зміщення акценту радіоелектронної атаки в інформаційну інтелектуальну область, сферу управлінської діяльності командування збройними силами супротивника; перехід від рішення окремих функціональних завдань військ до всебічного багатофункціонального ведення РЕБ в інтересах об'єднаних сил; розширення частотного діапазону і комплексу завдань РЕБ на основі прийняття на озброєння нового покоління технічних засобів радіоелектронної атаки, радіоелектронного захисту, радіоелектронного забезпечення бойових дій; значне збільшення кількості цілей, які одночасно спостережуються, контролюються, подавлюються і уражуються, одним комплексом радіоелектронної боротьби; розширення переліку об'єктів розвідки, впливу і захисту, сил і засобів РЕБ у зв'язку з прийняттям на озброєння засобів РЕБ спрямованої енергії; створення багатофункціональних і багатосферних систем РЕБ блочно-модульного типу з відкритою архітектурою побудови.

Таким чином, у наш час радіоелектронна боротьба потребує важливих змін у технічному оснащенні та способах застосування сил і засобів РЕБ, перебудови її ідеології, а також ретельного науково обґрунтованого перегляду застарілих підходів до розроблення та застосування способів її ведення.

ЛІТЕРАТУРА

1. Расторгуев С. П. Информационная война: Проблемы и модели. – М. : Радио и связь, 1999. – 416 с.

2. Costa K. J. Pentagons Kicks Off Effort to Reexamine the Basic Principles of War // Inside the Pentagon. – 2004, July. – P. 25 – 30.

3. Балабін В. В. Інформаційні технології як фактор забезпечення національних інтересів у воєнній сфері / В. В. Балабін, С. В. Лєнков, А. О. Рось // Збірник наукових праць ВІКНУ. – 2006. – Вип. 1. – С. 9 – 14.

4. Пермяков О. Ю. Застосування сучасних інформаційних технологій в збройній боротьбі / О. Ю. Пермяков // Modern information technologies in the Sphere of security and Defence. – 2008. – №2. – С. 69 – 74.

5. Романченко І. С. Мережоцентрична система ведення війни – міф XXI сторіччя чи виклик Збройним Силам України / І. С. Романченко, А. І. Сбітнєв // Наука і оборона. – 2006. – №3. – С. 12 – 17.

6. Романченко І. С. Формування єдиного інформаційного простору поля бою – фундаментальний принцип воєнного мистецтва / І. С. Романченко, А. І. Сбітнєв // Наука і оборона. – 2008. – №2. – С. 19 – 25.

7. Попов М. Основные направления строительства вооруженных сил за рубежом / М. Попов // Зарубежное военное обозрение. – 2004. – № 1. – С. 2 – 10.

8. Net-Centric Environment Joint Functional Concept // DOD, 2005. – Appendix B. Glossary.

9. Азов В. Концепция создания единой информационно-управляющей структуры ВС США / В. Азов // Зарубежное военное обозрение. – 2003. – № 1. – С. 3 – 10.

10. Pigeau, Ross and Carol McCann. „Re-Conceptualizing Command And Control". Canadian Military Journal, 3.1: 53 – 64, 2002.

11. Черниш О. М. Основи формування нової ідеології ведення радіоелектронної боротьби у війнах і збройних конфліктах майбутнього / О. М. Черниш, С. О. Тищук, С. М. Шолохов // Наука і оборона. – 2006. – № 4. – С. 48 – 51.

12. Певцов Г.В. Наукові основи обґрунтування способів бойового застосування сил та засобів радіоелектронного подавлення в операціях / Г.В. Певцов, С.М. Шолохов, Г.М. Тіхонов, І.М. Тіхонов // Системи управління, навігації та зв'язку. – К.: ЦНДІ НіУ, 2008. – № 3 (7). – С. 120 – 125.

д.т.н. Певцов Г. В.(ХУПС)
к.т.н. Яцуценко А. Я. (ХУПС)
к.т.н. Карлов Д. В. (ХУПС)
Трофименко Ю. В.(ХУПС)
Борцова М. В.(ХАІ)

ОСНОВИ ЕНЕРГЕТИЧНОГО ВИЯВЛЕННЯ І ОЦІНЮВАННЯ ПАРАМЕТРІВ РАДІОСИГНАЛІВ

При енергетичному виявленні радіосигналів, як і в класичній теорії виявлення, для прийняття рішення про виявлення радіосигналу використовується критерій мінімуму середнього ризику. На відміну від класичного підходу, енергетичне відношення правдоподібності $L\left(y^2\right)=\frac{p_{sn}(y^2)}{p_n(y^2)}$ - це відношення щільності ймовірності розподілу сумарної енергії сигналу і шуму $p_{sn}(y^2)$ до щільності ймовірності розподілу енергії внутрішнього шуму приймача $p_n(y^2)$. Енергетичне відношення правдоподібності враховує закон збереження енергії. Очевидним є припущення, що енергетичне відношення правдоподібності $L\left(y^2\right)$ функціонально пов'язано з оцінками енергії поточної реалізації **y**:

$L\left(y^2\right) \Box K\left(y^2\right)=\frac{W_{sn}}{\overline{W_n}}$ $\forall i\in 1...m$, де $W_{sn}=\sum_{k=0}^{n}\left\{y_k\right\}^2\Delta t_k$ -оцінка енергії суми радіосигналу і шуму, n – загальна кількість дискретних вимірів на интервалі статистичного аналізу τ;

$\overline{W_n}=\frac{1}{M}\left[\sum_{k=0}^{n}\left\{\xi_k\right\}^2\Delta t_{k1}+\sum_{j=0}^{n}\left\{\xi_j\right\}^2\Delta t_j+...\right]$ – усереднене на M інтервалах значення енергії внутрішнього шуму. Відношення статистичної оцінки сумарної енергії сигналу і шуму до усередненої енергії шуму за декілька попередніх інтервалів аналізу називатимемо надалі енергетичним відношенням правдоподібності, маючи на увазі при цьому тільки його функціональний зв'язок. Поріг прийняття рішення про виявлення радіосигналу L_0 у радіолокації визначається за критерієм Неймана-Пірсона з виразу умовної ймовірності хибної тривоги. Для моделі χ^2-розподілу суми квадратів амплітуд оцифрованих гаусівських шумових вибірок умовна ймовірність хибних тривог має вигляд:

$$F=\frac{1}{\sqrt{2^n\sigma^{2n}}\Gamma(n/2)}\int_{L_0}^{\infty}\left((y)^{2\left[\left(n/2\right)-1\right]}\right)\exp\left(-\frac{(y)}{2\sigma^2}\right)dy.$$

Щільність ймовірності розподілу квадрата суми випадкових величин має вигляд інтегралу згортки гаусівської функції розподілу і χ^2 – розподілу:

$$f(y)=\frac{1}{\sigma^2}\int_{-\infty}^{\infty}f_{\chi^2}\left(\frac{t}{\sigma^2},n\right)f_N\left((y-t),\sum a_i^2,\sqrt{\sum 4a_i^2\sigma^2}\right)dt.$$

Умовна ймовірність правильного виявлення енергії сумарного детермінованого сигналу і гаусівського шуму для різної тривалості радіосигналів при фіксованій умовній ймовірності хибної тривоги F і збігу інтервалу аналізу з тривалістю радіосигналу залежно від відношення енергій сигналу і шуму, отримані методом чисельного інтегрування, подана на рис.1. На рис. 2 приведені графіки залежності умовної ймовірності правильного виявлення D енергії суми детермінованого радіосигналу з випадковою початковою фазою і гаусівського шуму при збігу інтервалу аналізу з тривалістю (a) і з половиною тривалості радіосигналу (b) для $F=10^{-6}$;

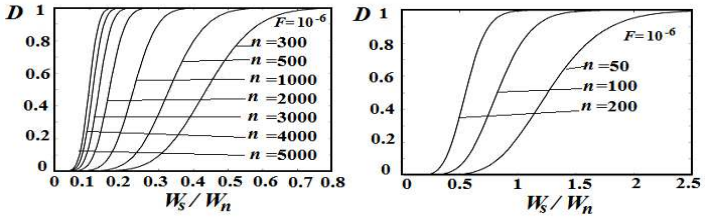


Рис.1 Умовна ймовірність правильного виявлення сумарної енергії детермінованого радіосигналу різної тривалості і гаусівського шуму від відношення енергій радіосигналу і шуму

10^{-8}; 10^{-10} від амплітудного відношення сигнал/шум q відомого способу виявлення при тривалості сигналу пропорційною *n* вибірок і отримані з імітаційної аналого-цифрової моделі статистичним шляхом для несучої частоти $f = 2 \cdot 10^8$ Гц і частоти оцифрування $f_ц = 2 \cdot 10^9$ Гц при усереднюванні 10^5 реалізацій на кожну точку.

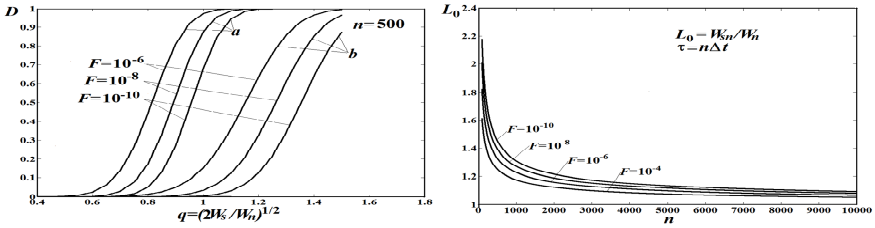


Рис. 2 Графіки залежності умовної ймовірності правильного виявлення радіосигналів і порогу прийняття рішення L_0 про виявлення радіосигналу від його тривалості

Виграш в дальності виявлення цілей при використанні енергетичного критерію в порівнянні з відомим (Табл.1) оцінюється за відношенням максимальних дальностей виявлення цілей при енергетичному виявленні r_E і при відомому способі виявлення r_A:

$$\frac{r_E}{r_A} = \sqrt[4]{\frac{\gamma_\Sigma^A}{\gamma_\Sigma^E}} .$$

*Таблиця*1

Виграш в дальності виявлення при енергетичному виявленні

n	W_s/W_n $F=10^{-6}; D=0,9$	q_E	q_A	r_E/r_A
500	0,45	0,9486	6,5	1,618
1000	0,3	0,7746	6,5	1,7
1500	0,25	0,7071	6,5	1,74
4500	0,145	0,538	6,5	1,86
6500	0,1	0,447	6,5	1,95
10^5	0,027	0,2323	6,5	2,299

Практична реалізація способу енергетичного виявлення можлива шляхом послідовного або паралельного статистичного аналізу інтервалів часу, рівних тривалості радіосигналу протягом періоду слідування радіосигналів. Енергетичне виявлення радіосигналу – це знаходження інтервалу часу, де сумарна енергія сигналу і шуму перевищує поріг виявлення.

На рис. 3 приведені графіки залежності середньоквадратичної помилки визначення дальності до цілі в довжинах хвиль зондуючого сигналу при тривалості радіосигналів τ~100; 300λ і затримці обробки інформації між часовими каналами виявлення Δτ: 10λ при аналого-цифровому моделюванні і усереднюванні 1000 реалізацій на кожну точку від енергетичного відношення сигнал/шум. На рис.4 приведені графіки залежності середньоквадратичної помилки визначення дальності до цілі від затримки радіосигналу в каналах виявлення при фіксованих значеннях енергетичного відношення сигнал/шум. В основу теорії оцінювання параметрів радіосигналу при енергетичному підході, як і в класичному випадку, покладена мінімізація умовного середнього ризику для кажної реалізації **y** шляхом пошуку оцінки

$\widehat{\boldsymbol{\alpha}} = \widehat{\boldsymbol{\alpha}}\left[\left(y + x_{emi}\right)^2\right]$ при заданих функціях вартості і використанні апостеріорного енергетичного відношения правдоподібності як вимірювального інструменту.

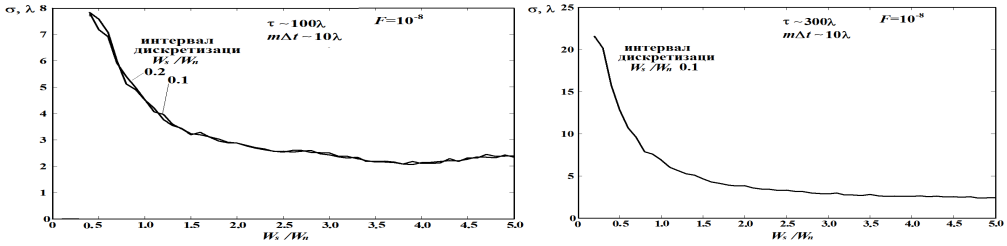


Рис. 3 Графіки залежності середньоквадратичної помилки визначення дальності до цілі від енергетичного відношення сигнал/шум

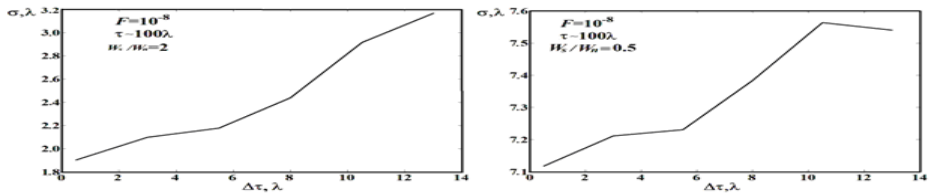


Рис. 4 Графіки залежності середньоквадратичної помилки визначення дальності до цілі від затримки радіосигналу в каналах виявлення

Енергетичний підхід до теорії оцінювання параметрів радіосигналу

Регулярна оцінка максимуму апостеріорної щільності ймовірності суми енергій сигналу и шуму знаходиться із умови $\frac{\partial \mathrm{p}\left(\boldsymbol{\alpha} / \mathbf{y}^2\right)}{\partial \boldsymbol{\alpha}_\mathrm{i}} = 0$ при $\boldsymbol{\alpha} = \widehat{\boldsymbol{\alpha}},$ де $\mathrm{i} = 1, 2, ...\mathrm{m}$ і співпадає з оцінкою апостеріорного математичного очікування. При відсутності апріорних даних $\mathrm{p}(\boldsymbol{\alpha}) = \mathrm{const}$ щільність ймовірності $p\left(\boldsymbol{\alpha} / y^2\right)$ замінюється на функцію енергетичної правдоподібності $\mathrm{p}\left(\mathrm{y}^2 / \boldsymbol{\alpha}\right)$, енергетичне відношення правдоподібності $\mathrm{L}\left(\boldsymbol{\alpha} / \mathrm{y}^2\right)$. Це призводить до умови максимуму енергетичного відношення правдоподібності $\frac{\partial \mathrm{p}\left(\mathrm{y}^2 / \boldsymbol{\alpha}\right)}{\partial \boldsymbol{\alpha}_\mathrm{i}} = 0$ при $\boldsymbol{\alpha} = \widehat{\boldsymbol{\alpha}},$ або до $\frac{\partial \mathrm{L}\left(\mathrm{y}^2 / \boldsymbol{\alpha}\right)}{\partial \boldsymbol{\alpha}_\mathrm{i}} = 0$ при $\boldsymbol{\alpha} = \widehat{\boldsymbol{\alpha}},$ що означає – після приймання реалізації **y** при відсутності апріорних даних регулярна оптимальна оцінка $\widehat{\boldsymbol{\alpha}}$ знаходиться із умови максимуму енергетичного відношення правдоподібності на виході приймача виявлення при використанні множини можливих значень $\boldsymbol{\alpha}$ еталонних (очікуваних) сигналів. На відміну від класичної теорії оцінювання використання енергетичного відношення правдоподібності дозволяє оцінити значення параметрів радіосигналів за енергетикою менших за рівень внутрішніх шумів.

Вимірювання (оцінка) параметрів виявленого радіосигналу здійснюється шляхом пошуку еталонного радіосигналу за максимумумом енергетичного відношення правдоподібності суми вхідного радіосигналу, шуму і змінного за параметрами еталонного радіосигналу по відношенню до усередненого значення енергії шуму для простої функції вартості: $\max_{\mathrm{j}} \frac{\mathrm{W_{сш}} + \mathrm{W_{етj}}}{\mathrm{W_{ш}}} > \mathrm{L}_0 \ \forall\ \mathrm{j} \in 1...\mathrm{N}$, де множина N – кількість змінних параметрів еталонного радіосигналу з заданим кроком дискретизації. Дослідження детермінованої моделі визначення максимуму сумарної енергії співвимірних виявленого радіосигналу із сукупністю еталонних показали наступну закономірність (рис.5): значення оцінки доплерівської частоти залежить від тривалості радіосигналу (рис.6) і при тривалих

радіосигналах виникає неоднозначність оцінки (рис.5b), оцінка початкової фази визначається кроком дискретизації еталонних радіосигналів.

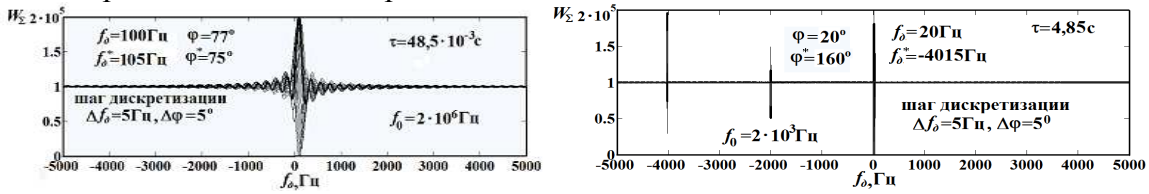


Рис. 5 Залежність максимуму сумарної енергії виявленого і еталонних радіосигналів в діапазоні доплерівських частот при фіксованій дискретизації для різних тривалостей

Графік залежності максимальної помилки (потенційній точності) визначення доплерівської частоти радіосигналу від його тривалості за максимумом сумарної енергії для кореляційного способу обробки інформації подано на рис.6.

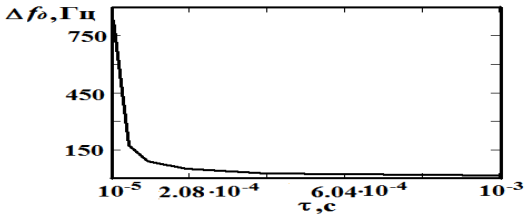


Рис.6 Потенційна точність визначення доплерівської частоти від тривалості радіосигналу при використанні енергетичного критерію і кореляційного способу обробки інформації

Можливість оцінки початкової фази і доплерівської частоти фазовим методом

Сутність фазового методу оцінювання початкової фази і доплерівської частоти радіосигналів полягає у формуванні із тривалого радіосигналу радіосигналів різної тривалості для досягнення однозначності оцінювання початкової фази і доплерівської частоти для різних класів об'єктів.

Дослідженню підлягала детермінована модель суми вхідного гармонічного і еталонного радіосигналів на частоті $f = 2 \cdot 10^8$ Гц та еквівалентної амплітуди шуму $n_{екв}$, визначеної із усередненої енергії шуму, для різних тривалостей радіосигналів $\tau = 10^{-3};\ 10^{-4}; 10^{-6}$ с :

Залежність енергетичного відношення правдоподібності при різній тривалості радіосигналів при синфазному складанні еталонного і виявленого радіосигналу в діапазоні ±3кГц для різних доплерівських частот виявленого радіосигналу подана на рис.7.

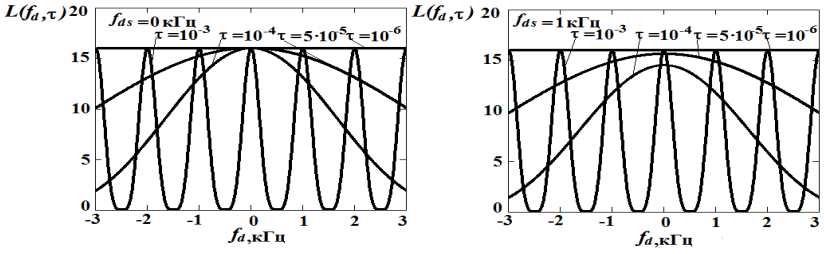


Рис.7 Залежність енергетичного відношення правдоподібності від доплерівської частоти при різній тривалості радіосигналу при рівних початкових фазах еталонного і виявленого радіосигналів

Залежність енергетичного відношення правдоподібності від початкових фаз прийнятого і еталонного радіосигналів за відсутності частотних зрушень в широкосмуговому каналі подана на рис.8. Із пропорції значень енергетичних відношень правдоподібності визначається початкова фаза вхідного радіосигналу,а її знак за розподілом max L у непарному квадратурному каналі. Розподіл максимумів відношення правдоподібності для різних доплерівських частот на виході каналів оцінювання при рівних амплітудах вхідного радіосигналу і шуму і амплітуді еталонних радіосигналів в два рази перевершуючих амплітуду вхідного радіосигналу подано на рис.9.

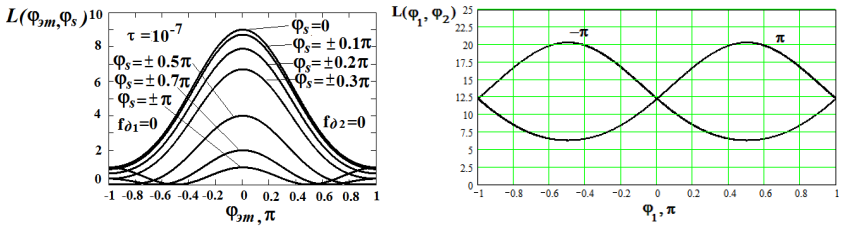


Рис.8 Залежність енергетичного відношення правдоподібності від початкових фаз прийнятого і еталонного радіосигналів у широкосмуговому парному і непарному квадратурних каналах

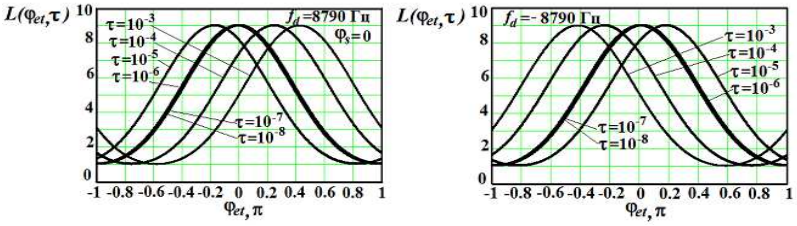


Рис.9 Розподіл максимумів енергетичного відношення правдоподібності для різних доплерівських частот на виході різносмугових каналів оцінювання в діапазоні фазових зрушень еталонних радіосигналів

Таким чином, для енергетичного оцінювання параметрів радіосигналів фазовим методом необхідно з тривалого радіосигналу сформувати різнотривалі вибірки, оцінити початкову фазу прийнятого радіосигналу в широкосмуговому радіоканалі, сформувати квадратурні еталонні радіосигнали і дешифрувати розподіл максимумів енергетичного відношення правдоподібності на парному виході різносмугових каналів.

Розглянуті основи енергетичного виявлення і оцінювання параметрів радіосигналів дозволяють виявляти і оцінювати параметри радіосигналів за енергетикою співвимірною (або меншою) з внутрішніми шумами радіоприймача без впливу і при впливі активних маскуючих перешкод, що дозволить покращити якісні показники озброєння і зменшити енергетичні витрати для вирішення тих же завдань.

ЛІТЕРАТУРА

1. Г.В. Пєвцов, А.Я. Яцуценко, Д.В. Карлов, Ю.В. Трофименко Метод енергетичного виявлення радіосигналів //Системи управління, навігації та зв'язку. – К.: – 2010.– №4 (16). – с. 72 – 76.

2. Патент на корисну модель 57216. Україна, МПК G01S 7/02. /Процес енергетичного виявлення радіосигналів Г.В.Пєвцов, А.Я.Яцуценко, та ін.; – №201012202; заявл. 15.10.2010; опубл. 10.02.2011, Бюл. №3.

3. Пєвцов Г.В., Яцуценко А.Я., Карлов Д.В., Трофименко Ю.В., Клімішен О.О. //Патент на корисну модель 64707. Україна, МПК G01S 7/34. /Спосіб багатоканального за часом енергетичного виявлення радіосигналів; – №201106721; заявл. 30.05.2011; опубл. 10.11.2011, Бюл. №21.

4. Пєвцов Г.В., Яцуценко А.Я., Карлов Д.В., Трофименко Ю.В., Челпанов А.В., Шевченко В.І. // Патент на корисну модель 64706. Україна, МПК G01S 7/34. /Спосіб енергетичного виявлення радіосигналів при впливі активних маскуючих перешкод; – №201106697; заявл. 30.05.2011; опубл. 10.11.2011, Бюл. №21.

5. Пєвцов Г.В., Яцуценко А.Я., Карлов Д.В., Трофименко Ю.В., Клімішен О.О., Остапова А.М. Основи енергетичного виявлення-оцінювання параметрів радіосигналів //Сборник научных трудов. 4-го Международного радиоэлектронного форума (МРФ 2011). – Харьков. – 2011. – С. 192 – 195.

6. G. Pevtsov, A. Yatsutsenko, Yu. Trofimenko, D. Karlov, M. Bortsova Theoretical Basics of Radar Signals Energy Detection [Electron recourse]: Proc. of the 14th International Conference on Mathematical Methods in Electromagnetic Theory. – Kharkov.: KNAME. – 2012 – 1 CD-ROM.

Плуговий Ю. А. (ГУЗІС)

РОЗВИТОК СИСТЕМИ ЗВ'ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ НА ОСНОВІ ПЕРСПЕКТИВНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ, КОМПЛЕКСІВ ТА СИСТЕМ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Сучасні погляди на реструктуризацію системи управління Збройними Силами, перерозподіл інфраструктури системи пунктів управління та впровадження у її склад нових автоматизованих систем (комплексів) управління та комплексів (засобів) зв’язку призводять до зміни структури системи зв’язку Збройних Сил України.

Історія, як і науково-технічний прогрес не стоять на місці, а це значить що з впровадженням сучасних інформаційних технологій виникає потреба у розвитку системи зв’язку Збройних Сил.

Метою розвитку системи зв’язку Збройних Сил України є створення єдиного інформаційно-телекомунікаційного середовища.

Розвиток системи зв’язку Збройних Сил України на основі впровадження сучасних телекомунікаційних систем, комплексів та систем зв’язку спеціального призначення забезпечить:

– покращення якості обміну інформацією;

– надання службовим особам органів військового управління інформаційно-телекомунікаційних послуг (мови, даних, відео тощо);

– підвищення показників стійкості, мобільності, пропускної спроможності і розвідзахищеності мереж та ліній зв’язку на основі:

широкого впровадження новітніх інформаційно-телекомунікаційних технологій;

перспективних цифрових комплексів, засобів зв’язку і автоматизації.

Реалізацію плану розвитку системи зв’язку вважається за доцільне здійснити шляхом поступового переходу системи зв’язку на цифрові комплекси і засоби зв’язку та засоби автоматизації.

Це забезпечить поетапне переозброєння стаціонарного і мобільних компонентів системи зв’язку.

Цей шлях вважається оптимальним, оскільки він може базуватись на збалансованому оборонному бюджеті та передбачати перерозподіл видатків з утримання Збройних Сил України.

Головним напрямом розвитку системи зв’язку є реалізація вимог проекту Концепції розвитку системи зв’язку Збройних Сил України на період до 2020 року.

Виходячи із зазначеного слід назвати шляхи розвитку єдиного інформаційно-телекомунікаційного середовища:

забезпечення сумісності засобів, комплексів зв’язку і автоматизації усіх ланок управління Збройних Сил України;

створення автоматизованих мереж радіозв’язку;

створення системи транкінгового зв’язку Збройних Сил України;

ефективне використанням орендованих цифрових каналів (потоків);

побудова цифрових радіорелейних, тропосферних, волоконно-оптичних ліній прив’язки до мереж операторів зв’язку України та Державної телекомунікаційної мережі спеціального призначення;

розгортання мереж (ліній) широкосмугового швидкісного радіодоступу;

створення системи супутникового зв’язку Збройних Сил України;

створення сучасної системи захисту інформації та кібернетичної безпеки в ІТС;

створення автоматизованої системи управління зв’язком;

проведення модернізації існуючих засобів зв'язку військового призначення, що знаходяться на озброєнні;

розробка та впровадження новітніх засобів та комплексів зв'язку вітчизняного та закордонного виробництва, в тому числі подвійного призначення.

Визначення шляхів розвитку системи зв'язку Збройних Сил України доцільно здійснювати з урахуванням тенденцій розвитку систем військового зв'язку провідних країн світу, а також тенденцій розвитку державної телекомунікаційної мережі загального користування і телекомунікаційних мереж інших військових формувань та правоохоронних органів.

Розвиток системи зв'язку Збройних Сил України повинен враховувати:

перспективну структуру ЗС до 2017 року;

перспективну систему управління ЗС;

перспективну структуру пунктів управління ЗС;

вимоги, що ставить перед системою зв'язку Єдина автоматизована система управління Збройними Силами України.

Для реалізації політики у сфері реформування та розвитку системи зв'язку Збройних Сил України у 2012 році Головним управлінням зв'язку та інформаційних систем Генерального штабу Збройних Сил України були розроблені та затверджені пріоритетні напрями розвитку системи зв'язку до 2017 року, з урахуванням необхідного фінансування. Зокрема для забезпечення створення цифрової системи зв'язку Збройних Сил України до 2017 року передбачається:

переоснащення системи зв'язку ЗС України на цифрові засоби: для 100 % стаціонарної компоненти та для 25 % польової компоненти до 2014 року.

створення цифрової прив'язки стаціонарних ІТВ до 2014 року (ця робота бере свій початок з 2010 року);

впровадження захищеного автоматичного телефонного зв'язку;

модернізація засобів радіорелейного та тропосферного зв'язку (до кінця 2017 року);

створення автоматизованої системи управління зв'язком (до кінця другого кварталу 2015 року з подальшим удосконаленням створеної системи до 2017 року);

створення системи супутникового зв'язку Збройних Сил України на базі національного супутника (до 2017 року);

створення цифрової автоматизованої системи радіозв'язку з використанням самоналагоджувальних мереж зв'язку (до 2016 року з подальшим удосконаленням створеної системи до 2017 року);

створенням сучасної системи захисту інформації та кібернетичної безпеки в ІТС з впровадженням апаратури засекречування IP шифрування вітчизняного виробництва в мережах передачі даних, ВКЗ.

Враховуючи це, розвиток стаціонарного компоненту системи зв'язку полягає у побудові перспективних телекомунікаційних мереж, на базі впровадження IP-протоколів та технології MPLS, що дозволить забезпечити:

– створення єдиного транспортного середовища;

– надання необхідних інформаційних та телекомунікаційних послуг службовим особам органів управління;

– ефективне управління ресурсами телекомунікаційних та інформаційних систем (мереж);

– створення єдиної системи адресування, нумерації та пошуку абонентів;

– сумісну роботу з телекомунікаційною мережею загального користування України, системами зв'язку інших військових формувань та правоохоронних органів, Державною телекомунікаційною мережею спеціального призначення;

– сумісність з мобільним компонентом системи зв'язку під час його розгортання та застосування;

– впровадження комплексних систем захисту інформації та забезпечення кібернетичної безпеки.

Основу телекомунікаційної системи стаціонарного компоненту Збройних Сил України в майбутньому буде складати транспортна мережа Державної телекомунікаційної мережі спеціального призначення до якої будуть підключатись головні (базові) ІТВ, регіональні (територіальні) ІТВ, а в окремих випадках периферійні ІТВ.

На кінець 2017 року ми плануємо використовувати телекомунікаційний ресурс в таких межах:

Головні (базові) ІТВ повинні віртуально з'єднуватися між собою лініями зв'язку. До головних (базових) ІТВ за територіальним принципом, будуть підключені регіональні (територіальні) ІТВ пунктів управління, штабів, установ.

До регіональних (територіальних) ІТВ, за територіальним принципом, будуть підключені периферійні ІТВ пунктів управління, штабів, установ з ієрархічним розподілом функцій доступу програмно-апаратним способом.

Обмін інформацією між пунктами управління різного призначення буде здійснюватись як по фізичним так і по віртуальним каналах зв'язку.

На напрямках зв'язку між ІТВ буде використовуватись в тому числі, орендований телекомунікаційний ресурс, лінії прямого радіо- та супутникового зв'язку, цифрові кабельні, радіорелейні та волоконно-оптичні лінії зв'язку та прив'язки Збройних Сил України.

Розвиток структури стаціонарного компоненту планується проводити за регіональним принципом „кущовим" методом виходячи з забезпечення циркуляції інформаційних потоків, що виникають між органами управління, враховуючи ієрархічну структуру системи управління.

Іншим пріоритетом розвитку системи зв'язку Збройних Сил України є переобладнання її мобільного компонента.

Комплекси та засоби зв'язку мобільного компоненту повинні забезпечувати необхідний рівень організаційно-технічної та апаратно-програмної взаємодії між собою та стаціонарним компонентом системи зв'язку Збройних Сил України та інших військових формувань і правоохоронних органів.

Розвиток мобільного компоненту полягає у розробці, закупівлі та впровадженні новітніх засобів військового призначення для обладнання:

комплексних апаратних зв'язку різного призначення у тому числі засекреченого зв'язку;

комплексних апаратних доступу;

командно-штабних машин;

штабних машин з кінцевими засобами зв'язку, автоматизованими робочими місцями та іншими засобами зв'язку;

станцій тропосферного зв'язку;

пунктів управління зв'язком;

комплексів моніторингу стану захищеності ІТС;

уніфікованих апаратних технічного забезпечення.

При цьому планується використовувати новітні засоби зв'язку військового призначення, які можуть застосовуватися окремо, це:

станції радіорелейного зв'язку;

станції супутникового зв'язку;

станції широкосмугового швидкісного радіодоступу;

широкосмугові багатодіапазонні радіозасоби;

рухомі, переносні та абонентські радіо- засоби.

З урахуванням перспективної структури Збройних Сил України управління військами (силами) планується здійснювати:

в стратегічній ланці управління ЗС України з використанням як стаціонарної, так і мобільної компоненти системи зв'язку з відповідних пунктів управління;

в оперативно-тактичній і тактичній ланці управління ЗС України шляхом використання засобів зв'язку широкополосного доступу встановлених в мобільних комплексних апаратних зв'язку, а також з використанням радіорелейних напрямків в якості резервних ліній зв'язку.

Заходи щодо розвитку системи зв'язку ЗС України пропонується проводити у три етапи, а очікуваними результатами по етапах розвитку системи зв'язку ЗС України стануть:

за результатами виконання **першого етапу** (2012-2014 роки) слід очікувати:

– переоснащення на новітні цифрові програмно-апаратні засоби та комплекси стаціонарного компоненту системи зв'язку;

– закупівлю цифрових засобів зв'язку в тому числі іноземного виробництва (з урахуванням критерію „ефективність-вартість") для визначення кращих зразків під час дослідної експлуатації елементів мобільних компонентів;

– створення технічної основи для впровадження елементів Єдиної автоматизованої системи управління;

– взаємосумісну роботу стаціонарного компоненту системи зв'язку Збройних Сил України з системами зв'язку інших військових формувань та правоохоронних органів України;

– завершення створення стаціонарної складової системи захисту інформації та кібернетичної безпеки в стаціонарних ІТС.

За результатами виконання **другого етапу** (2015-2017 роки) слід очікувати:

– переоснащення, на цифрові засоби зв'язку, мобільного компоненту системи зв'язку Сил негайного реагування – аеромобільних (повітрянодесантних) бригад, бригади морської піхоти, бригад надводних кораблів, розвідувальних батальйонів, частин, підрозділів Сил спеціальних операцій і військової розвідки, а також рухомих ІТВ допоміжних ПУ Генерального штабу та Сил спеціальних операцій;

– завершення створення мобільної складової системи захисту інформації та кібернетичної безпеки в ІТС.

– розгортання в Україні виробництва (в тому числі спільного) новітніх засобів і комплексів зв'язку із залученням вітчизняних (іноземних) виробників.

За результатами виконання **третього етапу** (2018-2020 роки) слід очікувати:

– повного переоснащення мобільного компоненту системи зв'язку Збройних Сил України;

– нарощування можливостей системи захисту інформації та кібернетичної безпеки в ІТС.

к.т.н. Раєвський В.М. (ВІТІ НТУУ „КПІ”)
Залужна С.В. (ВІТІ НТУУ „КПІ”)

МОЖЛИВОСТІ СУЧАСНИХ ЗАСОБІВ РАДІОЗВ’ЯЗКУ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ЗА ДОСВІДОМ БАГАТОНАЦІОНАЛЬНИХ ВІЙСЬКОВИХ НАВЧАНЬ ”COMBINED ENDAEVOR - 2012”

У вересні 2012 року зв’язківці Збройних Сил україни приймали участь у традиційних багатонаціональних військових навчаннях **”Combined Endeavor – 2012”** (укр. „Спільні зусилля”) що проводяться у Німеччині і входять до більш загальної програми „Партнерство заради миру”. Навчання мають за мету підготовку військових коаліційних сил до спільних дій під час участі в багатонаціональних операціях шляхом спільного планування, підготовки, тестування та інтеграції телекомунікаційних та інформаційних систем і систем автоматизованого управління військами, розвиток тактик, технологій та процедур забезпечення взаємосумісності зазначених систем Учасники навчань мали можливість досягнути взаємосумісності прийнятих на озброєння та перспективних телекомунікаційних та інформаційних систем і систем автоматизованого управління військами, та провести з учасниками тренування, спрямовані на підготовку та набуття спроможності працювати в коаліційному середовищі (рис. 1).

Рис. 1. Емблеми навчань **”Combined Endevor”** та агентства інформаційної безпеки

В цьогорічних навчаннях приймали участь 42 країни – як члени НАТО, так і партнери організації (рис. 2).

Рис. 2. Склад учасників міжнародних навчань

Навчання цього року мали відмінність – проходили на фоні загальної тактичної обстановки. Передбачалось, що землетрус силою 7,7 балів вразив умовну країну TYTAN, розташовану в районі Африканського Рогу, в результаті чого країна зазнала серйозних руйнувань, загинули люди і муніципальні служби припинили роботу. Порушено роботу всієї інфраструктури країни (електро та водопостачання, лікарні, комунікації). В багатьох міських районах були зареєстровані випадки грабежів, місцеві банди розширили зони свого впливу. Також було повідомлено, що вони перешкоджають розповсюдженню будь-яких видів гуманітарної допомоги. Інформаційні агентства повідомили, що велика кількість постраждалих шукають притулку в країні PETRAGEROS. Зареєстровані випадки загибелі дітей внаслідок тяжких умов. Уряд PETRAGEROS відразу ж оголосив, що не готовий прийняти такий потік біженців. Користуючись ситуацією, що склалася сили держави KAMON перейшли кордон і захопили західну та північну частини країни TYTAN. TYTAN попросив Організацію Об'єднаних Націй про негайну військову та гуманітарну допомогу допомогу і запобігання подальшого просування сил KAMON (рис. 3).

Рис. 3. Карта оперативної обстановки навчань

Рада Безпеки ООН санкціонувала розгортання багатонаціональних сил для надання допомоги уряду TYTAN, виводу сил KAMON, відновлення безпеки, розподілу гуманітарної допомоги і стабілізації обстановки в країні.

До складу багатонаціональних сил за сценарієм навчань входили і підрозділи Збройних Сил України – механізований батальйон, рота високомобільних десантних військ та два корабля ВМС України. Для забезпечення управління зазначеними підрозділами була розгорнута відповідна система зв'язку (рис. 4), що надавала можливість передавати всі види сучасної інформації (передача голосу та даних, електронна пошта, робота в інформаційній системі старшого штабу що використовує програмний продукт C2PC) та здійснювати управління не тільки місцеве управління, але і віддаленими підрозділами – рота високомобільних десантних військ територіально знаходилась в м. Житомир, кораблі ВМС України знаходились у м.Севастополь. Для двох останніх підрозділів управління здійснювалось як по проводовим лініям зв'язку так і по короткохвильовим лініям зв'язку з використанням радіостанцій корпорації Harris RF-5800H з підсилювачем потужності 150 Вт

та радіостанція вітчизняного виробництва ТОВ „Телекарт-прилад” Р-1150 з підсилювачем потужності 400 Вт (рис. 5).

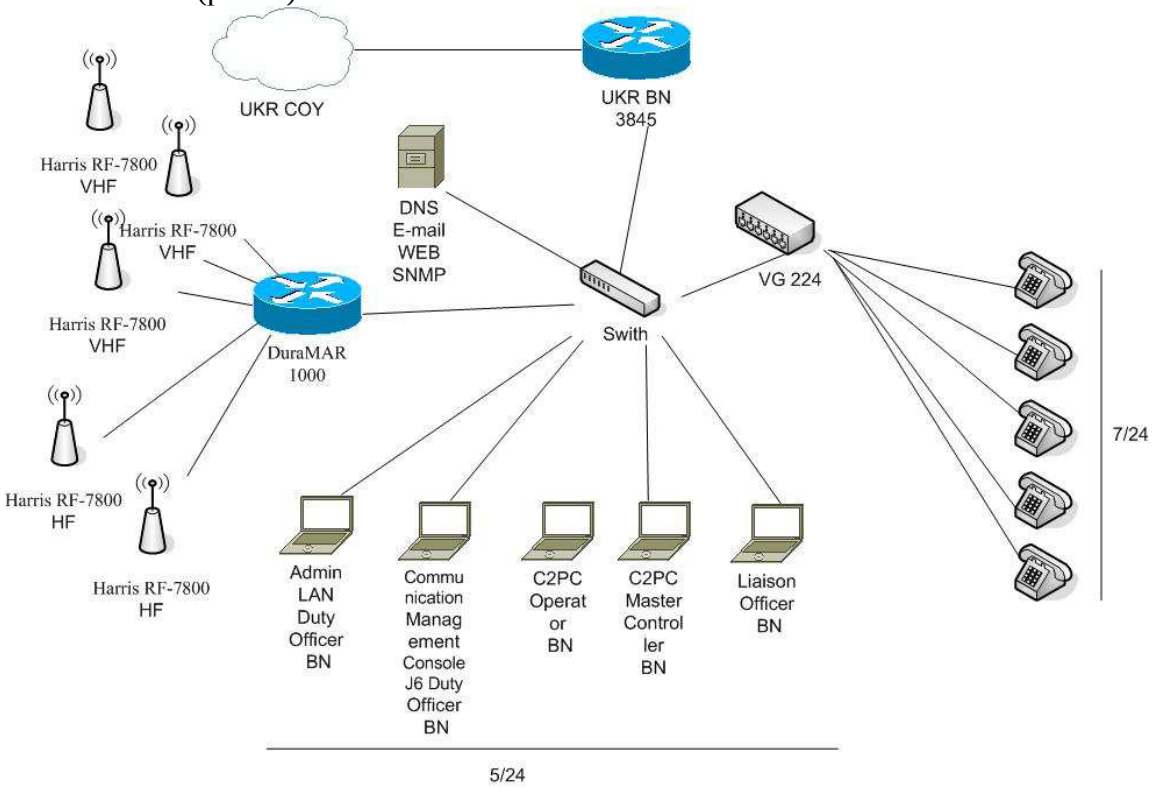


Рис. 4. Структура телекомунікаційної мережі українського батальйону

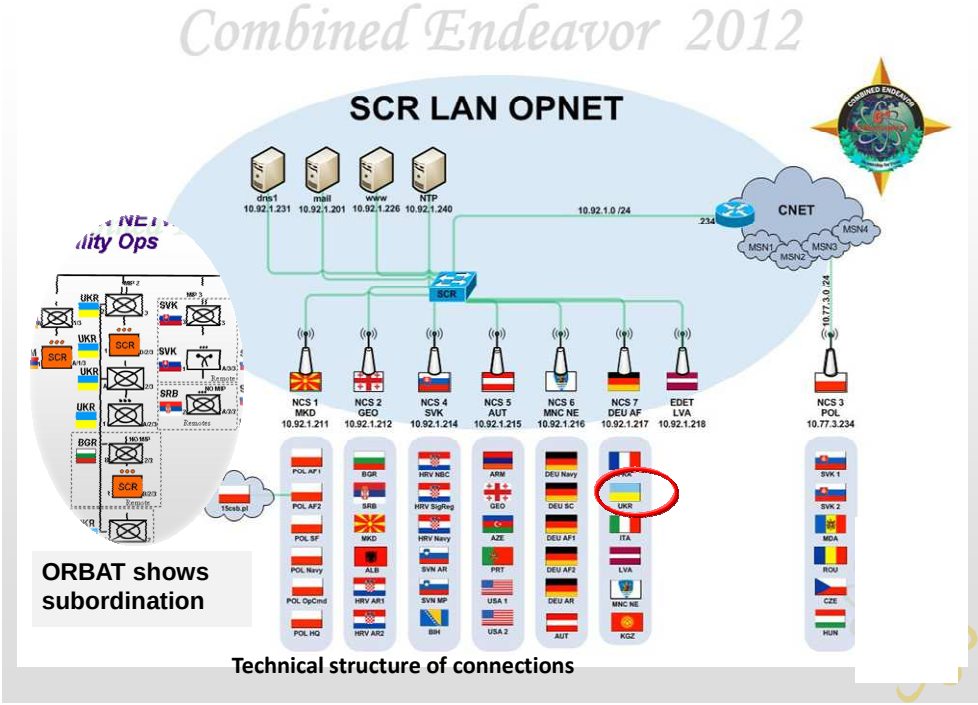


Рис. 4. Забезпечення управління засобами короткохвильового радіозв’язку

Після проведення трьох етапів умовної миротворчої операції було відновлено територіальну цілісність умовної африканської країни, відновлено роботу уряду, громадський порядок та роботу муніципальних служб.

Також зазначимо, що паралельно з основними навчаннями проходили два семінари. Перший з них – Семінар із захисту інформації в інформаційно-телекомунікаційних системах **„Ciber Endeavor ”**, що вдосконалював знання з напрямів:

аналіз відомих кіберконфліктів та технічних аспектів кібератак;

боротьба з кіберзлочинністю та прогнозування її розвитку;

національні кіберстратегії та концепції кіберзахисту США та інших держав;

загальна структура та організація роботи кіберкомандування НАТО у Європі;

організація інформаційної безпеки організацій;

забезпечення кібербезпеки і моніторингу кіберпростору;

прогнозування розвитку майбутніх кібервійн та конфліктів;

способи та алгоритми зниження кіберзагроз;

принципи тестування мережевого обладнання та програмних засобів кіберзахисту

аналіз поведінки шкідливих програм;

аналіз прикладів кібератак і викликів для інформаційних систем;

основні способи та методи технічного моніторингу кіберпростіру та кіберзахисту;

створення та використання програм захисту та забезпечення конфіденційності.

Інший присвячений питанням частотного менеджменту „Phoenix Endeavor” на якому вивчались питання:

пакет прикладних программ щодо планування та управління частотами **SPECTRAmil** фірми „LS telkom”

1. **Програмні засоби управління запитами та результатами частотної авторизації**:

SPECTRAweb – для загрузки даних в on-line;

SPECTRAplus – частотного авторизаційного процесу.

2. **Програмні засоби спектральної інженерії**:

SPECTRAmpt – планування місії тактичного рівня;

SPECTRAemc – інженерії військового спектру.

3. **Програмні засоби радіомоніторингу**:

MONITORplus – програмний засіб менеджменту директив моніторингу і його результатів;

Interface to LS Observer – програмний засіб для динамічного спектрального менеджменту;

SPECTRAplan – програмний засіб для планування військового спектру.

Таким чином, можна зазначити, що військовослужбовцями зв’язківцями Збройних Сил України під час навчань:

отримано важливу системну інформацію щодо принципів побудови мереж зв’язку, інформаційних систем та підходів до захисту інформації і кіберзахисту в країнах – учасницях навчання;

ознайомлені з практичною програмно-апаратною реалізацією зазначених принципів;

проведено тестування цифрового телекомунікаційного обладнання та програмного забезпечення, що плануються до прийняття на озброєння підрозділів Сухопутних військ ЗС України, визначених для участі у багатонаціональних операціях, виявлені їх функціональні можливості та підготовлені висновки та рекомендації щодо їх використання (доопрацювання);

надано практику особовому складу ЗС України щодо роботи у складі багатонаціональних штабів, які розгортаються для проведення багатонаціональних операцій, та у спільному плануванні, розгортанні, підготовці та використанні телекомунікаційних мереж та інформаційних систем і систем автоматизованого управління військами;

проведено оцінку відповідності сил та засобів, які знаходяться у готовності до розгортання для підтримки міжнародних миротворчих операцій, вимогам та стандартам організацій, під проводом яких може проводиться операція, з урахуванням рекомендацій і стандартів НАТО та комерційних стандартів.

д.т.н. Романюк В.А. (ВІТІ НТУУ „КПІ”)

СВІТОВІ ТЕНДЕНЦІЇ ВДОСКОНАЛЕННЯ ТАКТИЧНИХ МЕРЕЖ ЗВ’ЯЗКУ

На початку XXI століття посилилася тенденція до переходу від концепції „платформо-центричної війни” до „мережецентричної війни”, основною ідеєю якої є інтеграція всіх сил і засобів в єдиному інформаційному просторі, що дозволяє багаторазово збільшити ефективність їх бойового застосування за рахунок синергетичного ефекту.

Впровадження мережевих технологій у військову сферу стало дійсно революційним кроком, спрямованим на підвищення бойових можливостей збройних сил, але вже не тільки за рахунок підвищення вогневих, маневрених та інших характеристик індивідуальних платформ озброєння, а в першу чергу за рахунок скорочення циклу бойового управління.

Концепція мережецентрічної війни дозволяє в ході бойових дій виробляти перехід до мережецентричного управління військами (силами), тобто виконувати мережевий розподіл, одночасно доводячи інформацію до всіх ланок управління військами в масштабі часу, близькому до реального.

У концептуальному плані модель мережецентричної війни являє собою систему, що складається з трьох решіток-підсистем: сенсорної, інформаційної та бойової. Основу цієї системи складає інформаційна решітка, на яку накладаються взаємно пересічні сенсорна і бойова решітки. Інформаційна решітка-підсистема пронизує собою всю систему в повному обсязі. Елементами сенсорної системи є сенсори (засоби розвідки), а елементами бойової решітки – засоби враження. Ці дві групи елементів об’єднуються органами управління та командування.

Тобто мережецентричне ведення бойових дій характеризується не тільки в забезпеченні передачі розвідувальної інформації всім учасникам цих дій у реальному масштабі часу, але і високим рівнем організації (самоорганізації) функціонування елементів бойових порядків. Основною ознакою такої самоорганізації є безперервний оптимальний цілерозподіл в масштабах зони відповідальності або навіть театру військових дій.

Тактичній ланці висуваються більш жорсткі тимчасові вимоги до циклів управління. Транспортну основу інформаційних систем складають тактичні системи зв'язку і насамперед їх мобільна компонента. Мобільна компонента покликана забезпечити інформаційний обмін в інтересах усіх військ, що діють в тактичній зоні незалежно від їхнього підпорядкування і задач, які вони виконують.

Передбачається, що її архітектура буде неоднорідною ієрархічною, яка складається з трьох основних рівнів (рис. 1): 1-й – мобільні радіомережі нижньої ланки управління; 2-й – мережі мобільних базових станцій (МБС), що утворюють опорну мережу; 3-й – повітряна мережа, яка може бути реалізована на телекомунікаційних аероплатформах (безпілотних літальних апаратах) [2]. Додатковий нульовий рівень можуть утворювати сенсорні мережі (мережі телеметрії). Створення кожного рівня передбачає поліпшення показників якості функціонування всієї системи зв’язку.

Основні характеристики складових мобільної компоненти наведені в таблиці 1. Перший рівень являє собою сукупність мобільних радіомереж нижньої ланки управління побудованих за принципом мереж MANET [3]. Мобільні абоненти (солдат, танк, вертоліт тощо) оснащені радіотерміналами (переносними комп’ютерами із прийомопередавачами), які реалізують функції маршрутизації. Абоненти здійснюють інформаційний обмін безпосередньо між собою або використовують ретрансляцію (маршрутизацію) повідомлень. В якості ретранслятора (точніше маршрутизатора) може виступати будь-який мобільний абонент свого рівня або мобільна базова станція – елемент другого рівня ієрархії, що перебуває з ним в межах радіозв’язності.

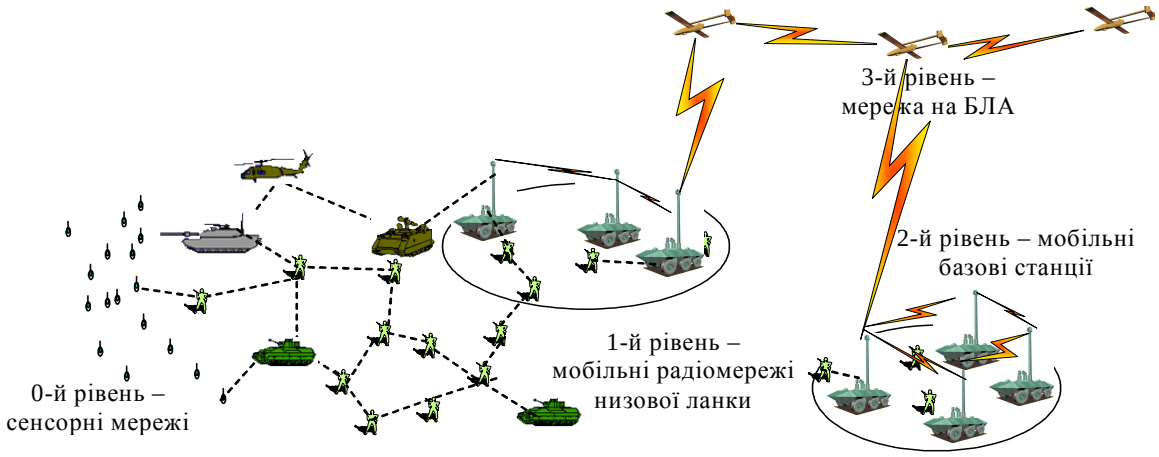


Рис. 1. Перспективна архітектура мобільної компоненти

Таблиця 1

Основні характеристики	**Мобільні радіомережі 1-й рівень**	**Мережа МБС – 2-й рівень**	**Сенсорні мережі – 0-й рівень**	**Мережа на літальних апаратах**
Розмірність	Сотні-тисячі	Десятки	Сотні-тисячі	Десятки
Принцип організації та побудови	Самоорганізація мережі, комутація пакетів, кожен вузол – маршрутизатор інформаційних повідомлень			
Мобільність	Висока	Низька	Низька	Дуже висока
Тип та спосіб управління	Розподілений, технологічний	Зоновий, організаційно-технологічний	Розподілений, (ієрархічний) технологічний	Зоновий, організаційно-технологічний
Способи розподілу радіоресурсу	Випадковий	Детермінований, гібридний	Випадковий	Детермінований
Потужність передавача терміналу; відстань зв'язку та швидкість передачі (залежать від частоти, потужності передавача, типу антени тощо)	Солдат – Од. Вт, до 1 км; транспортний засіб –20 Вт, декілька км; 0.01 – 1 Мб/с	Десятки Вт; до 10 км; між МБС > 20 Мб/с (радіоканал), між МБС >100 Мб/с (оптичний канал); між МБС-МА – 0.01-1 Мб/с; між МБС-БЛА >20 Мб/с	Визначається типом сенсорів; (для наземних – мВт, сотні метрів > 0.01 Мб/с)	Десятки Вт; десятки км; >20 Мб/с

Переваги мобільних радіомереж очевидні: відсутність етапу планування (можливість самоорганізації), швидке розгортання, децентралізоване управління (дуже висока живучість), робота в русі всіх елементів мережі тощо (табл. 2).

Визначено вимоги до перспективних радіозасобів:

– висока пропускна здатність радіоканалу (> 200 Кб/с);

– багатодіапазонність і багатофункціональність (FDMA/TDMA/CDMA);

– здатність програмування всіх видів і режимів роботи;

– автоматизація процесів ведення зв'язку (режим „включив та працюй" – Plug-and-Play) та можливість самоорганізації мережі;

– інтелектуальність, децентралізованість й оптимізація функцій управління мережевими ресурсами (маршрутизація, навантаження, топологія, радіоресурс, безпека й т.д.);

– робота з різними видами трафіка (мова, дані, відео);

– наявність системи позиціювання, спрямованих антен, робота в русі;

– модульність виконання, відкрита архітектура, низьке енергоспоживання.

В той же час існують значні *труднощі створення мобільних радіомереж* – необхідність рішення великої кількості наукових проблем (маршрутизація, розподіл радіоресурсів, управління потужністю, управління топологією, децентралізоване управління, безпека,

забезпечення заданої якості передачі інформації тощо) при обмеженнях ресурсу радіотерміналу (за ємністю пам'яті, продуктивністю процесора, енергоємністю батареї). Пропозиції щодо частини їх рішення можуть бути знайдені в [3].

Таблиця 2

Переваги (недоліки)	**За рахунок чого досягнуто (напрямки вдосконалення)**
(+) Висока живучість, мобільність всіх елементів мережі	Управління мережею – децентралізоване, здатність до самоорганізації. Кожний вузол – маршрутизатор, адаптація до умов функціонування
(+) Висока швидкість передачі в радіоканалі – потенційно 1...54 Мб/с	Зсув діапазону частот (сотні Мгц, од. ГГц). адаптація протоколу IEEE 802.11 до тактичних вимог, еволюція OFDM (Orthogonal Frequency-Division Multiplexing), оптимізація використання радіоресурсу, спрямовані антени (інтелектуальні фазові решітки), застосування технології MIMO (Multiple Input Multiple Output)
(+) Висока продуктивність мережі	Застосування нових ефективних інтелектуальних методів управління мережею, введення додаткових мережевих рівнів (мобільних базових станцій, безпілотних літальних апаратів, супутників)
(–) Незначна відстань безпосереднього зв'язку	Зв'язок в умовах прямої видимості – дальність зв'язку залежить від частоти, потужності, типу антени тощо. Недолік усувається використанням за рахунок маршрутизації
(+) Передача різних видів трафіку	Застосування нових протоколів канального та мережевого рівнів (протоколів підтримки заданої якості обслуговування)
(+) Маршрутизація	Застосування нових ефективних методів маршрутизації
(+) Висока безпека	Застосування гібридних систем захисту (симетричних та асиметричних), створення розподілених трастових центрів, систем виявлення вторгнень
(+) Висока завадозахищеність	Використання широкосмугових сигналів (метод частотних стрибків – FHSS, метод прямої послідовності – DSSS), в перспективі застосування гібридних схем розподілу ресурсів (FDMA/TDMA/CDMA), використання HIP (Host Identify Protocol) тощо

Другий рівень мобільної компоненти утворює мережа мобільних базових станцій (наземна магістральна мережа). Вона призначена для поліпшення якості зв'язку, а насамперед, підвищення продуктивності мобільної компоненти та надання заданої якості обслуговування абонентів.

Додатковою складовою мобільної компоненти можуть служити сенсорні мережі, що забезпечують прийом і передачу розвідувальної інформації про супротивника та видачу її органам управління військами та зброєю. Сенсорні пристрої являють собою інтегровану платформу, яка поєднує можливості сенсорів (зовнішніх датчиків, що реєструють сукупність параметрів – акустичних, вібраційних, радіаційних, хімічних, біологічних тощо) з мікрокомп'ютерами, які з'єднані у бездротову мережу.

Для зв'язку між географічно розділеними угрупованнями військ (зонами мережі) або підвищення надійності зв'язку між МБС та продуктивності мобільної компоненти створюється верхній рівень – повітряна магістральна мережа на телекомунікаційних аероплаформах.

Визначені вимоги до перспективних радіозасобів:

– висока пропускна здатність радіоканалу (> 200 Кб/с);

– багатодіапазонність і багатофункціональність (FDMA/TDMA/CDMA) роботи;

– здатність програмування всіх видів і режимів роботи;

– самоорганізація мережі (режим Plug-and-Play);

– інтелектуальність, децентралізованість й оптимізація функцій управління мережевими ресурсами (маршрутизація, навантаження, топологія, радіоресурс, безпека й т.д.);

– робота в різних мережах і з різними видами трафіка (мова, дані, відео);

– наявність системи позиціювання, спрямованих антен;

– робота в русі, модульність виконання й відкрита архітектура;

– низьке енергоспоживання.

Аналіз останніх публікацій дозволив визначити основні напрямки підвищення продуктивності бездротових мереж (табл. 3). Виграш в цієї таблиці вказаний в умовних одиницях.

Таблиця 3

Проблема	Технології (способи рішення)	Виграш
На канальному рівні		
Збільшення пропускної здатності радіоканалів	Зсув діапазону частот (сотні Мгц, одиниці ГГц), використання оптичного діапазону	10
	Оптимізація використання радіоспектру	2…20
	Спрямовані антени	2…30
На мережевому рівні		
Маршрутизація	Нові гібридні протоколи маршрутизації	2…10
Вертикальні елементи архітектури	Безпілотні літальні апарати, супутники	2…4
Управління ресурсами мережі	Інтелектуалізація процесу управління мережами	3…5

Так наприклад в США за останні десять років втричі зросла кількість тактичних радіозасобів, їх загальна пропускна здатність збільшена на порядок (2001 рік в США – 365000 радіозасобів, 11 типів, 46 Мбіт/с; в 2011 році – 919000 радіозасобів, 20 типів, 9.6 Гбайт/с) [4].

Висновки

1. Система зв’язку тактичної ланки розвивається в напрямку застосування відкритої архітектури, впровадження новітніх телекомунікаційних технологій, які використовуються у комерційних системах зв’язку.

2. Запропонована нова архітектура мобільної компоненти систем військового зв’язку – 3-х рівнева ієрархія неоднорідних мобільних радіомереж (мобільних абонентів – мобільних базових станцій – безпілотних літальних апаратів) типу MANET.

3. Застосування запропонованої архітектури мобільної компоненти дозволить створити транспортну основу мережецентричних способів ведення бойових дій та призведе до появи принципово нових форм (способів) ведення бойових дій, змінить форми та способи управління військами, а також дозволить значно збільшити бойову ефективність військ.

4. В інституті проводяться теоретичні дослідження, які стосуються створення математичного забезпечення управління мобільною компонентою мереж зв’язку військового призначення. Отримані наукові результати можуть скласти основу побудови перспективної інтелектуальної мобільної компоненти мереж зв’язку військового призначення.

ЛІТЕРАТУРА

1. Кондратьев А.Е. Проблемные вопросы исследования новых сетецентрических концепций вооруженных сил ведущих зарубежных стран // Военная мысль, 2011, № 9. – С. 61 – 74.

2. Романюк В.А. Еволюція тактичних радіомереж: Тези доповідей та виступів учасників VI науково-практичного семінару [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”], (Київ, 20 жовтня 2011р.) / Романюк В.А. – К.: ВІТІ НТУУ „КПІ”, 2011. – С. 45 – 52.

3. Самоорганизующиеся радиосети со сверхширокополосными сигналами / [С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк]. – К.: НПП „Издательство „Наукова думка” НАН Украины”. – 444 с.: ил.

4. Tactical Radios 2011 // Compendium by Armada. – 2011. – № 4. – 32 p.

к.т.н. Харченко В.М. (ДП „НДІ РЕТ”)
к.ф.-м.н. Харченко О.В. (ІРЕ НАНУ)

КОГНІТИВНІ РАДІОСИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Відповідно до визначення, наведеному в Звіті MCE-R 2117, „Когнітивне радіо” – це радіосистема, яка використовує технології радіозв’язку з програмованими параметрами (Software Defined Radio-SDR) і інші технології для автоматичного налаштовування режиму роботи що забезпечує досягнення бажаних цілей. В рамках Євросоюзу було визначено, що когнітивні радіосистеми повинні підтримувати декілька технологій радіодоступу та мати здатність динамічного вибору вільного радіочастотного ресурсу.

Враховуючи, що правильно спроектована система завжди знаходиться в процесі модернізації що не завершується на інтервалі життєвого циклу, а також загальносвітові тенденції розвитку засобів цифрового радіозв’язку, були сформульовані основні вимоги до систем зв’язку спеціального призначення:

– широкодіапазонність;

– скритність функціонування і завадостійкість системи зв’язку, яка повинна забезпечуватися застосуванням спеціальних сигналів і методів їх обробки;

– можливість адаптації до завадової обстановці;

– можливість використання різних протоколів управління мережею (в тому числі і децентралізованого управління);

– багатофункціональність (мультимедійність);

– можливість модернізації радіостанції за рахунок впровадження на програмному рівні нових видів модуляції (наприклад, Orthogonal Frequency Division Multiplexing - OFDM або Orthogonal Code-Division Multiplexing – OCDM) і протоколів передачі інформації без зміни конструкції і схемотехнічних рішень;

– можливість роботи з радіостанціями „старого парку”;

– можливість ретрансляції та квітування коротких цифробуквених повідомлень або інформаційних пакетів;

– наявність вбудованої системи криптографічного захисту;

– наявність вбудованої навігаційної системи, що дозволяє синхронізувати мережі зв’язку та відображати розташування радіостанцій на цифровій карті;

– ергономічний інтерфейс користувача;

– високий ступінь уніфікації і модульність конструкції радіостанції та програмного забезпечення.

Очевидно, що системи радіозв’язку спеціального призначення можуть застосовуватися в різних ланках системи управління військами і експлуатуватися в різних умовах. Це робить необхідним розробку не окремо взятої радіостанції, а функціонально повного ряду засобів радіозв’язку, що забезпечує управління, як на тактичному, так і на стратегічному рівнях. Програмна і апаратна уніфікація дозволять суттєво зменшити вартість їх виготовлення і наступні експлуатаційні витрати.

1. Загальні принципи забезпечення перешкодозахищеності і скритності передачі інформації

Сучасні радіозасоби, призначені для забезпечення радіозв’язком підрозділів при веденні бойових дій і в ході антитерористичних заходів, повинні мати можливість скритої і помехозащищенной передачі інформації (мови і даних) по радіоканалах в умовах впливу комплексу негауссовских і нестаціонарних завад, а також багатопроменевого поширення радіохвиль.

Скритність передачі при заданій дальності зв’язку може бути досягнута:

– за рахунок застосування направленої передачі і просторової селекції прийнятих сигналів;

– за рахунок істотного зменшення часу випромінювання сигналів;

– за рахунок зниження спектральної щільності при використанні складних сигналів з розширеним спектром.

При роботі в повнозв’язної мережі застосування направленої передачі практично виключається, а необхідність передачі мови не дозволяє суттєво зменшити час випромінювання радіосигналів. Таким чином, застосування сигналів з розширеним спектром є найбільш доцільним.

Основними видами сигналів з розширеним спектром є широкосмугові шумоподібні сигнали (ШШС) і сигнали з псевдовипадковою перебудовою робочої частоти (ППРЧ). Слід зазначити, що сигнали з ППРЧ, на відміну від ШШС, забезпечують істотно меншу енергетичну скритність функціонування радіосистем передачі інформації, оскільки вони повинні передаватися значно вище рівня шуму. Сигнали з ППРЧ не дозволяють розділяти промені по часу приходу і, як наслідок, схильні до впливу інтерференційних перешкод. У теж час, ШШС можуть передаватися істотно нижче рівня шуму, оскільки існує можливість їх когерентного накопичення навіть в умовах багатопроменевого поширення сигналів. Дослідження показують [1 – 3], що при постановці оптимальних перешкод для кожного з даних сигналів, забезпечується рівна перешкодозахищеність, але скритність функціонування систем радіозв’язку з ШШС зменшує вірогідність подавлення радіоканалу.

Відомо, що при впливі стаціонарних гауссовских перешкод з рівномірною спектральною щільністю, перешкодостійкість прийому не залежить від форми (виду) сигналів і повністю визначається відношенням енергії сигналу до спектральної щільності шуму, а також взаємокореляційними властивостями ансамблю сигналів що використається. Однак це твердження справедливе за умови ідеальної синхронізації, що при використанні складних сигналів з великою базою є непростим завданням.

Для реальних каналів радіозв'язку характерним є наявність зосереджених за часом і по спектру завад, а також інтерференційних перешкод (завмирань), обумовлених багатопроменевістю поширення радіохвиль, що ще більше ускладнює завдання побудови ефективної системи синхронізації. Для вирішення поставленого завдання необхідно застосування процедур синхронізації інваріантних до статистичних характеристиках перешкод [4, 5].

Особливу увагу слід приділяти можливості одночасного функціонування на обмеженій території декількох незалежних (не синхронізованих) мереж радіозв’язку та підтриманню синхронізму після встановлення з’єднання. Додатковим обмеженням на побудову системи синхронізації є вимога на максимально допустимий час входження в синхронізм, який при організації роботи в мережі в напівдуплексному режимі передачі не повинен перевищувати 0,2 ... 0,3 секунди.

Для систем зв’язку з ППРЧ характерна наявність фази початкової синхронізації, яка, як правило, є досить тривалою, а для підтримки синхронізму необхідно використовувати або опорні генератори з дуже високою стабільністю, або окремий канал синхронізації, що істотно знижує перешкодозахищеність системи зв’язку. В той же час, для систем зв’язку з ШШС можлива швидка початкова синхронізація та її подальше підтримання при використанні робочих сигналів, що не мають ознак синхронізуючої послідовності.

Застосування складних сигналів забезпечує перешкодозахищеність функціонування системи зв'язку тільки у разі відсутності у імовірного супротивника апріорних відомостей про форми кодових послідовностей що використовуються і закону зміни робочої частоти. Це припускає наявність досить великого ансамблю сигналів з хорошими взаємокореляційними властивостями, розмірність якого повинна практично виключати можливість використання переборних алгоритмів їх демодуляції. Для передачі інформації необхідно мати можливість оперативної зміни алгоритму обробки прийнятих сигналів в залежності від форм кодових послідовностей що завантажуються з ансамблю, що потребує використання програмованих цифрових узгоджених фільтрів при демодуляції сигналів з великою базою.

Наявність зосереджених за часом і спектром перешкод обумовлює необхідність застосування нелінійних алгоритмів обробки сигналів або компенсації потужних перешкод. Однак, в завантаженому перешкодами діапазоні частот можливі значні енергетичні втрати і погіршення взаємокореляційних властивостей сигналів, що неминуче буде призводити до зниження перешкодостійкості прийому. Для підвищення перешкодостійкості прийому доцільно максимально розширити частотний діапазон роботи системи радіозв'язку, що забезпечить можливість адаптації до завадової обстановці. Вибір ділянки робочого діапазону найменш ураженого перешкодами може бути виконаний шляхом послідовного панорамного аналізу з подальшим вибором по заданому критерію оптимальної робочої частоти, яка може призначатися адміністратором мережі в автоматичному чи напівавтоматичному режимах.

2. Функціонально повний ряд радіостанцій спеціального призначення

Однією із обов'язкових вимог, що пред'являються до систем радіозв'язку спеціального призначення, є функціональна повнота ряду радіостанцій, що забезпечують всі необхідні види радіозв'язку. Досить повний функціональний ряд утворюють радіостанції R & S ® MR300 виробництва фірми R & S, радіостанції FalconIII виробництва фірми Harris RF Communications, радіостанції, розроблені в концерні „Созвездие" (Росія, м. Воронеж) Р-168-25УЕ, Р-168 МКМЕ, „Тайга" і Р-168-5КВЕ, а також радіостанції Р-005У, Р-030У та Р-002ПП виробництва ООО „Телекарт-Прилад" (Україна, м. Одеса). Однак вони не в повній мірі відповідають вимогам, що пред'являються до SDR-радіостанціям і, тим більш, не можуть бути віднесені до когнітивних системам радіозв'язку.

Проведений аналіз принципів побудови і складності розробки радіостанцій різного призначення дозволив запропонувати послідовність розробки і виготовлення SDR-радіостанцій, що утворюють досить повний функціональний ряд:

1. Розробка та виготовлення багатофункціональної, широкодіапазонним УКХ SDR-радіостанції з максимальною потужністю передавача 30 – 50 Вт, призначеної для установки на об'єктах бронетанкової техніки, в якій, поряд з ППРЧ та іншими сигналами, застосовуються шумоподібні сигнали з базою що перевищує 1000. Ця радіостанція є найбільш складною і може розглядатися як базова для уніфікованого ряду радіостанцій.
2. Розробка та виготовлення носимого варіанту УКХ SDR-радіостанції зі складними сигналами і максимальною потужністю передавача 4 Вт, на базі якої можуть бути розроблені „маяки" для вантажів що скидаються з літаків і пошукові пристрої (пеленгатори) для цих вантажів.
3. Розробка та виготовлення варіанту КХ-УКХ SDR-радіостанції зі складними сигналами і максимальною потужністю передавача 50 Вт (діапазон роботи 1,5 ... 108 МГц), в якій при роботі в КВ діапазоні використовуються складні сигнали з великою базою і шириною спектру сигналу 100 ... 250 кГц. Висока стійкість ШШС до частотно-селективних завмирань забезпечує значний енергетичний виграш (від 7 до 20 разів).
4. Розробка та виготовлення базової та абонентської УКХ SDR-радіостанцій зі складними сигналами для систем метеорного зв'язку, які функціонують в діапазоні 30 ... 100 МГц.
5. Розробка та виготовлення завадозахищених модемів, що забезпечують скритність передачі інформації і засновані на SDR-технологіях, для систем супутникового зв'язку, радіорелейних і тропосферних систем.

Подальша модернізація програмного забезпечення вказаних вище SDR-радіостанцій дозволить без зміни конструкції і схемотехнічних рішень побудувати на їх основі когнітивні системи радіозв'язку спеціального призначення.

3. Засоби адаптації при побудові когнітивних радіосистем спеціального призначення що використовують ШШС і мають вбудовану навігаційну систему

Наявність вбудованої навігаційної системи і електронних карт в SDR-радіостанції УКХ діапазону відкриває нові методи управління потужністю випромінювання радіохвиль і швидкістю передавання сигналів. Знаючи координати кореспондуючих пунктів не складно

визначити профіль траси, характер підстилаючої поверхні, особливості рельєфу місцевості і, використовуючи відомі моделі поширення радіохвиль [6, 7], оцінити рівень сигналу в точці прийому. В залежності від отриманого результату на низькій швидкості можуть передаватися сигнали управління параметрами радіостанції (потужністю, частотою, сигнально-кодовими конструкціями, протоколами передачі і.т.д.), що забезпечують задану якість передачі інформації. Інформація про взаємне розташування радіостанцій і рельєф місцевості дозволяють вибрати найбільш раціональний маршрут доведення інформації при ретрансляції повідомлення. Використання ШШС для передачі інформації в КВ діапазоні дозволяє виконати розділення і оптимальну обробку багатопроменевих сигналів на заданій частоті, а також оцінити імпульсну перехідну характеристику КВ радіоканалу і вибрати робочу частоту найменш схильну до впливу інтерференційних завмирань.

Алгоритми адаптації при організації метеорних радіоканалів слід розглянути окремо.

4. Система метеорного радіозв'язку як елемент функціонально повної системи зв'язку спеціального призначення

Метеорний зв’язок в Україні недостатньо вивчений і не знайшов належного практичного застосування. У теж час, не дивлячись на уривчастість і відносно невелику середню пропускну здатність (до декількох кілобит на секунду), метеорний зв’язок має цілий ряд переваг, що вигідно відрізняють його від інших традиційних видів зв’язку:

– значна дальність дії радіоканалу (до 2000 км) і відсутність так званих „мертвих зон”, що дозволяє охоплювати великі території і ставить метеорний зв’язок в один ряд з іншими видами „загоризонтного” зв’язку.

– відносно малі розміри метеорного сліду і геометрія поширення радіохвиль забезпечують прийом сигналу від конкретного метеора в обмеженій зоні, що дозволяє, з одного боку, одночасно обслуговувати велику кількість кореспондентів на одній робочій частоті, з іншого – дає перевагу системам метеорної зв’язку з електромагнітної сумісності, скритності функціонування і завадостійкості.

– відносно малі енергетичні витрати при передачі сигналів по метеорному каналу, що обумовлені низьким рівнем шумів і малим поглинанням в іоносфері, забезпечують малі габаритні розміри і низьке енергоспоживання апаратури зв’язку.

– стійкість до природних і штучних іоносферних збурень дозволяє працювати в північних широтах. Дана властивість представляє особливий інтерес в надзвичайних і критичних ситуаціях, коли метеорні системи можуть виявитися єдиними, здатними в короткий термін забезпечити зв’язок з експедиціями в Арктиці й Антарктиці.

В даний час у багатьох розвинених країнах, таких як США, Канада, Норвегія, Японія та ін. розробляються, удосконалюються і застосовуються системи зв’язку через метеорний радіоканал. Метеорний радіозв’язок використовується у важкодоступних та віддалених районах, на флоті, в системах автоматичного дистанційного збору даних в інтересах гідрометеорологічних служб, в системах попередження надзвичайних ситуацій і стихійних лих, для диспетчеризації транспортних засобів та збору інформації про їх місцезнаходження, для забезпечення високоточної синхронізації рознесених у просторі еталонів часу і частоти.

Використанню метеорної радіозв’язку приділяють увагу військові, дипломатичні та спеціальні відомства, оскільки метеорний радіоканал забезпечує скритність передачі інформації і його дуже складно запеленгувати і подавити.

Системи метеорної зв’язку широко використовуються в інтересах міністерства оборони США і в НАТО. Система метеорної зв’язку ВПС США, що призначена для підвищення стійкості роботи наземних засобів управління і забезпечення безперервності управління в період нанесення противником ядерного удару і після нього, розглядається в даний час як основний засіб управління стратегічними силами. В інтересах Об’єднаної системи аерокосмічної оборони США і Канади (North American Aerospace Defense Command, NORAD), для управління силами ППО розгорнуті дві системи метеорної радіозв’язку, розташовані на Алясці і в штаті Вашингтон. Подальший розвиток метеорної зв’язку ВПС

США спрямоване на інтеграцію цих систем в єдину систему метеорної зв'язку, яка охопить всі основні оперативні центри.

Дослідження, засновані на використанні радіофізичного моделі метеорного сліду [8], показують, що застосування ШШС з шириною спектру що перевищує 10 МГц дозволяє ефективно протистояти частотно-селективним завмиранням сигналів і, за рахунок цього, підвищити пропускну здатність метеорного радіоканалу. Одночасно збільшується скритність функціонування радіосистеми, оскільки потужність некогерентної компоненти розсіяного сигналу в будь-якій точці спостереження буде знаходитися значно нижче рівня шуму.

Застосування ШШС і антен з малим рівнем бічних пелюстків дозволяють значно спростити заходи щодо забезпечення електромагнітної сумісності з радіозасобами окіл базової станції.

Основними характеристиками метеорного радіоканалу, що визначають його пропускну здатність, є характер зміни потужності сигналу в точці прийому і час, протягом якого забезпечується задана якість передачі інформації. Оскільки дані характеристики є випадковими, залежними від маси і швидкості метеороида, а також від розташування метеорного сліду, очевидно, що вибір швидкості і протоколу передачі інформації повинні бути адаптивними. Є підстави вважати [8], що, із спостереження розсіяного сигналу на початковому інтервалі, можна для кожного випадково метеорного радіоканалу що виникає запропонувати сигнально-кодову конструкцію і протокол передачі які дозволяють наблизитися до реальної пропускної здатності. Слід зазначити що розробка таких алгоритмів адаптації знаходиться в початковій стадії і може бути об'єктом наукових досліджень.

ЛІТЕРАТУРА

1. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью.//В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, Н.П. Мухин, Г.С. Нахмансон; Под ред. В.И. Борисова.– М.: Радио и связь, 2003. – 640 с.

2. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты.//В.И. Борисов, В.М. Зинчук, А.Е. Лимарев, Н.П. Мухин, В.И. Шестопалов; Под ред. В.И. Борисова.– М.: Радио и связь, 2000. – 384с.

3. Системы широкополосного радиодоступа 4 поколения: выбор сигнально-кодовых конструкций./ В.И. Николаев, А.В. Гармонов, Ю.И Лебедев // Первая миля. – 2010 .– №5/6. – с.56 – 59.

4. Харченко В.Н. Метод построения системы синхронизации сложных составных сигналов / Харченко В.Н., Лаврут А.А., Лаврут Т.В. // Радиоэлектронные и компьютерные системы. – 2006. - №5 (17). – С. 193 – 197.

5. H.V. Kharchenko. Two-Criterial DSSS Synchronization Method Efficiency Research / H.V. Kharchenko, I.O.Tkalich, Y.I.Vdovychenko // Proceedings of 7-th IEEE East-West Design and Test Symposium (EWDTS'09). - Kharkov-Moscow: KNURE, 2009.– p.165 – 174.

6. Метод прогнозирования распространения сигнала на конкретной трассе для наземных служб „из пункта в зону" в диапазонах УВЧ и ОВЧ. Рекомендация МСЭ – R Р.1812-1.

7. Распространение радиоволн за счет дифракции. Рекомендация МСЭ-R Р.526 – 9.

8. Харченко Е.В. Рассеяние радиосигнала на метеорном следе. Вісник Харківського національного університету імені В. Н. Каразіна. Серія "Радіофізика та електроніка". №966, випуск 18, 2011. с. 90 – 96.

д.т.н. Бараннік В.В. (ХУ ПС ім. Івана Кожедуба)
к.т.н. Гуржій П.М. (ВІТІ НТУУ „КПІ”)
Додух А.Н. (ХУ ПС ім. Івана Кожедуба)
Школьник А.Ю. (НАУ)

МЕТОД КОДУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ КООРДИНАТНО-СТРУКТУРНОГО ТА ПОРЯДКОВО-МАСШТАБНОГО ПОДАННЯ ФРАГМЕНТА ЗОБРАЖЕННЯ

Основними ключовими механізмами, які визначають методологію процесів стиску та відновлення зображень є [1 – 3]:

1. Види надмірності, які скорочуються. Методологія усунення надмірності зображень визначає клас трансформацій, що використовуються, та методів кодування, надаючи таким чином вплив на потенціальні можливості щодо ступеня компактного представлення, часу обробки і рівня внесених спотворень. Для запропонованого підходу методологія скорочення надмірності базується на формуванні для фрагмента зображення двох складових, а саме:

– нерівномірна координатно-структурна складова, яка формує локально-структурну архітектуру фрагмента зображення. Компонентами такої складової є довжини апертур, що виявляються уздовж рядків зображення;

– порядково-масштабна складова, яка визначає яскравість і колірну насиченість архітектурної форми фрагмента зображення. Компонентами такої форми є апроксимуючі яскраві (колірні) величини апертур.

Створюються потенційні можливості для усунення: статистичної надмірності; психовізуальної надмірності; структурної надмірності.

2. Наявність попереднього перетворення колірної моделі.

3. Типи і параметри кодерів, що використовуються для скорочення надмірності.

4. Наявність можливості для додаткового зниження часу обробки і передачі даних для фіксованого обсягу компактно поданих відеоданих.

У процесі побудови методу кодування пропонується організовувати такі підходи:

1. Формувати кодовий опис заданої довжини, кодовим словом буде машинне слово одномірної довжини, приймаючи значення від 16 до 64 біт у залежності від системи.

2. Формувати двокомпонентне кодове подання на базі спільного використання елементів координатно-структурного і порядково-масштабного представлення фрагмента зображення. Це забезпечить обробку цілісної інформації про фрагмент зображення.

Формування кодової комбінації пропонується здійснювати на основі двокомпонентного інтегрованого принципу. У цьому випадку, на відміну від біт-орієнтованого принципу, додаткова група розрядів формується на основі зваженого додавання компоненти апертурно-яскравого опису фрагмента зображення. Це дозволяє:

– додатково підвищити ступінь стиснення за рахунок скорочення кількості незначущих старших розрядів у кодових комбінаціях;

– підвищити оперативність обробки фрагментів зображень,;

– знизити обчислювальну складність, що необхідна для реалізації процесів обробки, а саме: скоротити кількість звернень до зовнішнього запам’ятовуючого пристрою; скоротити обсяг пам’яті, що відводиться для зберігання проміжних даних.

ЛІТЕРАТУРА

1. Лабутіна І.А. Дешифрування аерокосмічних знімків: Навчальний посібник. – М: Аспект-Пресс, 2004. – 184 с.

2. Бараннік В.В. Методологічний аналіз системи аерокосмічного відеомоніторингу надзвичайних ситуацій / В.В. Бараннік, А.В. Яковенко, А.Ю. Школьник // Сучасна Спеціальна техніка, К.: № 4 (27). – 2011. – С. 12 – 22.

д.т.н. Бараннік В.В. (ХУ ПС ім. Івана Кожедуба)
к.т.н. Гуржій П.М. (ВІТІ НТУУ „КПІ”)
Краснорyцкий А.О. (ХНУРЭ)
Рогоза І.Є. (НАУ)

ДЕКОМПРЕСОВАНЕ ПОДАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ РЕКОНСТРУКЦІЇ БІНАРНОЇ СТРУКТУРИ ТРАНСФОРМАНТ

Розробляється метод декомпресованого подання зображень на основі реконструкції бінарної структури трансформант. Для реконструкції сегментованих зображень з контрольованою похибкою враховуються як базові технологічні процеси (трансформація сегментів на основі двовимірного дискретно-косинусного перетворення, використання кольорорізницевої моделі для опису зображень), так і відмінні особливості технології кодування бінарних трансформант [1 – 5].

Розглядаються етапи формування концептуальних складових методу реконструкції стислих зображень:

– перша складова виражається в необхідності виділення із загального кодового потоку тієї його частині, яка відповідає відновлювальному сегменту;

– пропонується проводити відновлення трансформанти на основі послідовного виділення кодового значення розширеного позиційно структурне вагове число (ПСВ), і подальшій його реконструкції. А саме, відновлення значення елементу ПСВ числа організовується на основі оператора, який задає позиційне структурно-вагове декодування за реверсною технологією, що забезпечує здобуття елементів розширеного ПСВ числа без втрати інформації на основі підстав раніше отриманих елементів ПСВ числа. Така властивість дозволяє проводити реконструкцію елементів ПСВ чисел в умовах, коли їх довжина заздалегідь невідома;

– переведення трансформанти з бітового опису в компонентний, організовується на основі третьої концептуальної складової;

– здобуття зображень досягається на основі виконання зворотних трансформаційних процесів і збірки окремих сегментів (десегментації). Дані процедури реалізується на основі четвертої концептуальної складової.

Це створює умови для зниження бітової швидкості стислого представлення сегменту зображення на основі додаткового скорочення структурної надмірності без використання службових даних.

ЛІТЕРАТУРА

1. Gonzalez, Rafael C; Woods, Richard E. Digital Image Processing, 2nd ed. – published by Pearson Education, Inc. publishing as Prentice Hall., 2002. – 793 p.

2. Ватолин В.И., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с.

3. Бараннік В.В. Методологічний аналіз системи аерокосмічного відеомоніторингу надзвичайних ситуацій / В.В. Бараннік, А.В. Яковенко, А.Ю. Школьник // Сучасна Спеціальна техніка, К.: № 4 (27). – 2011. – С. 12 – 22.

4. Аудиовизуальные системы связи и вещания: новые технологии третьего тысячелетия, задачи и проблемы внедрения в Украине / [О.В. Гофайзен, А.И. Ляхов, Н.К. Михалов и др.] // Праці УНДІРТ. – 2000. – № 3. – С. 3 – 40.

5. Баранник В.В. Метод сжатия изображений на основе неравновесного позиционного кодирования битовых плоскостей /В.В. Баранник, Н.К. Гулак, Н.А. Королева //Радіоелектронні і комп’ютерні системи. – Х.: ХНАУ „ХАІ”, 2009. – Вип. 1. – С. 55 – 61.

д.т.н. Бараннік В.В. (ХУПС)
Сафронов Р.В. (ХУПС)

МЕТОД РЕКОНСТРУКЦІЇ ЗОБРАЖЕНЬ В НЕРІВНОМІРНОМУ БАЗИСІ СПЕКТРАЛЬНИХ КОЕФІЦІЄНТІВ

При обробці та доставлені відео трафіка в сучасних телекомунікаційних системах невід'ємними етапами обробки відеоданих являються стиснення відео, передачі відеопотоку и відновлення його на приймальній стороні.

Для організації відновлення потоку відеоданих широко застосовуються методи декомпресії, що базуються на реконструкції зображень з подальшим декодуванням компонент трансформант статистичними декодерами.

Методи, що використовуються для відновлення відеоданих недостатньо ефективні при обробці зображень та не задовольняють вимогам, що висуваються до них щодо часу обробки та якості відновлення відеоданих.

Значить, вдосконалення технологій та методів відновлення трансформованих зображень з метою зниження часу обробки та підвищення якості реконструкції є актуальною науково-прикладною задачею.

Пропонується метод реконструкції трансформованих сегментів зображень в нерівномірному базисі спектральних коефіцієнтів (НБСК).

Показано, що для усунення суттєвих недоліків, що притаманні статистичним декодерам, необхідно вдосконалювати технології та методи реконструкції трансформованих зображень.

Метою досліджень є розробка методу реконструкції зображень в НБСК, який дозволяє проводити відновлення сегментованих зображень у відповідності із заданими показниками часу відновлення та якості реконструкції зображень.

Розглянутий метод реконструкції зображень усуває основні недоліки, що притаманні процесу відновлення відеоданих, що реалізовані за допомогою статистичних декодерів:

– виключено використання маркерів, а саме для розділення службової та інформаційної частин кодової конструкції;

– помилки, що внесені під в результаті завад в каналі зв'язку, при відновленні зображення не мають руйнівних наслідків для усього сегменту зображення. Це обумовлено тим, що помилки розповсюджуються тільки в межах одного коду одномірного числа в нерівномірному базисі спектральних коефіцієнтів.

Тому їх вплив розповсюджується лише на один стовбець трансформанти;

– елементи трансформанти декодуються незалежно друг від друга. В цьому випадку вдається забезпечити паралельну обробку даних.

– Для відновлення елементів сегментів відеоданих використовується система основаній, що виступає у якості службової інформації. Зникає необхідність використання кодових таблиць та організації пошуку по ним.

– Запропонована технологія дозволяє скоротити час обробки відеоданих та знизити об'єм оперативних пристроїв пам'яті.

