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

V-та НАУКОВО-ТЕХНІЧНА КОНФЕРЕНЦІЯ

„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”

20-21 жовтня 2010 року

(Доповіді та тези доповідей)

Київ – 2010

ББК
Ц4 (4Укр)39
П-768

У збірнику матеріалів п’ятої 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)

1. **Бовда Е.М.** Склад і можливості глобальної системи управління Збройних Сил США 13
2. **Колачов С. П., Соколенко С. М.** Сучасний стан створення національної системи розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки 17
3. **Кувшинов О. В.** Методологія оперативного управління радіоресурсом військових систем радіозв'язку 23
4. **Міночкін А.І., Романюк В.А.** Інтелектуальні мобільні радіомережі 28
5. **Науменко М.І., Черних Ю.О., Приходько Ю.І.** Проблеми і напрями сучасного етапу розвитку військової освіти 37
6. **Стрюк О.Ю.** Метод максимізації корисності Mesh-радіомережі на основі показників сприйняття якості обслуговування абонентів 44
7. **Субач І.Ю.** Напрямки вдосконалення систем підтримки прийняття рішень інформаційно-аналітичного забезпечення Збройних Сил України 50

(Тези доповідей)

1. **Ананьїн О.В.** Організація електронного документообігу в підрозділах управління Збройних Сил України 55
2. **Андреєв Б.М., Терещенко О.М.** Особливості вимірювань сигналів телекомунікаційних мереж 57
3. **Архіпов В. В., Любарський С. В.** Технології інформаційного впливу на об'єкт інформаційної розвідки в мережах спеціального призначення 59
4. **Барсюков С.В.** Аналіз стандарту 802.16e-2005 мережі широкосмугового доступу на основі технології WiMAX 60
5. **Барсюков С.В.** Аналіз перспектив технології LTE 61
6. **Башкиров О.М.** Організація інформаційної диверсії проти комплексів автоматизації 62
7. **Бердников О.М.** Рішення *Triple Play* на базі технології *ADSL2+* 63
8. **Бердников О.М.** Планування проектів телекомунікаційних транспортних мереж 64
9. **Бессалов А. В. , Кокотов О. В.** Криптосистема на еліптичних кривих Едвардса над полем характеристики два 65
10. **Білан А.М., Зеленко О.В.** Методики підвищення якості роботи оператора АСУ військового призначення 66
11. **Біленький А.В., Процюк Ю.О., Філіпенко А.І.** Аналіз надійності програмного забезпечення для спеціалізованих обчислювальних систем 69
12. **Богданов В.В.** Застосування критерію ризику для оцінки захищеності автоматизованої системи 70
13. **Богданов В.В.** Методика оцінки ефективності систем фізичного захисту інформаційно-комунікаційних систем 72
14. **Бугера М.Г., Сілко О.В**. Застосування геоінформаційних систем в інформаційно-аналітичних підрозділах Збройних Сил України 74
15. **Бурячок В.Л., Бурячок Л.В., Боголій С.М.** Порівняльне оцінювання програмних засобів однакового функціонального призначення 75
16. **Бухал Д.А., Зеленко О.В., Зіборєва О.Б.** Вплив якості телекомунікаційної системи на своєчасність інформаційного забезпечення управління 77
17. **Валюх А.І.** Методика підготовки даних для аналізу фактів в інформаційних системах спеціального призначення 78
18. **Венгеровська О.В., Раєвський В.М.** Забезпечення декаметрового радіозв'язку через винесений ретранслятор як елемент стримування воєнного конфлікту 79
19. **Волков О.В., Сидоркін П.Г., Страшна А.В.** Проблеми і перспективи реалізації технічного і криптографічного захисту 81
20. **Волобуєв А.П., Бондаренко О.Є.** Переваги систем зв'язку на основі надвисотних аероплатформ 83
21. **Восколович О.І.** Методика адаптивної зміни параметрів сигнально-кодових конструкцій в каналах системи MIMO 85
22. **Гімпельс І.В.** Застосування Softswitch в мережах мобільного зв'язку 86
23. **Голь В.Д., Волков О.В.** Застосування перспективних радіозасобів тактичного рівня 87
24. **Голь В.Д., Якименко В.В.** Алгоритм ідентифікації базової станції в стандарті *GSM* 88
25. **Голь В.Д., Якименко В.В.** Аналіз безпеки зв'язку в різних стандартах мобільного зв'язку 89
26. **Горбенко В.І., Заремський М.Й., Нищук А.М.** Методика вибору функціонально повного набору елементів для синтезу автоматизованих комплексів радіомоніторингу 90
27. **Горбенко В.І., Картавих В.Ю.** Процедури контролю і управління інформаційними мережами

спеціального призначення 91
28. **Горбенко В.І., Матковський Р.М.** Елементи захисту конфіденційної інформації в модулі контрольного опитування 92
29. **Горбенко В.І., Ніколаєв С.М., Ратанін Є.Г.** Методика визначення протоколів передачі даних автоматизованим комплексом 93
30. **Горьков В.К., Савісько П.А.** Оцінка надмірності представлення інформації текстових документів в технічних засобах автоматизованих систем управління військами 94
31. **Грабовський О.В., Любарський С.В.** Методика оцінки ефективності систем перевірки знань. 95
32. **Грабчак В.І., Грабчак З.М.** Оцінка складності формування та декодування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішній ступені 96
33. **Грабчак В.І., Пасько І.В., Грабчак З.М.** Кодові схеми захисту інформації доказової стійкості на просторових кривих 98
34. **Грохольський Я.М.** Ймовірнісний захист вагомих розрядів рівномірних кодів 100
35. **Гупало А.Ю.** Енергетичний аналіз сукупності завад в зоні дії радіоелектронних засобів пунктів управління військами та озброєнням 101
36. **Гурський Т. Г., Борисов І. В., Коротков В. С**. Шляхи підвищення прихованості в системах радіозв'язку з OFDM 102
37. **Довбня С.Я.** Особливості підвищення кваліфікації фахівців в галузі технічного захисту інформації 104
38. **Драчук О.В.** Виявлення комп'ютерних атак на основі аналізу поведінки мережевих об'єктів 106
39. **Єрохін В.Ф., Черкасова Ю.О.** Методика вибору структури та довжини кодограми для високонадійної передачі команд (коротких повідомлень) у радіомережах 107
40. **Жердєв М.К., Пистряк В.В.** Обгрунтування необхідності удосконалення методів контролю технічного стану цифрових пристроїв зразків озброєння та військової техніки 109
41. **Жилінський І.В., Тупкало В.Є.** Проектування автоматизованих систем управління зв'язком спеціального призначення 110
42. **Жук О. Г.** Вибір режиму роботи засобів радіозв'язку в складній радіоелектронній обстановці 111
43. **Жук П.В.** Аналіз існуючих телекомунікаційних протоколів для побудови перспективних мобільних радіомереж військового призначення 112
44. **Загороднюк Ю.Г., Куцаєв В.В., Тамаровський В.В.** Один із можливих напрямків створення системи навігації наземних рухомих об'єктів 115
45. **Загребельний О.Ю.** Методи доступу в мобільних радіомережах з різними мережними архітектурами 116
46. **Залогін С.М., Колачов С.П., Садиков О.І.** Обгрунтування тактико-технічних вимог до телекомунікаційної мережі автоматизованої системи управління перевезеннями спеціального призначення 120
47. **Захараш О.М.** Планування мережі радіодоступу CDMA 2000 122
48. **Зінченко А.О., Жук О.В., Філіпов В.В.** Пропозиції щодо реформування вузлів зв'язку Збройних Сил України 123
49. **Зінченко А.О., Пучков О.О., Ромащенко Р.А**. Оцінка можливості застосування технології *FRAME RELAY* у телекомунікаційних мережах спеціального призначення 124
50. **Ізофатов Д.О.** Моделювання прогнозування трафіку в комп'ютерній мережі 126
51. **Ільїнов М.Д., Воробйов А.О.** Розрахунок зовнішніх електричних характеристик подвійної лінійної антенної решітки вібраторного типу 127
52. **Ільїнов М.Д., Павлюк О.М.** Зовнішні характеристики антен горизонтальної поляризації з ненаправленим випромінюванням в азимутальній площині 129
53. **Ільїнов М.Д., Шафранський О.П., Павлюк О.М.** Аналіз методів розрахунків ліній радіозв'язку з рухомими об'єктами 131
54. **Іщенко О.М., Петросян І.А.** Моделювання каналів зв'язку для HAPS систем 133
55. **Кадет Н.П., Зацаріцин О.О**. Шляхи удосконалення інформаційної боротьби в Збройних СилахУкраїни 134
56. **Каравацький В.О., Яценко О.А.** Основні вимоги до побудови сучасного центрального пульта управління стаціонарного вузла радіозв'язку 135
57. **Карловський І.В., Штаненко С.С.** Застосування нейроінформаційних технологій в інформаційно-телекомунікаційних системах 136
58. **Кіруша К. С.** Конвергенція стільникових мереж на основі технології NGN-SOFTSWITCH 137
59. **Климович О.К., Саєнко О.Г., Данько В.О.** Механізми реалізації сервісу захищених віртуальних мереж в комп'ютерній мережі військового призначення 138
60. **Коваленко А.О.** Алгоритми пошуку квадратних корнів в полях Галуа 139