При дослідженні інформаційних характеристик трансформант дискретного косинусного перетворення, виявлені кращі показники по часу обробки відносно існуючих технологій (від 1,5 разів та більше).

Бачинський В.Й. (ВІТІ НТУУ „КПІ”)
к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)
Вакуленко О.В. (ВІТІ НТУУ „КПІ”)

ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Відповідно до Концепції розвитку зв’язку України до 2015 року, з урахуванням економічного стану держави, необхідності вирішення проблеми забезпечення населення соціально значущими послугами, якості і надійності сучасних мереж телекомунікацій, і, з огляду на потребу входження України в світовий інформаційний простір рівноправним партнером, пріоритетними напрямами подальшого розвитку телекомунікаційних мереж є: реконструкція (цифровізація) телефонних мереж загального користування і подальше нарощування телефонної ємності, враховуючи реальний платоспроможний попит; подальша розбудова сучасної транспортної телекомунікаційної мережі, яка б забезпечила потреби створення в Україні інформаційного середовища; прискорення розвитку мереж телекомунікацій усіх видів;впровадження нових і новітніх технологій.

Технічне переоснащення мереж, їх цифровізація із застосуванням сучасних інтелектуальних технологій, з одного боку, вимагають створення іншої системи управління, а з іншого боку, дають змогу створити автоматизовану систему управління телекомунікаціями на новому технологічному рівні, завдяки чому можна ефективніше використовувати ресурси мереж телекомунікацій, зменшити експлуатаційні витрати, зокрема зменшенням кількості персоналу, поліпшити якість надання послуг і розширити їх номенклатуру, підвищити надійність мереж. Велике значення у цьому процесі належить правильному вибору моделі системи управління та оцінки її ефективності.

Система управління мережами телекомунікацій забезпечує планування, введення в дію мереж і послуг телекомунікацій, а також функціональну підтримку систем технічної експлуатації мереж і послуг. На сьогодні питаннями стандартизації управління телекомунікаційними мережами займаються кілька міжнародних організацій. Найбільш важливими моделями управління цих організацій є такі:

модель Міжнародного союзу електрозв’язку з питань телекомунікацій (ITU-T), ґрунтується на концепції TMN;

модель Форуму управління телекомунікаціями (Tele Management Forum, TM Forum), на базі концепції SmartTMN;

модель IETF, в основу якої покладено стандартні базові засоби мережного управління (Network Management Framework) мережі Інтернет;

модель мережного управління ATM-форуму (на базі моделі IETF з використанням елементів TMN);

модель управління фірми IBM;

моделі із застосуванням технологій управління TINA та CORBA.

Однозначної відповіді на запитання, яка технологія є найкращою і на яку орієнтуватись у найближчому майбутньому, дати не можна. Єдине, що можна сказати: реалізація управління мережами телекомунікацій можлива за допомогою кожної із цих технологій і майже однаково ефективна. Усі вони застосовують перспективний компонентний підхід, усі використовують схожий механізм віддаленого виклику процедур і роботи з віддаленими об’єктами, усі мають переваги і недоліки, більшість із них орієнтуються на широко розповсюджений протокол TCP.

Отже, вирішальні аргументи на користь певної технології – найкраща динаміка її поширення, розвитку програмного забезпечення, найдешевші засоби підтримання розробки технології. Адекватно оцінити переваги або недоліки певної моделі управління дозволяє метод експертних оцінок.

к.т.н. Бердников О.М. (ІСЗЗІ НТУУ „КПІ”)

СКЛАДНОСТІ ВПРОВАДЖЕННЯ МЕРЕЖ *LR-PON* ТА МЕТОДИ ЇХ ВИРІШЕННЯ

На сучасному етапі розвитку пасивні оптичні мережі (*Passive Optical Network – PON*) зарекомендували себе багатообіцяючою технологією розвитку мереж абонентського доступу. Поряд з чисельними перевагами *PON*, значним недоліком є фіксований та досить низький енергетичний бюджет (≈ 26 дБ), який встановлює жорстке обмеження на протяжність мережі (до 20 км) та її здатність до розгалуження (до 128 абонентів). На практиці дані параметри стають ще меншими, через наявність в мережі багаторазових розгалужень та з’єднувачів. В зв’язку з цим існує необхідність збільшення енергетики мережі шляхом використання підсилювачів – так званий перехід до пасивних оптичних мереж великої протяжності мереж (*Long Reach PON – LR-PON*).

Впровадження мереж *LR-PON* не тільки усуне вищевказані недоліки мереж *PON*, але й зробить значний крок в сторону конвергенції міських мереж та мереж доступу в один сегмент, дозволивши при цьому зменшити кількість мережевих технологій та інтерфейсів, що використовувались для їхньої взаємодії. Предметом дослідження даної доповіді є складності у впровадженні *LR-PON* та методи їх подолання.

Варто зауважити, що використання підсилювачів у *PON* потребує підведення гарантованого живлення до проміжних вузлів, що суперечить основній концепції *PON*, яка передбачає повну пасивність на усій ділянці від центрального офісу до кінцевого обладнання. Проте в силу того, що вузли підсилення дозволять об’єднати декілька сегментів мережі в один, та в подальшій перспективі будуть розміщуватись у місцевих центральних офісах, даний відхід від концепції є оправданим.

Використання підсилювачів у мережах *PON* зумовлює ряд складностей, які накладають обмеження на вибір оптичних підсилювачів, та потребують вирішення за допомогою додаткових схем. Найбільш суттєвими складностями є наявність підсиленого спонтанного випромінення (*Amplifier Spontaneous Emission – ASE*) та пульсуюча природа трафіку від абонентів до центрального офісу. Тоді як проблема наявності *ASE* вирішується застосуванням дворівневих схем проміжного підсилення, аналогічних до схем підсилення в магістральних мережах, для подолання складностей, які накладає пульсуюча природа висхідного трафіку, потрібні нові підходи та методи підсилення.

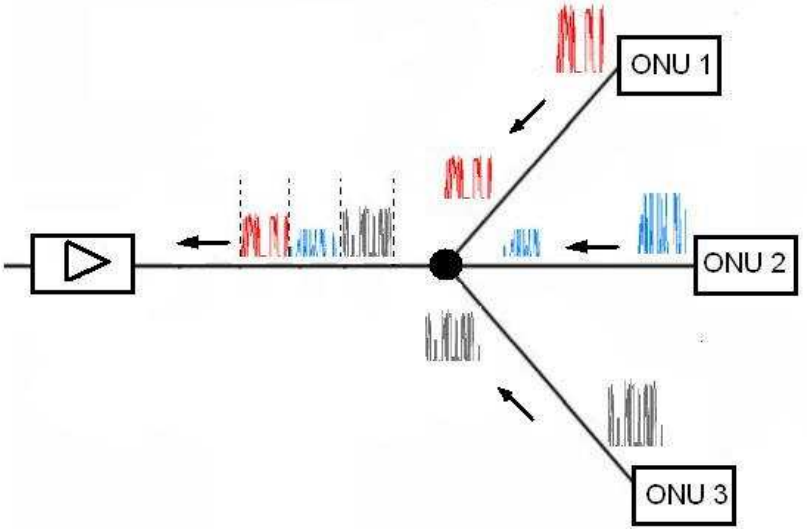


Рис. 1. Пояснення, щодо пульсуючої природи висхідного трафіку в мережах *PON*

Тоді як в напрямку від центрального офісу до абонентів трафік на вході підсилювача є рівномірним, у зворотньому напрямку виникає пульсуючий трафік, при підсиленні якого виникають складності. Даний вид трафіку є нетиповим явищем для магістральних та міських мереж, а також абонентських мереж в їх привичному розумінні. Пульсація потужності

висхідного сигналу є побічним продуктом логічної топології *PON* „точка-багатоточка”, та відсутності логічної обробки сигналу *PON* у проміжних вузлах. Внаслідок різної віддаленості абонентів від центрального офісу, кожен із сигналів зазнає різного рівня ослаблення на розподільчій ділянці мережі, тому у груповому *TDMA* сигналі спостерігаються скачки потужності при переході з сигналу одного абонента на сигнал іншого (рис. 1).

У зв’язку з цим, важливо, щоб підсилювачі володіли швидкою перенастройкою рівня підсилення.

Підсилювачі з повільною перенастройкою рівня підсилення спотворять висхідний трафік, що призведе до значного збільшення *BER* в оптичному лінійному тракті. Тому використання широкопоширених та відносно дешевих підсилювачів на основі волокна легированого ербієм (*Erbium Doped Fiber Amplifier – EDFA*) у напрямку від абонентів до центрального офісу ускладнене, в силу їх інерційності. Одним із можливих виходів з даної ситуації є використання разом з підсилювачами на активному волокні додаткових контрольних схем та стабілізуючих сигналів по виділених волокнах (рис. 2).

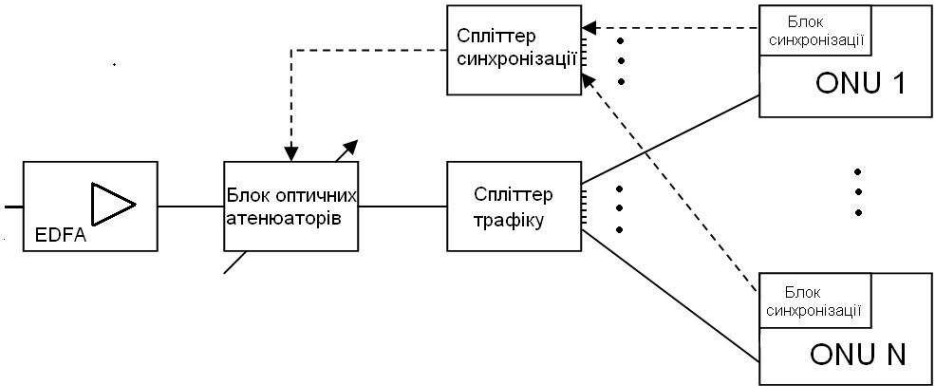


Рис. 2. Схема вирівнювання пульсацій трафіку групового сигналу

Даний метод вирівнювання пульсацій трафіку значно ускладнює схему, його впровадження потребує використання додаткових спілтерів та оптичних волокон.

Альтернативним та більш доцільним підходом є використання в якості підсилювачів *PON* напівпровідникових оптичних підсилювачів (*Semiconductor Optical Amplifier – SOA*). Напівпровідникові оптичні підсилювачі є найбільш привабливим варіантом збільшення протяжності мереж *PON*. Вони забезпечуть високий коефіцієнт підсилення, низький шум, низькі поляризаційні втрати та швидку динаміку зміни рівня підсилення, що задовольняє вимоги до проміжного підсилення.

Іншими перевагами використання *SOA* відносно інших волоконних підсилювачів є їх малий розмір, висока надійність і низьке споживання енергії.

Проте недоліком *SOA* є залежність рівня підсилення від температури. Це породжує потребу в використанні наряду з *SOA* термостабілізуючого обладнання, особливо у вуличних умовах їх розміщення.

ЛІТЕРАТУРА

1. Byoung-Whi Kim, Huan Song, Biswanath MukherjeeLong-Reach. „Optical Access Networks: A Survey of Research Challenges, Demonstrations, and Bandwidth Assignment Mechanisms”, IEEE Communication Surveys & Tutorials, vol. 12, 2010 (ст. 178…190).

2. Huan Song. „Long-Reach Passive Optical Networks”, дисертація, University of California, 2009.

3. Russell P. Davey, Daniel B. Grossman. „Long-Reach Passive Optical Networks”, Journal of Lightwave Technology, vol. 27 № 3., 2009 (ст. 273...280).

Березань Ю.В. (в/ч А1906)
Жуков Є.В. (в/ч А1906)

ОЦІНКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНО-ПОШУКОВИХ СИСТЕМ ІНТЕРНЕТУ

Для вирішення завдань пошуку інформації за відповідними тематиками в мережі інтернет необхідно використовувати відомі інформаційно-пошукові системи(ІПС).

Однак найбільш відомі ІПС мають не однакові різні показники релевантності щодо відповідності пошукового запиту користувача.

Для оцінки ефективності функціонування інформаційно-пошукових систем пропонується використати концепцію на основі релевантності й глибини пошуку для перших 10 сторінок, які видає інформаційно-пошукова система (ІПС).

Релевантність визначалося як відношення знайдених релевантних документів до десяти перших розглянутих результатів. Тестові варіанти містили запити, релевантність яких не можна було визначити без участі користувача: по ступеню відповідності інформації з документа й реальної інформаційної потреби користувача; по ступеню близькості предмета (тематики) інформаційної потреби й знайденого документа; по ступеню корисності інформаційного ресурсу для завдання, розв'язуваного користувачем, з погляду тимчасових витрат, способу взаємодії користувача із системою й т.п. .

Під глибиною користувальницького пошуку розуміється сума двох величин $\boldsymbol{D = m + c}$, де $\boldsymbol{m}$ – відстань від першого результату до релевантного, а $\boldsymbol{c}$ – кількість кликів „мишею", що знадобилися для виходу на релевантну сторінку. Максимально кращий результат $D = 1$ досягається при $m = 1$ (релевантний документ перебуває на першому місці в списку) і $c = 0$ (користувач одержує необхідну інформацію із фрагмента тексту). Під кликами розумілися саме переходи зі сторінки на сторінку за допомогою кликів миші; використання скролера або клавіш „page up" „page down" не враховувалося.

Кожна ІПС оцінювалася по сумі величин D для перших десяти результатів. Якщо релевантні документи не були знайдені в перших десяти результатах, то дана ІПС одержувала максимальну кількість балів – $D = (m = 10) + (c = 10) = 20$, що було найгіршим результатом, оскільки оцінка проводилася по регресивній шкалі. Для знаходження релевантного документа робилося не більше 10 кликів. Якщо після 10 кликів релевантний документ не був знайдений, системі приписувалася максимальна кількість балів. Оскільки на сторінці могло бути досить багато (до декількох десятків) посилань на інші сторінки, були сформульовані наступні правила переходу по посиланнях. Першим відкривалося посилання, у якому зустрічалися всі знаменні слова запиту + термін, що відображає умови релевантності.

Також пріоритетом користувалися посилання, у яких використовувалася більша кількість ключових слів запиту.

Якщо ключові слова запиту не використовувалися в посиланнях, то вони відкривалися послідовно, до 10 кликів. Якщо при переході по посиланнях відкривалася сторінка іншої пошукової системи й потрібно було вказувати ключовий термін для подальшого пошуку, то це розглядалося як негативний результат .

Дані запити можна розділити на запити, що припускають однозначну інтерпретацію релевантності, і запити, що припускають багатозначне трактування релевантності. При визначенні релевантності документів, знайдених по таких запитах, релевантними вважалися документи, що містять будь-який опис зазначених у запиті об'єктів.

Білан А.М. (НЦЗІ ВІТІ НТУУ „КПІ”)
Мальцева І.Р. (НЦЗІ ВІТІ НТУУ „КПІ”)

АНАЛІЗ СУЧАСНИХ ЗАГАЛЬНОСВІТОВИХ ТЕНДЕНЦІЙ ПОБУДОВИ ТА РОЗВИТКУ СИСТЕМ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НАЙБІЛЬШ ТЕХНІЧНО РОЗВИНУТИХ КРАЇН СВІТУ

Проблема забезпечення кібербезпеки дедалі частіше стає предметом широкої дискусії як на національному, так і міжнародному рівнях. На сьогоднішній день більшість потужних держав світу (США, Росія, Китай, Індія та інші) знаходяться в процесі трансформації власних військових потенціалів з огляду на можливості використання мережі Інтернет [1].

Спецпідрозділи більше 20 країн світу, мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і „обвал” структур супротивника. Згідно з офіційними заявами, такі підрозділи створено в США (U.S. Cyber Command), Великобританії (Cyber Security Operations Centre при уряді Великобританії), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence).

Про рівень занепокоєності провідних держав світу у сфері кібербезпеки свідчить і бажання врегулювати на міжнародному рівні можливість визнання кібератаки „актом війни”.

На сьогоднішній день найбільш потужними та активними вважають військові кіберпідрозділи КНР та США. За даними ФБР, КНР на сьогоднішній день має армію у 180000 хакерів, які займаються щоденними атаками на кібермережі США. З 180 тис. хакерів 30 тис. є військовими, а 150 тис. – комп’ютерними експертами з приватного сектору.

Не менш активною політикою в сфері кібербезпеки є у США:

збільшено держзамовлення на розробку нових засобів ведення війни і зокрема – кіберозброєнь та нових, більш захищених, військових мереж;

створено проекти нормативних документів, що спрямовані на покращення взаємодії в сфері кібербезпеки союзниками США та убезпечення власного Інтернет простору в разі виникнення ситуацій, що загрожують національній безпеці.

Великобританія (потенціал якої в сфері кіберзахисту вважається одним з найпотужніших) все ще розбудовує власні сили безпеки у кіберпросторі. Великобританія у 2010 році запустила у повноцінному режимі роботу Оперативного центру з кібербезпеки (20 співробітників) з метою координації вже існуючих різноманітних центрів із кібербезпеки різних відомств та створення майданчику для співпраці між урядом та приватним сектором із проблем кібербезпеки. Крім того у Великобританії ефективно працює Командування урядових комунікацій (Government Communications Headquarters), що забезпечує як захист критично важливої урядової інформації, так і отримання розвідувальних даних за допомогою новітніх комунікативних засобів.

Згідно з відкритими даними, активно створюються відповідні підрозділи у Південній та Північній Кореї, Російській Федерації, Франції.

Політика країн Заходу в сфері внутрішнього інформаційного (кіберпростору) все частіше набуває окремих рис політики тих країн, що традиційно відносять до авторитарних, хоча і з певними суттєвими відмінностями [2].

ЛІТЕРАТУРА

1. Лопатин В.Н., Информационная безопасность России: Человек. Общество. Государство. – Санкт-Петербург: Фонд „Университет”, 2010.

2. Хозиков В., Информационное оружие. – СПб: Издательский дом „Нева”, М: Издательство „ОЛМА-ПРЕСС”, 2003. – 480 с.

Біленький А.В. (НЦЗІ ВІТІ НТУУ „КПІ”)
Живило Є.О. (НЦЗІ ВІТІ НТУУ „КПІ”)
Білан А.М. (НЦЗІ ВІТІ НТУУ „КПІ”)
Мальцева І.Р. (НЦЗІ ВІТІ НТУУ „КПІ”)

АНАЛІЗ ДІЯЛЬНОСТІ ВІЙСЬКОВИХ ТА ПРАВООХОРОННИХ ОРГАНІВ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ УКРАЇНИ

В Україні в системі забезпечення кібербезпеки держави задіяно низу військових та правоохоронних органів:

1. Міністерство оборони України (МО) (та його спеціальні підрозділи – зокрема Головне управління розвідки);
2. Службу безпеки України;
3. Державну службу спеціального зв’язку та захисту інформації;
4. Міністерство внутрішніх справ України (МВС);
5. Службу зовнішньої розвідки.

Водночас, діяльність цих відомств не завжди відповідним чином забезпечується. Так в системі Міністерства оборони України існують спеціальні підрозділи на які покладено задачі із забезпечення кібербезпеки військових інформаційних ресурсів та мереж. В цій діяльності, зокрема, задіяні підрозділи Військової розвідки (Головне управління розвідки МО України) та підрозділи радіоелектронної боротьби. Водночас, матеріально-технічне та, частково, кадрове забезпечення даних служб залишається на незадовільному рівні, а значна частина матеріально-технічної бази практично не оновлювалась протягом тривало часу. Крім зазначеного, ситуація у вітчизняній кібербезпековій сфері характеризується наявністю кількох суттєвих проблем [1].

По - перше, в Україні відсутні системні нормативні документи, що описували б саме загрози Україні у кіберпросторі, давали їх визначення та формували цілісну державну політику із кібербезпеки. „Стратегія національної безпеки України” (від 12лютого 2007 року) зазначає, що Україна має „розробляти та впроваджувати національні стандарти та технічні регламенти застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність”, однак по-перше, сама „Конвенція про кіберзлочинність” (ратифікована українським парламентом ще в 2005 році), хоч і стосується проблеми убезпечення кіберпростору, однак більш зосереджена на протидії карним діям (шахрайство, підробка, поширення дитячої порнографії, порушення авторських прав тощо) із використанням комп’ютерної техніки та різноманітних мереж, а по-друге – в самій Конвенції відсутнє визначення терміну „кіберзлочинність”.Більше уваги кібербезпеці та питанням, пов’язаним з нею, приділено у „Доктрині інформаційної безпеки України”. Водночас, Доктрина передбачає здійснення цілої низки заходів у воєнній сфері у зв’язку із необхідністю посилення інформаційної безпеки держави, однак до останнього часу відсутні будь-які офіційні заяви про їх впровадження на практиці.

Це призводить до того, що навіть спеціальні підрозділи силових відомств, у назві яких вживається поняття „кіберзлочинність”, „кібербезпека”, не забезпечені відповідними нормативними документами для визначення предмету своєї роботи.

По-друге, в Україні відсутні загальнонаціональні міжвідомчі координаційні структури, що могли б узгоджувати та координувати діяльність різних силових відомств під час здійснення як розслідування злочинів у кіберпросторі так і створенні ефективної системи захисту вітчизняного кіберпростору (в тому числі – у військовій сфері). На сьогоднішній день можна спостерігати ситуації, коли деякі правоохоронні органи не бажають співробітничати з МО України з проблем кібербезпеки через законодавчу (нормативну)

невизначеність прав та обов'язків даних структур чи невідповідність даних нормативних документів вимогам часу.

По-третє, більшість представників відомств, що задіяні в системі забезпечення кібербезпеки України, відмічають незадовільне кадрове забезпечення відомств відповідними фахівцями у сфері інформаційної безпеки.

По-четверте, не завжди прозорим є розподіл обов'язків спеціальних державних інституцій щодо убезпечення кіберпростору держави. Дана проблема є продовженням невизначеності нормативного поля і зокрема – відсутністю стратегічних документів, в яких би подібне розділення обов'язків (можливо із визначенням відповідального відомства) було зроблено.

По-п'яте, незважаючи на зусилля спеціальних відомств, на думку деяких фахівців, Україна все ще залишається уразливою (особливо її телекомунікаційна складова), не в останню чергу через надмірно широке впровадження західних програмних продуктів (зокрема фірми Microsoft) та використання матеріально-технічної бази іноземного виробництва. Актуальною залишається проблема створення національної операційної системи (принаймні для використання в системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом є і суттєві зауваження з боку ключових вітчизняних безпекових організацій).

Проведений аналіз тенденцій у політиці провідних держав щодо протидії загрозам в кіберпросторі та зміні внутрішньої інформаційної політики цих держав, зважаючи на посилення кібербезпекової компоненти, дозволив зробити наступні висновки:

1. Більшість держав світу активно модернізує власні сектори безпеки у відповідності до викликів сучасності, і особливо – зважаючи на потенціал використання мережі Інтернет у військових цілях.

2. З огляду на заяви високопосадовців Сполучені Штати Америки (США) та експертів, що задіяні в підготовці нової „Стратегічної концепції Організація Північноатлантичного договору (НАТО)" щодо необхідності розглядати кібернапади на критично-важливу інфраструктуру як „акт війни", що підпадають під статтю 5 Північноатлантичного договору, варто очікувати посилення дискусії на найвищому міжнародному політичному рівні ОБСЄ, керівних органів НАТО, Генеральної Асамблеї та Ради безпеки ООН, Самітів Великої вісімки, щодо можливості закріплення відповідних змін в міжнародно-правових актах та статутних документах провідних міжнародних безпекових організацій, що дозволять ідентифікувати кібернапади або їх сукупність як акти війни.

3. Тенденція посилення контролю з боку правоохоронних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі тощо свідчить про довгострокову тенденцію формування в мережі Інтернет класичних прав та обов'язків громадянина та держави, що існують в традиційній державі та формування своєрідних „цифрових суверенітетів".

4. Незважаючи на декларовані бажання основних геополітичних суб'єктів протидіяти мілітаризації кіберпростору, можна констатувати збільшення ролі суто військових структур у забезпечення безпеки національної критично-важливої інфраструктури (національного кіберпростору) [2]. Швидше за все, ініціативи в межах ООН щодо вироблення комплексних підходів до міжнародної інформаційної безпеки будуть або повністю невдалими, або обмежено вдалими (на рівні декларативної згоди). В таких умовах Україна має бути готова не лише до ведення оборонних війн, однак активно створювати власні засоби ведення війни у кіберпросторі.

ЛІТЕРАТУРА:

1. Інформаційні технології та тенденції розвитку міжнародної інформації // Вісник книжкової палати – 2010. – №6 – С. 32.

2. Даниелова А. Основные направления информатизации американского общества / А. Даниелова // США-Канада. – 2009. – №5 – С. 27.

Біленький А.В. (НЦЗІ ВІТІ НТУУ „КПІ”)
Живило Є.О. (НЦЗІ ВІТІ НТУУ „КПІ”)

МАЙБУТНЄ КІБЕРПРОСТОРУ ТА НАЦІОНАЛЬНІ ІНТЕРЕСИ УКРАЇНИ: НОВІ МІЖНАРОДНІ ІНІЦІАТИВИ ПРОВІДНИХ ГЕОПОЛІТИЧНИХ ГРАВЦІВ

Майбутнє кіберпростору вже не є виключно проблемою окремих держав – потрібні узгодженні рішення принаймні ключових геополітичних „гравців”.Можливість визнання кібернападу „актом війни”, а кіберзброю прирівняти до зброї масового ураження переводить проблему в категорію актуальних загроз національній безпеці.З метою вирішення даної проблеми низка ключових світових держав (США, КНР, Російська Федерація) виступають з власними ініціативами щодо впорядкування на глобальному рівні питань кібербезпеки (інформаційної безпеки), однак запропоновані підходи не лише слабко узгоджуються між собою, а й подеколи протирічать одне одному.

Ініціативи Сполучених Штатів Америки щодо майбутнього кіберпростору:

ключова зовнішньополітична ініціатива США, щодо перспектив розвитку кіберпростору була оприлюднена 16 травня 2011 року з назвою Міжнародна стратегія для кіберпростору (International Strategy for Cyberspace).

Документ виокремлює три стратегічні цілі, що мають бути досягнуті за реалізації Стратегії, і серед них – „Стабільність через норми” (сприятиме передбачуваності поведінки держав, що дозволить попереджувати конфліктні ситуації чи непорозуміння).

Основні положення:

– США не бачать необхідності додатково ухвалювати принципово нові міжнародні документи[1];

– приватний сектор має виконати свою роль у захисті інтернет – свободи. Приватні компанії, що торгують технологіями, які можуть бути використані для придушення „свободи слова” (системи спостереження, моніторингу інтернет – трафіку тощо) мають фактично вдаватися до самообмежень при обранні клієнтів для своєї продукції;

– недопущення використання урядом тематики „управління інтернетом” з метою посилення „контролю за інтернетом”. В більш широкому сенсі США виступають категорично проти будь – яких бар’єрів у кіберпросторі, що можуть трактуватися як своєрідні „кордони держави в кіберпросторі”.

Ініціативи Російської Федерації та Китайської Народної Республіки щодо майбутнього кіберпростору:

Основна концептуальна відмінність, що вирізняє американський та російсько-китайський підхід – неготовність виділити кібербезпеку в якості самостійної компоненти, вважаючи її лише елементом більш широкого (а іноді й доволі абстрактного) поняття „інформаційно – психологічної безпеки”.

Ключовий документ російської сторони – Конвенція про забезпечення міжнародної інформаційної безпеки.

Основні положення:

– неправомірне використання інформаційних ресурсів іншої держави без узгодження з цією державою;

– діяльність в інформаційному просторі з метою підриву політичної, економічної та соціальної системи іншої держави;

– маніпулювання інформаційними потоками і інформаційним простором інших держав;

– протидія доступу до новітніх інформаційно – комунікативних технологій.

В рамках ООН сторони розпочали супровід своєї пропозиції в межах Першого та Третього комітетів [2].

Основні зауваження Російської Федерації та Китайської Народної Республіки щодо майбутнього кодексу (документу):

– проект є спробою домогтися від ООН схвалення дій щодо посилення контролю над інтернет – простором;

– якщо такий кодекс буде прийнятий, це майже неминуче підірве свободу ЗМІ;

– подібні ініціативи є неприпустимими, оскільки потенційно можуть бути використані для зведення бар'єрів на шляху потоку інформації чи обміну думками;

– низький рівень участі громадянського суспільства, закріплення провідної ролі держави, потенціал для звуження універсальних прав людини.

Україна вже зараз відноситься до тих країн, для яких кіберзлочинність – актуальна проблема сьогодення.

Український погляд на міжнародні ініціативи щодо майбутнього кіберпростору:

І. Елементи, на які варто звернути увагу при прийнятті рішень:

1. Політичні чи нормативно – правові ініціативи.

2. „Право на самозахист": формат реалізації у чинному міжнародному нормативно –

– правовому полі. Односторонні дії.

3. Баланс „цифрового суверенітету": від тотальної відкритості (США) до ключової ролі держави (РФ-КНР).

4. Інформаційно-психологічний компонент кібербезпеки: проблеми законодавчого закірплення („інформаційна війна", „масована психологічна обробка").

5. Наявність спільних підходів.

ІІ. Висновки та очікуваний розвиток подій:

1. Геополітичні „гравці" активно пропонують свій порядок денний щодо майбутнього кіберпростору.

2. Пропоновані американською стороною ініціативи, що найшвидше, так і не будуть реалізовані в повному обсязі в загальносвітовому масштабі, й не в останню чергу через неприйнятність окремих положень цих ініціатив для інших країн.

3. США обрали результативну стратегію налагодження двосторонньої співпраці (Австралія, Японія, Індія) у межах своєї Стратегії та розширення дії Конвенції про кіберзлочинність як чинного міждержавного правового документа.

4. Сумнівними є перспективи ініціатив РФ та КНР (як Правил, так і Кодексу). Стратегічно прийняття міжнародного документа (як на рівні політичної декларації, так і міжнародного правового документа у вигляді Конвенції) є правильним кроком до посилення загальносвітової стабільності в кіберпросторі, однак малоймовірним на практиці.

5. Певна невизначеність деяких із зазначених документів (зокрема запропонований Кодекс РФ) зробить вкрай складним впровадження її у практику на національному рівні.

6. Усі запропоновані ініціативи в їх нинішніх редакціях не вповні відповідають національним інтересам України.

7. Створення реального міжнародного консенсусу з проблем кіберпростору між ключовими геополітичними „гравцями" є об'єктивною необхідністю, адже унеможливить подальше стрімке зростання кіберзагроз як на національному, так і міжнародному рівні.

8. Україна об'єктивно зацікавлена в тому, щоб брати в цих дискусіях активну участь, в тому числі – у профільних групах експертів.

9. Вироблення консенсусного документа з проблем кіберпростору цілком може стати провідною темою під час головування України в ОБСЄ в 2013 році. Сама історія формування цієї структури свідчить про можливість вироблення консенсусного бачення на базі добровільно взятих на себе політичних зобов'язань.

ЛІТЕРАТУРА

1. Барак Обама. Дерзость надежды / Барак Обама. – Азбука- классика, 2008 – 145 с.

2. Резолюция Генеральной Ассамблеи ООН A/RES/57/239 „Создание глобальной культуры кибербезопасности", http://daccessdds.un.org/doc/UNDOC/GEN/N02/738/25/.

к.т.н. Богданов В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Жук О.В. (ВІТІ НТУУ „КПІ”)
Діянчук І.М. (ВІТІ НТУУ „КПІ”)

МОДЕЛЬ ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ ФІЗИЧНОГО ЗАХИСТУ НА ОСНОВІ КРИТИЧНОЇ ТОЧКИ ВИЯВЛЕННЯ ПОРУШНИКА

Для аналізу систем фізичного захисту (СФЗ) і оцінки їх ефективності існує ряд методів та моделей, що дозволяють оцінювати як існуючі, так і проектовані системи. Найвідомішою і достатньо докладною методикою аналізу СФЗ є методика, що розроблена Сандійською національною лабораторією (США), яка отримала назву – модель EASI (Estimate of Adversary Sequence Interruption). Аналіз СФЗ за допомогою моделі EASI має суттєві обмеження в зв’язку з відсутністю імовірнісної оцінки результатів зіткнення порушників і сил охорони, оцінки сил вторгнення на етапі перевірки достовірності сигналів тривоги, аналізується лише один певний маршрут. Тому важливою задачею при побудові ефективної СФЗ є визначення так званої критичної точки виявлення (КТВ) порушника, де час його затримки дещо перевищує час реагування сил охорони об’єкта (рис. 1).

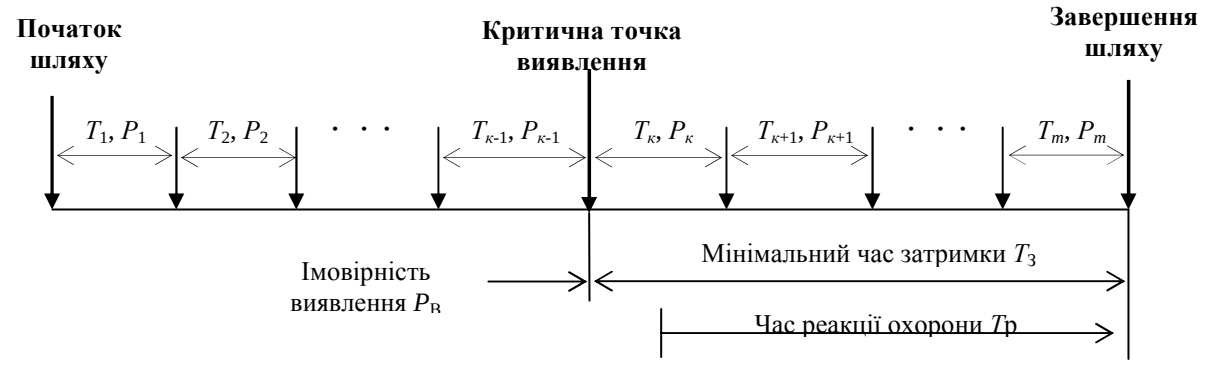


Рис. 1. Ілюстрація своєчасного виявлення як міри ефективності системи фізичного захисту

З метою автоматизації відповідних розрахунків, демонстрації ефекту зміни базових показників СФЗ на певному маршруті на положення КТВ і вибору оптимальних параметрів системи розроблена комп’ютерна модель оцінки ефективності СФЗ на основі КТВ порушника.

Враховуючи, що затримка без попереднього виявлення і сповіщення сил реагування не має сенсу, мірою ефективності системи можна вважати сумарний час затримки порушника $T_{Зj}$ та результуючу імовірність своєчасного виявлення порушника до досягнення цілі $P_{Вj}$:

$$T_{Зj} = \sum_{i=k_j}^{m_j} T_{ij} \geq T_р, \qquad P_{Вj} = 1 - \prod_{i=1}^{k_j - 1} \overline{P}_{ij} \ ,$$

де m_j – загальне число елементів системи захисту по j-му маршруту порушника; k_j – точка, де $T_{Зj}$ починає перевищувати час реагування сил охорони $T_р$; T_{ij} – час затримки елемента i по j-му маршруту; $\overline{P_{ij}}$ – імовірність того, що елемент i по j-му маршруту не виявить порушника, $\overline{P_{ij}} = 1 - P_{ij}$.

Для побудови ефективної СФЗ необхідно визначити найбільш уразливі маршрути на території підприємства та розрахувати основні параметри ефективності – $T_{Зj}$, $T_р$ і $P_{Вj}$. Шляхи, що представляються найбільш доступними, можуть бути введені в модель, де для кожного з них підраховуються значення $P_{Вj}$**.** Найкращою мірою ефективності системи є своєчасне виявлення, куди входять $P_{Вmax}$, $T_{Зmin}$, $T_р$. Роботу можна вважати закінченою, а систему захисту – придатною до впровадження, коли після допрацювання всіх шляхів проникнення порушника на підприємство імовірності $P_{Вj}$ будуть приблизно однакові.

к.т.н. Богданов В.В. (ВІТІ НТУУ „КПІ”)
Мартинюк В.В. (ВІТІ НТУУ „КПІ”)
Богданова О.В. (ВІТІ НТУУ „КПІ”)

ПРОБЛЕМИ І ПЕРСПЕКТИВИ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1. Одним з найважливіших технічних аспектів безпеки інформаційно-комунікаційних систем і мереж, наряду з радіоелектронним захистом і застосуванням захищених інформаційних технологій є інженерно-технічний захист інформації.

Інженерно-технічний захист інформації представляє собою сукупність спеціальних органів, технічних заходів і засобів для їх використання в інтересах захисту конфіденційної інформації:

фізичних засобів захисту, призначених для створення перепон на шляху порушника (охоронні та охоронно-пожежні системи, охоронне телебачення, охоронне освітлення, засоби фізичного захисту);

апаратних засобів захисту – різноманітних технічних конструкцій, які забезпечують припинення розголошення, захист від витоку та протидію несанкціонованому доступу до джерел конфіденційної інформації;

програмних засобів захисту – системи спеціальних програм для забезпечення захисту інформації від несанкціонованого доступу, копіювання, вірусів та засобів програмного захисту каналів зв’язку;

засобів криптографічних захисту (КГЗ) – апаратних, програмних та програмно-апаратних засобів, що реалізують захист інформації за допомогою криптографічних перетворень.

2. Для аналізу систем фізичного захисту (СФЗ) і оцінки їх ефективності існує ряд методів та моделей, що дозволяють оцінювати як існуючі, так і проектовані системи. Найвідомішою і достатньо докладною методикою аналізу СФЗ є комп’ютерна модель EASI (Estimate of Adversary Sequence Interruption). В той же час аналіз СФЗ за допомогою моделі EASI має суттєві обмеження в зв’язку з відсутністю імовірнісної оцінки результатів зіткнення порушників і сил охорони, оцінки сил вторгнення на етапі перевірки достовірності сигналів тривоги, аналізується лише один певний маршрут. Тому важливою задачею при побудові ефективної СФЗ є визначення так званої критичної (граничної) точки виявлення (КТВ) порушника, де імовірність виявлення порушника становить $P_{\text{В}j}$, а час його затримки $T_{\text{З}j}$ дещо перевищує час реагування сил охорони об’єкта $T_{\text{р}}$. З метою автоматизації відповідних розрахунків, демонстрації ефекту зміни базових показників СФЗ на певному маршруті на положення КТВ і вибору оптимальних параметрів системи розроблена комп’ютерна модель оцінки ефективності СФЗ на основі КТВ порушника. Найкращою мірою ефективності системи є своєчасне виявлення, яке характеризується імовірністю виявлення $P_{\text{В}max}$ та $T_{\text{З}min}$.

3. В умовах, коли до систем захисту інформації (СЗІ) пред'являється багато різних, інколи протилежних вимог, актуальною представляється задача розробки інженерних методів вибору найкращого варіанту СЗІ з урахуванням усієї сукупності покажчиків якості на основі системного підходу і системного аналізу. При цьому задача багатокритеріальної оптимізації зводиться до того, щоб з множини M_s варіантів системи S вибрати такий варіант (систему S_0), який має найкраще значення вектора $Q = \left(q_1,...,q_j,...,q_m\right)$, виходячи з вибраного критерія переваги. Слід відмітити, що при виборі раціонального варіанту в якості вимог до СЗІ можуть бути використані якісні і кількісні показники нормативно-методичного і організаційного характеру, технічні характеристики, ступінь кваліфікації персоналу тощо.

4. В значній більшості практичних задач щодо вибору раціонального варіанту СЗІ особливий інтерес представляють не тільки кількісні показники їх ефективності, а і

функціонування при різних критичних умовах – завадах, загрозах, атаках тощо. Найбільш потужним і універсальним методом дослідження інформаційних систем управління різного призначення є імітаційне моделювання. При імітаційному моделюванні вибрана математична модель об'єкта, що досліджується, відтворює алгоритм (логіку) його функціонування в часі при різноманітних співвідношеннях параметрів системи і навколишніх умов. Як приклад можливості застосування вищеприведеного системного підходу щодо дослідження інформаційних об'єктів шляхом моделювання для таких складових інформаційної системи управління як засоби криптографічного захисту розроблена бібліотека *Cryptography*, яка призначена для побудови і дослідження моделей систем і алгоритмів криптографічних перетворень інформації і працює в середовищі *MATLAB*.

5. Основною задачею при розробці програмного забезпечення захисту інформації є забезпечення гарантій виконання політики безпеки, визначення дестабілізуючих факторів та загроз безпеці, застосування новітніх методів запобігання загрозам і підвищення надійності. Для цього розробляються та застосовуються методи оперативного виявлення дефектів при виконанні програм та спотворень даних шляхом введення в них часової, інформаційної та програмної надмірності. Реалізація інформаційної безпеки об'єктів, що захищаються, на всіх функціональних рівнях захисту забезпечується найкращим чином при використанні комплексного підходу, коли кожна програмна компонента виконує відповідні функції по захисту від несанкціонованого доступу і одночасно здійснюється контроль коректності функціонування механізмів захисту.

6. Найбільш проблемними напрямами реалізації КГЗ є наступні:

передача великих обсягів конфіденційної інформації від віддалених абонентів (на відстані сотні і тисячі кілометрів, зокрема маються на увазі миротворчі контингенти);

забезпечення цілісності повідомлень, що передаються між абонентами різних рівнів впорядкованості;

збереження інформації (документів) на носіях в зашифрованому вигляді;

управління ключами з можливістю впровадження окремих елементів інфраструктури відкритих ключів;

вдосконалення алгоритмів апаратного шифрування і впровадження засобів програмного шифрування з можливістю використання сучасних засобів зв'язку;

дослідження статистичної безпеки КГ алгоритмів в сучасних і перспективних зразках ТСЗ.

Серед можливих напрямів вирішення цієї проблеми можна назвати наступні: впровадження сучасних алгоритмів автоматизації обробки і розпізнавання інформації (від удосконалення класичних до нейронних і генетичних алгоритмів), представленої в різних формах; використання шифруючих ЕОМ, ЕОМ з нульовою зоною, приладів типа PRAGMA, перспективних програмно-апаратних засобів криптографічного захисту інформації, пристроїв співспряжіння апаратних засобів шифрування з програмними ЕОМ; застосування стеганографічних методів захисту при передачі зображень, мовних повідомлень і текстової інформації; використання гібридних технологій шифрування, що поєднують можливості і переваги потокового і блочного шифрування; дослідження можливостей впровадження в криптографічну апаратуру кращих світових алгоритмів потокового і блокового шифрування, електронного цифрового підпису; створення в ЗС України інфраструктури керування відкритими ключами, головними завданнями якої є виготовлення, відновлення, скасування і поширення відкритих ключів з забезпеченням їх суворої автентифікації та сертифікації.

7. Слід відмітити, що серед можливих потенційних причин ненадійності систем технічного і криптографічного захисту особливої уваги заслуговує людинний фактор. Непрофесійні дії користувачів зводять нанівець самий стійкий алгоритм і саму коректну його реалізацію. Ці фактори необхідно ураховувати при науковому вирішенні проблем технічного і криптографічного захисту і в навчальному процесі, впроваджуючи на всіх видах занять сучасні інформаційні технології і інформаційно-комунікаційні ресурси.

Боголій С.М. (ВІТІ НТУУ „КПІ”)
Фомін М.М. (ВІТІ НТУУ „КПІ”)
к.т.н. Штаненко С.С. (ВІТІ НТУУ „КПІ”)

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

На сьогодні перспективним напрямком розвитку телекомунікаційних технологій є використання техніки цифрової обробки сигналів – однієї з найдинамічніших та швидко розвиваючих технологій у світі. Цифрова обробка сигналів – це інформатика реального часу, покликана вирішувати задачі прийому, обробки, скорочення надмірності і передачі інформації в реальному часі.

Новим імпульсом в розробці цифрових пристроїв обробки, передачі і збереження інформації являється радикальна зміна технологічних можливостей новітніх процесорних систем [1]. Завдання, які ставляться перед виробниками процесорної техніки, це 1 млрд. транзисторів в процесорі, тактова частота до 10 ГГц, а продуктивність 100 млрд. операцій в секунду. Усе це можливо в результаті застосування нейронного, оптичного та квантового процесорів, а також в результаті застосування нанотехнологій (молекулярна електроніка, біохімічні і органічні рішення, квазімеханічні рішення на основі нанотрубок) [2].

Методами молекулярної електроніки з вуглеводневих з’єднань вдається отримати аналоги діодів і транзисторів і як наслідок – основні булеві модулі І, АБО і НІ, з яких потім можна будувати схеми будь-якої складності. Передбачається, що на молекулярних пристроях пам’яті (сучасний кристал кремнію) можна буде зберігати великі об’єми інформації [3].

Застосування оптичного і квантового процесора відкриє шлях до підвищення тактової частоти процесорів, за рахунок зміни опору та ємності внутрішньосхемних з’єднань.

Необхідно відзначити, що провідні виробники світу оголосили про виявлення четвертого пасивного елементу електронних ланцюгів – мемристора, здатного працювати в умовах змінного струму, електричний опір якого залежить від полярності напруги, прикладеної до нього. Головною якістю мемристора є саме мемристивність – залежність опору від заряду, пройденого через елемент. Мемристивні системи досі використовували тільки як математичні абстракції для моделювання процесів обробки сигналу, поведінки нелінійних напівпровідникових систем, електрохімічних процесів та навіть для моделювання роботи нейронів головного мозку людини. Проте на практиці ефект мемристивності (пам’ятливості) так і не був реалізований, оскільки мав дуже маленькі значення для різних мікроелектронних систем. Все змінилося з приходом нанорозмірних об’єктів.

Застосування інженерного підходу в біології при проектуванні нових функціональних систем дозволить в найближчому майбутньому вийти на абсолютно інший технологічний рівень – біологічну схемотехніку. Якщо базовими компонентами електронних схем є окремі транзистори, то для їх біологічних аналогів основу складають гени – високовпорядковані ділянки послідовностей ДНК, що виконують певні функції. Вражаючим є той факт, що створювані сьогодні синтетичні біологічні системи за функціональними властивостями являються практично ідентичними першим електричними схемам, які проектувалися для оптимізації процесу виробництва перших напівпровідникових мікросхем.

ЛІТЕРАТУРА

1. Зубарев Ю.Б. Цифровая обработка сигналов – информатика реального времени / Ю.Б. Зубарев, В.В. Витязев, В.П. Дворкович // Российский научно-технический журнал DSP – Москва, С. 23 – 38.

2. Валиев К.А. Квантовые компьютеры: надежность и реальность. / К.А. Валиев. – Регулярная и хаотическая динамика, 2002. – 352 с.

3. Плотников Г.С. Физические основы молекулярной электроники / Г.С. Плотников, В.Б. Зайцев. Учебное пособие. – М.: Физический факультет МГУ, 2000. – 164 с.

к.т.н. Богуш Ю.П. (ІСЗЗІ НТУУ „КПІ”)
Богуш К.Ю. (ІСЗЗІ НТУУ „КПІ”)
к.т.н. Бердников О.М. (ІСЗЗІ НТУУ „КПІ”)

РОЗПІЗНАВАННЯ МОВИ ДЛЯ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

У загальному випадку, розпізнавання мови полягає у визначенні змісту сказаного – перетворенні мови в текст. Особливістю є то, що мовний сигнал має високий ступінь надмірності щодо інформації, яку він несе.

Розпізнавання мови, як і інші завдання загальної теорії розпізнавання образів, полягає у віднесенні вихідних даних до певного класу за допомогою виділення істотних ознак, що характеризують ці дані, із загальної маси несуттєвих даних [1].

Виділення з мовного сигналу істотних ознак, що несуть значеннєву інформацію й усунення надмірності пропонується забезпечити шляхом використання принципів, що застосовувані для сильного стиску (компресії) мовного сигналу у вокодерних системах передачі. Чим нижче інформаційна швидкість вокодеру, тем тісніше зв'язок вокодерного перетворення з розпізнаванням мови й усе більшою мірою аналізатор вокодеру нагадує систему розпізнавання. Виходячи з наведених принципів, що лежать в основі розпізнавання, вибір алгоритму вокодерного перетворення повинен ґрунтуватися на мінімізації швидкості кодування мови при максимальнім збереженні змісту переданої інформації, у якості заходу якого пропонується використовувати складову розбірливість. Варто відзначити, що використання оцінки *MOS* (*Mean Opinion Score*) тут недоречно, тому що вона відображає натуральність мови, а не можливості передачі змісту [табл. 1].

Таблиця 1

Порівняльні характеристики кодерів мови

Кодер	Швидкість кодування, кбіт/с	*MOS*	Складова розбірливість, %
PCM (ІКМ)	64	4,3	95
ADPCM (АДІКМ)	32	4,1	94
LD-CELP	16	4,0	94
RPE-LTP (*GSM*)	13	3,5	
QCELP	9,6	3,4	
CELP	4,8	3,2	93
LPC	2,4	2,5	90
MBE	2,4/1,2	-	87/84

Актуальним завданням сьогодні є застосування систем розпізнавання мови в рамках напрямку штучного інтелекту, наприклад, для забезпечення мовних інтерфейсів взаємодії інтелектуальних систем.

Завдання навчання таких систем пропонується розв’язати за допомогою побудови „бази знань” – зіставлення кожної наявної функції системи всім можливим варіантам їх голосового виклику [2].

Запропоновані методи реалізовані у вигляді базової програмної реалізації системи розпізнавання мови, яка забезпечує розпізнавання слів і виконання команд на основі розпізнаних послідовностей слів [3].

ЛІТЕРАТУРА:

1. Дж. Ту, Р. Гонсалес. Принципы распознавания образов. Пер. с англ. / Под ред. Ю.И. Журавлева. – М.: Мир, 1978. – 457 с.

2. Бердников О.М., Богуш К.Ю. Модель системи пофонемного розпізнавання мови на основі акустичних параметрів смугового вокодеру / Збірник наукових праць ВІТІ НТУУ “КПІ”. – 2010. – № 2. – с. 11…18.

3. Бердников О.М., Богуш К.Ю., Богуш Ю.П. Розпізнавання мовлення в системах штучного інтелекту / Збірник наукових праць ІСЗ НТУУ „КПІ”. – 2012. – № 1. – с. 21…25.

Борисов О.В. (ВІТІ НТУУ „КПІ”)
Уманець Я. Л. (ВІТІ НТУУ „КПІ”)

МЕТОД ОБРОБКИ СИГНАЛІВ В СИСТЕМІ MIMO

Однією з технологій, що дозволяють значно збільшити пропускну здатність радіоканалів є технологія „багато входів – багато виходів” (MIMO – Multiple-Input Multiple-Output), яка дозволяє більш ефективно використовувати потужність передавача і боротися із завмираннями сигналів [1]. Підвищення ефективності досягається за рахунок використання методів просторово-часової обробки (STC – Space Time Coding), що забезпечують передачу і приймання паралельних потоків інформації. Теоретично пропускна здатність системи MIMO з STC може бути збільшена пропорційно кількості антен на передавальному боці (за умови, що кількість приймальних антен не менша ніж кількість передавальних антен) у порівнянні з традиційними системами радіозв’язку з однією передавальною антеною (SISO – Single-Input Single-Output). Аналіз відомих систем STC [2] показує, що підвищення спектральної ефективності системи MIMO, як правило, пов’язане з ускладненням демодулятора STC і зі зниженням завадостійкості системи. Для обчислення оцінок переданих символів можуть використовуватися різні методи: метод мінімуму середньоквадратичної помилки, алгоритм V-BLAST (Vertical Bell Laboratories Layered Space Time Architecture), метод максимальної правдоподібності [1 – 2]. Аналіз відомих методів демодуляції сигналів в системах MIMO з просторово-часовою обробкою виявив їх основні недоліки. Так одні мають низьку точність, а інші велику обчислювальну складність. Тому *метою* роботи є розробка методу обробки сигналів на приймальному боці, який забезпечує задану якість передачі інформації і характеризується помірною обчислювальною складністю. В [2] описаний ітераційний квазиоптимальний метод демодуляції сигналів в системі MIMO. У цьому алгоритмі сигнали користувачів розбиваються на групи, потім установлюються початкові значення оцінок інформаційних символів і формуються репліки для кожної групи сигналів. Після вирахування реплік із вхідного сигналу утворюються статистики для демодуляції. Демодуляція кожної групи сигналів здійснюється за допомогою оптимального алгоритму. Оцінки інформаційних символів визначаються за кілька ітерацій. В [2] проаналізовані характеристики демодуляції для сіми ітерацій для різних варіантів систем BLAST. Складність цього методу значно менша в порівнянні з методом максимальної правдоподібності, при цьому характеристики цього алгоритму помітно перевищують характеристики V-BLAST, але є значна відмінність від характеристик алгоритму максимальної правдоподібності. Завадостійкість цього методу можна значно покращити шляхом врахування ступеня точності оцінок на проміжних ітераціях. З математичного розрахунку методу обробки сигналів на приймальному боці було видно що, на кожній ітерації враховується не тільки оцінка, отримана на попередньому кроці, але й ступінь точності оцінювання символів. Для проведення оцінки ефективності розробленого методу було розроблено імітаційну модель в середовищі програмування *Matlab* (*Simulink*). Моделювання проводилося для системи з 4 приймальними й 4 передавальними антенами при використанні квадратурної амплітудної модуляції. За результатами моделювання можна зробити вивід про те, що запропонований метод має характеристики, близькі до характеристик демодулятора, оптимального за критерієм максимальної правдоподібності, але значно меншу обчислювальну складність. Цей метод може використовуватися для демодуляції в системах з більшою кількістю антен і з високою кратністю модуляції.

ЛІТЕРАТУРА

1. Capacity limits of MIMO channels / A.J. Goldsmith, S.A. Jafar, N. Jindal, S. Vishwanath // IEEE J. Select. Areas Commun. – 2003. – Vol. 21, № 6. – P. 684 –702.

2. Andrews J.G. Inteference cancellation for celluar systems: A contemporary overview / Andrews J.G. // IEEE Wireless Communications Magazine. – 2005. – vol. 12, № 2. – P. 19 – 29..

Бохно Г.Т. (ВІТІ НТУУ „КПІ”)

СИСТЕМИ ГЛОБАЛЬНОГО ПОЗИЦІОНУВАННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗБЕРЕЖЕННЯ ВАНТАЖІВ

При проектуванні, запуску й експлуатації мереж транспортних перевезень однією з основних проблем є задача забезпечення якості обслуговування при зберіганні та переміщенні вантажів. З метою гнучкого і безперервного контролю та управління пересуванням вантажів необхідна точна інформація про їх місцезнаходження.

Вирішення цієї задачі забезпечується широким застосуванням на транспортних рухомих об’єктах та вантажах засобів навігації. Для цього всі рухомі одиниці, що беруть участь в перевезенні, та об’єкти, що потребують перевезення, повинні бути оснащені системами навігації, які здатні безперервно, надійно та точно визначати їх територіальне місцезнаходження в різних метеоумовах та в будь-який час доби і пору року. Найбільш повно в досягненні зазначених цілей зарекомендували себе комплексні системи навігації до складу яких входять елементи автономних навігаційних систем та супутникових радіонавігаційних систем. Спільна обробка інформації, отриманої від різних незалежних систем навігації, дозволяє підвищити точність та достовірність визначення місцезнаходження вантажів та транспортних рухомих об’єктів [1].

Навігаційна інформація, отримана з комплексних навігаційних систем, знаходить широке застосування не тільки в цивільних транспортних мережах, а й у військових мережах тилового та технічного забезпечення (логістики). Навігаційне забезпечення є одним з важливих елементів бойового забезпечення військ та оперативного сервісного забезпечення цивільних користувачів, які керують рухомими об’єктами.

Метою даної роботи є розробка варіанту використання системи глобального позиціонування для забезпечення збереження вантажів, які циркулюють в військових транспортних мережах, із застосуванням глобальної системи визначення координат GPS (Global Positioning System) в якості складової частини комплексної системи навігації.

Проведено аналіз існуючих систем навігації наземних рухомих об’єктів та їх експлуатаційно-технічних характеристик, детально розглянуті принципи роботи систем супутникового позиціонування NAVSTAR та Galileo [2]. Проведено аналіз шляхів модернізації цих систем, що, в свою чергу, надасть значну користь при вирішенні завдань, де необхідно швидке та точне позиціонування рухомих об’єктів. Розглянуто ряд питань, які відносяться до наслідків модернізації глобальних систем визначення координат, що дозволять вдосконалити конструкцію приймачів сигналів та їх програмне забезпечення.

Таким чином, в результаті виконання роботи була запропонована оптимізація варіанту використання системи глобального позиціонування GPS для забезпечення збереження військових вантажів, перевагою якої є зменшення економічних витрат на їх перевезення за рахунок вирішення “транспортної задачі” з урахуванням категорій важливості вантажів.

Результати, отримані в ході виконання даної роботи, можуть бути використані при розробці комплексних систем навігації військового призначення.

ЛІТЕРАТУРА

1. Волчко П.І., Іванов В.І., Корольов В.М. та інші. „Вимоги до характеристик навігаційної інформації і систем навігації наземних рухомих об’єктів у сучасному штатному процесі”. Сучасні досягнення геодезичної науки та виробництва, № 5. С. 280 – 283, Ліга-Прес, Львів, 2000.

2. „La navigation par satellite, le point de vue des utilisateurs europeens”. Bara J. M., Navigation (France). 2000. № 191. C. 69 – 75.

Бунаков В.П.(ЦНДІ ОВТ ЗСУ)
Степаненко Ю.К. (ЦНДІ ОВТ ЗСУ)
Семенюк Р.П. (ЦНДІ ОВТ ЗСУ)

ШЛЯХИ УДОСКОНАЛЕННЯ АКТИВНИХ ПРИЙМАЛЬНО-ПЕРЕДАЮЧИХ АНТЕН

Необхідність вдосконалення активних приймально-передаючих антен (АППА) для створення компактних засобів зв'язку індивідуального використання пов'язана з подальшим зменшенням габаритних розмірів антени, високочастотної частини передавачів, покращенням їх енергетичного потенціалу.

Активна приймально-передаюча антена виконується як окремий блок й складається із самої антени, активного пристрою приймально-передаючого каналу, а також пристрою розв'язки тракту й захисту приймальної частини.

Об'єднання антени з активними елементами дозволяє, в порівнянні з пасивними випромінювачами, зменшити їх розміри, розширити полосу пропускання, здійснити електронне керування параметрами антени, покращити відношення сигнал-шум по приймальному каналу, підвищити потужність випромінювання й ККД передаючого каналу.

Безпосередній вибір схеми побудови АППА визначається вимогами до потужності випромінювання передаючого каналу, чутливості приймальної системи з приймальним каналом та геометричними розмірами самої антени.

Підвищення потужності випромінювання АППА може бути реалізовано шляхом використанням більш потужних активних пристроїв або побудовою передаючого каналу АППА за багатоканальною схемою.

Активні елементи розташовуються в безпосередній близькості від випромінювачів, що дозволяє виключити використання високочастотного тракту, а у ряді випадків – і фазообертачів при роботі з високим рівнем потужності і, отже, зменшити втрати в них і збільшити ККД, а також зменшити вимоги до них за рівнем прохідної потужності. Наявність активного елементу в тракті прийому-передачі антени призводить до зміни характеристики тракту в режимі прийому і передачі електромагнітних коливань.

Застосування активних елементів при побудові АППА призводить до виникнення ряду побічних ефектів, а саме: випромінювання на частотах гармонік при передачі, зниження внутрісистемної електромагнітної сумісності.

Недоліками АППА, що проявляються під час їх використання, є:

– необхідність розв'язки приймально-передаючого тракту;

– використання для захисту приймального каналу обмежувальних пристроїв, що призводить до порушення узгодженості в частотному діапазоні.

Перспективним напрямом розвитку АППА є використання волоконно-оптичних систем для розводки сигналів від випромінюючих елементів для обробки і управління активними модулями. Оптичне управління в АППА має такі переваги: велику завадостійкість, високу сумісність з напівпровідниковими активними елементами, малу вагу і габаритні розміри.

Таким чином, активні приймально-передаючі антени на теперішній час знайшли своє використання під час розробки та модернізації засобів зв'язку, радіолокаційних станцій та іншої техніки спеціального призначення і є перспективними з погляду підвищення завадозахищеності, економічної ефективності, а також покращення електромагнітної сумісності радіоелектронних засобів.

Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Висоцька Т.М. (ВІТІ НТУУ „КПІ”)
Корчагіна Н.С. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ВИБОРУ РАЦІОНАЛЬНОГО СЦЕНАРІЮ МОДЕРНІЗАЦІЇ МЕРЕЖІ ДОСТУПУ

Методика вибору раціонального сценарію модернізації мережі доступу дозволяє шляхом перебору технологій, варіантів сценаріїв модернізації мережі доступу, розрахунку техніко-економічних характеристик здійснити вибір раціонального сценарію модернізації на основі прагматичного підходу. Мета розробки та вибору сценарію модернізації мережі доступу полягає в забезпеченні ефективності прийняття управлінських рішень Оператором зв’язку по проведенню заходів пов’язаних з підтриманню конкурентоспроможності телекомунікаційної компанії та отримання прибутків. Під ефективністю слід розуміти – одержання найкращого результату від використання наявних ресурсів.

Постановка задачі:

Задано:

– перелік технологій для забезпечення абонентського доступу;

– характеристики експлуатованої мережі доступу та її структура;

– сума інвестицій виділених для проведення модернізації;

– перелік телекомунікаційного обладнання.

Необхідно:

– розробити та вибрати раціональний сценарій модернізації мережі доступу;

– розрахувати основні техніко-економічні характеристики модернізованої мережі.

Обмеження:

– характеристики мережі доступу розраховуються на основі існуючого телекомунікаційного обладнання відомих фірм виробників та згідно вимог керівних документів і ДСТУ;

– час на розробку сценарію та розрахунки техніко-економічних показників визначає Оператор зв’язку.

Основні етапи реалізації методики.

1. Аналіз характеристик експлуатованої мережі доступу.
2. Формування цілей модернізації мережі доступу.
3. Вибір технологій використовуваних в мережі доступу.
4. Розробка *i*-го сценарію модернізації на підставі вибраних технологій.
5. Розрахунок техніко-експлуатаційних характеристик *i*-го сценарію модернізації мережі доступу.
6. Вибір телекомунікаційного обладнання та визначення переліку робіт по модернізації мережі доступу.
7. Розрахунок економічних характеристик і-го сценарію модернізації мережі доступу
8. Розрахунок часу на проведення модернізації мережі доступу.
9. Запис результатів розрахунків характеристик *i*-го сценарію модернізації мережі доступу в базу даних.
10. Визначення закінчення розробки всіх можливих сценаріїв модернізації мережі доступу настає тоді коли шляхом перебору можливостей створений *i*-тий сценарій із множини реальних сценарії $\{I\}$.
11. Вибір раціонального сценарію модернізації мережі доступу по визначеним критеріям оптимальності.
12. Процес вибору раціонального сценарію закінчується коли ухвалюється найбільш раціональний сценарій на основі рішення багатокритеріальної оптимізаційної задачі та експертних оцінок.

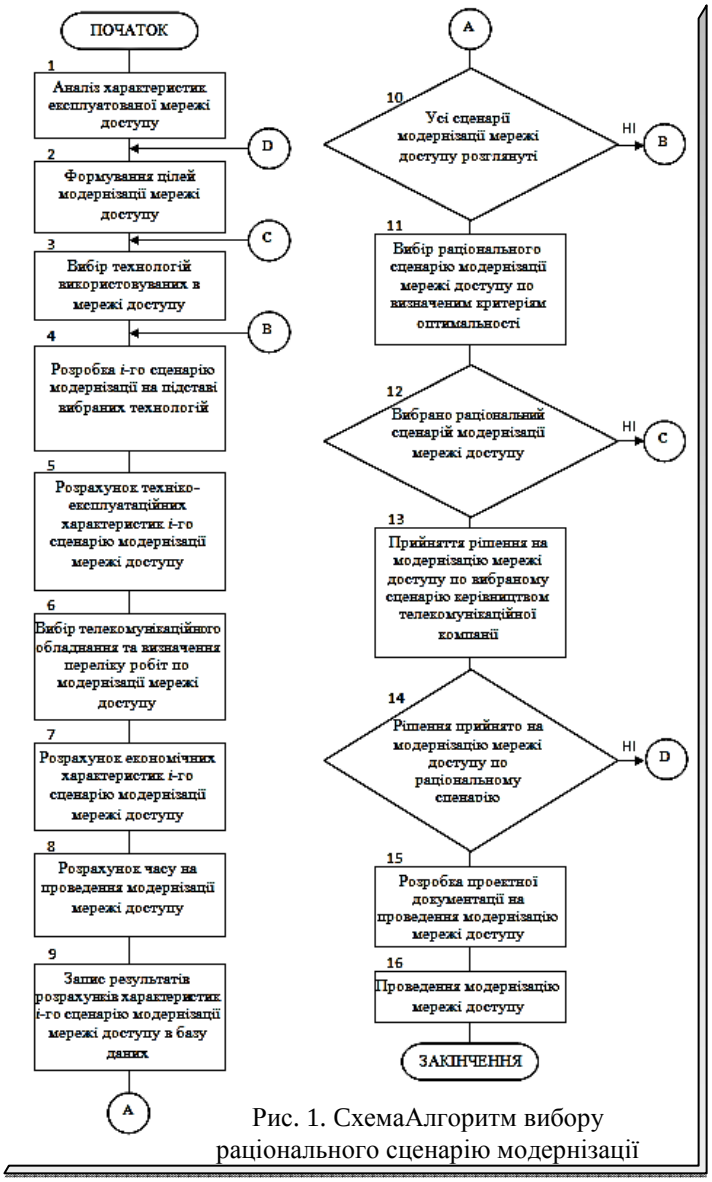


Рис. 1. СхемаАлгоритм вибору раціонального сценарію модернізації

13. Прийняття рішення на модернізацію мережі доступу по вибраному сценарію керівництвом телекомунікаційної компанії здійснюється на підставі експертних оцінок та прагматичного підходу з врахуванням внутрішніх і зовнішніх чинників, які впливають на бізнес телекомунікаційної компанії.

14. Процес прийняття рішення на модернізацію мережі доступу закінчується ухваленням керівництвом телекомунікаційної компанії раціонального сценарію.

15. Розробка проектної документації на проведення модернізацію мережі доступу здійснюється на підставі державних стандартів та вимог керівних документів. Розробка проектної документації може проводитись силами телекомунікаційної компанії або іншою організацію на договірній основі.

16. Проведення модернізацію мережі доступу проводиться згідно проектної документації та плану-графіку в визначені керівництвом телекомунікаційної компанії терміни.

На рис. 1. представлений алгоритм реалізації цієї методики.

Методика вибору раціонального сценарію модернізації мережі доступу надає можливість здійснити більш ефективний та прагматичний вибір сценарію модернізації мережі доступу. Ефективність застосування даної методики полягає в чіткому формуванні цілей та визначенні прагматичних оцінок застосування технології на мережах доступу. Виходячи з цього, розробка методик планерування сучасних мереж доступу і відповідних інструментальних засобів можна рахувати за важливе завдання для Операторів зв'язку.

ЛІТЕРАТУРА

1. Винницький В.П., Хиленко В.В. Методы системного анализу и проектирование телекоммуникационных сетей. – К.: Интерлинк, 2002. – 192 с.

2. Руководящий технический материал по модернизации сетей доступа. – СПб.: НТЦ Протей, 2005. – 122 с.

3. Соколов Н.А. Сети абонентского доступа: принципы построения. – Пермь: ЗАО „ИГ „Энтер-профи"", 1999. – 256 с.

4. Соколов Н.А. ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ. Монография в 4-х главах. – М.:Альварес Паблишинг, 2004, – 640 с.

5. Соколов Н.А. Эволюция местных телефонных сетей. – Пермь: ТОО „Типография Книга", 1994. – 144 с.

6. Филипс Д., Гарсиа-Диас А. Методы анализу сетей. – М.: Мир, 1984. – 496 с.

Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Захараш О.М. (ВІТІ НТУУ „КПІ”)
Кононова І.В. (ВІТІ НТУУ „КПІ”)

ПРИНЦИПИ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ СУЧАСНИМИ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

В умовах розмаїття телекомунікаційних та інформаційних технологій, їх швидкого прогресу та конвергенції, різноманітності типів та розгалуженості мереж, зростаючого попиту користувачів на нові послуги та підвищення вимог до їх якості, конкуренції операторів на ринку телекомунікацій тощо постають усе нові й нові завдання, пов'язані з управлінням мережами. Набуває особливої ваги визначення та вирішення проблем і завдань готовності до управління мережами в умовах надзвичайних ситуацій, надзвичайного стану та особливого періоду. В цих умовах повинно здійснюватися централізоване управління ресурсами мереж телекомунікацій загального користування, а також відомчих мереж (незалежно від форм власності або відомчої приналежності), і використання цих ресурсів для управління державою, безпеки, проведення відновних робіт, ліквідації наслідків надзвичайних ситуацій тощо, а також забезпечення максимально можливого рівня якості надання послуг усім споживачам. Саме ці завдання СУ (системи управління телекомунікаційними мережами має вирішувати НЦУ (національний центр оперативно-технічного управління мережами телекомунікацій).

Створювані СУ сучасними телекомунікаційними мережами мають бути автоматизованими і враховувати перспективні технології і концепції, а також відповідати стандартам і рекомендаціям міжнародних організацій.

В основу організації СУ телекомунікаційними мережами України в цілому й окремими мережами телекомунікацій покладено принципи:

багаторівневості, ієрархічної побудови;

централізації управління з можливістю децентралізації функцій управління;

інтегрованого підходу до вирішення завдань управління телекомунікаційними мережами в межах загальної території;

створення гнучкої архітектури на базі методології відкритих систем, що надає можливість реконфігурацп і нарощування функцій управління;

забезпечення високого рівня автоматизації процесів управління і застосування новітніх технологій обробки інформації;

використання єдиної системи стандартів з технічного, інформаційного і програмного забезпечення на базі рекомендацій ITU, стандартів ETSI, ISO, державних та галузевих стандартів.

Функціональна структура СУ телекомунікаційними мережами щодо попередження і дій у надзвичайних ситуаціях має охоплювати повний перелік проблем, що стосуються надзвичайних ситуацій, включаючи етапи їх прогнозування, попередження і підготовки до функціонування в умовах надзвичайних ситуацій, а також ліквідації їх наслідків.

Система управління телекомунікаційними мережами повинна бути спроможна функціонувати в таких чотирьох режимах:

режим повсякденної діяльності (стаціонарне функціонування);

режим підвищеної готовності (активна підготовка і здійснення превентивних заходів);

надзвичайний режим (дії у надзвичайній ситуації);

післянадзвичайний режим (ліквідація довгострокових наслідків надзвичайних ситуацій).

Під час очікування виникнення надзвичайної ситуації та за її виникнення повинні забезпечуватись:

організація роботи щодо взаємодії рятувальних і аварійно-відновних підрозділів операторів телекомунікацій під час ліквідації наслідків надзвичайних ситуацій;

управління створенням у регіоні, де може виникнути надзвичайна ситуація, окремої телекомунікаційної мережі та забезпечення її „прив'язки"до вузлів і станцій магістральної (зонової) мережі із використанням мобільних (рухомих) засобів телекомунікацій;

контроль за ходом відновлення зруйнованої стаціонарної мережі за допомогою рухомих контейнерних і, по можливості, стаціонарних технічних засобів телекомунікацій; уточнення переліку апаратури, кабельної продукції, будівельних та інших матеріалів, необхідних для відновлення працездатності об'єктів телекомунікацій, і контроль за їх постачанням у регіон надзвичайних ситуацій. Має забезпечуватись ефективне управління заходами, пов'язаними з використанням рухомих технічних засобів телекомунікацій для заміни, якщо потрібно, зруйнованих стаціонарних мережних вузлів (станцій), а саме: збереженням; технічним обслуговуванням; ремонтом; контролем технічного стану; впровадженням в експлуатацію; використанням за призначенням; збиранням даних; веденням розрахунків; матеріальним забезпеченням.

Для пріоритетного використання мереж і засобів телекомунікацій під час надзвичайних ситуацій оператори телекомунікацій повинні надавати:

лінії зв'язку, виділені канали зв'язку;

абонентську ємність стаціонарних телекомунікаційних мереж;

абонентську ємність мереж стільникового зв'язку, радіотелефонного зв'язку, пейджингового зв'язку тощо;

доступ до мереж передачі даних і телематичних служб;

канали радіозв'язку, використовувані в зоні надзвичайних ситуацій;

абонентські термінали рухомого зв'язку (з оформленням відповідних договорів з операторами).

Отже, сучасні телекомунікаційні системи базуються на спільному використанні технічних засобів телекомунікацій та обчислювальної техніки. Відмови в роботі таких систем призводять до величезних збитків. Щоб уникнути таких збитків, потрібно підвищити надійність телекомунікаційних мереж, одним із напрямів забезпечення підвищення надійності є ефективне управління ресурсами мереж.

ЛІТЕРАТУРА

1. Гордиенко В.Н., Тверецкий М.С. Многоканальные телекомуникационные системы: Учебник для вузов. − М.: Горячая линия −Телеком, 2005. − 416 с.

2. Кільчицький Є.В. Ефективне управління телекомунікаційними мережами та послугами в екстремальних умовах: підходи до вирішення проблеми//Зв'язок. – 2002. – №2. – с. 21 – 23.

3. Методи підвищення показників якості системи управління телекомунікаційними мережами: Монографія/ Хиленко В.В., Беркман Л.Н., Колченко Г.Ф., Варфоломеєва О.Г. – К.: Норіта-плюс, 2007. – 236 с.

4. Стеклов В.К., Беркман Проектування телекомунікаційних мереж: Підруч. для вищ. навч. закл. за напрямком „Телекомунікації". – К.: Техніка, 2002. – 792 с.

5. Стеклов В.К., Беркман Телекомунікаційні мережі. – К.: Техніка, 2001. – 650 с.

6. Управління телекомунікаціями із застосуванням новітніх технологій: Підруч. для студентів вищ. навч. закл. за напрямом „Телекомунікації"/Кривуца В.Г., Беркман Л.Н., Стеклов В.К. та ін. – К.: Техніка, 2007. – 384 с.

Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Садиков О.І. (ВІТІ НТУУ „КПІ”)
Явіся В.С. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ПОБУДОВИ МУЛЬТИСЕРВІСНОЇ МЕРЕЖІ ДОСТУПУ ЗА ПОКАЗНИКОМ ВАРТОСТІ

Методика побудови мультисервісної мережі доступу за показником вартості дозволяє шляхом послідовних етапів на основі оцінки ринку телекомунікаційних послуг та прогнозу стану економіки провести вибір сценарію побудови мережі доступу за показником вартості.

Мета розробки методика побудови мультисервісної мережі доступу за показником вартості полягає в забезпеченні ефективності прийняття управлінських рішень Оператором зв’язку по проведенню заходів пов’язаних з підтриманню конкурентоспроможності телекомунікаційної компанії та отримання прибутків.

Під ефективністю слід розуміти – одержання найкращого результату від використання наявних ресурсів.

Постановка задачі:

Задано:

– перелік технологій для забезпечення мультисервісного абонентського доступу;

– характеристики експлуатованої мережі доступу та її структура;

– перелік телекомунікаційного обладнання.

Необхідно:

– розробити та вибрати раціональний сценарій побудови мережі доступу за показником вартості;

– розрахувати основні техніко-економічні характеристики мережі доступу.

Обмеження:

– характеристики мережі доступу розраховуються на основі існуючого телекомунікаційного обладнання відомих фірм виробників та згідно вимог керівних документів і ДСТУ;

– час на розробку сценарію та розрахунки техніко-економічних показників визначає Оператор зв’язку.

Основні етапи реалізації методики

1. Визначення вихідних даних.
2. Визначення обмежень та допущень щодо побудови мережі доступу.
3. Оцінка ринку телекомунікаційних послуг. Головною метою такої оцінки є визначення середньої вартості на основні види інфокомунікаційних послуг провідних телекомунікаційних операторів. Результатом є визначення тарифу абонентської плати за надання пакету послуг: $C_{абон} \leq C_{абонрин\ сер}$.
4. Проведення прогнозу стану економіки на визначений період.
5. Розрахунок розмірів прибутку за визначений період.
6. Вибір сценарію побудови мережі доступу.
7. Проектування структури та топології мережі доступу для j-го сценарію.
8. Розрахунок експлуатаційних характеристик мережі доступу для j-го сценарію.
9. Розрахунок вартості реалізації мережі доступу для j-го сценарію та запис результатів до бази даних.
10. Усі сценарії побудови мережі доступу розглянуті.
11. Прийняття рішення щодо побудови мережі доступу за j-м сценарієм.

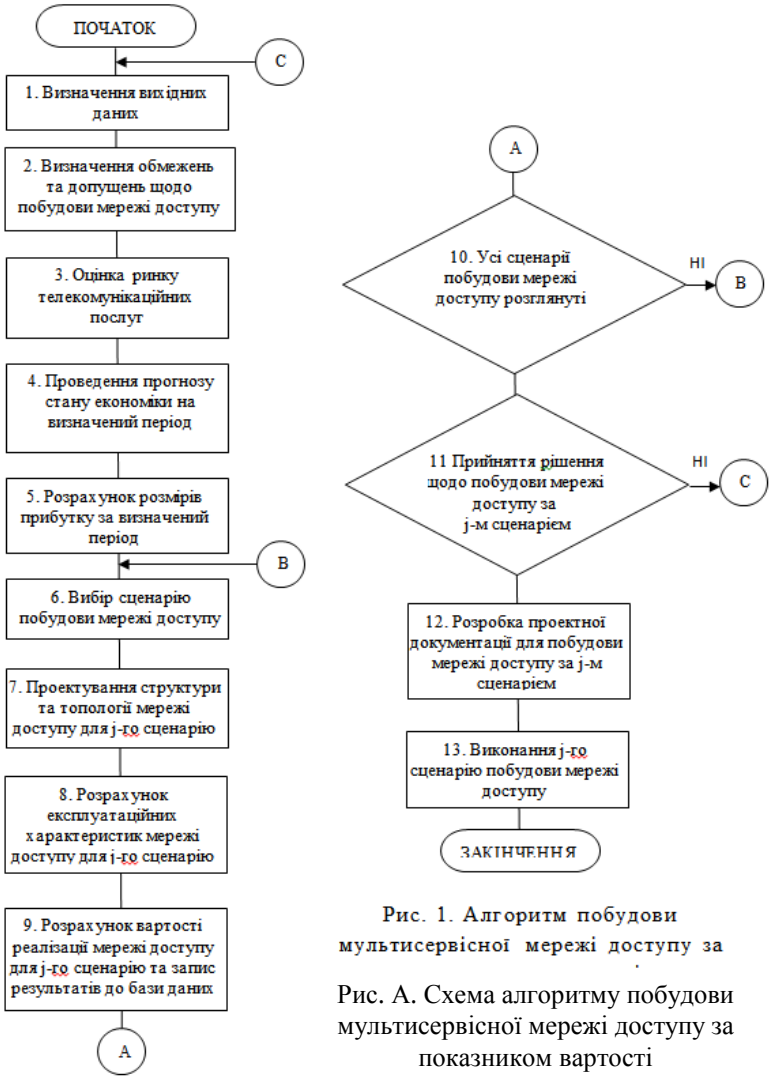


Рис. 1. Алгоритм побудови мультисервісної мережі доступу за

Рис. А. Схема алгоритму побудови мультисервісної мережі доступу за показником вартості

12. Розробка проектної документації для побудови мережі доступу за j-м сценарієм.

13. Виконання j-го сценарію побудови мережі доступу.

Сутність методики побудови мережі доступу за показником вартості відображена в алгоритмі, який представлений на рис А.

Підводячи підсумок можна зазначити, що дана методика не являється закритою.

По мірі появи нових методів або методик рішень задач розрахунку та оптимізації характеристик мережі доступу ця методика може уточнюватись та розширюватись.

ЛІТЕРАТУРА

1. Винницький В.П., Хиленко В.В. Методы системного анализу и проектированиетелекоммуникационныхсетей. – К.: Интерлинк, 2002. – 192 с.

2. Парфёнов Ю.А., Мирошников Д.Г. Цифровые сети доступа. Медные кабели и оборудование. − М.: Эко-Трендз, 2005. − 288 с.

3. Рогинский В.Н., Харкевич А.Д., Шнепс М.А. и др. Теориясетейсвязи: Учебник для вузовсвязи / Под ред. В.Н. Рогинского. – М.: Радио и Связь, 1981. – 428 с.

4. Росляков А.В. Сети доступа. Учебноепособие для вузов. – М.: Горячаялиния – Телеком, 2008. – 96 с.

5. Руководящийтехническийматериал по модернизациисетейдоступа. – СПб.: НТЦ Протей, 2005. – 122 с.

6. Соколов Н.А. Сети абонентскогодоступа: принципыпостроения. – Пермь: ЗАО „ИГ Энтер-профи”, 1999. – 256 с.

7. Соколов Н.А. ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ. Монография в 4-х главах. – М.:Альварес Паблишинг, 2004, – 640 с.

8. Соколов Н.А. Эволюцияместныхтелефонныхсетей. – Пермь: ТОО „Типография Книга”, 1994. – 144 с.

9. Филипс Д., Гарсиа-Диас А. Методыанализусетей. – М.: Мир, 1984. – 496 с.

Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Явіся В.С. (ВІТІ НТУУ „КПІ”)
Фомін М.М. (ВІТІ НТУУ „КПІ”)

ТЕСТУВАННЯ ВІДОМЧИХ ПАСИВНИХ ОПТИЧНИХ МЕРЕЖ

Одне з головних завдань, що стоять перед сучасними телекомунікаційними мережами доступу – так звана проблема „останньої милі”, надання якомога більшої смуги пропускання індивідуальним і корпоративним абонентам при мінімальних витратах.

Цю проблему можна вирішити за допомогою пасивної оптичної мережі – PON (Passive optical network) – технологія пасивних оптичних мереж.

Суть технології PON полягає в тому, що між приймально-передавальним модулем центрального вузла OLT (optical line terminal) і віддаленими абонентськими вузлами ONT (optical network terminal) створюється повністю пасивна оптична мережа, що має топологію дерева. У проміжних вузлах дерева розміщуються пасивні оптичні розгалужувачі (сплітери) - компактні пристрої, які не потребують живлення і обслуговування. Число ONT, підключених до одного OLT, може бути настільки великим, наскільки дозволяє бюджет потужності і максимальна швидкість приймально-передавальної апаратури.

Основні переваги технології PON:

– економія волокон (до 128 абонентів на одне волокно, протяжність мережі до 60 км);

– ефективне використання смуги пропускання оптичного волокна;

– швидкість до 2,488 Гбіт/с по низхідному потоку і 1,244 Гбіт/с по висхідному потоку;

– надійність (у проміжних вузлах дерева знаходяться тільки пасивні оптичні розгалужувачі, не потребують обслуговування);

– масштабованість (деревоподібна структура мережі доступу дає можливість підключати нових абонентів найбільш економічним способом);

– можливість резервування як всіх, так і окремих абонентів;

– гнучкість (використання ATM, як транспорту дозволяє надавати абонентам саме той рівень сервісу, який їм потрібен).

При тестуванні мережі PON є важливими наступні питання:

– реальне загасання в оптичній лінії між центральним вузлом і абонентським пристроєм (діючого або того, що готується до підключення).

– місцезнаходження проблемної ділянки, якщо реальне загасання в лінії виявилося вище очікуваного (розрахункового або опорного).

Для вирішення першого питання досить провести прості вимірювання за допомогою оптичного тестера. Вирішення другого питання більш складне і вимагає застосування оптичного рефлектометра (OTDR), а також певного досвіду розшифровки рефлекторам:

1. Всі необхідні вимірювання повинні проводитися на працюючій мережі PON без відключення абонентів (крім, тестованого). Таке тестування здійснюється на неробочій довжині хвилі із застосуванням додаткових пристроїв (хвильових мультиплексорів DWDM, фільтрів), щоб випромінювання вимірювальної апаратури не вносило перешкод в корисний сигнал.

2. Випромінювання вимірювальної апаратури (тестера, рефлектометра) повинні вводиться у волокно відразу після OLT з використанням хвильового мультиплексора (DWDM). Це випромінювання здатне викликати перешкоди на оптичному приймачі абонентського пристрою, тому перед кожним абонентським пристроєм ONT необхідно встановити фільтр.

Для вимірювання загасання в оптичній лінії між OLT і ONT використовується оптичний тестер на 1625 нм. Передавач тестера підключається до вільного кінця хвильового

мультиплексора на OLT. Приймач тестера підключається до вільного кінця волокна перед фільтром.

При вимірюванні загасання без відключення абонентського пристрою потрібно використовувати не фільтр, а хвильовий мультиплексор на центральному вузлі.

Загасання на довжині хвилі 1625 нм трохи вище, ніж на 1550 і 1490 нм (в середньому на 10%). Тому тестування загасання на довжині хвилі 1625 нм дає оцінку зверху для загасання на робочих довжинах хвиль. Якщо ця оцінка вкладається в допустиму (23 дБ), то загасання на робочих довжинах хвиль свідомо задовольняє вимогам по бюджету. Якщо загасання на довжині хвилі 1625 нм перевищує допустиме значення, то для точного визначення загасання на робочих довжинах хвиль необхідно провести перерахунок на основі паспорту оптичного кабелю.

Вимірювання в PON за допомогою оптичного тестера дозволяє отримати реальне значення загасання на ділянці від OLT до ONT, але не дає відповіді на питання, де знаходиться проблемна ділянка, якщо це згасання виявилося вище очікуваного (розрахункового або опорного). Для локалізації проблемної ділянки використовується більш складний пристрій – оптичний рефлектометр (OTDR).

Рефлектометр з тестовим модулем на 1625 нм підключається до вільного кінця хвильового мультиплексора на OLT. Випромінювання рефлектометра поширюється по дереву PON і за рахунок відображення на перешкодах і зворотного розсіювання в оптичному волокні частково надходить назад на вхід рефлектометра. Таким чином, знімається рефлектограма дерева PON - графік загасання в лінії в залежності від відстані. Кожен пік або стрибок загасання на цьому графіку відповідає певному елементу мережі або події в волокні.

Пропонуємо проводити тестування мережі PON з використанням рефлектометра. Відомо, що після кожної зміни топології мережі (підключення нового абонента, заміни сплітера і т.п.) знімається опорна (еталонна) рефлектограма, яка відповідає нормальному стану мережі. При виявленні проблем в мережі (наприклад, якщо загасання, виміряне оптичним тестером, виявилося вище розрахункового) знімається нова рефлектограма, яка порівнюється з опорною. Нові події на рефлектограмі локалізують місце розташування проблемної ділянки.

За допомогою рефлектометра можна вести моніторинг мережі PON і виявляти деградації волокна ще до того, як виникнуть проблеми. Для цього необхідно регулярно (наприклад, раз на тиждень) знімати рефлектограму мережі і порівнювати її з опорною рефлектограмою. При появі будь-яких відхилень і тим більше нових подій на рефлектограмі необхідно аналізувати їх можливі причини і при необхідності проводити адекватні профілактичні заходи.

Використання даного варіанту тестування PON дозволить підвищити рівень надійності мережі та зменшити час на пошук та виявлення пошкоджень у мережах, що експлуатуються.

ЛІТЕРАТУРА

1. Андрушко Л.М., Вознесенкий В.А., Каток В.Б. и др.Справочник по волоконно-оптическим линиям связи / Під ред. Свечникова С.М. и Андрушко Л.М. – К.: Техніка, 1988. – 239 с.

2. Бейли Д., Райт Э. Волоконная оптика: теория и практика. – М.: ОБРАЗ, 2006. – 320 с.

3. Берлин Б.З. и др.Волоконно-оптические системы связи на ГТС: Справочник – М.: Радиосвязь, 1994. – 160 с.

4. Портнов Э.Л.Оптические кабели связи и пассивные компоненты волоконно-оптических линий связи: Учебноепособие для вузов. – М.: Горячаялиния-Телеком, 2007. – 464 с.

5. Руководство по монтажу соединительных муфт на оптических кабелях связи марок ОЗКГ-2 и ОЗКГ-3. – М.: ССКТБ, 1990.

Васильців А.А.(ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В.(ВІТІ НТУУ „КПІ”)
Лук’янчук І.В .(ВІТІ НТУУ „КПІ”)

АВТОМАТИЗАЦІЯ ПОШУКУ ПОТЕНЦІЙНО-НЕБЕЗПЕЧНИХ ДЕФЕКТІВ РЕАКЦІЇ ПРОГРАМ ДЛЯ ВПРОВАДЖЕННЯ КІБЕРНЕТИЧНОГО ВПЛИВУ

На сьогоднішній час інформаційні технології впроваджуються у сфери діяльності людини. Не виключенням є військові організації, від рівня надійності яких напряму залежить національна безпека країни. Однак з стрімким розвитком виникає проблема захисту від комп’ютерних атак, техніка яких також постійно розвивається.

Для проведення кібернетичного впливу необхідна попередня інформаційна підготовка, одним із можливих елементів якої є пошук потенційно-небезпечних дефектів програм, які можна використати для проведення атаки.

На сьогодні існує цілий ряд засобів аналізу коду програм, як вихідного так і в двійковому вигляді, але всі вони дають результат у вигляді інформаційних повідомлень про можливу вразливість у тому чи іншому місці програми, інколи з рекомендаціями для усунення, частіше всього не враховуючи програмний засіб як цілісну систему взаємозалежних елементів виконання – що ускладнює пошук шляхів використання цих вразливостей в інтересах кібернетичного впливу, а це в свою чергу є не зовсім прийнятним результатом в умовах, коли від цього залежить хід політичних, економічних та інших міжнародних процесів в плані інтересів держави. Даним програмним засобам не вистачає математичного апарату, який би враховував не тільки особливості окремих елементів коду але й зробив би аналіз їх виконання на взаємодію в ході виконання програми.