61. **Коваленко І.Г.** Енергозберігаючі методи множинного доступу в безпровідних сенсорних мережах 141
62. **Ковбасюк Д.А., Хусаінов П.В.** Мультиагентний підхід до виявлення атак мережевого рівня на основі штучних нейронних мереж 143
63. **Козубцов І.М.** Метод віртуально-пізнавального представлення курсантам звітних етапів навчальної дисципліни 144
64. **Коцюба В.П., Станіщук А.Б.** Організація захисту об'єктів та комплексів зв'язку від інформаційного впливу 147
65. **Кравчук С.О., Міночкін Д.А.** Застосування багатоантенної технології MIMO в системах мобільного зв'язку специфікацій LONG TERM EVOLUTION 148
66. **Кривоножко Г.Є., Криховецький Г.Я., Срібний С.П.** Шляхи підвищення ефективності автоматизованого управління військами 149
67. **Кривцов І.В., Сілко О.В.** Методика оцінки ефективності системи безпеки модульного об'єктно-орієнтованого середовища навчання 151
68. **Кувшинов О. В., Липський О. А.** Контроль каналу зв'язку при пакетній передачі даних 152
69. **Кузавков В.В., Логінов М.В.** Методика оцінки розповсюдження мовного сигналу 153
70. **Линник А.І.** Впровадження четвертого покоління стільникового зв'язку 155
71. **Лисенко О.І., Валуйський С.В.** Підвищення структурної надійності безпроводових епізодичних мереж із повітряними ретрансляторами 157
72. **Литвин К.М.** Алгоритм спряжених градієнтів в нейронних мережах 158
73. **Лубенець А.А.** Телефона мережа зв'язку на платформі ASTERISK 159
74. **Лук'янчук І.В.** Обробка сигналів земних станцій на борту супутника ретранслятора з цифровим діаграмо утворенням 160
75. **Лунькова Г.В.** Створення моделі віртуального навчального середовища Академії сухопутних військ 161
76. **Любарський С.В., Шаціло П.В**. Використання параметричних моделей Item Response THEORY для реалізації адаптивних алгоритмів оцінки знань в комп'ютерних систем навчання 163
77. **Люлін Д.О., Єрохін В.Ф.** Багаточастотні цифрові сигнали для КХ-радіоліній за стандартами НАТО та підходи до підвищення завадостійкості їх демодуляції 165
78. **Мазниченко Ю.А., Панченко І.В., Васільєв А.Г.** Перспективи використання і тенденції розвитку систем супутникового зв'язку на основі технології VSAT у Збройних Силах України 166
79. **Макарчук О.М.** Автоматизовані системи управління навчальними закладами: стан і перспективи 167
80. **Макарчук О.М.** Аналіз методів підвищення завадостійкості в системах радіозв'язку 168
81. **Макарчук О.М., Микитюк А.В.** Аналіз характеристик системи захисту інформації 170
82. **Мєшков І.Н., Мусієнко В.А., Кайдаш І.Н.** Напрямки розвитку засобів радіозв'язку в тактичній ланці управління 171
83. **Микусь С.А., Розум І.Ю.** Проблеми взаємосумісності існуючих телекомунікаційних системи спеціального призначення з телекомунікаційною мережею загального користування 173
84. **Мохор В.В., Цуркан В.В.** Використання пробіт-методу для кількісного оцінювання ризику загроз безпеці інформації 174
85. **Наталенко П.П., Колачов С.П., Кисиленко П.П.** Безпека системи маршрутизації в корпоративній мережі 176
86. **Наталенко П.П., Шелепенко Ю.В., Білий О.С.** Технічна реалізація системи маршрутизації корпоративної мережі 177
87. **Науменко Ю.Б.** Методика проектування систем захисту інформації на основі об'єктно-орієнтованого підходу 179
88. **Науменко М.І., Шелепенко Ю.В., Кривенко С.С**. Аналіз можливостей впровадження сигнально кодових конструкцій 180
89. **Недайбіда Ю.П., Ляшенко В.Г., Шугалій О.О.** Питання системотехнічного забезпечення АСУ на сучасному етапі розвитку Збройних Сил України 182
90. **Нестеренко М. М., Маньківській В. Б., Пасько С. П.** Оцінка часу затримки повідомлень в мережах *IP* та *MPLS* 184
91. **Нестеренко М.М., Семеріч П.Ю.** Основні підходи щодо побудови систем управління конвергентних телекомунікаційних мереж 185
92. **Нечушкін М.П., Харченко Н.М.** Визначення варіанта побудови мобільного компоненту перспективної системи зв'язку та автоматизації тактичної ланки управління 187
93. **Овсянніков В.В., Місюра С.М.** Перспективи розвитку системи захисту персональних даних в Україні 189
94. **Осиченко О.Б. Мужеський К. К.** Методика побудови і перевірки програмної моделі мережі за

допомогою команд операційної системи та переферійного обладнання 191
95. **Паламарчук Н.А.** Порядок введення об'єктів інформаційної діяльності в дію 193
96. **Паламарчук С.А.** Доцільність застосування інфраструктур відкритих ключів *PKI* та *SPKI* в Збройних Силах України 194
97. **Пашковський В.В.** Оцінка ефективності застосування ДІС в алгоритмах діяльності операторів станцій РТР в умовах невизначеності 195
98. **Пелих О.О.** Новий підхід до побудови транспортної мережі мобільного оператора зв'язку 197
99. **Пермяков О.Ю., Залужний Р.М., Лаврінчук О.В.** Проблема синтезу структури навігаційного забезпечення окремих груп споживачів 199
100. **Пермяков О.Ю., Савченко В.А.** Концепція побудови інтелектуальних систем підтримки прийняття рішень військового призначення на основі геоінформаційних технологій 200
101. **Піддубний В.О., Корбут В.М., Піддубний В.В.** Поліпшення прийому сигналу в місцях з важкодоступним проходженням радіохвиль 202
102. **Піскун С.Ж.** Завадозахищеність типових алгоритмів входження в синхронізм ліній і систем зв'язку з псевдовипадковим перелаштуванням робочої частоти 203
103. **Погрібняченко А.І.** Аналіз можливостей системи SDH другого покоління – NG-SDH 204
104. **Правило В.В., Могилевич Д.І., Явіся В.С.** Особливості TMN-платформ і стратегії переходу на архітектуру TMN 205
105. **Прокопенко Є. М.** Аналіз характеристик засобів радіоелектронного подавлення систем радіозв'язку 206
106. **Радзівілов Г.Д., Мацаєнко А.М., Назарчук Б.О.** Автоматизація розробки програм радіозв'язку 207
107. **Раєвський В.М.** Підвищення пропускної спроможності телекомунікаційних мереж адаптивними агоритмами фізичного рівня 208
108. **Раєвський В.М., Турянський К.М.** SDR – технологія як перспективний шлях побудови радіозасобів нового покоління 209
109. **Розум І.Ю., Микусь С.А.** Організаційні та технічні заходи із захисту систем зв'язку тактичного рівня 210
110. **Ролік О.І., Тимофєєва Ю.С.** Метод формування матриці несправність-симптом в інформаційно-телекомунікаційних системах 212
111. **Романенко В.П.** Моделювання процесу групового пошуку дефектів при ремонті військової техніки зв'язку 213
112. **Романюк В.А., Стемпковська Я.А.** Методи покриття поверхні сенсорними вузлами 214
113. **Руденко С.Є.** Перспектива впровадження в технології LTE в Україні 215
114. **Савісько П.А., Горьков В.К.** Алгоритм адаптивної обробки інформації про динамічні об'єкти противника в підсистемах єдиної автоматизованої системи управління Збройними Силами України 216
115. **Сакевич С.О.** Технологія безпровідного доступу WiMAX: стан і перспективи 217
116. **Сальник Ю.П.** Вдосконалення розвідувального забезпечення бойових дій сухопутних військ 218
117. **Самойлов І.В., Кокотова М.О.** Аналіз вимог до інформаційної безпеки когнітивних радіосистем 219
118. **Самойлов І.В., Толюпа С.В.** Використання генетичного алгоритму та нейронної мережі для видобування нечітких відношень з експериментальних даних 220
119. **Самохвалов Ю.Я., Коваленко І.М., Бурба О.І.** Методика комплексного формування вимог до автоматизованих систем спеціального призначення 221
120. **Сєткін В.В., Гамалій Н.В.** Захист інформації від витоку технічними каналами 222
121. **Сілко О.В., Шугалій Є.П.** Методика дослідження функціональних залежностей техніко-економічних показників типових обчислювальних модулів для систем обробки інформації від їх параметрів 223
122. **Слотвінська Л.І.** Аналіз відбитків з засвідчувальних друкарських форм 224
123. **Слюсар В.І., Бондаренко М.В.** Потенційна точність оцінки напрямку на абонента цифровою антенною решіткою в умовах джитеру АЦП 225
124. **Слюсар В.І., Зінченко А.О.** Технологія МУЛЬТИ-МІМО як засіб апартного поєднання систем зв'язку та радіолокації 226
125. **Слюсар В.І., Копієвська В.С.** Оцінка рівня комплексно-сполученого відгуку сигналу по виходу плоскої цифрової антенної решітки 228
126. **Слюсар В.І., Троцько О.О., Копієвська В.С.** Методи врахування нелінійної частотної модуляції OFDM сигналів при зв'язку з надзвуковими літальними апаратами 230
127. **Сова О.Я.** Інтелектуалізація управління потоками даних в мобільних радіомережах військового призначення 231

128. **Соколов В.В.**Технологія програмуванняактивних динамічних сполук об'єктів 232
129. **Солодовник В.І.** Області застосування, перспективи та проблеми впровадження бездротових сенсорних мереж 234
130. **Сорока М.В**.Вплив інформаційної боротьби на розвиток АСУ 235
131. **Субач І.Ю., Саєнко О.Г., Власенко О.В.** Рішення задачі аналізу даних про збої в роботі інформаційної мережі шляхом застосування технологій інтелектуального аналізу даних 236
132. **Танасієнко П. В., Нестеренко М. М.** Аналіз основних типів вірусів в комп'ютеризованих системах 237
133. **Тимченко О.М., Іванов Б.П.** Оцінка ефективності функціонування систем зв'язку і автоматизації управління 239
134. **Тищенко М.Г.** Математична формалізація задачі раціонального вибору програмного забезпечення підрозділу дистанційного навчання на прикладі вибору системи управління навчальним процесом 240
135. **Ткаленко О.М.** Організація технічного обслуговування систем комутації 242
136. **Ткаченко А.Л., Мазниченко Ю.А., Панченко І.В.** Моделювання нечіткого регулятора при вихідних роз'єднаних на відрізок 1-2а трикутних функціях приналежності модифікованим методом 243
137. **Ткачов П.О.** Захист інформації на оптичних носіях від нелегального копіювання 244
138. **Труш О.В., Борисов О.В.** Забезпечення безпеки резервування інформації в системах розподіленого зберігання даних 245
139. **Фесьоха В.В.**Тестове дослідження стійкості програмного забезпечення до руйнівних інформаційних впливів, спрямованих на використання помилок управління пам'яттю 247
140. **Хлапонін Ю.І., Мальцева І.Р.** Аналіз систем управління ідентифікаційними даними користувачів виробництва провідних світових компаній 248
141. **Хусаінов П.В., Головко О.О.** Оцінка об'єктів програмно-ініційованих атак 249
142. **Хусаінов П.В., Гуреєв Ю.В.** Організація паралельного пошуку об'єктів атаки 250
143. **Хусаінов П.В., Редзюк Є.В.** Інформаційна модель прийняття рішень адміністратора локальної обчислювальної мережі 251
144. **Хусаінов П.В.** Алгоритмізація завдань впливу на інформаційно-телекомунікаційну систему 252
145. **Чевардін В.Є., Коваленко А.О., Ізофатов Д.О.** Перспективи розвитку несиметричних криптографічних систем захисту інформації 253
146. **Чумак В.К., Бортнік Л.Л.** Перспективи боротьби з навмисними завадами в системах радіозв'язку з використанням технологій MC-CDMA 255
147. **Шаціло П.В., Любарський С.В**. Методика вибору моделі подання знань в інтелектуальних навчальних системах 256
148. **Шацький І.О., Залужний О.В., Терезюк О.Е.** Розрахунок коефіцієнта направленої дії низькопрофільного випромінювача над циліндричною поверхнею 258
149. **Шворов С.А., Лукін В.Є.** Методичні засади планування та проведення занять з використанням інтелектуальних засобів дистанційного навчання 260
150. **Шевченко А.С.** Узагальнена модель порушника безпеки інформаційних активів безпроводових інформаційно-комунікаційних систем відомчого призначення в інформаційній боротьбі 262
151. **Юденок І.С., Білько Н.Ю., Лобанова М.М.** Вимоги до перспективної системи інформаційного забезпечення Збройних Сил України 264
152. **Явіся В.С., Могилевич Д.І., Правило В.В.** Методи запобігання взаємній інтерференції на базових станціях систем широкосмугового безпровідного доступу 265