Аналізатор вихідних текстів програми, який візуалізував взаємозв’язок окремих елементів програми з потенційно-небезпечними функціями – які призводять до порушення цілісності адресного простору процесу (зокрема, найбільш поширений тип вразливостей „переповнення буферу”) – це допомогло б краще сприймати адресний простір коду та його вразливі ділянки коду, але не дозволяє враховувати можливий хід виконання коду – це дозволило би звузити варіанти пошуку ділянок, які можна використати для реалізації кібернетичного впливу.

Як відомо, математичний апарат мереж Петрі дозволяє проводити моделювання систем паралельного функціонування, що дає змогу в поєднанні з кінцевими автоматами накладати так звані контрольні точки на потенційно-небезпечні ділянки коду – при переході моделі програми в певну точку виконання, постійно слідкуючи за її елементами пам’яті можна знайти вразливу ділянку а також отримати повний звід щодо її використання – це досягається за допомогою попереднього створення шаблонів потенційно-небезпечних функцій, які потребують додаткового контролю при виконанні.Для поєднання цих двох складових пошуку шляхів використання вразливостей, пропоную представляти модель коду програмного забезпечення у вигляді орієнтованого графа, вершинами якого будуть функції, реалізовані в коді, ребрами – переходи до інших функцій, при переході з однієї вершини на другу буде відбуватись порівняння стану змінних та і у випадку збігу з шаблоном мережі Петрі – будуватиметься перелік рекомендацій щодо використання вразливої ділянки коду на основі взаєморозміщення та взаємовпливу елементів програми в адресному просторі під час її виконання – а після цього відбуватиметься обхід елементів всього графу з метою виявлення вразливостей та аналізу вимог для їх використанння.

Отже, враховуючи сучасні тенденції кібернетичного впливу, можна зробити висновок, що дана пропозиція є перспективною та потрібною для впровадження з метою забезпечення кібернетичної стійкості в сфері інформаційної боротьби а також для впровадження в навчальний процес при підготовці фахівців в даній сфері.

д.т.н. Васюта К.С. (ХУПС)
Сірик А.О. (в/ч А1906)
Озеров С.В. (ХУ ПС)

ПІДВИЩЕННЯ СКРИТНОСТІ СИСТЕМ ВІЙСЬКОВОГО РАДІОЗВ'ЯЗКУ ЗА РАХУНОК ВИКОРИСТАННЯ СКЛАДНИХ ХАОТИЧНИХ СИГНАЛІВ

Проблема забезпечення скритності систем військового радіозв'язку, принципом якої є робота „під шум", являється актуальною і досі не знайшла свого вирішення у більшості прикладних завдань. Вирішенню цієї задачі сприяє використання різних методів і засобів, серед яких важливу роль відіграють інформаційні носії, в якості яких використовуються випадкові і хаотичні процеси, а також сигнали складної форми та оптимальні методи їх обробки. На даний час в системах військового зв'язку для скритої роботи використовують широкосмугові сигнали з великою інформаційною місткістю. Проаналізувавши скритність широкосмугових сигналів, стає зрозуміло, що вони не є сигналами, які б забезпечували роботу „під шум" і тому повною мірою не виконуються вимоги щодо скритності систем, у яких вони використовуються.

Альтернативне вирішення проблеми забезпечення скритності дає застосування шумоподібних сигналів, що формуються нелінійними динамічними системами, які демонструють хаотичну поведінку. Такі сигнали не відрізняються від шуму при візуальному аналізі та мають набір специфічних властивостей, що роблять їх привабливими з точки зору процесів обробки і побудови систем зі скритою роботою. В основі цих систем лежать явища синхронізації генераторів динамічного хаосу. Динамічним хаосом називають складні періодичні коливання, що породжуються нелінійними системами. Ці коливання мають властивості, притаманні звичайним випадковим процесам, такими як суцільний спектр потужності і експоненціально спадаючою кореляційною функцією та непередбачуваністю на великих інтервалах часу. Хаотичні коливання, на відміну від випадкових процесів, мають такі динамічні властивості, як висока чутливість до початкових умов і параметрів та експоненціальний розгін близьких фазових траекторій.

Використання динамічного хаосу в системах передачі інформації дозволяє отримати наступні переваги:

– створення хаотичних коливань за допомогою достатньо простих динамічних схем, дозволяє забезпечити велику кількість різноманітних закритих каналів зв'язку;

– збільшення швидкості передачі за рахунок використання декількох інформаційних параметрів хаотичного генератора;

– можливість самосинхронізації приймача і передавача;

– можливість отримання різноманітних методів введення повідомленнь в хаотичний сигнал. Шумоподібність і самосинхронізація систем зв`язку, заснованих на хаосі, дають потенційні переваги над традиційними системами з розширенням спектру, що базуються на псевдовипадкових послідовностях. Крім того, вони дозволяють отримати простішу апаратну реалізацію з більшою енергетичною скритністю та забезпеченням високої оперативності.

До теперішнього часу, на основі хаосу запропоновано декілька моделей для розширення спектру інформаційних сигналів і побудови передавачів і приймачів з простою архітектурою. Проте, ще не досить глибоко досліджені особливості реалізації таких моделей в системах військового зв`язку, що і представляє інтерес для подальшого розвитку цього напрямку.

ЛІТЕРАТУРА

1. Дмитриев А.С., Панас А.И. Динамический хаос: новые носители информации для систем связи. – М.: Издательство Физ.-Мат. литературы, 2002.–252 с.

2. Малинецкий Г.Г. Хаос. Структуры. Вычислительный эксперимент: Введение в нелинейную динамику. М., 2002.

Волосян Ю.М. (ВІТІ НТУУ „КПІ”)
Голь В.Д. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ВИМІРЮВАННЯ ПАРАМЕТРІВ МЕРЕЖІ *AON* З ВИКОРИСТАННЯМ ЗАСОБІВ *OTDR*

Волоконно-оптичні системи передачі (ВОСП) є практично ідеальним рішенням для забезпечення передачі значних інформаційних потоків на великі відстані, і є адекватною реакцією на зростаючі обсяги трафіку, пов’язані зі стрімким процесом інформатизації суспільства.

У ВОСП сьогодні все частіше використовується технологія спектрального розподілу каналів (СРК), при якій в одному оптоволокні передають декілька оптичних сигналів з різними довжинами хвиль. Пристрої такого роду дозволяють по одній парі оптичних волокон передавати трафік різних протоколів (*SDH/IP/ATM*) з різними швидкостями. Найголовніше завдання перспективної технології спектрального розподілу каналів – модернізація та розширення можливостей створених мереж для істотного підвищення їх пропускної здатності з залученням мінімуму коштів.

Використання СРК дозволяє створювати *AON* (*All Optical Network* – повністю оптичну мережу). Одним з завдань даної технології є доведення оптичного сигналу (волокна) до кінцевого користувача. Втілення *AON* потребує застосування відповідної функціональної елементної бази, складність такої бази та велика розгалуженість і структурність створюваних мереж викликає необхідність подальшого вдосконалення методів їх контролю. Високу ефективність у рішенні даного питання показує метод заснований на застосуванні вимірювання засобами *OTDR* (*Optical Time Domain Reflectometer*). *OTDR* дозволяє визначати місцезнаходження дефектів і пошкоджень, вимірювати рівень втрат сигналу в будь-якій точці оптичного волокна. *OTDR* реалізується за допомогою оптичного рефлектометру (ОР). Сьогодні ОР – основні вимірювальні прилади для інсталяції та технічного обслуговування ліній передачі із структурою точка-точка.

Під час тестування ОВ розрізняють методи: одночасного та різночасного тестування волокон багатоточкових мереж; тестування по вільному („темному”) чи по активному волокну. Кожен з методів має свою точність та обмеження, отже доцільно використовувати системи автоматизованого контролю оптичних волокон, які мають бути адаптовані до потреб певного замовника. Такі системи потребують створення.

В основі пропонованого методу – принцип використання оптичного рефлектометру (ОР) для проведення рефлектографічних вимірювань із наступним порівнянням реально отриманих результатів часу затримки відбиття та рівня відбитого сигналу з параметрами, отриманими в результаті машинного моделювання *OTDR* вимірювань. За допомогою розробленої методики існує можливість проводити аналіз прогнозу працездатності, виявляти і усувати несправності *AON*.

Отже, розвиток телекомунікаційних технологій, що використовують волоконно-оптичні лінії зв’язку в глобальних мережах передачі даних і в комутованих телефонних мережах загального користування, вимагає вирішення задачі контролю ВОСП з метою скорочення часу на відновлення зв’язку через обриви волокна та для прогнозу можливих порушень, викликаних зміною в часі характеристик компонентів ВОСП.

Найбільш ефективно дане завдання може бути вирішене за допомогою систем автоматизованого видаленого контролю оптичних волокон з використанням порівняння реальних результатів вимірювань та машинного моделювання *OTDR*.

Волощук А.В.(ВІТІ НТУУ „КПІ”)
Лук’янчук І.В.(ВІТІ НТУУ „КПІ”)

ОСОБЛИВОСТІ ТА ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕХНІЧНОЇ ЗБРОЇ

Останнім часом на сторінках газет і журналів, у виступах вчених-теоретиків і практиків все частіше зустрічаються такі поняття як інформаційний вплив, інформаційна війна, інформаційна зброя. Більш того, висловлюються думки, що з настанням третього тисячоліття лідерство в світі буде визначатися не стільки економічним потенціалом держави, скільки його здатністю контролювати інформаційні процеси.

Інформаційна зброя, відповідно до одного з існуючих визначень – це комплекс програмних і технічних засобів, призначених для контролю інформаційних ресурсів об’єкта впливу і втручання в роботу його інформаційних систем. Інформаційну зброю можливо класифікувати за методами впливу на інформацію, інформаційні процеси та інформаційні системи супротивника. Цей вплив може бути фізичним, інформаційним, програмно-технічним або радіоелектронним.

В **інформаційно-технічній боротьбі** головними об’єктами нападу і захисту є системи управління та зв’язку, телекомунікаційні системи, різні радіоелектронні засоби. Саме тут на самому початку і сформувалося поняття „інформаційна зброя”, яка отримала широке поширення після завершення воєнної операції проти Іраку в 1991 р. Тоді вирішальний внесок у поразку Іраку внесло комплексне застосування засобів розвідки, управління, зв’язку, навігації та радіоелектронної боротьби, сукупність яких і була визначена як інформаційна зброя театру військових дій.

Головними прийомами інформаційних впливів тут є закладні пристрої „логічні бомби”, комп’ютерні віруси, спеціальні програми та інші засоби руйнування, придушення, фальсифікації інформації і засобів захисту від них.

В **інформаційно-психологічній боротьбі** головними об’єктами нападу і захисту є психіка особового складу Збройних силових структур, населення протиборчих сторін, системи формування громадської думки і прийняття рішень.

Серед основних засобів впливу на людину слід зазначити, зокрема, психотропну зброю (пси-зброю). Її дія заснована на використанні дистанційного впливу пси-обдарованого оператора (екстрасенса) на іншу людину з метою коригування поведінки або впливу на фізіологічні функції. Існує також можливість створення відповідних технічних пристроїв, наприклад різного роду бойових психотропних пристроїв (генераторів).

Інформаційні методи впливу реалізуються за допомогою всієї сукупності засобів масової інформації та глобальних інформаційних мереж типу „Інтернет”, станціями голосової дезінформації. Так як основним елементом інформаційної інфраструктури є люди, мотивація діяльності яких базується на їх фізіологічних, соціальних та інформаційних потребах, то правильно розраховане застосування так званих інформаційно-психологічних методів впливу надає прямий вплив на рівень безпеки держави.

Отже, очевидно, що та сторона, яка має в своєму розпорядженні великий об’єм інформації про супротивника, краще підготовлена до війни. Важливо враховувати особливості національної культури супротивника, способи подачі і сприйняття ним інформації.

В даний час знання того, як конфронтуюча сторона використовує інформаційні системи (комунікаційні мережі, бази даних), а також алгоритми систематизації знань і прийняття рішень, має виняткове значення.

Восколович О.І. (ВІТІ НТУУ „КПІ”)

РЕЗУЛЬТАТИ ПЕРЕВІРКИ АДЕКВАТНОСТІ ІМІТАЦІЙНОЇ МОДЕЛІ СИСТЕМИ MIMO З ПСЕВДОВИПАДКОВОЮ ПЕРЕСТРОЙКОЮ РОБОЧОЇ ЧАСТОТИ

Відомчі засоби радіозв’язку (ЗРЗ) повинні забезпечувати передачу інформації у складній радіоелектронній обстановці, а саме умовах багатопроменевого просторового каналу та при наявності в каналі зв’язку навмисних завад. Одним з перспективних шляхів вирішення проблеми є використання системи зв’язку з рознесеними передавальними і приймальними антенами – системи MIMO (*multiple-input multiple-output*) з псевдовипадковою перестройкою робочої частоти (ППРЧ) [1]. Дана система функціонує з використанням методики управління параметрами радіозасобів MIMO з псевдовипадковою перестройкою робочої частоти, запропонованої в [2]. Сутність якої полягає в управлінні режимами роботи ЗРЗ, а саме режимом роботи MIMO (режими просторового мультипексування, просторового рознесення власних каналів та комбінований), режимом роботи ППРЧ (кількість частотних підканалів, швидкість перестроювання) та сигнально-кодових конструкцій в залежності від завадової обстановки.

Для оцінки ефективності запропонованої методики було проведено імітаційне моделювання роботи системи MIMO з ППРЧ при різному ступені дії навмисних завад, що діють на канал зв’язку. Імітаційне моделювання проводилось у програмному середовищі *MathCad* [3] із використанням отриманих в [2] математичних співвідношень.

Таким чином, виникає задача проведення перевірки адекватності імітаційної моделі системи MIMO з псевдовипадковою перестройкою робочої частоти.

Адекватність імітаційнної моделі системи радіозв’язку з MIMO та ППРЧ може бути підтверджена шляхом порівняння результатів, які отримані за допомогою розробленої моделі, і результатів, які отримані за допомогою відомих аналогічних імітаційних моделей. В якості подібної була обрана імітаційна модель, що представлена групою *Iterative Solutions*. Ця модель дозволяє проводити моделювання характеристик завадостійкості майже всіх відомих мобільних систем передачі інформації.

Адекватність моделі перевірялася за допомогою критерія Фішера.

В результаті перевірки адекватності імітаційної моделі, розраховане значення критерія Фішера, що визначалось як відношення дисперсії адекватності до дисперсії відтворення з порівнянням цього значення з критичним (табличним).

При моделюванні характеристик завадозахищеності ЗРЗ MIMO з ППРЧ в якості значень кількість ступенів вільності *m*, *n* обрані $m = 10$, $n = 7$, рівень значущості *q* обрано $q = 0{,}05$, критичне значення $F_{\text{кр.}} = 3{,}4$.

При порівнянні значень було виявлено, що отримані значення не перевищують критичних (табличних) значень, таким чином модель-замісник вважається адекватною моделі-оригіналу.

Проведені дослідження доказали адекватність використаної статистичної моделі.

ЛІТЕРАТУРА

1. Восколович О. І. Аналіз параметрів при проектуванні радіомодемів спеціального призначення з багаточастотними сигналами / О. І Восколович // Тези V – науково-практичного семінару ВІТІ НТУУ „КПІ”, 2009. – С. 93.

2. Восколович О. І. Методика управління параметрами радіозасобів MIMO з псевдовипадковою перестройкою робочої частоти / О. І. Восколович, О. В. Кувшинов// Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2011. – Вип. 2 – С. 12 – 22.

3. Кирьянов Д. В. Самоучитель Mathcad 11: Монография / Д. В. Кирьянов – СПб.: БХВ-Петербург, 2003. – 560 с.

Ганжа Д.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Кисельов Р.В. (ВІТІ НТУУ „КПІ”)

ТРОПОСФЕРНА ЛІНІЯ ЗВ’ЯЗКУ ПРИ ДТР ТА ЗВУКОВИХ ХВИЛЯХ

Для побудови існуючих військових мереж тропосферного зв’язку використовуються тропосферні лінії, які мають складну та громіздку побудову за рахунок розгортання великої кількості станцій. Тропосферні мережі зв’язку мають великий час розгортання і недостатньо високу надійність, для підвищення якої застосовується 100% резервування основного обладнання. Вихід з ладу однієї станції може привести до втрати зв’язку на лінії максимальної довжини. В станціях, які будують тропосферну лінію використовуються антени з підвищеними геометричними параметрами, що забезпечують необхідний коефіцієнт підсилення антени. Це значно ускладнює їх конструкцію при розгортанні лінії зв’язку, зменшують мобільні станції та підвищують час побудови тропосферна радіолінія. Велике значення для суттєвого зменшення масо-габаритних показників, поліпшення якості зв’язку та підвищення ефективності боротьби із завмираннями мають технічні рішення, що можуть використовуватися в сучасних тропосферних станціях, реалізованих з використанням поліпшеної елементної бази, новітніх технологій; це – скануючи антенні решітки, багатопроменеві фазові антенні решітки, а також використання методів створення штучних неоднорідностей на шляху тропосферного розповсюдження. За допомогою цих рішень може бути розроблена перспективна та більш ефективна мережа зв’язку.

В роботі детальніше розглядається саме метод створення штучних неоднорідностей за допомогою звукової хвилі. Швидкість звукової хвилі звичайно на п’ять порядків менша швидкості електромагнітної хвилі у просторі. Таким чином, електромагнітна хвиля, що падає на звукову хвилю, зустрічає фактично статичну фазову решітку з періодичністю звукової хвилі λ. Електромагнітна хвиля, що має часову і просторову когерентність (несуча), падаючи на таку фазову решітку, дифрагує в дальній зоні з утворенням декількох порядків дифракції. Така акустоелектромагнітна взаємодія, в якій акустична хвиля розглядається як фазова решітка, може бути покладена в основу стаціонарного дальнього тропосферного розсіювання електромагнітна хвиля.

На трасі тропосферна радіолінія в області пересікання діаграм направленості антен формується акустичний фронт від джерела акустичних коливань: динамічні сирени, які на частотах 400Гц створюють звуковий тиск в 300 Па і мають відносно високі к.к.д. сирена С-34 має к.к.д. 27%.

Суттєво поліпшити ефект розсіювання електромагнітна хвиля на акустичній решітці шляхом застосування аерозолів дисперсних систем з газоподібним середовищем і твердою або рідкою електропровідністю дисперсною фазою. Ввід аерозолів в поле акустичної хвилі призводить до акустичної коагуляції процесу зближення і укрупнення звішених в газі мілких твердих часток (наприклад, металевого алюмінієвого пилу).

Звукове поле сприяє розповсюдженню аерозолів вздовж розповсюдження акустичної хвилі і викликає сили, під дією яких відбувається зближення часток. Для створення звукового поля можна використовувати акустичні сирени і свистки, що забезпечують інтенсивність звукової хвилі 145…160дБ в діапазоні частот від 400 до 5 кГц.

Взаємодія (перекриття) електромагнітна хвиля та звукової хвилі може бути покладено в основу стаціонарного дальнього тропосферного розповсюдження.

Головко Д.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)

МОДЕЛЬ РОЗПОДІЛУ ПРАВ ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ СУПРОВОДУ НАВЧАЛЬНОГО ПРОЦЕСУ

Основною проблемою інформаційних систем супроводу навчального процесу (ІС СНП) є розподіл прав доступу (*access rights*). Права доступу до інформації – сукупність правил, що регламентують порядок і умови доступу суб’єкта до інформації, встановлених правовими документами чи власниками інформації. Права доступу визначають набір прав (читання, запис, виконання), дозволених для виконання суб’єктам (наприклад, користувачам системи) над об’єктами даних. Аналізуючи сучасні ІС СНП більшість з яких контролюють права на рівні типів об’єктів системи, або безпосередньо вказувати права для пари користувач-запис. Такий механізм реалізується розробником ІС СНП в код програми.

Для сучасних ІС СНП необхідно вказувати динамічні права, тобто не вручну вказувати доступне множину об’єктів, а описувати цю множину за допомогою визначеної логічної умови. Найбільш поширеним підходом до вирішення зазначеної проблеми є метод, заснований на ролях. Пропонується підхід, який використовує досить простий і гнучкий механізм, реалізуються за допомогою динамічної генерації специфічних *SQL* – запитів в залежності від заданих параметрів.

При прийнятті рішення про надання доступу звичайно аналізується наступна інформація:

ідентифікатор суб’єкта (ідентифікатор користувача, мережеву адресу комп’ютера). Подібні ідентифікатори є основою довільного (або дискреційного) управління доступом;

атрибути суб’єкта (мітка безпеки, група користувача). Мітки безпеки – основа примусового (мандатного) управління доступом.

Суть підходу полягає в динамічній генерації *SQL* запитів – опис правил генерації здійснюється розробниками спеціалізованої конфігурації, а вхідні параметри для процедури генерації вказують адміністратори системи.

Для кожного типу об’єкта існує свій набір прав, тому можливо виділити такі:

1. Права, які на виході для кожного користувача повинні повернути доступне для нього безліч об’єктів.

2. Права, які для пари користувач – об’єкт повинні повернути булеве значення: чи має право на виконання операції чи ні.

Другий тип прав можливо звести до першого шляхом використання процедури приналежності цього об’єкта до дозволенного для користувача об’єктів. Нехай – множина об’єктів типу *i*. Y_{ijk} – оператор доступних об’єктів типу *i* права *j* для суб’єкта *k*. $A_{ijk} = Y_{ijk}(A_i)$ – множина об’єктів типу і доступних суб’єкту (користувачу або групі) *k* для права *j*. Для визначення права типу 1 і використовується дане безліч. Для визначення права типу 2 перевіряємо умову, $Y \in Y_{ijk}$, де $Y \in A_i$. Якщо ця умова виконується, то суб’єкт *k* має право виконати операцію *j* над цим об’єктом.

Введення класів та підкласів доступу суб’єктів до об’єктів контролю доступу забезпечує можливість гнучкої та динамічної зміни прав доступу суб’єктів до об’єктів при коригуванні політики безпеки в ІС СНП.

На основі наведених міркувань описана підхід щодо реалізації моделі розподілу прав доступу в ІС СНП. Дана модель значно поліпшить захист інформації від несанкціонованого доступу та коригування інформації в ІС СНП. Суть підходу полягає у динамічній генерації *SQL* запитів – опис правил генерації здійснюється розробниками спеціалізованої конфігурації, а вхідні параметри для процедури генерації вказують адміністратори системи.

к.т.н. Горбенко В.І. (ВІТІ НТУУ „КПІ”)
Картавих В.Ю. (ВІТІ НТУУ „КПІ”)

МЕТОД ВИЗНАЧЕННЯ ПАРАМЕТРІВ МЕРЕЖЕВОГО ТРАФІКУ ПІДСИСТЕМИ МОНІТОРИНГУ ІНФОРМАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ТЕОРІЇ ФРАКТАЛІВ

Сучасні тенденції розвитку інформаційних мереж спрямовані на застосування протоколів з комутацією пакетів і витиснення застарілих технологій комутації каналів. Ці тенденції забезпечують розвиток сучасних інформаційних технологій, таких як передача голосу через *IP* протокол (*VoiceOverIP*), реалізація трансляції телебачення через інтернет (*IP TV*) та багатопротокольна комутація за мітками (*MultiProtocol Label Switchig MPLS*). Ці тенденції актуальні й для інформаційних мереж спеціального призначення (ІМСП), в яких активно застосовуються протоколи передачі даних з комутацією пакетів стеку протоколів *TCP/IP*. Для здійснення управління мережевим обладнанням у *TCP/IP* застосовується протокол *SNMP*. Виробники телекомунікаційного обладнання і розробники операційних систем активно підтримують даний протокол різних версій, який став стандартом дефакто управління мережами. Таким чином, перспективою розвитку ІМСП є багатопротокольна мережа з комутацією пакетів на базі стеку протоколів *TCP/IP*, управління якою здійснюється за допомогою програмного комплексу, що застосовує *SNMP* протокол для моніторингу мережевих елементів і дистанційного управління ними. Даний протокол підтримує два режими роботи. Перший реалізує метод регулярного збору інформації про стан об’єкта. Другий інформує підсистему моніторингу про встановлення параметрів у відповідні значення, зазделегідь визначені адміністратором мережі. При застосуванні протоколу *SNMP* для передачі службової інформації використовуються телекомунікаційні можливості самої ІМСП. При цьому мережевий елемент може виступати як менеджер підсистеми моніторингу і здійснювати контроль за працездатністю мережі безпосередньо, наприклад з використанням технології *IP SLA* світового виробника комутаційного обладнання *CISCO*.

Виходячи з вище наведеного, актуальною є задача визначення параметрів мережевого трафіку, що буде генеруватися підсистемою моніторингу, під час її стаціонарного режиму роботи. Сучасні дослідження в напрямках моделювання мережевого трафіку мереж з комутацією пакетів спрямовані на застосування теорії фракталів для розрахунку параметрів, що характеризують трафік. У них доведена неможливість застосування класичних методів теорії телетрафіку при моделюванні мереж із комутацією пакетів, обгрунтована самоподібність трафіку в цих мережах та запропоновані методи визначення параметрів. Ці методи призначені для розрахунку характеристик сумарного трафіку ІМСП – складні та потребують велокого обчислювального ресурсу для своєї реалізації..

У доповіді пропонується метод визначення параметрів мережевого трафіку підсистеми моніторингу ІМСП на основі теорії фракталів. В основу методу покладена модель самоподібного трафіку, яка дозволяє розрахувати параметри трафіку підсистеми моніторингу. Відмінністю методу є декомпозиція загального трафіку ІМСП на дві складові: трафік програмно-технічних комплексів ІМСП та трафік підсистеми моніторингу. Це дає змогу визначити основні параметри трафіку підсистеми моніторингу, а саме об’єм службового трафіку, його інтенсивність, час затримки тощо. Урахування корисного трафіку при визначенні параметрів підсистеми моніторингу дозволяє створити алгоритми динамічного переконфігурування підсистеми моніторингу в залежності, від потреб кінцевих користувачів, що зменшить вплив підсистеми моніторингу на виконання основних завдань ІМСП. Таким чином, застосування теорії фракталів дозволяє побудувати адекватну модель трафіку, яка генерується підсистемою моніторингу, врахувати завантаження мережі корисним трафіком і його вплив на роботу підсистеми моніторингу. Існування адекватної моделі мережевого трафіку підсистеми моніторингу дозволить проводити теоретичні розрахунки завантаження мережі підсистемою моніторингу без експериментів.

к.т.н. Горьков В.К. (НУОУ)
к.т.н. Савісько П.А. (НУОУ)

КЛАСИФІКАЦІЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ) ЗБРОЙНИХ СИЛ США

В сучасних умовах основним фактором досягнення переваги над противником є: впровадження у війська інформаційних і нанотехнологій; використання космічних навігаційних та розвідувальних систем; активне проведення інформаційно-психологічних заходів; застосування зброї на нових фізичних принципах; перехід до адаптивних форм воєнних дій. Ці фактори зумовили розробку в США концепції майбутніх війн шостого і сьомою покоління – концепції ведення воєнних дій у єдиному інформаційному просторі або з використанням об'єднаних інформаційно-командних мереж (NCW-Network-Centric Warfare – бойові дії з опорою на мережеві системи управління).

Відповідно до цієї концепції передбачається за допомогою впровадження у війська передових інформаційних технологій поєднувати розосереджені у великому бойовому просторі різнорідні сили і засоби (особовий склад; органи і пункти управління, органи бойового забезпечення; озброєння і військову техніку наземного, повітряного і морського базування) у формування з високою мережевою архітектурою – глобальні і локальні інформаційні мережі.

За оцінками експертів Пентагону ці формування в порівнянні з традиційними будуть мати безумовні переваги і забезпечувати:

– створення в реальному масштабі часу єдиної картини оперативно-тактичної обстановки;

– істотне скорочення часу доведення даних про важливі об–єкти і цілі супротивника від систем виявлення до засобів вогневої поразки;

– значне випередження супротивника в прийнятті і виконанні рішень, плануванні воєнних дій;

– швидку концентрацію розосереджених у бойовому просторі різних засобів поразки для нанесення ударів по важливих об’єктах та цілях супротивника.

Очікується, що в результаті реалізації цих можливостей бойова ефективність формувань з мережевою архітектурою в порівнянні з існуючими зросте багаторазово.

На даний час, в рамках концепції мережоцентричних війн в ЗС США створюється єдина глобальна мережоцентрична система, яка об’єднає розосереджені в єдиному бойовому просторі JWS (Joint Warfighting Space) види ЗС та забезпечить горизонтальну і вертикальну інтеграцію сил і засобів. Мережоцентрична система являтиметься інструментом реалізації концепції NCW. Основними складовими концепції NCW є мережоцентричні сили – засоби ураження, розвідки і зв’язку національних (коаліційних) збройних сил країн-учасниць мережоцентричної війни, інтегровані в єдиний розвідувально-ударний комплекс без територіального (географічного) зосередження сил і засобів. Сили, які приймають участь в мережоцентричних війнах, являються високоінтелектуальними, що означає можливість їх самосинхронізації, автономного функціонування, самостійного прийняття оптимального рішення на застосування засобів ураження і оперативного перенацілювння засобів ураження відповідно до змін бойової обстановки.

В рамках Net-Centric Warfare поняття театру воєнних дій трансформовано в поняття єдиний бойовий простір JWS (Joint Warfighting Space). Концепція Net-Centric Warfare являє собою технологію війн революційно нового типу, яка передбачає тотальну комп’ютеризацію сил і засобів в єдиний інформаційно-управляючий комплекс, який забезпечує гіпершвидкий обмін інформацією між складовими системи з метою оптимального застосування сил і засобів.

В США системи АСУ умовно позначаються CnX (Cn – позначення інформаційних систем класу C2, C3, C4, C5, що прийняті для узагальнення, n – кількість компонентів цієї

системи, а X…– інші її компоненти, що починаються з літер, відмінних від „C”). Це дозволяє поєднати процеси збору, обробки, передачі, відображення і використання інформації для підготовки та ведення бойових дій з максимальною ефективністю.

Основне призначення інформаційних систем (ІС) класу CnX полягає у всебічному забезпеченні командування та оперативного складу інформацією не лише про свої сили та війська, а й про сили противника у певній оперативній обстановці.

Метою створення та застосування таких систем є досягнення інформаційної переваги над противником на певному рівні оперативних дій. Найпростішими ІС є системи С2 або C&C. Це англомовне скорочення має наступну повну форму: Command and Control System – система командування та управління. Наведена у таблиці 1 інформація показує, що ІС командування та управління (С2) з часом ускладнюється шляхом поєднання з засобами зв’язку, застосування комп’ютерів (як індивідуальних засобів інформатизації та комунікації окремих військовослужбовців), взаємодії із засобами розвідки, спостереження та розпізнавання. Вони поступово перетворюються на системи дистанційного управління вогневими засобами, функціонально сумісними з подібними ІС.

Класифікація основних інформаційних систем

Таблиця 1

Скорочена назва	Англомовна назва	Переклад
C^2/C&C	Command and Control System	Система командування та управління
C^2IS	Command, Control and Information System	Система командування, управління та інформації
C^3	Command, Control and Communication System	Система командування, управління та зв’язку
C^3I	Command, Control, Communication and Intelligence System	Система командування, управління, зв’язку та розвідки
C^4	Command, Control, Communication and Computers System	Система командування, управління, зв’язку та комп’ютерів
C^4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance System	Система командування, управління, зв’язку, комп’ютерів, розвідки, спостереження та розпізнавання
C^4I	Command, Control, Communication, Computers and Intelligence System	Система командування, управління, зв’язку, комп’ютерів та розвідки
C^4I^2	Command, Control, Communication, Computers, Intelligence and Interoperability System	Функціонально сумісна система командування, управління, зв’язку, комп’ютерів та розвідки
C^5I	Command, Control, Communication, Computers, Combat and Intelligence System	Система командування, управління, зв’язку, комп’ютерів, бою та розвідки

Наведена у таблиці інформація показує, що ІС командування та управління (С2) з часом ускладнюється шляхом поєднання з засобами зв’язку, застосування комп’ютерів (як індивідуальних засобів інформатизації та комунікації окремих військовослужбовців), взаємодії із засобами розвідки, спостереження та розпізнавання. Вони поступово перетворюються на системи дистанційного управління вогневими засобами, функціонально сумісними з подібними ІС.

к.т.н. Горьков В.К. (НУОУ)
к.т.н. Савісько П.А. (НУОУ)

МЕТОД ДІГРАМНОГО СТИСКУ ТЕКСТОВОЇ ІНФОРМАЦІЇ ПРИ АВТОМАТИЗАЦІЇ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ПІДСИСТЕМАХ АСУ

Одним з питань, що можливо вирішувати практично при створенні автоматизованих інформаційних систем, є стиск даних – скорочення неминучої надмірності подання інформації в технічних засобах автоматизації.

Природа цієї надмірності пов'язана з дискретністю технічних пристроїв, надмірністю семіотичної системи подання інформації й з недосконалістю проектування структур даних.

Особливості подання інформації в ЕОМ дозволяють виділити чотири види надмірності даних текстових документів:

1. Статистична надмірність за рахунок подання нерівно ймовірних символів даних кодовими комбінаціями фіксованої довжини.

Дослідження подання текстів різних інформаційних областей в технічних засобах автоматизації показує, що вони кодуються з статистичною надмірністю 40 – 43 % відсотків.

2. Ергодична надмірність. Пов’язана з кодуванням послідовних символів без обліку їхніх ергодичних властивостей (присутність ергодичной надмірності – 11–13 %).

3. Надмірність використання потужності коду ЕОМ (до 25 %).

4. Надмірність ланцюжків ідентичних символів, яка характерна для документів табличних форм, – 5 – 8 %.

Як показує досвід, ефективне скорочення надмірності в послідовностях даних досягається конструюванням алгоритмів стиску з урахуванням конкретних видів надмірності даних і їхніх характеристик.

Нижче пропонується один з можливих способів скорочення надмірності даних в АСУ – метод діграмного стиску текстової інформації з максимальним використанням потужності коду ЕОМ, що реалізує ідею кодування блоками довжиною два символи й орієнтований на скорочення всіх видів надмірності даних.

Опис методу

Нехай є код ЕОМ, що може розглядатися як безліч B потужності $N: B\{b_j\}$, $b_j = 0 \div N-1$, $j = \overline{1, N}$.

Нехай дискретне джерело текстової інформації генерує символи первинного алфавіту $A = \{a_i\}, i = \overline{1, M}$ потужності M, де M звичайно й $M \prec N$. Думаємо, що кожний символ a_i з’являється з імовірністю p_i. $P = \{p_i\}$ – розподіл ймовірностей появи символів, що генерує джерело.

Безліч символів, що генерує джерело, може розглядатися і як безліч діграм $D = \{a_i a_j\}$. Під діграмою будемо розуміти послідовність, що складається із двох будь-яких елементів безлічі A, де $i, j = \overline{1, M}$.

Позначимо діграму $a_i a_j$ через d_k. Безліч діграм $D = \{d_k\}$ має потужність K. Максимальне значення K при даному M може бути дорівнює M^2. Думаємо, що кожна діграма з’являється з імовірністю $\tilde{p}_k$, де $k = \overline{1, K}$. Безліч $\tilde{P} = \{p_k\}$ – розподіл ймовірностей діграм, що генерує джерело. Між елементами безлічей D і $\tilde{P}$ існує відношення C – „бути характеристикою”: $\tilde{p}_k C d_k$.

Для подальших міркувань, зберігши наявні між елементами безлічей D і $\tilde{P}$

відношення C, упорядкуємо безлічі D і $\tilde{P}$ по не зростанню значень елементів безлічі $\tilde{P}$: $\tilde{P}_{k-1} \geq \tilde{P}_k$, де $k = \overline{1,K}$.

Для опису послідовностей символів, що генерує дискретне джерело, розширимо алфавіт джерела A до потужності N, включивши в нього підмножина D' безлічі D. При цьому розширений алфавіт $\overline{A}$ буде являти собою об'єднання безлічей A і D':

$$\overline{A} = A \cup D' \quad (1)$$

$$D' \subset D,\ D' = \{d_1, \cdots, d_{N-M}\} \quad . \quad (2)$$

Підмножина D' має потужність $N - M$ і складається з діграм, що найбільше часто зустрічаються в безлічі D. Таким чином,

$$\overline{A} = \{a_1, ..., a_M, d_1, ..., d_{N-M}\}. \quad (3)$$

Безліч елементів коду B також розглядаємо як об'єднання двох безлічей B_1 і B_2, що мають потужності M і $N - M$ відповідно:

$$B_1 = \{b_1, ..., b_M\},\ B_2 = \{b_{M+1}, ..., b_N\}. \quad (4)$$

Причому, у нашім випадку $$A \equiv B_1. \quad (5)$$

Діграмне кодування/декодування буде полягати у встановленні взаємно однозначної відповідності елементів безлічей $\overline{A}$ і B, а саме: A і B_1, D' і B_2.

При цьому справедлива наступна теорема.

Теорема . При діграмному кодуванні відображення розширеного алфавіту $\overline{A}$ кодом B може забезпечити коефіцієнт стиску K_{cm}, обумовлений вираженням:

$$K_{cm} \geq 1 - \frac{1}{2} \sum_{k=1}^{N-M} \tilde{p}_k \ ,$$

де $-\sum_{k=1}^{N-M} \tilde{p}_k$ – сума імовірностей *N-M* диграм безлічі D', що найбільше часто зустрічаються в безлічі D.

Теорема 1 дозволяє:

1) оцінити очікуваний ефект стиску текстової інформації з результатів статистичного тестування не проводячи натурних випробувань стиску;

2) указує на відсутність стиску - $K_{cm} = 1$ (при $\sum_{k=1}^{N-M} \tilde{p}_k = 0$) і максимальний ефект стиску при діграмному кодуванні - $K_{сж} = 0{,}5$ (при $\sum_{k=1}^{N-M} \tilde{p}_k = 1$).

Нижче приводиться алгоритм діграмного кодування. Для формального опису алгоритму введемо деякі поняття.

Вхідний потік – послідовність символів $s_1, s_2, ..., s_w$, що генерує дискретне джерело, – може розглядатися як безліч $S = \{s_w\}$ потужності W, $w = \overline{1,W}$, між елементами якого існує бінарне відношення R "випливати один за іншим": $s_{w-1} R s_w$.

Процедура стиску – процедура встановлення взаємно однозначної відповідності елементів безлічей $S, \overline{A}$ і B.

Вихідний потік – послідовність $q_1, q_2, ..., q_T$ – безліч $Q = \{q_t\}$ потужності $T, t = \overline{1,T}$ - результат дії процедури стиску. Між елементами безлічі Q також існує відношення $R: q_{t-1} R q_t$.

Алгоритм діграмного стиску

Для $w = \overline{2,W}$ і $t = \overline{1,T}$

$$q_t = \begin{cases} b_{M+j} \in B_2 = \{b_{M+1},...,b_{M+j},...,b_N\}, \text{ якщо} \\ s_{w-1}s_w = d_j \in D' = \{d_1,...,d_j,...,d_{N-M}\},\ j = \overline{1,N-M} \\ \\ b_i \in B_1 = \{b_1,...,b_i,...b_M\}, \text{ якщо} \\ s_{w-1}s_w \notin D' \text{ і } s_{w-1} = b_i = a_i \in A = \{a_1,...,a_i,...,a_M\}, i = \overline{1,M} \end{cases}$$

Суть діграмного стиску в наступному. Із вхідного потоку виділяються символи s_{w-1} і s_w – чергова діграма й визначається, чи включена вона в розширений алфавіт $\overline{A}$. Тут можливі два випадки:

а) якщо включено, то у вихідний потік відправляється код цієї діграми, елемент безлічі B_2.

б) якщо розглянута діграма розширеному алфавіту не належить, то у вихідний потік відправляється символ s_{w-1}, а символи s_w і s_{w+1} утворять нову діграму і процес триває.

Описаний метод був реалізований у вигляді комплексу програм моделі системи стиску даних, яка складається із трьох фаз: фаза 1 – попередній аналіз даних і формування розширеного алфавіту $\overline{A}$ у вигляді таблиць кодування/декодування; фаза 2 – процедура діграмного стиску; фаза 3 – процедура декодування стислих даних. Результати стиску різних текстів розглянутим методом показані в таблиці 1.

Таблиця 1

Характери-тики експерименту стиску	Літературні тексти	Тексти по техніці зв'язку	Тексти по теорії інформації	Тексти програм Basic
Обсяг вибірки (симв.)	20000	16000	17000	16000
Потужність алфавіту M	42	58	56	60
Коефіцієнт стиску K_{CT}	0,545	0,556	0,546	0,532

Висновок

Результати стиску даних текстів різних джерел інформації показують, що метод діграмного стиску може забезпечити ефект зменшення обсягів інформації в технічних пристроях інформаційних систем 40-45 процентов відсотків (теоретично – до 50 відсотків). Тим самим можливо фактично збільшити пропускну здатність каналів зв’язку при обміні інформацією між об’єктами АСУ або збільшити ємність запам’ятовувальних пристроїв.

В процесі подальших досліджень основна увага необхідно спрямовувати на разработку систем стиску даних, що адаптуються до різних джерел інформації.

ЛІТЕРАТУРА

1. К. Шеннон. Роботи з теорії інформації й кібернетики. М.: МУЛ,1963.

2. Aronson Jules Data compression – A comparison of methods.„U.S.Dep.Commer.Nat.Bur.Stand.Spec.Publ.”1997,N500-12,IV,31 pp.

к.т.н. Грохольський Я.М. (ВІТІ НТУУ „КПІ”)

ПРИНЦИП ВИНЕСЕНОГО КОМПАНДУВАННЯ

Розглядається тракт базової цифрової каналоутворювальної апаратури ІКМ-30, яка формує цифровий потік Е1. В Україні прийнятий європейський стандарт цієї апаратури. Використання ІКМ-30 та відповідних систем вищих ієрархій на різних лініях зв’язку розширюється. Передбачається, що лінії зв’язку повинні бути достатньо якісними (ймовірність помилкового прийому одиничного елемента не повинна перевищувати $P \leq 10^{-3}$). У противному випадку апаратура переходить в аварійний режим функціонування із втратою зв’язку по каналах ТЧ. Тому є проблематичним використання ЦСП з ІКМ без необхідної модернізації у польових системах зв’язку різних спеціалізованих структур при виникненні ситуацій з погіршенням якісних показників ліній зв’язку.Технічні рішення, прийняті при побудові систем з ІКМ, орієнтовані на мовні сигнали, для яких щільність ймовірностей миттєвих значень зростає при наближенні до нуля і зменшується при наближенні до встановленого значення динамічного діапазону зміни сигналу [1]. Це враховувалось при розробці принципу компандування (нелінійного підсилення сигналу: у більшій степені підсилюються малі миттєві значення сигналів і в меншій степені більші миттєві значень), що суттєво зменшує шум квантування [2]. При компандуванні пряму операцію підсилення на передавальній стороні здійснює компресор, а зворотну на приймальній стороні – експандер. У реальних системах до сигналу завжди добавляється певний шум апаратурного походження та шум з кабельної лінії і процеси перетворення здійснюються над сумішшю сигналу та шуму. Якщо абонент достатньо віддалений від апаратури, то основним буде шум, який накладається на сигнал в абонентській лінії. Разом із сигналом він надходить на компресор і аналого-цифровий перетворювач (АЦП). Збільшити відношення сигнал/шум перед АЦП, а, отже, і на виході каналу, можна, якщо компандер **винести з апаратури в кінцевий абонентський апарат**. Сигнал отримує в апараті відповідне підсилення при незмінності потужності шумів в абонентській лінії і відношення сигнал/шум перед АЦП зростає. Для технічної реалізації телефонний апарат необхідно доопрацювати, розмістивши в ньому компандер. Відповідні зміни повинні бути реалізовані і в апаратурі. Слід зазначити, що все більшу питому вагу у трафіку каналів ТЧ займають немовні сигнали (факс, передача даних, Internet, IP-телефонія, телевимірювання, ін.), і цей процес має сталу тенденцію до розширення. Тому технічні рішення, прийняті при побудові систем з ІКМ, з орієнтуванням на мовні сигнали, для інших сигналів не відповідають принципам оптимальності. Зокрема, при передачі гармонічних посилок з випадковою початковою фазою, рівномірно розподіленою в межах $0 - 2\pi$, щільність ймовірностей найменша при переході синусоїди через нуль і максимальна при переході через амплітудне значення. Така протилежність, порівняно з мовними сигналами, знижує відношення сигнал/шум на виході каналу для гармонічних сигналів, використання яких при різних модуляційних алгоритмах зміни початкової фази зростає. Рішення може бути знайдене на основі створення адаптивної системи компандування стосовно характеристик різних сигналів. Слід зазначити, що при погіршенні якісних показників лінії зв’язку (ймовірність помилок у цифровому лінійному сигналі $p \geq 10^{-3}$) визначальними у відношенні сигнал/шум на виході каналу ТЧ будуть шуми декодування кодових комбінацій з помилками, тому, у цьому випадку, захист кодових комбінацій від помилок є визначальним. Стандартизовані системи з ІКМ європейського стандарту повинні бути модернізовані для використання у системі польового зв’язку на основі реалізації принципів підвищення вірогідності.

ЛІТЕРАТУРА

1. Джон К. Беллами. Цифровая телефония: Пер. с англ. – М.: Эко-Трендз, 2004. – 640с.
2. В.Э. Гуревич и др. ИКМ в многоканальной телефонной связи. – М.: Связь, 1973.з – 336с.

к.в.н. Гулак Ю.С. (НУОУ)

ПРОБЛЕМНІ ПИТАННЯ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Аналіз розвитку та застосування сучасних засобів розвідки свідчить, що розвідувальні зусилля противника активно зосереджуються на добуванні інформації, що циркулює в інформаційно-телекомунікаційних системах (ІТС). Це забезпечується як шляхом агентурної розвідки, так і в значній мірі перехопленням інформації по технічних каналах витоку інформації, за допомогою технічних засобів розвідки. Істотна частина проблем забезпечення захисту інформації, що циркулює в інформаційно-телекомунікаційних системах може бути вирішена організаційними заходами. Проте, з розвитком інформаційних технологій спостерігається тенденція зростання потреби застосування технічних заходів і засобів захисту інформації. Будь-який захист починається з визначення того, що потрібно захищати, від яких загроз і якими засобами. Визначання інформації, яка має захищатися, зводиться до того, що вона повинна мати фундаментальні властивості захищеної інформації. Ці властивості іноді є взаємовиключаючими, що ускладнює забезпечення їх одночасної підтримки. Тому, захист інформації починається з встановлення співвідносин між цими властивостями для конкретної предметної сфери. Саме ці співвідносни, що містять правила розподілу, збереження і обробки інформації, і є змістом політики безпеки інформації.

Часто доводиться створювати систему захисту інформації в умовах великої невизначеності. Тому прийняті заходи і встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Природно, що для забезпечення можливості варіювання рівнів захищеності, засоби захисту повинні володіти певною гнучкістю. Особливо важливим ця властивість є в тих випадках, коли встановлення засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги з часом змінюються. У таких ситуаціях властивість гнучкості позбавить власників інформаційно-телекомунікаційних систем від необхідності вживання кардинальних заходів щодо повної заміни засобів захисту. Досвід теоретичних досліджень і практичних заходів щодо забезпечення технічного захисту інформації показує, що можливості зловживань щодо здобуття інформації, яка циркулює в ІТС, розвиваються та удосконалюються швидше ніж засоби захисту. Тому вирішення завдань захисту інформації в інформаційно-телекомунікаційних системах не може бути зведено просто до створення комплексу механізмів захисту, та вимагає організації регулярного захисту інформації в широкій інтерпретації цього поняття.

Механізми захисту повинні бути зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов’язано із знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових витрат при звичайній роботі органів управління, а також не повинно вимагати від них виконання рутинних малозрозумілих операцій. Можна настільки посилити заходи захисту інформації, що поряд зі збільшенням рівня її безпеки погіршаться умови виконання органами управління своїх функціональних обов’язків.

Таким чином варто відзначити, що неможливо охопити весь спектр питань, що виникають при розгляді проблеми захисту інформації, що циркулює в ІТС, і весь спектр відповідей на них, знайдених на сьогоднішній день. Жодна, найдосконаліша система захисту інформації, зі всілякими рішеннями, не може дати стовідсоткової гарантії на безпеку даних. Адже люди, що розробили систему захисту інформації, знають всі слабкі місця в ній. Як показує досвід, що б не зробила людина, в цьому завжди знайдуться слабкі сторони, адже все передбачити не можливо. Проблем щодо забезпечення технічної безпеки ще дуже багато, але ризик можна звести до мінімуму, використовуючи комплексні системи (підходи) до захисту інформації, яка циркулює в ІТС.

к.т.н. Гунченко Ю.О. (ВІКНУ)
д.т.н. Шворов С.А. (ВІТІ НТТУ ,,КПІ”)
Фесьоха В.В. (ВІТІ НТТУ ,,КПІ”)

МЕТОДИЧНИЙ АПАРАТ ВИЗНАЧЕННЯ УЗАГАЛЬНЕНОГО ПОКАЗНИКА ФУНКЦІОНАЛЬНОГО СТАНУ ОПЕРАТОРІВ АСУ

Вирішення проблеми оцінки функціональних станів (ФС) операторів АСУ значно загострилося в екстремальних умовах, коли різко збільшуються навантаження на людину. Саме тому задачі зв’язку ФС і ефективності виконання діяльності, визначення найбільш досконалих способів діагностики ФС, механізмів його регуляції, математичної обробки та об’єктивного аналізу отриманих результатів займають провідне місце в сучасних дослідженнях в області інженерної психології, ергономіки, психології праці, медицини та фізіології.

У сучасній практиці оцінка функціональних станів стикається зі значними розбіжностями у формуванні й інтерпретації комплексу інформативних параметрів і способів їх обробки. Крім того, аналіз комплексу таких інформативних параметрів показує наявність великої кількості різнорідних значень, що вимірюються в порядковій шкалі, шкалах інтервалів, відношень і абсолютній шкалі. Переважна більшість існуючих методів обробки експериментально отриманої інформації не пристосована для врахування різнорідності (різношкальності) значень виміряних параметрів.

Велика кількість факторів, від котрих залежить функціональний стан, а також різноманітність функцій, у яких проявляється його специфічність, є основною складністю у вирішенні задач оцінки і прогнозування ФС. Вирішити ці задачі можна лише шляхом використання інтегральних методів визначення ФС. Проблеми невизначеності та багатофакторності виникають як у середині кожної складової ФС, так і при згортці сукупності оцінок в інтегральний (узагальнений) показник ФС.

Для вирішення задачі класифікації, тобто віднесення ФС, що характеризується набором фізіологічних, психологічних та енергетичних показників, до одного з декількох станів, пропонується застосовувати так званий нечіткий гібридний класифікатор. Такий класифікатор є системою, що об’єднує в структурному і функціональному відношеннях принципи нейронних мережних моделей і нечітку логіку обробки даних відповідно.

Поставлена задача вирішується за допомогою 4-х прошаркової нейро-нечіткої мережі.

Перший прошарок мережі створює на виході ступінь належності як міру відповідності виміряних показників ФС заданим вимогам.

Другий прошарок є об’єднуючим по кожному конкретному показнику і потрібен для того, щоб урахувати можливість попадання i-го признаку одночасно в дві класифікаційні групи (як правило, з різним ступенем належності).

Третій прошарок призначений для об’єднання нечітких оцінок всередині кожної групи фізіологічних, психологічних і енергетичних показників.

Четвертий прошарок представлений єдиним нейроном, входами якого є зважені значення мір відповідності ФС оператора АСУ кожної групи показників, а виходом – міра відповідності ФС в цілому заданим вимогам.

Така нейро-нечітка мережа може бути класифікована як синхронна багатопрошаркова гетерогенна мережа з локальними зв’язками, але без зворотних зв’язків. Останнє дозволяє зняти питання про динамічну врівноваженість нейромережі, що є важливою перевагою наведеної структури.

Таким чином, запропоноване рішення для оцінки ФС людини-оператора із застосуванням нечіткого гібридного класифікатора доцільно покласти в основу методики розрахунку узагальненого показника ФС оператора АСУ в мобільному технічному комплексі діагностики.

к.т.н. Гуржій П.М. (ВІТІ НТУУ „КПІ”)
к.т.н. Слободянюк О.В. (КПНУ ім. І.Огієнка)
Процюк Ю.О. (ВІТІ НТУУ „КПІ”)
Куліца О. С. (ХУ ПС ім. Івана Кожедуба)

ОЦІНКА МОЖЛИВОСТІ ЗМЕНШЕННЯ НАВАНТАЖЕНЬ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

У зв’язку зі збільшенням обсягів використання мультимедійного контенту в інформаційно-телекомунікаційних системах (ІТС), більш гостро зростає проблема останньої мілі. У дійсний час існує велика кількість технологій останньої мілі, а універсального рішення цієї проблеми не існує, кожна технологія має свої переваги та недоліки, при цьому потребує значних фінансових витрат пов’язаних в основному з необхідністю впровадження більш потужного обладнання. Зменшити навантаження на комутаційне обладнання ІТС, у тому числі систем спеціального призначення, можливо за рахунок використання методів стиску, а тому подальший розвиток та вдосконалення існуючих методів компактного представлення мультимедійних даних є актуальною проблемою. Існуючі методи стиску без втрати якості дозволяють зменшити об’єм відеоповідомлень у середньому до 1,5 – 2,2 раз, однак такі коефіцієнти досягаються тільки при обробці слабко та середньонасичених зображень, а при обробці висонасичених зображень коефіцієнти не перевищують 1,3 рази [1, 2]. У роботах [3 – 5] для додаткового підвищення коефіцієнта стиску відеоданих був запропонований метод стиску зображень на основі змішаного поліадичного кодування масивів довжин серій і кольорових координат. Проведемо оцінку коефіцієнта стиску, та часу, що витрачається на обробку зображень запропонованим методом.

Для одержання значень часу обробки й коефіцієнта стиску зображень необхідно:

1. Визначити середній об’єм компактно представленого відеозображення.

2. Обчислити середню кількість машинних операцій, що витрачається на компактне представлення зображення та знайти середній час стиску $T_{ст}$ зображення.

Розглянемо перераховані задачі:

1. Визначення коефіцієнта стиску $k_{ст}$ зображень компактно представлених за допомогою розробленого методу. Значення $k_{ст}$ обчислюється за формулою:

$$k_{ст} = \frac{W_{поч}}{W_{ст}}, \qquad (1)$$

де $W_{поч}$ – початковий цифровий обсяг зображення; $W_{ст}$ – цифровий обсяг стислого зображення.

З формули (1) видно, що для визначення $k_{ст}$ необхідно обчислити обсяг стислого зображення $W_{ст}$.

Цифровий обсяг $W_{ст}$ стислого зображення дорівнює:

$$W_{ст} = W_{кк} + W_{дс} + W_{сі}, \qquad (2)$$

де $W_{кк}$ – сумарна кількість розрядів, необхідних для представлення поліадичних кодів колірних координат; $W_{дс}$ – обсяг кодового представлення поліадичних кодів довжин серій; $W_{сі}$ – кількість розрядів що витрачається на подання службової інформації.

Таким чином вираз для визначення $k_{ст}$ буде мати вигляд:

$$k_{ст} = \frac{W_{поч}}{W_{кк} + W_{дс} + W_{сі}}. \qquad (3)$$

2. Визначення кількості операцій, що витрачається на стиск зображення. Основна кількість операцій приділяється для формування масивів колірних координат, масивів

довжин серій та обчислення поліадичних чисел для елементів цих масивів. Для утворення всіх масивів колірних координат і масивів довжин серій необхідно виконати $Z_m \times Z_n$ операцій порівняння (де $Z_m \times Z_n$ – кількість елементів зображення в кадрові).

Якщо обробка масивів колірних координат і масивів довжин серій відбувається в змішаному поліадичному просторі, то витрачається додатково $\nu\, m_{дс}\, n_{дс}$ операцій порівняння. Враховуючи це, кількість операцій $k_{оп}$ обчислюється за формулою:

$$k_{оп} = Z_m \times Z_n + 10\nu m_{дс} n_{дс}, \qquad (4)$$

де $m_{дс}\, n_{дс}$ – кількість елементів у масиві довжин серій; ν – кількість масивів довжин серій.

На основі виразу (4) можна знайти час стиску:

$$T_{ст} = \frac{Z_m \times Z_n + 10\nu m_{дс} n_{дс}}{V_{ст}}, \qquad (5)$$

де $T_{ст}$ – час, необхідний для обробки масивів колірних координат і масивів довжин серій кадру в змішаному поліадичному просторі; $V_{ст}$ – швидкість стиску, що виражається в кількості операцій за секунду. Таким чином, отримані вирази для визначення часу обробки та кількості операцій, що витрачаються на стиск.

Аналіз залежності значень коефіцієнта стиску $k_{ст}$ від імовірності колірного перепаду p, розмірів масиву кольорових координат $m_{кк} \times n_{кк}$ і максимального значення довжини серії $\ell_{\max}$ показує що, у випадку поліадичного кодування масивів кольорових координат (C) та довжин серій (L) у змішаному поліадичному просторі ступінь стиску $k_{ст}$ зображень змінюється в межах від 2,9 до 63,6 залежно від класу зображень, розмірів масивів колірних координат і довжин серій, а також максимальної довжини серії $\ell_{\max}$. Ступінь стиску залежить від чотирьох складових: розмірів ділянок зображення, що мають однаковий колір (це визначає кількість структурної надмірності), кількості комбінаторної надмірності в масивах колірних координат і в масивах довжин серій, а також кількість структурної надмірності, яка усувається в результаті зменшення діапазонів даних масивів C та L. Залежно від класу зображення кількість комбінаторної та структурної надмірності буде різним. Для слабконасичених зображень збільшується кількість структурної надмірності, що обумовлено більшими розмірами ділянок зображення зафарбованих одним кольором. Для таких зображень зменшується кількість масивів C і L, а також вдається більшою мірою знизити діапазон значень елементів цих масивів. Тому найбільший ступінь стиску досягається для слабконасичених зображень.

ЛІТЕРАТУРА

1. Ватолин В.И., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с.

2. Gonzalez, Rafael C; Woods, Richard E. Digital Image Processing, 2nd ed. – published by Pearson Education, Inc. publishing as Prentice Hall., 2002. – 793 p.

3. Аудиовизуальные системы связи и вещания: новые технологии третьего тысячелетия, задачи и проблемы внедрения в Украине / [О.В. Гофайзен, А.И. Ляхов, Н.К. Михалов и др.] // Праці УНДІРТ. – 2000. – № 3. – С. 3 – 40

4. Баранник В.В., Бридня Е.А., Гуржий П.М. Разностное кодирование массивов служебных данных // Зб. наук. пр. ХУ ВС. – Х.: ХУ ВС. – 2005. – Вип. 2 (2). – С. 82 – 84.

5. Баранник В.В., Гуржій П.М. Полиадическое кодирование массивов длин серий в смешанной системе оснований // Авиационно-космическая техника и технология. – 2005. – Вип. 5 (21). – С. 47 – 51.

6. Баранник В.В., Гуржий П.М. Кодирование массивов цветовых координат в разностном полиадическом пространстве // Радіоелектронні і комп'ютерні системи. – 2005. – Вип. 1 (9). – С. 44 – 49.

к.т.н. Гурський Т.Г. (ВІТІ НТУУ „КПІ”)
Клімович С.О. (ВІТІ НТУУ „КПІ”)
Боголій С.М. (ВІТІ НТУУ „КПІ”)

НАПРЯМКИ ЗАСТОСУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ В РАДІОМЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В сучасних телекомунікаційних системах як загального, так і спеціального призначення, широко застосовуються псевдовипадкові послідовності (ПВП).

Основними напрямками застосування ПВП є наступні:

розширення спектра сигналу з метою підвищення завадозахищеності (наприклад, в апаратурі завадозахисту „Кулон” зі складу станції космічного зв’язку Р-440);

забезпечення множинного доступу (МД) в радіомережах з кодовим розподілом каналів (у мережах стільникового зв’язку стандартів на основі *CDMA – code division multiple access*);

формування закону перестроювання частоти в радіомережах з ППРЧ (наприклад, у засобах радіозв’язку комплексу „Акація ” вітчизняного виробництва);

криптографічний захист інформації шляхом реалізації методу гамування – поточне шифрування, що полягає у накладанні відкритого тексту на гаму шифру, що генерується на основі ПВП (у апаратурі засекречування дискретної інформації гарантованої стійкості).

Розглянемо основні характеристики ПВП та вимоги до них:

період, або довжина послідовності (повинна бути якомога більшою при достатній простоті її генерації на практиці);

автокореляційна функція (повинна мати низький рівень бокових пелюстків по відношенню до головного для забезпечення надійної синхронізації й зменшення впливу міжсимвольних й міжпроменевих завад);

функція взаємної кореляції (повинна мати низький рівень для забезпечення можливості одночасної роботи якомога більшої кількості користувачів, кожному з яких призначається індивідуальна ПВП);

аперіодична функція взаємної кореляції послідовності (повинна мати низький рівень для зменшення впливу взаємних завад користувачів однієї радіомережі);

потужність множини послідовностей (число кодових послідовностей, вибраних для реалізації, повинно бути великим й допускати при необхідності своє збільшення для підвищення прихованості передачі інформації);

лінійна складність послідовності (використовувані послідовності не повинні допускати несанкціонованого відтворення).

Всі вище перераховані параметри займають важливу роль при виборі того чи іншого сімейства послідовностей. Тому важливою задачею побудови й аналізу сімейств послідовностей є оптимізація цих параметрів. Результати аналізу літератури в даній предметній області свідчать про те, що короткі псевдовипадкові послідовності мають кращі у порівнянні з випадковими послідовностями кореляційні властивості. У випадку довгих послідовностей, не дивлячись на те, що кореляційні властивості випадкових послідовностей статистично прямують до оптимальних значень, виникають значні технічні труднощі, пов’язані з їх реалізацією. На сьогоднішній день в літературі наводяться дані про велику кількість різних видів ПВП, які за алгоритмом формування можна класифікувати на лінійні (наприклад, *M*-послідовності, утворені на їх основі послідовності Голда і Касамі) та нелінійні (наприклад, Бент-послідовності, *GMW*, де Брейна, послідовності повного циклу). Закон формування лінійних ПВП визначається деяким лінійним рекурентним співвідношенням. Нелінійні ПВП володіють кращою лінійною складністю, проте, гіршими кореляційними властивостями та є більш складними в реалізації.

Перспективним напрямком досліджень є створення радіомереж спеціального призначення з підвищеною завадозахищеністю на основі кодового розподілу каналів.

Системи радіозв’язку, в яких застосовуються сигнали з розширенням спектру, мають цілий ряд переваг:

можливість перекриття їх спектру зі спектрами сигналів інших систем без помітного зниження їх якості роботи, тобто висока електромагнітна сумісність з іншими системами;

висока завадозахищеність в умовах дії навмисних завад;

висока стійкість до частотно-селективних завмирань, що виникають внаслідок багатопроменевого розповсюдження сигналу, що особливо актуально для зв’язку в умовах міста;

підвищена прихованість й конфіденційність передачі інформації.

Основними задачами, які потребують розв’язання при створенні радіомереж з КРК, є наступні:

вибір виду ПВП;

створення множини ПВП, які будуть призначатися кореспондентам мережі (адресних послідовностей);

створення множини ПВП, яку буде використовувати базова станція для передачі в прямому каналі;

визначення необхідного значення бази широкосмугового сигналу для прямого та зворотного каналів (чим більша база сигналу, тим більший виграш по завадостійкості від обробки, проте, зверху це значення обмежується через зниження спектральної щільності потужності сигналу в точці прийому до рівня, який не дозволяє реалізувати прийом („згортку”) із необхідною якістю).

Розглянемо критерії вибору кодових послідовностей при реалізації МД з КРК.

В прямому каналі (від БС до МС) при підтримують кадрову і тактову синхронізацію адресних послідовностей робочих каналів однієї БС. Для мінімізації міжканальних завад в прямому каналі зв’язку в якості адресних послідовностей є можливим застосування ансамблів ортогональних сигналів, наприклад ансамбль функцій Уолша. Тоді корелятор на приймальній стороні відреагує тільки на ту адресну послідовність, еталон якої формується в приймачі, відгук на сигнали сусідніх каналів в ідеалі повинен бути нульовим.

В зворотному каналі ситуація може принципово відрізнятися через те, що у адресних послідовностей робочих каналів МС часові зсуви довільні, тобто має місце асинхронний режим роботи. Тому в зворотному каналі потрібен ансамбль сигналів з хорошими кореляційними властивостями. Об'єднуючи вимоги до АКФ та ВКФ як у прямому, так і у зворотному каналах можна ввести загальний мінімаксний критерій, що полягає у мінімізації максимальних викидів бокових пелюсток відповідних функцій. Слід відмітити, що АКФ та ВКФ ансамблів детермінованих послідовностей пов’язані таким чином, що в них неможливо досягнути одночасно хорошої авто- і взаємної кореляції.

Широке застосування в радіомережах з КРК отримали бінарні коди на основі *M*-послідовностей, що обумовлено хорошими властивостями їх періодичних автокореляційних функцій (ПАКФ). При достатньо великих довжинах *M*-послідовностей можна досягнути дуже малого значення величини рівня бокових пелюсток ПАКФ при значній величині основного. Ця властивість дозволяє виділяти окремі промені з загальної інтерференційної картини, а також з високим ступенем точності підтримувати кодову синхронізацію при багатопроменевому поширенні радіохвиль та пересуванні мобільних абонентів зі значною швидкістю.

Таким чином, для створення високоефективних завадозахищених радіомереж спеціального призначення на основі кодового розподілу каналів необхідно створити новий клас ПВП, розв’язавши при цьому низку взаємопов’язаних, в деяких випадках, протилежних завдань: максимізація об’єму та періоду з забезпеченням достатньо високої лінійної складності та прийнятної складності апаратної реалізації; оптимізація авто- і взаємокореляційних функцій; розробка методів і пристроїв генерації таких послідовностей.

Дудник В.Ю. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

ІНФОГРАФІЧНИЙ ОБРАЗ ОБ’ЄКТА МЕРЕЖІ ТА ЙОГО ВИКОРИСТАННЯ

Для підтримки нормальної роботи інформаційного забезпечення одним з ключових моментів є його безпека. Тому сьогодні будь-яка мережа у якості елементу безпеки має систему виявлення вторгнень, яка дозволяє оперативно відслідковувати спроби реалізації загроз та аналізувати їх. Сучасні системи виявлення вторгнень неможливі без використання підсистеми штучного інтелекту, а значить і бази знань для нього. Проте оскільки база знань ніколи не може бути абсолютно повною слід розуміти, що для перекриття неточностей і впровадження нових знань необхідна участь експертів. Експерт – спеціаліст, що має відповідний рівень фахових знань, для створення кваліфікованого висновку або судження з питань предметної області. При роботі експерта у будь-якій області важливим є розробка експертного інтерфейсу, адже від нього залежить ефективність його роботи. Оскільки сприйняття експерта річ індивідуальна, а основним завданням є створення комфортних умов для набуття системою нових знань інтерфейс має будувати модель предметної області, мати кластери параметрів та бути гнучким для користувальницьких налаштувань.

Інфографічна модель – об’єднана загальною стилістикою візуальна модель одно або різнотипних даних про об’єкт дослідження з використанням типових методів візуалізації (створення наочних об’єктів, створення умов для візуального спостереження) предметної області. Цей термін випливає з визначення інфографіки як сукупності особливих теоретичних і практичних питань геометричного моделювання об'єктів (предметів або процесів) і є методологічною основою проектування систем і конструювання технічних засобів візуалізації образів у інформаційних технологіях. Тому, у даному дослідженні увага приділяється комплексному підходу до відображення даних та комбінування загальновідомих підходів для визначення найкращого. У якості вхідних параметрів розглядаються основні параметри потоків даних у мережі (інтенсивність, час життя, тощо). У якості об’єкта мережі можна розглянути не тільки конкретний вузол, а й підмережу чи мережу в залежності від необхідної деталізації. Гнучке масштабування дає змогу експерту оцінити і систему (мережу), і системоутворюючі чинники (її вузли чи підмережі).

Для побудови такого образу з достатньою для аналізу кількістю параметрів у n-вимірному просторі пропонується використовувати поєднання сферичної системи координат, як об’ємну полярну систему координат, для представлення вихідних потоків об’єкта, кольорового обрамлення для протоколів прикладного рівня та ступеневу 3-хвимірну систему координат для відображення частини параметрів транспортного рівня. Також пропонується внести кольорову диференціацію інтенсивності потоків. Центральним елементом у ньому є сферичне представлення інформаційних потоків між даним об’єктом та іншими об’єктами мережі – мережами, підмережами, окремими вузлами, що в залежності від масштабування можуть виступати як окремими об’єктами так і сукупностями об’єктів. Під час попередніх досліджень був запропонований двовимірний варіант інфографічної моделі, який відображав структуру зв’язності мережі, проте як повноцінну модель її розглядати неможливо через відносно невелику кількість параметрів, що відображались, та недостатні можливості з масштабування.

Таким чином подальшу роботу планується проводити у напрямку розробки інфографічних моделей для експертних інтерфейсів як систем виявлення вторгнень, так і систем підтримки та прийняття рішень з метою підвищення ефективності роботи експерта. Це має за мету зменшення часу необхідного йому для аналізу стану мережі, покращення інтерфейсу з точки зору ергономіки. Ергономічна складова заслуговує окремої уваги через відсутність загальноприйнятих результатів досліджень у області побудови програмних інтерфейсів, хоч вона і відіграє одну з найважливіших складових у роботі експерта.

д.т.н. Єрохін В.Ф. (ІСЗЗІ НТУУ „КПІ”)
Гиндич Б.А. (ІСЗЗІ НТУУ „КПІ”)

ПРОЦЕДУРА ФОРМУВАННЯ OFDM-СИГНАЛУ В СТАНДАРТІ IEEE 802.16E-2005, 2009

Передача інформації за допомогою сигналів з ортогональним частотним поділом (OFDM – Orthogonal Frequency Division Multiplexmg) стала стандартом для багатьох сучасних радіосистем у зв’язку з рядом переваг, до яких відносяться: висока спектральна ефективність, низький рівень міжсимвольной інтерференції, висока якість передачі в умовах частотно селективних завмирань. До переліку відповідних стандартів відносяться: IEEE 802.11a,g – бездротові локальні мережі, IEEE 802.16 – широкосмуговий бездротовий зв’язок, DVB-T (Digital Video Broadcasting – Terrestrial) – цифрове телевізійне мовлення, DRM (Digital Radio Mondiale) – цифрове радіомовлення й ін. Сюди ж можна додати перспективну систему з підвищеною швидкістю передачі на основі сполученої технології ортогонального частотного й просторового поділу (MIMO-OFDM – multiple Input, multiple Output-OFDM) – 802.11n. У той же час системи передачі, що використовують даний тип сигналів, дуже чутливі до фазової нестабільності піднесівних. Вона може бути викликана нестаціонарністю фазової характеристики каналу, обумовленої доплеровским розсіюванням, фазовими флуктуаціями опорних генераторів на передавальній і приймальні сторонах. Як наслідок, зростає число помилок при передачі дискретної інформації. Проблема особливо гостро постає в каналах з багатопозиційною квадратурною амплітудно-фазовою модуляцією піднесівних.

Цілі і задачі дослідження.

1. Вирішити питання щодо наявності детермінованого (визначеного) зв’язку між кутовими параметрами (початковими фазами) складових OFDM – сигналу. Чи є аналітичний зв’язок між їх початковими фазами та який він. На наш погляд, є.

2. Все ж таки, як приймаються та демодулюються складові OFDM – сигналу? Тобто, що відбувається із фазами кожної піднесівної, чи вони аналізуються окремо чи групами (кластерами) по 14 піднесівних наприклад у випадку зони PUSC (partial usage of the subchannels – неповне використання підканалів) для зворотнього каналу OFDM – 1024.

Тільки вирішивши ці питання, можна перейти до синтезу та побудови імітаційної моделі щодо приймання OFDM – сигналу „в цілому”.

Доповідь буде базуватись на прикладі режимі WirelessMAN-OFDMA стандарту IEEE 802.16e-2005, 2009 призначеному для роботи в умовах відсутності прямої видимості між БС (базою станцією) й АС (абонентською станцією) у діапазоні частот до 11 Ггц. Даний режим заснований на застосуванні сигналів з OFDM із 2048, 1024, 512 або 128 піднесівними (тобто, з підтримкою різних смуг частот).

Ідея передачі даних сигналами з OFDM ґрунтується на технології передачі даних із використанням великої кількості піднесівних і полягає в тому, що потік переданих даних розподіляється по деякому набору частотних підканалів (піднесівних), тобто передача ведеться на них синхронно і паралельно. За рахунок поділу переданого високошвидкісного потоку даних відносно низькошвидкісні підканали, кожний з яких модулюється своєю інформацією, забезпечується висока завадостійкість прийому в умовах міжсимвольной інтерференції та впливу вузькосмугових завад. Сигнали з OFDM формуються за допомогою пристрою, що виконує зворотнє дискретне перетворення Фур’є. Отримані на виході цього пристрою часові відліки через цифроаналоговий перетворювач (ЦАП) і вихідні ланцюги передавача надходять у канал передачі. Сигнали на піднесівних частотах, очевидно, ортогональні за рахунок того, що їх початкові фази є однаковими – тобто, аналітично детерміновано пов’язані, а на довжині елементарного тактового інтервалу на кожній з піднесівних міститься ціле число періодів.

Піднесівні в OFDMA (OFDM Access – доступ) – символі діляться на 3-ри групи: інформаційні, нульові і пілотні.

Нульові піднесівні – як додатковий засіб боротьби з міжсимвольной інтерференцією, а також для забезпечення відповідності сигналу заданій спектральній масці, входять до складу захисного інтервалу. Амплітуда нульових піднесівних рівна нулю. Передача даних на них не здійснюється. *Інформаційні* – призначені для передачі даних. В стандарті вони називаються підканалами). У прямому каналі підканал може бути назначений одному або декільком абонентам, у зворотньому каналі одному абонентові призначаються один або декілька підканалів, причому абоненти мають можливість вести передачу одночасно. Піднесівні, що утворюють один підканал, можуть бути як суміжними, так і розподіленими. Розподіл символу на підканали призначено для підтримки множинного доступу, адаптивних антенних систем і масштабованості. *Пілотні* – для передачі відомих ПВП, призначених для корекції передатної характеристики каналу зв'язку за допомогою еквалайзера.

Стало відомо, що всі дії по реалізації когерентного прийому сигналів з OFDM здійснюються в блоці ШПФ паралельно. Блок ШПФ реалізує банк кореляторів, кожний з яких настроєний на певну піднесівну. Фазова синхронізація й корекція передатної характеристики каналу здійснюється в еквалайзері на основі пілотних піднесівних. Пілотні піднесівні являють собою спеціально виділені частоти, рівномірно розподілені в смузі займаних частот, на яких передається заздалегідь відома інформація. На основі аналізу принятих і переданих символів на пілотних піднесівних можна оцінити комплексний коефіцієнт передачі каналу й зсув фази на цих частотах і далі вирішити завдання інтерполяції передаточної характеристики каналу у всій смузі займаних частот.

Загальновідомо, що у різних зонах PUSC і FUSC (full usage of the subchannels – повне використання підканалів) пілотні й інформаційні піднесівні вибираються по-різному. У зоні FUSC набір пілотних піднесівних – один для всього діапазону займаних частот, у зоні PUSC – один для кожної групи. Застосування зон підвищує ефективність роботи БС (базової станції) із різними типами користувачів (абонентських станцій).

У різних зонах пілотні та інформаційні піднесівні вибираються по різному але принцип залишається однаковим, будь то зона FUSC, PUSC, TUSC1 (Tile Usage of SubChannels), 2 та ін., напрямок передачі (канал вверх чи вниз), спосіб формування підканалів (з використанням суміжних піднесівних чи несуміжних).

Відомо, що у еквалайзері здійснюється корекція частотної характеристики прямого каналу. Алгоритм роботи якого ґрунтується на виділенні в кожному фізичному тайлі (tile — мозаїчний елемент, термін стандарту IEEE 802.16e-2005, 2009) пілотних відліків та інтерполяції по них частотної характеристики для даного тайла. Для корекції передаточної характеристики каналу виділяються комплексні амплітуди (сигнальні точки), що відповідають пілотним піднесівним.

На відміну від зони PUSC прямого каналу у зворотньому корекція передаточной характеристики каналу здійснюється тільки в межах одного тайла незалежно від значення пілотних піднесівних сусідніх тайлів.

По завершенні процедури еквалайзинга пілотні піднесівні видаляються з послідовностей, залишаються тільки інформаційні піднесівні.

У роботі детально розглянуто формування сигналу у різних зонах. Знайдено відповіді на ряд поставлених запитань та з'ясовано як по пілотним піднесівним відбувається демодуляція OFDM-сигналу.

ЛІТЕРАТУРА

1. Єрохін В.Ф., Гиндич Б.А. Огляд розвитку технології OFDM стандартів BWN / В.Ф. Єрохін, Б.А. Гиндич, Збірник наукових праць ВІТІ НТУУ „КПІ", № 1, – 2012. – С 60.

2. Рашич А.В. Сети безпровідного доступа WiMAX: учеб. Пособие / А.В. Рашич – СПб.: Изд-во Политехн. Ун-та, 2011. – 179 с.

Єсаулов М.Ю. (ВІТІ НТУУ „КПІ”)

ЗАДАЧІ УПРАВЛІННЯ СППР СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Рішення комплексного завдання захисту інформації в інформаційно-телекомунікаційних системах передбачає реалізацію визначеної послідовності заходів: оцінку фактичного стану інформаційної безпеки ІТС, прогнозування стану інформаційної безпеки системи й ступеню впливу загроз і дестабілізуючих чинників, планування системи заходів захисту інформації у відповідності з факторами загроз і поточним значенням захищеності системи, визначення методів і механізмів забезпечення необхідного рівня захищеності та прийняття рішення щодо управління системою захисту інформації. Для виконання даних заходів своєчасно та якісно необхідно здійснювати збір, обробку та аналіз інформації про велику кількість факторів, врахувати дану інформацію при прийняті рішення щодо використання й вдосконалення механізмів захисту та управління системою захисту інформації. Ці функції й повинна реалізовувати система підтримки прийняття рішення (СППР) [1]. При побудові даної СППР потрібно використовувати основні підходи до розробки автоматизованих систем, що залежать від мети функціонування: параметри управління розраховуються на весь період управління, управління за впливами, коли зовнішні некеровані фактори заздалегідь відомі до прийняття рішення та управління зі зворотнім зв’язком за станом системи, якщо можливо кількісно виразити стан системи. Перший – при реалізації підсистеми комплексного захисту інформації; другий – при реалізації підсистеми прогнозування; третій – при реалізації підсистеми збору й попередньої обробки інформації та формування управлінських рішень.

Розглянемо задачі управління підсистем СППР, а також вхідну інформацію, яка необхідна для їх рішення, й вихідну інформацію (результатів рішення задач управління):

підсистема збору та попередньої обробки інформації – збір і збереження даних, контроль відповідності, стану й правильності функціонування елементів системи, аналіз параметрів зовнішнього середовища – експертна інформація про об’єкт управління, база знань (методи аналізу, нормативи, еталони, профілі захисту) – бази даних про елементи системи, класи потенційних загроз і уразливостей системи;

підсистема прогнозування – визначення поточних значень всіх необхідних параметрів, визначення та оцінка поточних значень показників захищеності – множина класів потенційних загроз, експертна інформація про значення достовірності нейтралізації загроз та потенційного збитку, база знань (методи розрахунку) – інтегральні показники захищеності системи;

підсистема формування управлінських рішень – прийняття рішення про використання механізмів захисту, раціональна організація системи захисту інформації – інтегральні показники захищеності системи, база знань (методи розрахунку, еталони, нормативи) – рекомендації щодо використання механізмів захисту;

підсистема комплексного захисту інформації – обґрунтування оптимально достатніх наборів механізмів захисту, прийняття рішення про модифікацію та вдосконалення системи захисту інформації – інтегральні показники захищеності системи, база знань (методи розрахунку, еталони, нормативи, профілі захисту) – рекомендації щодо вдосконалення системи захисту інформації.

Аналіз вищевказаного дозволяє зробити висновок про необхідність створення баз даних, а також відокремлення двох їх основних груп. До першої групи відносять бази даних, які утворюються стаціонарними джерелами даних і дозволяють активізувати систему й підтримувати її працездатність. Друга група формується динамічними джерелами даних і будується самою системою при обробці експертної (моніторингової) інформації.

ЛІТЕРАТУРА

1. Єсаулов М., Калатенко П. Структура системи підтримки прийняття рішення процесу управління захистом інформації // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. – Науково-технічний збірник Випуск 1 (16). – С.48 – 57.

Жупанов О.П.(ВІТІ НТУУ „КПІ”)
Лук’янчук І.В.(ВІТІ НТУУ „КПІ”)

АЛГОРИТМ ПОШУКУ РАЦІОНАЛЬНИХ ШЛЯХІВ ПЕРЕВІРКИ ОБ’ЄКТІВ КІБЕРНЕТИЧНОГО ВПЛИВУ

В умовах сьогодення інформаційний простір та інформаційні ресурси кіберпростору захищаються не тільки на рівні держави, а й суспільства та громадян. Відповідно, засоби та системи захисту інформації, насамперед програмні, є доступними для широкого кола громадян і активно поширюються у світовому кіберпросторі. І цей факт додатково впливає на рівень захищеності держави від внутрішніх та зовнішніх загроз застосування кібернетичних атак, а також на рівень національної безпеки в інформаційній сфері в цілому. Кібернетична війна є одним із різновидів інформаційної війни, або, як її називають американські воєнні експерти, війна в комп’ютерних мережах. Для ефективної реалізації кібернетичного впливу суб’єкт атаки повинен мати відомості для визначення цілей програми атаки. Дані відомості є результатом проведення інформаційної підготовки кібернетичного впливу. Ключовим питанням організації інформаційної підготовки є розробка алгоритмів планування перевірки потенційних об’єктів атаки, що базуються на загальній математичній постановці задачі відомої як „задача про комівояжера”. Сутність задачі полягає у знаходженні оптимального порядку перевірки („обходу”) певної множини об’єктів будь-якої природи, щоб цільова функція накладних витрат на таку роботу була б мінімальною. Такий алгоритм повинен буде забезпечити як задану точність обрахунків так і відповідність наявним обчислювальним ресурсам. В якості такого алгоритму може виступати „Мурашиний алгоритм”.

Мурашиний алгоритм (алгоритм оптимізації мурашиної колонії, англ. ant colony optimization, ACO) – один з ефективних поліноміальних алгоритмів для знаходження наближених рішень задачі комівояжера, а також аналогічних завдань пошуку маршрутів на графах. Підхід запропонований бельгійським дослідником Марко Доріго (англ. Marco Dorigo). Суть підходу полягає в аналізі та використанні моделі поведінки мурах, що шукають дороги від колонії до їжі. В природі, мурахи (початково) блукають довільним чином, і по знаходженні їжі повертаються до колонії, залишаючи по собі феромоновий слід. Якщо інші мурахи знаходять такий шлях, вони схильні припинити свої блукання, натомість слідувати позначеним шляхом, посилюючи його під час повернення у разі знайдення їжі.

Якість одержуваних рішень багато в чому залежить від настроювальних параметрів в ймовірнісно-пропорційному правилі вибору шляху на основі поточної кількості феромону і від параметрів правил відкладання і випаровування феромону. Можливо, що динамічна адаптаційна настройка цих параметрів може сприяти отриманню найкращих рішень. Важливу роль відіграє і початковий розподіл феромонів, а також вибір умовно оптимального рішення на кроці ініціалізації.

Перспективними шляхами покращення мурашиних алгоритмів є різні адаптації параметрів з використанням бази нечітких правил та їх гібридизація, наприклад, з генетичними алгоритмами.Таким чином, коли мураха знаходить вдалий (тобто короткий) шлях з колонії до джерела їжі, інші мурахи швидше слідуватимуть йому, і позитивний зворотний зв’язок зрештою призведе до обрання цього шляху всіма мурахами.

Проведений аналіз ефективності показує що описана система відповідає усім необхідним вимогам щоб бути рекомендованою до використання в цілях іформаційного забезпечення кібернетичного впливу.

Жупанов О.П.(ВІТІ НТУУ „КПІ”)
к.т.н Хусаінов П.В.(ВІТІ НТУУ „КПІ”)

ОПТИМІЗАЦІЯ ЧАСОВИХ ВИТРАТ ОБМІНУ ДАНИМИ МІЖ ЗАСОБАМИ КІБЕРНЕТИЧНОГО ВПЛИВУ

При підготовці до кібернетичного впливу суб’єкт атаки зобов’язаний потурбуватися про забезпечення анонімності його дій у комп’ютерних мережах. Даний факт не є новиною адже будь-який Інтернет провайдер за чинним законодавством зобов’язаний видати правоохоронним органам усю приватну інформацію про користувача за його IP адресою при наявності офіційного запиту. Для забезпечення скритності IP адреси у глобальній мережі достатньо використовувати анонімні proxy-сервери та шифрувати корисні дані існуючими алгоритмами але подібні рішення потребують додаткової конфігурації і не завжди ефективні тому існують такі автоматизовані системи як TOR (The Onion Routing) та I2P (Invisible Internet Project).

В основі такої системи як TOR лежить розподілена система вузлів між якими в зашифрованому вигляді передаються дані. Для з’єднання зазвичай використовується три сервери, які утворюють тимчасовий ланцюжок. Кожен сервер вибирається випадковим чином, при цьому він знає тільки те, від якого серверу отримав дані і кому вони призначаються. Мало цього – ланцюжки постійно змінюються. Навіть у випадку перехоплення даних на одному із серверів відстежити повний маршрут пакетів (в тому числі і їх відправника) не представляється можливим. Перед відправленням пакет послідовно шифрується трьома ключами: спочатку для третього(останнього) сервера, потім для другого і, врешті-решт, для першого. Коли перший сервер отримує пакет, він розшифровує „верхній” шар шифру і дізнається, куди відправити пакет далі. Другий і третій сервер працюють аналогічним чином.

Формалізувавши цю схему ми отримаємо граф в якому кожний маршрутизатор представлений у вигляді одного елементу, а ціною переходу між елементами буде часова величина що характеризує швидкість зєднання. Таким чином для підвищення швидкості роботи у такій мережі можна замінити випадковий вибір посередників на математично обґрунтований, що може бути знайдений застосуванням до такого графу мурашиних алгоритмів пошуку найкоротших шляхів. Мурашиний алгоритм це алгоритм що являє собою не що інше як природну модель поведінки мурах які постійно перебувають у пошуках їжі. Робота алгоритму побудована на моделюванні імовірністного руху мурах по елементам графу. Кожна мураха що досягла своєї мети повертаючись залишає на своєму шляху певну кількість феромону що приваблює інших мурах. Кількість феромону залежить від оптимальності знайденого шляху. Але даний випадок неможна зводити до звичайного формулювання задачі про коммівояжера оскільки в такому випадку ваші дії буде значно легше виявити. Отже для досягнення бажаного результату необхідно так відрегулювати алгоритм щоб він знаходив шлях який включав би максимальну кількість вузлів, і був пройдений за прийнятні часові проміжки. З самого початку свого існування мурашиний алгоритм вважався одним з кращих для вирішення подібних задач на практиці оскільки включає в себе достатню кількість налаштовуваних параметрів роботи. Таке формулювання є досить незвичним для звичайних оптимізаційних задач але в даному випадку від кількості вузлів що будуть виступати посередниками між об’єктами обміну даними і буде залежати імовірність збереження анонімності.

Впровадження описаних алгоритмів вибору посередників могло б суттєво підвищити ефективність роботи мережі. Використання подібних систем у наш час виправдовує себе, цей факт підтверджує і кількість людей що користуються даними технологіями. Використовуючи такі мережі ви можете не тільки забезпечити анонімний доступ до ресурсів але й не залежати від локальних заборон на використання певної інформації.

Зайцев О. Д. (ІСЗЗІ НТУУ „КПІ”)

ОБГРУНТУВАННЯ СТАТИСТИЧНИХ ТЕСТІВ ДЛЯ ОЦІНКИ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ОТРИМАНИХ ФІЗИЧНИХ ДЖЕРЕЛ.

Необхідність в генерації випадкових та псевдовипадкових послідовностей виникає при вирішенні різних криптографічних задач. Наприклад, криптосистеми використовують ключі, що мають бути згенерованими як випадкові послідовності. Багато криптографічних протоколів також потребують випадкові та псевдовипадкові вхідні дані на різних етапах, наприклад додаткові числа при генерації цифрових підписів, або для генерації запитів в протоколах аутентифікації. Окрім вирішення криптографічних задач, генератори випадкових послідовностей використовуються при моделюванні та симуляції процесів. Тому задача тестування випадкових та псевдовипадкових послідовностей є актуальною. Для визначення випадковості тієї чи іншої послідовності використовують сукупність статистичних тестів, що мають виявити відхилення в бінарній послідовності відносно випадковості. Ці відхилення можуть бути або внаслідок недосконалості конструкції генератора випадкової послідовності, що тестується, або внаслідок виходу з ладу генератора.

Граничні характеристики стійкості криптографічних систем захисту інформації досягаються у випадку, якщо для формування ключів, параметрів та синхромаркерів використовується генератор випадкових біт на основі фізичних датчиків шуму (джерел невизначеності) з найкращими параметрами рівноймовірності, незалежності та некорельованості. Обов’язковою умовою при формуванні ключових даних є використання джерел ентропії (невизначеності) – джерел шуму. Це забезпечує пряму та зворотню секретність, тобто непередбаченість ключових даних, що формуються. Тестом на непередбаченість випадкових послідовностей є „тест наступного біта”. Цей тест вважається пройденим, якщо після спостереження і аналізу як завгодно довгої бітової послідовності можна передбачити наступний біт, або декілька бітів з ймовірністю приблизно 0,5.

На різних етапах життєвого циклу апаратних генераторів випадкових послідовностей параметри фізичних електроних датчиків шуму, аналогово-цифрових перетворювачей і логічних схем формування випадкових бітів змінюються за рахунок старіння елементів, за рахунок змінення напруг живлення або зовнішніх кліматичних факторів.

Тому в системах з високою надійністю формування випадкових бітових послідовностей застосовують постійний апаратний контроль основних параметрів фізичних датчиків шуму, логічних схем формування віпадкових біт (tot-test), а також статистичний контроль вихідних випадкових бітових послідовностей. Відрізняють програмні методи статистичного контролю:

– перевірка статистичних властивостей випадкових бітових послідовностей малої довжини;

– постійне (оперативне) тестування (on-line test) – в процесі генерації випадкових послідовностей перевіряються всі вихідні випадкові біти;

– технологічне тестування – проводиться при включенні напруги живлення генераторів випадкових бітових послідовностей, через фіксовані часові інтервали та по запиту користувача при виникненні підозр про вплив зовнішніх факторів.

– повне тестування – здійснюється при прийомо-здаточних випробуваннях апаратних генераторів випадкових бітових послідовностей і/або при проведенні регламентних робіт.

Статистичний тест здійснюється шляхом обчислення статистичних параметрів по вихідній бітовій випадковій виборці. Статистичні параметри зазвичай обираються так, щоб вони могли бути ефективно обчислені і щоб вони відповідали нормальному розподілу – $\boldsymbol{N}$ (0,1) або χ^2-розподілу (розподілу хі-квадрат). Значення статистичних параметрів для вихідної

бітової послідовності обчислюються та порівнюються із значенням, що очікується для дійсно випадкової послідовності.

Статистичною гіпотезою, що обозначається H(0), називається ствердження відносно розподілу однієї або більше випадкових змінних. Тест статистичної гіпотези представляє собою процедуру, що ґрунтується на математичних перетвореннях значень, що спостерігаються, випадкових змінних, котрі призводять до прийняття або відкиданню гіпотези H(0). Тест тільки забезпечує вимірювання стійкості ствердження, що представлено даними, відносно гіпотези; тому, висновок тесту є не визначаючим, а ймовірнісним.

Рівнем значущості тесту – α – статистичної гіпотези H(0) називається ймовірність відкидання гіпотези H(0), коли вона є істинною.

H(0) буде позначати гіпотезу того, що задана двійкова послідовність була створена генератором випадкових біт. Якщо рівень значущості α тесту H(0) дуже високий, то тест може відкидати послідовності, котрі були насправді створені генератором випадкових біт (така помилка називається помилкою типу I, або помилкою першого роду).

В стандарті ISO/IES 18031 відзначено, що „помилка першого роду полягає в тому, що послідовність не є випадковою, коли насправді вона є випадковою”.

З іншого боку, якщо рівень значущості тесту H(0) доволі низький, то існує небезпека, що тест може прийняти послідовності, навіть якщо вони не були створені генератором випадкових біт (така помилка називається помилкою типу II, або помилкою другого роду).

Тому важливо, щоб тест мав рівень значущості, котрий близько відповідає меті; рівень значущості α між 0,001 і 0,05 може бути використовуваний на практиці.

Дана перевірка призначена для тестування статистичних властивостей випадкових та псевдовипадкових бітових послідовностей малої довжини, до котрих відносяться послідовності з довжинами n = {64, 128, 192, 256, 512, 768, 1024, 2048, 4096, 8192, 16384} біт. Саме такі довжини ключових даних використовують сучасні криптографічні алгоритми.

Необхідність тестування визначається тим, що не всі ключі і таблиці замін (сформовані на основі випадкових ключових даних) забезпечують максимальну стійкість шифрів. Так, для алгоритму DES відомо існування так званих „слабких ключів”, при використанні котрих зв’язок між відкритими і зашифрованими даними не маскується достатнім чином, і шифр відносно просто зламується.

Факт існування „слабких ключів” визнаний і для стандарту шифрування ГОСТ 28147-89. Вочевидь, нульовий ключ і тривіальна таблиця замін, по котрій кожне значення заміняється на себе самого , являються слабкими, тому що при використанні хоча б одного з них шифр достатньо просто зламується, яким би не був ключовий елемент.

Висновок про те, що навіть ідеальний генератор випадкових біт може виробляти „слабкі” ключі (оскільки вони , через рівноймовірність, мають таку ймовірність, як і решта „добрих” ключів), визначає необхідність тестування сформованих випадкових ключових даних.

Перевірка статистичних властивостей випадкових бітових послідовностей малої довжини здійснюється з урахуванням рекомендацій AIS 20 (Application Notes and Interpretation of Scheme). Перевірка включає виконання таких статистичних тестів:

– монобітний тест;

– тест серій;

– тест покера;

– автокореляційний тест.

При постійному (оперативному) контролі (on-line test) об’єм виборок випадкових бітових послідовностей та кількість тестів впливають на швидкість роботи апаратного генератора, тому для цього використовують тест AIS 31, що перевіряє бітові послідовності довжиною $\boldsymbol{n}$ = 20000 біт такими тестами:

– монобітний тест;

– тест серій;

– тест покера;
– тест довгих серій;
– диз'юнктивний тест;
– автокореляційний тест.

Тест AIS 31 оцінює конкретний бітовий блок обмеженої довжини. Тому результат тестування відноситься тільки до цього блоку і не може бути розповсюджений на апаратний генератор випадкової послідовності в цілому.

При технологічному тестуванні результати оцінюють не тільки блок біт, що перевіряється, а також свідчать про придатність всього апаратного генератора випадкової послідовності або про відповідність випадкової послідовності, що генерується, до моделі ідеального генератора випадкових біт. Для цього виду тестування рекомендовано 5 основних тестів:

– монобітний тест;
– тест серій;
– тест покера;
– тест довгих серій;
– автокореляційний тест.

Ці тестування можуть тривати від одної секунди до одної хвилини, тому довжина бітових послідовностей, що перевіряються може досягати 1 Мбайт і більше.

Повне тестування не обмежується в часі, тому об'єм виборок може досягати 100 Мбіт і більше. Тестування здійснюється у відповідності з рекомендаціями NIST SP 800-22(NIST STS). Для тестування використовується 16 статистичних тестів. Методика тестування, що запропонована NIST, є найбільш поширеною серед розробників засобів криптографічного захисту інформації і дозволяє найбільш точно виявити дефекти послідовності, що тестується. Безумовно, методика тестування згідно з рекомендаціями NIST SP 800-22(NIST STS) є найбільш повною, але для виявлення абсолютної більшості дефектів послідовностей, що тестуються, достатньо меншої кількості тестів, тому, що одні й ті ж дефекти можуть бути виявленими різними тестами.

Через це такі тести, як перевірка накопичених сум, перевірка максимальної довжини серії в блоці, спектральний аналіз на основі дискретного перетворення Фур'є, перевірка шаблонів, що перекриваються, перевірка шаблонів, що не перекриваються, перевірка випадкових відхилень, перевірка лінійної складності, можна не застосовувати в випадках, коли час для перевірки послідовності обмежений. З урахуванням цього запропоновано такий обов'язковий набір тестів, що дозволяє з великою мірою точності визначити наскільки випадковою є послідовність, що тестується:

– монобітний тест;
– частотний тест (в середині блока);
– тест серій;
– тест максимальної довжини серії в блоці;
– перевірка рангу двійкової матриці;
– універсальний тест Маурера;
– ентропійний тест.

Використання такого набору тестів дозволяє маже вдвічі скоротити час, що відведений для тестування послідовності. Саме такий набір тестів дозволяє виявити окрім звичайних статистичних дефектів послідовності (наприклад нерівномірність одиниць і нулів) і більш складні дефекти. В цьому наборі тестів в свою чергу найбільш важливими є ентропійний тест, що дозволяє виявити залежність символів в послідовності і регулярність властивостей джерела, і універсальний тест Маузера, що виявляє можливість стиснення послідовності (універсальний тест Маурера).

Залужний О.В. (ВІТІ НТУУ „КПІ”)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТА РОЗВИТКУ СИСТЕМ ОДНОСТОРОННЬОГО РАДІОЗВ’ЯЗКУ

Відповідно до ГОСТ 24375-80 односторонній радіозв’язок – радіозв’язок, при якому одна з радіостанцій здійснює тільки передачу, а інша (або інші) – тільки прийом. Прикладом таких систем є мережа пейджингового зв’язку.

Зазначимо, що сьогодні, системи з односторонньою радіопередачею вважаються застарілими і такими, що не мають ніякої перспективи в майбутньому. Звичайно, в цивільній сфері використання таких систем в подальшому буде обмеженим, але повна їх ліквідація є не розумною, оскільки в деяких ситуаціях вони можуть виявитись єдиним можливим засобом комунікації (природні та техногенні катастрофи, війни та ін.)

Особливо актуальним є використання систем одностороннього радіозв’язку відомчого призначення, що зумовлено рядом переваг, а саме:

безпека – відсутність передавача приймальної станції ускладнює можливість визначення місцезнаходження пристрою;

висока імовірність доведення повідомлення при використанні відповідних алгоритмів та правил;

необмежений час передачі повідомлення;

при застосуванні стаціонарних приймачів – забезпечення живленням від промислової мережі, і, взагалі, економна енергетика радіолінії, оскільки від кореспондента не вимагається режиму передачі;

при застосуванні складних сигналів використання загального діапазону частот, і навіть, робота безпосередньо на частотах передачі інших станцій.

В системах одностороннього радіозв’язку відомчого призначення особливо важливим питанням є передача коротких команд для управління підрозділами, або технікою (передача хибної команди, або її відсутність може призвести до виходу із ладу техніки та загибелі людей). Ці команди повинні бути передані та прийняті із як найвищою достовірністю, та унеможливлювати прийняття хибної команди.

В таких системах для доведення інформації із заданою достовірністю, як правило вводиться надлишковість, яка може бути реалізована різними способами – частотним, часовим, кодовим (використанням потужних завадостійких кодів та передавачів з достатнім рівнем вихідної потужності).

Прикладом такого використання є застосування керованих мін. Як відомо, Україна входить до числа тих країн, які приєдналися та ратифікували міжнародну угоду щодо заборони застосування, накопичення, виробництва і передачі некерованих протипіхотних мін (ППМ). Використання протипіхотних мін на 60 – 80 % збільшує час затримки супротивника. Без їх застосування значно підвищується вартість проведення оборонної операції. Значних затрат потребує утилізація протипіхотних мін, які залишились. Одним із можливих шляхів вирішення питань, що виникають внаслідок відмови від ППМ, є модернізація існуючих запасів. Створення нового модернізованого зразка ППМ з системою дистанційного управління через радіоканал дозволить перевести ППМ в категорію дистанційно керованих боєприпасів, дія Конвенції на які не розповсюджується. Тому однією із задач є створення відповідного обладнання. Високі вимоги до завадозахищенності та стійкості каналів таких радіоліній потребують спеціальних методів розробки систем складних сигналів та пристроїв їх обробки. Створення систем односторонньої радіопередачі, які гарантуватимуть безпомилкову передачу коротких команд для управління такими ППМ може бути одним із шляхів вирішення цієї проблеми.

Таким чином – розробка алгоритмів демодуляції складних сигналів, що приймаються на фоні потужних системних (ненавмисних) завад з апріорно визначеними параметрами є актуальною науково-технічною задачею для розвитку одностороннього радіозв’язку.

к.т.н. Зінченко А.О. (НУОУ)

ФАЗОВИЙ ВИМІР ВІДСТАНЕЙ ДО МНОЖИНИ ЦІЛЕЙ В MIMO-СИСТЕМАХ РАДІОЛОКАЦІЇ ТА ЗВ'ЯЗКУ

Інформаційне забезпечення бойових дій військ передбачає в якості одного з важливих завдань визначення місцезнаходження об'єктів ураження та відслідковування дислокації своїх підрозділів. Вирішення цього завдання в подальшому може бути полегшене завдяки розробці та впровадженню інтегрованих польових систем зв'язку та радіолокації, що діють за принципом MIMO. Серед можливих підходів для визначення координат джерел сигналів у таких системах заслуговує на увагу фазовий метод дальнометрії на основі використання N-OFDM сигналів, запропонований в [1]. Метою доповіді є узагальнення фазового методу дальнометрії на основі використання N-OFDM сигналів та цифрових антенних решіток (ЦАР) на випадок множини цілей.

Ключовим етапом у синтезі фазового методу виміру дальності є формування аналітичного опису відгуку ЦАР. Для цього доцільно скористатися матричною формою запису. Оскільки при фазових вимірах інформація про відстань закладена у фазах сигналів, то кінцевою метою відповідної обробки сигнальних напруг є оцінка їх квадратурних складових. Це завдання збігається за своєю сутністю з демодуляцією повідомлень, що передаються каналом зв'язку. Вважаючи, що на приймальному пристрої використовується лінійна антенна решітка, її відгук на відбитий від M цілей сигнал доцільно виразити в уніфікованому вигляді:

$$U=PA+n,$$

де U – вектор напруг прийнятих сигналів по виходу цифрової діаграми направленості ЦАР та синтезованих частотних фільтрів, P – сигнальна матриця, A – вектор комплексних амплітуд сигналів, що підлягає оцінюванню, n – вектор шумів виміру.

Оскільки в зазначеному варіанті вирішення задачі виміру відстаней від кожної з M цілей буде відбиватися багаточастотний пакет з E сигналів N-OFDM, структура сигнальної матриці P матиме вигляд $P = Q[\otimes]F$, де $[\otimes]$ – символ блокового кронекеровского добутку,

$$Q=\begin{bmatrix} Q_{11}(x_1) & \cdots & Q_{11}(x_M) \\ \vdots & \ddots & \vdots \\ Q_{R1}(x_1) & \cdots & Q_{R1}(x_M) \end{bmatrix}$$ – блокова матриця характеристик направленості антенних елементів $Q_{rt}(x_m)$ у напрямках на m-е джерело сигналів з кутовою координатою x_m, r=1, …, R – порядковий номер антенного елемента антенної решітки;

$$F=\begin{bmatrix} F_{11}(\omega_{11}) & \cdots & F_{11}(\omega_{1E}) & \cdots & F_{11}(\omega_{M1}) & \cdots & F_{11}(\omega_{ME}) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ F_{R1}(\omega_{11}) & \cdots & F_{R1}(\omega_{1E}) & \cdots & F_{R1}(\omega_{M1}) & \cdots & F_{R1}(\omega_{ME}) \end{bmatrix}$$ – блокова матриця АЧХ частотних фільтрів, синтезованих за допомогою дискретного перетворення Фур'є на E частотах відбитих від M цілей E сигналів N-OFDM.

Оптимальне оцінювання вектора комплексних амплітуд сигналів за методом максимальної правдоподібності може бути здійснене за відомими виразом $\widetilde{A}=\left(P^TP\right)^{-1}P^TU$ за умови попереднього виміру кутових координат та частот сигналів та подальшої перевірки гіпотез щодо кількості діючих джерел сигналів.

ЛІТЕРАТУРА

1. Зінченко А.О., Слюсар В.І. Фазовий метод виміру відстані в MIMO-системах радіолокації та зв'язку. // VI-й науково-практичний семінар „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення" (20 жовтня 2011 р., доповіді та тези доповідей). – Київ: ВІТІ НТУУ „КПІ", 2011. – С. 180.

к.т.н. Зінченко О. А. (НУОУ)
Возняк Р. М. (НУОУ)

МАТЕМАТИЧНА МОДЕЛЬ СПОТВОРЕННЯ СИГНАЛІВ OFDM В УМОВАХ НАВМИСНИХ ЗАВАД

Ефективним методом передачі сигналів в сучасних системах радіозв'язку є метод ортогонального частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). В таких системах висока швидкість передачі досягається за рахунок одночасної передачі даних по всіх підканалах, а швидкість передачі в окремому підканалі може бути і невисокою. Нова технологія передачі в цей час розглядається як одна з найбільш перспективних для побудови широкосмугових систем цифрового радіозв'язку по багатопроменевим каналам, що забезпечує досить високу частотну ефективність цих систем. Основними перевагами даного методу є відносно висока стійкість щодо частотно-селективних завмирань і вузькосмугових завад, а також висока спектральна ефективність.

На даний час розроблено багато методів управління параметрами OFDM-сигналу. Але при наявності в каналі навмисних завад ефективність функціонування засобів радіозв'язку з OFDM значно знижується, іноді до повної втрати переданої інформації. Спектральна щільність потужності завад при прийманні після прямого перетворення Фур'є розподіляється практично по всіх частотних підканалах, що або ускладнює, або й зовсім унеможливлює приймання OFDM-сигналу.

Найбільш універсальною і стійкою до різних способів підвищення завадостійкості, що застосовуються в системах і засобах радіозв'язку, є шумова завада в частині смуги.

Негативний вплив навмисних завад в системах радіозв'язку з OFDM може бути значно послаблений за рахунок застосування адаптивних алгоритмів формування та обробки сигналів, які дозволяють підвищити енергетичну ефективність засобів радіозв'язку. При цьому, важливим є завдання оцінки рівня спотворення сигналів з OFDM в умовах навмисних завад.

Тому в роботі досліджено вплив шумової завади в частині смуги на завадостійкість засобів радіозв'язку з OFDM для сигналів з 16-позиційною квадратурною амплітудною модуляцією.

Якщо припустити, що забезпечується ідеальна частотна синхронізація, нелінійні спотворення сигналу відсутні і ортогональність між піднесучими при проходженні каналу зв'язку не порушується, тоді піднесучі можна вважати незалежними між собою і завадостійкість для кожної окремої піднесучої групового сигналу з OFDM можна розрахувати за відомими з теорії потенційної завадостійкості формулами.

Визначено, що ефективне подавлення OFDM-сигналу з квадратурною амплітудною модуляцією досягається за рахунок концентрації потужності передавача станції завад для спотворення певної частини переданих символів. Для усунення шкідливого впливу організованих завад доцільно застосовувати такі заходи, як завадостійке кодування у поєднанні з перемежуванням, методи просторової компенсації завад, частотну адаптацію.

Запропонована модель дозволяє:

провести кількісну оцінку негативного впливу даних видів завад на якість зв'язку, що визначається ймовірністю помилкового приймання;

отримати математичні співвідношення при дії інших видів навмисних завад;

визначити заходи, спрямовані на боротьбу з навмисними завадами;

здійснювати прогнозування ймовірної стратегії постановника завад (на найгірший випадок);

проводити імітаційне моделювання радіоліній з використанням OFDM в умовах дії навмисних завад.

Розроблена математична модель може бути застосована на етапі ідентифікації адаптивних засобів радіозв'язку при реалізації механізму захисту від навмисних завад.

к.т.н. Іванченко С.О. (ІСЗЗІ НТУУ „КПІ”)

ІМОВІРНІСТЬ НЕМОЖЛИВОСТІ ВИЯВЛЕННЯ ФАКТУ ОБРОБКИ ІНФОРМАЦІЇ ЗАСОБАМИ РОЗВІДКИ ПРОТИВНИКА НА ОСНОВІ ОПТИМАЛЬНОЇ ОБРОКИ ПЕРЕХОПЛЕННИХ СИГНАЛІВ

Одним з важливих питань, при перевірці захищеності об’єктів інформаційної діяльності, в тому числі і інформації від витоку, що обробляється цифровими технічними засобами та системами, є забезпечення заданого ступеня гарантії захисту, яка може мати місце лише в тому випадку, якщо будуть використовуватись для цього обґрунтовані показники ефективності та достовірні, теоретично доведені методи їх оцінки. При цьому очевидно, що зазначена достовірність повинна базуватись на передбаченні того, що противник може використати найефективнішу техніку розвідки щодо перехоплення інформації, що реалізує майже ідеальний прийом та оптимальну оброку перехоплених сигналів.

Для об’єктів інформаційної діяльності, що потребують відповідних оцінок якості захисту, як відомо, одним із видів загроз є виявлення на них факту обробки інформації технічними засобами та системами за їх побічними випромінюваннями небезпечних сигналів в оточуюче середовищі. Останні можуть неконтрольовано розповсюджуватись на великі відстані від об’єктів та бути використані противником як їх демаскуючі ознаки. При цьому очевидно, що показником ефективності захисту є імовірність неможливості виявлення вище зазначеного факту, яка може мати місце завдяки природі згасання сигналів в середовищі та існування в ньому шумів звичайного походження як заважаючих факторів.

Виходячи з властивостей нерегулярності та невизначеності джерел інформації, в тому числі і джерел витоку, виявлення факту обробки інформації на об’єкті та, відповідно, оцінка захищеності від нього може здійснюватись за двома стратегіями:

– шляхом визначення наявності небезпечного сигналу в середовищі за максимум його демаскуючих параметрів, наприклад максимальної енергії реалізацій інформаційних знаків;

– шляхом визначення наявності небезпечного сигналу в середовищі за демаскуючими параметрами всіх інформаційних знаків. При цьому, як очевидно, оцінка захищеності повинна здійснюватись з врахуванням статистичних властивостей джерела за демаскуванням інформаційних знаків в середньому.

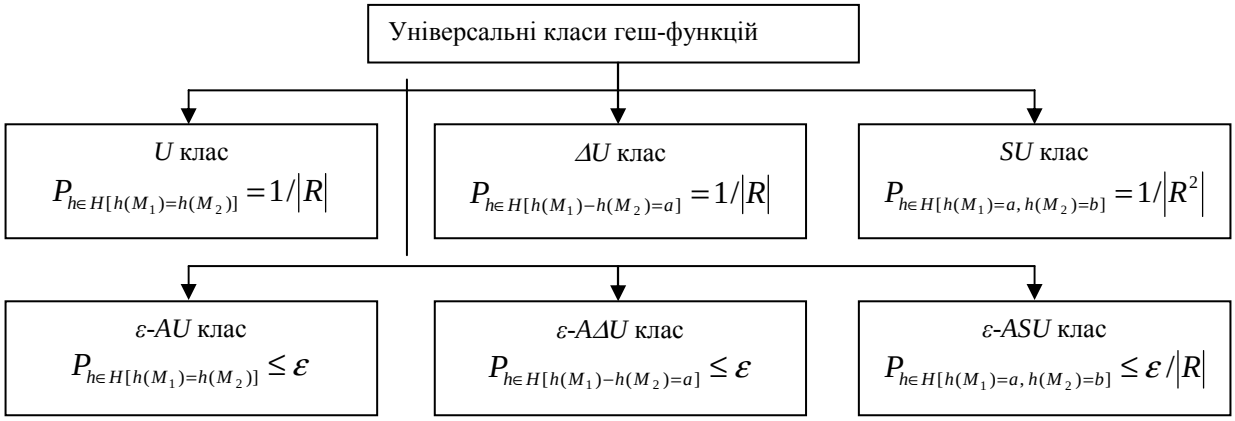
Відносно кожної стратегії, що можуть бути взятими за основу передбачуваним противником, на основі критерію оптимального прийому Котельникова (прийняття рішення щодо наявності інформаційного сигналу в ансамблі реалізацій за максимум апостеріорної імовірності) отримані співвідношення оцінки імовірності неможливості виявлення фактів оброки інформації на об’єктах інформаційної діяльності в точці можливого перехоплення противником сигналів, що враховують форми реалізацій інформаційних сигналів, їх потужності та тривалості, спектральну щільність шумових завад та час роботи об’єкту обробки та передачі інформації.

Використання зазначених показників та співвідношень дозволять кількісно оцінювати захищеність об’єктів інформаційної діяльності від загрози виявлення фактів оброки на них інформації, розробляти вимоги щодо забезпечення захищеності об’єктів та, за нормами зазначених показників, розраховувати норми на параметри шумових завад відносно інформаційних сигналів.

Ізофатов Д.О. (ВІТІ НТУУ „КПІ”)

МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ПОВІДОМЛЕНЬ В МОБІЛЬНИХ AD HOC МЕРЕЖАХ

Сучасна військово-політична ситуація в світі, досвід останніх конфліктів показують, що вирішальним фактором у сучасній війні є інформаційна перевага. Для ефективного управління військами в сучасному військовому конфлікті необхідна мобільна, надійна та живуча інформаційно-телекомунікаційна мережа. Забезпечити зростаючі вимоги мереж військового призначення неможливо без використання децентралізованих радіомереж. Прикладом таких мереж є мобільні ad hoc мережі (MANET). Одними з найбільших загроз мереж MANET є загрози цілісності та автентичності як відкритої, так і службової інформації. Механізмами забезпечення цілісності та автентичності, що використовуються сьогодні в ad hoc мережах є алгоритми генерації та верифікації MAC-кодів (Message Authentication Code), безключові геш-функції SHA-2, SHA-3, RIPEMD-160, MDx, алгоритми автентифікації користувачів на основі рукопотискання, алгоритми автентифікації на основі електронного цифрового підпису DSA, ECDSA. Метою даної роботи є аналіз механізмів забезпечення цілісності та автентичності повідомлень в ad hoc мережах з визначенням напрямків підвищення їх криптографічної стійкості та стійкості до колізій. В результаті проведеного аналізу були визначені перспективні шляхи подальшого розвитку методів забезпечення цілісності та автентичності повідомлень в мережах MANET для підвищення захищеності протоколів безпечної маршрутизації. Особливе місце серед усіх методів автентифікації повідомлень належить універсальним класам гешування, які дозволяють отримати теоретично доведену границю імовірності колізій. На рис. 1 наведена існуюча класифікація універсальних класів гешування.



Класифікація універсальних класів гешування

Аналіз підходів до побудови універсальних класів гешування дозволив виділити показники оцінки стійкості та обчислювальних витрат на криптографічні перетворення для перспективних методів автентифікації. Збільшення рівня криптографічної стійкості методів гешування на основі універсальних класів є одним зі способів підвищення надійності та захищеності протоколів безпечної маршрутизації. Розробка теоретичних засад щодо створення протоколів на основі моделі довіри, стійкість яких еквівалентна рішенню теоретико-складних задач математики, дозволить забезпечити безпеку інформації в мобільних ad hoc мережах з теоретично-доведеною криптографічною стійкістю.

В подальшій роботі планується вдосконалити існуючий алгоритм генерації та верифікації кодів автентичності повідомлень UMAC (Universal MAC) за рахунок використання в якості його ключової функції генератора псевдовипадкових послідовностей на основі криптоперетворень в групі точок еліптичної кривої.

к.т.н. Ільїнов М.Д. (ВІТІ НТУУ„КПІ”)
Воробйов А.О. (ВІТІ НТУУ„КПІ”)

РОЗРАХУНОК ХАРАКТЕРИСТИКИ НАПРАВЛЕНОСТІ ОДИНОЧНОГО КРОС-ПОЛЯРИЗАЦІЙНОГО ВИПРОМІНЮВАЧА

Найважливішим елементом будь-якої системи зв’язку з рухомими об’єктами є базова станція, а відповідно і її антенно-фідерний пристрій, як основна складова частина цього елемента, яка представляє собою досить складний радіотехнічний пристрій.

Аналізуючи особливості поширення радіохвиль на лініях радіозв’язку з рухомими об’єктами, таких як загасання, багатопроменеве розповсюдження, інтерференція та завмирання, а також принципи побудови систем мобільного радіозв’язку можна сформувати основні вимоги антенного пристрою базовою станції, найважливішими з яких є забезпечення необхідного коефіцієнта підсилення та формування заданої характеристики направленості в горизонтальній площині. Крім виконання цих вимог, на антени базових станцій в наш час покладаються функції по підвищенню рівня стабільності сигналу в точці прийому. Одним із направлень реалізації даних функцій є використання на базових станціях кросполяризаційних панельних антен – синфазних вібраторних антенних решіток, викоканих на плоскому екрані.

В більшості випадків у якості випромінюючих елементів таких антенних решіток виступають симетричні вібратори, розташовані над плоскою відбиваючою поверхнею (екраном) і орієнтовані під деяким кутом α відносно осі антенної решітки..

Розглянемо задачу про поле випромінювання такого похилого симетричного вібратора.

Прямих формул для розрахунку даного поля немає. Тому представимо поле такого симетричного вібратора, як сукупність полів вертикально та горизонтального вібраторів, що є проекціями реального вібратора.

Отже, поле випромінювання симетричного вібратора, розташованого під деяким кутом α відносно осі x (рис. 1а) можна представити у вигляді складових полів двох вібраторів, один з яких орієнтований по осі x (вертикальна складова) (рис. 1б), а інший - по осі y (горизонтальна складова) (рис. 1в), довжини плечей яких будуть дорівнювати проекціям реальних вібраторів на вказані осі.

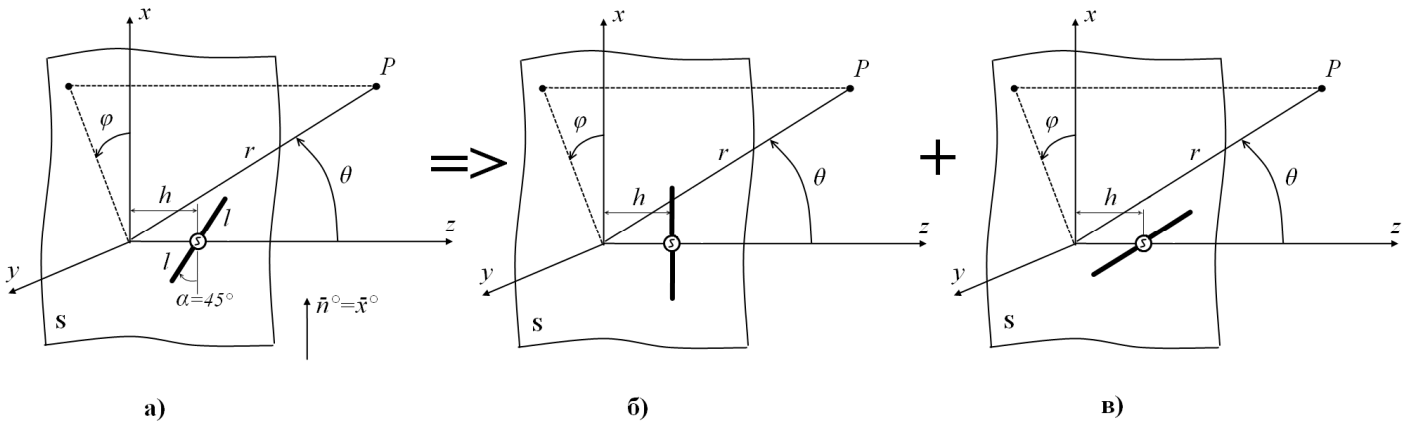


Рис. 1. Апертурна модель похилого симетричного вібратора.

Тоді, згідно з апертурною моделлю (рис. 1), вирази для складових електромагнітного поля (ЕМП) такого вібратора можна виразити наступними виразами:

– для вертикальної складової:

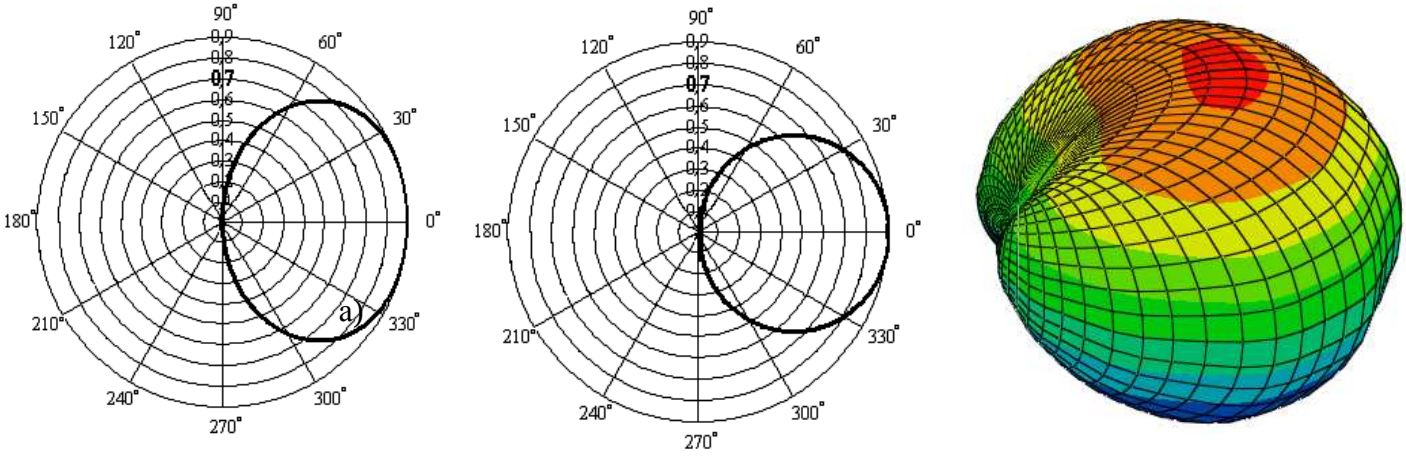
, (1)

де h – відстань вібратора від екрану;

– для горизонтальної складової:

(2)

Нехай в якості випромінюючого елемента буде виступати напівхвильовий симетричний вібратор з висотою підвісу (відстанню над екраном) $h = \lambda/4$ та кутом нахилу $\alpha = 45°$. Тоді його діаграми направленості двох ортогональних площинах будуть мати вид, представлений на рис. 2:



а) вертикальна складова ЕМП б) горизонтальна складова ЕМП в) просторова ДН

Рис. 2. Діаграми направленості похилого симетричного вібратора

Отримані результати наочно показують, що ширина діаграм направленості в горизонтальній площині складає: 2= 120°, 2 = 90°.

Вирішення задачі про поле випромінювання похилого симетричного вібратора над плоским екраном дозволяє зробити наступні висновки:

– по перше, за допомогою крос-поляризаційних антен можна обслуговувати зони покриття сектором в 90°;

– по-друге, виготовлення антенних решіток з випромінювачами у вигляді похилих симетричних вібраторів дозволяє зменшити масо-габаритні параметри антен, тим самим суттєво зменшити вітрове навантаження;

– по-третє, приймальні крос-поляризаційні антени дозволяють підвищити рівень сигналу в точці прийому.

ЛІТЕРАТУРА

1. Бузов А.Л. Антенно-фидерные устройства систем сухопутной подвижной радиосвязи / Бузов А.Л., Казанський Л.С., Романов В.А. – М.: Радио и связь, 1997. – 150 с.

2. Климашов И.А. Антенны для базовых станций сотовой связи / Технологии и средства связи. 2002. – 272 с.

3. Лавров А.С. Антенно-фидерные устройства. Учебное пособие для вузов. / Лавров А.С. Резников Г.Б. – М. : Советское радио, 1974. – 386 с.

4. Резников Г.Б. Антенны летательных аппаратов / Резников Г.Б. – М.: Советское радио, 1967. – 415 с.

к.т.н. Ільїнов М.Д (ВІТІ НТУУ„КПІ”)
Кравченко В.В (ВІТІ НТУУ„КПІ”)

ФРАКТАЛЬНІ АНТЕНИ

На сьогоднішній день, в світі існує безліч різних видів антен, в залежності від призначення і області застосування вони мають різну конструкцію. Тип антен, про який піде мова в цій статті, з’явився порівняно недавно, і принципово відрізняється від відомих, стандартних і загальноприйнятих рішень, в цих антенах апертура антени (її геометричні розміри) може бути зменшена в рази, що в метровому діапазоні дуже сильно позначиться як на вартості самої антени, так і на мобільності антени і антенної системи в цілому. Це новий напрямок в антеною техніці, а саме фрактальні антени вже на сьогоднішній день знайшли практичну реалізацію в різних радіотехнічних пристроях. Фрактальна антена – це антена, активна частина якої має вигляд самоподобной кривої або якийсь інший подібно делящейся або складається з подібних сегментів фігури.[1] Що б мати більш зрозуміле уявлення про таку форму, потрібно звернутися до фрактальної геометрії. Фрактальна геометрія стверджує, що практично будь-які природні форми з математичної точки зору є фракталами. Фрактал – від латинського: Fractus – зламаний, розбитий. Отримати фрактал можна розділивши фігуру на все більш дрібні об’єкти, розподіл може здійснюватися нескінченно. Таким чином, будь-яка з отриманих фігур буде ділитися на подібні, і в свою чергу бути частиною такої ж фігури. Побудова фракталів засноване на неевклідової геометрії (фрактальної геометрії) засновник якої доктор математичних наук, Бенуа Мандельброт. Прості приклади фрактальних множин це криві побудовані за принципом кривої Коха, опис якої у 1904р. запропонував шведський математик Нільс Фабіан Хельге фон Кох. Крива Коха є типовим геометричним фракталом. Процес її побудови виглядає наступним чином: беремо одиничний відрізок, поділяємо на три рівні частини і замінюємо середній інтервал рівностороннім трикутником без цього сегмента. В результаті утворюється ламана, що складається з чотирьох ланок довжини 1/3. На наступному кроці повторюємо операцію для кожного з чотирьох одержані ланок і т. д ... Отримана крива і є крива Коха (рис. 4).

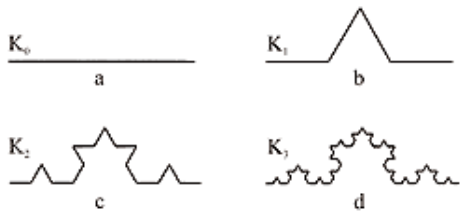
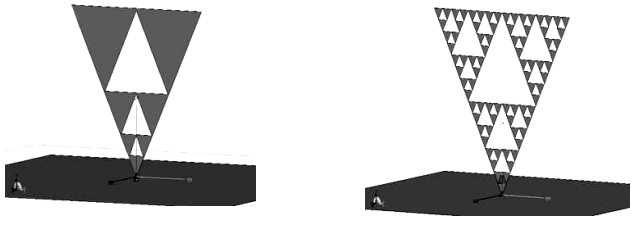


Рис 4 Алгоритм побудови кривої Коха

З появою нових стандартів і технологій (GSM, CDMA, Wi-Fi та ін) і освоєнням нових частотних діапазонів, а також з впровадженням в повсякденне життя пристроїв персонального радіодоступу створюються антени, які відповідають вимогам часу. Однією з таких антен є фрактальна антена, виконана на основі трикутника Серпинського (рис. 1).



а) б)

Рис. 1 Фрактальна антена Серпинського (а), модифікована антена (б)

Щоб його отримати, потрібно взяти (рівносторонній) трикутник з внутрішністю, провести в ньому середні лінії і викинути центральний з чотирьох утворилися маленьких трикутників. Далі ці ж дії потрібно повторити з кожним з решти трьох трикутників, і т. д. (рис. 2).

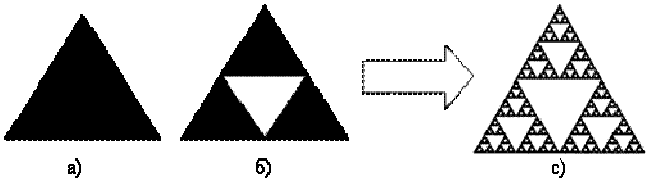


Рис 2. Етапи побудови килима Серпінського

Розглянемо антену Серпинського отриману шляхом проведення п’яти ітерацій. Таким чином виходить п’ять антен різного масштабу (позначені колами на рис.3), найменша з яких є простим трикутником. Якщо знехтувати внеском від центральної області на характеристики і допустити, що струм від фідера концентрується в тій області антени, яка порівнянна з довжиною хвилі, то можна очікувати, що така структура буде подібна п’яти симетричним вібраторам з трикутними плечима, кожен з яких працює на своїй резонансній частоті. [2] Масштабний коефіцієнт для цих п’яти вібраторів дорівнює двом (δ = 2), це означає, що висоти трикутників Серпинського будуть рівні 89; 44. (рис 3).

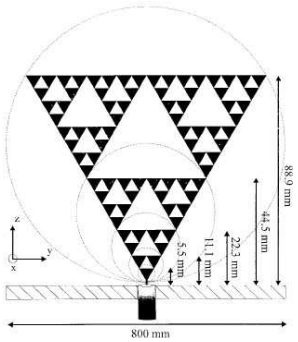


Рис 3. Фрактальна антена Серпінського, синтезована п’ятьма ітераціями

Одже, завдяки компактності і широкосмуговим властивостям, фрактальні антени здобули широкого практичного застосування не тільки в мобільних пристроях і стільникових системах зв’язку на базових станціях, а й в бездротовому зв’язку(в Bluetooth, Wi-Fi і GSM стандартах). Своє застосування фрактальні антени також знаходять у медицині і військових додатках. Таким чином, в одному гаджеті, наприклад, в мобільному телефоні, смартфоні, КПК, вдалося розмістити всі ці пристрої . Перераховуючи все вище сказане можна зробити висновок, що антени побудовані за принципами фрактальної геометрії мають максимально можливий коефіцієнт корисної дії.

ЛІТЕРАТУРА

1. Кроновер Р. М. Фракталы и хаос в динамических системах. Основы теории. М., Постмаркет, 2000.

2. Потапов А.А. Фракталы в радиофизике и радиолокации: топология выборки. 2005. – 848 с.

к.т.н. Ільїнов М. Д. (ВІТІ НТУУ „КПІ”)
Кузнєцов М. І.(ВІТІ НТУУ „КПІ”)

НИЗЬКОПРОФІЛЬНА АНТЕНА З КРУГОВОЮ ПОЛЯРИЗАЦІЄЮ ПОЛЯ

В теперішній час в радіотехнічній практиці (радіолокації, радіотелеметрії, радіоуправління, космічного радіозв’язку) находять широке застосування антен з обертаючою поляризацією електромагнітного поля.

Такі антенні пристрої збуджують в оточуючому просторі поля, вектор напруженості якого в процесі розповсюдження, міняє свою орієнтацію. За період високої частоти вектор робить один повний поворот в площині, перпендикулярним рухом хвилі.

Застосування антени з обертаючою поляризацією представляє значний практичний інтерес. В цілому такі антени застосовуються: для збільшення дальності виявлення цілей в радіолокації; для зменшення завад від дощу, снігу і т.д.; для забезпечення надійності прийому сигналів радіосистеми управління і контролю літаючими апаратами; для зменшення реакції дзеркала на випромінювач в дзеркальних антенах.

В останні роки визначилось нове направлення розвитку антен НВЧ – низькопрофільні антенні пристрої. Поява такого класу антен визвала збільшення потреби в легких, тонких, конформних і дешевих антенних пристроях, які можна розміщувати на ракетах і других літальних апаратах, не порушуючи їх аеродинамічні якості.

Судячи по даним зарубіжних друків, в теперішній час в США і ряду других держав приділяється серйозна увага роботам в тому напрямку. Створено і запатентовано значне число зразків низько профільних одноелементних антен і антенних решіток. Вирішений ряд важливих проблем теорії низькопрофільних антенних решіток [1].

В більшості випадків такі антени виконуються на тонкій (у порівнянні з довжиною хвилі) діалектричні підстилки над заземленою площиною (екран). Особисто антенний (випромінюючий) елемент може представляти собою квадратну, прямокутну, круглу або еліптичну пластину. Низькопрофільні антени (НПА) формують поле випромінювання з лінійною або круговою поляризацією. На рис. 1 представлені два варіанти низько профільних антен з полем кругової поляризації.

При збудженні прилягаючих сторін квадратного або круглого випромінюючого елемента (ВЕ) рівними сигналами, маючи фазовий зсув 90^0, виникають поля випромінювання з круговою поляризацією. На рис. 1 введені наступні позначення: напралений розгалужувач (НР), 1– випромінюючий елемент, 2 – шлейфний НР. Кругова поляризація може бути досягнута також збудженням кута квадратного низько профільного випромінювача (рис. 1б). в цьому випадку розмір А випромінюючого елемента вибирається трохи менше $\lambda d/2$, а розмір В – трохи більше $\lambda d/2$, де λd – довжина хвилі в діалектрику.

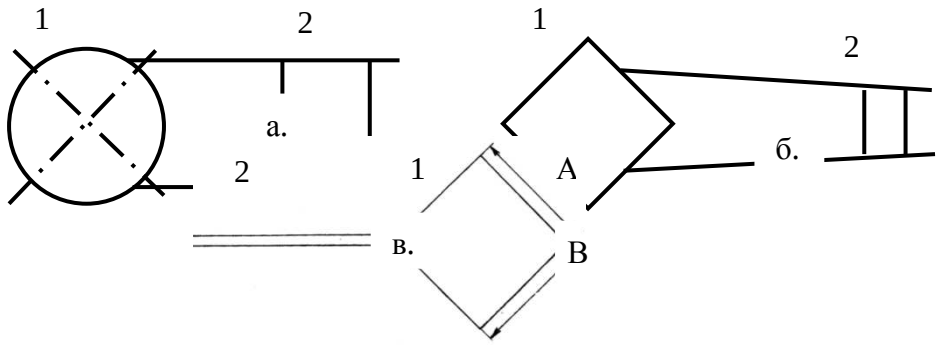
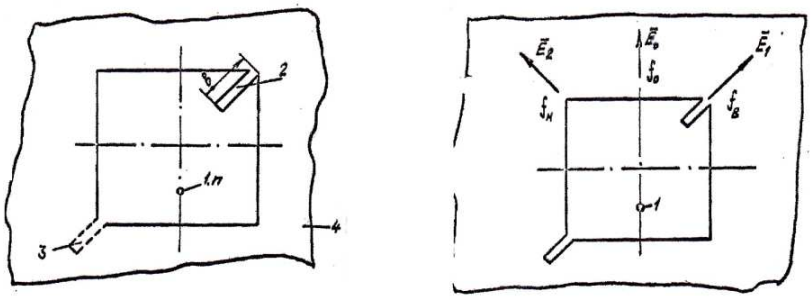


Рис.1 Типи низькопрофільних антен з круговою поляризацією

З практичної точки зору найбільший інтерес представляють НПА з круговою поляризацію при одній точці збудження, аналог якої зображено на рис. 1в . Однак таке технічне рішення має ряд суттєвих недоліків, а саме: необхідність використання

узгоджуючих пристроїв, розміщених в розкриві випромінювачів; планарний спосіб збудження випромінюючого елемента, що приводить до ефекту затемнення; втрати в лініях живлення, так як використовується відкрита полоскова лінія.

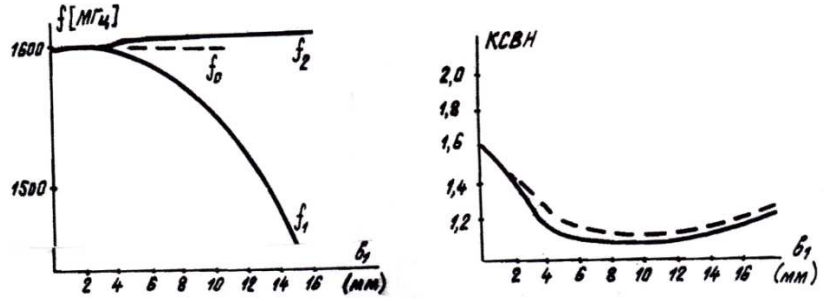
В роботі розглянуто нове технічне рішення по краях НПА з круговою поляризацією випромінюючого поля яке показано на рис. 2 . НПА з круговою поляризацією поля містить квадратний ВЕ (1), неоднорідні у вигляді щілини (2) або внетуля (3), екран (4).



а. б.

Рис. 2 Низькопрофільна антена з круговою поляризацією поля

При введенні неоднорідності в область між пластинами основна мода вироджується у дві ортогональні моди (рис. 2б) зі своїми вхідними імпедансами. При $f_н \approx f^e_0$, де $f_н, f^e_0$ – частоти мод і різними по характеру реактивних частин вхідного імпеданса поле випромінювання має кругову поляризацію, що підтверджується експериментальними дослідами. На рис. 3 показано результати експериментальних досліджень НПА неоднорідності на ВЕ.



а. б.

Рис. 3 Результати експериментальних досліджень низько профільної антени неоднорідності на випромінюючому елементі

На ВЕ результати практичних досліджень НПА з круговою поляризацією і торцевим, тоновим збудженням наглядно демонструє працездатність пропонує мого технічного рішення. Введення неоднорідностей ВЕ дозволяє не тільки створити поле кругової поляризації, але і отримати при необхідності двох частотну антену з лінійною поляризацією (рис.3а), при цьому не порушується узгодження випромінювача з фідером.

Таким чином НПА з круговою поляризацією при одній торцевій точці збудження суттєвим чином дозволяє спростити компоновку АР на основі подібних випромінювачів збільшити надійність, а також зменшити затрати на їх виготовлення.

ЛІТЕРАТУРА

1 Ломан В.І., Ільїнов М.Д. Низькопрофільні антенні пристрої М. „Радио и связь”, Ж. „Зарубежная радиоелектроника”, 1981 г., №10.

к.т.н. Ільїнов М.Д (ВІТІ НТУУ “КПІ”)
Макаренко М.Ю. (ВІТІ НТУУ “КПІ”)

АНТЕННІ ПРИСТРОЇ З ПОЛУСФЕРИЧНОЮ ДІАГРАМОЮ НАПРАВЛЕНОСТІ

.

Супутникові системи зв’язку (ССС) отримали широке поширення серед систем передачі інформації. Вони дозволяють отримувати доступ до послуг зв’язку там, де використання наземних або бездротових каналів не виправдано економічно або неможливо. Також ССЗ використовуються для організації каналу зв’язку між географічно віддаленими регіонами або країнами з нерозвиненою комунікаційною інфраструктурою.

Відносно новим напрямом розвитку ССС являється система супутникового зв’язку з рухомими об’єктами.Реалізація цього напрямку призвела до створення універсальної персональної антени супутникового зв’язку, абонент якої повинен бути доступний в будь-якій точці землі і мати доступ до телекомунікаційної мережі за допомогою переносного терміналу.

Супутникові системи радіонавігації 2-го покоління GPS (Global Positioning system)-Navstar (США) і ”Глонасс” (Глобальна навігаційна супутникова система, Росія), розгорнуті до теперішнього часу забезпечує нічне визначення місцеположення об'єкта (до одиниць метрів), дозволяють вирішувати безліч проблем в різних галузях народного господарства: авіації, морському та наземному транспорті, картографії, землеустрою і т.д.

Основу радіонавігаційної системи складають радіомаяки, які обертаються в космічному просторі навколо землі на висотах порядку 20 тис.км. і приймачі, що знаходять на поверхні Землі, координати яких підлягають визначенню.Геометрія спостереження споживачем (приймачів) навігаційних космічних апаратів (КА), визначає вимоги до зовнішніх характеристик антенного пристрою, як одного з найважливіших елементів всієї навігаційної супутникової системи.Ця вимога виражається в необхідності формування напівсферичної діаграми направленості, що в антенній техніці представляє досить складну задачу.

В даний час використовуються наступні типи антенних пристроїв (АУ), які дозволяють в деякій мірі вирішити цю проблему.Це такі антени як комбінація електричного і магнітного диполів, турнікетної антени з похилими плечима, сферичні, спіральні, низькопрофільні (мікрополоскові) антени і т.д.

В даній роботі проводиться аналіз зовнішніх характеристик турнікетної антени, виконаної на магнітних випромінювачах(щілин), яка відрізняється компактністю,аеродинамічністю, простим конструктивним виконанням.

Амплітудно-фазовий розподіл струмів на випромінюючих щілинах відомій,прив’язка антени до системи координат показано на рис.1

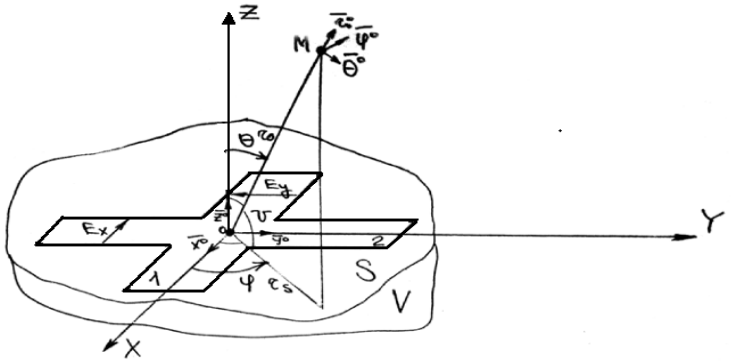


Рис.1 Щілинна турнікетна антена

Згідно методу Герца електричний вектор поля випромінювання антени, згідно[1] з відомим разподіленням джерел дорівнює:

$$\overline{E}(M) = \frac{ik\phi(\varphi o)}{4\pi}\int_v \{Wo[\overline{\varphi^o} - \overline{j^e}]\overline{r_o^o} + [\varphi^0\, j^м]\}e^{ikr\cos v}\, dv \qquad (1)$$

де, $\overline{j^e}$ и $\overline{j^м}$: вектори щільності еквівалентних електричних і магнітних струмів.

Спочатку вирішується задача про поле випромінювання одиночної щілини, яка розташована вздовж осі Х,при цьому:

$$\overline{j^e}=0;\ \overline{j_1^м} = -[\overline{n^0}\overline{Eм}] \neq 0; \qquad (2)$$

Тоді вираз для поля випромінювання одиночної щілини буде мати вигляд:

$$\overline{E}_1(M) = \frac{ik\psi(\varphi o)}{4\pi} EyL_{щ}(\theta^0 \sin\varphi + \overline{\varphi^0} + \cos\varphi) \qquad (3)$$

Аналогічно отримуєму вираз для 2-ої щілини, орієнтованої вздовж осі У:

$$E_2(M) = \frac{ik\psi(\varphi_0)}{4\pi} Ex\, L_{щ}(\overline{\varphi^0}\cos\theta\sin\varphi - \overline{\theta^0}\cos\varphi) \qquad (4)$$

Очевидно, що сумарне поле в точці нагляду буде визначатися наступним виразом:

$$E_2(M) = E_1(M) + E_2(M) \qquad (5)$$

При умові рівності полів Ех=Еу на випромінюючих щілинах, отримуємо:

$$E_м(M) = \frac{ik\psi(\varphi_0)}{4\pi} L_{щ}(\overline{\varphi^0}\cos\theta\sin\varphi - \overline{\theta^0}\cos\varphi) \qquad (6)$$

Або взявши модуль з цього виразу, отримуємо

$$F(M)=\sqrt{\cos^2\theta\{\sin\varphi - \cos\varphi\}^2 + [\cos\varphi + \sin\varphi]^2} \qquad (7)$$

З цього виразу наглядно слідує, що в двох ортогональних площинах характеристика направленості буде визначатися одним і тим же виразом:

$$F(M)=\sqrt{\cos^2\theta + 1} \qquad (8)$$

В вертикальній площині діаграма направленості має квазіполусферичний характер,коефіцієнт нерівномірності не більше -3дб.

Таким чином ,випромінювач у вигляді хрестообразної щілинної антени с кругувою поляризацією випромінюючого поля дозволяє формувати ХН с полусферичною ДН.

ЛІТЕРАТУРА

1. Лавров А.С.,Резников Г.Б. Антенно- фидерние устройства. М., „Сов.радио”,1974 г.

к.т.н. Ільїнов М. Д. (ВІТІ НТУУ „КПІ”)
Павлюк О. М.(ВІТІ НТУУ „КПІ”)

ЕЛЕКТРИЧНІ ХАРАКТЕРИСТИКИ КОЛІНЕАРНИХ АНТЕН

Аналіз електричних характеристик колінеарних антен, виконаних по схемі Франкліна показав основні їх недоліки, такі як: втрата коефіцієнта підсилення, за рахунок переміщення ефективних площин випромінюючих елементів; вузькодіапазоність по вхідному опору; необхідність застосування узгоджуючих пристроїв при живлені антени кооксиальним кабелем з хвильовим опором 50 або 75 Ом.

В даній роботі проведені теоретичні дослідження одного із найважливіших параметрів колінеарної антени Франкліна Za – вхідного опору, в залежності від фазової помилки фазозміщуючого пристрою між випромінюючими елементами, а також в залежності від їх конструктивних розмірів ($2a_1$, $2a_2$ – діаметри провідників; $2l_1$, $2l_2$ – лінійні розміри випромінювачів).

В основу розрахунку вхідного опору антени Франкліна покладена інженерна методика, тобто колінеарну антену ставлять у відповідності з довгою еквівалентною лінією з втратами [1]. В якості втрат виступає реальний опір випромінюючих елементів. Шляхом перерахунку визначається формула для розрахунку опору колінеарної антени, виконаної по схемі Франкліна. Вираз який дозволяє розрахувати вхідний опір має наступний вигляд:

$$Z_{A-A} = \rho_{в2}\frac{Z_н \sin Kl_2 - j\rho_{A2}\cos Kl_2}{\rho_{A2}\sin Kl_2 - jZ_н \cos Kl_2}$$

де: $Z_н = R_{\Sigma n2} + \frac{\rho_{a2}^2}{Z_{1-1}}$ – опір навантаження;

ρ_{a2}=120($\ln\frac{\lambda}{4a} - 1$) – хвильовий опір 2-го вібратора колінеарної антени;

l_2 – довжина плеча другого вібратора.

Опір навантаження ($Z_н$), представляє собою сукупність опорів випромінювання ($R_{\Sigma n}$) периферійних вібраторів, параметрів фазозміщуючого пристрою (θ – фаза, що дорівнює 180˚) перерахованих до другого вібратора.

Очевидно, що зміна параметрів фазозміщуючого пристрою, геометричних параметрів випромінювачів призводить до зміни вхідного опору колінеарної антени.

На Рис. 1 наглядно показана значна зміна активного опору та різка поява реактивної частини опору відносно помилки виконання фазозміщуючого пристрою. Тут ми наглядно бачимо, що при не значній помилці у виконані фазозміщуючого пристрою, при цьому відбувається збільшення активної складової вхідного опору колінеарної антени та поява його реактивної складової, що є негативним явищем.

Під час аналізу цього недоліку було знайдено рішення, а саме, при зміні діаметру випромінюючих елементів смуга по вхідному опору збільшується або зменшується. Таким чином, при діаметру випромінюючих елементів d=0.03м смуга по вхідному опору збільшується, відхилення активного значення опору від ідеального ($\ell=\lambda/2$) не є значним, а реактивна складова дорівнює нулю майже у всій смузі. При збільшені або зменшені діаметру випромінюючих елементів вище зазначений недолік знову проявляється. Таким чином, щоб досягти збільшення смуги по вхідному опору, а також щоб позбутися реактивної складової опору найбільш оптимальним діаметром випромінюючих елементів вважається d=0.03м.

Re(Z_{A-A}), Im(Z_{A-A}) Re(Z_{A-A}), Im(Z_{A-A})

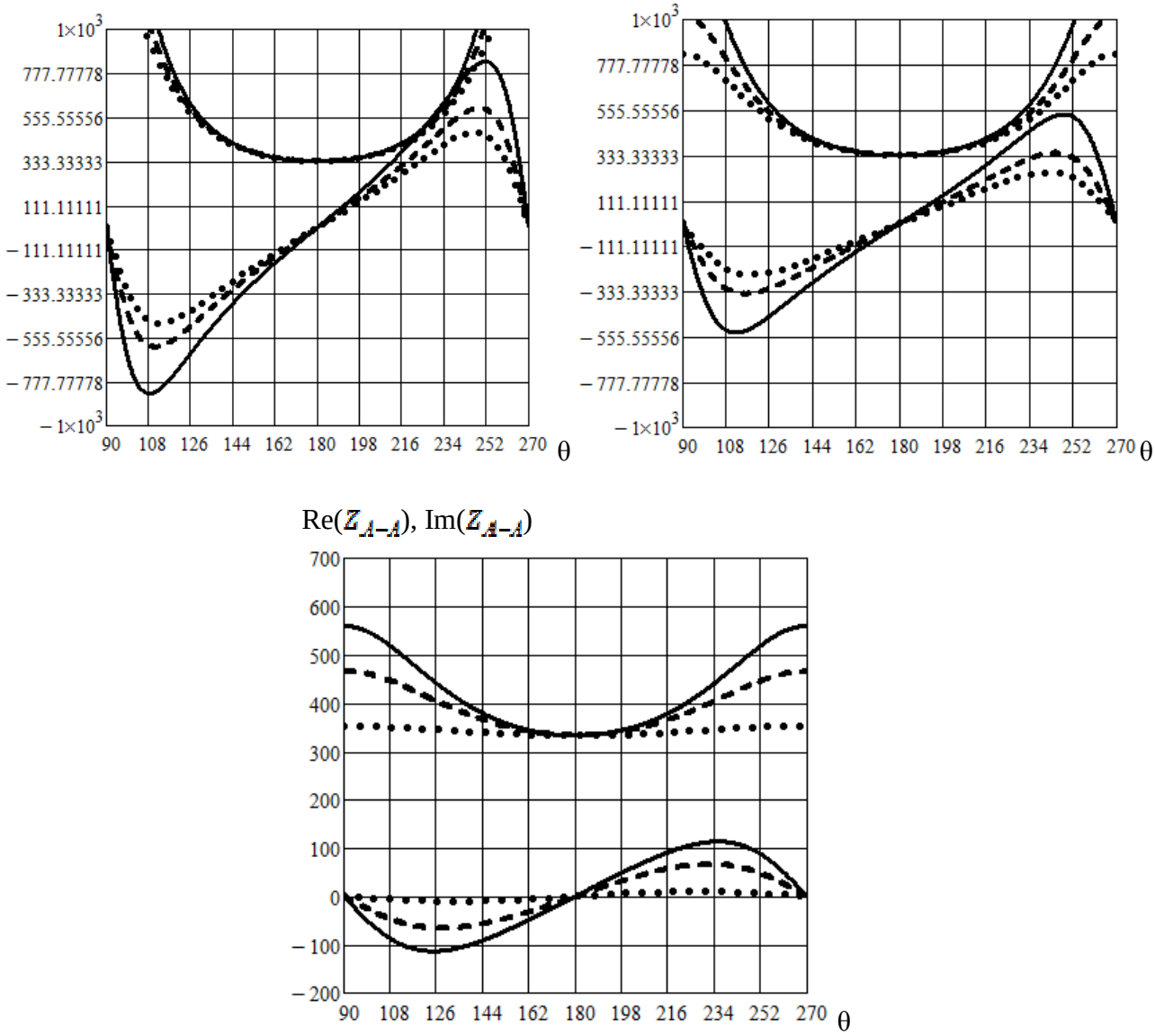


Рис. 1. Графіки залежності вхідного опору колінеарної антени.

ЛІТЕРАТУРА

1. Цибізов К.М., Ільїнов М.Д., Дзюба О.М. Методика розрахунку вхідного опору колінеарних антен, колінеарних решіток з кінцевим живленням. – К.: Журнал ,,Зв'язок", випуск №3, 2003. – 24 с

2. Ерохин Г.А. Чернышев О.В. Антенно-фидерные устройства и распространение радиоволн. – М.: Горячая линия – Телеком, 2007. – 491 с.

к.т.н. Ільїнов М.Д (ВІТІ НТУУ „КПІ”)
Чорненький О.В. (ВІТІ НТУУ „КПІ”)

ЕЛЕКТРИЧНІ ХАРАКТЕРИСТИКИ ПОДВІЙНОЇ ЛІНІЙНОЇ АНТЕННОЇ РЕШІТКИ

Вібраторні випромінювачі широко використовуються як елементи антенних решіток у метровому і дециметровому діапазоні хвиль.

Широке застосування вібраторних антенних решіток обумовлено рядом їх переваг: відносно малою масою,стійкістю до атмосферних зовнішніх впливів, можливостями складання та швидкого розгортання в мобільних радіотехнічних системах, реалізацією довільної поляризації та управління поляризаційною характеристикою випромінюваного поля, а також управління діаграмою направленості (ДН).

Конструктивно антенні решітки вібраторного типу виконані у вигляді сукупності симетричних вібраторів, розташованих над циліндричною поверхнею (трубою) або вібраторними антенами з плоским екраном які в технічній літературі дістали назву „панельні антени”.

В діапазоні метрових хвиль і в нижній частині дицеметрового діапазону в якості антен базових станцій з коефіцієнтом підсилення від 4 до 12 дБ використовують синфазні антенні решітки різноманітної компоновки: лінійні синфазні антенні решітки;подвійні лінійні синфазні антенні решітки;подвійні лінійні синфазні антенні решітки,с суміжним повертом випромінюючих елементів на 90^0,під назвою „Чінаре”; нелінійна синфазна антенна решітка. Саме широке застосування знайшли ленійні вібраторні антенні решітки.

Представлені антенні решітки мають вагомий недолік – велику нерівномірність діаграми направленості в горизонтальній площині.

Рівномірність випромінювання електромагнітного поля в азимутальній площині можна істотно поліпшити якщо конструкцію подвійної лінійної синфазної антенної решітки доповнити діаметральнорозташованими поруч випромінювачами. Конструкція такого випромінюючого елемента антенної решітки показана на рис 1.

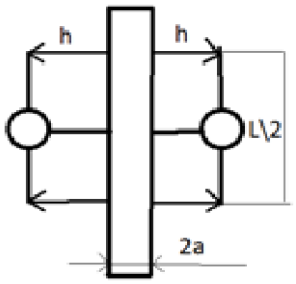


Рис.1. Подвійна антенна решітка із симетричним напівхвильвим вібратором над циліндричною поверхнею

Вираз для характеричтики спрямованості ДЛАР має наступний вигляд:

$$f(\theta,\varphi) = f_0(\theta,\varphi)\cdot N(\theta)\left\{2\left[v_0 + \sum_{n=1}^{\infty} j^n \cos n\,\varphi + \sum_{n=1}^{\infty} j^n Vm\cos[n(\varphi+\pi)]\right]\right\}$$

де $f(\theta,\varphi)$ – характеристика спрямованості симетричного вібратора у вільному просторі.

На Рис 2. представлена залежність коефіцієнта спрямованої дії ДЛАР від відстані між випромінюючими елементами та їх кількості, а також залежність коефіцієнта нерівномірності від відстані випромінювача від відбиваючої поверхні

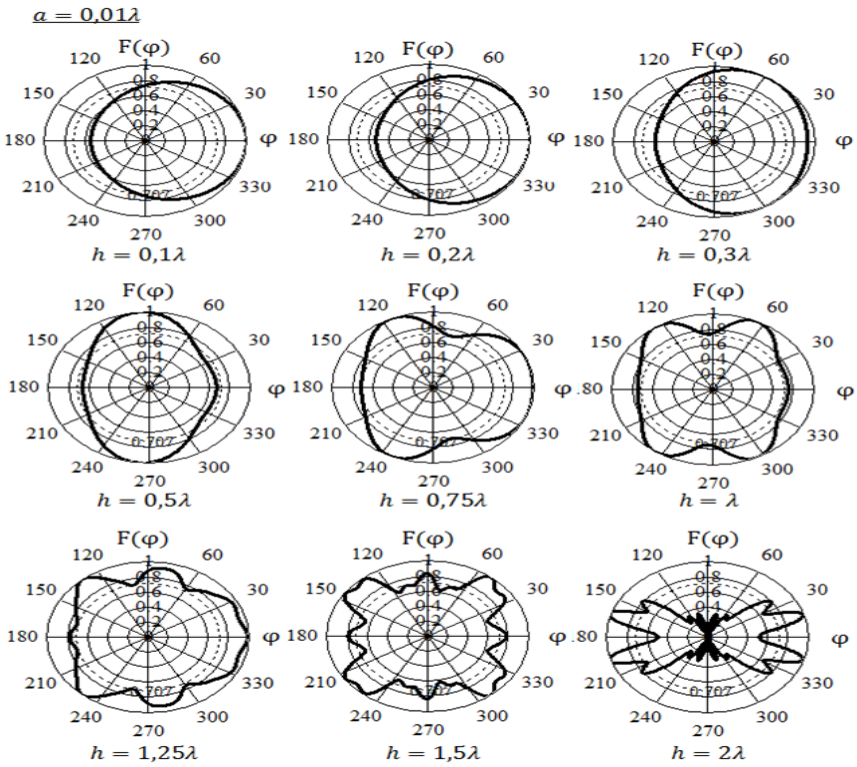


Рис 2.ДН $F(\varphi)$ подвійного симетричного напівхвильового вібратора над циліндричною поверхнею при a/λ=0,01

На рис 3 представлена залежність коефіцієнта нерівномірності від відстані випромінювача від відбиваючої поверхні.

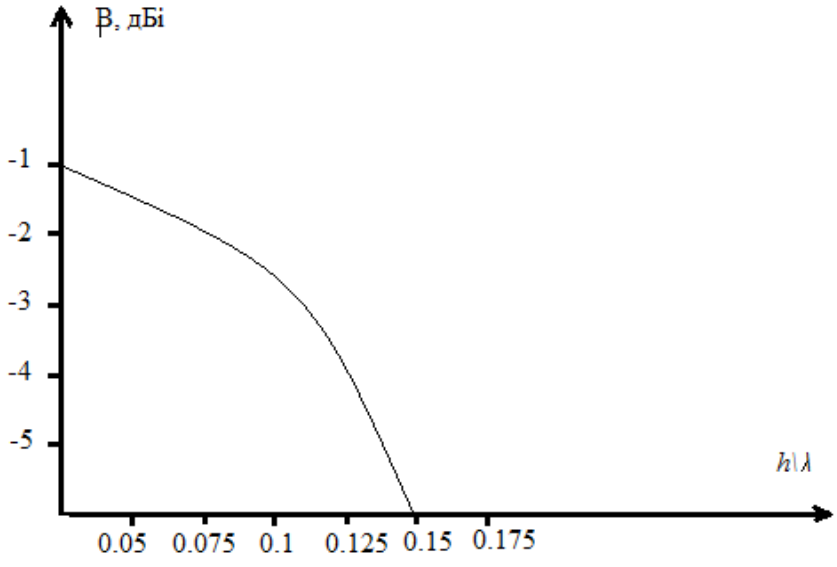


Рис 3. Залежність коефіцієнта нерівномірності $\beta = f\left(\frac{h}{\lambda}\right)$ подвійного симетричного напівхвильового вібратора над циліндричною поверхністю при $\frac{a}{\lambda} = 0.1$

Таким чином, можна сказати, щопри теоретичних дослідженнях електричних характеристик ДЛАР такі решітки показують хороші показники коефіцієнта неріномірності та в цілому шорокі функціональні можливості в плані формування характеристики спрямованості.

к.т.н. Ільїнов М.Д. (ВІТІ НТУУ „КПІ”)
Чорний О.В. (ВІТІ НТУУ „КПІ”)

ЗОВНІШНІ ХАРАКТЕРИСТИКИ БАГАТОВХОДОВОЇ НИЗЬКОПРОФІЛЬНОЇ АНТЕНИ

Низькопрофільна антена являє собою дві металеві пластини, рознесені між собою на відстані $d << \lambda$, де λ – робоча довжина хвиль.

Одна з пластин (верхня) грає роль випромінюючого елементу, інша (нижня) – роль екрану.

В обсязі між пластинами вводиться вузол зі збудженням, розрізняють такі типи збудження: струмове, коли провідник зі струмом вводиться в обсяг між пластинами; планарне – коли лінії живлення розміщені у площині верхньої пластини; безконтактне (електромагнітне) – коли лінія живлення розміщується планарно між пластинами. Збудження низькопрофільної антени може бути несиметричним і симетричним, коли в об’єм між пластинами вводиться кілька джерел, симетрично розміщених відносно центру випромінювання енергії [1].

Антени з декількома джерелами носять назву багатовходових антен. Вони знайшли широке застосування в організації базових станцій систем рухомого радіозв’язку, основною задачею яких є забезпечення великої канальної ємності та незалежної одночасної роботи декількох приймачів та передавачів

Одним із представників багатовходових антен являється багатовходова низькопрофільна антена.

Низькопрофільна антена із симетричним живленням відноситься до класу багатовхідних антен, при цьому кардинально змінюються її функціональні можливості, а саме: з’являється можливість формування на одному розкриві декількох характеристик спрямованості різного виду; з’являється можливість підключення до однієї антени 2-х, 3-х радіостанцій одночасно; поліпшуються внутрішні характеристики низькопрофільних антен.

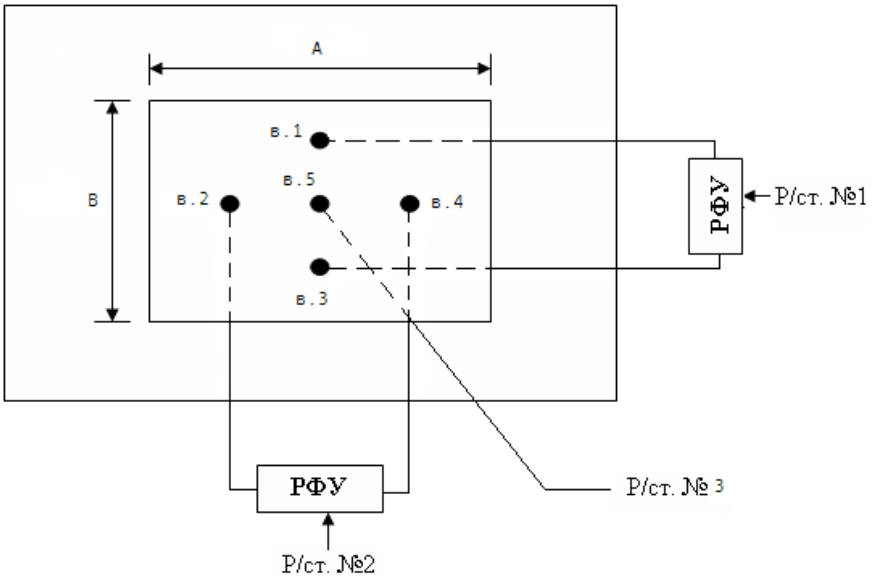


Рис.1 Багатовходова низькопрофільна антена зі струмовим збудженням

На рис.1 показаний один з варіантів багатовходової низькопрофільної антени зі струмовим збудженням, тут введено наступні позначення: В 1 ... В 5 – струмові збудники; РФУ – радіорозподільчий фазовий пристрій; АхВ – розміри верхньої пластини.

У відповідності з методикою [1] розрахунку зовнішніх характеристик низькопрофільних антен із простою конфігурацією верхньої пластини (1), характеристика направленості такого випромінювача визначається виразом:

$$F(\theta,\varphi)=\cos\left[\frac{1}{2}(Kd\sqrt{\varepsilon'}\cos\theta)-\psi_0\right]\frac{\sin(\frac{\pi}{2\sqrt{\varepsilon'}}\sin\theta\sin\varphi)}{\frac{\pi}{2\sqrt{\varepsilon_1}}\sin\theta\sin\varphi}\sqrt{\cos^2\varphi+\sin^2\varphi\cos^2\theta} \quad (1),$$

де ε' – відносна діелектрична проникність матеріалу, який заповнює об'єм між пластинами; ψ_0 – різниця фаз між випромінюючими щілинами.

На рис.2 показано діаграми направленості багатовходової низькопрофільної антени для 2-х режимів роботи: режим роботи іоносферними хвилями (рис 2 а) і режим роботи земними хвилями (рис 2 б).

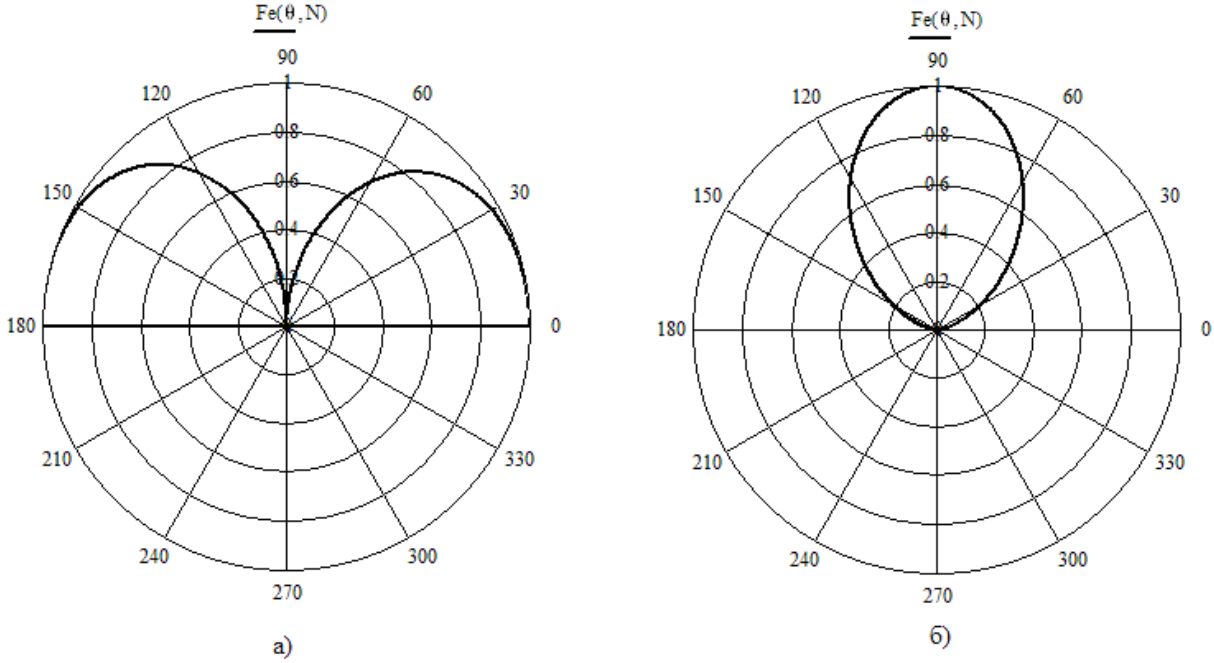


Рис.2 Діаграма направленості багатовходової низькопрофільної антени

Таким чином, отримані результати наочно показують, що багатовхідна низькопрофільна антена дозволяє на даному розкриві формувати різні за типом діаграми спрямованості.

У практичному плані такі антени можуть бути використані для підключення декількох радіостанцій на одну антену при роботі в різних режимах, що особливо актуально для рухомих пунктів управління з метою зменшення загального числа антен, а також для компоновки, наприклад, пеленгаційних компактних антенних пристроїв.

ЛІТЕРАТУРА:

1. Цибизов К.И., Ильинов М.Д. Микрополосковые антенны СВЧ. – К.: Общество „Знания", 1980.

к.т.н. Ільїнов М.Д. (ВІТІ НТУУ „КПІ”)
Юпик М.В.(ВІТІ НТУУ „КПІ”)

ВПЛИВ ХАРАКТЕРИСТИК АНТЕННО-ФІДЕРНИХ ПРИСТРОЇВ НА ЯКІСТЬ РАДІОРЕЛЕЙНОГО ЗВ’ЯЗКУ

Радіорелейний зв’язок – це особливий вид радіозв’язку на ультракоротких хвилях з багаторазовою ретрансляцією сигналу, структурна схема якого зображена на рис.1

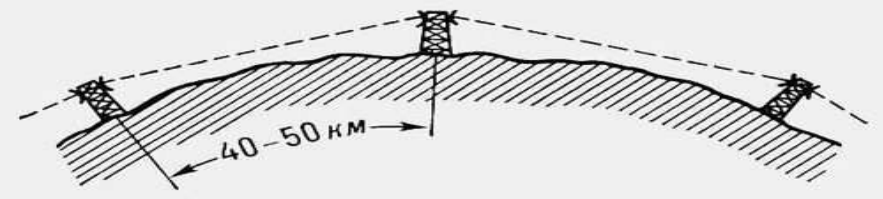


Рис.1 Структурна схема радіорелейного зв’язку

Наземний радіорелейний зв’язок здійснюється звичайно на деци- і сантиметрових хвилях. Антени сусідніх станцій звичайно розташовують у межах прямої видимості, тому що це найнадійніший варіант. Для збільшення радіусу видимості антен їх встановлюють якнайвище – на щоглах (вежах) висотою 70-100 м (радіус видимості – 40-50 км) та на високих будівлях.

Міжнародні рекомендації та вимоги до параметрів антен для РРЛ

У відповідності до вимог європейського стандарту ETSI (European Telecommunications Standards Institute) антени класифікуються за наступними ознаками: (див.рис.2)

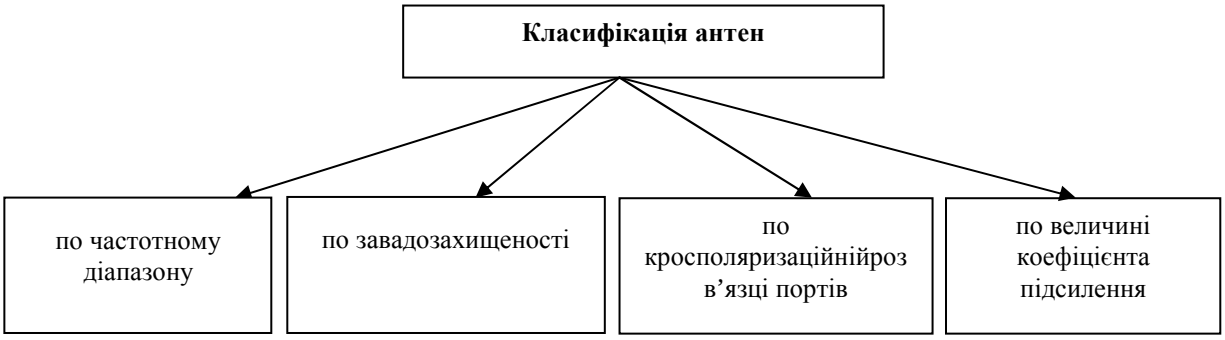


Рис.2 Класифікація антен

Крім класифікації антен , згідно стандартів ETSI, антени мають відповідати наступним вимогам: (див. рис.3)

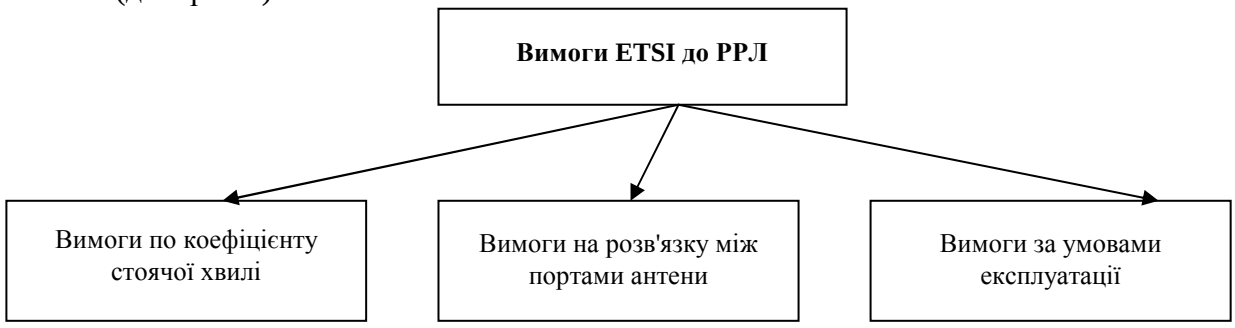


Рис.3 Вимоги європейського стандарту ETSI до РРЛ

Вплив параметрів антен на стійкість сигналу на прольотах РРЛ

Антенні пристрої відіграють важливе значення в енергетичному потенціалі радіолінії. Потужність сигнала на вході приймача ($P_{прм}$), може бути виражена через потужність передатчика ($P_{пер}$), коефіцієнти підсилення передаючої та прийомної антени ($G_{пер}$ та $G_{прм}$), ККД фідерних трактів ($\eta_{\text{пер}}$ та $\eta_{прм}$), а також множник ослаблення (V<<1) середовища поширення.

Основним параметром, що визначає якість зв'язку, є відношення потужності сигнала та потужності шуму на виході канала ($\left(\frac{P_c}{P_ш}\right)_{ВИХ}$).

Слід також врахувати, що в результаті обробки сигнала при прийомі, відношення $\frac{P_c}{P_ш}$ може бути покращено в α раз:

$$\left(\frac{P_c}{P_{\text{ш}}}\right)_{ВИХ} = \alpha\left(\frac{P_{\text{с}}}{P_ш}\right)_{ВИХ} \tag{1.1}$$

$$A = \frac{P_{пер}\cdot \text{G}_1 \cdot G_2 \cdot \eta_{ф1}\cdot \eta_{\text{ф2}}\cdot \alpha}{\kappa \text{T}_{\Sigma\cdot\Delta} f \cdot \left(\frac{P_c}{P_ш}\right)_{\text{ВИХ}}} \geq \frac{1}{V} \tag{1.2}$$

Безрозмірну величину А, що визначається лише параметрами апаратури, називають *енергетичним потенціалом радіолінії.* З виразу (1.2) можна стверджувати про важливе значення та місце антенних пристроїв в радіорелейних лініях щодо забезпечення надійності передачі достовірної інформації.

Одним із важливих параметрів радіорелейних ліній є стійкість сигналу в точці прийому. Під характеристикою стійкості сигналу зазвичай розуміється інтегральний розподіл його рівня, що показує, з якою ймовірністю рівень сигналу може стати меншим заданого рівня.

Введена функція стійкості дозволяє досить просто оцінити вплив ширини діаграми направленості (ДН) антен на стійкість сигналу на прольоті РРЛ. Це явище було виявлено при проведенні спеціальних експериментальних досліджень, які показали, що стійкість сигналу па прольотах РРЛ для малих відсотків часу при використанні антен з великим підсиленням гірше, ніж при використанні антен з меншою спрямованістю.

Отже, виходячи з вищесказаного, можна зробити висновок, що антенно-фідерні пристрої відіграють важливе значення в радіорелейному зв'язку. Обґрунтуванням цього є енергетичний потенціал радіорелейних станцій, який забезпечує якість та надійність передачі сигналу на радіорелейних лініях. Крім того, параметри антенно-фідерних пристроїв визначають розв'язку між портами радіорелейних станцій.

ЛІТЕРАТУРА

1. Липатов А.А. Техника сверхвысоких частот. – К.: КВВИУС, 1977. – 118 с.

2. Фролов О.П. Антенны и фидерные тракты для радиорелейных линий связи. – М.: Радио и связь, 2001. – 414 с.

Каравацький В.О. (в/ч А1906)

ВИКОРИСТАННЯ СКЛАДНИХ ВИДІВ МОДУЛЯЦІЇ ЯК ОДИН З МЕТОДІВ ПІДВИЩЕННЯ НАДІЙНОСТІ ЗВ'ЯЗКУ НА РАДІОЛІНІЯХ ДЕКАМЕТРОВОГО ДІАПАЗОНУ

На сучасному етапі розвитку та розбудови Збройних Сил України командуванням ставляться все більш жорсткі вимоги до якості оснащення, професіональної підготовки особового складу, більш економічного використання наявної техніки та більш повного використання новітньої техніки, якою оснащуються війська.

Як відомо, передавач амплітудно-модульованого сигналу без подавлення несучої частоти велику кількість випромінювання тратить вхолосту, тобто випромінювання здійснюється, але корисного навантаження воно не несе. Досі з цим явищем боролись різними методами, а саме: подавленням несучої, використанням однополосної модуляції тощо. Разом з цим таке явище може принести певну користь. Воно може бути використане як спосіб підвищення надійності радіолінії та достовірності телефонної трансляції з амплітудною модуляцією за рахунок, по-перше, дублювання мовної інформації цифровою з іншим видом модуляції і по-друге, організації додаткового каналу зв'язку без використання іншого передавача, частот та апаратних засобів. Цього можна досягнути:

1) використанням передавачів нового парку з підвищеною стабілізацією несучої частоти та введенням складного виду модуляції типу АМ+ЧТ(амплітудна модуляція та частотна телеграфія), що дозволить організувати низькошвидкісний канал з частотною маніпуляцією несучої не виходячи за рамки девіації частоти несучої передавачів, обумовлених стандартами. Головний недолік такого підходу обумовлюється низькою швидкістю передачі сигналу або інформації (примітка: девіація частоти передавача складає в абсолютному значенні декілька герц, відповідно і швидкість передачі даних буде обмежена та складатиме декілька Бод);

2) використанням передавачів нового парку з підвищеною стабілізацією несучої частоти та введенням складного виду модуляції типу АМ+ЧМ(амплітудно-частотна модуляція), що дозволить організувати низькошвидкісний канал з частотною модуляцією несучої не виходячи за рамки девіації частоти несучої передавачів, обумовлених стандартами. Головний недолік такого підходу обумовлюється низькою швидкістю передачі сигналу або інформації (примітка: девіація частоти передавача складає в абсолютному значенні декілька герц, відповідно і швидкість передачі даних буде обмежена та складатиме декілька Бод);

3) створенням службового каналу АМ передавачів введенням складного виду модуляції типу АМ+ВФМ (ВФМ – відносна фазова маніпуляція), що дозволить організувати низькошвидкісний канал з ВФМ за рахунок модуляції несучої передавача. Недоліками такого підходу є невелика швидкість передачі, можливий вплив на АМ сигнал фазового шуму, що створює цифрова послідовність ВФМ сигналу. Перевага полягає в тому, що випромінювана потужність передавача використовується з користю навіть при подавленні несучої.

Виходячи з вищенаведеного можна зробити висновок, що при використанні новітніх зразків техніки радіозв'язку стає можливим не тільки вирішення питання ефективності використання режиму передачі з амплітудною модуляцією але й додатково виникає можливість створення цифрового каналу радіозв'язку хоча з маленькою швидкістю, але який підвищує надійність передачі повідомлень при односторонній передачі. Також це може дозволити використовувати засоби автоматичної реєстрації, передачу коротких повідомлень, дублювання текстових повідомлень у цифровому вигляді тощо. За деяких умов стає можлива модернізація передавачів старого парку для використання складних сигналів, що підвищить не тільки ефективність використання передавачів, але й надасть додаткові можливості по використанню апаратури старого парку, яка досі стоїть на озброєнні ЗСУ України.