Contents

(Reports)

1. **E. Bovda** Composition and possibilities of global system management military powers of the USA 13
2. **S. Kolachov, S. Sokolenko** Current state of national system of development and setting on manufacture of arms, military and special technics 17
3. **O. Kuvshinov** Methodology of radio-resource operative management for military radio communication systems 23
4. **A. Minochkin, V. Romanjuk** Intellectual mobile ad-hoc networks 28
5. **M. Naumenko, U. Chernih, U. Prihod`ko** Problems and directions of the military educational system development on the modern stage 37
6. **O. Striyuk** The method of mesh radio network utility maximization based on perceived quality of service 44
7. **I. Subach** Ways of improvement of decision support systems of information-analytical maintenance of Armed forces of Ukraine 50

(Tethys)

1. **O. Ananin** Construction elektronic circulation of documents in subdivision control of the Armed Forces of Ukraine 55
2. **B. Andreev, O. Tereshchenko** Features of measurement signals of telecommunications networks 57
3. **V. Arhipov, S. Liubarskii** Technologies of informational influence on the object of the data reconnoitering in special networks 59
4. **S. Barsyukov** Analysis standard 802.16e-2005 broadband access technology-based WIMAX 60
5. **S. Barsyukov** Analysis technology perspectives LTE 61
6. **O. Bashkirov** Organization of information diversion against automation complexes 62
7. **O. Berdnikov** Triple Play solution based on ADSL2+ technology 63
8. **O. Berdnikov** Telecommunication backbone networks planning design 64
9. **A. Bessalov, O. Kokotov** Cryptosystem on elliptic edwards curves under the field of characteristic two 65
10. **A. Bilan, A. Zelenko** Operator working quality increase techniques for military-purpose automatic control systems 66
11. **A. Belenkiy, U. Protsyuk, A. Filipenko** Reliability analysis software for scpecialized computer systems 69
12. **V. Bogdanov** Application risk criterion for estimation of protected of cas 70
13. **V. Bogdanov** Method of estimation of efficiency of systems of physical defence informatively communication systems 72
14. **M. Bygera, O. Silko** Application of gis systems in information-analytical Armed Forces of Ukraine 74
15. **V. Buryachok, L. Buryachok, S. Bogoliy** Comparative evaluation of software the same functional purpose 75
16. **D. Bykhal, A. Zelenko, O. Ziboreva** Quality of service influence of traffic military telecommunication system on timeliness of dataware of control 77
17. **A. Valyukh** Methods of preparing data for analysis of the facts in the information systems for special purposes 78
18. **O. Vengerovskaya, V. Raevsky** Radio communication maintenance through the taken out repeater as the element of restraint of the military conflict 79
19. **A. Volkov, P. Sidorkin, A. Strashna** Problems and prospects of realization of technical and cryptographic defense 81
20. **A. Volobuev, O. Bondarenko** Advantages of communication systems based on high altitude platform stations 83
21. **O. Voskolovich** A method of adaptive change parameters of alarm-code constructions is in channel of system MIMO 85
22. **I. Gimpels** Application Softswitch in mobile networks 86
23. **V. Gol', O. Volkov** Application perspective radiofacilities tactful level 87
24. **V. Gol', V. Yakumenko** Algorithm authentications base stations in standard *GSM* 88
25. **V. Gol', V. Yakumenko** Analysis safety of connection in different standards mobile communication 89
26. **V. Gorbenko, M. Zaremsky, A. Mishuk** Methods of choosing a functionally complete set of elements for the synthesis of automated rf monitoring 90
27. **V. Gorbenko, V. Kartavih** Special purpose information networks control and management procedures 91

28. **R. Matkovskiy** Elements of protection of confidential information in unit poll 92
29. **V.Gorbenko, S.Nikolaev, E.Ratanin** Method of determining the records of data automated complex 93
30. **V. Gor`kov, P. Savis`ko** An estimation of text documents information presentation surplus in the technical means of the military automated control systems 94
31. **O. Grabowsky, S. Lyubarsky** Method of assessment of knowledge tests 95
32. **V. Grabchak, Z. Grabchak** Estimation of codograms forming and decoding complication in the generalized cascade codes with algebro-geometric codes on external degrees 96
33. **V. Grabchak, I. Pas`ko, Z. Grabchak** Charts of convincing stability information defence codes on space curves 98
34. **Y. Grocholskiy** Possible defence of valuable digits of even kodas 100
35. **A. Gupalo** Energy analysis of disturbance totality in the operating zone of radio-electronic means of troops and armament control centers 101
36. **T. Gurskyy, I. Borisov, V. Korotkov** Ways of increasing of privacy in radio communication systems with OFDM 102
37. **S. Dovbnya** Features of training professionals in the field of information protection 104
38. **O. Drachuk** Detection computer attacks based on analysis of network objects behavior 106
39. **V. Yerokhin, J. Cherkasova** The technique of the structure and the length of codogram choice for highly reliable transfer of commands (short messages) in the radio networks 107
40. **M. Zherdev, V. Pistryak** Rationale for the improvement of technical methods of digital devices, samples of armament and military equipment 109
41. **I. Zilinckiy V. Tupkalo** Design of automated control systems for special-purpose communication 110
42. **O. Zhuk** A choice of the radio facilities operation mode in a complicated radio-electronic situation 111
43. **P. Zhuk** An analysis of existent telecommunication protocols for construction of perspective military mobile ad-hoc networks 112
44. **U. Zagorodnuk, V. Kutsaev, V. Tamarovsky** One of the possible directions for creating navigation system of ground mobile objects 115
45. **O. Zagrebelny** Topology-dependent MAC Policies for Wireless Mobile Ad-Hoc Networks 116
46. **S. Zalogin, S. Kolachov, O. Sadykov** Ground of tactical fnd technical requirements to telecomunications network of the automated system management the traffic by transportation 120
47. **A. Zakharash** Planning CDMA 2000 radio access network 122
48. **A. Zinchenko, O. Zhuk, B. Philipov** Suggestions concerning reformation of ukrainian armed forces signal centers 123
49. **A. Zinchenco, O. Puchkov, R. Romaschenko** The evaluation of potential of *FRAME RELAY* utilization in special-purpose communication networks 124
50. **D. Izofatov** The simulation of the computer network traffic forecasting 126
51. **M. Iljinov, A. Vorobjov** Calculation of external electrical characteristics of double linear array of dipole type 127
52. **M. Iljinov, O. Pavlyuk** External characteristics of antennas horizontal polarization with non-directional in the azimuth plane radiation 129
53. **M. Il'inov, O. Shafranskiy, O. Pavlyuk** Analysis methods calculations lines of radio contact with mobile objects 131
54. **O. Ischenko, I. Petrosyan** Communication chanals modeling for HAPS systems 133
55. **N. Kadet, O. Zatsaritsyn** Ways of information struggle improvement in Armed Forces of Ukraine 134
56. **V. Karavatckiy, O. Yatsenko** Basic requirements for the construction of a modern remote control stationary node communication 135
57. **I. Karlovckiy, S. Shtanenko** Application neyroinformatsiynyh technologies in information and telecommunication system 136
58. **K. Kirusha** The convergence of cellular networks based on NGN-softswitchtechnology 137
59. **O. Klimovich, A. Saenko, V. Danko** Mechanisms of realization of service of the protected virtual networks in a computer network of military designation 138
60. **A. Kovalenko** The algorithms of searching square roots in Galois fields 139
61. **I. Kovalenko** Saving energy media access control techniques in wireless sensor networks 141
62. **D. Kovbasuk, P. Khusainov** Multi-agent approach to network layer attack detection based on artificial neural networks 143
63. **I. Kozubtsov** Method of virtually cognitive presentation to students of the current stages of educational discipline 144