д.т.н. Карлов В.Д.(ХУПС)
Квиткин К.П.(ХУПС)
Бісова О.В.(ХУПС)

ОСОБЛИВОСТІ ОЦІНКИ ПРОСТОРОВОЇ ФУНКЦІЇ РОЗУЗГОДЖЕННЯ ПРИ ОБЛІКУ ФЛУКТУАЦІЇ ФАЗИ СИГНАЛУ, ВІДБИТОГО ВІД ЦІЛІ, ЛОЦИРУЕМОЇ ЗА МЕЖАМИ ДАЛЬНОСТІ ПРЯМОЇ ВИДИМОСТІ НАД МОРЕМ

З аналізу бойових дій протиборчих сторін в локальних конфліктах витікає, що застосовуючи засоби повітряного нападу (ЗПН) при підході до об'єктів знищення все більше використовуються польоти на малій висоті з досить високою швидкістю.

Найбільшу ефективність цей метод має при застосуванні ЗПН в приморських районах.

При цьому особливістю локації ЗПН є мала дальність прямої видимості, а якщо врахувати швидкість польоту сучасних ЗПН, час, відпущений системам ППО на знищення цілі, виявляється занадто малим.

Проте існує можливість збільшення дальності виявлення, пов'язана з особливостями поширення радіохвиль над морем.

Суть використання цього методу полягає в тому, що над морем існує тропосферний радіохвилевід, що дозволяє збільшити дальність локації цілей, проте при цьому випромінювання радіолокаційних сигналів робиться під малим кутом місця, що викликає істотний вплив неоднорідностей тропосфери на сигнал, що поширюється.

В основному цей вплив призводить до істотного збільшення флуктуацій фази сигналу, що у свою чергу приведе до збільшення помилок виміру кутової координати цілі.

У доповіді аналізується вплив випадкових флуктуацій фази на середнє значення квадрата модуля просторової функції розузгодження за параметрами кутової координати і кривизну фазового фронту. Розгляд проводиться у рамках допущень про те, що амплітудний розподіл уздовж антенної системи вважався рівномірним, а дисперсія фазових флуктуацій – постійною.

Передбачається, що фазові флуктуації розподілені за нормальним законом з нульовим середнім значенням, кореляційна функція має довільний вигляд, а її параметри вибрані з умови найкращої апроксимації отриманих в експериментах кореляційних функцій.

У доповіді приведені результати математичного моделювання, побудовані графіки спотворених фазовими флуктуаціями діаграм спрямованості, отриманих для випадку, коли просторова кореляційна функція фазових флуктуацій має експоненціальний або осцилюючий характер.

Розглянута оцінка впливу фазових флуктуацій з довільною кореляційною функцією на спотворення квадрата модуля середньої просторової функції розузгодження по параметру „кривизна фазового фронту", а також проаналізована залежність спотворень від дисперсії фазових флуктуацій і відносного радіусу кореляції фаз флуктуацій.

Коваленко І.Г. (ВІТІ НТУУ „КПІ”)

ЕНЕРГОЗБЕРІГАЮЧИЙ МЕТОД МНОЖИННОГО ДОСТУПУ В СЕНСОРНИХ РАДІОМЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Проведений аналіз існуючих методів множинного доступу в сенсорних радіомережах, виявив переваги та недоліки окремих методів [1 – 3]. Визначено, що існуючі методи не враховують обсяги даних, що збираються окремими вузлами, і неефективні для СР з неоднорідними вузлами [4].

Запропонован новий енергозберігаючий метод множинного доступу сенсорної радіомережі спеціального призначення з надлишковою кількістю неоднорідних вузлів.

*Суттю з*апропонованого методу множинного доступу в сенсорних радіомережах спеціального призначення з надлишковою кількістю неоднорідних вузлів є розподіл канального ресурсу між вузлами в залежності від навантаження та віддалення від шлюзу. Планування часових інтервалів для поточного вузла в розробленому методі базується на зібраної з дочірніх вузлів інформації про робоче навантаження, робочій цикл батьківського вузла та виділений батьківським вузлом робочий цикл для поточного вузла.

В новому методі для організації збору даних СР навколо шлюзу пропонується створонити зону детермінованого доступу до каналу. Для віддалених вузлів, які не входять в зону детермінованого доступу пропонується організувати випадковий доступ до каналу за допомогою одного з відповідних існуючих протоколів.

В методі пропонується ввести два часових періоду відповідно детермінованого та випадкового доступу . Під час організації випадкового доступу до каналу віддалених вузлів, вузли зони детермінованого доступу знаходяться в режимі сну і навпаки.

Граничні вузли зони детермінованого доступу до каналу функціонують в обидва періода: під час періоду випадкового доступу знаходяться в режимі прийому данихі від віддалених вузлів, а під час детермінованггго періоду передають дані в напрямку шлюзу.

Застосування двох типів доступу до каналу в мережі дозволить зменшити споживання енергетичних ресурсів вузлами, що більш навантажені для передачі трафіку, і забезпечить спрощення синхронізації вузлів, гнучке масштабування мережі та гнучкий доступ віддалених вузлів до окремих зон детермінованого доступу.

Приклад розподілення типу доступу вузлів до каналу показаний на рис. 1. Кількість вузлів, що входять до зони детермінованого прийому може визначатись максимальною кількістю ретрансляційних ділянок для відповідної зони або алгоритмами функціонування мережі.

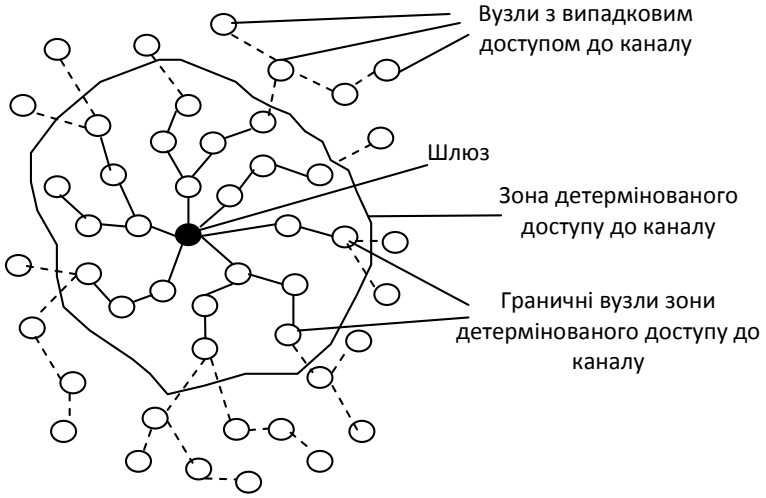


Рис.1

Розроблений метод включає наступні етапи

1. Збір даних про робочі навантаження.

2. Розподіл часових інтервалів.

3. Визначення періоду випадкового доступу

4. Коригування розкладу часових інтервалів.

Оцінку ефективності енергозбереження проведено відносно інстуючих методів МД в СР збору данних за наступними показниками [3]:

1) споживання енергетичного ресурсу;

2) затримка при передачі данних від віддалного вузла з найбільшою кількістю ретрансляцій до шлюзу;

3) глобальна затримка при передачі даних в мережі, яка характеризує максимальну середню частоту дискретизації передачі данних окремимими вузлами;

4) „час життя" мережі [2].

Таким чином, запропонований метод новий енергозберігаючий метод множинного доступу в сенсорних радіомережах спеціального призначення з надлишковою кількістю неоднорідних вузлів забезпечує розподіл канального ресурсу між вузлами мережі в залежності від навантаження та віддалення від шлюзу і має кращі показники ефективності ніж існуючі метододи даного класу, а саме [3]:

– менше споживання енергетичного ресурсу вузлами мережі;

– меншу затримку при передачі данних від віддалного вузла з найбільшою кількістю ретрансляцій до шлюзу;

– меншу глобальну затримку при передачі даних в мережі, яка характеризує максимальну середню частоту дискретизації передачі данних окремимими вузлами;

– до 15% більший час життя мережі збору даних.

При визначення енергоефективності розробленого методу не враховувалась можливість агрегації даних на вузлах СР, застосування якої може зменшити обсяги даних в мережі і ще зменшити використання енергетичних ресурсів вузлів СР і збільшити час життя СР.

ЛІТЕРАТУРА

1. Коваленко І.Г. Енергозберігаючі методи множинного доступу в безпровідних сенсорних мережах: Збірник матеріалів V науково-технічної конференції [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ", 2010. – С. 141 – 142.

2. Коваленко І.Г., Романюк В.А., Діянчук І.М. Аналіз методів енергозбереження в сенсорних радіомережах // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2011. – № 1. – С. 76 – 84.

3. Коваленко І.Г. Енергозберігаючий метод множинного доступу в сенсорних радіомережах спеціального призначення з надлишковою кількістю неоднорідних вузлів// Збірник наукових праць ВІТІ НТУУ „КПІ„. – 2012. – № 1. – С. 37 – 49 .

4. Коваленко І.Г., Романюк В.А., Діянчук І.М. Метод енергозбереження сенсорної радіомережі спеціального призначення з надлишковою кількістю неоднорідних вузлів при забезпеченні заданих показників перекриття зон моніторингу та зв'язності вузлів // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2011. – № 3. – С. 52 – 64.

Коваленко С. В. (ВІТІ НТУУ „КПІ”)
Шевченко В. С. (ВІТІ НТУУ „КПІ”)

ПРОЕКТУВАННЯ ТРАНКІНГОВИХ РАДІОМЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Радіозв’язок в існуючій системі зв’язку спеціального призначення організовується з використанням індивідуальних радіозасобів, закріплених за певними посадовими особами, яким призначаються визначені позивні та частоти у кожній радіомережі (напрямку), в якій вони є кореспондентами. Сеанси зв’язку здійснюються у радіонапрямках за принципом прямих зв’язків – „кожен з кожним”, або у радіомережах. На озброєнні знаходяться переважно радіостанції 2 – 4-го поколінь, суттєвими недолікоми яких є незадовільна завадозахищеність, що проявляється як у нездатності протидіяти навмисним завадам, так і у створенні високого рівня внутрішньосистемних завад, робота на фіксованих робочих частотах, які легко викрити противнику.

З урахуванням сучасних поглядів на розвиток систем радіозв’язку спеціального призначення перспективним напрямком є побудова радіомереж з використанням принципів та засобів транкінгового зв’язку.

Сучасні системи транкінгового зв’язку призначенні для побудови локальних і багатозонових мереж, що дають різні види послуг при високій якості зв’язку. Зокрема, підтримується мовний зв’язку і передача даних між абонентами і групами абонентів, доступ до відомчих телефонних мереж, мереж загального користування і мереж передачі даних.

Проектування транкінгових мереж зв’язку передбачає виконання наступних основних розрахунків.

1. Розрахунок потрібного числа радіоканалів. Виконується розрахунок кількості абонентів, що будуть користуватися даною мережею, після чого робиться розрахунок кількості каналів в мережі.

2. Розрахунок інтенсивності навантаження. Інтенсивність поступаючого навантаження розраховується виходячи із кількості абонентів базової станції в районі навантаження в час найбільшого навантаження на одного абонента.

3. Розрахунок числа каналів необхідних для підключення мережі. Розрахунок кількості каналів проводиться за формулою Ерланга, або за таблицями Ерланга. Число каналів мікростільникової мережі від базових станцій розраховується при вірогідності втрат $p = 0{,}05$. Тому вірогідність втрат виклику в мережах стільникового зв’язку не повинна перевищувати 5%.

4. Економічні розрахунки мережі зв’язку, де враховується склад та тип обладнання (стаціонарне базове обладнання, диспетчерська стаціонарна радіостанція, мобільне обладнання), яке буде застосовуватися.

5. Розрахунок мережі безпроводового доступу. Розраховується зона обслуговування базової станції по моделі Окамури-Хата. Виходячи з експериментальних даних, отриманих Окамурою, Хата запропонував аналітичну модель емпіричних втрат розповсюдження сигналів, яка дозволяє розрахувати загасання радіосигналу в міських і сільських умовах.

Серед транкінгових стандартів найбільш повно вимогам відомчих систем спеціального призначення відповідає стандарт TETRA V+D, який може бути використаний для управління повсякденною діяльністю військ (сил), та з деякими змінами може бути покладений в основу власного стандарту транкінгового зв’язку спеціального призначення.

к.т.н. Ковбасюк С. В. (ЖВІНАУ)
Каневський Л. Б. (ЖВІНАУ)

АНАЛІЗ ЗАЛЕЖНОСТІ ТОЧНОСТІ ВИЗНАЧЕННЯ ПАРАМЕТРІВ РУХУ ЦІЛІ ВІД РАКУРСУ СПОСТЕРЕЖЕННЯ У ДВОПОЗИЦІЙНІЙ СИСТЕМІ

Україна, як космічна держава, активно приймає участь у різних міжнародних космічних програмах, тому перед балістиками стоять актуальні завдання: об'єктивного контролю процесу виведення КА; надання послуг із забезпечення їх управління. Реалізація цих завдань потребує мати оперативну і достовірну інформацію про навколоземну ситуацію, що вимагає від системи контролю й аналізу космічної обстановки своєчасного та ефективного ведення каталогу космічних об'єктів (КО).

Розвиток теоретичних основ багатопозиційної радіолокації відкриває перспективи значного підвищення ефективності застосування інформаційно-вимірювальних засобів (ІВЗ) різного призначення. Саме тому, одним з шляхів підвищення точності визначення параметрів руху КО є використання багатопозиційних систем, до складу яких входять автономно працюючі ІВЗ. Точність оцінювання в такій системі залежить від кількості її елементів, тактико-технічних характеристик кожного ІВЗ, ракурсу на ціль, бази розміщення між ІВЗ та від часового інтервалу спостереження цілі.

Якщо залежність впливу кількості ІВЗ, величини бази на результуючу точність достатньо досліджені й свідчать про ефективність застосування великобазових комплексів, то вплив ракурсу на ціль не достатньо досліджено.

Таким чином, у доповіді представлені результати роботи, що були спрямовані на:

– удосконалення існуючих методів обробки траєкторної інформації, зокрема в оптичних засобах спостереження, оскільки вони єдині на сьогодні ІВЗ, що використовуються з метою контролю космічного простору;

– розробку методики визначення з підвищеною точністю параметрів руху КО у великобазовому двопозиційному оптичному комплексі, де додатково досліджено залежність показників точності від ракурсу на ціль.

Аналіз запропонованих підходів свідчить про те, що в умовах апріорної невизначеності вектора початкових значень руху КО необхідно використовувати метод балансу диференціальних спектрів (побудований на основі математичного апарату академіка Пухова Г. Є.). Для розв'язку крайової задачі на одному мірному витку слід застосувати метод Гаусса-Ньютона з використанням динамічної моделі руху. Підвищення точності шляхом побудови багатопозиційного оптичного комплексу слід проводити з використанням великих баз, між ІВЗ. Структурну оптимізацію багатопозиційного комплексу слід проводити методом багатокритеріальної оптимізації за нелінійною схемою компромісів професора Ворорніна А. М. Оптимальне значення шуканих параметрів можна отримати на основі адаптивного алгоритму, що залежить від ракурсу на КО, який спостерігається в спільній зоні великобазового багатопозиційного комплексу.

Переваги розробок з'ясовувались шляхом циклу випробувань з використанням моделювання в інтегрованому середовищі символьної (аналітичної) математики MAPLE відповідно до визначеної моделі похибок даних. Було з'ясовано, що запропоновані підходи дають змогу розв'язати задачу оперативного визначення параметрів орбіти КО (у межах одного витка) та підвищити точність шуканих результатів у 10 – 12 разів по вектору положення і у 20 – 24 рази по швидкості зміни цього вектора, порівняно з автономним ОЗС.

Практична цінність таких досліджень полягає у тому, що розроблена методика може бути використана для створення гнучкої структури ІВЗ для супроводження КО за цілевказівками, а також для розрахунку потенціально можливих точністних характеристик великобазового багатопозиційного комплексу при вирішенні балістико-навігаційних задач.

к.т.н. Козубцов І.М. (НЦЗІ ВІТІ НТУУ „КПІ”)
Герасименко О.О. (НЦЗІ ВІТІ НТУУ „КПІ”)
Ткач В.О. (НЦЗІ ВІТІ НТУУ „КПІ”)

ЗАРУБІЖНИЙ ДОСВІД ІНТЕГРАЦІЇ ВІЙСЬКОВОЇ ТА ЦИВІЛЬНОЇ ОСВІТИ

Постановка проблеми та зв'язок її з важливими науковими завданнями. Метою сучасного етапу розвитку військової освіти є підготовка військових фахівців з високим рівнем професіоналізму із загальною та військово-професійною культурою, створення умов для безперервного підвищення рівня знань, практичних навичок військових фахівців, їх творчого розвитку та самореалізації.

Для України, перш ніж проводити необґрунтовані заходи в ході реформи, важливо ознайомитися з зарубіжним досвідом інтеграції військової та цивільної освіти, досвіду підготовки військових фахівців деяких країн важливий, має позитивні якості.

Аналіз останніх досліджень і публікацій за проблемою. На основі аналізу літературних джерел проведено окремі дослідження проблем принципів перспективних напрямів і шляхів інтеграції військової освіти з цивільною освітою у деяких країнах світу з урахуванням посилення військово-професійної спрямованості навчання. До новаторів сучасності, що здійснювали дослідження інтеграції військової з цивільною освітою, слід віднести наукові праці Нещадима М.І. [1], Ільницької У.В. [2], Полякова С.Ю. [3], Моісєєнко О.М., Гавриленко А.С. [4]. Трансформації системи військової освіти, як підґрунтя підготовки нової генерації військових фахівців, були присвячені роботи Серветник Р.М. [5], Радецького В.Г., Телелима В.М., Даника Ю.Г. [6] та ін. Проблемні питання євроінтеграції вищої освіти на сучасному етапі реформування Збройних Сил України висвітлювали Мночкін А.І., Тхоржевський І.В. та Костенко В.А. [7]. Однак всі дослідження носять кластерний характер.

Формулювання цілей статті. Метою статі є висвітлення основних результатів НДР „Перспктива-ВО” щодо аналізу досвіду інтеграції військової з цивільною освітою та відпрацювань теоретико-практичних рекомендацій дисертаційного дослідження.

Результат дослідження. Заслуговує на увагу реформування військової освіти, зарубіжний досвід підготовки військових фахівців та досвід інтеграції військової та цивільної освіти.

Ізраїльська система підготовки військових кадрів є ефективною системою, що охоплює все населення, починаючи зі школи. Офіцерські курси організовують на навчальних базах та військових полігонах. Тривалість навчання складає від 6 місяців для командирів піхотних взводів до 20 місяців для офіцерів флоту. Тільки у Військово-повітряній Академії, де готують пілотів, термін навчання складає 3 роки і по закінченню випускникам разом з офіцерським званням присвоюють перший академічний ступінь. Вся система навчання нерозривно пов'язана з вирішенням реальних бойових завдань. Значну частину часу курсанти проводять в полі і на навчаннях, де негайно закріплюються отримані теоретичні знання. Нахил робиться на оволодіння майбутніми офіцерами практичних навиків командування підрозділами.Така розгалужена система військової освіти в Ізраїлі охоплює практично все населення країни. За багато років воєн і збройних конфліктів вона довела свою ефективність в підготовці командних кадрів і стала прикладом для армій багатьох держав. Система військової освіти Ізраїлю знаходиться в постійному розвитку і реагує на вимоги сучасної війни і державного будівництва. Отже, система військової та цивільної освіти розділена, однак, домінуючим є військове спрямування розвитку думки, націленої на підвищення обороноздатності держави. За таких умов інтеграція і зміна на домінування набік цивільної компоненти для Ізраїлю є недоцільним.

Система інтегрованої підготовки офіцерських кадрів Білорусі. Вперше в новій редакції Концепції національної безпеки Білорусі забезпеченість військовими кадрами названа одним з основних індикаторів національної безпеки [8, с. 25]. У Білорусії підготовка військових

кадрів в країні здійснюється в закладах освіти «Військова академія Республіки Білорусь», на семи військових факультетах і чотирьох військових кафедрах при цивільних ВНЗ. У Військовій академії навчаються офіцери оперативно-тактичної ланки за 18 спеціальностями і спеціалізаціями, офіцери тактичної ланки – за 90 спеціальностями і спеціалізаціями, а офіцери запасу – за 48 спеціальностями. З 2003 р. проводиться навчання студентів і по програмах підготовки молодших військових фахівців [9]. Зі створенням факультету Генерального штабу ЗС, в 2006 р. можна вважати завершення створення білоруської національної військової школи [10, с. 21].

Крім того, підготовка білоруських офіцерів з вищою військовою освітою здійснюється у військових академіях Росії. Отже, в Республіці Білорусь спостерігається планомірний процес інтеграції військової освіти в цивільну освіту.

Підготовка офіцерських кадрів у Франції здійснюється з числа студентів, які опанували складні технічні, військово-медичні та адміністративно-господарські спеціальності. Цивільні ВНЗ практично всіх країн НАТО зацікавлені підвищенням кваліфікації та перепідготовкою кадрового офіцерського складу та ряду категорій офіцерів запасу.

Із зазначеного видно, що набутий офіцером рівень освіти дає йому можливість обіймати посади на різних рівнях управління в межах визначеної рівнем освіти ланки відповідно до військового звання. Водночас перед призначенням офіцера на вищу посаду виникає необхідність надання йому додаткових знань, умінь і навичок, пов’язаних з особливостями функцій за вищою посадою. Це завдання реалізується шляхом самостійної підготовки, курсової підготовки, стажування на посадах вищого рівня. Тому завданням органів кадрової політики, кадрового менеджменту є глибоке вивчення та постійне врахування потреб збройних сил у тих чи інших фахівцях, стеження за проходженням служби кожним окремим спеціалістом, просування його на посаді та обов’язкове підвищення його професіоналізму у певних сферах діяльності.

Підготовка офіцерських кадрів ФРН. Підготовка офіцерського складу Бундесверу здійснюється з урахуванням комплектування збройних сил кадровими офіцерами. Вона включає певні етапи навчання у військах, школах родів військ, офіцерських школах, військових університетах і академії служби генерального штабу Бундесверу [11].

Важливо підкреслити, що після 39 місяців військової служби молодші офіцери прямують на навчання в один з двох університетів бундесверу (Гамбург і Мюнхен) в цілях здобування вищої цивільної освіти протягом трьох-чотирьох років. Розглядаючи систему формування офіцерського складу бундесверу в цілому, відзначимо, перш за все, чітке розділення з урахуванням системи комплектування бундесверу кадровими офіцерами і офіцерами за контрактом наявність різних категорій офіцерів і порядку їх навчання і підготовки. Після закінчення університету – навчання продовжується на офіцерських курсах в школах родів військ для поглиблення військових знань (1 місяць), після чого випускникові присвоюється військове звання „капітан”. Після закінчення терміну першого контракту (12 років) слідує другий контракт, що дає право на подальшу освіту офіцера і його просування по службі. Офіцери надалі прямують на навчання в академію Бундесверу.

Таким чином, освіта офіцерів Бундесверу носить перманентний, цілеспрямований характер. Система передбачає постійне підвищення кваліфікації, перепідготовка в контексті сучасної освітньої концепції long-life-learning (освіта крізь все життя).

Система вищої військової освіти США [12] можна умовно поділити на військову компоненту освіти, що включає:

військові училища (академії) видів збройних сил;

військово-навчальні заклади, в яких офіцери здобувають вищу військову освіту;

спеціалізовані військово-навчальні заклади;

курси перепідготовки і удосконалення;

та цивільну компоненту, що включає:

інститут заочного навчання військовослужбовців;

курси військової підготовки офіцерів резерву при цивільних вузах (Reserve).

Розглянемо інтегровану частину освіти. В інституті заочного навчання відбувається підвищення рівня загальноосвітньої, спеціальної і професійної підготовки військовослужбовців, а також отримання середньої професійно-технічної і вищої освіти. В інституті функціонують заочні відділення при коледжах і університетах, а також на основі договорів з цивільними навчальними закладами США. Студенти університетів і коледжів можуть за бажанням закінчити курси позавійськової підготовки офіцерів резерву (ROTC) при своїх навчальних закладах. Термін навчання за програмою ROTC складає 2 або 4 роки. Близько 50% випускників, що закінчили чотирилітній цикл навчання, стають офіцерами сухопутних військ, ВПС і ВМС. Командування позавійськової підготовки співробітничає більш ніж з 600 цивільними вищими навчальними закладами США, що складає майже 20% від всіх закладів, що функціонують в країні. Офіцерів резерву для сухопутних військ готують при 300 університетах і коледжах, ВПС – 200, ВМС – 65, морської піхоти – 60. Студенти, курси ROTC, що успішно закінчили, і що виявили бажання служити в регулярних військах, отримують тільки загальну військову підготовку. Конкретної військової спеціальності вони набувають протягом декількох місяців на відповідних курсах в школах родів військ (сил) і служб, а також у військових навчальних центрах і лише після цього направляються в частин відповідного виду Збройних сил [13, с. 63]. Головними особливостями американської системи підготовки офіцерів є: безперервність навчання та участь цивільних навчальних закладів в комплектуванні первинних офіцерських посад; наявність мережі шкіл, навчальних центрів, курсів підготовки, перепідготовки і підвищення кваліфікації військових кадрів, число і рівень яких змінюється залежно від обстановки і потреби ЗС в тих або інших спеціальностях; короткостроковість військової підготовки командних кадрів ЗС США у військових коледжах, що є за своєю суттю вищими академічними курсами.

Досвід інтеграції військової освіти з цивільною освітою в Польщі. Існуючі форми інженерної освіти у ВНЗ на основі військових факультетів при цивільних ВНЗ не задовольняють потреби армії, що постійно ростуть, з погляду як кількості, так і професійно-військової підготовки.

Збройним силам потрібні фахівці, яких в цивільних ВНЗ не готують. Таким чином, в керівництві Міністерства оборони було ухвалило рішення про створення власного політехнічного навчального закладу – Військового Технічного Університету „Wojskowa Akademia Techniczna im. J. Dąbrowskiego w Warszawie” [14]. Спочатку університет складався з п’яти факультетів. Згодом додано е два і заочну форму навчання магістрів.

Зараз Військовий технічний університет є найбільшим військовим політехнічним університетом в Польщі, де здійснюється навчання військових і цивільних студентів. Навчальний заклад безпосередньо підпорядковано Міністерству оборони Польщі, а не Міністерству освіти та науки. Керівництво закладом здійснює ректор, що перебуває на дійсній військовій службі. А от його заступники – проректори за штатом є цивільними.

Реформування системи військової освіти в Росії. У зв’язку з системними змінами в ЗС, по приведенню чисельності офіцерського складу у відповідність до потреб військової організації держави, Міністерство оборони підготувала 21 липня 2008 р., президент Російської Федерації ухвалив пропозицію по формуванню перспективної мережі ВВНЗ, до 2013 року: три військові навчально-наукові центри (ВННЦ) Сухопутних військ, Військово-повітряних сил та Військово-морських сил [15, с. 7]; шість військових академій; один військовий університет. Першим кроком у формуванні нової мережі вузів стало розпорядження Уряду РФ від 24 грудня 2008 р. №1951-р., відповідно до якого з 2009 року в системі військової освіти почали створюватися ВННЦ. Вони стали новою формою інтеграції військової освіти і науки. Центри почали створювати на базі військових академій, що об’єднують освітні установи, які реалізовують освітні програми різних рівнів, а також інші установи і організації, зокрема наукові.

Система підготовки офіцерів передбачає одноразове здобуття офіцерами

фундаментальної вищої освіти. Перед призначенням на кожну нову посаду кожен офіцер проходить підготовку, термін якої залежать від майбутньої посади. Такий підхід формує систему безперервної військової освіти і підготовки офіцерів впродовж всієї служби. Один раз, здобувши вищу освіту, він має всі шанси вирости від лейтенанта до генерала [16]. Навчання в профільних військових академіях і у Військовій академії Генерального штабу (ВАГШ) планується замінити на 10-місячні підготовчі курси. Офіцер кожні три роки може підвищувати свій освітній рівень на різних курсах в системі додаткової підготовки. Наприклад, командир батальйону – у видовій академії, командир бригади – у ВАГШ. Змінився вміст навчального процесу що передбачає обов'язкові курси лідерства, ґрунтовної лінгвістичної підготовки та інтенсивні заняття фізпідготовкою і спортом [16]. Із-за надлишку офіцерських кадрів в 2010-2011 рр. було припинено набір курсантів у ВВНЗ. Одним з напрямів вдосконалення системи підготовки і комплектування військ (сил) офіцерськими кадрами в умовах оптимізації штатної чисельності військових посад, що підлягають заміщенню офіцерами, стало створення і розвиток нової форми підготовки офіцерських кадрів – навчальних військових центрів (НВЦ). З 1 вересня 2008 р. розпочато підготовку офіцерів в НВЦ для Збройних сил при 37 провідних цивільних освітніх установах, розташованих по всій території Росії [17, с. 10]. Підготовка російського офіцера згідно прийнятої в армії Болонської системи із залишенням підготовки військових фахівців з освітньо-кваліфікаційним рівнем „спеціаліст" [18]. Така система дозволяє випускникам військових вузів зробити подвійну кар'єру.

Висновки і перспективи подальших досліджень у даному напрямку. Проаналізувавши досвід підготовки офіцерів в зарубіжних країнах можна зробити деякі висновки, щодо інтегрованої системи підготовки офіцерських кадрів:

інтеграція військової освіти в систему цивільної в Україні є унікальною, оскільки в багатьох країнах військова освіта є замкнутою системою, а у нас вона є невід'ємною складовою національної системи освіти, та зберегла не мало позитивних елементів з тієї, що залишилася від радянської військової школи;

реформа системи військової освіти України здійснюється з урахуванням світового досвіду, інноваційних технологій і спрямована на забезпечення підготовки офіцерських кадрів на компетентнісних засадах для сучасних Збройних Сил;

перевага над деякою іноземною військовою системою освіти полягає, і в тому, що випускники військових ВНЗ здобувають військову спеціальність (спеціалізацію), згідно ОКХ, ОПП, кваліфікацію офіцера військового управління тактичного рівня отримують диплом державного зразка, який надає кваліфікацію інженера з галузі знань. Це забезпечить після завершення військової кар'єри знайти своє місце у цивільному житті;

на сьогодні Військовий інститут телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут" є структурним підрозділом НТУУ „КПІ" де позитивно вирішується інтеграція військової освіти з цивільною, зазначимо, що ця складна справа є актуальною і у інших країнах Європи та світу;

інтеграція військової освіти з цивільною освітою є найбільш ефективною для країн, які мають невеликі за чисельністю збройні сили, і які не мають потреби у великій кількості військових фахівців.

Реалізація військової освіти в кожній країні є абсолютно різною. Європа відходить від схематичності, вона не нав'язує свою структуру. Немає ніяких уніфікованих вимог в Європі щодо дипломів та їх сертифікації. Є тільки такі вимог, які дозволяють приєднуватися до Болонського процесу, увійти до єдиного освітянського простору. Це:

наявність першого етапу вищої освіти – бакалаври;

наявність другого етапу вищої освіти – магістри;

наявність післядипломного рівня, який включається в систему освіти.

Процес реформи системи військової освіти України, виходячи із положень Концепції реформування Збройних Сил України на період до 2017 року якою передбачено зокрема

скорочення кількості й номенклатури, підготовку зменшеної чисельності офіцерських кадрів високої кваліфікації в умовах обмеженого фінансування, повинен бути всебічно і детально обґрунтованим і носити безперервний характер.

ЛІТЕРАТУРА

1. Автореф. дис... д-ра пед. наук: 13.00.04 / М.І. Нещадим; Ін-т педагогіки і психології проф. освіти АПН України. – К., 2004. – 56 с. – укр.

2. Ільницька У.В. Паблік рилейшнз Збройних сил як фактор демократизації та оптимізації цивільно-військових відносин : Дис... канд. політ. наук: 23.00.02 / Національний ун-т „Львівська політехніка". – Л., 2006. – 213 арк. – Бібліогр.: арк. 201 – 213.

3. Поляков С.Ю. Організаційно-правові засади військової освіти в Україні (адміністративно-правовий аспект): дис... канд. юрид. наук: 12.00.07 / Національна юридична академія України ім. Ярослава Мудрого. – Х., 2006.

4. Моісєєнко О.М., Гавриленко А.С. Інтеграція військової та цивільної освіти – співпраця на користь суспільства [Электронный ресурс]. – Режим доступу URL: http://www.confcontact.com/20110225/pe1_moiseenko.php.

5. Серветник Р.М. Трансформація системи військової освіти – підґрунтя підготовки нової генерації військових фахівців [Электронный ресурс]. Вісник Національної академії оборони України 4 (12) / 2009. – Режим доступу URL: http://www.nbuv.gov.ua/portal/soc_gum/Vnaou/2009_4/Serwetnik.pdf.

6. Радецький В.Г., Телелим В.М., Даник Ю.Г. Питання трансформації оборонних структур України та удосконалення системи військової освіти // Наука і оборона. – 2009. – №1. – С.15 – 18.

7. Тхоржевський І. В., Кортенко В. А. Проблемні питання євроінтеграції вищої освіти на сучасному етапі реформування Збройних Сил України // Військова освіта. – К., 2004. – №2 (14) – С. 82 – 94.

8. Об утверждении Концепции национальной безопасности Республики Беларусь: Указ Президента Респ. Беларусь от 9 нояб. 2010 г. №575 // Нац. реестр правовых актов Респ. Беларусь. 2010. №276. 1/12080.

9. Савик С.А. Подготовка офицерских кадров в Республике Беларусь в контексте реформирования системы военного образования в ведущих странах НАТО и СНГ [Электронный ресурс]. ФГБУ „Федеральный центр образовательного законодательств" Журнал „Право и образование" – Режим доступу URL: http://www.lexed.ru/pravo/journ/0612/sav.doc.

10. Жадобин Ю.В. Долг каждого гражданина // Беларуская Думка. 2011. №3. – С.16 – 24.

11. Андреев В.И., Шеховцов Н.П. К проблеме аксиологических оснований подготовки офицеров в армиях развитых стран мира (на примере ВС США, ФРГ, Великобритании, Франции) // Вестн. Акад. воен. наук. 2006. – №3. – С.104 – 109.

12. Матвеенко А.А. Система высшего военного образования в США // ART of WAR. 2010.01.30. [Электронный ресурс]. – Режим доступу URL: http://artofwar.ru/k/kamenew_anatolij_iwanowich/sshasistemawoennogoobrazowanijanachalo21weka.shtml.

13. Бакович М.Н. Организационно-правовое регулирование подготовки офицеров запаса для вооруженных сил США и Великобритании // Воен. мысль. 2008. –№10. – С.59 – 66.

14. Wojskowa Akademia Techniczna / Military University of Technology [Электронный ресурс]. – Режим доступу URL: http://www.wat.edu.pl.

15. Гафутулин Н. Военная реформа XXI века // Красная звезда. 2009. 11 февр. С. 7.

16. Приезжева Е.Г. Военная школа на этапе перемен // РИА Новости [Электронный ресурс]. 31 окт. 2011. – Режим доступу URL: http://ria.ru/interview/20111031/473707349.html.

17. Панков Н.А. Готовить офицерские кадры – по-новому // Российское воен. обозрение. 2008. – №9. – С.8 – 13.

18. Армия по уши в болонской системе. 12 сентября 2011 [Электронный ресурс]. – Режим доступу URL: http://topwar.ru/6731-armiya-po-ushi-v-bolonskoy-sisteme.html.

к.т.н. Кокотов О.В. (ВІТІ НТУУ „КПІ”)
Артюх С.Г. (ВІТІ НТУУ „КПІ”)

ПРОЕКТ КЛАСИФІКАТОРУ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ

Сучасний етап розвитку ринку радіоелектронних засобів (РЕЗ) в Україні характеризується різким зростанням асортименту радіообладнання, яке виробляється, ввозиться та реалізується на території країни та збільшенням його функціональних можливостей. Це суттєво ускладнює процедури, які пов’язані з регулюванням доступу РЕЗ на територію України. Вирішення цієї проблеми потребує уніфікації назв радіообладнання і створення класифікатора РЕЗ, що дасть можливість автоматизувати процедури державного регулювання користуванням радіочастотним ресурсом [1].

До класифікації РЕЗ з метою регулювання доступу на територію України, висуваються наступні вимоги:

– принципи класифікації повинні бути зрозумілі суб’єктам ринку радіотелекомунікаційного обладнання та відображати основні властивості обладнання;

– з урахуванням євроінтеграційних прагнень України, при класифікації необхідно забезпечити виконання вимог Директив Євросоюзу;

– критерії для поділу РЕЗ на групи повинні бути технічно обґрунтовані.

З врахуванням вищезазначених вимог був створений проект Класифікатору радіообладнання (КРО). Під час розробки КРО використовувався підхід заснований на класифікації за суттєвими ознаками (типологія). В якості ознак застосовані наступні: вид радіообладнання, тип системи, категорія радіообладнання, тип радіообладнання.

Структура КРО побудована за комбінованою ієрархічно-офсетною схемою: чотири рівні ієрархічної класифікації та фасетні групи (рис. 1). За допомогою фасетних груп розглядаються додатково реалізовані технології та їх комбінації.

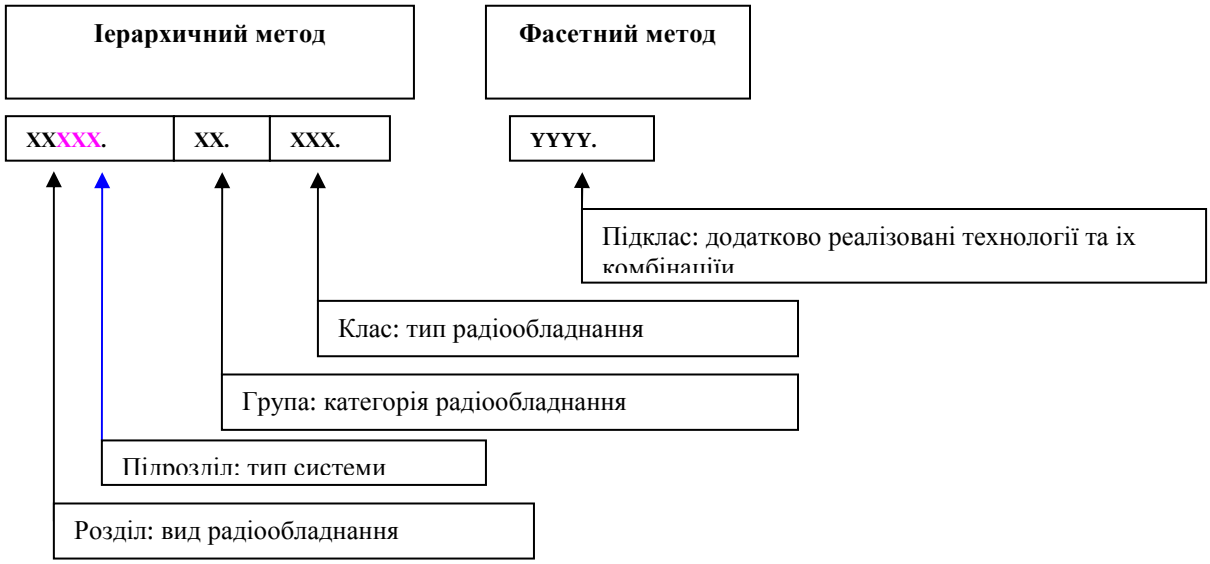


Рис. 1. Структура класифікатору радіообладнання

Застосування КРО дозволяє уніфікувати назви РЕЗ, уникнути неоднозначностей при ведені Реєстру РЕЗ і ВП, що можуть застосовуватися на території України в смугах радіочастот загального користування та створює умови для автоматизації процедур реєстрації та обліку РЕЗ.

ЛІТЕРАТУРА

1. Хаіров Є.В., Тичинський А.В., Несторенко О.В., Бондаренко А.В. Класифікація радіообладнання як складова державного регулювання використання радіочастотного ресурсу України / Зв’язок. – 2012. – №1 – с.7 – 13.

к.т.н. Кокотов О.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Самойлов І.В. (ВІТІ НТУУ „КПІ”)
Коротков В.С. (ВІТІ НТУУ „КПІ”)

КОНЦЕПЦІЯ БОЙДА ЯК ТЕОРЕТИЧНА ОСНОВА ІНФОРМАЦІЙНИХ ВІЙН

Відповідно до ідей Дж. Бойда і його послідовників будь-яка діяльність у військовій сфері з певним ступенем наближення може бути представлена у вигляді кібернетичної моделі OODA (Observe – спостерігай, Orient – орієнтуйся, Decide – вирішуй, Act – дій) [1]. Зазначена модель припускає багаторазове повторення петлі дій, складеної із чотирьох послідовних взаємодіючих процесів: спостереження, орієнтація, рішення, дія. Фактично має місце розвиток ситуації за спіраллю і на кожному етапі цієї спіралі здійснюється взаємодія із зовнішнім середовищем і вплив на противника.

Цю модель відносять до розряду кібернетичних, тому що в ній реалізується принцип „зворотного зв’язку”, відповідно до якого частина виходу з системи знову подається на її вхід, щоб уточнити, а якщо буде потрібно, і скорегувати розвиток системи на наступних етапах. У ряді офіційних доктринальних документів МО США, зокрема в спільній публікації Joint Publication 3-13.1, петля OODA розглядається в якості єдиної типової моделі циклу прийняття рішень для систем командування і керування (C2 systems), як своїх військ, так і військ противника.

Відмітна риса циклу OODA від інших циклічних моделей полягає в тому, що в будь-якій ситуації завжди передбачається наявність противника, з яким ведеться збройна боротьба.

Противник також діє та приймає рішення в рамках своєї аналогічної петлі. Із чотирьох етапів OODA-циклу три безпосередньо пов’язані з обробкою інформації і з комп’ютерними технологіями. Четвертий етап (Action – дія) носить у цілому „кінематичний” характер і пов’язаний з переміщенням у просторі, захистом і поразкою противника на основі вогневих засобів.

Щоб зберегти часові рамки OODA-циклу для дій своїх сил і забезпечити більш високий, ніж у противника, темп бою, необхідно прискорити всі чотири етапи циклу, які реалізуються військами (силами). Протягом двадцятого століття всі зусилля військових, учених і інженерів були спрямовані на вдосконалювання озброєння і технологій у частині кінематичної частини петлі OODA. Результатом цих зусиль було збільшення мобільності, точності і вогневої здатності озброєння.

Однак на сучасному етапі наступила технологічна межа кінематичної частини OODA-циклу – могутніші види зброї наносять неприйнятний супутній збиток, а більш швидкісні і більше захищені платформи озброєння та засоби доставки вражаючого фактора до цілі припускають непомірні на сучасному етапі матеріальні витрати. У зв’язку з цим з’явилася необхідність в удосконалюванні інших етапів OODA-циклу.

Перші три кроки OODA-циклу зв’язані безпосередньо із процесами збору інформації, її розподілу, осмислення, аналізу і прийняття рішень на основі отриманої інформації. Чим швидше здійснюються збір, розподіл, аналіз, сприйняття інформації, тим швидше приймається рішення.

Саме швидкість і правильність прийняття рішень стають найбільш важливими в реальних бойових діях на сучасному етапі. Це послужило поштовхом до розробки концепції мережно-центричної військової діяльності (network-centric warfare) або мережно-центричної війни.

У найбільш загальному випадку створення мережних структур спрямовано на скорочення часу циклу бою й підвищення темпу бойових (військових) дій на всіх рівнях військової організації. Таким чином, організація мережі є механізмом прискорення етапів

спостереження й орієнтації, а також підвищення ефективності – для етапу прийняття рішень.

Завдяки створенню єдиного інформаційно-комунікаційного простору досягається інформаційна перевага (інформаційне домінування) на полі бою, що дозволяє в багато разів ефективніше й оперативніше реалізувати бойовий потенціал угруповань військ (сил) у ході воєнних дій. З'являється можливість випереджати противника на всіх етапах підготовки й ведення бойових дій. Противна сторона втрачає можливості почати хоч які-небудь відповідні кроки й, в остаточному підсумку впадає в стан „повного шоку" [2, 3].

Інформаційна перевага визначається, як здатність збирати, обробляти й розподіляти безперервний потік інформації про ситуацію, перешкоджаючи супротивникові робити те ж саме.

Відповідно до концепції Бойда воно відповідає здатності призначити й підтримувати такий темп проведення операції, що перевершує будь-який можливий темп дій противника, дозволяючи домінувати протягом усього її проведення, залишаючись непередбаченим, і діяти, випереджаючи противника в його відповідних акціях. Інформаційна перевага завойовується в процесі інформаційного протиборства (ІП).

ІП складається з дій, що вживаються з метою досягнення інформаційної переваги в забезпеченні національної військової стратегії шляхом впливу на інформацію та інформаційні системи противника з одночасним зміцненням і захистом власної інформації, а також власних інформаційних систем і інфраструктури.

З точки зору теорії Бойда ІП дозволяє вирішити два завдання:

1. Знизити швидкість реалізації циклу OODA і зменшити якість прийнятих рішень противника за рахунок проведення наступальних інформаційних операцій;

2. Не дати противнику знизити швидкість реалізації власного циклу OODA і зменшити якість прийняття власних рішень за рахунок проведення оборонних інформаційних операцій.

Вирішення першого завдання є бажаним під час ведення ІП, в той час як виконання другого завдання є обов'язковим.

Це пов'язано з тим, що невдале проведення оборонної інформаційної операції призведе до „паралічу" систему управління від дій противника і не можливості адекватно ситуації впливати на нього. Тому інформаційна безпека є важливою складовою ІП.

Висновки:

1. Кібернетична модель OODA (OODA-цикл), яка запропонована Дж. Бойдом є універсальною для опису процесів, які проходять в умовах конкурентної боротьби на різних рівнях.

2. Відповідно до концепції Бойда на сучасному етапі розвитку військових систем та озброєння досягнення інформаційної переваги є важливим елементом досягнення перемоги в збройній боротьбі.

3. Цикл OODA можливо використовувати для опису процесів функціонування системи управління інформаційною безпекою. Впровадження циклу OODA для опису системи ІБ дає можливість врахувати дії противника під час проведення оборонної інформаційної операції.

ЛІТЕРАТУРА

1. Ивлев А.А. Основы теории Бойда. Направления развития, применения и реализации. / М., 2008.

2. Гриняев С. Концепция ведения информационной войны в некоторых странах мира, / С.Гриняев // Зарубежное военное обозрение, №2, 2002, с.20 – 28.

3. Иванов О. Американские концепции „стратегического паралича" / О. Иванов // Обозреватель – Observer, №3, 2008, с. 57 – 68.

Кондратюк А.Г. (ВІТІ НТУУ „КПІ”)

КОМПЛЕКСНА МЕТОДИКА ОБРОБКИ ВИХІДНОГО ДОКУМЕНТАЛЬНОГО ПОВІДОМЛЕННЯ НА КІНЦЕВИХ ЗАСОБАХ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Забезпечення достовірного приймання документальних повідомлень з заданою якістю на кінцевих засобах телекомунікаційної мережі (ТКМ), побудованої за технологією комутації пакетів, завжди було актуальною проблемою. Існуючий алгоритм обробки вихідних повідомлень на кінцевих засобах телекомунікаційної мережі передбачає перевірку правильності прийому повідомлень, яка здійснюється на канальному й транспортному рівнях моделі взаємодії відкритих систем (OSI). Згідно цього алгоритму повідомлення не буде прийняте у наступних випадках: 1) якщо на канальному рівні в кадрі повідомлення виявлені помилки та механізми завадостійкого кодування неспроможні їх виправити; 2) на транспортному рівні виявлені помилки передачі або отримані не всі пакети повідомлення. Тобто, у випадку викривлення або неотримання хоча б одного пакета все повідомлення прийнятим не буде, а викривлений (не отриманий) пакет буде запитано повторно. Під впливом завад, що здійснюється на ТКМ, кількість повторних запитів може доходити до безкінечності. В результаті цього, відправлене повідомлення не буде отриманим, що є неприпустимим.Одним з шляхів рішення цієї проблеми є спроба зменшення кількості транзакцій (перезапитів) при передачі текстової інформації з використанням комплексної методики обробки вихідного документального повідомлення на кінцевих засобах телекомунікаційної мережі. Сутність даної методики полягає у модифікації алгоритму прийому-передачі повідомлень інформаційним напрямком ТКМ. Модифікований алгоритм виконує наступні кроки: здійснюється перевірка правильності отримання кадрів вихідного повідомлення засобами канального рівня – при правильному прийомі кадри передаються для подальшої обробки на транспортний рівень; у випадку виявлення помилок викривлений пакет не буде відкидатися адресатом, а надходить до спеціального буферу на час обробки. Обробка викривленого пакета здійснюється на прикладному рівні спеціалізованою програмою згідно методики відновлення текстової інформації. Перевірка достовірності відновлення інформації здійснюється засобами завадостійкого каскадного коду, який використовується під час передачі повідомлень мережею. Зазначений код складається з двох складових частин: внутрішнього та зовнішнього завадостійкого кодів. За результатами висновків внутрішнього завадостійкого коду, який перевіряє кількість розрядів, що дорівнює одному символу, які прийняті в обраній системі кодування, визначаються символи, що не містять помилок. За допомогою зовнішнього коду визначається відповідність всього отриманого повідомлення переданому, включно з варіантами отриманими під час прогнозування; відновлена інформація зберігається в спеціальному буфері; використовуючи механізми транспортного рівня (протокол TCP), на прийомному боці здійснюється накопичення пакетів, що належать до одного повідомлення, які передаються на прикладний рівень; на прикладному рівні прогнозується інформація, яка була втрачена під час передачі цього повідомлення, або ще не надійшла до споживача відповідно до методики прогнозування груп символів в пакеті повідомлення; здійснюється вибір з можливих варіантів пакетів повідомлення (відновленого та прогнозованого) одного, який має найбільшу вірогідність відповідності вихідному повідомленню згідно методики підвищення достовірності прийнятих текстових повідомлень; виконується перевірка вибраного пакета повідомлення засобами канального рівня; приймається рішення на транспортному рівні щодо подальшого прийому пакетів. Таким чином, використання комплексної методики обробки вихідного документального повідомлення на кінцевих засобах телекомунікаційної мережі дозволить вдосконалити алгоритм обробки прийнятих пакетів документального повідомлення на кінцевих засобах, що призведе до зменшення кількості перезапитів викривленої (недоотриманої) інформації, а разом з тим підвищить пропускну спроможність напрямків ТКМ спеціального призначення.

Кравченко К.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)

ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ МОДУЛЯЦІЇ ПІДНЕСУЧИХ ТЕХНОЛОГІЇ LTE

В мережах технології LTE (Long Term Evolution) використовують модуляцію типа OFDM, для її піднесучих стандарт передбачає наступні види модуляції: квадратурну фазову модуляцію QPSK (Quadrature Phase Shift Keying); 16- або 64-рівневу квадратурну амплітудну модуляцію (QAM-16, QAM-64) з рівномірним або нерівномірним розташуванням вершин векторів сигналу в кодовому просторі сигналів.

QPSK менш ефективна з точки зору використання частотного діапазону. Позиції її символів в сузір’ї розміщені набагато далі один від одного і система сприятлива до більш високого рівня шуму, не створюючи при цьому символьних помилок. QPSK не має проміжних станів між чотирма кутовими символьними позиціями, тому зменшується можливість неправильно розпізнати символ в демодуляторі. Для QPSK потрібна менша потужність передавача, щоб досягти того ж самого значення частоти бітової помилки, як в QAM (Quadrature Amplitude Modulation) вищого порядку.

При квадратурній амплітудній модуляції (QAM) змінюється як фаза, так і амплітуда сигналу, що дозволяє збільшити кількість кодованих біт і при цьому істотно підвищити завадостійкість. В даний час використовуються способи модуляції, в яких число кодованих інформаційних біт на одному символьному інтервалі може досягати 8 ... 9, а число позицій можливих станів сигналу − 256 ... 512.

Модуляція QAM, порівняно з QPSK, має більшу пропускну здатність каналу зв’язку оскільки в одному символі передається більша кількість бітів інформації, але меншу завадостійкість, оскільки зменшуються різниці між суміжними значеннями амплітуд і фаз.

Очевидно, що чим вищий рівень модуляції, тим більшими швидкісними можливостями і меншою завадостійкістю вона володіє. QAM модуляція більш чутлива ніж QPSK до нелінійних спотворень і шумів радіотракту.

Системи зв’язку все більше ускладнюються і все більше піддаються виникненню помилок через шум і спотворення. Частота виникнення помилок у системах QAM вищого порядку збільшується більш швидко, ніж у QPSK із-за внесеного шуму й інтерференції між символами.

Вибір конкретного виду модуляції проводиться залежно від необхідної швидкості передачі даних і завадостійкості. Якщо необхідно забезпечити високу спектральну ефективність передачі, тобто передачу великої кількості інформації при використанні меншої частотної смуги і при цьому виконується умова для якісного розповсюдження сигналу, тобто завадова обстановка дозволяє здійснювати передачу, то тоді доцільно вибирати метод модуляції з великою кількістю позицій (типу QAM-16, QAM-64 і навіть більше).

А якщо навпаки завадова обстановка складна або нам потрібно забезпечити неспотворену передачу сигналів з меншою кількістю помилок, то тоді доцільно використовувати модуляцію з малою кількістю позицій (типу QPSK). Можливі й інші критерії вибору виду модуляції, що використовується (наприклад швидкість передачі інформаційних сигналів і т.д.).

Кукін І.В. (НДІ ДПСУ)

ПЕРСПЕКТИВИ РОЗВИТКУ ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ ДЕРЖАВНОГО КОРДОНУ

Зі схваленням Кабінетом Міністрів України розпорядженням № 2031 від 27 жовтня 2010 року Концепції інтегрованого управління кордонами (ІУК) в оперативно-службову діяльність органів та підрозділів Державної прикордонної служби України розпочато запровадження сучасних механізмів державного управління. Відокремлення в ІУК фізичної, інформаційної, технічної та оперативної складових обумовлює актуальність розвитку технічних засобів охорони державного кордону як окремих компонентів системи автоматизованого управління силами та засобами відділів прикордонної служби.

Концептуальні питання розвитку технічної складової охорони державного кордону розглянуті в роботах М. М. Литвина [1], Д. В. Хруста [2], О. В. Ананьїна [3], М. І. Лисого [4] та ін., проте особливості функціонування перспективних зразків технічних засобів охорони державного кордону залишаються недостатньо дослідженими.

Метою доповіді є визначення особливостей нових зразків технічних засобів охорони локальних ділянок місцевості на державному кордоні України, які можуть інтегруватися до систем підтримки управлінських рішень.

Одним з перспективних напрямів удосконалення технічної складової ІУК М. М. Литвином визначено створення систем автоматизованого дистанційного контролю за локальними ділянками з використанням інфрачервоних, мікрохвильових, сейсмічних датчиків, тепловізорів [1, с. 309]. У ході дослідження сучасних прикордонних технологій Д. В. Хрустом зроблений висновок про необхідність розробки технічних засобів для охорони локальних ділянок місцевості, які можуть застосовуватись як елементи системи підтримки прийняття рішень [2, с. 52].

Кожен різновид технічних засобів має певні переваги та недоліки, які обумовлені застосованими в ньому фізичними принципами та способами організації інтерфейсу з людиною. Так, Д. В. Хрустом було показано, що «… тільки інтегровані рішення, в яких різні джерела доповнюють і створюють максимально повну інформацію, демонструють найбільшу ефективність у досягненні цілей та завдань з висвітлення обстановки …» [2, с. 52]. Невід'ємним компонентом сучасних технічних систем охорони державного кордону України є створення на базі цифрових електронних карт геоінформаційної системи для оперативного та цілодобового відображення даних обстановки [2, с. 51].

Поєднання в єдиній телекомунікаційній системі різних технічних засобів охорони державного кордону дає змогу керувати діями прикордонних нарядів з єдиного центру управління службою, що підвищує ефективність управлінських рішень та оперативність реагування на зміни обстановки [3, с. 64]. Також імплементація до технічних засобів охорони державного кордону інтерфейсів із системами підтримки прийняття рішень дає змогу створювати оптимальні розподілені системи технічного контролю [4, с. 236]. Проте, вирішення зазначених завдань потребує виявлення нових властивостей та функцій, що можуть бути реалізовані у перспективних зразках технічних засобів охорони державного кордону [3, с. 65].

На нашу думку, запровадження механізмів державного управління в ІУК може полягати у включенні до алгоритмів роботи технічних засобів охорони державного кордону інтерфейсів із загальними функціями державного управління, якими є: організація, мотивація, контроль та забезпечення. Так, інтерфейс із загальними функціями державного управління може бути досягнутий за рахунок обміну даними між технічним засобом та телекомунікаційною системою про закріплену за ним особу, місце знаходження (координати місцевості), час переведення засобу в активний (робочий) режим, результати фіксації факту виявлення потенційного правопорушника, передача сигналів для управління іншими

технічними засобами охорони державного кордону, направлення сервісної інформації про технічний стан, потребу планового обслуговування або заміни елементів живлення та інших складових частин.

У ході практичної реалізації Концепції ІУК можуть бути запропоновані перспективні ергономічні вимоги до технічних засобів охорони державного кордону, що ґрунтуються на загальних принципах державного управління. Так, з метою удосконалення охорони локальних ділянок місцевості нами пропонувалось використання технічних засобів з інфрачервоними датчиками [5, с. 14]. Запропонований спосіб швидкого їх встановлення на місцевості з використанням можливості тимчасового переключення інфрачервоного випромінювання до оптичного діапазону можна розглядати як елемент функції мотивації персоналу за рахунок простоти користування приладом.

Необхідність зміни режимів роботи технічних засобів при спрацюванні одного з приладів обумовлюється необхідністю врахування в ході прийняття рішень вичерпної інформації з різних джерел. Так, з використанням інфрачервоного датчика можна виявити лише ознаки порушення певного рубежу. З використанням двох таких датчиків можна встановити напрямок руху потенційного правопорушника [5, с. 15]. Проте неможливо без участі людини відрізнити помилкові спрацювання від природних факторів, появи на зазначеному рубежі тварин, виникнення технічних або програмних збоїв.

Заміна інфрачервоних датчиків чисельними засобами відеоспостереження ускладнює вимоги до телекомунікаційних систем, елементів живлення та не усуває помилок оператора під час дистанційного контролю за чисельними ділянками місцевості. Якщо забезпечити можливість при спрацюванні інфрачервоного датчика в автоматичному режимі включити конкретні засоби відеоспостереження на місцевості, то можна в реальному часі виводити лише необхідну для прийняття рішень інформацію оператору центру управління службою.

Таким чином, розвиток технічних засобів охорони локальних ділянок потребує врахування сучасних наукових досягнень у сфері управління оперативно-службовою діяльністю прикордонних підрозділів. Це дає змогу створити необхідні умови інтеграції технічних засобів охорони державного кордону до систем підтримки прийняття рішень. Розглянуті підходи можуть застосовуватися для підвищення ефективності та керованості автоматизованих систем управління.

ЛІТЕРАТУРА

1. Литвин М. М. Основи інтегрованого управління кордонами : курс лекцій / М. М. Литвин. – Хмельницький : НАДПСУ, 2011. – 368 с.

2. Хруст Д. В. Основні напрямки забезпечення подальшого впровадження в практику охорони державного кордону сучасних прикордонних технологій / Д. В. Хруст // Збірник наукових праць Національної академії Державної прикордонної служби України. – Хмельницький : НАДПСУ, 2009. – № 49. Ч. ІІ. – С. 51 – 53.

3. Ананьїн О. В. Концептуальні засади використання інфраструктури телекомунікацій для створення технічних систем охорони на державному кордоні / О. В. Ананьїн // Збірник наукових праць Національної академії Державної прикордонної служби України. – Хмельнийький : НАДПСУ, 2010. – № 53. Ч. ІІ. – С. 64 – 67.

4. Лисий М. І. Загальна структура оптимізаційної моделі розподіленої системи технічного контролю державного кордону // Перспективи розвитку озброєння і військової техніки в Збройних силах України : І Всеукраїнська науково-практична конференція, 04–05 березня 2008 року : Тези доп. – Львів : ЛСІВ НУ “Львівська політехніка”, 2008. – С. 236.

5. Городнов В. П. Спосіб виготовлення технічних засобів охорони державного кордону для охорони локальних ділянок / В. П. Городнов, О. А. Бінькowський, І. В. Кукін // Освітньо-наукове забезпечення діяльності правоохоронних органів України : Всеукраїнська науково-практична конференція [Серія: Військово-технічні науки], (Хмельницький, 14 листопада 2008 року). – Хмельницький : НАДПСУ, 2008. – С. 14 – 15.

Лазаренко М.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

УДОСКОНАЛЕННЯ ОЦІНКИ ОБ’ЄКТІВ КІБЕРНЕТИЧНОГО ВПЛИВУ

З розвитком сучасних інформаційних технологій суспільства, а також їх розвитком у воєнній сфері гостро постає питання завоювання та утримання інформаційної переваги над противником на випадок утворення можливого конфлікту сторін.

В контексті інформаційного протиборства сторін одна з можливих форм отримання інформаційної переваги є кібернетичний вплив. Він досягається шляхом нав’язування обчислювальним процесам інформаційних служб, які виступають об’єктами кібернетичного впливу, спеціальної послідовності даних (вектору атаки) використовуючи засоби віддаленої комп’ютерної взаємодії.

Практичним вирішенням даної задачі пропонується розробка розподіленого програмно-технічного комплексу, де буде відбуватись розподілення частин роботи щодо проведення кібернетичного впливу між кількома вузлами мережі та їх паралельне виконання. Для ефективної реалізації кібернетичного впливу суб’єкт атаки повинен мати початкові відомості для визначення цілевказання програми атаки. Ними виступає апріорна інформація, яка є результатом перевірки наявності обчислювального процесу служб та сервісів на вузлах комп’ютерної мережі.

Ключовим елементом являється оцінка кількісних та якісних характеристик об’єктів кібернетичного впливу. Використання кількісної характеристики було запропоновано в бакалаврській роботі, де була розроблена розподілена інформаційна система, підзадачі якої урівнювалися тільки за кількісними показниками, що дало змогу лише зменшити часові показники проведення інформаційної підготовки масованого кібернетичного впливу на об’єкти комп’ютерної мережі. Додання якісного показника дозволить більш повно підійти до планування розбиття головної задачі, та удосконалити оцінку інформаційної підготовки об’єктів кібернетичного впливу.

Для характеристики якісного параметру будемо використовувати наступні критерії:

1. Вибір характерних ознак.
2. Визначення ваги критеріїв оцінки кожної з ознак.
3. Визначення коєфіцієнтів відповідності об’єкта кібернетичного впливу критеріям оцінки на основі аналізу наявних апріорних показників.
4. Критерії оцінки.
5. Можливість зміни параметрів якісного показника, в залежності від цілевказання суб’єкту масованого кібернетичного впливу.

Отже, для удосконалення проведення масованого кібернетичного впливу на об’єкти комп’ютерної мережі запропоновано варіант розподіленої системи, яка розбиває цілевказання, на підзадачі які будуть виконуватись паралельно на окремих вузлах комп’ютерної мережі, при цьому урівнюючи їх плечі за багатокритеріальними показниками.

Доповідь присвячена висвітленню варіанта багатокритеріальної оцінки об’єкта кібернетичного впливу за кількісними та якісними критеріями на основі адитивного показника, де будуть розглянуті наступні питання:

– додання якісної характеристики об’єкту кібернетичного впливу;
– процедура визначення ваги критеріїв оцінки;
– вимоги до розробки алгоритму обчислення багатокритеріальної оцінки об’єкта атаки.

к.т.н. Ліпатов А.О. (НЦЗІ ВІТІ НТУУ „КПІ”)
Мазниченко Ю.А. (НЦЗІ ВІТІ НТУУ „КПІ”)
Черкасова Ю.О. (НЦЗІ ВІТІ НТУУ „КПІ”)

ЗАХИСТ ЛІНІЙ СУПУТНИКОВОГО ЗВ’ЯЗКУ ВІД РАДІОЕЛЕКТРОННОГО ПРИДУШЕННЯ

Суттєвою особливістю військових систем супутникового зв’язку є необхідність захисту їхніх супутників-ретрансляторів (СР) і земних станцій (ЗС) від навмисних завад. Тому при розробці СР і ЗС необхідно обов’язково враховувати можливий завадовий вплив противника.

Основними системно-організаційними методами захисту ліній військових систем супутникового зв’язку від радіоелектронного придушення (РЕП) є:

покращення захищеності ліній супутникового зв’язку (СЗ) від радіотехнічної розвідки противника;

підвищення стійкості роботи ліній СЗ при впливі комплексів РЕП;

покращення співвідношення енергетичних характеристик ліній СЗ та комплексів радіоелектронного придушення.

У зазначених методах реалізуються відомі технічні рішення [1, 2, 3, 4], такі як:

робота передавачів з мінімально необхідною потужністю;

використання вузькоспрямованих антен з малими боковими пелюстками діаграми спрямованості;

застосування сигналів з розширенням спектру;

регулярна зміна параметрів використовуваних сигналів;

спотворення демаскуючих ознак ліній СЗ з наданням їм ознак об’єктів прикриття (наприклад, лінії комерційного зв’язку);

використання резервних СР, незадіяних у звичайних умовах;

компенсація завади, прийнятої основним каналом прийому, цією завадою, але прийнятою додатково створеним каналом та ін.

Безперервний пошук методів підвищення завадозахищеності ліній та систем супутникового зв’язку продовжується. Результатом пошуку стало нове технічне рішення стосовно підвищення завадозахисту системи супутникового зв’язку [5], яке вирізняється просторовим розміщенням передавальної та приймальної земних станцій, недоступністю навмисним завадам міжсупутникової радіолінії, а також наявністю імітатора ефективного впливу завади.

Взагалі, захист від природних, взаємних та організованих завад систем супутникового зв’язку базується на відмінності структури та закономірностей змінюваності параметрів корисних сигналів і заважаючих впливів. Тому необхідно проводити їхнє комплексне дослідження, враховуючи тактико-технічні характеристики зарубіжних засобів радіорозвідки і можливі завади.

ЛІТЕРАТУРА

1. Военные системы космической связи / Под ред. Косякова Е.Н. – СПб: ВКА им. А.Ф. Можайского, 2003.– 388 с.

2. Базовые средства, комплексы и системы военной связи. Энциклопедический справочник, т. 1/ Под ред. Азарова Г.И.– Мытищи: 16 ЦНИИИ МО РФ, 2005.– 137 с.

3. Вартанесян В.А. Радиоэлектронная разведка. – М.: Воениздат, 1991. – 254 с.

4. Палий А.И. Радиоэлектронная борьба. – М.: Воениздат, 1989.– 350 с.

5. Пат. № 73395. Завадозахищена система супутникового зв’язку / Ліпатов А.О. та ін. Зареєстровано в Державному реєстрі патентів України на корисні моделі 25.09.2012.

Луцук І.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)

ПОРІВНЯННЯ ТЕХНОЛОГІЙ ПЕРЕДАЧІ ДАНИХ В СИСТЕМАХ СУПУТНИКОВОГО ЗВ’ЯЗКУ

На сьогоднішній день для передачі інформаційного трафіку можливе використання представлених нижче технологій передачі даних в системах супутникового зв’язку.

Технологія SCPC (Single Channel per Carrier) використовується для організації виділеного супутникового каналу між деякими точками. В основі технології лежить принцип виділення двох частотних каналів між абонентами (один на прийом, другий на передачу), при чому дані канали жорстко закріплюються за даними абонентами. Отже перевагою мережі SCPC буде висока готовність і гарантована швидкість каналу, а недоліком – висока вартість обладнання, мала ефективність використання частотного ресурсу на супутнику. Крім того, оскільки кількість інформації, що передається в одиницю часу, на центральній станції більше, ніж на периферійних, то ЦЗССЗ (Центральна земна станція супутникового зв’язку) повинна мати антену більшого розміру і (або) більшу потужність передавача. Такі мережі широко використовуються, але кількість абонентських станцій в них, як правило, невелика – від двох до двадцяти.

Технологія MCPC/SCPC (MCPC – Multiple Channels per Carrier). У такій мережі центральна станція використовує для передачі всім абонентським станціям мережі єдину несучу. Поділ даних, призначених різним абонентським станціям, здійснюється не за частотою, а за часом. Отже частотну смугу, призначену для передачі від центру до периферії: центральна станція може динамічно перерозподіляти її в залежності від потреб тієї чи іншої абонентської станції. Однак на ЦЗССЗ зберігається набір модемів за кількістю напрямків до абонентів, тобто для кожної абонентської станції потрібна виділена смуга частот для організації передачі в напрямок на супутник. Отже частотний діапазон, як і в попередній технології використовується неефективно.

DVB-RCS (Digital Video Broadcasting – Return Channel via Satellite) – це мережа супутникового зв’язку, яка використовує принцип поділу супутникового частотного ресурсу TDM/FTDMA (*Time-division multiplexing* / Frequency-Time Division Multiple Access). Ця технологія основана на багаточастотному почерговому доступі абонентських станцій до ЦЗССЗ. З метою забезпечення високої завадостійкості в технології DVB-RCS використовується модуляція QPSK (Quadrature Phase Shift Keying), і подвійний захист завадозахисними кодами: кодом Вітербі і вкороченим кодом Ріда-Соломона. Це дозволяє використовувати на прийомі невеликі антени і дешеве електронне обладнання. Недолік мережі DVB-RCS – відсутність можливості встановлення прямих зв’язків між абонентськими станціями, тому вимоги до ЦЗССЗ будуть набагато вищими ніж до абонентських станцій, оскільки всі потоки проходять саме через неї.

Основою сучасних систем управління військами є система зв’язку і автоматизації. Розвиток системи супутникового зв’язку військового призначення у ЗС України є необхідною складовою для впровадження сучасних автоматизованих систем управління військами. Аналіз вище вказаних технологій передачі даних може забезпечити вибір оптимального варіанту побудови системи супутникового зв’язку військового призначення у ЗС України, який буде відповідати усім вимогам, що ставляться перед даною системою.

Мазниченко Ю.А. (ВІТІ НТУУ „КПІ”)
Чередниченко О.Ю. (ВІТІ НТУУ „КПІ”)
Бондаренко О.Є. (ВІТІ НТУУ „КПІ”)

СИСТЕМИ СУПУТНИКОВОГО ЗВ’ЯЗКУ З ЗОНАЛЬНИМ ОБСЛУГОВУВАННЯМ

Останнім часом кількість абонентів систем рухомого супутникового зв’язку (СРСЗ) постійно зростає. При відносно вузькому (виділеному для супутникового зв’язку) частотному діапазоні, щоб задовольнити зростаючі потреби абонентів, застосовуються різні способи забезпечення множинного доступу у поєднанні з ефективною для використовуваної частотної смуги модуляцією. Забезпечення множинного доступу до супутникового ретранслятора (СР) є загальносистемною проблемою супутникового зв’язку. Одним із можливих способів забезпечення множинного доступу до загального ретранслятора є зональне обслуговування: комбінування традиційних сигнальних (частотно-часових) методів розділення каналів з просторовим рознесенням парціальних зон, що створюються за допомогою променів багатопроменевих бортових антен супутникового ретранслятора. Іншими словами, зональне обслуговування – це множинний доступ з частотно-просторовим розділенням променів. При цьому для збільшення кількості обслуговуваних користувачів з’являється можливість повторного використання частот у різних променях. Це досягається просторовим рознесенням променів, для яких визначена одна й та сама смуга частот [1, 2].

Для найбільш ефективної реалізації системи супутникового зв’язку із зональним обслуговуванням доцільним є застосування на супутниках антен з вузькими променями. Така система забезпечує енергетичний виграш у порівнянні з традиційною аналоговою багатопроменевою антеною з фіксованими променями, завдяки можливості зменшити потужність передавачів на супутнику і на абонентських терміналах. Також з’являється додатковий виграш від повторного використання частот за рахунок точнішої просторової настройки променів.

Найбільш перспективним способом реалізації багатопроменевої антени з вузькими променями є застосування технологій цифрового діаграмоутворення з використанням цифрових антенних решіток (ЦАР). Ключова особливість ЦАР – цифрове формування променів діаграми спрямованості антени. Можливість оперативного перенацілювання приймально-передавальних променів, залежно від територіального розподілу абонентів, забезпечує динамічну оптимізацію обслуговуваної зони покриття [3, 4, 5].

Таким чином, підвищити ефективність функціонування систем рухомого супутникового зв’язку можна використовуючи метод зонального обслуговування. Це досягається застосуванням технологій цифрового діаграмоутворення з використанням цифрових антенних решіток. Крім того, зазначений метод дозволить ефективніше розподіляти частотний ресурс.

ЛІТЕРАТУРА

1. Аболиц А.И. Системы спутниковой связи. Основы структурно-параметрической теории и эффективность. – М.: ИТИС, 2004. – 426с.: ил.

2. Спутниковые сети связи: Учеб.пособие / В.Е. Камнев, В.В. Черкасов, Г.В. Чечин. – М.: „Альпина Паблишер”, 2004. – 536 с.: ил.

3. R. C. Hansen, Phased Array Antennas. New York: John Willey & Sons, 2001 – 489 с.

4. C. A. Balanis, Antenna Theory: Analysis and Design. Second Edition. New York: John Willey & Sons, 1997 – 941с.

5. Системы спутниковой святи с подвижными объектами: Учеб.пособие / А.П. Дятлов,. – Таганрог, ТРТУ 1997. – 97с.

к.т.н.Максимов В. В. (ІТС НТУУ „КПІ”)
Наталенко О. І. (ІТС НТУУ „КПІ”)

ОРГАНІЗАЦІЯ МУЛЬТИМЕДІЙНОГО ЗВ’ЯЗКУ НА КАФЕДРІ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

У ході розвитку мереж телефонії і передачі даних була розроблена концепція NGN, що припускає конвергенцію мереж IP-телефонії з ТфЗК, ЦСІО, інтелектуальними мережами, мережами мобільного зв’язку та мережею Інтернет. З метою взаємодії з усіма мережами та типами сигналізації було розроблено пристрій Softswitch, тобто, програмний комутатор, який став ядром мультисервісної мережі.

Першою організацією, що займається просуванням стандартів по Softswitch і забезпеченням функціональної сумісності різних технологій Softswitch був заснований у 1999 році Міжнародний Softswitch-консорціум ISC (International Softswitch Consortium), перейменований пізніше в IPCC (International Packet Communication Consortium).

Згідно з розробленою в рамках Консорціуму IPCC моделі архітектури Softswitch передбачаються чотири функціональні площині: транспортна, яка відповідає за транспортування повідомлень по мережі зв’язку (включає в себе домен IP-транспортування, домен взаємодії і домен доступу, відмінний від IP); площина управління обслуговуванням виклику і сигналізації, яка управляє основними елементами мережі IP-телефонії (включає в себе контролер медіашлюза, Call Agent, Gatekeeper); площина послуг і додатків, яка реалізує управління послугами в мережі (містить сервери додатків і сервери ДВО); площина експлуатаційного управління, яка підтримує функції активізації абонентів і послуг, техобслуговування, білінгу й інші експлуатаційні завдання.

Основне завдання Softswitch – погоджувати різні протоколи сигналізації як мереж одного типу, наприклад, при сполученні мереж H.323 і SIP, так і при взаємодії мереж комутації каналів з IP-мережами. Основні типи сигналізації Softswitch – сигналізація для управління з’єднаннями, сигналізація для взаємодії різних Softswitch між собою і сигналізація для керування транспортними шлюзами. Основними протоколами сигналізації управління з’єднаннями сьогодні є SIP-T, ОКС-7 і H.323. Як опції використовуються протокол E-DSS1 первинного доступу ISDN, протокол абонентського доступу через інтерфейс V5. Основними протоколами сигналізації керування транспортними шлюзами є MGCP і Megaco/H.248, а основними протоколами сигналізації взаємодії між комутаторами Softswitch є SIP-T і BICC.

На кафедрі телекомунікаційних систем дисципліна „Проектування телекомунікаційних мереж наступного покоління” уведена в навчальні плани у 2011/2012 навчальному році і входить до базової підготовки спеціалістів і магістрів напряму 6.050903 „Телекомунікації” спеціальностей 7.092401 „Телекомунікаційні системи та мережі”. Дана дисципліна ґрунтується на знаннях, отриманих студентами при вивченні дисциплін „Телекомунікаційні мережі”, „Мережі з комутацією пакетів”. Основний матеріал дисципліни спрямований на вивчення та закріплення теоретичних основ проектування, а також розрахунку мереж NGN, що розкривається в таких темах: „Застосування рішень NGN для розвитку мереж зв’язку, „Стратегії впровадження технологій NGN при розвитку мережі ТфЗК”, „Застосування технологій NGN для розвитку мережі ТфЗК і ІМЗ”, „Методологія проектування мереж зв’язку”, „Методика проектування мереж зв’язку”, „Проектування розподіленого абонентського концентратора”, „Проектування розподіленого транзитного комутатора», „Проектування розподіленого SSP”, „Проектування конфігурації мережі на основі NGN рішень”, „Розподіл навантажень. Розрахунок транспортного ресурсу взаємодії комутаторів пакетної мережі”, „Розрахунок продуктивності комутаторів пакетної мережі”.

Для забезпечення студентів якісними знаннями з вищезазначеної дисципліни, а також вироблення практичних навичок роботи з апаратурою нового покоління, кафедра

Телекомунікаційних систем Інституту телекомунікаційних систем повинна створити взірцеву інтегровану мережу зв'язку, яка відповідає концепції NGN. Звісно, невід'ємною частиною комплексу мультимедійних засобів, які конфігуруються в лабораторному комплексі кафедри Телекомунікаційних систем у єдину мережеву систему в межах концепції NGN, є Softswitch, в якості якого може фігурувати IP-АТС. У якості програмного рішення для створення IP-АТС можна використовувати Asterisk.

Asterisk – це програмна IP-АТС, розроблена компанією Digium як програмне забезпечення з вільним і відкритим вихідним кодом. Функції Asterisk, з-поміж інших, включають: голосовий зв'язок, конференц-зв'язок, голосову пошту, інтерактивні голосові меню, автоматичне перенаправлення викликів тощо. Програмне забезпечення Asterisk працює на різних програмно-апаратних платформах, що включає такі операційні системи, як Linux, FreeBSD, OpenBSD, NetBSD, Solaris. Також є окремий проект для організації IP-АТС на базі Asterisk на операційній системі Windows.

IP-АТС Asterisk підтримує наступні VoIP протоколи: персонального обміну версія 1 і 2 (IAX1/2); мультимедійного обміну H.323; мультимедійного обміну SIP; управління шлюзами MGCP; „тонкого" під'єднання SCCP; двотональний DTMF; багаточастотний MF/MFC-R2; абонентський цифровий EDSS1; виносного управління GR-303/V5.1/V5.2; загальноканальної сигналізації SS7; Skype; Google Talk.

IP-АТС Asterisk підтримує такі аудіокодеки: G.711 (A-Law, μ-Law); G.722; G.723.1; G.726; G.729; GSM; iLBC; Linear; LPC-10; Speex.

Використовуючи протоколи VoIP, Asterisk надає можливість здійснення телефонних розмов, використовуючи IP-мережу або мережу Інтернет в якості середовища передачі голосових даних. За наявності комп'ютерної та телефонної мережі є можливість конвергенції послуг і функцій, які ними надаються, у єдине телекомунікаційне середовище. Asterisk може працювати як з аналоговими лініями FXO/FXS, так і цифровими ISDN BRI/PRI. За допомогою певних комп'ютерних плат Asterisk можна підключити до ліній T1/E1, які дають змогу працювати з десятками і сотнями телефонних ліній. Asterisk може працювати як з аналоговими, так і з програмними телефонами.

На рис.1 показана типова схема підключення IP-АТС Asterisk.

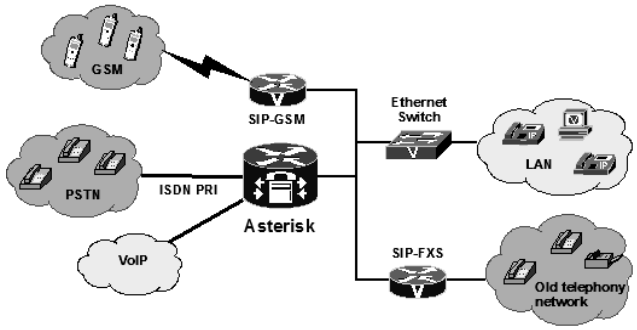


Рис. 1. Типова схема підключення IP-АТС Asterisk

IP-АТС Asterisk надає такі функції управління дзвінками: отримання нагадувань; голосова пошта; аутентифікація; автоматичний секретар; чорні списки; безумовна пере адресація; запис докладної інформації про дзвінок (CDR); переадресація дзвінка, якщо абонент зайнятий; переадресація дзвінка, якщо абонент не відповідає; запис телефонних переговорів; прослуховування телефонних переговорів; постановка дзвінка в просту чергу; маршрутизація дзвінка в залежності від номера ініціатора або отримувача дзвінка; переадресація дзвінка; очікування дзвінка; визначення номера або імені абонента; мультиплеєрні конференції; робота з базами даних з сценарію роботи АТС і т.д.

В якості корпоративної IP-АТС Asterisk надає: підключення внутрішніх абонентів корпоративної телефонної мережі; підключення до операторів телефонії (місцевий фіксований телефонний зв'язок; мобільний зв'язок у стандартах GSM і CDMA; оператори IP-

телефонії); підключення віддалених співробітників до корпоративної АТС; підключення віддалених офісів; традиційні функції УВАТС (переадресація, утримання, перехоплення дзвінка, і т.д.); організація аудіо-конференцій для проведення нарад; створення інтерактивних голосових меню (IVR); голосова пошта з персональними скриньками співробітників; запис детальної статистики дзвінків (CDR); маршрутизація викликів за найменшою вартістю дзвінка (LCR); можливість запису і прослуховування телефонних переговорів. Програмно-апаратна платформа на базі IP-АТС Asterisk може використовуватися як для заміни УВАТС, так і для повноцінної заміни РАТС, оскільки застосовувані в цьому програмному забезпеченні алгоритми добре масштабуються на велику кількість обладнання та користувачів.

Для демонстрації можливостей IP-АТС і перспектив застосування її для організації мультимедійного зв'язку на кафедрі телекомунікаційних систем було організовано демонстраційний стенд на базі однієї з лабораторій кафедри.

Демонстраційний стенд включає:

– сервер Asterisk на базі операційної системи з вільним і відкритим програмним кодом GNU/Linux;

– два програмні SIP-телефони (програмне забезпечення – Phoner Lite) на базі операційної системи Windows;

– один апаратний SIP-телефон фірми Dlink;

– два Ethernet-комутатора фірми Dlink;

– один маршрутизатор Mikrotik.

Структурну схему такої мережі представлено на рис. 2.

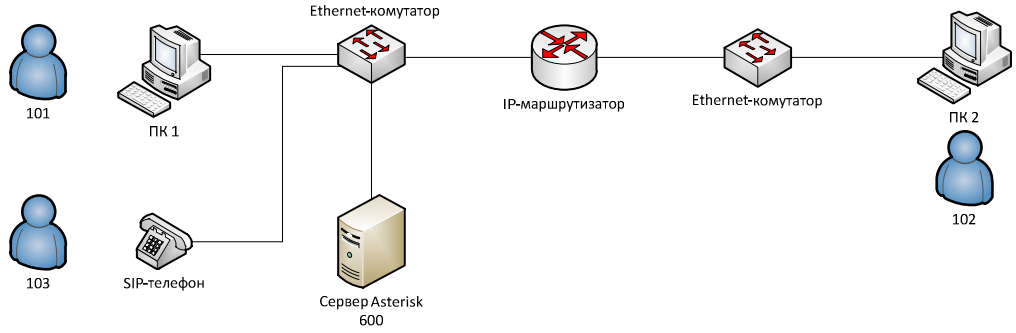


Рис. 2. Схема організації зв'язку демонстраційного стенду на базі IP-АТС Asterisk

Сервер Asterisk побудовано на базі звичайного персонального комп'ютера під керування операційної системи з вільним і відкритим вихідним кодом GNU/Linux, а саме з використанням дистрибутива Ubuntu Server 11.10. Використовувана версія Asterisk – 1.8.4.4.

Користувачам виділено номери 101, 102 і 103 (див. рис. 1), а на сервері налаштовано автовідповідач із тестуванням відлуння для перевірки зв'язку користувачами. Номер автовідповідача 600. У ході випробувань наведена вище схема продемонструвала достатню якість голосового зв'язку. Однак для впровадження її для обслуговування більшої кількості абонентів потрібно враховувати вимоги до якості обслуговування, тобто, до затримки передавання пакетів, для чого потрібно відповідним чином налаштувати пріоритезацію трафіку на комутаторах, маршрутизаторах, а також на сервері. Для цього потрібно використовувати керовані комутатори L2 з підтримкою QoS, а також клієнтські робочі станції з підтримкою алгоритмів планування передавання мережевих пакетів, які дають змогу уникнути переповнення буферу зв'язку, що може погіршити якість надання послуг. Таким алгоритмом є, наприклад, CoDeL, реалізацію якого включено в останні версії операційної системи GNU/Linux.

До переваг наведеної вище схеми організації зв'язку відносяться:

1. Інтеграція всіх послуг зв'язку в рамках єдиної IP-мережі, що відповідає концепції NGN.

2. Зручність налаштування потрібних послуг, оскільки відповідні дії виконуються інженером обслуговування віддалено безпосередньо з його робочого місця.

3. Зручність і швидкість додавання нових послуг, а також можливість робити це в безпечному режимі, не порушуючи роботу наявних послуг мережі.

4. Простота додавання нових абонентів – оскільки на кожному робочому місці використовується ПК, необхідно лише під'єднати його до корпоративної мережі, налаштувати на ньому програмний SIP-телефон і під'єднати голосову гарнітуру. Також можна обладнати робоче місце апаратним SIP-телефоном, що більш зручно та звично для користувача.

5. Економія коштів під час створення такої системи зв'язку, оскільки використовується програмне забезпечення з вільним і відкритим вихідним кодом.

Схема зв'язку з використанням IP-АТС Asterisk має вказані нижче недоліки:

1. Виникає необхідність модернізації локальної мережі для забезпечення необхідної якості обслуговування (QoS). Це включає використання й відповідне налаштування керованих комутаторів L2, маршрутизаторів, які підтримують пріоритезацію трафіку, а також робочих станцій.

2. Виникає необхідність повторного навчання кадрів, що може тривати відчутний проміжок часу, а також може потребувати відповідних матеріальних витрат.

3. Зменшується надійність мережі, оскільки за виходу з ладу сервера зв'язку весь спектр мультимедійних послуг зв'язку стає недоступним. Ця проблема може вирішуватися резервуванням, що, однак, потребує додаткових матеріальних затрат.

4. Виникає необхідність застосування й налаштування додаткового медіашлюзу для сполучення корпоративної мережі зв'язку з телефонною мережею загального користування.

5. Постають питання організації інформаційної безпеки конвергованої мережі надання мультимедійних послуг. Питання забезпечення безпеки в сучасних телекомунікаційних мережах мають особливо високу актуальність, тому що від їх вирішення напряму може залежати діяльність критично важливих установ, наприклад, банківських. Це також стосується і зв'язку, який використовується у військових цілях. Для розв'язання цього питання потрібно застосовувати додаткові засоби, які включають створення віртуальних приватних мереж із шифруванням (наприклад, OpenVPN) або застосування набору протоколів IPSec. У будь-якому випадку, питання безпеки – це тема окремого дослідження, тому що використання шифрування збільшує затримку передавання пакетів, що може негативно відобразитися на якості надання послуг, наприклад, голосового зв'язку.

Отже, використання IP-АТС Asterisk дає змогу реалізувати принципи конвергенції мереж, закладені в концепції NGN, надати користувачам нові послуги, а також збільшити керованість мережі зв'язку. Однак для реалізації надійного зв'язку з використанням IP-технологій потрібно значну увагу приділити якості обслуговування (QoS), враховуючи те, що транспортна IP-мережа використовуватиметься для передавання різнорідного трафіку, що призводитиме до конфліктів під час його обслуговування.

ЛІТЕРАТУРА

1. Меггелен Дж., Мадлен Л., Смит Дж. Asterisk: будущее телефонии, 2-е издание. – Пер. с англ. – СПБ: Символ_Плюс, 2009. – 656 с., ил.

2. Бакланов И.Г. NGN: принципы построения и организации. – М.: Эко-Трендз, 2008. – 400 с.

3. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. – СПб.: БХВ – С-П, 2006. – 368 с.

4. В. Маслаков. Linux на 100%. СПб: Питер, 2009. 336 с., ил.

5. Колисниченко Д. Н. Linux. От новичка к профессионалу. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2010. – 784 с.: ил.

6. Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley. Unix and Linux system administration handbook. 4th edition. Boston: Prentice Hall. – 1340 с.

Манокін Є.В. (НДІ ДПСУ)

ОЗНАКИ ЩОДО ВИБОРУ СИСТЕМ ВИЯВЛЕННЯ АТАК У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ

Стрімкий розвиток інформаційних технологій зумовлює створення нових загроз для інформації, які можуть негативно впливати не тільки на окремий інформаційний вузол та організаційно-технічні системи, а й на цілі галузі, від яких залежить економіка, обороноздатність країни тощо. Враховуючи те, що сучасні телекомунікаційні мережі інтегровані в глобальні інформаційні мережі, джерело загроз для інформації може знаходитись в будь-якій точці світу.

Виходячи з цього, у правоохоронних органах створені підрозділи які відповідають за захист даних у своїх структурах. На думку автора, для ефективної протидії несанкціонованих дій в інформаційно-телекомунікаційних системах Державної прикордонної служби України часткова відповідальність за технічний захист службової інформації слід покласти на персонал. Для цього мають бути створені методики організаційної, технічної та правової складової цього процесу.

Питання аналізу та вибору оптимальних рішень реалізацій систем захисту інформації на прикладі систем виявлення атак досліджувались Д. Г. Леоновим, А. В. Лукацьким, І. Б. Медведовським, Б. В. Семьяновим , Д. Ю. Гамаюновим , та іншими. Але підходи до оптимального вибору систем виявлення атак в інформаційно-телекомунікаційних системах Державної прикордонної служби України залишаються недостатньо дослідженими, що призводить до слабкої ідентифікації комп’ютерних атак на ранньому етапі їх розвитку та своєчасному реагуванню на них.

Мета роботи полягає в узагальненні ознак для вибору оптимальних рішень під час проектування та впровадження систем виявлення атак на об’єктах інформаційної діяльності Державної прикордонної служби України.

Складні інноваційні проекти щодо розроблення та впровадження захищених інформаційних мереж у 80-х роках XX століття дали поштовх для розвитку нового напряму в сфері інформаційної безпеки, який спрямований на виявлення зловмисних дій в інформаційно-телекомунікаційних системах організацій. До таких зловмисних дій можна віднести мережеві атаки проти певних сервісів або вузлів, несанкціонований доступ до інформаційних систем, дію шкідливого програмного забезпечення. Зазначений напрям інформаційної безпеки отримав назву „виявлення атак” (instrasion detection).

Системи виявлення атак (IDS – intrusion detection system) – це програмний або програмно-апаратний комплекс, який за допомогою певних алгоритмів здатен розпізнавати підозрілі трафіки чи аналізувати роботу конкретного хоста, щодо виявлення несанкціонованих дій у відповідному інформаційному просторі.

Головне призначення цих систем:

– ідентифікація відомих, а по можливості і невідомих загроз на інформаційну структуру (виявлення фактів сканування, зондування чи атаки тощо), яка підлягає захисту, та попередження про це персонал, який відповідає за забезпечення інформаційної безпеки;

– контроль дій всіх суб’єктів інформаційної системи;

– надання даних щодо формування сценарію атаки;

– надання можливості контролю та проведення аудиту інформаційної безпеки не тільки відповідному фахівцю, але і звичайному користувачу;

– надання доказової бази під час розгляду певних інцидентів;

– виявлення недоліків міжмережевих екранів (встановлення IDS після міжмережевого екрана дає змогу конфігурувати його політику безпеки шляхом аналізу інформаційного потоку, який він пропускає);

– збирання інформації щодо нових типів атак;

– складання звітів;

– блокування певних вузлів Інтернету [1].

Реалізація IDS може бути об'єднана з мережевим екраном та засобами захисту від вірусів, а може бути реалізована як незалежна система. Під час використання IDS враховуються три методи виявлення підозрілої активності, а саме: мережевий, хост-орієнтовний та комбінований [2, с. 299].

Архітектура систем виявлення атак включає [3, с. 8]:

– консоль управління;

– сервер, який аналізує інформацію мережевих датчиків та зберігає інформацію про атаки;

– сенсорна підсистема ;

– підсистема аналізу;

Для більш глибокого аналізу та оптимального вибору IDS можна застосовувати дві групи ознак. Перша група ознак призначена для аналізу методів виявлення підозрілої активності. Друга група ознак призначена для аналізу самих систем виявлення атак як окремого елемента інформаційної безпеки.

До першої групи слід віднести такі ознаки:

– рівень спостереження за системою;

– верифікованість;

– адаптивність;

– стійкість.

До другої групи ознак слід віднести:

– клас виявлення атак;

– маштабованість;

– відкритість;

– реакція системи у відповідь на атаку;

– захищеність;

– метод виявлення підозрілої активності.

Висновок.

Використання запропонованих ознак щодо аналізу та оптимального вибору систем виявлення атак дозволить підвищити рівень захищеності інформаційних ресурсів організації за рахунок поширення організаційних, правових, технічних механізмів на дії користувача інформації, що надасть змогу більш ефективно реагувати на нові, раніше не задокументовані загрози, несанкціонований доступ до інформації та інші негативні впливи на інформаційні ресурси Державної прикордонної служби України.

ЛІТЕРАТУРА

1. Амелин Р. В. Информационнная безопастность [Електроний ресурс] / Р. В. Амелин // Учебно-методическое пособие по вопросам информационной безопасности. – Режим доступу : http://nto.immpu.sgu.ru/sites/default/files/3/__77037.pdf.

2. Леонов Д. Г. Атака из Интернета / Д. Г. Леонов, А. В. Лукацкий, И. Д. Медведовский, Б. В. Семьянов //. – М. : Солон-Р, 2002. – С. 299.

3. Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов : дис. на соискание ученой степени кандидата физико-математических наук. : 05.13.11 / Д. Ю. Гамаюнов. – М., 2007. – С. 8.

к.т.н. Манько О. В. (ЖВІ НАУ)
к.т.н. Міхєєв Ю. І. (ЖВІ НАУ)

АВТОМАТИЗОВАНА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАСТОСУВАННЯ ТЕХНІЧНИХ ЗАСОБІВ ПРИ ПЛАНУВАННІ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ

Аналіз останніх військових конфліктів свідчить про високу динаміку зміни обстановки, що призводить до необхідності оперативного збору інформації та своєчасної корекції планів застосування технічних засобів. Однак ці завдання ускладнюються у зв'язку із різноманітністю технічних засобів, що задіяні та особливістю їх застосування у ході проведення спеціальних операцій. Підвищити оперативність аналізу обстановки з подальшим вибором варіантів дій можливо шляхом впровадження єдиної автоматизованої системи підтримки та прийняття рішень, що є пріоритетним напрямом розвитку збройних сил розвинутої держави. Розроблена система повинна мати здатність накопичувати та зберігати інформацію про наявні сили й засоби, інформаційно-психологічну обстановку в заданому районі з відображенням районів: відселення; загострення криміногенної ситуації; нестабільної соціально-політичної обстановки; компактного проживання національних меншин; посиленого морально-психологічного забезпечення дій своїх військ і.т.д. Необхідним при розробці такої системи є використання геоінформаційних технологій для відображення існуючої обстановки в районах проведення операції на цифрових картах.

У доповіді розглядаються принципи побудови автоматизованої системи підтримки та прийняття рішень щодо застосування технічних засобів, обґрунтовуються вимоги до її складу та тактико-технічних характеристик. Наведено зміст основних етапів розробки такої системи, а саме: ідентифікації, концептуалізації, формалізації, реалізації та випробувань.

Представлено програмну реалізацію подібної системи, яка здатна відображати поточну обстановку на цифровій карті та містить у своєму складі базу прийнятих умовних позначень технічних засобів та довідкову інформацію про них, має можливість розраховувати зони дії засобів трансляції радіо- та телевізійних сигналів, прогнозувати оптимальний склад пересувних радіотелевізійних засобів, що планується задіяти при вирішенні цільового завдання.

Проведений аналіз результатів роботи прототипу програмної реалізації автоматизованої системи підтримки прийняття рішень щодо застосування технічних засобів під час проведення командно-штабних навчань „Адекватне реагування 2011"та тактико-спеціального навчання „Перспектива 2012" показав, що оперативність нанесення поточної обстановки в можливому районі загострення конфлікту порівняно з прийнятими методами підвищується на 25 %, що в цілому впливає на підвищення ефективності проведення військових операцій сьогодення.

ЛІТЕРАТУРА

1. Крысько В. Г. Секреты психологической войны: цели, задачи, методы, формы и опыт / В. Г. Крысько. – Минск, 1999. – 156 с.

2. Шуляк П. І. Деякі погляди на створення та застосування перспективних формувань сухопутних військ / П. І. Шуляк, Д. П. Музиченко Ю. В. Пунда.: Наука і оборона. Наук.–практ. Журнал МОУ. №1, 2011 – С. 13– 17.

3. Постников А. Н. Единая система автоматизированного управления Вооруженными силами – жизненная необходимость. [Электронный ресурс]. – Режим доступу: http://www.ng.ru/realty/2011-01-14/1_automate.html.

4. Автоматизированные системы управления сухопутными войсками США. [Электронный ресурс]. – Режим доступу: http://252.ucoz.ru/load/avtomatizirovannye_sistemy_upravlenija_sukhoputnymi_vojskami_ssha.

к.т.н. Масесов М.О. (НЦЗІ ВІТІ НТУУ „КПІ”)

АНАЛІЗ ПЕРСПЕКТИВ ВПРОВАДЖЕННЯ ТЕХНОЛОГІЇ MIMO В СУЧАСНІЙ РАДІОЕЛЕКТРОННІЙ АПАРАТУРІ

Аналіз застосування сучасних інформаційних технологій у радіоелектронній апаратурі та бездротових системах зв’язку показав, що основними тенденціями їх впровадження є застосування спектрально-ефективних методів цифрової обробки сигналів і антенної технології MIMO (Multiple Input – Multiple Output). Розуміння фізичних процесів, розробка та удосконалення визначених методів дає змогу обґрунтовано аналізувати їх застосування та формулювати перспективні тенденції їх подальшого впровадження. Тому обрана тематика досліджень є актуальним науковим завданням.

Теоретичне обґрунтування обробки сигналів у багатоантенній технології MIMO досить докладно описано в різноманітних джерелах численних авторів. Свою практичну реалізацію технологія MIMO одержала в стандартах бездротового зв’язку сімейств 802.11 та 802.16. Крім того, технологія MIMO планується до використання у подальшому в четвертому й, перспективно, у п’ятому поколіннях систем радіозв’язку.

Проведений аналіз показав, що технологія MIMO знайшла своє застосування та активно впроваджується в нижче приведеній радіоелектронній апаратурі:

– пристрої бездротового зв’язку для побудови локальних обчислювальних мереж;

– системи радіолокації;

– цифрові антенні решітки з вбудованими приймально-передавальними пристроями;

– вимірювальна радіоапаратура;

– бази радіодоступу й абонентські радіотерминали зв’язку.

Крім того, відомі й теоретично обґрунтовані варіанти застосування технології MIMO у засобах радіорелейного й тропосферного зв’язку. Нерозривно з MIMO слід розглядати технологію OFDM (N-OFDM) – ортогональну (неортогональну) частотну дискретну модуляцію, яка найбільш вдало з нею інтегрується. Однак у системах спеціального призначення зазначені технології слід адаптувати до особливостей їх застосування й можливого впливу навмисних перешкод, що визначає широке коло подальших досліджень.

Заслуговують на увагу також теоретичні та практичні засади створення інтегрованої системи радіолокації та зв’язку спеціального призначення, що ґрунтується на застосуванні антенної технології MIMO і мульти-MIMO. Переваги такої системи проявляються в економії засобів зв’язку спеціального призначення та широкому просторовому розмаху побудованої системи радіолокації – система в реальному масштабі часу буде в змозі виводити інформацію про виявлені повітряні цілі, а також виконувати завдання, традиційні зв’язку. Серед недоліків такої системи слід зазначити значне ускладнення обробки сигналів у цифровому сегменті тропосферної (радіорелейної) станції, теоретичне обґрунтування можливості поділу й обробки сигналів зв’язку й радіолокації. Тому створення такої системи є досить складною науковою та прикладною проблемою. В якості напрямків подальших досліджень слід зазначити створення математичної моделі роботи перспективного комплексу з інтеграцією завдань радіолокації та зв’язку, розробку й обґрунтування математичного апарату обробки сигналів у цифровому сегменті станції, вибір обчислювальної апаратної платформи комплексу й обґрунтування практичної реалізації запропонованої системи.

ЛІТЕРАТУРА

1. Слюсар В. И. Системы MIMO: принципы построения и обработка сигналов / В. И. Слюсар // Электроника: наука, технология, бизнес. – 2005. – № 10. – С. 52 – 59.

2. Зинченко А. А. Некоторые аспекты реализации интегрированной системы связи и радиолокации / А. А. Зинченко, Н. А. Масесов // Информационные системы и технологи : междунар. науч.-техн. конф., 20 апреля 2012 г. : тезисы докл. – Н. Новгород, 2012. – С. 132.

к.т.н. Масесов М.О. (НЦЗІ ВІТІ НТУУ „КПІ”)
Радченко М.М. (НЦЗІ ВІТІ НТУУ „КПІ”)
Зеленко О.В. (НЦЗІ ВІТІ НТУУ „КПІ”)
Нечушкін М.П. (НЦЗІ ВІТІ НТУУ „КПІ”)

КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА САЙТАХ

На початку 90-х років минулого століття виникла нова загроза національній безпеці України. З’явилися такі поняття, як „інформаційне протиборство”, „інформаційна війна”, „інформаційна зброя”. У США, в Європі, а пізніше й в Україні почали проводитися науково-дослідні та дослідно-конструкторські роботи в області інформаційної безпеки та захисту інформації, розроблятися нормативні й керівні документи, прийматися нові стандарти. У цей час питанню інформаційної безпеки приділяється підвищена увага на урядовому рівні „Великої вісімки”. У промислових групах США, поряд з Федеральним центром захисту інфраструктури при ФБР США й Головним федеральним центром, передбачена організація власних корпоративних центрів аналізу інформації. Таким чином, у США створюється багатоступенева система інформаційного захисту. Після подій 11-го вересня 2001 року питання інформаційної безпеки перебувають під пильною увагою також і приватних осіб. Європейські країни прийняли документ за назвою „Загальні критерії” (оформлений пізніше у вигляді стандарту ISO 15408: 1999-1-3), що впорядковує критерії безпеки. В свою чергу, Верховної Радою України був прийнятий закон України „Про захист інформації в інформаційно-телекомунікаційних системах”. Цей документ дає досить чітку систему поглядів на мету, завдання, принципи й основні напрямки забезпечення інформаційної безпеки. Крім того, були прийняті ряд підзаконних нормативних актів, що регламентують особливості дії закону в різних галузях і сферах діяльності міністерств, відомств та підприємств.

Швидкий розвиток процесів автоматизації, використання комп’ютерів у всіх сферах сучасного життя, крім безсумнівних переваг, спричинило появу ряду специфічних проблем. Одна з них – необхідність забезпечення ефективного захисту інформації. Виходячи із цього створення правових норм, що закріплюють права й обов’язки громадян, колективів і держави на інформацію, а також захист цієї інформації стають найважливішим аспектом інформаційної політики держави.

Як показав досвід останніх подій в Україні, інформаційна безпека сайтів урядового підпорядкування не може забезпечити гарантованого захисту від несанкціонованого доступу сторонніх осіб (груп осіб). Тому дослідження за обраною тематикою є актуальною науковою і практичною задачею.

Для розуміння сутності роботи слід визначити найбільш ймовірні та характерні вразливості, які існують для інформації на сайтах. Під вразливостями на сайтах будемо мати на увазі недоліки, які можуть порушити цілісність роботи сайту або викликати неправильну роботу. Причин може бути багато: від помилок програмістів до ненадійних паролів і вірусів. У роботі приведені результати досліджень щодо можливих вразливостей сайтів та запропоновані концептуальні засади забезпечення їх інформаційної безпеки.

Проведений авторами аналіз показав, що характерними прикладами атак на сайти є підміна головної сторінки сайту, видалення файлової системи, підміна інформації, розміщення вірусів, розсилання спаму, створення високого навантаження на сайт.

Для перевірки і своєчасного виявлення загроз для сайту існує два основних способи: використання сканерів вразливостей – спеціальних програм для аналізу роботи сайту та виявлення можливих шляхів несанкціонованого втручання в роботу; самостійне тестування сайту – робота експертів для виявлення потенційних “дір” в роботі сайтів.

Для захисту сайтів найбільш широко застосовуються наступні методи:

1. Використання паролів. Паролі не повинні бути простими, їх слід регулярно змінювати. Паролі до адміністративної панелі мають бути складніше за паролі користувачів.

2. Резервне копіювання. Копії сайту необхідно робити періодично й зберігати їх на жорсткому зовнішньому диску.

3. Перевірка файлів сайту на віруси через сканери. Можна використовувати онлайн-сканери (unmaskparasites.com, vms.drweb.com/online/, 2ip.ru/ site-virus-scaner/, antivirus-alarm.ru/proverka/).

4. Закриття непотрібних з'єднань (наприклад, ftp після використання).

5. Використання антивірусного програмного забезпечення для захисту.

6. Використання аутентифікації й авторизації – необхідно ретельно закривати інформацію, що не повинна бути доступна користувачеві; ділити користувачів на групи й визначати права доступу для кожної групи.

7. Забезпечення заборони щодо внесення html або js-кодів у коментарях на сайті. Заборона вводити й відправляти код через форми, обмеження довжини символів у полях.

Серед основних заходів, які необхідно виконати при виявленні несанкціонованого доступу, слід зазначити наступні: зміна паролю у панелі керування, а також паролю в ftp-клієнті; видалення заражених файлів (які, як правило, мають довгі незрозумілі назви, дати останньої зміни будуть збігатися або будуть близькі один до одного); перевірка сайту на наявність вірусів-хробаків й інших вразливостей; використання безпечних протоколів (SSH і SFTP); перевірка сайту спеціалізованими органами (організаціями).В якості висновків слід зазначити, що інформація в сучасному світі є одним з основних об'єктів інтересу як державних спецслужб, правоохоронних і контролюючих органів, так і конкурентів або зловмисників. Витік інформації може призвести до значних економічних втрат. В останні роки у зв'язку з технічним прогресом особливого розвитку одержало викрадання інформації з використанням науково-технічних засобів, у тому числі електронно-обчислювальної техніки. Протистояти цьому можуть тільки висококваліфіковані фахівці в області захисту інформації, і тільки ті, які постійно вдосконалюються й підвищують свій рівень. Таким чином, підготовка кваліфікованих фахівців з інформаційної безпеки стоїть окремим актуальним питанням для вищих навчальних закладів як Збройних Сил України, так і держави в цілому. Слід також мати на увазі, що загрози безпеки інформації постійно змінюються та модифікуються, тому необхідно постійно міняти засоби захисту, вдосконалювати методи й алгоритми забезпечення інформаційної безпеки.

ЛІТЕРАТУРА

1. Закон Україну „Про інформацію".

2. Закон України „Про захист інформації в автоматизованих системах".

3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах".

4. Закон України „Про державну таємницю".

5. Закон України „Про основи національної безпеки України".

6. Положення про технічний захист інформації в Україні. Указ Президента України від 27.09.1999 № 1229.

7. Концепція технічного захисту інформації в Україні. Постанова КМ України від 08.10.1997 № 1126.

8. Про деякі питання захисту інформації, охорона якої забезпечується державою. Постанова КМ України від 13.03.2002 № 281.

9. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.

10. ДСТУ 3396 1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

11. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

Мельничук І. В. (ВІТІ НТУУ „КПІ”)
к. т. н. Хусаінов П. В. (ВІТІ НТУУ „КПІ”)

ВИМОГИ ДО ПЕРСПЕКТИВНИХ СИСТЕМ НАВ’ЯЗУВАННЯ КІБЕРНЕТИЧНОГО ВПЛИВУ

Останнім часом воєнні відомства багатьох країн розглядають форми та способи створення систем нав’язування кібернетичного впливу (КВ) як одну з важливих складових озброєння. Хоча досі немає чіткої термінології, але такі системи зазвичай називають кібернетичною зброєю. Під цим терміном ми будемо розуміти сукупність програмних та апаратних засобів, які дозволяють суттєвим чином впливати на об’єкт атаки, змінюючи його нормальне функціонування. Кібернетична зброя відноситься до нових видів зброї, і необхідно розробляти власні зразки такої зброї для підтримання здатності ведення бойових дій у кіберпросторі. Система нав’язування КВ повинна володіти деякими важливими якостями, а саме: 1. Скритність. Окремий вузол системи повинний виглядати так, щоб ніхто не міг запідозрити його істинного призначення. Свої дії він повинний також приховувати або маскувати під інші, які не викликають підозри. Пропонується маскування власних дій під дії іншої відомої програми, яка встановлена у багатьох клієнтів. 2. Децентралізованість. У системі з єдиним центром управління є принципова проблема – з локалізацією і знищенням центру управління ми втрачаємо контроль над системою, або навіть гірше – зловмисник перехвачує контроль над нею. Таким чином, сучасна система повинна мати декілька центрів управління із можливістю динамічної їх зміни. Потрібно передбачити можливість авторизації та аутентифікації командного центру з метою недопущення захоплення сторонньою особою контролю над системою. 3. Можливість розширення. З часом виникають нові задачі і для їх виконання окремі вузли повинні бути спроможні виконувати їх шляхом підключення додаткових модулів. Модулі повинні додаватися та відключатися динамічно. Таким чином, стає можливим створювати різні конфігурації окремих вузлів для типових задач. 4. Кросплатформеність. На даний час спостерігається різноманіття апаратних та програмних платформ. Необхідно намагатися підтримувати якомога більше різних платформ з метою збільшення кількості окремих вузлів системи. Особливу увагу слід звернути на мобільні платформи – останнім часом помічається значне зростання інтернет-активності саме з мобільних пристроїв, такі як смартфони та планшети. 5. Автоматичне реконфігурування. При втраті зв’язку з сусідніми вузлами вузол автоматично знаходить нових сусідів, підвищуючи надійність системи. При необхідності використовуються дані з сусідів для створення зв’язків.

На даному етапі дослідження ставиться акцент увагу на децентралізованості. Для досягнення мети пропонується використати наступну організацію: не виділяти окремо клієнтську і серверну частини та використати метод „шпигунських клітинок” – кожний вузол знає про сусідів, але не про всю мережу. У випадку демаскування вузла система залишиться працездатною, будуть виявлені лише найближчі сусіди. Якщо системі потрібно буде подати певну команду, ця команда буде подана лише одному вузлу, який передасть цю команду всім сусідам – а ті, відповідно, поширять її на всю систему. До переваг цього методу відноситься децентралізованість і, як наслідок, висока живучість та можливість управління системою з будь-якого вузла. Також деякі вузли можуть бути локальними командними центрами для інших вузлів, що дозволяє різним сегментам системи виконувати окремі незалежні завдання. До недоліків можна віднести зменшення швидкості реагування системи зі зростанням її розміру за рахунок затримки передачі команд між сусідніми вузлами. На даний час йде вибір мови програмування, середовища розробки, програмних бібліотек для роботи з мережею. Висуваються наступні вимоги: поширеність середовища розробки та наявність документації для неї, кросплатформена мова програмування, документовані бібліотеки для роботи з мережею.

к.в.н. Микусь С.А. (НУОУ)
к.в.н. Розум І.Ю. (НУОУ)

АНАЛІЗ ПРОЦЕСУ ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

В сучасних умовах ведення бойових дій особливо важливе значення має безперервне і якісне управління. Несвоєчасно отримана інформація про противника збільшує тривалість циклу управління і знижує ефективність прийнятих рішень Тільки своєчасна і достовірна інформація є основою для прийняття правильних рішень. Розкриття змісту інформації, що передається, або отримання з телекомунікаційної системи військового призначення дає можливість противнику завдавати випереджувальних ударів і тим самим більш ефективно використовувати свої сили та зброю. Тому боротьба за воєнну перевагу розгортається не тільки навколо створення нових видів зброї та засобів їх доставки, але і за досягнення переваги у системах управління. Основними характерними особливостями телекомунікаційної системи військового призначення є: наявність мети функціонування, процесу управління, великої кількості взаємопов’язаних і спільно функціонуючих елементів, визначеної ієрархічної структури, а також безперервна зміна стану елементів. Основною метою функціонування телекомунікаційної системи військового призначення є забезпечення зв'язком системи управління в будь-яких умовах обстановки. Ефективність її функціонування багато в чому залежить від якості управління її елементами.

Якість функціонування телекомунікаційної системи військового призначення можна характеризувати по будь-якій одній властивості або групі властивостей, але найбільш повно і об'єктивно це можна робити, виходячи з того, в якій мірі телекомунікаційна система військового призначення відповідає своєму цільовому призначенню. Тому для оцінки її якості використовується поняття ефективності функціонування системи [1 – 2]. Ефективність функціонування телекомунікаційної системи військового призначення – це ступінь її відповідності цільовому призначенню у визначених умовах функціонування. Для того, щоб кількісно оцінити ефективність функціонування телекомунікаційної системи військового призначення, необхідно мати чисельну міру, яка характеризувала б ступінь придатності системи до виконання покладених на неї завдань. Таку міру називають показником ефективності функціонування системи.

Телекомунікаційна система військового призначення складається з сукупності взаємопов’язаних та взаємозалежних елементів, яким притаманні визначені властивості, які в тій чи іншій мірі впливають на її ефективність. Величини, які характеризують структуру і властивості телекомунікаційної системи військового призначення і її складових підсистем називають параметрами системи. Параметри телекомунікаційної системи слід розділити на дві групи: зовнішні і внутрішні [3 – 4]. Зовнішні параметри телекомунікаційної системи військового призначення – це параметри, які характеризують систему з точки зору споживача або системи більш високого рівня, тому зовнішні параметри слід вибирати як показники ефективності функціонування телекомунікаційної системи військового призначення. Це зумовлено тим, що саме ці показники характеризують спроможність системи виконувати покладені на неї завдання системою більш високого рівня.

Внутрішні параметри – це параметри системи, які забезпечують виконання зовнішніх параметрів. Телекомунікаційна система військового призначення функціонує в навколишньому середовищі, і тому її ефективність залежить не тільки від параметрів самої системи, але й від умов, у яких вона функціонує. Ці умови характеризуються показниками, які називаються параметрами обстановки.

Таким чином, показники ефективності функціонування телекомунікаційної системи військового призначення залежать від зовнішніх і внутрішніх параметрів системи, а також від параметрів обстановки. Процес оцінки ефективності функціонування телекомунікаційної

системи військового призначення можна розділити на наступні основні етапи [5 – 6]:

постановка задачі;

вибір показника ефективності функціонування телекомунікаційної системи військового призначення ;

вибір зовнішніх та внутрішніх параметрів системи, а також параметрів обстановки, які впливають на показник ефективності функціонування телекомунікаційної системи військового призначення;

побудову моделі телекомунікаційної системи військового призначення;

дослідження моделі і визначення показника ефективності функціонування телекомунікаційної системи військового призначення в залежності від параметрів системи та параметрів обстановки (задача аналізу), або визначення структури і параметрів системи, які забезпечують встановлене значення показника ефективності функціонування при відомих або прогнозованих параметрах обстановки (задача синтезу);

прийняття рішення.

В ході постановки задачі чітко визначається перелік основних факторів, що суттєво впливають на функціонування телекомунікаційної системи військового призначення і дається їх коротка характеристика.

Показник ефективності функціонування необхідно вибрати так, щоб він об'єктивно характеризував телекомунікаційної системи військового призначення і відповідав меті, для досягнення якої призначена система. Для вибору показника ефективності функціонування телекомунікаційну систему військового призначення доцільно розглядати як складову частину (підсистему) системи більш високого рівня. Показник ефективності функціонування повинен бути чутливим (критичним) до змін параметрів системи та обстановки, достатньо простим та наочним, а також узагальнюючим (результуючим).

Для формування узагальненого показника ефективності функціонування телекомунікаційної системи військового призначення найчастіше використовуються такі методи:

дробове представлення узагальненого показника ефективності функціонування;

підсумовування показників з різними ваговими коефіцієнтами;

переведення часткових показників у розряд обмежень.

На практиці найбільш широко використовують метод переведення часткових показників у розряд обмежень, суть якого полягає у тому, що найважливіший показник намагаються максимізувати, а на інші накласти обмеження.

Результати оцінки ефективності функціонування телекомунікаційної системи військового призначення дають змогу відповідним посадовим особам приймати обґрунтовані рішення щодо побудови телекомунікаційної системи військового призначення та внесення необхідних змін в існуючу телекомунікаційну систему з метою забезпечення її функціонування у конкретних умовах оперативно-тактичної обстановки.

ЛІТЕРАТУРА

1. Барабаш Ю. Л. Основи теорії ефективності складних систем / Барабаш Ю. Л.. – К. : НАОУ, 1999. – 85 с.

2. Елементи дослідження складних систем військового призначення / [Загорка О. М., Мосов С. П., Сбітнєв А. І., Стужук П. І.]. – К. : НАОУ, 2005. – 100 с.

3. Венцель Е. С. Исследование операций / Венцель Е. С. – М. : Сов. Радио, 1972 – 135 с.

4. Венцель Е. С. Тория вероятностей / Венцель Е. С. – М. : Физматгиз, 1962 – 564 с.

5. Казачинский В. З., Левитський Г. Е. Математические методы решения военно-специальных задач / В. З. Казачинский, Г. Е. Левитський. – К. : ВА ПВО СВ, 1980. – 291 с.

6. Методологические основы системного решения актуальных задач войск ПВО Сухопутных войск. – К. : ВА ПВО СВ, 1987 – 300 с.

к.т.н. Могилевич Д.І. (ВІТІ НТУУ „КПІ”)
к.в.н. Дружинін С.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Климович О.К. (ВІТІ НТУУ „КПІ”)

МЕТОДИЧНІ ОСНОВИ ОЦІНКИ СИСТЕМИ ЗАХИСТУ АВТОМАТИЗОВАНИХ РОБОЧИХ МІСЦЬ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Актуальність проблеми забезпечення захисту інформаційних ресурсів інформаційно-телекомунікаційної мережі військового призначення, яка підлягає охороні, є очевидною. В умовах сучасного застосування нових зразків озброєння, засобів обчислювальної техніки і зв’язку, створення та використання інформаційних систем, інформація циркулює, накопичується, зберігається і поширюється у електронному вигляді. Крім того, в теперішній час набули широке поширення засоби та методи несанкціонованого та негласного добування інформації [1]. В зв’язку зі стрімким розвитком інформаційно-телекомунікаційних систем удосконалення існуючої системи захисту інформаційних ресурсів повинно здійснюватися на підставі обґрунтованих критеріїв оцінки захищеності даних систем.

Метою дослідження є забезпечення комплексного захисту інформації, що циркулює в локальних обчислювальних мережах інформаційно-телекомунікаційної мережі військового призначення. Наводиться класифікація загроз в сучасних локальних обчислювальних мережах, вибирається необхідна архітектура системи захисту від несанкціонованого доступу, проводиться оцінка доцільності її використання.

На різних етапах використання автоматизованих робочих місць локальних обчислювальних мереж інформаційно-телекомунікаційної мережі військового призначення можуть використовуватися різні методи оцінки їх захищеності. Використання різних методів оцінки захищеності обумовлює вибір базового методу. На основі проведеного аналізу в якості базового методу вибрано дельфійський метод [2, 3], в основі якого існує експертна група, що створена з метою збирання інформації з певних джерел по визначеній проблемі оцінки захищеності автоматизованих робочих місць локальних обчислювальних мереж інформаційно-телекомунікаційної мережі військового призначення.

Таким чином, запропоновані рекомендації щодо можливих напрямків вдосконалення системи захисту інформації за рахунок використання у якості базового одного з експертних методів оцінки захищеності автоматизованих робочих місць локальних обчислювальних мереж інформаційно-телекомунікаційної мережі військового призначення. Зазначені принципові складності, що виникають під час отримання інформації від експертів, сформульовано основні вимоги до віртуальних систем розділення та віртуальних систем захисту інформаційних потоків при проведенні експертного опитування. Основу розглянутого системного підходу по відношенню до оцінки системи захисту автоматизованих робочих місць локальних обчислювальних мереж інформаційно-телекомунікаційної мережі військового призначення складає фрагментація системи на декілька підсистем з подальшим захистом окремих підсистем.

ЛІТЕРАТУРА

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.

2. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – СПб.: „Наука и техника”, 2004.

3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО „ТИД ДС”, 2001. – 688 с.

Морозов К.В. (ВІТІ НТУУ „КПІ”)
Шевченко В.С. (ІТС НТУУ„КПІ”)

ОСНОВНІ ХАРАКТЕРИСТИКИ НЕНАПОЛЕГЛИВОГО ПРОТОКОЛУ CSMA/CD В ДОДАТКОВИХ ПРИПУЩЕННЯХ

При розгляді еталонної моделі взаємодії відкритих систем на окрему увагу заслуговує підрівень управління доступом до мережі, що знаходиться між рівнем управління передачі даних (канальний рівень) та фізичним рівнем. Під методом множинного доступу розуміють сукупність алгоритмів та вирішуючих правил, що являють собою визначену послідовність процедур, які в обов’язковому порядку виконуються кожною абонентською станцією при передачі повідомлень або при відновленні порушень зв’язку. Визначення значень та стандартизація параметрів методу в деякому документі або стандарті дозволяє називати його протоколом. Розрізняють методи випадкового та детермінованого доступу. Серед перших найбільш відомий метод множинного доступу з контролем випромінювання і виявленням конфліктів (МДКВ/ВК). Англомовна назва методу – Carrier Sense Multiple Access /Collision Detection (CSMA/CD). Цей метод заснований на контролі випромінювання в середовищі передачі і усуненні конфліктів, що виникають через спроби одночасного початку передачі більшою кількістю радіостанцій, ніж може обслужити базова станція, шляхом повторення спроб захоплення лінії через випадковий інтервал часу. При його застосуванні усі станції рівноправні по доступу до мережі. Якщо базова станція вільна, то довільна станція, що бажає почати передачу, захоплює ресурс базової станції. Будь-яка інша станція, що бажає почати передачу в деякий момент часу t, якщо виявляє зайнятість базової станції, відкладає передачу до моменту $t + \Delta t$, де Δt – затримка. Розрізняють наполегливий і ненаполегливий МДКВ/ВК у залежності від того, як визначається Δt. Поряд з вищезазначеним традиційним методом інтенсивно розвивається напрямок в теорії демодуляції цифрових сигналів, що отримав назву „статистична теорія розділення цифрових сигналів (СТРЦС)”. Виявилось, що існує клас досить ефективних баєсовських алгоритмів розділяння цифрових сигналів, що взаємно заважають один одному. Припущення про ефективний прийом деякої заданої кількості сигналів з заданою якістю потребує аналізу змін характеристик відомих протоколів доступу. СТРЦС дає обґрунтування можливості успішної демодуляції не тільки однієї, але й двох, трьох та більше заявок.Стосовно впровадження процедур одночасної успішної демодуляції більше ніж одного сигналу визначення характеристик класичних протоколів доступу вже проводилось. Проте, в зазначених публікаціях не було висунуто припущення, що можна обслуговувати тільки пари заявок, що співпадають за тривалістю та скиданням одиночних виявлених заявок в джерело повторних викликів. З метою подальшого визначення характеристик протоколу МДКВ/ВК при обслуговуванні тільки пар заявок що співпадають за тривалістю та скиданням одиночних виявлених заявок в джерело повторних викликів, необхідне відповідне рівняння стаціонарності цього методу. Для чого побудуємо відповідну аналітичну модель та одержимо систему рівнянь, що описує поведінку досліджуваного методу. Нормована пропускна спроможність протоколу випадкового множинного доступу з контролем випромінювання та визначенням конфліктів в додаткових припущеннях про обслуговування тільки пар заявок, що співпадають за тривалістю та скиданням одиночних виявлених заявок в джерело повторних викликів асимптотично наближається до значення „2.0”.

Порівняння параметрів зазначеного протоколу з відомими надасть змогу вибрати ефективний алгоритм множинного доступу що буде застосовуватись при проектуванні та виготовленні перспективних засобів зв’язку.

Некитюк І.М. (ВІТІ НТУУ „КПІ”)

ПОРІВНЯЛЬНИЙ АНАЛІЗ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ MOBILE WIMAX І LTE

Системам радіозв’язку відведена значима роль у функціонуванні систем військового зв’язку в різних ланках управління. Засоби радіозв’язку, що перебувають на озброєнні ЗС України не відповідають сучасним вимогам з погляду бойової готовності, мобільності, пропускної спроможності, стійкості, безпеки та високоманеврених бойових дій.

Зазначені обставини обумовлюють необхідність пошуку шляхів підвищення ефективності військових систем радіозв’язку за допомогою вдосконалення існуючих та доповнення їх новими елементами, побудованими на основі нових принципів організації зв’язку. Одним із перспективних напрямків є впровадження сучасних радіотехнологій, які добре зарекомендували себе на ринку телекомунікацій, наприклад – технології *WiMax*.

Результати практичної експлуатації демонструють, що *WiMax* здатний забезпечувати високу пропускну спроможність і велику область покриття. Пікова швидкість цієї технології, досягає 75 Мбіт/с, а середня – 20 Мбіт/с. Дальність передачі коливається в інтервалі від 5 до 8 км, максимум 80 км (при відповідній антені й максимальній потужності передачі).

Максимальна швидкість передачі даних за допомогою мобільного *WiMax* складає близько 20 Мбіт/с, при цьому на кожен призначений для користувача пристрій виділятиметься канал з пропускною спроможністю від 1 до 5 Мбіт/с. Дистанція якісного з’єднання може досягати 3 км. Позитивна властивість стандарту - широкий діапазон робочих частот, від 2 до 11 ГГц. Метод доступу до середовища передачі - OFDMA, режим передачі - часовий дуплекс(TDD). Ключовою особливістю стандарту є забезпечення якісної, з незначним зниженням пропускної спроможності зв’язком терміналів, що пересуваються зі швидкістю до 60 км/год.

Однією зі значних переваг передових бездротових систем, таких як *WiMAX*, є висока спектральна ефективність. Наприклад, 802.16-2004 (фіксований) забезпечує спектральну ефективність 3,7 (біт/с)/Гц, інші бездротові системи поколінь 3,5-4*G* пропонують приблизно таке ж значення. Така ефективність *WiMAX* багато в чому забезпечується об’єднанням *SOFDMA* з антенними смарт-технологіями.

Системи *Long Term Evolution (LTE)* – це революційне поліпшення мереж 3*G*. *LTE* представляє перехід від систем *CDMA* до систем *OFDMA*, а також повний перехід до *IP*-систем з комутацією пакетів. Для забезпечення зворотної сумісності необхідні дворежимні абонентські пристрої. Тому плавний перехід від систем 3*G* до *LTE* вельми складний.

Основні характеристики *LTE*: технологія *OFDMA* в низхідному каналі і *SC-FDMA* – у висхідному; модуляція – до 64-*QAM*; ширина каналу – до 20 МГц; дуплексування – *TDD* і *FDD*; адаптивні антенні системи; гнучка мережа доступу. У системі *LTE* застосовуються технології і методи, що застосовуються в мобільному *WiMAX*, тому слід очікувати схожої ефективності систем LTE.

Таким чином, мобільний *WiMAX* реліз 1.5 і LTE мають схожі характеристики. В обох на лінії від бази використовується OFDMA з багаторівневою модуляцією і кодуванням. Пікові швидкості практично однакові при однакових кратностях модуляції і швидкостях коригуючого коду. В обох використовується *FDD* і *TDD*. Дуплексована ширина каналу до 20 МГц. В обох використовується MIMO великої кратності і зменшення затримки. Як для мереж LTE, так і для мереж WiMAX необхідний новий спектр, завадозахищеність і енергетична ефективність обох технологій приблизно однакова. Проте, мобільний WiMAX має дворічний виграш за часом виходу на ринок, пропускна здатність і спектральна ефективність мобільного WiMAX має кращі параметри, ніж LTE.

Таким чином, на основі порівняння відомостей щодо результатів спостережень за практичною експлуатацією технологій бездротового доступу, а також з урахуванням можливостей забезпечення завадозахищеності та захисту інформації, можна зробити висновок, що бездротова радіотехнологія *Mobile WIMAX* цілком може бути використана для побудови радіомереж спеціального призначення.

к.т.н. Нестеренко М.М. (ВІТІ НТУУ „КПІ”)
Висоцький Г.В. (ВІТІ НТУУ „КПІ”)
Козак О.А. (ВІТІ НТУУ „КПІ”)

ГІБРИДНІ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ *QOS* В *IP*-МЕРЕЖАХ

Для сучасних інформаційно-телекомунікаційних мереж характерним є необхідність передачі повідомлень різного типу, при цьому існує тенденція збільшення об’ємів передачі мультимедійного трафіка. Одним з основних завдань управління такою мережею є організація ефективної доставки інформації. Тому, забезпечення якості обслуговування (*Quality of Service – QoS*), для всіх видів трафіку, є досить актуальною задачею.

Для забезпечення виконання показників *QoS* в *IP*-мережах використовуються наступні методи: резервування ресурсів (на час з’єднання запитуються і резервуються всі необхідні, для виконання програмних додатків, ресурси); пріоритизація трафіку (поділ трафіку в мережі на класи з пріоритетним порядком обслуговування деяких з них); перемаршрутізація (дозволяє при перевантаженні в мережі перевести трафік на резервний маршрут; саме цим способом забезпечується *QoS* у переважній більшості контролерів *Session Border Controller – SBC*). У сучасних *IP*-мережах перераховані методи найшли використання в: моделі інтегрованого сервісу – *Integrated Service* (*IntServ*); моделі диференційних послуг – *Differentiated Service* (*DiffServ*); гібридній моделі для надання *QoS* з кінця в кінець *IntServ-DiffServ*.

Основною перевагою *IntServ* являється забезпечення гарантованої *QoS,* шляхом класифікації кожного інформаційного потоку даних та відповідно: резервуванням необхідної смуги пропускання в каналі зв’язку, забезпечення мінімальної затримки при передачі пакетів або мінімальний рівень їх втрат в залежності від класу обслуговування. Самий істотний недолік *IntServ* пов’язаний з масштабованістю *Resource ReSerVation Protocol* (*RSVP*), який є основою даної моделі. Особливо це проблематично для високошвидкісних магістральних мереж, оскільки *RSVP* проводить резервування тільки для одного інформаційного потоку та для підтримання актуальності кожного з’єднання необхідно використовувати достатньо великий обсяг сигнальної інформації.

В зв’язку з цим, була запропонована модель *DiffServ*, особливість якої полягає в забезпеченні параметрів *QoS* на підставі вимог різних груп користувачів, диференціюючи трафік за встановленим класом (пріоритетом). Тобто, вхідний трафік ідентифікується, нормалізується, профілюється та реалізується пріоритетне обслуговування в активному обладнанні мережі. Недолік даної моделі полягає в тому, що в випадку перевантажень в мережі затримки передачі можуть мати досить велике значення, а пакети з меншим пріоритетом будіть просто відкинуті.

Найбільш перспективною на сьогодні є модель *Int-DiffServ* завдяки тому, що використовує кращі сторони представлених моделей на різних ділянках мережі. Домінуючим компонентом *Int-DiffServ* є технологія мультипротокольної комутації по мітках (*Multiprotocol Label Switching – MPLS*), яка призначена для зменшення часу передачі *IP*-пакетів за рахунок комутації останніх на основі добавлених міток. Однак, *MPLS* стає технологією з контролем забезпечення *QoS* тільки при використанні *RSVP-TE*.

В свою чергу, *RSVP-TE* не лише резервує необхідний рівень, якості обслуговування на всіх ділянках встановленого маршруту, але й має функцію динамічного переведення на резервний маршрут в випадку перевантажень або виходу з ладу елементів мережі.

Однак, при використанні запропонованих мережевих технологій виникає ряд питань стосовно їх переваг в порівнянні з традиційною *IP*-маршрутизацією. Тому, для вирішення задачі оцінки величини ефекту застосування *MPLS* необхідно розробити адекватні математичні моделі, які будуть визначати апаратні та програмні витрати активного обладнання в залежності від розмірності мережі та протоколів передачі та сигналізації.

Ольшанський В.В. (ВІТІ НТУУ „КПІ”)

ОЦІНКА ЗАВАДОЗАХИЩЕНОСТІ СИГНАЛІВ З ППРЧ З ФАЗОВОЮ МАНІПУЛЯЦІЄЮ ПРИ ВПЛИВІ НАВМИСНИХ ЗАВАД

Важливе місце в забезпеченні переваги в управлінні військами та зброєю в сучасних операціях (бойових діях) посідає радіоелектронна боротьба. В умовах сучасного бою ефір стає такою ж ареною боротьби, як суша, море та повітряний простір. Постійне вдосконалення засобів радіорозвідки та радіозавад, впровадження автоматизованих комплексів радіоелектронного подавлення призвело за останні роки до істотного підвищення можливостей по радіоподавленню засобів радіозв’язку.

Одним з ефективних методів підвищення завадозахищеності засобів радіозв’язку (ЗРЗ) при впливі навмисних завад є застосування псевдовипадкового перестроювання робочої частоти (ППРЧ). У системах з ППРЧ розширення спектра в межах заданої смуги частот здійснюється за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, який невідомий постановнику завад.

Для подавлення ЗРЗ з ППРЧ можуть застосовуватися різні види організованих завад. Негативний вплив навмисних завад в системах і засобах радіозв’язку з ППРЧ може бути значно послаблений за рахунок застосування адаптивних алгоритмів формування та обробки сигналів, які дозволяють підвищити енергетичну ефективність засобів радіозв’язку. При цьому, важливим є завдання оцінки рівня спотворення сигналів з ППРЧ в умовах навмисних завад. В роботі проведено дослідження впливу шумових завад, полігармонійної (багатотональної) завади та завади у відповідь на завадозахищеність засобів радіозв’язку з ППРЧ при передачі сигналів методом фазової маніпуляції (ФМ).

При оцінці завадозахищеності засобів радіозв’язку в умовах впливу навмисних завад за показник кількісної міри оцінки була прийнята середня імовірність помилки на біт інформації. Побудовано графіки залежностей середньої імовірності помилки на біт від відношення сигнал/завада для різних видів навмисних завад.

На основі проведеної оцінки завадозахищеності сигналів, які передаються засобами радіозв’язку з псевдовипадковим перестроюванням робочих частот в умовах впливу найгірших завад можна зробити такі висновки.

1. Шумова завада, яка має оптимальне значення смуги частот, що подавлюється, з погляду забезпечення завадозахищеності є найгіршою. Однак з метою оптимізації поточної ширини спектра завади в частині смуги і потужності завади в складі системи радіоелектронного подавлення необхідно мати станцію радіотехнічної розвідки для вимірювання параметрів сигналів засобу радіозв’язку, який подавлюється. Завадозахищеність засобу радіозв’язку може бути істотно підвищена за рахунок збільшення коефіцієнта розширення спектра сигналу.

2. Ефективність впливу на засіб радіозв’язку з ППРЧ широкосмугової шумової завади значно уступає ефективності найгіршої шумової завади в частині смуги.

3. Найгірші багатотональні завади ефективніше найгірших шумових завад у частині смуги. Але технічна реалізація та ефективність найгірших багатотональних завад залежить від апріорної інформації про характеристики сигналів засобів радіозв’язку у постановника завад. Тому створення найгірших шумових завад у частині смуги є більш реальним на практиці.

4. Вплив найгірших шумових завад у відповідь призводить до заміни експонентної залежності середньої імовірності помилки на біт від відношення сигнал/завада на лінійну і більше не впливає на зниження завадозахищеності ЗРЗ.

Онисько В. В. (в/ч А0653)
к.в.н. Вертегел С.Г. (в/ч А1906)
Сірик А.О. (в/ч А1906)

НАПРЯМИ РОЗВИТКУ СУЧАСНИХ АВТОМАТИЗОВАНИХ СИСТЕМ РОЗВІДКИ ЗБРОЙНИХ СИЛ

Головною метою розвитку автоматизованих систем воєнної (військової) розвідки провідних країн світу є забезпечення відповідності їх оперативно-технічних характеристик вимогам до сучасних систем управління розвідки збройних сил в мирний та у воєнний час. А саме, інтеграція всіх сил та засобів в єдиний інформаційний простір, що дозволяє суттєво підвищити ефективність бойового застосування і відповідно збільшити бойові можливості, як угруповання військ так і в цілому всіх збройних сил.

Виходячи з цього основні зусилля повинні бути зосереджені на вирішенні завдань щодо підтримки існуючих систем спеціального зв'язку і автоматизації у визначених ступенях бойової готовності, їх постійна модернізація та поступовий розвиток.

Загальна тенденція розвитку систем управління розвідки полягає у переході до більш високого рівня автоматизації інформаційно-аналітичної діяльності та телекомунікаційного обладнання.

Основними напрямами розвитку сучасних автоматизованих систем воєнної розвідки є:

1. Підвищення ефективності оперативної та тактичної розвідки за рахунок автоматизації процесів добування, оборобки та доведення інформації до споживачів у реальному (близькому до реального) масштабі часу для прийняття управлінських рішень, оцінки і випереджувального моніторингу воєнно–політичної (воєнно-стратегічної) обстановки у визначених зонах відповідальності для виявлення загроз національній безпеці держави.

2. Досягнення інформаційної переваги за допомогою об'єднання органів управління збройних сил і розвідки у єдину інформаційну мережу, архітектура якої повинна створювати умови для накопичення значних інформаційних та геоінформаційних ресурсів.

3. Забезпечення стійкого та безперервного управління черговими силами та засобами розвідки у мирний час та в ході проведення операцій (бойових, спеціальних дій) у разі вогневого та радіоелектронного впливу при втраті до 50 % наявних радіоелектронних засобів, центрів (пунктів) управління розвідки.

4. Доведення загального рівня автоматизації розвідувальної та інформаційно–аналітичної діяльності органів управління до 70 % від кількості функцій, які ними виконуються.

5. Досягнення вищого рівня взаємодії між різними видами військової розвідки у збройних силах.

6. Впровадження новітніх інформаційних технологій у діяльність органів розвідки, таких як супутникові радіонавігаційні системи та засоби космічного зв'язку до батальйону, роти і взводу включно.

7. Вдосконалення методів комплексного захисту інформації, яка циркулює в системі розвідки.

Таким чином, для реалізації напрямів розвитку автоматизованих систем воєнної розвідки, необхідно впровадження єдиного механізму створення концепції та програми автоматизованої системи воєнної розвідки в складі Єдиної автоматизованої системи управління Збройними Силами України, яка б відповідала всім вимогам сьогодення та тенденціям розвитку збройної боротьби в світі.

Осиченко О.Б. (ВІТІ НТУУ „КПІ”)
Головко О.О. (ВІТІ НТУУ „КПІ”)
Юрченко О.В. (ВІТІ НТУУ „КПІ”)

МЕТОД ФІЛЬТРАЦІЇ ПОТОКУ ЗАПИТІВ ДЛЯ ЗАХИСТУ WEB-СЕРВЕРА

Сьогодні *web*-сервери функціонують на основі динамічного методу формування *web*-сторінок (ДМФС), що на практиці призводить до безлічі реалізацій спеціально організованих комп’ютерних атак, спрямованих на підміну інформації на *web*-сторінках. У зв’язку з цим, актуальною є задача забезпечення безпечного функціонування *web*-серверів в умовах комп’ютерних атак підміни контенту і практичної реалізації відповідних технічних рішень.

Аналіз джерел показав, що для реалізації процедури виявлення комп’ютерных атак найчастіше використовується сигнатурний метод, але його ефективність на пряму пов’язана з обов’язковою підтримкою в актуальному стані бази цих сигнатур атак. Процес фільтрації запитів до *web*-серверів з ДМФС істотно ускладнюється, у зв’язку із складністю виявлення атак сигнатурним методом модифікованих порушником комбінацій значень параметрів доступу. Успіху реалізації атаки в цьому випадку сприяє неможливість повного опису варіантів комп’ютерної атаки сигнатурним методом.

Для підвищення захищеності *web*-серверів з динамічним формуванням сторінок від комп’ютерних атак підміни контенту потрібна методика фільтрації потоку запитів, що враховує можливі зміни в структурі запитів.

Враховуючи, що користувачі не обмежені у формуванні значень змінних доступу запитів, і з метою збереження функціональності *web*-ресурса необхідно розробити процедуру оцінки міри небезпеки запиту, що розпізнається *web*-сервером як небезпечний.

Із цією метою введемо відповідні процедури, засновані на математичному апараті теорії нечітких множин.

Нехай, задана початкова множина безпечних запитів до певного ресурсу *web*-сервера $Z=\left\{z_i, i=\overline{1,m}\right\}$, і множина значень його змінних доступу $K=\left\{k_i, i=\overline{1,n}\right\}$, за якими повинні оцінюватись запити. При цьому розглядаються однотипні запити, коли у кожному запиті $z\in Z$ присутні усі змінні доступу із множини $k\in K$. Для кожного із значень змінних доступу $k\in K$ та відоме нечітке відношення переваги Ψ_k на множині коректних запитів Z, тобто відома функція приналежності $\mu_\Psi\left(z_i, z_j, k\right)$, значення якої розуміється як ступінь переваги запиту z_i перед запитом z_j за змінною доступу k.

Елементи безлічі K різні за важливістю, тобто на безлічі значень змінних доступу задані відношення, що характеризуються величинами $\lambda(k_1,k_2)$, які розуміються як ступінь, з яким значення k_1 вважається не менш важливим, ніж значення k_2.

Завдання полягає у тому, що за наявною інформацією про значення змінних доступу запиту, що поступив, здійснити оцінку міри його небезпеки на основі початкової безлічі безпечних запитів Z.

Рішення поставленої задачі пропонується шукати, спираючись на поняття нечіткої множини недомінованих альтернатив, функція приналежності якого визначається наступним виразом:

$$\mu_\Psi^{нд}(z)=\inf_{z_i\in Z}[1-\max\{0,\mu_\Psi(z_i,z)-\mu_\Psi(z,z_i\}]=1-\sup_{z_i\in Z}\max\{0,\mu_\Psi(z_i,z)-\mu(z,z_i)\} \qquad (1)$$

де $\mu_\Psi(z,z_i)$ – функція приналежності нечіткого відношення переваги на множині Z.

Значення $\mu_\Psi^{нд}(z)$ є степенем, з яким запит z не домінується жодним із запитів множини Z. Іншими словами, це степінь, з яким запит z можна вважати безпечним з точки зору близькості значень його змінних доступу до запиту з безпечної множини.

Для знаходження множини недомінованих запитів за множиною значень змінних доступу K розглянемо нечітку множину (Z,μ_{Θ_1}), де μ_{Θ_1} – функція приналежності перетину Θ_1 вихідних відношень Ψ_k. Підмножина недомінованих запитів у множині (Z,μ_{Θ_1}) співпадає з множиною недомінованих запитів для початкового набору функцій $\mu_\Psi(z,z_i)$. При цьому перетину відношень Ψ_k, заданих на множині значень змінних доступу K, відповідає функція приналежності μ_{Θ_1}:

$$\mu_{\Theta_1}(z,z_i)=\min\{\mu_\Psi(z,z_i,k_1),\mu_\Psi(z,z_i,k_n)\} \tag{2}$$

Шляхом підстановки формули (1) у формулу (2), отримуємо вираз для функції приналежності нечіткої підмножини недомінованих запитів на множині (Z,μ_{Θ_1}):

$$\mu^{нд}_{\Theta_1}(z)=1-\sup_{z_i\in Z}\max\{0,\mu_{\Theta_1}(z_i,z)-\mu_{\Theta_1}(z,z_i)\} \tag{3}$$

Проте вираз (2) не враховує відмінності змінних доступу по мірі їх важливості, що задаються величинами $\lambda(k_1,k_2)$. Тому необхідно ввести звертання відношень виду:

$$\mu_{\Theta_2}=(z,z_i)=\sum_{j=1}^{n}\delta_{\lambda j}\mu_\Psi(z,z_i,k_j),\ \sum_{j=1}^{n}\delta_{\lambda j},\delta_{\lambda j}\ge 0,\ j=\overline{1,n} \tag{4}$$

де коефіцієнти $\delta_{\lambda j}$ мають сенс коефіцієнтів важливості і можуть бути визначені на основі заданої множини відношень за формулою:

$$\delta_{\lambda j}=\lim_{s\to\infty}\delta^{(s)}_{\lambda j},\quad \delta^{(s)}_{\lambda j}=\frac{\sum_{i=1}^{n}\lambda^{(s)}(k_j,k_i)}{\sum_{j=1}^{n}\sum_{i=1}^{n}\lambda^{(s)}(k_j,k_i)} \tag{5}$$

де $\delta^{(s)}_{\lambda j}$ відносна сила s-го порядку признака $k_j;\lambda^{(s)}(k_j,k_i)$– ji-й елемент матриці λ піднесений до степеня s.

Відповідно до формули (1), функція приналежності нечіткої підмножини недомінованих запитів на множині (Z,μ_{Θ_2}) визначається виразом:

$$\mu^{нд}_{\Theta_2}(z)=1-\sup_{z_i\in Z}\max\{0,\mu_{\Theta_2}(z_i,z)-\mu_{\Theta_2}(z,z_i)\} \tag{6}$$

Результуючу безліч недомінованих запитів знаходимо як перетин множин $\mu^{нд}_{\Theta_1}$ і $\mu^{нд}_{\Theta_2}$, функція приналежності якої $\mu^{нд}(z)$ визначається виразом:

$$\mu^{нд}(z)=\min\{\mu^{нд}_{\Theta_1}(z),\mu^{нд}_{\Theta_2}(z)\} \tag{7}$$

Для прийняття введемо відповідні критерії, якщо допускається вибір максимально безпечного запиту:

$$Z^{нд}_i=\{z\mid z\in Z,\mu^{нд}_i(z)=\sup_{z_1\in Z}\mu^{нд}(z_i)\} \tag{8}$$

і якщо допускається вибір запиту з мірою безпеки не нижче встановленого H:

$$Z^{нд}_i=\{z\mid z\in Z,\mu^{нд}_i(z)>H\} \tag{9}$$

Рішення задачі виявлення комп'ютерних атак підміни контенту на *web*-сервери із динамічним формуванням сторінок дозволяє підвищити захищеність їх функціонування. У розрахунках, заснованих на застосуванні математичного апарату теорії нечітких множин, враховується виконання вимог по її захищеності.

Наукова новизна роботи полягає в уявленні процедури фільтрації у взаємозв'язку із вимогами по її рівню, а також із синтаксисом мови і структурою *HTTP*-запитів; у інваріантності запропонованої моделі до програмно-апаратного забезпечення *web*-сервера.

Практична значущість визначається можливістю впровадження розробленого методу до комплексної методики захисту діючих програмно-апаратних комплексів.

Охріменко В.О.(ІСЗЗІ НТУУ „КПІ”)

ЕЛЕКТРОТЕХНІЧНІ АНАЛОГІЇ В МОДЕЛЮВАННІ ПРОЦЕСІВ НАНЕСЕННЯ ЗБИТКУ ВІД ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Останнім часом питання управління інформаційною безпекою набувають все більшої актуальності. Важливою в даних питаннях є задача побудови строгих і адекватних моделей процесів інформаційної безпеки, частково – складання ефективних математичних описів процесів нанесення збитку для мінімізації останнього.

Аналіз сутностей процесів управління інформаційною безпекою та процесів, що протікають в електричних ланцюгах, з наступними висновками про їх аналогії та можливі загальні методи їх дослідження викладено в [1]. У даній публікації особливо акцентовано увагу на необхідність розглядати дані процеси в часі. Електротехнічні аналогії процесів, що існують в системі управління інформаційною безпекою, приведені в [2]. До процесів оптимізація котрих дозволить підвищити ефективність систем управління інформаційною безпекою, віднесені і процеси нанесення збитку. Також відомі ідеї доповіді Булдижова В.І. „Электротехнические аналогии при управлении информационной безопасностью организаций” [3].

Розглянемо сутність процесів нанесення збитку в термінах словника ISO GUIDE 73:2009. RISK MANAGEMENT – VOCABULARY [4].

Відповідно [4] ризик (Risk) породжується джерелом ризику (Risk source), – деякою сутністю, що має специфічний внутрішній потенціал. Електротехнічним аналогом потенціалу джерела ризику приймемо джерело (генератор) напруги із законом зміни вихідної напруги в часі $u(t)$.

Оскільки актив має внутрішню властивість – вразливість (Vulnerability), внаслідок якого він є чутливим до впливу джерела ризику, то її електротехнічним аналогом, є не що інше, як провідність Y. Як наслідок, зворотна провідності величина R, – опір активу до впливу джерела ризику.

Виникнення або зміна специфічного набору обставин називається подією (Event), а термін „інцидент” є однією з його інтерпретацій. Результатом події є її як позитивні так і негативні наслідки (Consequense).

Аналогом кількісної характеристики властивості інформаційного активу (конфіденційність, цілісність, доступність) представлено заряд $q_P(t)$ елемента ємності, де $P = \{К, Ц, Д\}$, – кортеж властивостей активу. Наслідком впливу на інформаційний актив є зміна кількісних характеристик властивостей активу, аналогічно тому, як змінюється заряд на пластинах конденсатора під впливом прикладеного до його пластин напруги. Дана аналогія також застосовна і для опису інших характеристик і/або властивостей активу, котрі виражені кількісно і підлягають дослідженню.

Зміна кількісної характеристики властивості активу за нескінченно малий проміжок часу $dq_P(t)/dt$ є швидкість зміни властивості активу. Електротехнічним аналогом швидкості впливу на актив є електричний струм $i_P(t)$, миттєве значення якого визначається аналогічно: зміною заряду за нескінченно малий проміжок часу. В даному випадку $q_P(t)$ – функція миттєвого значення кількісної характеристики властивості активу.

Проводячи аналогію з законом Ома, можна сказати, що: швидкість зміни кількісної характеристики властивості активу $i_P(t)$ в елементарній системі „вплив джерела ризику – актив” прямо пропорційна впливу потенціалу джерела ризику $u(t)$ і обернено пропорційно опору активу R до впливу даного джерела ризику .

Виходячи з викладеного вище, величина зміни кількісної характеристики властивості активу:

$$\Delta q_P(t) = \int_{t_0}^{t} i_P(t)dt,$$

де $\Delta q_P(t)$ – функція величини змін кількісної характеристики властивостей активу;

t_0 – момент початку впливу на кількісну характеристику.

Тоді функція миттєвого значення кількісної характеристики властивості активу:

$$q_P(t) = q_P(t_0) + \Delta q_P(t)$$

$$q_P(t) = q_P(t_0) + \int_{t_0}^{t} i_P(t)dt \ .$$

Цілком імовірно, що величина збитку на момент часу t є функція $\Delta Q(t)$:

$$\Delta Q(t) = \Delta q_P(t) \times F(t),$$

де $F(t)$ – деяка функція.

Цілком природно, що для того, щоб закон Ома був дійсний для опису процесів нанесення збитку, необхідно подальше дослідження вище викладених аналогій і створення адекватної моделі.

Окремою науковою задачею, пов'язаною зі створенням моделей джерел ризику [2] в чутливих до часу випадках, є дослідження функції $u(t)$ – потенціалу джерела ризику. Також, практичний інтерес представляє дослідження функції $F(t)$. Це робить можливим моделювати процес нанесення збитку в реальному часі.

Таким чином, наведені аналогії процесів впливу електричного струму і нанесення збитку. В подальшому використання наведених аналогій в поєднанні з загальновідомими методами дослідження електричних ланцюгів може допомогти у створенні ефективних математичних описів процесів нанесення збитку.

ЛІТЕРАТУРА

1. Богданов А.М., Мохор В.В. О моделировании систем управления информационной безопасностью на основе процессного подхода / А.М. Богданов, В.В. Мохор // Модеювання та інформаційні технології: зб. наук. праць / ІПМЕ ім. Г.Є.Пухова НАН України. – Київ, 2011. – Вип. 59. – С. 83 – 85.

2. Охрименко В.А., Зинченко Я.В. Моделирование систем управления информационной безопасностью с применением электротехнических аналогий / В.А. Охрименко, Я.В. Зинченко // Спеціальні телекомунікаційні системи та захист інформації / ІСЗЗІ НТУУ „КПІ". – Київ, 2012. – Вип. 22. (в друку).

3. Электротехнические аналогии при управлении информационной безопасностью организаций: тезисы ежег. XXX наук.-техн. конф. молодых ученых и специалистов, 12 – 13 янв. 2011. – К.: НАН Украины, ИПМЭ им. Г. Е. Пухова, 2011. – С. 18. – 70 с.

4. Мохор В.В., Богданов А.М. Изложение руководства „ISO Guide 73:2009. Risk Management – Vocabulary" на русском языке / В.В. Мохор, А.М. Богданов // Das Management. – 2001. – Вип. 2. – С. 04 – 06.

к.т.н. Павлюк В. В.(ЖВІНАУ)
Ставісюк Р. Л. (ЖВІНАУ)

АНАЛІЗ ПЕРСПЕКТИВ РОЗВИТКУ ШИРОКОСМУГОВИХ АНТЕННИХ СИСТЕМ НАДВИСОКОЧАСТОТНОГО ДІАПАЗОНУ

В даний час надвисокочастотний діапазон знаходить все більш інтенсивного застосування в системах широкосмугового зв'язку, радіолокації, радіонавігації, телеметрії та радіоелектронної протидії.

До числа беззаперечних переваг застосування діапазону міліметрових хвиль відносяться: збільшення пропускної здатності систем, значне підсилення антен при їх малій апертурі, збільшення завадозахищеності каналу зв'язку та зменшення геометричних розмірів антен.

Прикладами сучасних засобів надвисокочастотного діапазону є бортова радіолокаційна станція літаків F-16 Fighting Falcon, що працює в діапазоні частот від 8 до 12,5 ГГц (проходить тестування для розширення до 26 ГГц), цифрова система радіорелейного зв'язку „МЕРИДІАН", що використовує робочі частоти 4, 5, 6, 7, 8,11, 13, 15, 18, 23, 36 ГГц, радіолокаційна станція супроводження і підсвітки цілі для зенітних ракет RIM-24 „Тартар" і RIM-66 „Стандарт" SM-1, що працює в діапазонах від 4 до 6 ГГц та від 8 до 10 ГГц, трьох координатна радіолокаційна станція Фрегат-М2ЭМ (Fregat-M2EM), що працює в Е діапазоні частот.

Згідно з Постановою Кабінету Міністрів України „Про затвердження національної смуги частот України" передбачене використання діапазону частот від 29,9 до 32,3 ГГц для супутникової служби дослідження Землі, частотного діапазону від 32,3 до 37,5 ГГц для радіолокаційних служб космічних досліджень, частотного діапазону від 41 до 48,2 ГГц для радіомовної супутникової, аматорської супутникової, радіонавігаційної супутникової служб. В загальному планується використання діапазону частот до 155 ГГц.

Розробка радіотехнічних засобів, робочий діапазон частот яких визначається десятками гігагерц передбачає створення антенно-фідерної системи, яка є невід'ємною частиною радіоелектронних комплексів. Антени сучасних радіотехнічних комплексів, як найбільш складна їх частина та система, що повинна виконувати ряд різнопланових завдань, визначають ефективність радіотехнічних засобів вцілому. До переліку вимог, які висуваються до антенних систем надвисокочастотного діапазону відносяться форма діаграми спрямованості, масогабаритні характеристики, складність виготовлення, мобільність антени, поляризаційні характеристики та ін.. При переході до діапазону надвисоких частот з'являється потреба в передачі широкосмугових сигналів. Це в свою чергу висуває до антенної системи надвисокочастотного діапазону вимогу щодо широкосмуговості.

Аналіз показує, що подальший розвиток радіоелектронної апаратури і використання області більш високих частот потребує створення антенної системи, яка б задовольняла поставленим вимогам.

Перспективним напрямком у створенні широкосмугових антен надвисокочастотного діапазону є розробка антен на базі жолобкового хвилеводу. Даний тип хвилеводу із складним поперечним перерізом є технологічно простим та дешевим, а також має ряд переваг над існуючими антенами надвисокочостотного діапазону. Його направляючі властивості визначаються особистими режимами роботи.

Особливість конструкції жолобкового хвилеводу, яка забезпечує самофільтрацію паразитних вищих типів хвиль, дає можливість вирішити ряд основних вище згаданих недоліків.

Панченко І. В. (ВІТІ НТУУ„КПІ”)
Малих В. В. (ВІТІ НТУУ „КПІ”)
Бондаренко Л. О. (ВІТІ НТУУ„КПІ”)

ПЕРСПЕКТИВИ РОЗВИТКУ МЕРЕЖ КОРОТКОХВИЛЬОВОГО РАДІОЗВ’ЯЗКУ

Реалізація бойових можливостей ЗС України істотно залежить від якісних показників системи управління та її матеріальної основи – системи зв’язку. Бойова готовність, ймовірнісно-часові та оперативно-технічні характеристики систем управління і зв’язку є такими ж важливими показниками, як кількість і якість засобів збройної боротьби.

З метою підвищення ефективності функціонування компонентів систем військового зв’язку планується широке використання в їх складі засобів і систем радіозв’язку КХ діапазону, що дозволить розв’язати існуючі проблеми по безперервності та стійкості бойового управління вже найближчим часом і відкриває подальші перспективи на поліпшення оперативно-технічних характеристик системи військового зв’язку в цілому.

Ряд недоліків радіозв’язку в КХ діапазоні об’єктивно сприяли більш швидкому розвитку кабельних (в тому числі і волоконно-оптичних), радіорелейних, тропосферних і супутникових систем зв’язку. [1]. Найбільш важливими особливостями поширення коротких хвиль в іоносфері, які накладають обмеження на використання високошвидкісних і широкосмугових систем КХ радіозв’язку є багатопроменеве поширення, частотні й тимчасові варіації характеристик радіолінії. Вплив цих особливостей іоносферної радіолінії на сигнали систем КХ радіозв’язку залежить від протяжності та географічного розташування радіотрас, часу доби, пори року, сонячної та магнітної активності. До переваг КХ радіозв’язку слід віднести оперативність встановлення прямого зв’язку на великі відстані, простоту організації радіозв’язку з рухомими об’єктами, можливість забезпечення зв’язку через великі важкодоступні простори (зони підвищеного зараження, важкопрохідні водні й гірські райони, лісові масиви тощо), високу мобільність засобів КХ радіозв’язку, досить просте відновлення зв’язку в разі його порушення (у разі впливу як випадкових, так і навмисних перешкод) і низьку вартість одного каналу на кілометр дальності зв’язку. [2]

Одночасно КХ радіозв’язку притаманні такі недоліки, як різке згасання сигналу на трасі радіозв’язку, різний характер завмирання сигналу, обмежена ємність використовуваного діапазону частот. Якість зв’язку істотно залежить також від часу доби, року і стану іоносфери. Крім того, системи КХ радіозв’язку характеризуються чутливістю до випадкових і навмисних перешкод, а також до висотних ядерних вибухів, малим відношенням швидкості передачі до займаної смуги частот, значною доступністю для засобів радіорозвідки і одночасно малим відношенням сигнал-завада в точці прийому.

Шляхи усунення цих недоліків і визначають ті напрямки, по яких у даний час ведеться пошук заходів щодо підвищення ефективності КХ радіозв’язку. [3]

У зарубіжній пресі відзначається, що відродження інтересу до КХ зв’язку в даний час пояснюється ще й встановленою в ході досліджень вразливістю у воєнний час супутникових систем зв’язку, що отримали в 80-і роки досить широке поширення.

Еволюція систем КХ радіозв’язку представлена на рис.1

Для зручності аналізу шляхів удосконалення ефективності КХ радіозв’язку можна виділити напрямки:

– організаційно-технічні;

– апаратурно-технічні.

До організаційно-технічних заходів можна віднести:

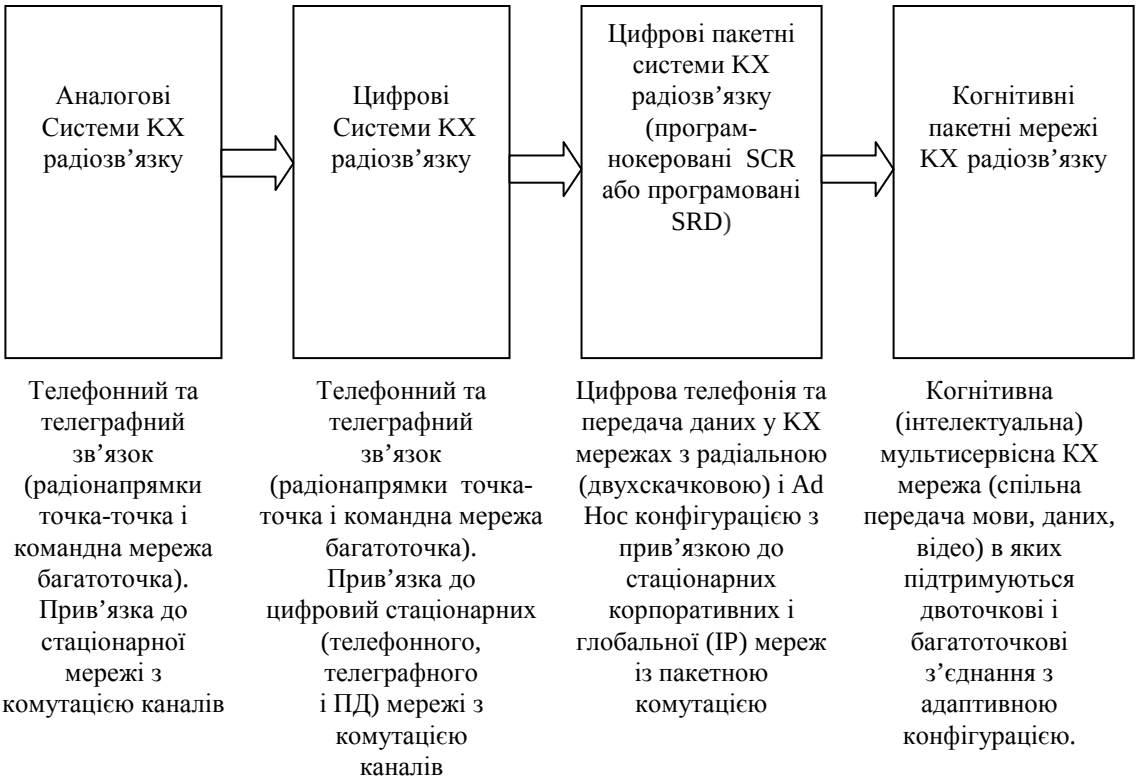
– організацію ретрансляції на трасах середньої та великої протяжності;

– побудову КХ мереж із використанням „базових основ” (сукупності декількох базових радіоцентрів, пов’язаних між собою кільцевою схемою, через які забезпечується зв’язок між кореспондентами даної мережі);

– організацію КХ радіозв’язку з ретранслятором винесеним із зони;

– організація лавинного КХ радіозв’язку;

– організацію рознесеного прийому.



Мал. 1 Еволюція систем КХ радіозв’язку

До апаратурно-технічних заходів можна віднести:

– перехід до цифрового зв’язку в КХ діапазоні;

– перехід до когнітивних (інтелектуальних) мультисервісних КХ мереж;

– використання методів адаптації;

– застосування КХ антен із керованою діаграмою спрямованості;

– упровадження прогнозування в процесі ведення КХ радіозв’язку;

– удосконалення ергономіки і надійності засобів КХ радіозв’язку;

– підвищення технічної надійності апаратури.

Проведення досліджень у галузі КХ радіозв’язку є доцільними та актуальними у напрямках створення програмованих засобів, здатних адаптуватися до засобів радіозв’язку Держав-партнерів та забезпечувати стійке управління військами та зброєю у складних завадових обставинах, оскільки технічні засоби радіозв’язку складають матеріальну основу управління військами і зброєю у всіх видах Збройних Сил України.

Проведений аналіз переконливо свідчить про наявність великого числа напрямків досліджень у підвищенні ефективності КХ радіозв’язку.

ЛІТЕРАТУРА

1. Иностранная техника и экономика средств связи. Обзоры, 1996, вып. 1.

2. Комарович В. Ф., Ромвненко В. Г. КВ радиосвязь. Состояние и направления развития. УДК 621.396.7.

3. Мишин В.Е. Проблемы использования КВ диапазона при построении радиосетей.

Пашков В.Ю. (ВІТІ НТУУ „КПІ”)
к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ”)

ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО ОБМІНУ ІНФОРМАЦІЙНИМИ ПОВІДОМЛЕННЯМИ В КЛІЄНТ-СЕРВЕРНИХ АРХІТЕКТУРАХ НА ОСНОВІ WEB-СЕРВІСІВ

Порушення безпеки інформаційної системи спеціального призначення розглядається як інцидент безпеки інформаційно-аналітичного процесу управління мережами через втрату конфіденційності, цілісності, доступності інформаційних ресурсів. Саме тому актуальним є підхід до вирішення проблеми шифрування інформації даних, які передаються по мережі спеціального призначення, для забезпечення конфіденційності інформації.

Взаємна інтеграція цільових завдань різних організацій і установ, що відбувається зараз у всьому світі, неминуче тягне за собою появу технологій і стандартів інтеграції обслуговуючих їх додатків та інформаційних систем спеціального призначення. Найбільш популярною технологією такої інтеграції в даний час слід визнати технологію застосування *WEB*-сервісів. *Web*-клієнт та *Web*-сервіс в концепції *ASP.NET* взаємодіють на логічному рівні за протоколом *HTTP* з укладеними в нього принципами *SOAP*.

Аналіз технологічних підходів, забезпечення конфіденційності інформаційних повідомлень, які передаються за протоколом *SOAP* у відкритому вигляді, обумовив звернутися до методів експертного оцінювання з метою обгрунтування вибору раціональної моделі криптографічного захисту даних для інтеграції її в алгоритм роботи модулю інтерпритації *SOAP*-повідомлень клієнт-серверних архітектур на основі *WEB*-сервісів.

Результати розрахункового прикладу, де для визначення коефіцієнтів відносної важливості був використаний метод Ротштейна і 9-ти бальна шкала Сааті, а для встановлення найкращої альтернативи − метод аналізу ієрархій, свідчать, що найбільш придатною моделлю організації криптозахисту *SOAP*-повідомлення виступає симетричний алгоритм блочного шифрування *AES* (*Advanced Encryption Standard*).

Розглянуті основні режими роботи алгоритмів блочного шифрування: *ECB*, *CBC*, *CFB*, *OFB*, *CTR*. Для вибору режиму роботи алгоритму *AES*, який найбільш відповідає для паралельної реалізації, був запропонований перелік критеріїв, таких як: можливість розпаралелювання процедури шифрування та розшифрування, простота реалізації режиму, можливість попередніх обрахувань. Відповідно до проведеного аналізу для розробки паралельної версії алгоритму пропонується режим *CTR*. Операції шифрування та розшифрування можуть виконуватися паралельно. Внаслідок того, що операція додавання по модулю два є симетричною, процес шифрування й розшифрування виглядає однаково. Алгоритм запропонованого режиму шифрування та розшифрування *CTR* наведений нижче:

$c_j := E_K(t_j) \oplus x_j$ for all $j>0$;

$x_j := D_K(t_j) \oplus c_j$ for all $j>0$,

де t_i – лічильник;

c_j – зашифрований текст;

x_j – розшифрований текст;

$E_K(t_j)$ – функція шифрування;

$D_K(t_j)$ – функція розшифрування.

Запропонований підхід в організації конфіденційності інформації в *SOAP*-повідомленнях на основі алгоритму блочного шифрування *AES* відрізняється від існуючих технологічних рішень можливостю паралельного виконання деяких операцій та спрямуванням процесу шифрування/розшифрування не усієї структури *SOAP*-повідомлення, а тільки сегменту цієї структури, що містить корисні (не службові) дані. Це забезпечить суттєве скорочення показнику часу виконання операцій криптозахисту *SOAP*-повідомлення.

д.т.н. Певцов Г. В.(ХУПС)
к.т.н. Яцуценко А. Я. (ХУПС)
к.т.н. Карлов Д. В. (ХУПС)
Трофименко Ю. В.(ХУПС)
Борцова М. В.(ХАІ)

ОСНОВИ ЕНЕРГЕТИЧНОГО ВИЯВЛЕННЯ І ОЦІНЮВАННЯ ПАРАМЕТРІВ РАДІОСИГНАЛІВ

В сучасних умовах проведення швидкоплинних повітряно-наземних операцій з використанням останніх досягнень інформаційних технологій, використанням інтегрованих систем зброї з широким застосуванням орбітальних систем різного призначення постає актуальне питання отримання повної вірогідної інформації про плинний повітряно-наземний стан угруповання противника за декількома високоточними вимірами з метою швидкого розпізнавання його задуму на ведення бойових дій.

З розвитком нових цифрових технологій, коли стала можливою статистична обробка радіолокаційної інформації на інтервалах часу рівних періоду слідування зондуючих сигналів, виникає доцільність розробки алгоритмів виявлення слабких відбитих від цілей радіолокаційних сигналів при плинній оцінці статистичних характеристик випадкового процесу як в однопозиційних, так і в багатопозиційних радіолокаційних системах.

У зв'язку з цим виникла необхідність розвитку відомої теорії виявлення радіосигналів і оцінювання їх параметрів на фоні внутрішніх шумів і активних маскуючих перешкод. На відміну від класичного підходу, який грунтується на критерії мінімуму середнього ризику і використовує відношення правдоподібності як відношення щільності ймовірності сумісного розподілу амплітуд радіосигналу і внутрішнього шуму радіоприймача до щільності ймовірності розподілу амплітуд внутрішнього шуму, запропоновано урахувати закон збереження енергії М.В. Ломоносова шляхом використання енергетичного відношення правдоподібності як відношення щільності ймовірності розподілу сумарної енергії радіосигналу і шуму до щільності ймовірності розподілу енергії шуму. Така постановка задачі враховує закон збереження енергії і забезпечує можливість виявлення радіосигналів за енергетикою співвимірних або менших за енергетику внутрішніх шумів. Використання відношення щільності ймовірності розподілу енергії сумарного радіосигналу і шуму до щільності ймовірності розподілу енергії шуму дозволяє здійснити байесівську статистичну оптимізацію процесу виявлення. Байесівський підхід вимагає використання всіх апріорних даних щодо засобу виявлення і умов його застосування і дозволяє на основі апостеріорного статистичного аналізу випадкового процесу прийняти оптимальне рішення про виявлення радіосигналу.

Процес енергетичного виявлення – це пошук інтервалу часу, де сумарна енергія радіосигналу і шуму по відношенню до усередненої енергії шуму перевищила поріг виявлення. Це апостеріорне відношення сумарної енергії сигналу і шуму до усередненої енергії шуму функціонально пов'язано зі щільностями ймовірності розподілу сумарної енергії радіосигналу і шуму. Враховуючи цей функціональний зв'язок ми апостеріорне відношення сумарної енергії сигналу і шуму до усередненої енергії шуму називатимемо енергетичним відношенням правдоподібності. Максимальна чутливість радіоприймача обмежується рівнем флуктуацій плинного значення енергії шуму на інтервалі статистичного аналізу рівному апріорному значенню тривалості зондуючого радіосигналу відносно усередненого значення енергії шуму.

Поріг прийняття рішення в радіолокації визначається критерієм Неймана-Пірсона і полягає в обмеженні ймовірності хибних тривог. Прийняття рішення про виявлення радіосигналу здійснюється після порівняння значення енергетичного відношення правдоподібності для довільного закону розподілу випадкових величин з порогом прийняття

рішення. Для моделі суми квадратів амплітуд оцифрованих гаусівських шумових вибірок умовна ймовірність хибних тривог має вигляд χ^2-розподілу.

Практичне застосування запропонованого способу енергетичного виявлення полягає у розбиванні періоду слідування зондуючих радіосигналів на інтервали статистичного аналізу рівному тривалості радіосигналу, визначенні дисперсії випадкового процесу на кожному інтервалі статистичного аналізу, енергетичного відношення правдоподібності для кожного інтервалу аналізу і порівнянні з заданим порогом виявлення. Це одноканальний у часі спосіб енергетичного виявлення. Багатоканальне виявлення передбачає максимальне зрушення у часі вхідної реалізації випадкового процесу на половину тривалості радіосигналу і наявності додаткових каналів виявлення, зрушених на час пропорційний відношенню половини тривалості радіосигналу до числа каналів і знаходженні максимуму енергетичного відношення правдоподібності на виході всіх каналів виявлення.

Важливим є те, що оптимальне енергетичне виявлення радіосигналу можливе без використання очікуваного радіосигналу в умовах апріорної невизначеності як форми радіосигналу, його тривалості, модуляції, так і несучої частоти.

Розпізнавання впливу маскуючих шумових перешкод можливе за рахунок запам'ятовування значення рівня власних шумів попередніх вимірювань при апріорній відсутності маскувальних радіоперешкод.

В основу теорії оцінювання параметрів радіосигналу при енергетичному підході, як і в класичному випадку, покладена мінімізація умовного середнього ризику для кажної реалізації випадкового процесу шляхом пошуку оцінки параметрів виявлених радіосигналів при складанні їх із множиною еталонних радіосигналів (кореляційна обробка радіосигналів) і заданих функціях вартості та пошуку максимального значення апостеріорного енергетичного відношения правдоподібності. Значення еталонного радіосигналу якому відповідає максимальне значення апостеріорного енергетичного відношения правдоподібності і є оцінкою параметру радіосигналу.

На відміну від класичної теорії оцінювання використання енергетичного відношення правдоподібності дозволяє оптимально оцінити значення параметрів радіосигналів за енергетикою менших за рівень внутрішніх шумів.

Дослідження детермінованої моделі визначення максимуму сумарної енергії співвимірних виявленого радіосигналу із сукупністю еталонних показали наступну закономірність: значення помилки оцінки доплерівської частоти залежить від тривалості радіосигналу (як і в класичному випадку) і при тривалих радіосигналах виникає неоднозначність оцінки, оцінка початкової фази визначається кроком дискретизації еталонних радіосигналів. З метою оптимізації обчислювальних затрат слід використовувати різнокрокове квантування еталонних радіосигналів, поступово наближаючись до оптимального значення оцінюваного параметру.

Сутність фазового методу оцінювання початкової фази і доплеровської частоти радіосигналів полягає у формуванні із тривалого радіосигналу радіосигналів різної тривалості для досягнення однозначності оцінювання початкової фази і доплерівської частоти для різних класів об'єктів.

Для енергетичного оцінювання параметрів радіосигналів фазовим методом необхідно з тривалого радіосигналу сформувати різнотривалі вибірки, оцінити початкову фазу прийнятого радіосигналу в широкосмуговому радіоканалі, сформувати квадратурні еталонні радіосигнали і дешифрувати розподіл максимумів енергетичного відношення правдоподібності на парному виході різносмугових каналів.

Розглянуті основи енергетичного виявлення і оцінювання параметрів радіосигналів дозволяють виявляти і оцінювати параметри радіосигналів за енергетикою співвимірною (або меншою) з внутрішніми шумами радіоприймача без впливу і при впливі активних маскуючих перешкод, що дозволить покращити якісні показники озброєння і зменшити енергетичні витрати для вирішення тих же завдань.

к.т.н. Правило В.В. (ВІТІ НТУУ ,,КПІ”)
Краснощок Я.О. (ВІТІ НТУУ ,,КПІ”)

МОЖЛИВОСТІ ЗАСТОСУВАННЯ ГІБРИДНИХ СИСТЕМ ПЕРЕДАЧІ

У своїх межах гібридні системи передачі є вигідною альтернативою проводовим системам. На сьогоднішній день існує декілька основних гібридних рішень – це використання широкосмугових радіоканалів WiFi/WiMax, радіорелейних ліній (РРЛЗ) разом з атмосферними оптичними лініями зв’язку (АОЛЗ).

В основі атмосферних оптичних ліній зв’язку лежать технології організації високошвидкісних каналів зв’язку за допомогою інфрачервоного випромінювання, що робить можливим мультисервісну передачу даних (текстові, звукові, графічні дані) між об’єктами через атмосферний простір, надаючи оптичне з’єднання без використання оптоволокна.

До основних переваг атмосферних оптичних ліній зв’язку можна віднести:

– висока пропускна здатність і якість цифрового зв’язку;

– не потрібно отримувати дозвіл на використання частотного діапазону;

– висока захищеність каналу від несанкціонованого доступу і скритність;

– високий рівень завадостійкості і перешкодозахищеності;

– можливість встановити лазерну атмосферну лінію там, де важко прокласти проводову лінію зв’язку;

– швидкість і простота розгортання FSO-мережі.

Поряд з основними перевагами безпроводових оптичних систем добре відомі і їх головні недоліки:

– залежність доступності каналу зв’язку від погодних умов (такі погодні умови як туман, дощ, сніг значно знижують ефективний діапазон роботи FSO-систем);

– необхідність забезпечення прямої видимості між випромінювачем і приймачем;

– обмежена дальність зв’язку.

Обладнання, яке реалізує гібридний канал, об’єднує переваги лазерних атмосферних каналів зв’язку (висока швидкість передачі інформації в дуплексному режимі) і широкосмугових радіо засобів (можливість ефективної роботи при несприятливих погодних умова: туман, сніг і т.д.). Основний режим роботи комбінованих ППМ являється лазерний режим.

Високоефективні гібридні системи, засновані на використанні технології FSO, є реальною альтернативою, якщо мережному розробнику необхідно враховувати вплив звичайних в даній місцевості погодних умов, протяжність лінії безпроводового зв’язку, вимоги до смуги пропускання і потенційну можливість використання системи FSO в якості допоміжних резервних каналів зв’язку.

Завдяки своїм перевагам, гібридні системи передачі – дозволяють вирішувати проблеми ,,останньої милі”, розвивати міські мережі передачі даних і голосу, здійснювати підключення домашніх мереж або офісів до мережі Інтернет, а також організовувати резервні канали зв’язку або розширювати існуючі канали при високому ступені захищеності. Крім того, технологія використовується для комунікацій між космічними апаратами.

Таким чином, галузі для застосування технології, можуть бути різними, в залежності від сфери застосування, та завдань, що будуть вирішуватись. Особливу увагу слід звернути на управляння ризиками, що має критичне значення для лікарень та оздоровчих центрів. які повинні дотримуватися федерального законодавства, що вимагає від них збереження конфіденційності історій хвороби пацієнтів. В місцях де прокладання кабелів недоцільне, чи має суттєві труднощі через особливості рельєфу, гібридні системи передачі будуть найкращим варіантом.

к.т.н. Правило В.В. (ВІТІ НТУУ „КПІ”)
Ніщенко В.І. (ВІТІ НТУУ „КПІ”)

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА ВІДОМЧА МЕРЕЖА НОВОГО ПОКОЛІННЯ (NGN)

Процес інформатизації набирає обертів у всьому світі. Ідея ,,Глобального інформаційного суспільства” (ГІС) вимагає максимальної інформатизації всіх сторін життя. Сьогодні безліч операторів зв’язку стикаються з проблемою повної або часткової реорганізації своїх мереж у зв’язку з невідповідністю до вимог користувачів. Збільшення швидкості, підвищення надійності, забезпечення відповідної якості і, авжеж, зростання кількості послуг – ті фундаментальні критерії, що зростають з кожним днем. І як вихід з даної ситуації доцільно впроваджувати концепцію NGN (New Generation Network).