64. **V. Kotsyuba** Organization of communication objects and complexes protection from informational influence 147
65. **S. Kravchuk, D. Minochkin** Application of MIMO multiaerial technology in mobile communication of Long Term Evolution specifications 148
66. **G. Kryvonozhko, G. Krikhovetsky, S. Sribniy** Ways to increase efficiency of automated management by armies 149
67. **I. Krivcov, O. Silko** Methods of assessment of security systems module object-oriented learning environment 151
68. **A. Kuvshinov, A. Lipsky** Control of communication channel at packet sending of data 152
69. **V. Kuzavkov, M. Loginov** An evaluation method of speech signal's propagation 153
70. **A. Linik** Introduction of fourth generation mobile communication 155
71. **O. Lisenko, S. Valuiskiy** An increase of structural reliability of wireless episodic networks with air retransmitters 157
72. **K. Lytvyn** conjugate gradient method for neural networks 158
73. **A. Lubenets** Telephone network communication platform ASTERISK 159
74. **I. Luk'janchuk** Signal mining of earth station retrasmition with digital diagramforming 160
75. **G. Lun`kova** Virtual educational environment model creation for Academy of the ground forces 161
76. **S. Liubarskii, P. Shacilo** Using parametric models for Item Response Theory of adaptive algorithms in computer knowledge assessment of learning 163
77. **D. Liulin, V. Yerohin** HF radiolinks multifrequency digital signals according to the NATO standards and approachs to increasing of noise immunityof their demodulation 165
78. **Y. Maznychenko, I. Panchenko** Vasiliev Perspectives of usage and tendency of development of satellite communications systems on the basis of technology VSAT in Armed Forces of Ukraine 166
79. **O. Makarchuk** Automated control systems by educational establishments: state and prospects 167
80. **O. Makarchuk** An analysis of methods increase of antijammingness is in systems of radio contact 168
81. **A. Mykytuyk** Analysis of characteristics of security 170
82. **I. Meshkov, V. Musienko, I. Kaydash** Directions of development of facilities of radio contact are in tactical link of management 171
83. **S. Mikus,` I. Rozum** Problems of existent special purpose telecommunication systems and general-purpose telecommunication network use concurrency 173
84. **V. Mokhor, V. Tsurkan** Using probit-method for information security risk assessment 174
85. **P. Natalenco, S. Colachov, S. Kisilenco** A Routing security in corporate networks 176
86. **P. Natalenko, G. Shelepenco** Biliy Technical aspects of a routing system realization for corporate networks 177
87. **Y. Naumenko** A design technique systems of priv is on basis of the object-oriented approach 179
88. **M. Naumenko, G. Shelepenko, S. Kryvenko** The signal-code sequences utilization capability analysis 180
89. **U. Nedabida, V. Lyashenko, O. Shugaliy** Questions of the system-technical providing of the ASU on the modern stage of development Military Powers of Ukraine 182
90. **M. Nesterenko, V. Mankivskiy, S. Pasko** An estimation of time massages delay in networks IP and MPLS 184
91. **M. Nesterenko, P. Semerich** Basic approaches in relation to construction of systems management convergence telecommunication networks 185
92. **M. Nechushkin, N. Harchenko** Determination of variant of construction of a mobile component of a perspective communication and control system of a tactical level 187
93. **V. Ovsjannikov, S Misyura** Future development of protection personal data in Ukraine 189
94. **A. Osychenko, К. Mygeskij** Method of construction and reviews software model using commands network operating systems and equipmentperipheral 191
95. **N. Palamarchuk** Order of introduction the objects of informative activity in an action 193
96. **S. Palamarchuk** Expedience of application of infrastructures of the opened keys *OF PKI* but *SPKI* in Military Powers Of Ukraine 194
97. **V. Pashkovs`kiy** An estimation of DIS application efficiency in the algorithms of the PTP stations operators activity in the conditions of indeterminacy 195
98. **O. Pelykh** A new approach to build networks of mobile communication operator 197
99. **O. Permiakov, R. Zalugniy, O. Lavrinchuk** Problem of separate groups of users navigation providing structure synthesis 199
100. **O. Permiakov, V. Savchenko** Conception of military intellectual expert support system construction using geo-information technologies 200
101. **V. Poddubny, V. Korbut, V. Poddubny** Improve reception in areas inaccessible to the passage of

radio waves 202
102. **S. Piskun** Jameproofing of Typical Frequency-Hopping Lines and Systems Synchronization Algorithms 203
103. **A. Pogribnyachenko** Analisis of second generation NG-SDH system possibilities 204
104. **V. Pravilo, D. Mogilevich, V. Yavisya** TMN-platform features and strategy of junction to TMN architecture 205
105. **I. Prokopenko** Analysis of descriptions of facilities of radio electronic suppression of system of radio contact 206
106. **G. Radzivilov, A. Matsaenko, B. Nazarchuk** Automating the development of radio communication programs 207
107. **V. Raevsky** Increase of throughput of telecommunication networks by adaptive algorithms of physical level 208
108. **V. Raevsky, K. Turyansky** SDR - technology as the perspective way of construction of radio means of new generation 209
109. **I. Rozum, S. Mikus`** Organizational and technical measures for tactical level communication networks protection 210
110. **O. Rolik, U. Timofeeva** A method of a defect-symptom matrix forming in the information-telecommunication systems 212
111. **V. Romanenko** The process design of group search defects at the repair of military connection technique 213
112. **V. Romanuk, Y. Stempkovska** Metod of the Covering of the Sensor 214
113. **S. Rudenko** A prospect of LTE technology implementation in Ukraine 215
114. **P.Savis`ko, V. Gor`kov** An algorithm of adaptive information processing about the dynamic objects of enemy in the subsystems of the Ukrainian Armed Forces Unique Automated Control Syste 216
115. **S. Sakevych** Technology wireless access WiMAX: status and prospects 217
116. **U. Sal`nik** The ground forces battle actions reconnaissance providing improvement 218
117. **I. Samoylov, M. Kokotova** Analysis of requirements то information security of cognitive radiosystem 219
118. **I. Samoylov, S. Tolupa** Using genetic algorithm and neural network to extract unclear relations with experimental data 220
119. **U. Samokhvalov, I. Kovalenko, O. Burba** Method of complex formation requirements for automated systems for special purpose 221
120. **V. Sietkin, N. Gamaliy** Organization of information protection from its leakage via technical channels 222
121. **O. Silko, E. Shygaley** Research method fumctional dependence technical and economic indicators representative indicators representative module for data processing system pf their parameters 223
122. **L. Slotvinska** Analisis of confirmative printing form's imprints 224
123. **V. Slusar, M. Bondarenko** Potential accuracy estimation of sending to the subscriber by a digital aerial grate in the conditions of ADC Delay Variation 225
124. **V. Slusar, A. Zinchenko** MULTI-MIMO technology as mean of communication and radio-location networks hardware combination 226
125. **V. Slusar, V. Kopievs`ka** An estimation of the complex united response signal level on the output of flat digital aerial grate 228
126. **V. Slyusar, O. Trotsko, V. Kopievska** The methods of counting nonlinear frequency modulation OFDM signal for communication with supersonic aircrafts 230
127. **O. Sova** Intellectualization of data flow control in military mobile radio networks 231
128. **V. Sokolov** Programming technology of active dynamic connections of objects 232
129. **V. Solodovnyk** Introduction of wireless sensor networks scopes of applications, prospects and problems of 234
130. **M. Soroka** Information struggle influence upon automated control systems development 235
131. **I. Subach, O. Saenko, O. Vlasenko** Solving the data analysis problem of informational network faults by using the intellectual data analysis technologies 236
132. **P. Tanasiєnko, M. Nesterenko** Analysis of the main types of viruses in the computerized systems 237
133. **O. Tymchenko, B. Ivanov** Effectiveness assessment of communication and control automation systems operation 239
134. **M. Tischenko** Mathematical formalization of software rational choice for remote leaning subsection on the example of educational process control system choice 240
135. **O. Tkalenko** The organization of maintenance service of systems of switching 242
136. **A. Tkachenko, Y. Maznychenko, I. Panchenko** Design of fuzzy controller are received at days off separated on a piece 1-2a triangular membership functions by the modified method 243
137. **P. Tkachev** Protecting information on compact disks from unauthorized copying 244

138. **O. Trush, O. Borisov** Reservation safety information in data storage systems distributed 245
139. **V. Phesyoha** Test study of stability of software for information impact failure to exploit errors of memory 247
140. **Y. Khlaponin, I. Maltzeva** Identity and Access Management systems analysis of production users of leading world companies 248
141. **P. Khusainov, A. Holovko** Assessment of objects of program initiated attacks 249
142. **P. Khusainov, Y. Gureev** Parallel search of the object attacks organization 250
143. **P. Khusainov, E. Redzuk** Information model of decision manager local area network 251
144. **P. Khusainov** Algorithmization tasks of impact of information and telecommunication system 252
145. **V. Chevardin, A. Kovalenko, D. Izofatov** Asymmetrical cryptography security systems development perspective 253
146. **V. Chumak, L. Bortnik** Prospects of fight against intentional hindrances in systems radio contact with the use of technologies MC-CDMA 255
147. **P. Shacilo, S. Liubarskii** Method choice model of knowledge in intelligent learning systems 256
148. **I. Shatskiy, O. Zalygniy, O.Terezuk** A calculation coefficient of the directed action of low-profile emitter is above cylinder surface 258
149. **S. Shvorov, V. Lukin** Methods of planning and conducting lessons with using of intellectual meanses of distance learning 260
150. **A. Shevchenko** Generalised model of information assets infringer in wireless information and communication systems of departmental appointment in information struggle 262
151. **I. Yudenok, N. Bilko, M. Lobanova** Requirements to the perspective dataware system of Armed Forces of Ukraine 264
152. **V. Yavisya, D. Mogilevich, V**. **Pravilo** Methods of prevention of mutual interference are on the base stations of systems of broadband wireless access 265

к.т.н. Бовда Е.М. (ВІТІ НТУУ „КПІ”)

СКЛАД І МОЖЛИВОСТІ ГЛОБАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ США

Глобальна система управління збройних (ГСОУ) сил США являє собою організаційно-технічну єдність командних органів, пунктів управління, систем зв’язку, автоматизованих та інших спеціальних технічних систем. Оперативне управління збройними силами здійснюється за допомогою глобальної системи оперативного управління через головнокомандувачів об’єднаних командувань. Її технічну основу складають автоматизовані системи, системи зв’язку та комп’ютерні мережі. ГСОУ функціонально пов’язана з системами бойового управління видів збройних сил, що дозволяє здійснювати як централізоване керівництво країною, так і децентралізоване управління військовими формуваннями (силами) аж до окремого підрозділу. У цілому це багаторівнева система, де є взаємопов’язані керуючі і керовані органи. ГСОУ складає основу оперативного управління всіма компонентами збройних сил. Вона призначена для забезпечення функцій вищого військового керівництва США (президента, міністра оборони, голови КНШ), пов’язаних з оцінкою обстановки, своєчасним прийняттям рішень про застосування збройних сил (ЗС) і відданням відповідних наказів та директив їх керівному складу (рис. 1.).