NGN – мережа з комутацією на базі пакетів, яка здатна надавати телекомунікаційні послуги і має можливість використовувати декілька широкосмугових транспортних технологій, які забезпечують якість обслуговування і в якій функції, що відносяться до послуг, незалежні від технологій, що відносяться до транспортування. Вона гарантує вільний доступ для користувачів за їх вибором до мереж і конкуруючих постачальників служб і послуг. Аналіз основних принципів функціонування обладнання NGN показав, що:

1. Завдяки принципу демократичності існує велика кількість способів організації мережі, оскільки будь-яка технологія, що забезпечує передачу трафіку та / або надання послуг, може вважатися транспортною. Аналогічно, будь-яка технологія, що забезпечує доступ абонентів до ресурсів транспортної мережі, може вважатися абонентською або технологією доступу.
2. Найдоцільнішим рішенням рівня транспорту є організація єдиної IP-мережі.
3. Найбільш перспективним рішенням рівня управління є використання SoftSwitch, який володіє цілим рядом переваг: архітектура Softswitch піддається більшій масштабованості , ніж архітектура АТС, як у бік розширення, так і в сторону зменшення ємності. Таким чином, постачальники послуг, які використовують системи Softswitch, отримують набагато більше гнучкості при наданні послуг новим абонентам. Завдяки тому, що Softswitch розділяє рівень надання послуг і рівень управління викликом, можна швидко і з мінімальним витратами розгортати нові послуги, що користуються попитом. У разі міграції всіх мереж в пакетні технології, модель Softswitch (завдяки універсальності обладнання та використанні відкритих протоколів) дозволить операторам швидко адаптуваться в умовах нової технології та легко налагодити співпрацю в умовах конвергенції мереж в одну єдину NGN мережу.

Запропонована у моїй роботі архітектура відомчої мережі дозволяє в найкращій мірі використовувати транспортний ресурс завдяки організації єдиної IP-мережі та пакетної комутації. Використання різнорівневих програмних комутаторів (четвертого та п’ятого рівня) дозволяє централізувати управління мережею, при цьому ми досягнемо значного заощадження коштів при розширенні мережі за допомогою використання Softswitch 4-го рівня.Також вагомою перевагою даної мережі є застосування мультисервісних абонентських концентраторів – mAccess.MAK, та абонентських шлюзів малої місткості mAccess.MTU, які в свою чергу відрізняються кількістю підключених абонентів, але дозволяють підключати як цифрові так і аналогові кінцеві засоби. Це означає, що при розгортанні даної мережі нам не потрібно буде повністю замінювати все обладнання на цифрове. Процес ,,цифровізації” може відбуватись поступово у відповідності до наших можливостей. Конвергенція з телефонною мережею загального користування здійснюється за допомогою використання магістрального шлюзу - mGate.ITG, який підтримує такі протоколи : ЗКС №7, EDDS1, R2/R1.5, SIP, H.323, H.248, SIGTRAN.

к.т.н. Правило В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
к.т.н.Могилевич Д.І. (ВІТІ НТУУ „КПІ”)

СИСТЕМА УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ В УМОВАХ ПЕРЕХОДУ ДО МЕРЕЖ НОВОГО ПОКОЛІННЯ

Аналіз сучасного стану розвитку мереж та послуг телекомунікацій показує, що нові технології передачі, комутації та обробки інформації дозволяють ефективно модернізувати телекомунікаційні мережі. Це досягається за рахунок поступового переходу до мереж наступного покоління – *NGN* (*Next Generation Network*), які підтримують широкий спектр інфокомунікаційних послуг. Відмінною особливістю ідеології *NGN* є використання технологій *IP* (*Internet Protocol*) для передачі та комутації. Ця властивість *NGN* стимулює розробку принципів побудови телекомунікаційних мереж, які відповідають таким вимогам:

– можливість поетапного перетворення транспортних і телефонних мереж, які є в даний час основою системи телекомунікацій в Україні;

– збереження інвестицій операторів телекомунікацій, які були направлені на розвиток транспортних і телефонних мереж в попередні роки;

– здатність надати потенційним клієнтам сучасні види інфокомунікаційних послуг для забезпечення високої конкурентоспроможності експлуатаційних компаній;

– мінімізація витрат на побудову мереж *NGN* та їх поетапний розвиток.

На сьогоднішній день в телекомунікаційних мережах використовуються напівавтоматизовані процеси управління та окремі автоматизовані системи управління, що вирішують деякі завдання на рівнях управління елементами мережі та, частково, на рівні управління мережею. Лише в деяких нових цифрових телекомунікаційних мережах впроваджені та впроваджуються автоматизовані системи управління.

Широке впровадження новітніх телекомунікаційних технологій та швидке розширення номенклатури телекомунікаційних послуг, необхідність автоматизованого управління не тільки телекомунікаційними мережами, а й телекомунікаційними послугами, необхідність у близькому майбутньому інтеграції систем управління телекомунікаційними мережами, телекомунікаційними послугами та бізнесом у єдину систему управління діяльністю оператора телекомунікацій потребує створення автоматизованої системи оперативно-технічного управління телекомунікаційними мережами оператора телекомунікацій.

В даний час питаннями стандартизації управління телекомунікаційними мережами займаються кілька міжнародних організацій. Найбільш важливими є:

концепція *TMN* Міжнародного союзу електрозв’язку з питань телекомунікацій (*ITU*);

модель Форуму управління телекомунікаціями (*TeleManagement Forum – TM Forum*), заснована на концепції *Smart TMN*;

модель IETF, заснована на стандартних базових засобах мережного управління (*Network Management Framework*) мережі *Internet*;

модель мережного управління *ATM*-форуму (на основі моделі *IETF* з використанням елементів *TMN*);

модель управління фірми *IBM*; моделі з застосуванням технології управління *CORBA*.

Концепція *TMN* передбачає ієрархію управління за такими рівнями: елементами мережі; мережею; послугами; бізнесом. Стандарти щодо концепції *TMN* реалізовані в основному для рівнів елементного і мережного управління. Логічним розвитком моделі *TMN* є концепція *TM Forum* – Smart *TMN*, яка передбачає можливість управління в умовах мережі з обладнанням багатьох виробників на всіх рівнях управління, обумовлених концепцією *TMN*.

За концепцією *TM Forum* для опису моделі ведення бізнесу оператора вводяться поняття процесів і функцій.

Функція – складова частина процесу, що ініціюється якою-небудь подією. Для виконання функції необхідні деякі вхідні дані, а результатом її є набір вихідних даних. Функції, як правило, завжди спеціалізовані.

Процес – набір функцій. При цьому процес може містити в собі дочірні процеси, і усі вони здатні оперувати тим самим набором функцій, що надає можливість створити прозоре управління шляхом організації обміну інформацією між підпроцесами.

Найбільш перспективним напрямком розвитку систем управління є впровадження концепції *TMN* з врахуванням положень *Smart TMN*.

Особливості управління мережами наступного покоління визначаються особливостями її архітектури, а саме:

а) організація з'єднання в *NGN* має принципові відмінності від його встановлення в традиційних телефонних мережах з комутацією каналів. Це пов'язано з тим, що медіатрафік і сигнальна інформація для управління обслуговуванням виклику в *NGN* передаються за різними маршрутами та обробляються різними мережними пристроями, а не єдиним вузлом комутації;

б) медіатрафік проходить, як правило, безпосередньо між шлюзами доступу або транспортними шлюзами. Сигналізація управління обслуговуванням виклику проходить через програмні комутатори *Softswitch*, а в простіших випадках − через прокси-сервери *SIP* або *H*.323;

в) під час надання послуги сеансового доступу споживачу до мережі вузол мережі, що відповідає за ідентифікацію споживача, не бере участь в передачі інформації, яка призначена для споживача, та, як наслідок – неможливо отримати всю необхідну інформацію щодо споживачів і параметрів з'єднання на єдиний пристрій управління.

Основними вимогамии, яким повинна задовольняти система управління *NGN* є:

а) необхідність розподілу функцій управління в декількох мережних пристроях, зокрема:

1. у пристрої управління викликами і сеансами зв'язку;
2. у пристрої мережі, що відповідає за перенесення призначеної для споживача інформації;

б) застосування відкритих інтерфейсів управління, що дозволяють управляти різнотипним обладнанням (включаючи мережні вузли, міжмережні шлюзи тощо), яке входить до складу *NGN*, зокрема, використання стандартизованих протоколів − *CMIP, SNMP* та інших протоколів управління, а також формальних мов для опису інтерфейсів (*CORBA IDL, JAVA, GDMO*);

в) структура системи управління *NGN* повинна забезпечувати гнучкість реалізації та сумісність з іншими рішеннями, високу надійність, та як результат − якість обслуговування.

г) оператор телекомунікацій повинен мати можливість модифікувати програмне забезпечення для реалізації специфічних функцій та впроваджувати нові послуги шляхом зміни конфігурації.

ЛІТЕРАТУРА

1. Семенов Ю.В. Проектирование сетей следующего поколения. – С.– Пб.: Гипросвязь, 2005. – 239 с.

2. Гольдштейн Б.С., Гольдштейн А.С. SoftSwitch. – СПб.: БХВ – Санкт-Петербург, 2006.

3. Фокин В.Г. Управление телекоммуникационными сетями. Учебное пособие. – Новосибирск. – СибГУТИ, 2001. – 112 с.

4. Цитрон В.В, Слюсар В.А. Управление сетями электросвязи //Зв'язок.– 2000.– № 4.

5. Копейка О.В., Слюсар В.А., Цитрон В.В. Некоторые аспекты создания системы управления сетями святи // Вісник Українського будинку економічних та науково-технічних знань. – 2002.– №2.

Прокопенко Є. М. (ВІТІ НТУУ „КПІ”)

МОДЕЛЬ ІНФОРМАЦІЙНОГО КОНФЛІКТУ РАДІОЕЛЕКТРОННИХ СИСТЕМ

Провідні країни світу приділяють велику увагу розробці та удосконаленню систем та засобів радіоелектронної боротьби. Засоби радіоелектронного подавлення (РЕП), що знаходяться на їх озброєнні, здатні з високою ефективністю та у короткий час подавити систему радіозв’язку, побудовану на традиційних принципах. Враховуючі це, стає досить складним завдання забезпечення стійкого радіозв’язку в умовах РЕП. Успішне її вирішення неможливо без застосування спеціальних технічних і організаційних заходів по забезпеченню завадозахищеності систем радіозв’язку.

Процес функціонування системи радіозв’язку (СРЗ) в умовах складної радіоелектронної обстановки з достатнім ступенем точності може бути представлений сукупністю моделей фізичного, канального та мережного рівнів. Для вирішення завдань структурного і функціонального аналізу, а також синтезу алгоритмів функціонування СРЗ необхідно розглянути моделі, що найбільше повно описують об’єкт дослідження та умови його функціонування. Відомі моделі СРЗ дозволяють враховувати умови функціонування СРЗ відповідно до цільової функції. Однак їх недоліком є відсутність алгоритмічного опису адаптивних властивостей, без яких неможливо успішне функціонування СРЗ в умовах стохастического характеру змін завадової обстановки. В умовах антагоністичної протидії СРЗ і системи РЕП модель адаптивної системи радіозв’язку доцільно доповнити ігровим підходом, який враховує різноманітність і ефективність стратегій в умовах невизначеності.

Процес передачі інформації може бути поданий як конфлікт між системою радіозв’язку та джерелом завад, оскільки він відповідає формальним ознакам конфлікту. При цьому джерелом завад є середовище поширення сигналів і постановники організованих завад (система РЕП). При аналізі роботи системи радіозв’язку часто зручно вважати, що „середовище поширення” також поводиться як розумний супротивник, прагнучи створити якнайгірші умови для зв’язку. Система радіозв’язку і джерело завад мають набір альтернатив – режимів роботи. Вони можуть вплинути на якість процесу передачі інформації, вибравши відповідний режим. Необхідно визначити як здійснювати цей вибір, тобто сформувати стратегію управління режимами роботи.

Формалізувати опис конфлікту дозволяє теорія ігор. Оскільки інтереси системи зв’язку і джерела завад прямо протилежні і немає причин для узгодження їх дій, можна застосувати апарат скінчених матричних антагоністичних ігор. Апарат скінчених антагоністичних ігор може бути використаний в тих випадках, коли система радіозв’язку і джерело завад мають скінчений набір режимів роботи, наприклад, декілька градацій потужності, обмежений набір робочих частот і так далі. Можливим є вибір і зміна режиму роботи. При цьому необхідно мати кількісні оцінки ситуацій, відповідні всім поєднанням режимів, що вибираються учасниками конфлікту. Для зниження розмірності ігрових матриць використовуються різні алгоритми, які видаляють найменш ефективні і рідко використовувані стратегії за результатами прогнозування. При цьому результат гри багато в чому залежатиме від ступеня інформованості сторін про ймовірність використання тієї або іншої стратегії супротивника.

В запропонованій моделі ігрового управління радіоресурсом СРЗ, на відміну від відомих, для опису конфлікту застосовується модель нескінченно-крокової матричної гри із запізнюванням та помилками в інформованості сторін про дії військової системи радіозв’язку та системи радіоелектронного подавлення, а при побудові матриці гри враховуються показники інформованості про стратегію системи РЕП та важливості поточного циклу управління СРЗ. Розроблена модель дозволяє визначити стратегію управління параметрами і режимами роботи систем і засобів радіозв’язку, яка забезпечує максимальне гарантоване математичне очікування виграшу.

к.т.н. Радзівілов Г.Д.(ВІТІ НТУУ „КПІ”)
Бєляков Р.О.(ВІТІ НТУУ „КПІ”)

АНАЛІЗ ЗАДАЧ УПРАВЛІННЯ AQM МАРШРУТИЗАТОРА ПІДТРИМУЮЧОГО ПОТОКИ TCP

Для телекомунікаційних систем з комутацією пакетів характерно явище перевантаження, для боротьби з якими використовують методи активного управління чергою – Active Queue Management (AQM). Системи AQM маркерують/відкидають певну частину пакетів, які потрапляють в маршрутизатор, до моменту переповнення відповідної канальної черги. У роботі [1] описані лініоризовані AQM системи з RED, PI і PID алгоритмами як системи автоматичного управління.

При аналізі систем управління зі зворотнім зв’язком першочергове значення має їх стійкість. Стійку систему визначають як систему, яка має обмежену реакцію при дії обмеженого вхідного сигналу або сигналу порушення. Якщо замкнута система стійка, необхідно визначити її відносну стійкість, яка характеризується запасом стійкості по модулю, запасом стійкості по фазі і ширина смуги пропускання. Необхідність зазначених запасів стійкості обумовлена тим, що урівняння елементів системи, як правило, ідеалізовані, параметри елементів визначаються з похибкою і мають технологічний розкид, при експлуатації параметри деяких елементів змінюються через старіння. Відносну стійкість, нарівні з іншими показниками, наприклад, показниками точності і швидкодії, відносять до основних показників якості системи. Для аналізу відносної стійкості доцільно використовувати частотні характеристики системи. Частотний критерій стійкості також може підказати, як змінити параметри системи, щоб збільшити її відносну стійкість.

Для AQM виконання задач включає ефективне використання черги, регулювання затримки черги, і робастність.

Для ефективного використання черги слід уникати перенавантажень або пустоти. Утворена ситуація призводить до втрат пакетів та до не бажаних ретрансляцій (передач), що призводить до неефективного використання каналу.

Час необхідний для обробки пакетних даних при маршрутизації черги називається затримкою черги. Цей час разом із затримкою розповсюдження, вважається мережевою затримкою яку також бажано утримувати якомога меншою, тобто tradeoff (альтернативу, компроміс) для моделі AQM. Робастність: AQM характеризує нечутливість до різноманітних відхилень, для підтримки роботи закритого циклу не залежно від різних умов мережі . Ці умови включають кількість TCP сесій, і змін передачі і ємності каналу зв’язку. AQM система з PID-регулятором при зміні навантаження трафіку, при настройці PID-регулятора, має достатню стійкість і робастність, але зі збільшенням навантаження швидкодія системи зменшується. В той же час RED показує високий рівень використання у витраті (розтраті) великих затримок. При зменшенні затримки черги, понижаючи динамічний діапазон RED, використання погіршується. Модель PI здатна забезпечувати низьку затримку і високий рівень використання.

Таким чином для телекомунікаційних систем з комутацією пакетів з використанням систем AQM необхідно керуватися дослідженнями частотних характеристик системи, щоб збільшити їх відносну стійкість. А також підвищити ефективність використання черги, регулювання їх затримок, та покращити робастність.

ЛІТЕРАТУРА

1. Гостев В.И., Невдачина О.В., Кучер С.В. Робастность AQM систем с RED, PI и PID алгоритмами при изменении нагрузки трафика // Матеріали XVIII міжнародної конференції з автоматичного управління (Автоматика-2011), м. Львів, 28 – 30 вересня 2011 року.– Львів: Видавництво „Львівська політехніка”. – 2011. –С.93 – 94.

к.в.н. Розум І.Ю. (НУОУ)
к.в.н. Микусь С.А. (НУОУ)

МЕТОДОЛОГІЯ ОЦІНКИ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ЗВ'ЯЗКУ ЗАГАЛЬНОВІЙСЬКОВИХ ЧАСТИН

Погляди військових фахівців на еволюцію збройної боротьби щодо тенденцій розвитку форм і способів застосування військових частин та підрозділів, зростання бойових можливостей економічно розвинених країн світу та їх ролі у збройній боротьбі щодо інтеграції всіх сил і засобів у єдиному інформаційному просторі, накази та директиви Міністра оборони України та начальника Генерального штабу – Головнокомандувача Збройних Сил України, результати командно-штабних навчань свідчать про те, що існуючий рівень ефективності функціонування системи зв'язку військових частин не забезпечує виконання покладених на неї завдань. Це, насамперед, викликано невідповідністю систем зв'язку загальновійськових частин (СЗ ЗВЧ) вимогам щодо стійкості, мобільності та пропускної спроможності. Отже, в практиці військ виникає нагальна проблема у пошуку шляхів та обґрунтуванні рекомендацій щодо її підвищення до потрібного рівня. Для цього треба мати відповідний науково-методичний апарат оцінки ефективності функціонування СЗ ЗВЧ, зокрема методикам оцінки стійкості, мобільності та пропускної спроможності.

Питанням удосконалення СЗ ЗВЧ присвячені дослідження С.Я. Довбня, А.А. Лобанова, С.Г. Саннікова, А.А. Корецького, В.М. Волкова, А.В. Іващенка, Л.П. Щербини та інших, які свого часу зробили вагомий внесок у розвиток теорії ефективності СЗ ЗВЧ. Проте внаслідок еволюційних процесів у збройній боротьбі запропонований дослідниками науково-методичний апарат оцінки ефективності функціонування СЗ ЗВЧ не враховують деяких нових факторів, які в сучасних умовах істотно впливають на ефективність функціонування СЗ ЗВЧ, а саме: характеристики нових зразків вогневого і радіоелектронного ураження, використання факторного простору у розрахунку експлуатаційної надійності з урахуванням надійності каналу зв'язку з резервуванням, імовірності прийняття рішення на застосування противником навмисних завад, імовірності пошкоджень з різними ступенями (слабого, середнього і сильного) у ході ведення бою. Методики оцінки мобільності СЗ ЗВЧ не враховують показники ймовірності (оптимістичної, найбільш ймовірної і песимістичної) оцінок, пов'язаних із зміною структури СЗ ЗВЧ, та процесу реагування органів військового управління на вихід з ладу того чи іншого пункту управління в ході динаміки ведення бою. Методики оцінки пропускної спроможності СЗ ЗВЧ не враховують характеристики сучасних засобів передачі інформації, обсяг якої постійно зростає, та показники можливого радіоелектронного впливу противника на радіолінії. Саме тому наявний науково-методичний апарат не може бути використаний в інтересах сучасних досліджень, але може бути покладений в основу для подальшого удосконалення. Таким чином, виникає необхідність удосконалення науково-методичного апарату оцінки ефективності функціонування СЗ ЗВЧ для надання науково обґрунтованих рекомендацій щодо її підвищення.

У ході досліджень краще застосовувати наукові методи: аналізу та синтезу – для визначення особливостей застосування ЗВЧ; системного підходу – для аналізу впливу зовнішніх і внутрішніх чинників на ефективність функціонування СЗ ЗВЧ у воєнному конфлікті; теорії ймовірностей та статистичної обробки результатів – для оцінки ефективності функціонування СЗ ЗВЧ за показниками стійкості та мобільності; теорії мереж зв'язку – для оцінки пропускної спроможності в каналах та напрямках зв'язку. Удосконалені методики оцінки стійкості СЗ ЗВЧ можуть базуватися на об'єднанні (синтезі) часткових методик з надійності, завадостійкості й живучості і відрізняється від відомих комплексністю за рахунок використання факторного простору у розрахунку експлуатаційної надійності з врахуванням надійності каналу зв'язку з резервуванням, додатковим урахуванням показників впливу радіоелектронного придушення за рахунок імовірності прийняття рішення на

застосування противником навмисних завад, додатковим урахуванням показників впливу вогневого ураження за рахунок імовірності пошкоджень з різними ступенями (слабого, середнього і сильного) та урахуванням кількох уражальних чинників з одночасним використанням кількох типів боєприпасів у ході ведення бою. Удосконалені методики оцінки мобільності СЗ ЗВЧ можуть відрізняється від відомих застосуванням методу PERT-аналізу і базується на оцінках (оптимістичної, найбільш ймовірної і песимістичної), пов'язаних із зміною структури СЗ ЗВЧ із додатковим урахуванням показників реагування органів військового управління на вихід з ладу того чи іншого пункту управління в ході динаміки ведення бою. Удосконалені методики оцінки пропускної спроможності СЗ ЗВЧ можуть базується на теорії мереж зв'язку і відрізняється від відомих можливістю одночасно враховувати характеристики як аналогових, так і дискретних каналів зв'язку (визначення максимальної допустимої пропускної спроможності окремого каналу зв'язку (радіомережі), кількість інформаційних напрямків, вузлів зв'язку, системи зв'язку загалом), додатковим урахуванням показників радіоелектронного впливу противника на радіолініях.

Дослідження показують, що ЗВЧ у воєнному конфлікті може вести оборонний, наступальний бої, брати участь в операції, що, у свою чергу обумовили більш жорсткі вимоги до її системи зв'язку, зокрема до стійкості, мобільності та пропускною спроможності.

Узагальнений показник ефективності функціонування СЗ ЗВЧ $W_{СЗ}$ за кожним варіантом характеризується сукупністю її показників ефективності:

$$W_{СЗ}(t) = f\{G_{СЗ}, T_{СЗ}, S_{СЗ}\},$$

де $G_{СЗ}$ – показник ефективності функціонування СЗ ЗВЧ за можливістю її стійкого функціонування;

$T_{СЗ}$ – показник ефективності функціонування СЗ ЗВЧ за її мобільністю;

$S_{СЗ}$ – показник ефективності функціонування СЗ ЗВЧ за її пропускною спроможністю;

Сучасні можливості противника істотно впливають на виконання цих вимог, а оцінка ефективності функціонування СЗ ЗВЧ через її систему управління (СУ) забезпечить достатній рівень точності й об'єктивності оцінювання ступеня відповідності СЗ ЗВЧ її СУ та вимогам, які висуваються до неї: за стійкістю, мобільністю та пропускною спроможністю, що обумовило обрання інтегрального показника ефективності функціонування СЗ ЗВЧ.

$W^i_{СЗ} = W_{G_{СЗ}} + W_{T_{СЗр}} + W_{S_{СЗ}}$, з критерієм оцінки $W^i_{СЗ} \geq W^{потр}_{СЗ}$.

ЛІТЕРАТУРА

1. Методики по расчету и оценке полевых систем связи. – Л. : ВАС, 1985. – 80 с.
2. Авсюкевич А. Н. Эффективность и электронная защита военных систем связи / Авсюкевич А. Н., Комарович В. Ф., Симонов М. В.. – Л. : ВАС, 1980. – 220 с.
3. Елементи дослідження складних систем військового призначення / [Загорка О. М., Мосов С. П., Сбітнєв А. І., Стужук П. І.]. – К. : НАОУ, 2005. – 100 с.
4. Барабаш Ю. Л. Основи теорії ефективності складних систем / Барабаш Ю. Л.. – К. : НАОУ, 1999. – 38 с.
5. Казачинский В. З., Левитський Г. Е. Математические методы решения военно-специальных задач / В. З. Казачинский, Г. Е. Левитський. – К. : ВА ПВО СВ, 1980. – 291 с.

д.т.н. Романенко І.О. (ВІТІ НТУУ „КПІ”)
Івахненко Т.О. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ЕКСПЕРТНОГО ОЦІНЮВАННЯ ТА ЇХ ЗАСТОСУВАННЯ У ЗАДАЧАХ ПІДГОТОВКИ ВІЙСЬК ДЛЯ ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ

На сучасному етапі швидкого зростання можливостей технічних засобів, телекомунікаційних та інформаційних технологій відбуваються суттєві зміни в формах та змісті освіти України, в тому числі в Збройних Силах (далі ЗС) України, здійснюються широкомасштабні програми її інформатизації [1].

Перед ЗС України стоїть одна із важливих задач пошуку шляхів підвищення ефективності процесів підготовки військ (сил) ЗС України в умовах обмежених ресурсів. Перспективним шляхом є автоматизація окремих форм навчання особового складу ЗС України та поступове їх поєднання в єдину автоматизовану систему підготовки ЗС України. В цих умовах питання оцінки рівня підготовленості і порядку оцінювання військ (сил) ЗС України до виконання завдань за призначенням потребує наукового обґрунтування. У зв’язку з цим актуальним стає задача дослідження методів експертного оцінювання підготовки військ (сил), їх застосування для виконання завдань за призначенням [2 – 4].

Одним з можливих варіантів визначення чисельних значень зазначених показників, який дозволить більш об’єктивно аналізувати існуючу інформацію за показниками, що характеризують забезпечення системи підготовки, може бути реалізація методики, яка у якості вихідної інформації для бойової підготовки передбачає використовувати апріорні оцінки показників рядом авторитетних спеціалістів – експертів у галузі військових наук. Вироблення складних рішень у ситуації невизначеності або складання науково – технічного прогнозу викликає необхідність участі групи ерудованих у військовій сфері фахівців кожного роду військ, добре обізнаних у багатьох галузях знань, що дає можливість багатобічного аналізу кількісних та якісних аспектів проблем, що досліджуються [5].

Експертні оцінки служать ефективним засобом вирішення великої кількості неформальних завдань в самих різних галузях людської діяльності.

Під час прогнозування стану бойової підготовки, метою експертного опитування є обґрунтування кількісних значень відібраних показників та одержання оцінки відносної важливості цих показників при застосуванні методу автоматизованої оцінки рівня підготовленості військ (сил) до виконання завдань за призначенням.

Необхідно відзначити, що специфіка та різноманітність проблем, що вирішуються за участю експертів, суттєво обмежують можливості створення єдиних „універсальних” правил і моделей експертизи.

Запропонуємо рекомендації необхідні до вибору форм проведення опитування експертів, методу проведення опитування експертизи порівнюючи переваги та недоліки стосовно військової справи.

Вибір того чи іншого методу опитування експертів визначається цілями експертизи, сутністю проблеми яка вирішується, повнотою і достовірністю вихідної інформації, часом який є і витратами на проведення опитування.

Аналізуючи наданий матеріал, враховуючи специфіку військової справи, робимо висновки. Нам необхідний метод, що дозволить завчасно знайомитися з предметною областю кожному експерту індивідуально.

Оцінювати колективно, але усуваючи принцип конформізму, тобто експерти працюватимуть інкогніто по відношенню один до одного, використовуючи анкетування, як метод опитування. Багатоетапне опитування та ітеративність процедури забезпечить краще узгодження думок.

Таблиця 1

Порівняльна таблиця методів проведення опитування експертів з огляду пристосування до військової справи

методи	переваги	недоліки
Очні	Гарантує надійність отриманих даних	Великі витрати труда і часу
Заочні	Мала собівартість відносно очного опитування, спрощення процедури опитування	На гарантує надійність отриманих даних
Індивідуальні	Оперативність, можливість в повній мірі використовувати індивідуальні властивості експерта, відсутність тиску авторитетів, низькі витрати на експертизу	Висока міра суб'єктивності одержаних оцінок з за обмеженості знань одного експерта
Групові	Можливість різнобічного аналізу проблем, проведення ретельнішого аналізу ситуацій, розгляд великої кількості варіантів рішень, залучення знань і досвіду багатьох фахівців, зменшення міри невизначеності відносно важливих варіантів дій	Складність процедури отримання інформації і формування групової думки по індивідуальних судженнях експертів, можливість тиску авторитетів в групі, не завжди чітко визначається відповідальність за прийняте рішення
Дельфійський	ітеративна процедура опитування забезпечує краще узгодження думок експертів, виключення впливу конформізму	Складність проведення процедури

Проведений аналіз дозволив обрати необхідний метод експертного оцінювання по вибору коефіцієнту важливості шкал оцінки основних предметів навчання професійної підготовки особовим складом для виконання завдань за призначенням, а саме модифікований метод Дельфі з додаванням окремих процедур.

ЛІТЕРАТУРА

1. Закон України „Про вищу освіту" № 2984-III від 17.01.2002 р.

2. Указ Президента України від 20.10.2005 № 1497/2005 „Про першочергові завдання щодо впровадження новітніх інформаційних технологій".

3. Наказ Міністра оборони України від 21.03.2011 № 440 „Про затвердження Інструкції про порядок проведення інспекційних заходів".

4. Коротков Э.Н.Современные концепции обучения и их применение в подготовке военных кадров / Э.Н. Коротков – М.:ВПА.1976. – 212 с.

5. Петренко Л. М. Педагогічна експертиза: технологія експертного оцінювання результатів навчальних досягнень учнів / Л.М. Петренко. – Х. :Вид. група „Основа", 2007. – 176 с. – Б-ка журн. „Управління школою"; Вип. 5(53).

Романюк А.В. (ІТС НТУУ „КПІ”)

ЕНЕРГОЕФЕКТИВНА МЕТРИКА ВИБОРУ МАРШРУТІВ В БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

Бездротові сенсорні мережі (БСМ) на сьогоднішній день мають велику популярність і перспективність в зв’язку з широким спектром їх застосування. БСМ можуть застосовуватись як у військових цілях, наприклад на полі бою, так і у цілях медичного, біологічного та екологічного моніторингу тощо.

Мережа складається з групи вузлів (сенсорів). Кожний вузол має обмежену енергію батареї. Між вузлом-відправником та адресатом може бути велика кількість маршрутів по яким буде здійснюватися передача даних. Припустимо, що кожний вузол генерує деякий об’єм інформації, який має бути доставлений вузлу-адресату. Вузол спроможний передавати пакети даних іншому вузлу, якщо він має достатню залишкову енергію батареї. Якщо вузол знаходиться на великій відстані від вузла-сусіда, то для передачі інформації буде використано значну кількість енергії, що призведе до швидкого зниження заряду батареї. Після повної розрядки акумулятора, вузол не буде доступний для передачі даних, і загальний час життя мережі зменшиться. Для максимізації часу життя мережі маршрути мають бути прокладені так, щоб витрати енергії були оптимізовані між вузлами відповідно до їх залишкової енергії батареї та витрат енергії на передачу, яка залежить від відстані між вузлами.

В роботах [1, 2] розглянуті різноманітні метрики вибору маршруту для алгоритмів маршрутизації в БСМ: потужність передавача вузла, залишкова енергія батареї, витрачена на прийом та передачу енергія. Авторами запропоновані різні адитивні згортки цих метрик.

Однак, запропоновані метрики не забезпечують баланс витрат енергії батареї в БСМ та потребують вдосконалення. Тому пропонується нова метрика вибору маршруту, яка враховує відстань і, відповідно, витрати енергії на передачу між сусідніми вузлами та залишкову енергія батареї вузлів. Метрика радіоканалу *i-j* розраховується наступним чином:

$$C_{ij} = e_{ij}/e_{бi} + e_{ji}/e_{бj},\ i, j \in N,$$

де e_{ij} (e_{ij}) – витрати енергії для передачі одиниці інформації від вузла i (j) вузлу j (i); $e_{бi}$ ($e_{бj}$) – залишкова енергія батареї вузлів; N – множина вузлів мережі.

Використання цієї метрики дозволить забезпечити баланс витрат енергії між вузлами мережі та забезпечить максимізацію часу життя мережі. Додатково для забезпечення заданої якості передачі в залежності від типу трафіку можливо введення додаткових критеріїв якості маршруту: максимальне число ретрансляцій, максимальний час доставки повідомлень, мінімальна пропускна здатність.

В подальшому буде запропонована математична модель оцінки ефективності функціонування алгоритмів маршрутизації, які будуть використовувати нову метрику вибору маршруту, що дозволять підвищити час функціонування БСМ.

ЛІТЕРАТУРА

1. Narasimha Datta N., Gopinath K. A survey of routing algorithms for wireless sensor networks // J. Indian Inst. Sci., Nov.– Dec. 2006, 86, pp. 569 – 598.

2. Jain S.K., Kaushik P., Singha J. Review of energy efficient routing algorithm as LPP in wireless sensor network // Emerging Trends in Networks and Computer Communications (ETNCC) International Conference, 2011, pp. 314 – 319.

Руденко А.М. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ІСНУЮЧИХ СИСТЕМ РУХОМОГО РАДІОЗВ’ЯЗКУ ДЛЯ ПОБУДОВИ МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В теперішній час у спеціальних системах зв’язку України на озброєнні знаходяться радіозасоби 2 – 4-го поколінь, головними недоліками яких є незадовільна завадозахищеність, що проявляється як у нездатності протидіяти навмисним завадам, так і у створенні високого рівня внутрішньосистемних завад, робота на фіксованих робочих частотах, які легко викрити противнику, недостатня швидкість престройки частоти, що забезпечується засобами 4-го покоління. Засоби 5-го покоління тільки починають поступати на озброєння військ зв’язку.

Тому виникає необхідність пошуку шляхів підвищення ефективності спеціальних систем радіозв’язку за допомогою вдосконалення існуючих та доповнення їх елементами, побудованими на основі нових принципів організації зв’язку.

Швидкості доступу до мереж передачі даних, реалізовані в мережах стільникового радіозв’язку 2-го покоління не можуть задовольнити сучасним вимогам. Мережі третього покоління також не забезпечили очікуваний рівень якості послуг. Тому активно ведеться робота по створенню майбутніх мереж 4-го покоління.

Однією з найбільш перспективних є технологія WiMax, що дозволяє забезпечувати високу пропускну спроможність і велику область покриття. Ця технологія дозволяє покращити електромагнітну сумісність радіоелектронних засобів і, що найважливіше для радіозв’язку спеціального призначення, забезпечити вищий рівень прихованості передачі інформації.

В останні роки намітилася тенденція до конвергенції різнорідних мереж результатом якої повинно стати створення єдиної універсальної мережі наступного покоління , що буде функціонувати на базі технології комутації пакетів. Це є одним із шляхів досягнення високої ефективності використання пропускної спроможності мереж, підвищення швидкості доступу користувачів.

Важливим завданням при побудові радіомереж з комутацією пакетів є вибір методу множинного доступу та вибір варіанту топології мережі.

Широкосмугові (шумоподібні) сигнали (ШСС) спочатку використовувались у системах зв’язку спеціального призначення для забезпечення високого рівня розвід- та завадозахищеності. Тому доцільно використати саме кодовий розподіл каналів.

Щодо топології мережі, то одним з варіантів може бути традиційна стільникова з розміщенням базових станцій (БС) радіодоступу на автомобілях та інших рухомих засобах. Заслуговує на увагу концепція створення мережі з розміщенням БС на безпілотних літальних апаратах, що виключає широке використання наземного обладнання. Так можна, наприклад, організовувати резервні базові станції, які швидко відновлюватимуть зв’язок у тих районах, де наземні БС були виведені з якихось причин з ладу.

Ще один перспективний варіант топології – мобільні радіомережі (MANET) – динамічна архітектура побудови мереж, які самоорганізуються та не містять базових станцій і фіксованих маршрутів передачі інформації. Перевагами мобільних радіомереж є наступні: відсутність етапу планування, швидке розгортання, децентралізоване управління, робота в русі всіх елементів мережі.

Таким чином, з урахуванням сучасних поглядів на розвиток систем радіозв’язку та їх поступової конвергенції пропонується будувати військові радіомережі з використанням технології пакетної комутації. На основі аналізу методів множинного доступу та варіантів топології розроблено практичні рекомендації для побудови радіомереж спеціального призначення.

Савицький А.Д. (ВІТІ НТУУ „КПІ”)
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)

МОДЕЛЬ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ У СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Створення єдиного інформаційного простору на базі системи дистанційного навчання є важливим етапом на шляху підвищення якості та доступності освіти для військовослужбовців Збройних силах України. Використання інформаційних технологій дозволяє запропонувати більш зручну модель навчання і об’єднати більшу кількість викладачів вищих військових навчальних закладів та військовослужбовців без відриву від служби. Невід’ємною частиною системи дистанційного навчання є засоби контролю рівня засвоєння знань. Однак, на сьогоднішній день не в повній мірі впроваджені програмно-апаратні засоби, що дозволяють перевіряти, чи перебуває за віддаленим комп’ютером саме той навчаємий, за якого він себе видає. Тобто відсутні засоби гарантованої ідентифікації користувача. Вирішити цю проблему можна шляхом застосування додаткового програмного забезпечення розпізнавання користувачів, яке базується на технології визначення біометричного профілю користувача.

На даний момент існують спеціалізовані механізми ідентифікації, що використовують біометричні фактори оператора інформаційної системи. Це досягається завдяки класифікації психофізичних параметрів користувача, до яких належать клавіатурний почерк та психологічний особистісний профіль. У процесі взаємодії з комп’ютером індивідуальність користувача проявляється у швидкості набору символів, звички використовувати основну чи додаткову частину клавіатури, характеристики „подвійних” та „потрійних” натискань клавіш. У доповіді пропонується розглянути систему ідентифікації, яка базується на застосуванні спеціального „вхідного тестування”, що дозволяє отримати функції подібності та побудувати модель поведінки слухача, який проходить тестування. Побудови моделі передбачає два етапи: На першому етапі необхідно передбачити тестування у присутності викладача. Слухачеві пропонується пройти тестування за визначеним тестом з множини тестів з навчальних дисциплін $H = \{h_n\}$, $n = 1, \ldots, k$ та множини всіх завдань, що містяться в тесті $Z = \{z_m\}$, $m = 1, \ldots, z$. Результат виконання тесту представляється у вигляді бінарного вектора, котрий містить одиничний елемент у тій позиції, що відповідає варіанту, обраному у відведений проміжок часу на дане завдання, і нульовому – в іншому випадку. Сукупність таких векторів утворюють бінарну матрицю $M = \|m_{ni}\|$, яка відображує психологічний особистісний профіль слухача системи.

Другим етапом є порівняння профілю користувача (матриці M) з матрицею $M_l = \|m_{kil}\|$, де l-множина всіх відомих системі індивідуальних профілів користувачів системи дистанційного навчання. Для отримання кількісної характеристики подібності профілів використовується міра подібності:

$$P_u = \frac{S_1}{S_1 + S_{10} + S_{01}},$$

де S_1 – кількість спільних елементів моделі та вхідного тесту;

S_{10} – кількість елементів, що належать моделі, але відсутні у вхідному тесті;

S_{01}– кількість елементів, які відсутні в моделі, але наявні у вхідному тесті.

Аналіз кількісної міри коефіцієнту подібності дозволяє зробити висновок про особистість слухача який тестується.

На основі наведеної моделі пропонується розробити програмне забезпечення для ідентифікації слухачів системи дистанційного навчання. Застосування даного програмного забезпечення на клієнтській частині дозволяють точно ідентифікувати слухачів системи дистанційного навчання, що суттєво підвищить ефективність контролю та оцінювання якості їх знань.

к.т.н. Самойлов І.В. (ВІТІ НТУУ „КПІ”)
д.т.н. Толюпа С.В. (ДУІКТ)

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ДЛЯ НАСТРОЙКИ НЕЧІТКИХ ВІДНОШЕНЬ В СИСТЕМАХ ДІАГНОСТИКИ

На сьогодні актуальною науково-технічною проблемою є створення систем діагностування, які можуть опрацьовувати нечітку діагностичну інформацію. У базах знань таких систем міститься не тільки кількісна інформація, що характеризує стан об’єкта діагностики, а і якісна інформація, яка являє собою експертні оцінки. Для формалізації експертної інформації при моделюванні причинно-наслідкових зв’язків зручно використовувати теорію нечітких множин [1]. Нечітка модель діагностики будується на основі композиційного правила виведення Заде [2], в якому носієм діагностичної інформації є матриця нечітких відношень „причини–наслідки”, що зв’язує вектор мір значимості причин і вектор мір значимості наслідків.

Побудова моделі здійснюється в два етапи, які за аналогією з класичними методами можна вважати етапами структурної і параметричної ідентифікації. На першому етапі здійснюється формування і груба настройка моделі шляхом побудови бази знань за доступною експертною інформацією або за експериментальними даними. На другому етапі реалізується тонка настройка нечіткої моделі. Етап тонкої настройки зведений до задачі нелінійної оптимізації, для розв’язання якої в [3] використовується генетичний алгоритм. Недоліком методу є те, що генетичний алгоритм погано пристосований для врахування нових даних, що надходять в навчальну вибірку. В роботах [4, 5] був запропонований метод нейро-лінгвістичної ідентифікації нелінійних залежностей. Принциповою перевагою цього методу є можливість навчання нечітких баз знань, в реальному масштабі часу, тобто в режимі on-line. Недоліком методу є можливість влучення в локальний екстремум.

Постановка задачі. Нехай навчальна вибірка задана у вигляді M пар експериментальних даних:

$$\left\langle \hat{X}_p, \hat{Y}_p \right\rangle,\ p = \overline{1,\ M},$$

де $\hat{X}_p = \left(\hat{x}_1^p,\ \hat{x}_2^p,\ \ldots,\ \hat{x}_n^p \right)$ – вектор значень вхідних змінних в експерименті номер p;

$\hat{Y}_p = \left(\hat{y}_1^p,\ \hat{y}_2^p,\ \ldots,\ \hat{y}_m^p \right)$ – вектор значень вихідних змінних в експерименті номер p.

Припустимо, що $s_j,\ j = \overline{1,\ m}$, – деякий наслідок, який розглядається як лінгвістичний терм. Нечітка множина, за допомогою якої формалізується терм s_j, являє собою сукупність пар: $S_j = \left\{ \frac{\text{м}_1^{s_j}}{d_1},\ \frac{\text{м}_2^{s_j}}{d_2},\ \cdots,\ \frac{\text{м}_n^{s_j}}{d_n} \right\}$, де $\left\{ d_1,\ d_2,\ \ldots,\ d_n \right\} = D$ – універсальна множина причин; $\text{м}_i^{s_j}$ – ступінь належності елемента $d_i \in D,\ i = \overline{1,\ n}$ нечіткій множині s_j.

Нехай $Q = \left(q_1,\ q_2,\ \ldots,\ q_m \right)$ – вектор параметрів концентрації нечітких множин наслідків S_j такий, що матриця нечітких відношень має вигляд:

$$R = \begin{bmatrix} \left(r_{11}\right)^{q_1} & \left(r_{12}\right)^{q_2} & \cdots & \left(r_{1m}\right)^{q_m} \\ \left(r_{21}\right)^{q_1} & \left(r_{22}\right)^{q_2} & \cdots & \left(r_{2m}\right)^{q_m} \\ \cdots & \cdots & \cdots & \cdots \\ \left(r_{n1}\right)^{q_1} & \left(r_{n2}\right)^{q_2} & \cdots & \left(r_{nm}\right)^{q_m} \end{bmatrix}.$$

З урахуванням цієї матриці співвідношення, яке визначає залежність „причини–наслідки” для нечіткої моделі діагностики можна записати в такому вигляді:

$$Y = f\left(X, C_X, P_D, Q_R, P_S \right),$$

де X – множина вхідних змінних; Y – множина вихідних змінних; P_D (P_S) – вектори параметрів функцій належності вхідних (вихідних) змінних до нечітких термів причин (наслідків); C_X – вектор параметрів концентрації функцій належності, що моделюють неточність вхідних змінних.

Задача тонкої настройки нечітких відношень може бути сформульована так: необхідно підібрати такі вектори параметрів функцій належності вхідних і вихідних змінних, вектор параметрів концентрації нечітких множин наслідків та вектори параметрів концентрації функцій належності, що моделюють неточність вхідних даних, які забезпечують мінімальну відстань між теоретичними і експериментальними виходами об’єкта:

$$\sum_{p=1}^{M}\left[\sum_{j=1}^{m}\left[f_j\left(\hat{X}_p, C_X, P_D, Q_R, P_S \right) - \hat{y}_j^p \right]^2\right] = \min_{C_X, P_D, Q_R, P_S}.$$

Таким чином пропонується двофазна тонка настройка параметрів моделі на базі нечітких відношень. Перша фаза використовує наявну навчальну вибірку і генетичний алгоритм для грубого влучення в область глобального мінімуму нев’язки між модельними і експериментальними результатами. Друга фаза використовує нейро-нечітку мережу для підстройки параметрів моделі і їх адаптивної корекції по мірі появи нових експериментальних даних. Особливість даного підходу полягає в тому, що структура розв’язку на етапі генетичної настройки і на етапі нейронної підстройки відрізняється. Зокрема, кількість параметрів навчання на етапі генетичної оптимізації є меншою, ніж на етапі нейронної підстройки, що дозволяє зменшити область пошуку розв’язку і відповідно час його отримання. Крім того нейро-мережевий підхід забезпечує адаптацію параметрів моделі до варіації вхідних даних, що зумовлені неточністю результатів вимірювань.

ЛІТЕРАТУРА

1. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. – Винница: УНІВЕРСУМ-Вінниця, 1999. – 320 с.

2. Заде Л. Понятие лингвистической переменной и её применение к принятию приближенных решений. – М.: Мир, 1976. – 167 с.

3. Митюшкин Ю. И., Мокин Б. И., Ротштейн А. П. Soft Computing: идентификация закономерностей нечеткими базами знаний / МОН Украины. – Винница: УНІВЕРСУМ-Вінницяю – 2002. – 145 с.

4. Ротштейн А.П., Митюшкин Ю.И. Нейро-лингвистическая идентификация нелинейных зависимостей // Кибернетика и системный анализ. – 2000. – № 2. – С. 179 – 180.

5. Oh S. K., Pedricz W., Park H. S. Rule-based multi-FNN identification with the aid of evolutionary fuzzy granulation // Knowledge Based Systems. – 2010. – Vol. 17(1). – Pp. 1 – 13.

д.т.н. Самохвалов Ю.Я. (ВІТІ НТУУ „КПІ”)
Єрмоленко В.М. **(**ВІТІ НТУУ „КПІ”)

ШЛЯХИ ВДОСКОНАЛЕННЯ ПІДСИСТЕМИ ПОШУКУ ДОКУМЕНТІВ У СИСТЕМІ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Система електронного документообігу (СЕДО) Збройних сил України призначена для автоматизації процесу діловодства в органах управління Збройних сил України. Однією з основних функцій СЕДО є пошук документів.

На даний момент підсистема пошуку документів у СЕДО дозволяє здійснювати лише фактографічний пошук структурованих документів без урахування неоднозначності природної мови (синонімії, полісемії, меронімії). Однак, практика використання даної підсистеми показує, що у більшості випадків користувачам потрібен пошук документів без заздалегідь відомих атрибутів, тільки на підставі загальної теми. Тому, для забезпечення можливості здійснення пошуку за тематикою та за ключовими словами, необхідне впровадження моделей повнотекстового пошуку документів, які повинні забезпечувати:

об’єднання термінів запиту логічними операторами;

урахування синонімії, полісемії, меронімії термінів запиту;

ранжування результатів стосовно релевантності запиту.

Серед відомих моделей повнотекстового пошуку найбільш розповсюдженими є: булева, векторна, ймовірнісна, нечіткого пошуку та розширена булева. Булева модель спирається на теорію множин, де кожен термін пов’язаний з множиною документів. Дана модель дозволяє використовувати логічні оператори в запиті та за допомогою зовнішніх сховищ даних дає змогу усунути полісемію, синонімію та меронімію природної мови, але не дозволяє ранжувати результати пошуку, тому що ступінь релевантності має дві градації. У векторній моделі документи та запити представлені векторами. Використання вагових коефіцієнтів присутності термінів у документі дозволяє гнучко ранжувати результати пошуку та усунути синонімію, полісемію та меронімію природної мови за допомогою інформаційно-пошукових тезаурусів, але не дає змогу використовувати логічні оператори у запиті, який розглядається, як „купа слів”.

Ймовірнісна модель використовує вибірку документів, яка отримана в результаті суджень користувачів про їх релевантність запиту. Дана модель, як і інші, дозволяє усунути синонімію, полісемію та меронімію термінів; є можливість ранжувати результати пошуку, але відсутня можливість використання логічних операторів у запиті. Також суттєвим недоліком даної моделі є те, що вона потребує постійного навчання системи.

Модель нечіткого пошуку базується на теорії „нечітких” множин. Даний підхід дозволяє пом’якшити класичну булеву модель шляхом введення континууму градацій належності терміна документу, усунути синонімію, полісемію та меронімію термінів та провести ранжування за ступенем релевантності. На теорії „нечітких” множин були створені такі моделі, як: *Paise*-модель та *MMM* (*Mixed Min and Max*). Але для адекватної роботи системи необхідний опис ознак термінів. У розширеній булевій моделі поєднуються елементи булевої та векторної моделі. Основна ідея полягає у введенні параметризованої функції подібності документа запиту. Дана модель дозволяє використання логічних операторів у запиті, ранжувати результати пошуку та усунути синонімію, полісемію та меронімію природної мови.

Отже, з проведеного аналізу видно, що впровадження повнотекстового пошуку на базі розширеної булевої моделі дозволить значно поширити пошукові можливості користувачів СЕДО.

Симоненко О.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Сова О.Я. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ НАПРЯМКІВ РОЗВИТКУ СИСТЕМ ТА ЗАСОБІВ РАДІОЗВ’ЯЗКУ В ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ ВІЙСЬКАМИ

В умовах сучасних швидкоплинних та високоманеврених бойових дій отримання переваги над супротивником вимагає організації взаємодії між угрупованнями військ шляхом налагодження безперервного та надійного управління територіально-рознесеними підрозділами, які розміщені на значних географічних територіях. У зв’язку з цим у комплексі заходів із забезпечення національної безпеки розвинених країн світу пріоритетним стає питання, пов’язане із використанням досягнень в області новітніх інформаційних і телекомунікаційних технологій для розвитку і удосконалення системи військового управління, як одного із головних елементів державної і воєнної інфраструктури, який визначає ефективність застосування військ (сил) та озброєння.

Основними особливостями сучасних бойових дій, а також процесів управління військами, бойовими системами і озброєнням є: підвищена мобільність підрозділів і частин; розосереджене розгортання військ на територіях, розділених силами супротивника; значна інформаційна потреба органів управління; інтеграція систем зв’язку, навігації, розвідки й автоматизації та ін.; орієнтація на безпосередніх учасників бойових дій в тактичній ланці управління. Значення систем зв’язку в ході ведення сучасного бою є дуже високим, адже від їх правильного і швидкого функціонування залежить успішність бою чи операції. У зв’язку з цим, до систем зв’язку тактичних підрозділів пред’являються наступні вимоги: забезпечення безперервності бойового управління при розміщенні на місцевості з різним рельєфом; надійність зв’язку при високій мобільності абонентів; гарантована захищеність каналів від несанкціонованого доступу і впливу РЕБ противника; надання гарантованої якості обслуговування користувачів; мінімізація часу підключення абонентів до мережі.

Реалізація зазначених вище вимог можлива лише за використання систем радіозв’язку, при розробці яких визначаються наступні пріоритети: мобільність, передача різних типів трафіка (мова, відео, дані), здатність радіозасобів об’єднуватись в радіомережу без завчасно розгорнутої інфраструктури (відсутність етапу планування), здатність вузлів до самостійного формування правил доцільної поведінки за різних умов функціонування радіомережі (інтелектуальність).

Сьогодні зазначені вище пріоритети втілюються в життя провідними виробниками (*Harris Corporation* США, *ITT Communication* США, та ін.) при створенні сучасних засобів радіозв’язку (*PRC-117G*, *RF-7800M-MP*, *RF-7800S-TR* виробництво Harris; *PR4G Fastnet*, виробництво *Thales* та ін.).

Основними особливостями сучасних радіозасобів є: програмованість; наявність вузлової системи управління, яка використовує методи, що відносяться до різних рівнів моделі OSI; когнітивність (*cognitive radio*) – нова технологія, що дозволяє використовувати радіоресурс динамічним способом і володіє двома основними характеристиками: здатність до пізнання та реконфігурування. Однак, крім управління радіоресурсом, особливості функціонування та специфіка завдань, які покладаються на радіомережі тактичної ланки управління, вимагають вирішення низки інших задач управління: управління маршрутизацією, топологією, потоками даних, безпекою та ін.

Вирішення зазначених задач управління можливе за наявності системи управління вузлом радіомережі, здатної приймати рішення в умовах невизначеності та неповноти інформації про об’єкт управління. Тому, в якості напрямку подальших досліджень систем та засобів радіозв’язку доцільно вибрати застосування технологій обробки знань та штучного інтелекту з метою забезпечення здатності радіовузлів самоорганізовуватися в радіомережу для передачі різних типів трафіка із заданою якістю обслуговування.

к.т.н. Слободянюк О.В. (КПНУ ім. І.Огієнка)
к.т.н. Гуржій П.М. (ВІТІ НТУУ „КПІ”)
Петросян І.А. (ВІТІ НТУУ „КПІ”)

ОЦІНКА ЕФЕКТИВНОСТІ МЕТОДУ КОМПАКТНОГО ПРЕДСТАВЛЕННЯ АРХІТЕКТУРИ МУЛЬТИІЗОТОПНОГО ОПИСУ РЕЛЬЄФУ ЗОБРАЖЕНЬ У НЕІДЕАЛЬНИХ УМОВАХ

Найбільш важливою задачею при проектуванні систем компактного представлення зображень є забезпечення кодування та декодування вихідних даних без втрат. Для оцінки ефективності стиснення найчастіше використовують міри середньоквадратичного відхилення та відхилення сигнал/шум. У деяких випадках існує необхідність проведення процесу стиснення зображень з точністю „біт у біт” [1 – 6].

Теоретично була доведена та експериментально підтверджена відповідність класу точності „біт в біт” розробленого методу компактного представлення архітектури мультиізотопного опису рельєфу зображень [7]. Однак дослідження проводилося за ідеальних умов. Тобто за відсутності помилок у процесі передачі пакетів даних у телекомунікаційних мережах. Цей факт не дозволяв однозначно стверджувати про високу ефективність роботи методу стиснення в реальних умовах функціонування телекомунікаційних систем. Тому було сформульовано відповідну задачу та побудовано модель оцінки впливу одиночних та серійних (пакетних) помилок, що виникають на етапі транспортування пакетів даних, на якість відновлених зображень. Дана модель враховує ймовірність появи помилок у різних складових частинах стисненого представлення архітектури, а також їх вплив на значення коду-номера архітектури $C_{ф,св}$ та системи значень основ $Ф$. Було з’ясовано, що одиночні помилки не впливають на якість відновленого зображення. Хоча їх вплив на значення коду-номера є дещо більшим ніж на систему основ. Пакетні помилки також більш критичні для першого блоку стисненого зображення, а при появі їх у системі основ приводить до спотворення невеликої кількості пікселів. Однак, особливості побудови представлення архітектури мультиізотопного рельєфу зображень із поєднанням поліадичних властивостей побудованої системи основ зводить до мінімуму такі впливи. Зважаючи на це, можна зробити висновок, що використання даного методу стиснення у телекомунікаційних системах дозволить не лише підвищити якість відтворених зображень при менших об’ємах стиснених даних але й знизити кількість додаткової службової інформації, що накладається різноманітними методами захисту від завад у каналах передачі даних.

ЛІТЕРАТУРА

1. Ватолин В.И., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ – МИФИ, 2002. – 384 с.

2. Gonzalez, Rafael C; Woods, Richard E. Digital Image Processing, 2nd ed. – published by Pearson Education, Inc. publishing as Prentice Hall., 2002. – 793 p.

3. Лабутіна І.А. Дешифрування аерокосмічних знімків: Навчальний посібник. – М: Аспект-Пресс, 2004. – 184 с.

4. Баранник В.В., Бридня Е.А., Гуржий П.М. Разностное кодирование массивов служебных данных // Зб. наук. пр. ХУ ВС. – Х.: ХУ ВС. – 2005. – Вип. 2 (2). – С. 82 – 84.

6. Баранник В.В., Гуржій П.М. Полиадическое кодирование массивов длин серий в смешанной системе оснований // Авиационно-космическая техника и технология. – 2005. – Вип. 5 (21). – С. 47–51.

7. Кодирование трехмерных моделей видеокадров в инфотелекоммуникационных системах: монография / В.В. Баранник, В.П. Поляков, А.В. Слободянюк. – Каменец-Подольский: Калиграф, 2011. – С. 212.

к.т.н. Слотвінська Л. І. (ВІТІ НТУУ „КПІ”)

ТЕНДЕНЦІЇ РОЗВИТКУ МЕТОДІВ ТА СИСТЕМ ЗАХИСТУ БЛАНКІВ ДОКУМЕНТІВ

Бланки документів відносять до спеціальної поліграфічної продукції. Їх можна розділити на такі основні асортиментні групи: державні цінні папери та бланки (відомчі, документарні та галузеві); бланки документів, що є засобами платежів та одержання послуг; марки (акцизні, митні, гербові, поштові) та конверти; лотерейна і білетна продукція; етикеткова продукція.

Особливо потребують захисту від підроблення та фальсифікації різноманітні персоналізовані документи (1). Як правило, дану продукцію захищають багаторівневими системами складних методів та комбінуванням різних компонентів цієї системи. Кількість видів захисту на одному документі може сягати від 5 до 30 найменувань (2).

Захист бланків документів проводять за допомогою: методів дизайну, застосування спеціальних способів друку, виконання післядрукарських процесів, використання спеціальних захисних фарб та особливостей паперу чи іншої основи.

З розвитком комп’ютерних інформаційних технологій рівень виготовлення і захисту від підроблення покращився, став більш складним.

У багатьох розвинутих країнах світу документи виготовляють у вигляді полімерних карток (ламіновані, пластикові, з застосуванням елементів пам’яті, біометрії...). Цей вид документів має свою специфіку захисту (3).

Як додаткові елементи захисту від підробок можуть використовуватись приховані зображення, контрольні, невидимі і кольорові мітки, дефекти, спеціальний шрифт, шаблони для контролю та інші.

Для визначення напрямків розвитку елементів та методів захисту було проведено аналіз науково-технічної літератури поліграфічної галузі за 2000–2011 рік.

Обговорено результати аналізу з метою визначення сучасних напрямків розвитку систем захисту бланків документів. Аналіз науково-технічних джерел показав стрімкий розвиток струминного виду друку (4). Разом з тим не втрачає своїх позицій традиційний офсет. В результаті проведеної роботи встановлено, що більшість розробок методів захисту спеціальної поліграфічної продукції проводяться за трьома основними напрямками: захист паперового полотна, захист спеціальними фарбами, захист за допомогою технологічних особливостей спеціальних способів друку. Пропонується, наприклад, процес друку з захистом на рулонній офсетній машині (5). Або унікальна технологія трансферного нанесення фольги і вибіркового голографічного рисунка.

Цікавою є розробка технології цифрового друку фірми Canon з використанням вмонтованого модуля з прозорим тонером, який можна застосовувати для одержання водяних знаків. Також вперше в цифровому друці можна одержувати відбитки з металевими, блискучими і матовими ефектами.

ЛІТЕРАТУРА

1. Киричок П. О., Коростіль Ю. М., Шевчук А. В. Захист цінних паперів та документів суворого обліку. – К.: НТУУ „КПІ”, 2008. – 396 с.

2. Крылов А. „Таблица Менделеева” для защищенной полиграфии (Текст) / А. Крылов// Компьюарт. – 2008 – №11. Ч 1 – С 30–32. №12. Ч 2 – С 44 – 47.

3. Пластиковые карты строгой отчетности. (Текст) // Курсив. – 2005 – №6 (ноябрь-декабрь). – С 66 – 69.

4. Гудилин Д. Современные устройства каплеструйной печати. (Текст) / Д. Гудилин // Компьюарт. – 2008 – №1. – С 50 – 55.

5. Печать с защитой. Sicherheitscdruck bei Muller Martini. La Spada Lorena Viscon Print +Commi, 2009, 12, № 12. С.32.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗСУ)
Живило Є.О. (ВІТІ НТУУ „КПІ”)

ТАНДЕМНІ ДЕЦИМАТОРИ З БАГАТОКАСКАДНИМИ I/Q-ДЕМОДУЛЯТОРАМИ

Запропонований в [1] спосіб додаткового стробування (децимації) відліків аналого-цифрових перетворювачів (АЦП) дозволяє забезпечити знижений рівень бічних пелюсток амплітудно-частотної характеристики (АЧХ) приймальних каналів цифрових засобів зв’язку за рахунок використання попередньої квадратурної (I/Q) демодуляції напруг сигналів. Крім того, така тандемна схема формування квадратурних складових сигналів при одноканальному АЦП (рис. 1) дозволяє спростити вимоги до побудови аналогового тракту, що особливо важливо для здешевлення розробки цифрових антенних решіток в системах MIMO. Разом з тим, обмеженням розглянутого в [1] варіанту обробки сигналів (рис. 1) є застосування лише двох каскадів I/Q-демодуляції.

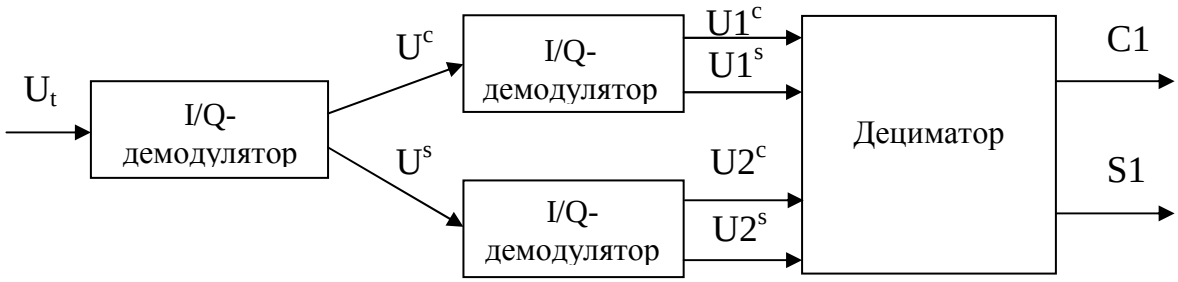


Рис. 1 Тандемна схема дециматора із 2-каскадною I/Q-демодуляцією

Метою доповіді є подальше удосконалення тандемної схеми децимації відліків АЦП за рахунок збільшення в ній кількості каскадів I/Q-демодуляції напруг сигналів.

За основу пропонованого рішення було взято відомий з [2] метод багатокаскадної I/Q-демодуляції, використавши аналогічно [2] в якості каскадоутворюючого сегменту схему, представлену на рис. 2. Зазначений каскадоутворюючий сегмент має бути інтегрованим необхідну кількість разів у розрив між першим та другим каскадами схеми, поданої на рис. 1. Як результат це дозволяє отримати тандемний дециматор, наведений на рис. 3, що ілюструє принцип нарощування кількості I/Q-демодуляторів у складі дециматора. Як видно, другий та третій каскади схеми на рис. 3 є ідентичними, тоді як перший та четвертий її каскади повторюють відповідно перший та другий каскади I/Q-демодуляторів тандемної схеми з рис. 1.

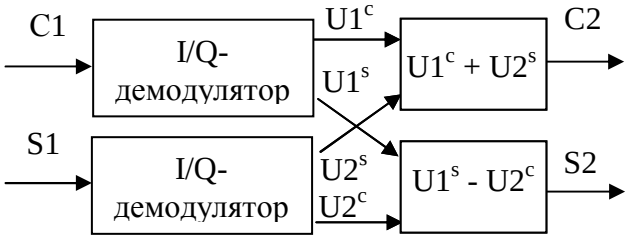


Рис. 2. Каскадоутворюючий сегмент для формування багатокаскадного I/Q-демодулятора

За результатами математичного моделювання було підтверджено, що застосування багатокаскадної схеми I/Q-демодуляції у складі тандемного дециматора дозволяє досягти більш глибокого пригнічення бокових пелюсток АЧХ дециматора. Це позитивно впливає на підвищення завадозахищеності приймальних пристроїв у засобах цифрового зв’язку.

Обробка відліків напруг в останньому каскаді дециматора рис. 3 описується виразами:

$$C2 = A1 + B2,\ S2 = B1 - C2,$$

$$A1_y = \sum_{t=0}^{N-1} \left\{ U5_t^c \cos(\omega_0 \tau t) + U5_t^s \sin(\omega_0 \tau t) \right\},\ A2_y = \sum_{t=0}^{N-1} \left\{ U6_t^c \cos(\omega_0 \tau t) + U6_t^s \sin(\omega_0 \tau t) \right\},$$

$$B1_y = \sum_{t=0}^{N-1} \left\{ U5_t^s \cos(\omega_0 \tau t) - U5_t^c \sin(\omega_0 \tau t) \right\},\ B2_y = \sum_{t=0}^{N-1} \left\{ U6_t^s \cos(\omega_0 \tau t) - U6_t^c \sin(\omega_0 \tau t) \right\},$$

де ω_0 – центральна радіальна частота АЧХ дециматора, τ – період дискретизації АЦП, t – порядковий номер відліків вихідних напруг результатів I/Q-демодуляції.

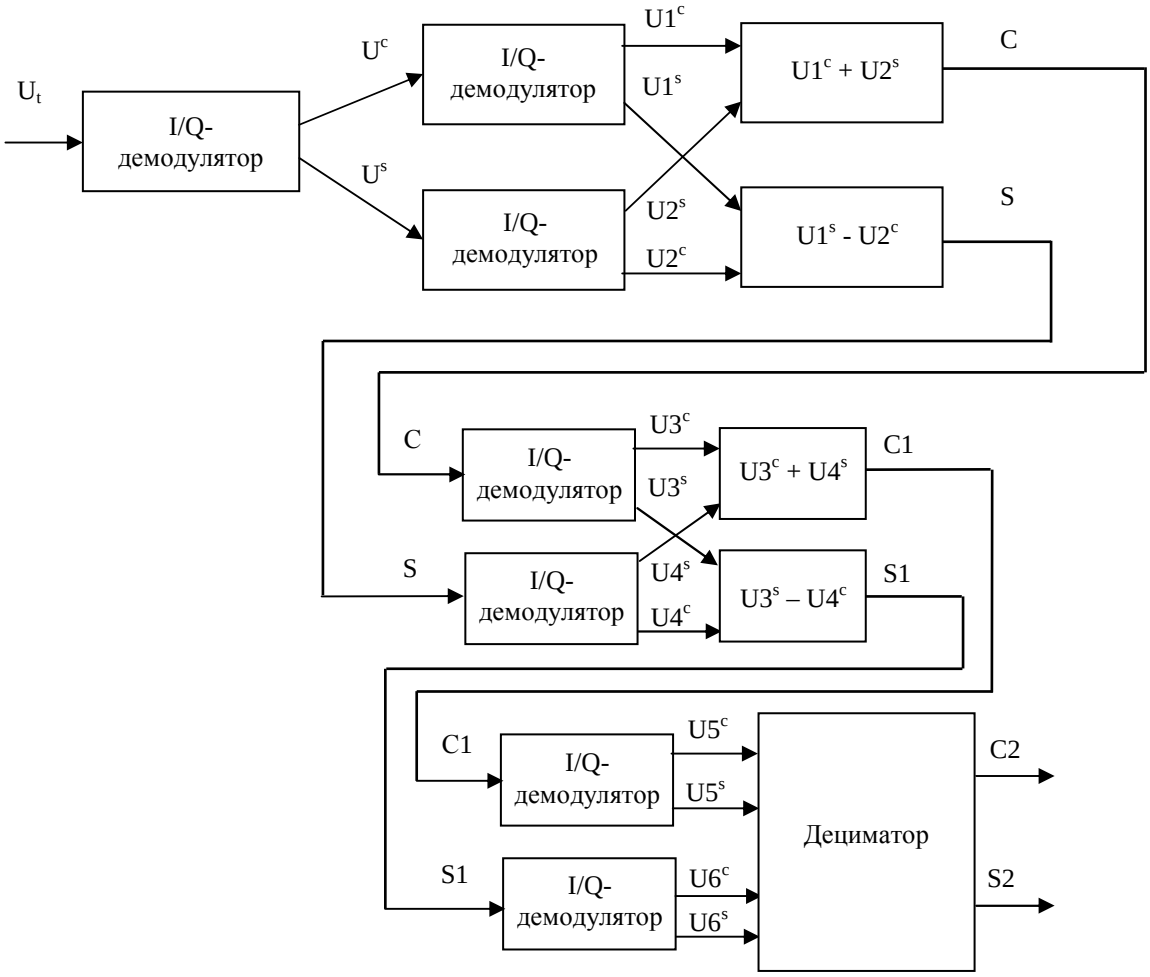


Рис. 3. Тандемна схема дециматора із 4-каскадною I/Q-демодуляцією

Подальші дослідження доцільно зосередити на пошуку шляхів заміни запропонованої у доповіді тандемної схеми дециматора з багатокаскадною децимацією на еквівалентний за формою АЧХ однокаскадний цифровий фільтр.

ЛІТЕРАТУРА

1. Патент України на корисну модель № 66359. МПК G01S 7/36 (2006.01), H03D 13/00 (2006.01). Спосіб додаткового стробування цифрових відліків сигналів. /Слюсар В.І., Копієвська В.С., Живило Є.О. – Заявка на видачу патенту України на корисну модель № u201110521 від 30.08.2011. – Патент опубліковано 26.12.2011, бюл. № 24.

2. Слюсар В.І., Сердюк П.Є. Метод багатокаскадної I/Q-демодуляції сигналів. // VI-й науково-практичний семінар „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення” (20 жовтня 2011 р., доповіді та тези доповідей). – Київ: ВІТІ НТУУ „КПІ”, 2011. – С. 181.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗСУ)
Сердюк П.Є. (ВІТІ НТУУ „КПІ”)

I/Q-ДЕМОДУЛЯТОРИ НЕПАРНОГО ПОРЯДКУ

Потреба у застосуванні завадозахищених засобів зв’язку спонукає до пошуку відповідних за властивостями методів цифрової обробки сигналів. Серед таких методів важливе місце займають квадратурні демодулятори (I/Q-демодулятори), що мають покращені частотно-селективні властивості при обробці відліків аналого-цифрових перетворювачів (АЦП) [1]. Багатокаскадне включення кількох I/Q-демодуляторів парного порядку в [1] дозволяє розширити смугу частот, в якій якість формування квадратурних складових сигналів задовольняє потребам [2], а також збільшити позасмугове пригнічення амплітудно-частотної характеристики (АЧХ), що позитивно впливає на завадозахищеність приймального пристрою. При цьому зменшується динамічний діапазон вагових коефіцієнтів.

В [2] було зазначено, що багатокаскадний I/Q-демодулятор може бути замінений майже еквівалентним за формою АЧХ однокаскадним демодулятором парного порядку, однак пропоновані в [2] варіанти забезпечують таку заміну лише з певним наближенням.

В доповіді пропонується новий клас I/Q-демодуляторів, що мають непарний порядок і дозволяють здійснити тотожну заміну багатокаскадних демодуляторів з парною кількістю каскадів. У загальному випадку, коли всі каскади багатокаскадної схеми I/Q-демодулятора ідентичні, порядок T еквівалентного однокаскадного I/Q-демодулятора може бути визначений відповідно до виразу:

$$T=K\times N - (K - 1), \qquad (1)$$

де K – кількість послідовно включених каскадів, N - порядок окремо взятого каскаду.

Таким чином, при двокаскадному включенні демодуляторів однакового порядку тривалість вибірки для формування відгуку однокаскадного еквівалентного за формою АЧХ демодулятора становить 2N-1 відліків, тобто завжди буде непарною. Це справедливо для послідовного з’єднання не тільки двох I/Q-демодуляторів парного порядку, але й непарного.

Узагальненням виразу (1) на випадок неідентичних за кількістю залучених відліків АЦП каскадів буде формула:

$$T = \sum_{k=1}^{K}\left(N_k - K + 1\right),$$

де K – кількість послідовно включених каскадів, N_k - порядок k-го каскаду.

Наприклад, згідно (1), два 6-відлікових каскади I/Q-демодуляторів з ваговими множниками a=1, b=4, c=3, можна замінити одним 11-відліковим демодулятором (2N - 1= =12 - 1=11 відліків), квадратурні складові якого формуються відповідно до співвідношень:

$$W^S = -(6\,u_1 - 32\,u_3 + 52\,u_5 - 32\,u_7 + 6\,u_9),$$
$$W^C = u_0 - 17\,u_2 + 46\,u_4 - 46\,u_6 + 17\,u_8 - u_{10}. \qquad (2)$$

Істотно, що синтезований двокаскадним включенням демодуляторів парного порядку еквівалентний однокаскадний I/Q-демодулятор (2) має непарний порядок, а також асиметричні вирази для формування відгуків квадратурних складових: одна з квадратур має парну кількість відліків, а інша – непарну, задіяні різні за величиною коефіцієнти). Однак усередині окремо взятої квадратурної складової коефіцієнти мають симетрію відносно центру вибірки, а їхня знакозмінна сума дорівнює нулю. Крім того, однаковою є й кількість вагових коефіцієнтів, що використовуються для формування квадратурних складових (у цьому випадку їх три на квадратуру). Всі вказані ознаки характеризують новий клас I/Q-демодуляторів, що мають непарний порядок і синтезуються двокаскадним з’єднанням I/Q-демодуляторів парного або непарного порядків.

АЧХ, що відповідають 11-відліковому демодулятору (2) і його двокаскадному еквіваленту, наведені на рис. 1, 2 у позиції 2. Штрихова лінія 1 ілюструє АЧХ однокаскадного I/Q-демодулятора 8-го порядку. Нижня (штрихпунктирна) лінія (позиція 3)

відповідає 16-відліковому I/Q-демодулятору з коефіцієнтами, розрахованими по одній незалежній змінній [2].

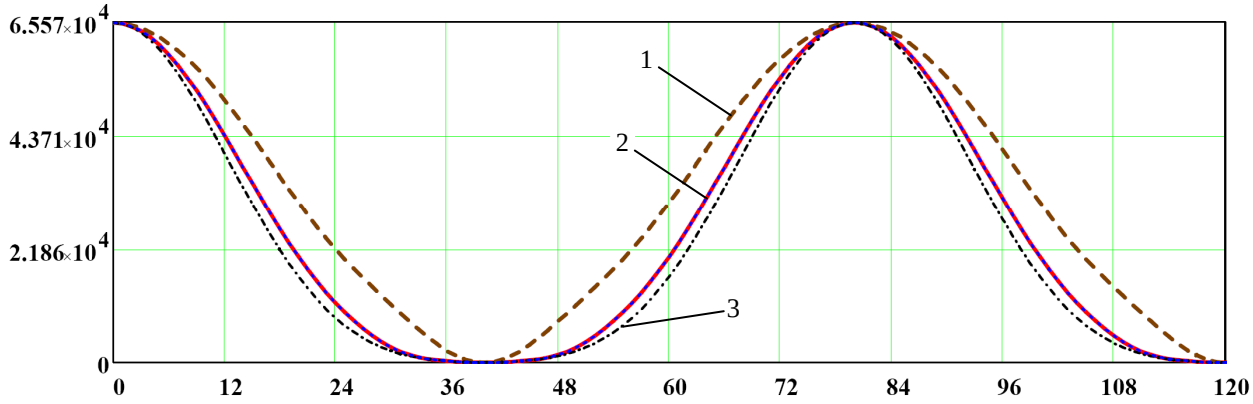


Рис. 1. АЧХ I/Q-демодуляторів 8-го (лінія 1), 11-го (2) (лінія 2) і 16-го порядків

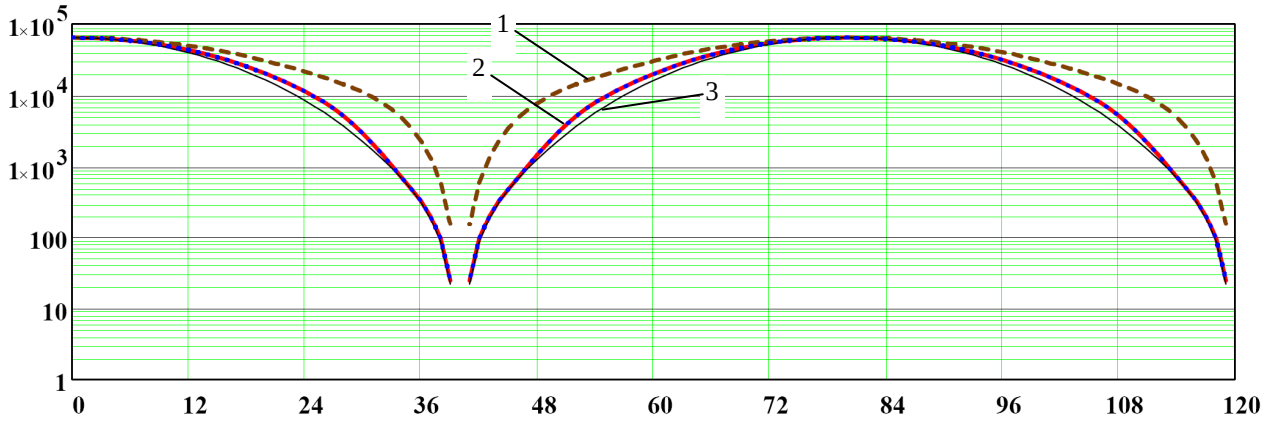


Рис. 2. Логарифмічний вид графіків АЧХ, наведених на рис. 1

Надалі необхідно дослідити можливість синтезу демодуляторів непарного порядку на основі розрахунку вагових коефіцієнтів шляхом рішення системи рівнянь, аналогічно методиці, запропонованій в [3] для синтезу I/Q-демодуляторів парного порядку. Така методика має розширити асортимент синтезованих I/Q-демодуляторів і дозволить одержати набори вагових коефіцієнтів, що забезпечують поліпшене пригнічення позасмугового прийому сигналів.

ЛІТЕРАТУРА

1. Слюсар В.І., Сердюк П.Є. Метод багатокаскадної I/Q-демодуляції сигналів. // VI-й науково-практичний семінар „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення” (20 жовтня 2011 р., доповіді та тези доповідей). – Київ: ВІТІ НТУУ „КПІ”, 2011. – С. 181.

2. Слюсар В.И., Сердюк П.Е. Сравнение одно- и двухкаскадной схемы цифровой I/Q-демодуляции. // V Международный научно-технический симпозиум „Новые технологии в телекоммуникациях” (ГУИКТ-Карпаты '2012). 17 – 21 января 2012 г. – Карпаты, Вышков.- С. 29 – 31.

3. Слюсар В.И., Методика синтеза I/Q-демодуляторов произвольной размерности./ Слюсар В.И., Малярчук М.В., Бондаренко М.В.// III-й Міжнародний науково-технічний симпозіум „Нові технології в телекомунікаціях”– (ДУІКТКАРПАТИ '2010, с. Вишків). – Київ: Державний університет інформаційно-комунікаційних технологій.– 2 – 5 лютого 2010. – С. 53 – 55.

Смірнягін А.Є. (ВІТІ НТУУ „КПІ”)
к.т.н. Нестеренко М.М. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ DDOS – АТАКАМ У КОРПОРАТИВНИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У зв’язку з бурхливим розвитком інформаційних технологій та використанням автоматизованих систем управління в різних сферах людської діяльності, актуальність питань захисту інформаційних ресурсів та комп’ютерних мереж ні в кого не викликає сумнівів. В останній час особливою популярністю користуються так звані *DDos*-атаки (*Denial of Service* – атака типу „відмова в обслуговуванні”) що пов’язано з відносною простотою їх реалізації, але значним деструктивним впливом, що зазнає об’єкт атаки. Одним з основних типів *DDos*-атак є *TCP/SYN-flood*, механізм проведення якого базується на використанні вразливостей протоколу *TCP*.

Методи виявлення *DDos*-атак поділяються на декілька великих груп:

1. Сигнатурні – методи, суть яких полягає у якісній оцінці трафіку, а саме виявленні певних залежностей або аномалій, що властиві початку *DDos*-атаки.
2. Статистичні – методи, засновані на кількісному аналізі трафіку, тобто проводиться моніторинг усього трафіку в мережі на предмет виявлення різких сплесків активності. Особливо, у випадках, коли це не зумовлено об’єктивними причинами.
3. Гібридні (комбіновані) – поєднують в собі переваги обох вище вказаних методів. Однак, при виявленні надмірної та не типової активності, рішення не приймається в той же час, а проводиться більш детальний та глибокий аналіз ситуації, по результатам якого приймається висновок про те, чи мала місце атака.

Існують також механізми, які дозволяють адміністратору мережі програмно зменшити вплив *TCP/SYN-flood* за рахунок: збільшення черги „напіввідкритих” *TCP*-з’єднань; зменшення часу утримання „напіввідкритих” *TCP*-з’єднань; включення механізму *TCP syncookies*; обмеження максимальної кількості „напіввідкритих” *TCP*-з’єднань з однієї *IP*-адреси до конкретного порту.

Однак, головними недоліками існуючих систем захисту, що реалізують вище вказані методи та механізми протидії є те, що вони мають велику собівартість не лише закупівлі, а їх супроводження. Крім того, дані системи в основному працюють по принципу відсікання запитів по інтенсивності, без перевірки їх легітивності. В наслідок цього, якість обслуговування користувачів, щодо доступності та часу відклику мережевих служб не враховується.

В зв’язку з вище прведеним, пропонується розробка аналітичної моделі, на базі якої буде проводитись оцінка ймовірності проведення *TCP/SYN-flood*-атаки з врахуванням забезпечення якості обслуговування користувачів в залежності від продуктивності апаратних засобів та можливостей програмного забезпечення. В її основі буд знаходитись математична модель, що враховує особливості середовища, а саме ймовірнісна модель для багатоканальних систем масового обслуговування змішаного типу з обмеженим буфером.

Це пояснюється тим, що внаслідок всплесків інтенсівності *TCP*-запитів при проведенні *TCP/SYN-flood*-атаки на перше місце виходить питання відмови в обслуговуванні через брак ресурсів буфера контролю та зберігання діючих *TCP*-з’єднань. Тобто, відмова наступає при відсутності вільних місць в черзі згідно теорії систем масового обслуговування.

При комплексному використанні запропонованої аналітичної моделі та механізмів протідії дозволить зменшити деструктивний вплив *TCP/SYN-flood* та провести обґрунтований розрахунок основних параметрів програмного забезпечення відповідних мережевих служб з врахуванням ймовірності обслуговування.

к.т.н. Сова О.Я. (ВІТІ НТУУ „КПІ”)
Уманець Я.Л. (ВІТІ НТУУ „КПІ”)
Клименко М.О. (ВІТІ НТУУ „КПІ”)

МЕТОДОЛОГІЯ СИНТЕЗУ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ УПРАВЛІННЯ ВУЗЛАМИ ПЕРСПЕКТИВНИХ МОБІЛЬНИХ РАДІОМЕРЕЖ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ ВІЙСЬКАМИ

Розвиток сучасних телекомунікаційних систем та мереж характеризується широким використанням безпроводових технологій, які надають користувачам доступ до необхідної інформації та сервісів за принципом „в будь-якому місці, в будь-який час”. Не є винятком і мережі спеціального призначення, які використовуються у разі надзвичайних ситуацій, стихійних лих чи у військовій сфері, зокрема в тактичній ланці управління військами. Прикладом таких мереж є радіомережі класу Ad-Hoc та Mobile Ad-Hoc Networks (так-звані мобільні радіомережі, МР) [1], які передбачають відсутність базових станцій та фіксованих маршрутів передачі інформації, а також надають можливість мобільним абонентам (вузлам) самоорганізовуватися в радіомережу без завчасно розгорнутої мережевої інфраструктури.

Однак, реалізація зазначених особливостей МР вимагає наявності системи управління у складі кожного мобільного вузла, здатної приймати рішення в умовах невизначеності, викликаних непередбачуваною природою середовища в якому функціонують МР, а також різними вимогами до передачі того чи іншого типу трафіка. У відповідності з класичним підходом до побудови автоматизованих СУ – основними складовими СУ вузлом МР є: апаратне, програмне (математичне) та інформаційне забезпечення.

Як показує проведений аналіз, сьогодні існує велика кількість праць, спрямованих на розробку алгоритмів, методів та методик, що відносяться до того чи іншого виду забезпечення СУ. Так, з метою реалізації здатності вузлів самоорганізовуватися в радіомережу та функціонувати в умовах невизначеності в [2] запропоноване застосування технологій обробки знань для „інтелектуалізації” процесів управління ресурсами МР, а також представлена узагальнена модель інтелектуальної системи управління (ІСУ) вузлом МР, яка складається з бази знань про стан вузла та МР, а також множини функціональних підсистем. Також в [3] авторами запропонована низка „інтелектуальних” методів управління ресурсами МР, використання яких передбачається в різних функціональних підсистемах вузлової СУ. Таким чином, як видно із вищезазначеного, на сьогодні спроби створення СУ вузлами МР носять фрагментарний характер, а задачі розробки методів управління ресурсами МР вирішуються відокремлено для кожної підсистеми вузлової СУ та на різних рівнях еталонної моделі OSI. Крім того, відсутність стандартизованого визначення „інтелектуалізації” управління і, разом з тим, системного підходу та єдиної концепції створення ІСУ вузлами радіомереж класу Ad-Hoc робить *наукову проблему*, повязану з розробкою методології синтузу ІСУ вузлами перспективних МР (далі методологія), *актуальною* на сьогоднішньому етапі розвитку безпроводових технологій.

Відповідно до загального визначення методології наукових досліджень, складовими запропонованої методології синтезу ІСУ є:

1. Об’єкт та предмет наукового дослідження;
2. Математичний апарат для створення ІСУ (для забезпечення здатності вузлової СУ функціонувати в умовах невизначеності);
3. Концептуальна модель внутрішньої організації ІСУ вузлом МР;
4. Концептуальна модель ієрархічної побудови ІСУ МР (рис. 1);
5. Множина інтелектуальних методів та методик управління, які відносяться до різних рівнів моделі OSI.

Враховуючи умови функціонування вузлів МР, які характеризуються невизначеністю, а також, беручи до уваги те, що різними вузлами радіомережі доводиться вирішувати суміжні

завдання управління, пропонується методи та методики управління радіомережею реалізувати у вигляді множини інтелектуальних агентів (ІА), котрі знаходяться в кожному вузлі МР. ІА – програмний продукт, здатний діяти в інтересах поставленої мети і володіти наступними властивостями: активність; мобільність; кооперованість і можливість комунікації з іншими агентами; сумісна робота на досягнення загальної мети. При цьому, головною властивістю ІА є інтелектуальність – здатність до самонавчання, логічної дедукції чи конструювання моделей навколишнього середовища для знаходження оптимальних способів поведінки.

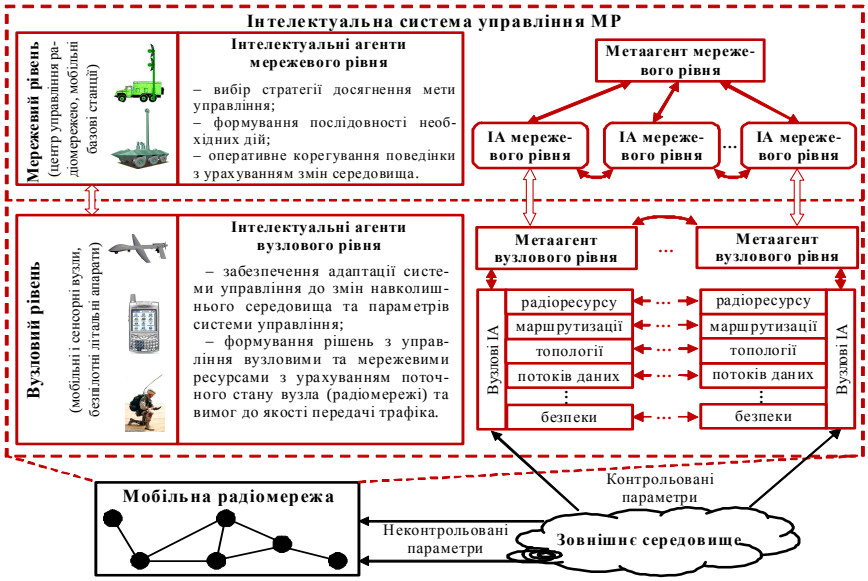


Рис. 1. Модель ієрархічної побудови інтелектуальної системи управління МР

На рис. 1. зображена модель ієрархічної побудови ІСУ, яка передбачає, що на мережевому рівні ІА здійснюють вибір стратегії досягнення мети управління МР (або її зоною), формування послідовності необхідних управляючих впливів для досягнення мережевої (зонової) оптимізації, а також оперативного коригування поведінки елементів радіомережі, виходячи з прогнозованих і планованих змін ситуації. На вузловому рівні інтелектуальними агентами вирішуються завдання управління окремими радіотерміналами або інформаційними напрямками з урахуванням виробленої на мережевому рівні стратегії поведінки мобільних вузлів та МР в цілому.

Таким чином, вперше запропонована методологія синтезу ІСУ вузлами перспективних МР тактичної ланки управління військами дозволить розробити положення системного підходу та створити єдину концепцію побудови вузлових систем управління, в основі якої лежатиме технологія інтелектуальних агентів. В ході подальших досліджень будуть розроблені методи координації взаємодії ІА, які працюють у складі різних вузлів МР.