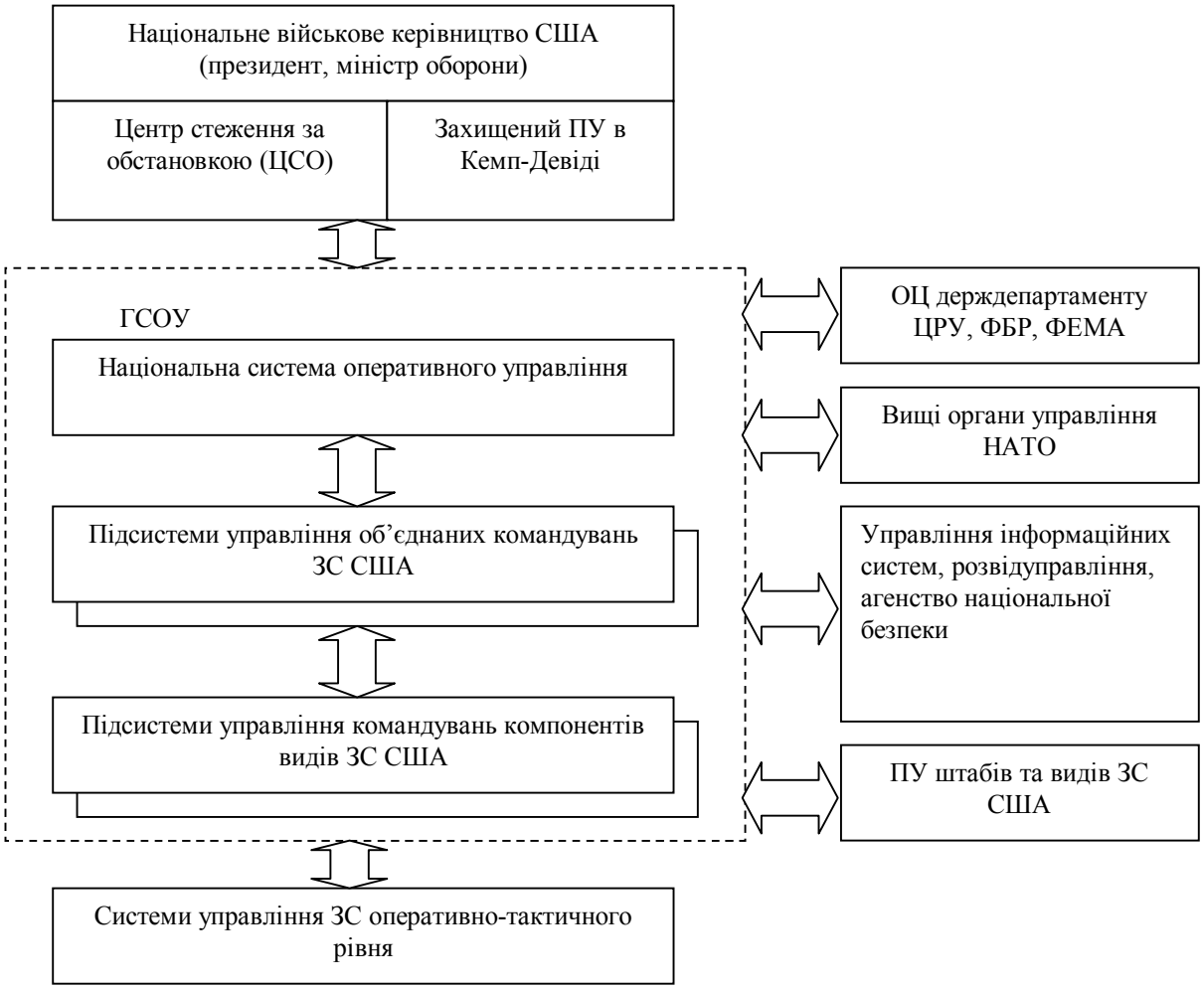


Рис. 1. Структура ГСОУ ЗС США

Ця система забезпечує вирішення таких основних завдань:

– своєчасне доведення до вищого військового керівництва США інформації про стан військово-політичної обстановки у світі, даних про склад, бойові можливості і характер діяльності збройних сил потенційних супротивників;

– тактичне попередження про повітряно-космічний напад на США;

– автоматизацію процесів прийняття президентом рішень з важливих військових питань, розробки й уточнення оперативних планів застосування стратегічних сил і сил загального призначення;

– безперервний контроль за станом бойової готовності всіх компонентів ВС та повсякденною діяльністю військ;

– доведення розпоряджень президента США на переведення збройних сил у підвищені ступені бойової готовності та їх бойове застосування;

– безперервне управління спільними діями ВС при виконанні ними бойових завдань у складі об'єднаних угруповань військ і коаліційних сил;

– управління діями контингентів збройних сил, виділених для надання допомоги цивільній владі при ліквідації наслідків надзвичайних ситуацій, стихійних лих або терористичних актів.

В організаційному плані ГСОУ є головною сполучною ланкою між національним військовим керівництвом і боєготовими силами і являє собою багаторівневу структуру, що охоплює органи оперативного управління ЗС від КНШ до штабів командувань компонентів видів збройних сил на континентальній частині США та в передових зонах.

На верхньому рівні ГСОУ сполучається з органами управління президента і державними органами, які беруть участь у стратегічному керівництві ЗС, а на нижньому – з органами управління військами. Розосередженість останніх по всьому світу і широкі зони їхньої відповідальності, що перекривають всю земну кулю, надають ГСОУ глобальний характер.

Вищий щабель в ГСОУ займає національна система оперативного управління (НСОУ), яка включає: основний і запасний командні центри (ОКЦ і ЗКЦ), повітряний командний пункт (ПКП), наземний мобільний командний пункт (НМКП) КНШ. На цьому рівні ГСОУ функціонально сполучається з органами управління президента США (Центром стеження за обстановкою (ЦСО) Білого дому і захищеним пунктом управління (ЗПУ) президента в Кемп-Девід); управліннями міністерства оборони: управлінням інформаційних систем (УІС), розвідувальним управлінням (РУМО), національним управлінням видової розвідки і картографії (НУВРК), агентством національної безпеки (АНБ); основними і запасними командними пунктами штабів видів ЗС США; основними, запасними командними пунктами (КП) штабів (пунктами управління) об'єднаних командувань (ОК) ЗС США; вищими органами управління НАТО; ОЦ держдепартаменту, ЦРУ, ФБР, ФЕМА.

В інтересах національного військового керівництва і КНШ ЗС США НСОУ забезпечує:

– доведення до президента, міністра оборони і голови КНШ інформації (розвідувального зведення) про військово-політичну обстановку в світі, даних про стан потенційних супротивників, їх бойових можливостях, реальних і прогнозованих діях;

– доповіді про бойовий склад, стан і діяльності стратегічних сил і сил загального призначення США, а також про їх ресурси і бойові можливості;

– тактичне попередження при повітряно-космічному нападі на США;

– автоматизацію процедур розробки та уточнення оперативних планів (варіантів бойового застосування стратегічних сил і сил загального призначення) відповідно до змін військово-політичної обстановки як в глобальному масштабі, так і в різних регіонах світу.

Наступний рівень управління ГСОУ складають підсистеми управління об'єднаних командувань. В даний час в національних збройних силах є дев'ять ОК, до складу яких виділені формування всіх видів ЗС. До них відносяться: об'єднане командування ЗС США в Європейській зоні; об'єднане командування ЗС США в зоні Тихого океану; об'єднане центральне командування; об'єднане командування ЗС США в зоні Центральної та Південної Америки; об'єднане командування ЗС США в зоні Північної Америки; об'єднане стратегічне командування; об'єднане командування стратегічних перебросок; об'єднане командування спеціальних операцій; об'єднане командування єдиних сил.

П’ять командувань (в Європейській зоні, в зонах Тихого океану, Північної, Центральної і Південної Америки, а також центральне) є регіональними і грають ключову роль у реалізації концепції „передової присутності” ЗС країни.

Чотири функціональних командування (стратегічне, стратегічних перебросок, спеціальних операцій і єдиних сил) зон відповідальності не мають і вирішують завдання як у глобальному масштабі, так і в інтересах регіональних об’єднаних командувань.