ЛІТЕРАТУРА

1. Романюк В.А. Мобільні радіомережі (MANET) – основа побудови тактичних мереж зв’язку / В.А. Романюк // IV Науково-практичний семінар ВІТІ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”. – К.: ВІТІ НТУУ „КПІ”. – 2007. – С. 5 – 18.

2. Романюк В.А. Интеллектуальные самоорганизующиеся радиосети: сборник тезисов докладов и выступлений участников XXI Международной Крымской конференции [„СВЧ-техника и телекоммуникационные технологии”], (КрыМиКо). / Романюк В.А., Сова О.Я., Жук П.В. – Севастополь, 2011. – С. 491 – 492.

3. Самоорганизующиеся радиосети со сверхширокополосными сигналами / [С.Г. Бунин, А.П. Войтер, М.Е. Ильченко, В.А. Романюк]. – К.: НПП „Издательство „Наукова думка” НАН Украины”, 2012. – 444 с.: ил.

Стемпковська Я.А. (ВІТІ НТУУ „КПІ”)
Романюк А.В. (ІТС НТУУ „КПІ”)

УПРАВЛІННЯ СТРУКТУРОЮ НЕОДНОРІДНОЇ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ З ВИКОРИСТАННЯМ РОБОТІВ РЕТРАНСЛЯТОРІВ-МАРШРУТИЗАТОРІВ

Процес функціонування неоднорідних безпроводових сенсорних мереж військового призначення передбачає виконання наступних етапів: планування, розгортання, бойового функціонування тощо. Ефективне функціонування мережі неможливе без відповідної системи управління мережею, яка включає в себе наступні підсистеми: управління мережею, управління енергозбереженням, управління часом життя та управління якістю обслуговування. Етап розгортання безпроводової сенсорної мережі та її бойового застосування передбачає рішення задач детермінованого або випадкового розташування сенсорів на місцевості з метою отримання зв’язної мережі та забезпечення максимальної якості обслуговування. Ця потреба задовольняється створенням неоднорідних (стаціонарних та мобільних) безпроводових сенсорних мереж військового призначення, які повинні вирішувати задачі передачі даних в умовах реального часу.

Метою досліджень є підвищення ефективності функціонування неоднорідної безпроводової сенсорної мережі в умовах ресурсних обмежень. Що передбачає розробку методичного апарату управління структурою неоднорідних безпроводових сенсорних мереж військового призначення із мобільними роботами ретрансляторами-маршрутизаторами, який дозволить оперативно виконувати задачі управління.

Оскільки в процесі бойового функціонування безпроводової мережі відбувається поступовий вихід з ладу окремих стаціонарних сенсорів, а саме, вичерпання їх енергетичних ресурсів. Розгорнута на місцевості неоднорідна безпроводова сенсорна мережа військового призначення втрачає зв’язність між окремими сенсорами, що призводить до неможливості передачі даних адресату окремими стаціонарними сенсорними вузлами мережі.

Для відновлення зв’язності між стаціонарними сенсорами в розгорнутій безпроводовій сенсорній мережі в якості таких додаткових вузлів доцільно використовувати мініатюрні роботи ретранслятори-маршрутизатори, що оснащені одним або декількома комплектами приймально-передавальної апаратури. Застосування цих засобів передбачає побудову та розгортання оновленої безпроводової сенсорної мережі тактичної ланки управління для забезпечення безперервної передачі інформації та максимізації часу життя мережі, тобто максимальної якості обслуговування.

У доповіді пропонується розглянути методики розміщення роботів ретрансляторів-маршрутизаторів в неоднорідній безпроводовій сенсорній мережі військового призначення, які дозволяють вирішити питання оцінки зв’язності вузлів неоднорідних безпроводових сенсорних мереж військового призначення (НБСМ ВП) при випадковому розміщенні сенсорів на полу бою.

Основними завданнями дослідження є:

– аналіз існуючих підходів до застосування, функцій, видів забезпечення НБСМ ВП;

– розробка методики оцінки зв’язності вузлів неоднорідних безпроводових сенсорних мережах військового призначення при випадковому розміщенні сенсорів на полі бою;

– розробка методики оцінки якості обслуговування в неоднорідних безпроводових сенсорних мережах військового призначення із мобільними ретрансляторами;

– розробка методики забезпечення зв'язності в маршрутах передачі неоднорідної безпроводової сенсорної мережі військового призначення із мобільними ретрансляторами.

Запропоновані методики дозволяють оцінити не лише зв’язність мережі, з урахуванням мобільності та маневреності роботів ретрансляторів-маршрутизаторів, а й прогнозувати її тривалість.

д.т.н. Субач І.Ю. (ВІТІ НУТУ „КПІ”)
Саєнко О.Г. (ВІТІ НУТУ „КПІ”)
Король М.А. (ВІТІ НУТУ „КПІ”)

АНАЛІЗ ЗАСОБІВ МОНІТОРИНГУ ІНФОРМАЦІЙНИХ МЕРЕЖ ТА ОБҐРУНТУВАННЯ ВИБОРУ ДЖЕРЕЛ ІНФОРМАЦІЇ ДЛЯ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ЇЇ ОПЕРАТИВНОГО ПЕРСОНАЛУ

На сьогодні в галузі інформаційних послуг спостерігається стрімке розширення спектру послуг пов’язаних з інтеграцією та розгортанням інформаційних мереж (ІМ) різноманітного призначення.

Для забезпечення високої якості обслуговування користувачів під час впровадження сучасних інформаційних технологій та надання високотехнологічних інформаційних послуг потрібна відповідна система управління та моніторингу ІМ, у складі якої має функціонувати система підтримки прийняття рішень оперативним персоналом (ОП) ІМ.[3]

Зазначена система має надавати ОП можливість проведення моніторингу і швидкої перебудови мережі, своєчасно знаходити і усувати несправності, забезпечувати розвиток мережі та оперативне підключення абонентів до нових інформаційних послуг.

До числа найбільш популярних програмних засобів моніторингу та управління інформаційними мережами відносяться такі системи, як: *Spectrum* компанії *Cabletron Systems*; *OpenView* фірми *Hewlett-Packard*; *NetView* корпорації *IBM*; *Solstice* виробництва *SunSoft* – підрозділу *Sun Microsystems*; *Multi Router Traffic Grapher (MRTG)* компанії *Activestate*, *Nagios* та інші.[4].

Основними можливостями наведених систем є: автоматичне виявлення пристроїв у мережі; відображення всіх пристроїв на графічній карті; збір і накопичення всіх подій у мережі; надання допомоги ОП у швидкому вирішенні проблеми; збір ключових параметрів роботи мережі для виявляти проблеми, шляхом застосування набору діагностичних утиліт; надання допомоги ОП під час аналізу і планування розвитку мережі, шляхом застосування набору готових звітів; надання доступу ОП з будь-якого місця шляхом застосування *Web*-технологій; керування великими мережами за допомогою розподіленої архітектури та інші.

Проте, всебічну підтримку та управління різнорідним обладнанням (різних виробників) на сьогодні не спроможний забезпечити ні один з проаналізованих засобів. Під час побудови топології мережі, яка складається з обладнання різних виробників, системи управління та моніторингу роблять помилки, приймають одне обладнання за інше, а під час управління ними підтримують тільки їхні основні функції. Додаткові функції зазначені системи просто не розуміють, тому не можуть ними скористатися.[1, 2]

Виходячи з наведеного, можна зробити висновок про те, що жодна з розглянутих систем в повній не задовольняє вимогам до систем управління ІМ військового призначення і потребує проведення низки наукових досліджень у напрямку вдосконалення їхніх можливостей щодо підтримки прийняття оперативних, обґрунтованих рішень ОП ІМ. Дані системи можуть розглядатися, як зовнішні джерела для отримання початкових даних про стан інформаційної мережі для СППР ОП.

ЛІТЕРАТУРА

1. Терелянский, П. В. Системы поддержки принятия решений. Опыт проектирования : монография / П. В. Терелянский ; ВолгГТУ. − Волгоград, 2009. − 127 с.

2. *Power D.J. A Brief History of Decision Support Systems. DSSResources.COM, World Wide Web, http://DSSResources.COM/history/dsshistory.html, version* 2.8, *May* 31, 2003.

3. Стефанюк В.Л. “Інформаційні системи і їх застосування”. – К.:Наука, 1999.

4. Ларичев О. И., Петровский А. В. Системы поддержки принятия решений. Современное состояние и перспективы их развития. // Итоги науки и техники. Сер. Техническая кибернетика. – Т.21. М.: ВИНИТИ, 1987, с. 131 – 164.

д.т.н. Субач І.Ю. (ВІТІ НТУУ „КПІ”)
Саєнко О.Г. (ВІТІ НТУУ „КПІ”)
Рубановська Н.О. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ЕФЕКТИВНОСТІ РОБОТИ ОПЕРАТИВНОГО ПЕРСОНАЛУ ІНФОРМАЦІЙНОЇ МЕРЕЖІ

Аналіз задач оперативного керування (ОК) інформаційною мережею (ІМ) військового призначення показує, що однією з основних задач є вирішення конфліктних ситуацій (КС), які виникають у процесі функціонування ІМ з метою відновлення її нормального функціонування.

Під КС розуміють ситуацію, яка виникає у процесі керування ІМ, яка не може бути вирішена без участі оперативного персоналу (ОП) та є зв’язаною з необхідністю вибору особою, що приймає рішення (ОПР) конкретної альтернативи керування при умові наявності інформації про стан ІМ та її системи керування (СК), вирішальних правил, а також власної системи переваг.

Конфліктні ситуації, які виникають під час функціонування ІМ, характеризуються високим рівнем відповідальності за рішення, що приймається, нестереотипністю та гострим дефіцитом часу на його прийняття.

Основними причинами виникнення КС у процесі функціонування ІМ можуть бути:

Ненадійність елементів ІМ, вихід їх з ладу;

Недосконалість СК, яка дуже часто обумовлюється неповнотою та недостатністю інформації про ІМ, недосконалістю методів та алгоритмів управління, помилками операторів;

Обмеженими можливостями СК ІМ;

Необхідністю СК вирішувати задачі керування в наслідок часткового або повного знищення;

Необхідністю подолання багатозначності, що виникає у процесі керування.

Встановлено, що аналіз інформаційних повідомлень про КС, які виникають у процесі функціонування ІМ відбувається в неавтоматизованому режимі. ОП ІМ аналізує повідомлення про КС та приймає рішення щодо їх вирішення на основі особистого досвіду, кваліфікації та інтуїції. Тому, час який витрачається на аналіз та вирішення КС не відповідає директивному, що негативно впливає на оперативність вирішення задач управління військами у цілому.

Крім того, значний об’єм інформації, що поступає на робочі місця ОП ІМ протягом короткого часу, створює велике психологічне навантаження на нього, що приводить до неправильних дій операторів та помилок у їх роботі.

У наслідок того, що психофізіологічні можливості людини по зберіганню і переробці інформації є обмеженими та не дозволяють їй в умовах дефіциту часу оперативно приймати обґрунтовані рішення тільки на основі її розумової діяльності, то актуальною задачею є автоматизація логіко-аналітичної діяльності ОП ІМ, заснована на використанні методів теорії підтримки прийняття рішень.

Крім того, аналіз показує, що процес функціонування ІМ характеризується одночасною появою декількох КС. Тому виникає необхідність у знаходженні оптимальної послідовності їх вирішення.

У доповіді розглянуто аналіз ефективності роботи ОП ІМ військового призначення. Оптимальне вирішенням КС може бути здійснено за рахунок застосування методики формування плану обробки інформаційних повідомлень про конфліктні ситуації, які відбуваються під час її функціонування.

Судніков Є.О. (НУОУ)
Диба І.О. (НУОУ)
Байдала В.Р. (НУОУ)

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ НАВЧАННЯ В ІНФОРМАЦІЙНІЙ СИСТЕМІ СУПРОВОДУ НАВЧАЛЬНОГО ПРОЦЕСУ

В законі України „Про інформатизацію" та указі Президента № 40 від 21.01.2004 р. „Про затвердження Положення про дистанційне навчання" наголошується на забезпечення розвитку інформаційних технологій у вищих навчальних закладах (ВНЗ), підвищення ефективності системи підготовки фахівців.

Для ВНЗ починається новий етап впровадження новітніх технологій за рахунок автоматизації як навчання так і життєдіяльності загалом.

Стрімкий розвиток технологій спонукає до змін практично в усіх галузях суспільства. Серед них і освітня галузь, яка останнім часом проходить непростий період трансформацій, відбувається бурхливий розвиток і практичне застосування дистанційної освіти в Україні. Разом з тим, суспільство очікує реалізації нової концепції у навчанні „освіта впродовж усього життя".

Стандартні і достатньо статичні п'яти-шестирічні університетські програми не здатні в повноті задовольнити перемінливі вимоги сьогодення. Тому навчання не може завершитися після п'ятого року інституту, воно має тривати і надалі. Технології дистанційної освіти мають зручні механізми підтримки безперервного навчання.

Технічна реалізація інформаційної системи супроводу навчального процесу (ІС СНП) це достатньо складний програмно-апаратний комплекс. З програмним забезпеченням працюють кілька категорій користувачів: викладачі, студенти (курсанти), автори навчальних курсів, адміністратори, деканат (управляє/контролює процес навчання). Для кожної з категорій користувачів ІС СНП необхідно реалізувати свій інтерфейс користувача.

Основними компонентами ПЗ для ІС СНП є:

– засоби розробки навчального контенту (*Authoring tools*);
– система управління навчанням (*CMI* або *LMS*);
– система доставки навчального контенту (веб-сайт).

Найбільш розповсюджені технологічні платформи для ІС СНП: *Microsoft SQL Server*, *IIS*; *JSP* (*Java*), *SQL*; *PHP; Lotus Domino*; *Perl* (*PHP*), *MySQL*, *ILIAS*, *MOODLE*.

Одним з найбільш важливих компонентів ІС СНП є модуль спілкування (комунікацій) між студентами, викладачами та адміністраторами системи. Електронне навчання дозволяє здійснити два вида комунікацій:

– асинхронні – обмін повідомленнями відбувається у довільний час (електронна пошта, форуми, дошки об'яв;

– синхронні – обмін повідомленнями відбуваються в реальному часі (відео- та аудіо-конференції, текстові конференції, сумісне використання додатків, віртуальний клас).

До технічних аспектів ІС СНП можливо віднести: розмежування прав доступу, безпеку, резервне копіювання, можливість розподіленої роботи, облік змін в системі, моніторинг ресурсів та завантаженість системи. ІС СНП висуває обмеження на кількість навчальних курсів, кількість студентів, розмір курсів та тестів, загальну та одночасну кількість користувачів в системі.

Інформаційна система супроводу навчального процесу ILIAS є відкритим вихідним кодом веб-системи управління навчанням (LMS). Вона підтримує управління навчальним контентом (в тому числі відповідність SCORM 2004) і має інструменти для спільної роботи, спілкування, аналізу та оцінки навчання. Інформаційна система може бути запущена на будь-якому сервері, який підтримує PHP і MySQL.

ILIAS – відкрита міжнародна система, що призначена для автоматизації та впровадження елементів дистанційного навчання (ДН) в учбовий процес. ILIAS має засоби для розробки та публікації учбових курсів, дозволяє створювати та керувати студентськими групами, тобто є повноцінною системою дистанційного навчання, що орієнтована на використання мережі Інтернет. Автори курсів можуть утворювати групу для роботи над навчальним модулем. Студенти мають можливість працювати із навчальним матеріалом, а також спілкуватись один з одним (через систему форумів) та з викладачем. ILIAS має наступні базові модулі:

– особистий робочий стіл користувача.

– учбове середовище з персональними налаштуваннями, тестами, глосарієм, функціями друку, пошуковим механізмом.

– засоби спілкування: система новин та форуми.

– система формування груп, що дозволяє встановити необхідні права для доступу до різноманітних ресурсів.

– редактор курсів для авторів.

– контекстно-залежна система допомоги для учнів та авторів.

– загальний інтерфейс адміністрування системою.

Окрім цього є додаткові зручні механізми, що дозволяють вести переписку з групою студентів. Студент зможе легко отримати доступ до необхідного матеріалу, пройти тестові завдання та поставити запитання викладачу.

Орієнтована в основному на:

– молодь, для якої не існує можливості отримати високоякісну освіту через обмежену спроможність традиційної системи освіти;

– осіб, проживання яких віддалене;

– керівників регіональних органів влади та управління, менеджерів різних рівнів;

– офіцерів Збройних Сил, що скорочуються, та членів їх сімей;

– осіб, які проходять дійсну службу в Збройних Силах;

– осіб, що бажають здобути нові знання або другу освіту.

Проведений аналіз застосування інформаційної системи супроводу навчального процесу у ВНЗ дозволив сформулювати основні вимоги щодо впровадження та використання їх у навчанні. Розглянуті технічні аспекти реалізації навчального процесу із застосування новітніх інформаційних технологій дозволяють зробити висновок про розвиток інформаційних технологій та підвищення ефективності навчання слухачів.

ЛІТЕРАТУРА

1. Браун М., Ханикат Д., Стандарти дистанційного навчання. – СПб.: “BHV”, 2003. – 95 с.

2. Bryan Chapman, Sue O. Hall. LCMS 2004-2005 Report: Comparative Analysis of Enterprise Learning Content Management Systems. Published June 2004 905 pages.

3. Richard Nantel. Live E-Learning 2004: Virtual Classrooms, Synchronous Tools, and Web Conferencing Systems. Version 1.1. Published May 2004. 422 pages. www.websoft.ru/db/wb/doc.html

4. Bryan Chapman, and the staff of brandon-hall.com. E-Learning Simulation Products and Services 2004. Published September 2003. 725 pages.

5. Ратшиллер Т., Геркен Т. PHP 4 Разработка Web-приложений. – СПб.: “Питер”, 2001. – 245 с.

6. www.distance-learning.ru/db/el/doc.html.

7. http://www.ilias.de/docu/goto.php?target=cat_581&client_id=docu.

Сьомко О.Ф. (ВІТІ НТУУ „КПІ”)
Марчевський Р.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Раєвський В.М. (ВІТІ НТУУ „КПІ”)

МНЕМОНІЧНА СХЕМА ЕКСПЛУАТАЦІЇ РАДІОСТАНЦІЇ Р-002

Більша частина радіозасобів випуску колишнього Радянського Союзу передбачала в конструкції радіостанції короткої інструкції щодо встановлення основних параметрів, які, як правило, розташовувались на транспортних кришках корпусу радіостанції. Вказане дозволяло операторам станцій, маючи уміння та навички за одним типом радіозасобів – налаштовувати інші, що спрощувало процес підготовки відповідних фахівців. Особливо зазначене набуло поширення під час запровадження комплексів радіозв’язку „Арбалет” та „Акведук” колишнього Радянського Союзу [1]. На даному етапі розвитку радіозасобів з’являються нові радіостанції, які допомагають обмінюватись інформацією з більшою швидкістю, на довші відстані та з кращими коефіцієнтами завадо захищеності (режим псевдовипадкового перелаштування робочої частоти та наявність маскиратора мови). Радіозасоби останніх поколінь є досить надійною та високопродуктивною технікою [2]. Висока продуктивність та надійність зв’язку забезпечується завдяки новому програмному забезпеченню та застосуванням новітніх технологій. Це позитивно впливає на розвиток радіозв’язку в Україні, але недоліком залишається недостатність технічної документації та керівництв по експлуатації радіозасобів. Завдяки великим об’ємам літератури, у солдатів строкової служби може виникнути незручність у освоєнні певних радіостанцій.

Радіостанції п’ятого покоління вітчизняного виробництва передбачають більш підготовлений особовий склад, який їх експлуатує та не мають вищезазначеної інструкції на корпусі станції щодо встановлення основних параметрів. Експлуатаційна документацій має великий об’єм матеріалу, який тяжко сприймається. Основну кількість складає технічний опис радіостанцій, тактико-технічні характеристики, вимоги щодо зберігання та транспортування станції, склад апаратури та нормативи по розгортанню.

Отже, виникає проблема в настройці радіостанцій п’ятого покоління у особового складу строкової служби, який не має можливості в ознайомленні з інструкціями по експлуатації даних радіозасобів. Або у якого недостатній рівень загальної освіти що не дозволяє опанувати матеріал з інструкції по експлуатації.

Вирішенням даної проблеми, є розробка мнемонічної схеми експлуатації та таблиці встановлення основних параметрів радіозасобів вітчизняного виробництва ТОВ „Телекарт-Прилад”. Зазначимо, що мнемоніка – це сукупність прийомів та способів, які полегшують запам’ятовування необхідної інформації шляхом створення асоціацій. За допомогою даної таблиці, встановлення основних параметрів (робоча частота, вихідна потужність, вид модуляції, тип кінцевого засобу, наявність маскиратора мови) буде проводитись набагато швидше. Розробивши та промислово виготовивши дану таблицю, її може бути розміщено на корпусі радіостанції. Провівши статистичні випробування по настройці вказаної радіостанціями операторами різних категорій (що вивчили інструкцію по експлуатації та ті що користуються мнемонічною схемою) можна вказати на ефективність її застосування що полягає в зменшенні часу для засвоєння порядку настройки радіостанції та вивчення її експлуатаційних можливостей.

ЛІТЕРАТУРА

1. Єрохін В.Ф., Раєвський В.М. Прогнозування основних характеристик перспективних радіостанцій силових структур // Зв’язок. – 2005. – №3. – С. 61 – 64.

2. Радіостанція УКХ носима 2Вт. Р – 002. Посібник по експлуатації: ААНЗ. 464424. 020 РЭ – Одеса., 2007. – 116 с.

к.т.н. Терновой М.Ю.(ІТС НТУУ „КПІ”)

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ З ВИКОРИСТАННЯМ АГЕНТНИХ ТЕХНОЛОГІЙ

Стрімкий розвиток глобальних інформаційно-телекомунікаційних мереж обумовлює необхідність зміни підходів до інтеграції та використання інформаційних ресурсів та сервісів. При цьому спостерігаються тенденції до винятково розподіленої схеми створення, підтримки й зберігання інформаційних ресурсів, які, як правило, є складовими частинами гетерогенних автоматизованих систем [1]. Існуючі підходи до інтеграції таких систем вимагають переробки або зміни існуючого програмного забезпечення [2], що потребує значних фінансових витрат. Отже, актуальною є задача інтеграції інформаційних ресурсів, що є частинами існуючих автоматизованих систем, яке не буде вимагати зміни цих систем.

Поставлену задачу в загальному випадку неможливо вирішити за допомогою монолітної системи. Рішення задачі, яке пропонується в даній роботі, полягає в інтеграції інформаційних ресурсів за допомогою мультиагентної системи, яка утворена групою взаємодіючих інтелектуальних агентів [3]. Інформаційний простір, який включає інформаційні ресурси та сервіси, можна представити у вигляді абстрактної алгебраїчної системи [4]. Для забезпечення інтеграції інформаційних ресурсів запропоновано використовувати мультиагентну систему, математичне представлення якої має наступний вигляд:

$$U_A =< A, S_A, \Omega_A >,$$

де A – множина програмних агентів;

S_A – відносини в мультиагентній системі;

Ω_A – множина операцій, які можуть виконувати агенти.

Тоді поняття мультиагентного простору можна визначити як розширення інформаційного простору:

$$E_A = E \cup U_A$$

Запропоновану модель було реалізовано у вигляді прототипу мультиагентної системи інтеграції розподілених баз даних. Прототип розроблявся з використанням принципів, які висуваються FIPA [5] до розробки мультиагентних систем. Для розробки використовувалась платформа JADE. Розроблений прототип було практично перевірено для інтеграції розподілених баз даних в корпоративному середовищі інституту телекомунікаційних систем.

ЛІТЕРАТУРА

1. Разработка фундаментальных основ создания распределенных информационно-вычислительных ресурсов. [Електронний ресурс]. – Режим доступу: http://www.ict.nsc.ru/sitepage.php?PageID=14.

2. Mbarka B. Control access policies for distributed resources. [Електронний ресурс]. – Режим доступу: http://www.fisoft1.com/sources/policies_report.pdf.

3. Neruda R. Cooperation of Computational Intelligence Agents, International Symposium on Collaborative Technologies and Systems (CTS'06), 2006. – с. 256 – 263.

4. Филатов В.А. Мультиагентные технологии интеграции гетерогенных информационных систем и распределенных баз данных : Дис. д-ра техн. наук: 05.13.06 / Харьковский национальный ун-т радиоэлектроники. – Х., 2004. – 341л. : рис. – Библиогр.: л. 313 – 336.

5. FIPA Agent Management Specification. [Електронний ресурс]. – Режим доступу: http://www.fipa.org/specs/fipa00023/SC00023K.html#_Toc75951006.

к.т.н. Ткаченко А.Л. (ВІТІ НТУУ „КПІ”)
Михайлов О.В. (ВІТІ НТУУ „КПІ”)
Шемендюк О.В. (ВІТІ НТУУ „КПІ”)

МОДЕЛЮВАННЯ НЕЧІТКОГО РЕГУЛЯТОРА З БАГАТОКАЛЬНОЮ НАСТРОЙКОЮ ДЛЯ СИСТЕМИ СТАБІЛІЗАЦІЇ БАЛІСТИЧНОЇ РАКЕТИ ЗА КУТОМ ТАНГАЖУ

Актуальність технології нечіткого моделювання обумовлена складностю математичних моделей реальних систем. Традиційні методи побудови моделей не приводять до задовільних результатів, коли початковий опис, що підлягає вирішенню проблеми, свідомо є неточним і неповним. Прагнення отримати вичерпну інформацію для побудови математичної моделі складної реальної системи часто в принципі неможливе. У цих випадках доцільно використовувати методи спеціально орієнтовані на побудову моделей, що враховують неповноту і неточність початкових даних. Саме у таких ситуаціях технологія нечіткого моделювання виявляється найбільш конструктивною.

Балістична ракета, у якої використовується велика кількість локальних систем автоматичного управління, є суттєво нестаціонарним об’єктом управління. Передаточні функції, які описують балістичну ракету як об’єкт управління, відрізняються від передаточних функцій крилатих літальних апаратів тим, що мають нестійкі ланки, тому рух некерованої ракети за програмною траєкторією був би нестійкий. У доповіді розглядається система стабілізації балістичної ракети за кутом тангажу (за каналом продольного руху).

Система складається з наступних функціонально необхідних елементів: елемент порівняння (вільного гіроскопу з потенціометричним датчиком, який характеризується відповідним коефіцієнтом), підсилювача з відповідним коефіцієнтом підсилення, та гідравлічного рульового механізму.

Прийняв за вихідну координату ракети кут тангажу, а за вхідну координату кут повороту руля визначимо передаточну функцію ракети. Залежність параметрів ракети від часу її польоту приведена в роботі Лебедева А.А. та Карабанова В.А. „Динамика систем управления беспилотными летательными аппаратами”.

Використавши інтерактивну систему MATLAB складемо математичну модель ракети та функціональну схему нечіткого регулятора з багатоканальною настройкою.

При використанні тільки одного каналу (звичайного нечіткого регулятора) в системі управління ракетою по куту тангажу в перебігу всього польоту ракети не вдається отримати такої якості системи, як при використанні багатоканального регулятора. Хоча стійке стеження по заданому куту тангажу цей регулятор забезпечує (складає 4% від амплітуди вхідної дії), але перехідний процес - коливальний, з перерегулюванням більше 50%, часом регулювання більш 20с і повільним загасанням. Таким чином, наявність багатоканального нечіткого регулятора дозволяє проектувати систему управління таким істотно нестаціонарним об'єктом як балістична ракета з вельми високою якістю управління (що характеризується аперіодичним перехідним процесом з малим часом регулювання і малою помилкою розузгодження при відпрацюванні програмної траєкторії польоту ракети). Тому застосування нечіткого регулятора для такого об'єкту управління є доцільним і перспективним. Аналізуючи роботу нечітких регуляторів на основі алгоритму „мінімаксного” нечіткого виведення Мамдані, відзначимо наступний факт. Вхідні параметри регулятора на єдиній універсальній множині можна визначити як *активні*, зміна яких впливає на результуючу функцію приналежності, а значить, і на вихідний параметр, і як *пасивні*, зміна яких не впливає на результуючу функцію приналежності, а значить, і на вихідний параметр .

При синтезі даних регуляторів (що забезпечують максимальну швидкодію або максимальну точність відпрацювання вхідного сигналу) використання замість трикутних функцій приналежності експоненціальних, гаусових, Z- і S-функцій часто дає кращі результати.

Толкачов В.С. (НУОУ)

ПИТАННЯ ЩОДО ВОЄННО-ЕКОНОМІЧНОЇ ОЦІНКИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНАХ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ)

Масштаби застосування інформаційних технологій стали такі, що поряд з проблемами продуктивності, надійності та стійкості функціонування інформаційно-телекомунікаційних систем (ІТС), виникають проблеми захисту циркулюючої в ній інформації від несанкціонованого доступу. Наявність можливостей несанкціонованого доступу до інформаційних ресурсів породжує низку інших порушень на цій основі – нецільового використання інформації для інших зловмисних дій і таке інше.

Необхідно пам'ятати, створення комплексної системи захисту інформації (КСЗІ) здійснюється, виходячи з установленого порядку функціонування ІТС, потрібного рівня й терміну захисту інформації та наявних можливостей щодо реалізації різних заходів.

Але разом з тим є необхідність щодо раціональної організації проведення проектних робіт із створення і експлуатації систем захисту інформації (СЗІ) в органах управління військами (силами) в межах виділеного бюджету.

Об'єктом воєнно-економічної оцінки є заходи, що направлені на забезпечення бойової готовності військ і проводяться в структурних ланках Збройних Сил.

Предметом воєнно-економічної оцінки рішень, щодо аналізу сучасних підходів до створення КСЗІ є пошук найбільш ефективних шляхів використання матеріальних, трудових і фінансових ресурсів під час побудови системи, формування різних способів досягнення поставленої мети, всебічний їх аналіз і знаходження найбільш прийнятних варіантів.

Воєнно-економічна оцінка передбачає оцінювання за двома групами показників, одна з яких відображає військовий (бойовий) аспект, інша – економічний (вартісний і часовий) аспект даного варіанту побудови ІТС оперативного угруповання військ (сил) (ОУВ(с)).

Перша група характеризує діяльність, обумовлену об'єктивними потребами практики. До економічного ж аспекту відносяться показники обсягу необхідних або втрачених ресурсів і тривалості досягнення мети. Часовий показник виникає в наслідок неможливості негайного задоволення всіма ресурсами, необхідними для досягнення мети, і миттєвого виконання всіх робіт, що входять до складу заходу. Може бути декілька шляхів досягнення мети. Тому воєнно-економічний аналіз припускає в загальному випадку оцінку за показниками: ефект – витрати – час. При вирішенні деяких часткових задач можлива оцінка тільки по одному або по двом показникам.

Головною метою воєнно-економічного оцінювання є не тільки економія ресурсів за всяку ціну, але і пошук таких варіантів вирішення проблем, які приводять до підвищення ефективності витрачання матеріальних, трудових і фінансових ресурсів.

Залежно від поставленої мети результатом рішення проблеми можуть бути: значення основних показників, що характеризують проектовану інформаційно-телекомунікаційну систему – очікуваного або отриманого ефекту, тривалості його отримання і об'єму необхідних ресурсів (завдання оцінки показників); оптимальний план створення, функціонування та нарощування ІТС ОУВ (завдання оптимізації діяльності).

Але разом з питанням проектування необхідно пам'ятати, що цілями системи захисту інформації є забезпечення необхідних рівнів безпеки інформації в ІТС. Завдання конкретизують цілі стосовно до видів і категорій інформації, що захищається, а також ІТС й відповідають на запитання, що треба зробити для досягнення цілей. Крім того, рівень захисту не можна розглядати в якості абсолютного заходу, безвідносно від збитку, який може виникнути від перехоплення інформації противником.

У якості орієнтира для оцінки необхідного рівня захисту необхідно визначити співвідношення між важливістю інформації, що захищається, і витратами на її захист. Рівень захисту раціональний, коли забезпечується необхідний рівень безпеки інформації й

мінімізуються витрати на її захист, які складаються з витрат на захист інформації $P_{ві}$ та збитку $P_{зі}$ за рахунок перехоплення інформації противником.

Між цими показниками існує досить складний зв'язок, тому що збиток через недостатню безпеку інформації зменшується зі збільшенням витрат на її захист.

Якщо перший показник може бути точно визначено, то оцінка збитку в умовах скритності розвідки й невизначеності прогнозу використання противником перехопленої інформації представляє досить складне завдання. Орієнтовна оцінка збитку можлива при наступних допущеннях.

Від інформації очікується одержати, певний результат, який можливо втратити при її перехопленні противником. Додаткові несприятливі фактори надзвичайно важко піддаються обліку. Тому в якості граничного заходу для оцінки збитку можна використовувати величину потенційного прибутку $P_{пі}$, яку очікується одержати від інформації, тобто: $P_{зі} \geq P_{пі}$.

У свою чергу величина збитку залежить від рівня захисту інформації, обумовленої витратами на неї. Максимальний збиток можливий при нульових витратах на захист інформації, при збільшенні витрат на її захист, імовірність перехоплення інформації противником, а, отже, і збиток зменшуються.

Ріст сумарних витрат на інформацію зі збільшенням витрат на її захист має місце в період створення або модернізації системи захисту інформації, коли відбувається нагромадження заходів і засобів захисту, які ще не виявляють істотного впливу на безпеку інформації. Наприклад, запобігання витоку інформації по окремих каналах без зниження ймовірності витоку по всіх інших не приводить до помітного підвищення безпеки інформації, хоча витрати на закриття окремих каналів можуть бути досить істотними. Отже, для ІТС існує певний "критичний рівень" витрат на захист інформації, при перевищенні якого ці витрати забезпечують ефективну віддачу. При деяких раціональних витратах на захист інформації вище критичного спостерігається мінімум сумарних витрат. При витратах нижче раціональних збільшується потенційний збиток за рахунок підвищення ймовірності перехоплення інформації противником, при більш високих витратах – збільшуються прямі витрати на захист.Обмеження системи являють собою людські, матеріальні та фінансові ресурси, які виділяються на захист інформації, а також обмеження у вигляді вимог до системи захисту інформації. Сумарні ресурси зручно виражати в грошовому еквіваленті. Незалежно від ресурсів які виділяються на захист інформації, вони не повинні перевищувати сумарної ціни інформації, яка захищається. Це верхній поріг ресурсів.

Обмеження у вигляді вимог до системи передбачають прийняття таких заходів щодо захисту інформації, які не знижують ефективність функціонування ІТС при їх виконанні. Наприклад, можна настільки посилити організаційні заходи захисту інформації, що поряд зі зниженням можливості її витоку погіршаться умови виконання органами управління своїх функціональних обов'язків. Очевидно, що КСЗІ тим ефективніша, чим менша ймовірність перехоплення інформації розвідкою противника, тим вище ймовірність не отримання її органом розвідки.

Однак, при порівнянні варіантів СЗІ по декільком частковим показникам виникають проблеми, обумовлені можливим протилежним характером зміни значень різних показників: показники ефективності одного варіанту можуть перевищувати значення аналогічних показників другого варіанту, інші навпаки – мають менші значення. Який варіант переважніше? Крім того, важливим показником СЗІ є витрати на забезпечення необхідних значень показників. Тому результати оцінки ефективності захисту по сукупності часткових показників, як правило, неоднозначні.

Для вибору раціонального варіанту шляхом порівняння показників декількох варіантів використовується інтегральний критерій у вигляді відношення ефективність/вартість.

к.т.н. Топольницький П.П. (ЖВІ НАУ)
к.т.н. Фриз .С.П. (ЖВІ НАУ)
Петрожалко В.В. (ЖВІ НАУ)

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВИКОРИСТАННЯ ЛІНІЙНОЇ ТА НЕЛІНІЙНОЇ ЗГОРТОК У СИСТЕМІ ПРИЙНЯТТЯ РІШЕНЬ ЩОДО ПЛАНУВАННЯ КОСМІЧНОЇ ЗЙОМКИ

На сучасному етапі розвитку людства все більше задач вирішуються за допомогою інформаційних систем. До таких систем відноситься і космічна система оптико-електронного спостереження (КС ОЕС).

За допомогою даної системи можна отримувати інформацію про об'єкти, що знаходяться у будь-якій частині земної кулі. На приклад, для вітчизняної КС ОЕС „Січ-2", щоб одержати знімок відповідного району необхідно подати заявку на зйомку до оператора КС.

На основі заявки замовника оператор формує замовлення щодо задіяння космічних засобів, в якому вказується: номер та вид замовлення, код споживача, дата початку та кінця дії замовлення, періодичність знімання, назва району, координати ділянки знімання, спектральні канали, тип підстильної поверхні, мінімально допустимий кут місця Сонця при зніманні, максимально допустимий кут крена космічного апарата (КА) при зніманні, кут тангажа КА при стереозніманні, код станції прийому інформації. Дані параметри можна розділити на три групи.

До першої віднесемо ті з них, що не змінюються в процесі планування, наприклад, номер замовлення, код споживача та ін., до другої групи – ті, які розраховуються і задаються оператором в процесі планування – керовані, до третьої – ті, які можуть бути передбачені, але некеровані оператором, тобто зовнішні умови функціонування космічної системи. Від параметрів другої і третьої групи безпосередньо залежить якість планування знімання заданого району, що в свою чергу впливає на ефективність функціонування космічної системи взагалі.

Різні параметри зйомки на різних витках мають суперечливий характер. До того ж необхідно враховувати досить велику кількість параметрів, що характеризують технічний стан усіх систем КА, наземних станцій управління та прийому інформації, зовнішніх природних та штучних умов.

Тому для ефективного рішення цієї задачі доцільно застосовувати систему підтримки прийняття рішення. Дана система дозволить максимально швидко зібрати, обробити та розрахувати найкращі можливі варіанти застосування космічних засобів, а також представити необхідні дані у зручному вигляді для подальшого прийняття рішення оператором КС.

Але найбільш складною задачею залишається оцінка пріоритетності одних параметрів майбутнього знімка відносно інших для замовника у випадку складних умов. Для цього необхідно, щоб замовник сам оцінив дані параметри, тобто визначив коефіцієнти важливості. Кінцевий результат вибору витка може відрізнятися також і в залежності від механізму, який покладений в основу прийняття рішення (математичного апарату).

Тому метою дослідження є порівняння лінійної та нелінійної згорток для можливості та доцільності їх використання у системі прийняття рішень щодо планування космічної зйомки при узгодженні вимог замовника та можливостей космічної системи. У доповіді наводяться результати відповідного порівняння.

Тучак Є. В. (ВІТІ НТУУ „КПІ”)
к.т.н. Любарський С. В. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ОРГАНІЗАЦІЇ МЕРЕЖЕВОЇ РОЗВІДКИ НА ОСНОВІ МУЛЬТИАГЕНТНИХ ТЕХНОЛОГІЙ ДЛЯ КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В теперішній час інтенсивний розвиток сфери військової діяльності вніс помітні корективи щодо підходів до вибору форм протиборства. Осмислення змін, які відбуваються під впливом інформатизації, призвело до виникнення і швидкого розвитку концепції інформаційної війни. Проблема інформаційного протиборства до сих пір не знайшла свого адекватного відображення в теорії оперативного мистецтва в Україні. Досвід, отриманий збройними силами провідних країн світу під час локальних конфліктів в сфері інформаційної боротьби, безсумнівно, повинен бути використаний в процесі вивчення та реформування Збройних сил України. Тому актуальною проблемою на сьогодні є процес організації та застосування нашими Збройними силами мережевої розвідки, як основного базового та перспективного методу ведення війн в інформаційному просторі.

Основними сучасними технологічними рішеннями в організації мережевої розвідки є наступні:

– мережева технологія „клієнт-сервер”;

– мультиагентні системи;

– локальні системи.

Вибір оптимальної структури інформаційної системи для організації мережевої розвідки пропонується здійснити на основі методів експертного оцінювання, серед яких перевага надається методу аналізу ієрархій. Кінцеві розрахункові результати при застосуванні даного методу свідчать про найбільшу сприятливість та доцільність використання мультиагентних технологій при організації мережевої розвідки.

Мультиагентні системи складаються з безлічі агентів, які між собою взаємодіють та здатні до самонавчання. Для організації процесу розподілу задачі в мультиагентних системах створюється підсистеми розподіленого вирішення проблеми. Процес декомпозиції глобальної задачі і зворотний процес композиції знайдених рішень відбувається під управлінням єдиного „центру”. При цьому мультиагентна система проектується строго зверху вниз, виходячи з ролей визначених для агентів і результатів розбиття глобальної задачі на підзадачі.

Методика організації мережевої розвідки на основі мультиагентних технологій передбачає виконання наступних етапів:

1. Впровадження агенту в об’єкт інформаційного дослідження. На цьому етапі актуальним є реалізація методів приховування процесів та методів саморозповсюдження програмного коду.
2. Встановлення інформаційного з’єднання з агентом за доступними протоколами комунікаційних мереж.
3. Організація аналізу отриманої інформації від агенту з метою узагальнення і якісної підтримки та прийняття рішення за напрямком інформаційного протиборства.

Таким чином, дана технологія у вигляді відповідної програмної реалізації пропонується для впровадження в процес роботи структурних підрозділів кібернетичної безпеки Збройних сил України, на які покладається завдання інформаційного протиборства, з метою використання її для отримання та детального аналізу важливої інформації про противника, здійснення складних розрахунків, швидкого прийняття рішення та, як наслідок, володіння вищою бойовою ефективністю в ході проведення інформаційної боротьби.

д.т.н. Уривський Л.О. (ІТС НТУУ „КПІ”)
Прокопенко К.А.(ІТС НТУУ „КПІ”)

ОЦІНКА ЗАВАДОСТІЙКОСТІ БАГАТОПОЗИЦІЙНИХ СИГНАЛІВ ВЕКТОРНО-ФАЗОВИМ МЕТОДОМ

Традиційно, ймовірність помилки біта (BER) MPSK і MQAM оцінюється за допомогою обчислення ймовірності помилки біта простим обчисленням або низькою/ високою межею [1], або комбінацією обох способів.

Це пов’язано з тим, що точний аналіз ймовірності помилки біта досить часто виявляється складнішим, і зазвичай представляється в незавершеній формі, яку потім необхідно розрахувати чисельно. В літературі [1 – 5] зустрічаються різні співвідношення, рекомендовані для обчислення ймовірності помилки маніпульованих сигналів ($P_{сим}$) і помилки інформаційного символу ($P_{біт}$).

Крім співвідношень, отриманих проф. Фінком Л.М. [2], співвідношення в згаданих джерелах є приблизними [3 – 4], тобто забезпечують належну точність визначення ймовірностей помилок в деякій обмеженій області значень енергетичного параметра h^2, і не задовольняють навіть фізичним змістом ймовірності поза цією областю.У свою чергу, точні результати, отримані проф. Фінком Л.М. [2], відносяться тільки до двох видів маніпуляції: BPSK і QPSK.

Для решти сигналів багатопозиційної фазової маніпуляції (PSK-8 і т.д) загальна ймовірність бітової помилки ототожнюється з імовірністю помилки одного біта. Для отримання точних аналітичних співвідношень для визначення ймовірностей $P_{сим}$ і $P_{біт}$ для більш широкого набору видів маніпуляції, пропонується оригінальний метод, який спирається на фізичні процеси взаємодії корисного сигналу і перешкоди.

При цьому сигнал, перешкода і їх взаємодія відображаються у векторній формі, що й зумовило назву векторно-фазового методу.

В основі методу лежить визначення ймовірності влучення результуючого (сумарного) вектора сигналу і перешкоди в деяку просторово-фазову область, в якій перешкода призводить до неправильного прийому символів багаторазової маніпуляції, і, як наслідок, до помилкового прийому бітів інформації.

Нехай в канал Зв’язку передається сигнал S. Під впливом перешкоди W сигнал S утворює результуючий сигнал r, який приходить на приймач. Якщо результуючий сигнал потрапляє в область реєстрації переданого сигналу, то сигнал приймається вірно, якщо ж результуючий сигнал знаходиться поза областю достовірної реєстрації переданого сигналу, то він приймається невірно.

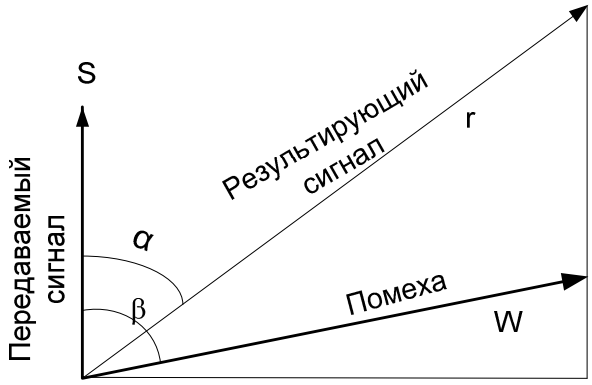


Рис.1. Векторне подання впливу перешкоди на результуючий сигнал

В даному випадку (BPSK), поведінка вектора перешкоди визначається співвідношенням:

$$W(\beta) = \frac{S}{\sin\alpha(ctg\beta - ctg\alpha)} = \frac{S}{-\cos\alpha} \quad (1)$$

В результаті розрахунку ймовірності попадання вектора перешкоди в область, що призведе до неправильного прийому біта інформації (π / 2 <α <π), отримуємо наступну формулу для BPSK:

$$P_{б\_BPSK}(h^2) = \frac{1}{\pi}\int_{\frac{\pi}{2}}^{\pi} e^{-\frac{h^2}{\cos^2\alpha}} d\alpha \quad (2)$$

Розрахунки ймовірності помилки з використанням формули (2) кількісно збігаються з отриманими проф. Фінком Л.М. [2].

Для QPSK розрахунок бітової ймовірності помилки зводиться до знаходження середньої ймовірності помилки по кожному біту.

При використанні кодування Грея, розташування інформаційних біт представлено на рис. 2. Розрахунок бітової ймовірності помилки QPSK зводиться до знаходження середньої ймовірності помилки кожного біта.

Так, для сигналу „00” помилка в першому біті виникне, якщо буде прийнятий сигнал „10” або „11”, а в другому – якщо буде прийнято „01” або „11”.

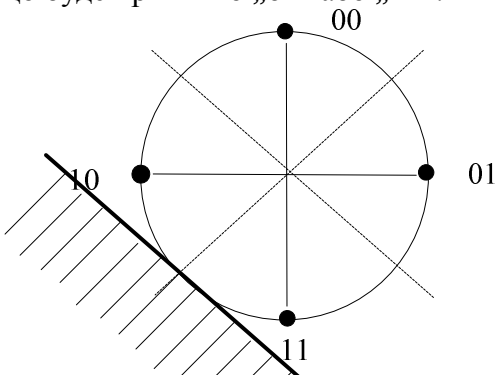


Рис.2 Сигнальний простір QPSK з використанням коду Грея

Область перешкоди, яка призведе до помилки 1го біта символу „00” заштрихована на рис.2. У випадку QPSK, бітові ймовірності помилки 1го та 2го біта будь-якого символу співпадають, і в результаті розрахунків виходить наступна формула:

$$P_{б\_QPSK}(h^2) = \frac{1}{2\pi}\int_{\frac{\pi}{4}}^{\frac{5\pi}{4}} e^{-\frac{h^2}{(\sin\alpha-\cos\alpha)^2}} d\alpha \quad (3)$$

Для випадку PSK-8 бітова ймовірність розраховується як середнє число суми ймовірностей помилок кожного з трьох бітів, що передаються в символі.

Імовірність же бітових помилок 1, 2, 3 біта визначається ймовірністю знаходження вектора перешкода в області, яка призведе до спотворення символ. Середня ймовірність помилкового прийому одиночного біта для випадку PSK-8:

$$P_{б\_PSK8}(h^2) = \frac{2P_{б1\_PSK8}(h^2) + P_{б2\_PSK8}(h^2)}{3}, \quad (4)$$

де $P_{б1\_PSK8}(h^2)$ – ймовірність помилки 1 біта, рівна ймовірності помилки третього біта, $P_{б2\_PSK8}(h^2)$ – ймовірність помилки 3-го біта:

$$P_{б1\_PSK8}(h^2)=\frac{\frac{1}{2\pi}\int\limits_{\frac{\pi}{8}}^{\frac{9\pi}{8}}\int\limits_{\frac{h^2\tan^2(\frac{\pi}{8})}{\left(\sin(\alpha)-\cos(\alpha)\tan(\frac{\pi}{8})\right)^2}}^{\infty}e^{-\eta}d\eta d\alpha+\frac{1}{2\pi}\int\limits_{\frac{3\pi}{8}}^{\frac{11\pi}{8}}\int\limits_{\frac{h^2\tan^2(\frac{3\pi}{8})}{\left(\sin(\alpha)-\cos(\alpha)\tan(\frac{3\pi}{8})\right)^2}}^{\infty}e^{-\eta}d\eta d\alpha}{2}d\alpha \quad (5)$$

$$P_{б2\_ФМ8}(h^2)=\frac{1}{2\pi}\left(\begin{array}{l}\int\limits_{\frac{\pi}{8}}^{\pi}\int\limits_{\frac{h^2\tan^2(\frac{\pi}{8})}{\left(\sin(\alpha)-\cos(\alpha)\tan(\frac{\pi}{8})\right)^2}}^{\infty}e^{-\eta}d\eta d\alpha-\int\limits_{\frac{5\pi}{8}}^{\pi}\int\limits_{\frac{h^2\tan^2(\frac{5\pi}{8})}{\left(\sin(\alpha)-\cos(\alpha)\tan(\frac{5\pi}{8})\right)^2}}^{\infty}e^{-\eta}d\eta d\alpha+\\ +\int\limits_{\pi}^{\frac{13\pi}{8}}\int\limits_{\frac{h^2\tan^2(\frac{5\pi}{8})}{\left(\sin(\alpha)-\cos(\alpha)\tan(\frac{5\pi}{8})\right)^2}}^{\infty}e^{-\eta}d\eta d\alpha-\int\limits_{\pi}^{\frac{9\pi}{8}}\int\limits_{\frac{h^2\tan^2(\frac{\pi}{8})}{\left(\sin(\alpha)-\cos(\alpha)\tan(\frac{\pi}{8})\right)^2}}^{\infty}e^{-\eta}d\eta d\alpha\end{array}\right) \quad (6)$$

Таким чином, перевагою співвідношень, отриманих з використанням векторно-фазового методу, є їх точність.

Результати, отримані за допомогою запропонованого методу, є коректними у всьому діапазоні досліджуваних параметрів, в той час як широко розповсюджені наближені формули є достатньо точними тільки у вузькому діапазоні значень вихідних величин.

Точність аналітичних розрахунків векторно-фазового методу забезпечується за рахунок громіздкість розрахунків чисельного інтегрування, хоча при цьому не містить допущення про їх наближеності.

ЛІТЕРАТУРА:

1. C. M. Chie, Bounds and approximations for rapid evaluation of coherent MPSK error probabilities, – IEEE Trans. Commun., vol. COM-33, pp. 271 – 273, Mar. 1985.

2. Финк Л.М. Теория передачи дискретных сообщений. – 2-е изд., перераб., и доп. – М.: Сов. радио, 1970. – 728 с.

3. Кантор Л.Я. Спутниковая связь и вещание. – М: Радио и связь, 1988.

4. J.G.Prokis, Digital Communication, 3rd ed. New York: McGraw-Hill, 1995.

5. Основи теорії телекомунікацій /Підручник /За заг. ред. проф. Ільченка М.Ю. – К.: 2010. – ІССЗІ НТУУ „КПІ” – с.786, іл.

к-т Усік В.О. (ВІТІ НТУУ ,,КПІ'')
к.т.н. Хусаінов П.В. (ВІТІ НТУУ ,,КПІ'')

ПРОГРАМНИЙ КОМПЛЕКС ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ФАХІВЦІВ КІБЕРНЕТИЧНОГО ЗАХИСТУ

Загрози інформаційній безпеці відомі вже досить давно, але в наш час із пошиоенням інформаційних технологій ця проблема набула нового значення. Зараз відома величезна кількість методів таких атак, і їх число постійно зростає. Ця загроза в повною мірою стосується як глобальної мережі Інтернет, так і корпоративних мереж, адже вони побудовані за схожими принципами. Знання принципів роботи атак є необхідною умовою ефективного захисту від них, але їх значна кількість методів та засобів комп'ютерних атак робить фактично неможливим знання їх усіх однією особою. Існує декілька проектів, які створили власні методи класифікації та аналізу атак на комп'ютеризовані інформаційні системи. До них можна віднести: *CAPEC (Common Attack Pattern Enumeration and Classification), The WASC (Web Application Security Consortium) Threat Classification, SANS*.

Нажаль, жодна з існуючих класифікацій не є універсальною, саме тому актуальною задачею являється створення репрезантативного, розвинутого ресурсу для ефективного інформаційно-аналітичного забезпечення фахівців кібернетичного захисту Збройних сил. При цьому, через відмінність в технологіях та зважаючи на специфіку завдань, що виконуються необхідною умовою являється врахування специфіки функціонування комп'ютерних мереж збройних сил. Адже комп'ютерні мережі військового призначення по своїй суті, являються корпоративними мережами і мають певні відмінності від мережі *Internet*. Це дозволить:

1) на основі аналізу існуючих даних, своєчасно визначити, який тип атаки застосовується;
2) підвищити швидкість вибору методів протидії, які необхідно застосувати в даній ситуації;
3) із появою нових методів віддалених атак, класифікувати їх на основі існуючої інформації;
4) швидко вносити зміни та доповнення до даної класифікації її розробникам;
5) оперативно реагувати на так звані "0-*day*" вразливості, адже для протидії цим вразливостям, хоча б мінімальна інформація про них повинна бути доступна фактично одразу після їх виявлення;
6) проводити підготовку нових спеціалістів, що здатні вести боротьбу у кіберпросторі.

Доцільним є створення такого ресурсу на базі сучасних *Web*-технологій, що дозволитьотримати такі переваги як:

1) практичність та простота у використанні;
2) доступність, адже для користування необхідно мати лише *Web*-браузер (входять в комплект поставки усіх основних операційних систем) та підключення до мережі;
3) сумісність з іншими подібними системами та класифікаціями;
4) кросплатформеність (*Web*-технології підтримуються усіма існуючими платформами);
5) розширення масштабу за рахунок перенесення даних сайтів з інших подібних проектів.

Для реалізації цих задач необхідно провести дослідження та аналіз існуючих систем класифікації атак, вивчити їхні переваги та недоліки, і на основі цих даних створити програмний комплекс інформаційно-аналітичного забезпечення фахівців кібернетичного захисту, придатний для використання у збройних силах та буде доступним для користувачів у режимі *online*.

Фастенков М.С. (ВІТІ НТУУ „КПІ”)
к.т.н. Раєвський В.М. (ВІТІ НТУУ „КПІ”)

ЗАСТОСУВАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ MIXWIN В РАДІОЗАСОБАХ НИЗОВИХ ЛАНОК УПРАВЛІННЯ ДЛЯ ПЕРЕДАЧІ ЦИФРОВОЇ ТЕКСТОВОЇ ІНФОРМАЦІЇ

Провівши аналіз радіозасобів, що знаходяться на озброєнні у ЗСУ, вони мають достатню ефективність, але не задовольняють вимогам сучасних радіозасобів, які є цифровими і здатні передавати цифрову інформацію. Причиною є обмежене фінансування, внаслідок чого продовжують використовуватися радіозасоби II та III поколінь, які морально та фізично застарілі.

Однією з основних видів інформації, що передається по радіоканалам є текстова і яка, до того ж, створена за допомогою ПЕОМ. Засоби нового покоління, наприклад, виробництва ТОВ „Телекарт-прилад” в недостатній кількості надходять у війська і не задовольняють вимогам – в наявності декілька сот при необхідності декількох тисяч. Дані радіозасоби дозволяють передавати цифрову текстову інформацію через підключений до них ПЕОМ з відповідним програмним забезпеченням.

Разом з тим, відсутні відповідні пристрої адаптації комп’ютерних пристроїв та аналогових радіозасобів каналоутворення, які дозволяли б передавати цифрову текстову інформацію по існуючим аналоговим каналам радіозв’язку.

З метою вирішення цієї проблеми для передачі вказаної інформації по існуючим аналоговим каналам зв’язку можна використати програмний продукт MixWin, що знаходить широке застосування у радіоаматорів. Вказаний програмний продукт шляхом з’єднання звукової карти ПЕОМ та аналогового входу каналу тональної частоти в масштабі реального часу здатний передавати текстову цифрову інформацію. MixWin може використовуватися як в режимі дуплекс, так і в режимі симплекс.

Використання програмного продукту MixWin в режимі дуплекс можливе за допомогою радіозасобів комплексу Р-161 (Р-160П та збуджувач „Лазурь”) та спеціального монтажного обладнання, утвореного роз’ємами канальної сторони та виходів типу „джек 3,5”. Але більшість радіозасобів низових ланок управління для ведення радіозв’язку використовують режим сиплекс (в тому числі носимі радіозасоби), при якому необхідно ставити станцію або на передачу, або на прийом. Ця задача вирішується шляхом створення спеціального монтажного обладнання, виходи підключення до ПЕОМ якого, крім лінійних виходів, містить роз’єм COM. Цей роз’єм забезпечує інтерфейс перемикання симплексного радіозасобу передача/прийом та дозволяє MixWin працювати з високою пропускною спроможністю.

MixWin дозволяє вести цифровий текстовий обмін інформацією використовуючи радіозасоби низових ланок управління (Р-159, Р-130, Р-111, Р-161А2М).

При здійсненні порівняльного аналізу вказаного програмного продукту що використовується разом з аналоговими радіостанціями попередніх поколінь з цифровими радіозасобами ТОВ „Телекарт-прилад” (Р-002, Р-005, Р-030) виявлено різницю часу, що витрачається на передачу інформації – до 2-3 хвилин на користь запропонованого методу.

Таким чином, запропоноване впровадження програмного продукту MixWin дозволить передавати текстову цифрову інформацію по існуючим аналоговим каналам зв’язку та підвищити ефективність ведення зв’язку в умовах обстановки мирного та воєнного часу.

Фесьоха В.В. (ВІТІ НТТУ ,,КПІ”)
д.т.н. Шворов С.А. (ВІТІ НТТУ ,,КПІ”)
Чередниченко О.Ю. (НЦЗІ ВІТІ НТТУ ,,КПІ”)

МОДУЛЬ АДАПТАЦІЇ КОМП’ЮТЕРНОЇ СИСТЕМИ НАВЧАННЯ

На сьогоднішній день забезпечення інтенсифікації процесу навчання вирішується застосуванням як окремих тестових і навчальних програм, так і комп’ютерних систем навчання (КСН). Інтелектуальні КСН здатні у тій чи іншій мірі враховувати індивідуальні особливості користувача системи (будувати модель) з метою вибору та представлення для нього найбільш підходящого навчального матеріалу, тим самим забезпечуючи відповідний рівень адаптації.

Поряд із цим питання адаптації КСН до конкретного користувача залишається відкритим, адже взаємодію ,,викладач – студент” або ,,студент – однокурсник” реалізувати досить складно, до того ж функціонування подібних систем орієнтоване на роботу з досить великою кількістю слухачів, тоді як побудована модель певної категорії користувачів може не підійти іншій.

Аналіз існуючих методів адаптації КСН до конкретного користувача показав їх часткову адаптацію до того, хто навчається на основі побудованої моделі, що свідчить про не достатньо високу їх ефективність і, як наслідок інтелектуальність.

Доцільним підходом до вирішення даної проблеми є побудова модулю адаптації КСН, функціональність якого передбачає застосування комбінованого методу адаптації до користувача на основі:

– інтелектуального аналізу рішень (*Intelligent analysis of student solutions*);
– побудови послідовності навчання (*Curriculum sequencing*);
– адаптивного представлення інформації (*Adaptive presentation*).

Функціональність модуля адаптації передбачає застосування першого методу на початковому етапі взаємодії користувача з системою, з метою визначення його рівня знань чи вмінь, аналізуючи відповіді (правильні, не правильні, не повні). Метод інтелектуального аналізу рішень дозволить визначити, що конкретно не знає чи не розуміє студент та забезпечить генерування подальшого ходу взаємодії.

Побудова послідовності навчання здійснюється на основі моделі навчального матеріалу, в якості якої використовується орієнтований граф, де вершинам графу відповідають розділи, теми, а ребрам – зв’язки між ними. Таким чином, відображаються найбільш підходящі методи навчання, які обираються на основі загального рівня підготовки користувача. Так, для найменш підготовлених можна рекомендувати логічні методи, для більш підготовлених – проблемні та пошукові.

Застосування третього методу передбачається на всьому етапі навчання із наданням можливості вибору представлення інформації користувачу у зручному для нього вигляді, з точки зору форми сприйняття (аудіальне, візуальне, кінестичне). До того ж, детальність представлення інформації залежить не тільки від виконання поточних завдань, а й від загального рівня підготовленості.

Побудова модуля адаптації КСН передбачає застосування аналізатора відповідей студента, збереження у базі знань інформації про індивідуальні особливості конкретного користувача та побудову моделі навчального матеріалу.

Таким чином, застосування даного модулю дозволить значно підвищити ефективність КСН, її інтелектуальність, гнучкість та сприятиме підвищенню адаптивних можливостей системи, тобто здатності КСН самостійно вирішувати задачі з предметної області, по якій вона проводить навчання.

к.т.н. Фриз В.П.(ЖВІНАУ)
Орищук І.О.(ЖВІНАУ)

РОЗРОБКА ТА СТВОРЕННЯ ПЕРЕСУВНОГО РАДІОТЕЛЕВІЗІЙНОГО КОМПЛЕКСУ

Досвід проведення психологічних операцій, в останніх військових конфліктах, провідними державами світу продемонстрував тенденцію широкого застосування мобільних радіотелевізійних комплексів. Вони використовувались для виготовлення і розповсюдження відеопродукції для цілеспрямованого формування певних образів, думок, почуттів з метою впливу на свідомість та підсвідомість окремих осіб, груп людей чи населення в цілому. А також для систематичного моніторингу змісту телевізійних каналів противника. Постійна модернізація існуючих та розробка нових зразків з використанням сучасних мультимедійних, супутникових технологій та систем передачі даних забезпечують ефективне використання таких комплексів.

Аналіз останніх публікацій показує, що на озброєнні підрозділів психологічних операцій провідних країн світу знаходяться сучасні мобільні радіотелевізійні комплекси. Основними завданнями, які вони вирішують, є моніторинг телевізійного ефіру та створення і розповсюдження власної відеопродукції різноманітного характеру. Для цього наприклад, підрозділи психологічних операцій армії США мають на озброєнні мобільний медіацентр та радіотелевізійну систему „Bravo”, а також радіотелевізійну систему повітряного базування „Commando Solo”. Служба психологічних операцій Війська Польського використовує комплекс радіотелевізійного моніторингу „Sarna”. Також проведений аналіз показав, що на озброєнні відповідних підрозділів Збройних сил України до недавнього часу були відсутні зразки подібної техніки.

Тому перед авторами було поставлено завдання розробити мобільний радіотелевізійний комплекс, який би дозволив вирішувати питання що до телевізійного моніторингу та створення власної відеопродукції. Для цього були визначені завдання, обґрунтована структура і склад, розроблений проект технічних умов для створення пересувного радіотелевізійного комплексу (ПРТК). Згідно з визначеними для ПРТК завданнями розроблена специфікація апаратури автоматизованих робочих місць. Для реалізації пересувного варіанту комплексу розроблені пропозиції і здійснено технічне супроводження переобладнання автомобілів „Газель”, налагоджено апаратуру, розроблено технічну документацію. ПРТК має наступні можливості:

– моніторинг телевізійного ефіру одночасно по 4 каналах як цифрового супутникового телебачення, так і аналогового ефірного;

– запис до 500 годин телевізійної інформації з трьох каналів на жорсткі диски автоматизованих робочих місць для подальшої обробки;

– створення відеопродукції різноманітного жанру з використанням сучасних комп’ютерних технологій нелінійного відеомонтажу;

– розроблення компонентів комп’ютерної графіки та анімації для використання у відеопродукції;

– отримання високоякісних фотографічних зображень з подальшою обробкою і створенням на їх основі мультимедійних презентацій та слайдів;

– запис фонограм для озвучення відеопродукції.

Результатом роботи є прийнятий ПРТК на озброєння та впровадження зразків у війська.

В доповіді, на основі 5 років експлуатації лабораторного варіанту ПРТК, наведено досвід його створення та експлуатації. Аналізуються реальні можливості комплексу та перспективи для подальшого його вдосконалення.

к.т.н. Хливнюк М.Г. (ЖВІНАУ)
Приймак С.Л. (ЖВІНАУ)

ЦИФРОВЕ ВИМІРЮВАННЯ ФАЗОВИХ ПОМИЛОК СИНХРОНІЗАЦІЇ В КАНАЛІ ЗВ'ЯЗКУ ФАЗОМЕТРИЧНИМ ПРИСТРОЄМ НА БАЗІ МІКРОКОНТРОЛЕРІВ AVR

Однією з існуючих проблем сучасних технологій забезпечення зв'язку є чутливість до помилок синхронізації внаслідок нестабільності фазової характеристики каналу та фазових флуктуацій генераторів, в результаті чого виникає випадковий фазовий зсув, який призводить до викривлень інформаційних повідомлень.

Вирішенням проблеми компенсації фазової помилки є застосування пілот-сигналів та компенсації фазової помилки за рахунок введення зворотного зв'язку в схему системи корекції фази. Ці методи передбачають проведення вимірювання фазових спотворень в каналі зв'язку, що може бути виконано за рахунок фазометричного пристрою побудованого за сучасними технологіями.

Для його побудови в залежності від призначення, технічних характеристик та елементної бази використовуються різноманітні схемні та структурні рішення.

Вибір методу вимірювання кута зсуву фаз залежить від діапазону частот, амплітуди сигналу і необхідної точності вимірювання.

Вимірювання кута зсуву фаз методом безпосередньої оцінки може бути виконане за допомогою фазометрів різних типів. Електронні аналогові фазометри дозволяють вимірювати кут зсуву фаз в діапазоні частот від десятків Гц до одиниць МГц. Відносна похибка складає 1 – 2 %, роздільна здатність приблизно 1^0.

Існуючий стан розвитку елементної бази дозволяє розробити сучасний цифровий фазометр принциповою особливістю якого є програмне керування його параметрами та побудова з використанням мікропроцесору.

Основою для побудови пристрою цифрового фазометра може бути інтегральний мікроконтролер AVR з розвинутою архітектурою і виконанням команд, що потребує короткого їх коду для зчитування за такт.

Особливістю таких мікроконтролерів є використання RISC – архітектури, яка характеризується потужним набором інструкцій, більшість з яких виконується за один машинний цикл, а значить високою швидкодією.

В доповіді розглядається створення сучасного цифрового фазометра з програмним керуванням на базі мікроконтролера AVR, в якому за критерієм мінімальної технічної складності, енергоспоживання та вартості забезпечується похибка вимірювання фазового зсуву $0{,}1^0$ в діапазоні 0,1-100 кГц. Працює фазометр з гармонічними сигналами, які подаються в канал зв'язку в якості пілотних для забезпечення роботи системи корекції фази.

Згідно з алгоритмом роботи фазометр проводить декілька вимірювань за один цикл та визначає тривалість циклу вимірювання, яка повинна бути більшою періоду низькочастотного сигналу в каналі передачі, що забезпечує оперативність та високу точність отримання результату.

Новизною в пропонуємому підході побудови фазометра є використання сучасної елементної бази, що дозволяє організувати роботу цифрового фазометра за гнучким алгоритмом який в подальшому можливо корегувати, надає можливість у відповідності до вимог часу та існуючих технологій проводити поступове оновлення вимірювальних пристроїв, та дає більш точніші оперативні результати самого вимірювання фазової помилки в каналі зв'язку.

к.т.н. Чевардін В.Є. (ВІТІ НТУУ „КПІ”)
к.т.н. Мазулевський О.Є. (ВІТІ НТУУ „КПІ”)

СУЧАСНІ ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В AD HOC МЕРЕЖАХ

Використання радіомереж з динамічною топологією є невід’ємним фактом розв’язання сучасних задач передачі, зберігання та обробки інформації в автоматизованих системах управління критичного застосування. В зв’язку з цим, задачі виявлення та блокування атак на окремі та на групи користувачів суттєво ускладнюється, що потребує додаткових обчислювальних та матеріальних витрат на аналіз загроз безпеки інформації та вдосконалення системи захисту від них. В таких умовах розробка моделі безпеки інформації в сучасних ad hoc мережах є актуальним науково-технічним завданням.

В результаті проведених досліджень були визначені сучасні загрози конфіденційності, цілісності та доступності інформації в мережі ad hoc. Більш розповсюдженими атаками є атаки з порушенням доступності інформації в мережі, які в свою чергу реалізуються з використанням сукупності простих атак: на витрату обчислювальних ресурсів вузлів мережі або на порушення цілісності та справжності маршрутної інформації (рис. 1).

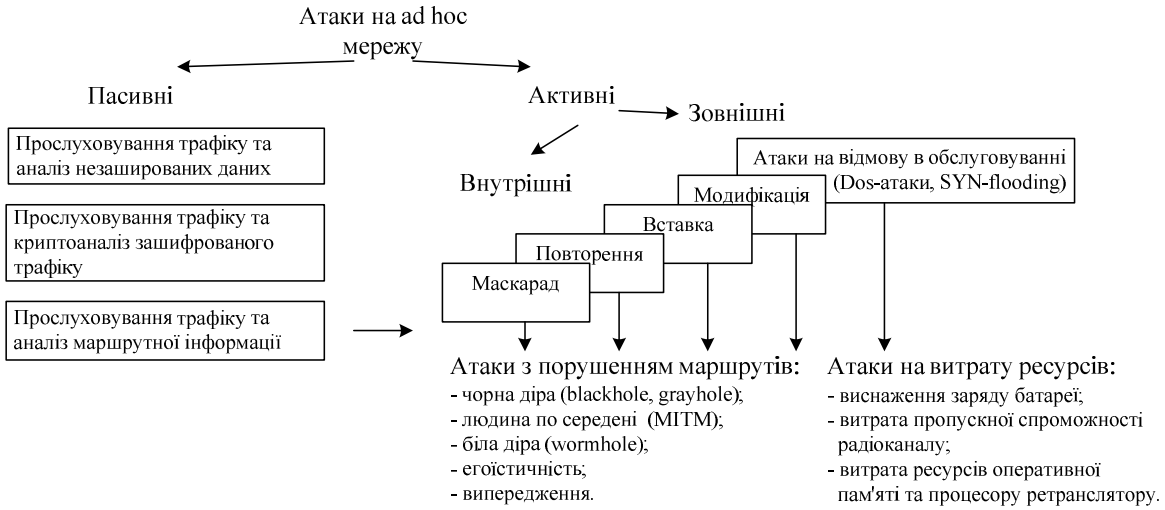


Рис. 1. Атаки на ad hoc мережу

Розроблена модель порушника безпеки інформації дозволяє класифікувати усі можливі види користувачів мережі в залежності від потенційної шкоди на інформацію на п’ять категорій. Визначені можливі негативні впливи на інформацію кожною категорією порушника безпеки інформації. Крім зовнішніх порушників безпеки інформації визначені найбільш потенційно небезпечні категорії внутрішніх порушників: категорія II – зареєстровані користувачі – особи, що мають санкціонований доступ до ресурсів ІТС; категорія III – незареєстровані користувачі – особи, що мають санкціонований доступ до приміщень з розташованими технічними засобами зі складу ІТМ, але не мають санкціонованого доступу до ресурсів ІТС.

На основі моделі порушника визначені етапи проведення будь-якої атаки на інші вузли мережі. Проведено аналіз сучасних механізмів безпечної маршрутизації в мережах ad hoc. Визначені шляхи вдосконалення методів захисту даних та маршрутної інформації в мережах з динамічною топологією. На основі моделі порушника, класифікації та принципів реалізації сучасних атак визначені вимоги щодо моделі загроз безпеки інформації в ad hoc мережі, які відрізняються від існуючих врахуванням особливостей організації та проведення сучасних атак на витрату обчислювальних ресурсів вузлів мережі або на порушення цілісності та справжності маршрутної інформації в мережі ad hoc.

Шевченко А. С. (ВІТІ НТУУ „КПІ”)
Толстих В. А. (ВІТІ НТУУ „КПІ”)

ДИФЕРЕНЦІАЛЬНО-ІГРОВІ МОДЕЛІ ПОВЕДІНКИ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ПРИ РЕАЛІЗАЦІЇ АТАК РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ В ХОДІ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Останні тенденції ведення інформаційних операцій найбільш розвинутими державами показує, що радіоелектронна боротьба (РЕБ), наряду з кібернетичними операціями, залишається найбільш дієвим засобом боротьби в ході бойових дій. Основними функціями РЕБ є радіо/радіотехнічна розвідка (РРТР) та радіоелектронне придушення (РЕП) радіоліній.

Під час проведення інформаційних операцій, основний акцент ставиться на атаки, що реалізують вплив на інформаційно-телекомунікаційні системи (ІТС), які призначені для управління збройними силами, іншими військовими формуваннями та структурами державного управління. В ході інформаційного конфлікту, при реалізації заходів РЕБ вразливою частиною ІТС є її безпроводова складова – безпроводові інформаційно-телекомунікаційні системи (БІТС). В умовах відсутності антагонізму, чи під час динамічного розвитку конфлікту, відсоток БІТС з загальної складу ІТС, призначеної для державного управління, досить високий. Враховуючи це є критичним питання захисту саме БІТС під час інформаційного конфлікту. Захист власних систем є одним зі складових етапів інформаційної операції. Захист БІТС вимагає володіння інформацією про характер загроз та можливий сценарій перебігу інформаційного конфлікту. Для спостереженням за ходом інформаційного конфлікту необхідно оцінювати атаки противника (порушника) на БІТС та дієвість їх механізмів захисту інформації (МЗІ), що дозволить в подальшому вчасно захистити інформацію, що передається спеціальними БІТС.

Для моделювання процесів атак та захисту БІТС під час інформаційної боротьби використовувалось диференціально-ігрове моделювання з застосуванням методу диференційних перетворень академіка Пухова Г.Є. [1], що дозволило враховувати динаміку змін стратегій гравців (порушника та МЗІ) та уникнути вирішення нелінійних диференціальних рівнянь. Під час дослідження окремо розглядались складові частини РЕБ: атаки перехоплення радіосигналів (РРТР) та атаки РЕП відносно фізичного та канального рівнів БІТС. Інтервал розгляду інформаційного конфлікту $t_{ІК}$ = 24 години.

Моделювання атак порушника та захисних дій МЗІ безпроводових ІТС було проведено з урахуванням змін їх стратегій. В якості критеріїв приймались інтенсивності атак порушника та захисних дій МЗІ. В результаті моделювання побудовані шаблони нормальної поведінки (ШНП) БІТС, які відображають оптимальний стан − рівновагу між платою порушника та МЗІ. Отримано оптимальні значення інтенсивностей атак перехоплення радіосигналів, РЕП БІТС та захисту від них, які характеризують рівновагу диференціальної гри та дозволяють визначити її ціну. Визначено, що для отримання переваги над противником необхідно досягти збільшення плати протилежною стороною, яка б складала більше ціни гри. Для цього необхідно змінювати власну стратегію в бік збільшення інтенсивності захисних дій МЗІ БІТС. Результати дослідження показали адекватну роботу методики диференційно-ігрового моделювання з використанням диференційних перетворень Пухова Г.Е. при моделюванні поведінки БІТС під час інформаційного конфлікту. Практична важливість результатів обумовлюється можливістю застосування даної методики в процесі проектування захищених БІТС. При знанні ресурсів порушника, можливо застосовувати ефективні механізми захисту інформації, що надійно захистять БІТС в ході інформаційних операцій.

ЛІТЕРАТУРА

1. Пухов Г.Е. Преобразования Тейлора и их применение в электротехнике и электронике. К.: Наукова думка. – 1978. – 260 с.

Шестаков В. І. (ЖВІНАУ)
Чернишук С. В. (ЖВІНАУ)

СТРУКТУРНИЙ СИНТЕЗ СИСТЕМИ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ ЗАГРОЗ ЗА РЕЗУЛЬТАТАМИ МОНІТОРИНГУ ВІДКРИТИХ ДЖЕРЕЛ ІНФОРМАЦІЇ

Поява нового середовища протиборства – кіберпростору – обумовила виникнення низки специфічних загроз безпеці, які прийнято називати кібернетичними. Переваги від реалізації таких загроз обумовлюють їх привабливість не лише для силових відомств провідних країн світу, але й для терористичних організацій та окремих зловмисників. Тому останнім часом погляди провідних фахівців у галузі безпеки спрямовані саме на її кібернетичну складову. При цьому чи не найбільша увага звертається на успішне вирішення завдання своєчасного виявлення ознак таких загроз з метою їх завчасної нейтралізації або стримування. Можливим підходом до вирішення зазначеного завдання може стати застосування складної розподіленої системи виявлення кібернетичних загроз за результатами моніторингу відкритих джерел інформації. Ефективне функціонування такої системи вимагає раціонального відображення множини функцій, які виконуються системою, на множину її взаємопов'язаних складових елементів, тобто вирішення задачі структурного синтезу системи. При цьому структура системи, що розробляється, повинна забезпечувати виконання ряду суперечливих вимог, які висуваються до системи: мінімальний час на добування необхідних даних, висока достовірність отриманої інформації, максимальне охоплення інформаційних джерел тощо. Для виконання зазначених вимог до складу системи виявлення кібернетичних загроз за результатами моніторингу відкритих джерел інформації у якості центральної компоненти доцільно включити автоматизовану систему, головною складовою якої є робочі місця (АРМ) операторів, що створюються на базі персональних комп'терів і здатні виконувати часткові фукнції системи.

Ефективне функціонування системи може здійнюватися лише за умови виконання її складовими усього спектру визначених часткових функцій. При цьому важливо розподілити пости на базі АРМ за частковими задачами таким чином, щоб охопити увесь перелік покладених на систему фукнцій. Отже, актуальною є задача синтезу структури зазначеної системи при заданих функціях, визначених можливостях складових елементів системи та встановленій кількості таких складових.

Для вирішення сформульованої таким чином задачі запропоновано методику структурного синтезу системи виявлення кібернетичних загроз за результатами моніторингу відкритих джерел інформації. На першому етапі структурного синтезу системи пропонується із застосуванням евристичних методів визначити загальні риси системи: сформувати обрис системи, визначити її призначення та функції, висунути системні вимоги до її функціонування, вибрати складові елементи. На другому етапі за допомогою методів багатокритеріального аналізу пропонується визначити оптимальний якісний склад системи на підставі заданих характеристик її складових компонентів. Пошук рішення задачі в умовах багатокритеріальності запропоновано здійснювати шляхом зведення початкового завдання до однокритеріальної форми з використанням нелінійної схеми компромісів у вигляді дискретної згортки.Третій етап синтезу передбачає оцінювання оптимальності синтезованої системи шляхом порівняння значення інтегрального показника ефективності її функціонування із заданими допустимими значеннями. На підставі такого оцінювання приймається рішення щодо відповідності синтезованої системи висунутим до неї вимогам.

Таким чином з метою забезпечення ефективного функціонування системи виявлення кібернетичних загроз за результатами моніторингу відкритих джерел інформації розроблено методику її структурного синтезу з використанням методів багатокритеріального аналізу, що представлена у доповіді. Працездатність розробленої методики підтверджено шляхом материматичного моделювання, результати якого свідчать про її універсальність.

Шкурман М.І. (ВІТІ НТУУ „КПІ”)
к.т.н. Чумак В.К. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ МЕТОДІВ ОЦІНЮВАННЯ ЧАСТОТНОЇ ХАРАКТЕРИСТИКИ АДАПТИВНИХ СИСТЕМ ЗВ’ЯЗКУ

Задача підвищення завадостійкості систем радіозв’язку була і залишається однією з найактуальніших у теорії та техніці електрозв’язку. Важливим етапом при проектуванні адаптивних систем радіозв’язку є вибір методів оцінювання частотних характеристик каналу зв’язку. Адаптивні методи дозволяють на основі результатів оцінки реально існуючих у каналі зв’язку завад забезпечувати близькі до оптимальних режими функціонування системи.

Проведено аналіз основних методів оцінки частотних характеристик каналів радіозв’язку. Їх можна розділити на 4 групи.

1. Одним з найменш критичних до обчислювальної складності алгоритмів є метод, заснований на періодичній передачі тестових сигналів заздалегідь відомої структури або зондуючих імпульсів.

2. Використання у складі повідомлення, що передається, пілот-сигналів, розташованих на строго визначених часових позиціях і з деякими фіксованими параметрами, дозволяє приймальному обладнанню виділити їх зі складу повідомлення, яке приймається на фоні шумів, і за аналізом параметрів пілот-тонів зробити висновок про стан каналу зв’язку в цілому.

3. При використанні методів оцінки якості каналу за робочим сигналом для оцінки стану каналу на прийомі використовують реалізації вхідного інформаційного сигналу, прийняті в умовах дії різних завад і схильні до спотворень.

4. Сліпою оцінкою мається на увазі оцінка невідомих сигналів, що пройшли лінійний канал з невідомими характеристиками на фоні завад. При цьому оцінювання параметрів сигналу ведеться тільки за доступними реалізаціями вхідного сигналу приймального пристрою. При використанні методів оцінки якості каналу за робочим сигналом для оцінки стану каналу на прийомі використовують реалізації вхідного інформаційного сигналу, прийняті в умовах дії різних завад і схильні до спотворень. Даний вид оцінки потребує апріорного знання одержувачем деякої інформації про переданий сигнал, наприклад про вид і кратність модуляції, значення довжини циклічного префікса і т.п. Вид і кратність модуляції визначає тип використовуваного сигнального сузір’я для представлення сигналу, що на прийомі дає можливість здійснити вимірювання дисперсії точок фазової площини, відповідних переданим інформаційним символам, і, задаючись деяким критичним значенням цього розсіювання, можна зробити висновок про якість каналу зв’язку.

5. Знання довжини циклічного префікса дозволяє визначати зсуви меж символів захисного інтервалу, що дає можливість оцінити часове і частотне запізнювання сигналу. Алгоритм оцінки за робочим сигналом дозволяє одержувати своєчасну і оперативну оцінку якості каналу. Однією з головних переваг даного методу оцінки є те, що він не впливає на пропускну спроможність системи передачі при своєчасному і оперативному отриманні оцінки, що в сучасних умовах розвитку високошвидкісних послуг стає дуже актуальним.

Таким чином, при проектуванні адаптивних систем радіозв’язку слід використовувати метод оцінки якості каналу за робочим сигналом, оскільки він не зменшує пропускну спроможність системи радіозв’язку і забезпечує оперативне і своєчасне отримання інформації про стан каналу при прийнятних обчислювальних затратах.

Шпак В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

ПРОГРАМНИЙ КОМПЛЕКС СИНТЕЗУ СИСТЕМ РОЗПОДІЛЕНИХ ОБЧИСЛЕНЬ

Аналіз свідчить, що практичне застосування сучасних інформаційних технологій вимагає для вирішення своїх задач значних обчислювальних ресурсів. Наприклад, корпорація *Google* у даний момент експлуатує приблизно 900 000 серверів по всьому світу для забезпечення роботи пошукової системи та її онлайн-сервісів. Корпорація *Amazon* побудувала найбільший віртуальний суперкомп’ютер та запустила кластер з 17024 ядрами, який має обчислювальну потужність у 240 терафлопс. Призначення цієї системи полягає у наданні високопродуктивних обчислювальних ресурсів установам та організаціям, які їх потребують для обробки великих об’ємів інформації. Відомі кілька принципових підходів до побудови високопродуктивних обчислювальних систем. Усі вони пов’язані із забезпеченням паралельних обчислень. Це передбачає декомпозицію великих обчислювальних задач на кілька підзадач, менш ресурсоємних. Архітектура таких систем може бути багатопроцесорна, тобто виконання однієї програми здійснюється багатьма процесорами, або багатомашинна – багатьма машинами з власною пам’яттю, з’єднаних швидкісними комунікаційними лініями. В останні роки набули широкої популярності різноманітні *grid*-системи. Це розподілена система, що виконує складні обчислення шляхом використання багатьох комп’ютерів, під’єднаних до мережі. Прикладом таких систем є: *Strategic Grid Computing Initiative* – президентська програма США для створення єдиного національного простору високопродуктивних обчислень, *EGEE* (*Enabling Grids for E-science*) – розвиток проекту *DataGrid*, метою якого є побудова найбільшої у світі *grid*-мережі. Однією з типових сфер застосування високопродуктивних обчислень є побудова образу нормальної активності об’єктів системи для захисту та виявлення на основі цих відхилень спроб кібернетичного впливу. Побудова образу нормальної активності базується на понятті інфографічної моделі, яка б відображала стани на певні зрізи часу. Щоб досягти цього, необхідно через певний період часу робити інфографічну модель інформаційної системи, яка б показувала стан інформаційних потоків у системі, та порівнювати суміжні стани цих моделей. Таким чином, при певному відхиленні цього значення від нормованого ми можемо робити висновки про інцинденти інформаційної безпеки. Враховуючи розміри сучасних інформаційних систем, для проведення таких обрахунків необхідні значні обчислювальні ресурси, які є досить коштовними для їх придбання, використання та технічної підтримки. Для обробки таких об’ємів інформації можливе використання розподілених обчислень, які є одним із методів вирішення ресурсоємних обчислювальних завдань із використанням двох і більше комп’ютерів, об’єднаних в мережу. Таким чином, задача управління розподіленими обчисленнями зводиться до розбиття головного завдання на невеликі підзадачі та одночасного виконання їх на різних комп’ютерах. Тому необхідно, щоб завдання, що розв’язується, було сегментоване – розділене на підзадачі, що можуть обчислюватися паралельно. Для розподіленого обчислення даних необхідно поєднувати комп’ютери в кластер, або використовувати спеціалізоване програмне забезпечення. Існує декілька готових рішень для вирішення таких задач:

– *Solaris Claster* – кластерне програмне забезпечення, яке дозволяє віддаленим вузлам працювати разом. При відмові одного з них інші продовжують виконувати його функції;

– *Linux Virtual Server* – широко розповсюджений засіб управління кластерними системами для *Linux* систем, має гарну масштабність, робочі властивості та надійність;

– *Beowulf* – обчислювальний кластер, який розбиває задачу на підзадачі, які паралельно виконуються та обмінюються даними по мережі. Таким чином, проаналізувавши методи обчислення ресурсурсоємних задач, планується розробка програмного комплексу розподілених обчислень. До його задач входить побудова образу нормальної активності вузла, а також виявлення відхилень, які обумовлені потенційно небезпечними загрозами.

к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Фомін М.М. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ПІДВИЩЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ РАДІОКАНАЛІВ

У сучасних системах зв’язку в наслідок розширення переліку послуг, що надаються користувачам, існує необхідність підвищення пропускної здатності, наприклад, у системах мобільного зв’язку, високошвидкісних безпроводових локально-обчислювальних мережах і ін. Пропускна здатність може бути збільшена за допомогою розширення смуги частот або підвищення потужності сигналів, що випромінюються. Проте, застосування цих методів має недоліки, тому що через вимоги біологічного захисту й електромагнітної сумісності підвищення потужності й розширення смуги частот обмежене. Найбільш гостро ця проблема проявляється саме у системах безпроводового зв’язку в наслідок інтерференції сигналів суміжних каналів.

Досить суттєво інтерференція проявляється в несприятливому впливі радіосигналу, що випромінюється передавачем одного каналу, на приймач сусіднього каналу. Якщо центральні частоти цих сусідніх каналів розташовані досить близько одна від одної так, що їх частотні спектри перекриваються, і антени розташовані поблизу одна від одної, то міжканальна інтерференція може перевищувати допустимі норми.

Традиційними способами боротьби із міжканальною інтерференцією є:

вживання антен зпараметрами, що забезпечують придушення такої інтерференції, а також територіальне рознесення антен;

частотне рознесення, що реалізується в системах Frequency Division Duplex, де канали прийому і передачі рознесені по частоті (зазвичай на 100 Мгц);

часове рознесення завдяки реалізації механізму синхронізації частотних каналів, що вживається в системах TimeDivision Duplex, та яке полягає в синхронізації за часом циклів передачі і прийому фреймів.

Тому, якщо зазначені способи не забезпечують необхідну швидкість передачі даних при виконанні умови забезпечення мінімальних міжканальних спотворень, які виникають в наслідок інтерференції, то одним з найефективніших способів розв’язку цієї проблеми може бути застосування адаптивних антенних решіток зі слабко корельованими антенними елементами, які спроможні синтезувати голчатий промінь діаграми спрямованості. Таке рішення, окрім зменшення взаємної інтерференції, дає змогу підвищити потужність сигналу, що передається на 12 дБ, а сигналу, який приймається – на 6 дБ, і тим самим збільшити дальність обслуговування абонентів та підвищити швидкість передачі даних шляхом зміни рівня квадратурно-амплітудної модуляції QAM, наприклад з QAM-16 на QAM-64.

У підсумку вибір методу підвищення пропускної здатності радіоканалів залежить від наявного частотного ресурсу та можливих варіантів розташування антен з урахуванням їх ваго-габаритних показників.

ЛІТЕРАТУРА

1. Явіся В.С., Могилевич Д.І., Правило В.В. Методи запобігання взаємній інтерференції на базових станціях систем широкосмугового безпровідного доступу // V Науково-технічна конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”. Збірник тез. – К.: ВІТІ НТУУ „КПІ”. – 2010. – С. 265.

2. Слюсар В.И. Системы MIMO: принципы построения и обработка сигналов. // Электроника: наука, технология, бизнес. – 2005. – № 8. – С. 52 – 58.