На третьому рівні управління ГСОУ знаходяться підсистеми управління командувань компонентів видів збройних сил, що входять до складу ОК, а також окремих командувань, що мають вузьку зону відповідальності в межах певного географічного району. На цьому рівні ГСОУ сполучається з органами управління формувань оперативно-тактичної ланки.

Підсистеми управління кожного з рівнів ієрархії ГСОУ самі по собі представляють досить складну структуру, що включає наступні елементи: основні і запасні командні центри (пункти управління); системи попередження (оповіщення); системи розвідувального забезпечення; системи зв’язку загального та спеціального призначення; автоматизовані системи управління, призначені для збору, обробки і розподілу інформації;засоби технічного та адміністративного забезпечення (прикладні програми, документацію, форми доповідей, а також засоби, які дозволяють користувачам входження в систему, введення і виведення повідомлень, документів і відеозображень).

З технічного боку ГСОУ – це територіально розподілена система інформаційно-обчислювальних центрів та автоматизованих робочих місць (АРМ), розгорнутих на КП штабів та пунктах управління збройними силами. Вони комутуються між собою розгалуженою мережею каналів відкритих і закритих систем зв’язку, що забезпечують проходження різної інформації: формалізованих розпоряджень, наказів, доповідей, повідомлень, а також таблиць, карт і схем. Встановлені в інформаційно-обчислювальних центрах і на АРМ сучасні високопродуктивні ЕОМ дозволяють автоматизувати різні функціональні сфери діяльності органів оперативного управління: проходження розвідувальної інформації, тактичне попередження, оцінку стану бойової готовності і ресурсів ЗС, планування застосування стратегічних сил і сил загального призначення, доведення наказів на застосування боєготових сил.

Сучасна ГСОУ є однією зі складових концепції технологічного прориву США у військовій області, що отримала назву „революція у військовій області” (Revolution in Military Affairs). Вона була сформульована і подана у 1993-1994 роках адміралом У.Оуенсом, що займав тоді пост заступника голови об’єднаного комітету начальників штабів. Створювана в ході реалізації цієї концепції так звана „система систем” включає в себе три складові частини: об’єднану систему спостереження і розвідки, автоматизовану систему бойового управління (АСБУ) силами та обміну інформацією С4І2 (Command, Control, Computers,Communications and Information / Intelligence); систему, що забезпечує застосування високоточної зброї.

Перша система забезпечує командування первинною інформацією, що надходить від джерел, що діють на всьому просторі поля бою. Вона узагальнює ці дані для того, щоб представити командуванню всіх рівнів єдину інформаційну картину про стан сил (як своїх, так і противника) і про навколишнє середовище (в тому числі метеоумови, стан поверхні ґрунту та гідрологічні умови моря, а також умови розповсюдження електромагнітних хвиль різних діапазонів у даному районі).

Друга система призначена для збору, обробки, об’єднання та аналізу первинних даних, а також для їх зберігання і передачі по запитам споживачів. На відміну від первинної ця інформація отримана в результаті класифікації цілей, розподілу за ними зброї та розробки даних наведення. Таким чином, ця система насичує тривимірний інформаційний простір поля бою даними планування бойових дій, управління та стрільби з метою досягнення панування над супротивником.

Третя система являє собою засоби, що забезпечують застосування зброї і поразки об’єктів високоточними боєприпасами, що дозволяє досягати цього панування. За

допомогою високоточної зброї наноситься ряд точних ударів, дія яких доповнює застосування звичайних засобів ураження.

Таким чином, кінцева мета створюваної „системи систем" управління – це збір, обробка, аналіз і розподіл інформації, що забезпечує наведення та застосування зброї з таким ступенем надійності і швидкістю, які не дозволять противнику прийняти адекватні відповідні заходи. Завдяки її застосуванню максимально знижується ступінь участі людини за рахунок повної автоматизації всіх перерахованих вище процесів.

Для вирішення завдання інтеграції систем управління видів збройних сил в основу побудови GCCS був покладений принцип створення єдиної операційної середовища інформаційної інфраструктури міністерства оборони DIICOE (Defense Information Infrastructure Common Operating Environment). Він передбачає три рівні узагальнення: ядро системи, набір функцій, загальних для всіх ЕОМ; єдина обчислювальна мережа.

Ядром COE є єдина операційна система ЕОМ, структура даних та програмних додатків, формат друкованих документів і вид інформації, що відображається. Це дозволяє виконати завдання, призначених для звичайних персональних комп'ютерів, на ЕОМ, встановлених на борту бойових кораблів і літаків.

Наступний рівень – загальний набір функцій для всіх ЕОМ з обміну користувачів інформацією в мережі і зберігання її в базах даних. Це було продемонстровано при випробуваннях системи GCCS (глобальна система управління – (Global Command and Control System)).

На третьому рівні відбудеться підключення користувачів до мережі передачі інформації міністерства оборони DISN (Defense Information System Network), за якою можуть передаватися оцифровані голосові, відео-і аналогові дані. У результаті цього GCCS і DISN стануть єдиною системою ГСОУ.

Програмами GCCS-A,-AF і-М передбачається розгортання автоматичних систем управління командувань СВ, ВПС і ВМС на континентальній частині США та в передових зонах, повністю сумісних з єдиною АСУ GCCS. Відповідно до програм „Ентерпрайз", „Горизонт" та „Коперник" планується створення в масштабі командувань компонентів видів збройних сил інтегрованих мереж телекомунікаційних систем за типом DISN, повністю з нею сумісних.

Таким чином, реалізація цих можливостей ГСОУ дозволить забезпечувати як централізоване, так і децентралізоване управління об'єднаними угрупованнями збройних сил в умовах їх негайного заподіяння у разі різкої зміни військово-політичної обстановки в будь-якому регіоні світу, з мінімально допустимим за часом періодом підготовки до ведення бойових дій, в тому числі і на необладнаних ТВД. Водночас це дозволить командуванню об'єднаних оперативних формувань США здійснювати адаптивний підхід до планування операцій, швидко реагувати на зміни обстановки в зоні бойових дій, випереджати супротивника у прийнятті рішень і в кінцевому підсумку забезпечити стратегічну і тактичну перевагу. Для ЗС України розглянуті підходи вже втілені в проекти перспективних АСУ. Залишилось тільки їх реалізувати.

ЛІТЕРАТУРА

1. *Роль и место* глобальной системы оперативного управления в стратегическом руководстве США. Полковник В. Азов. „Зарубежное военное обозрение" № 5, 2003 с 2 – 7.

2. *Глобальная система* оперативного управления вооруженными силами США и концепция ее развития. В.С. Ткачев, академик АВН, А.А. Лелехов, академик АВН.

3. *Автоматизированные системы* управления сухопутными войсками США. Полковник В. Масной; полковник Ю. Судаков, канд. технических наук. „Зарубежное военное обозрение" 2003 № 9, 10.

4. *Разработка АСУ* и информационных технологий в ВМС США. Капитан 1 ранга И.Быков.

к.т.н. Колачов С. П. (ВІТІ НТУУ „КПІ”)
Соколенко С. М. (ГУЗІС ГШ ЗСУ)

СУЧАСНИЙ СТАН СТВОРЕННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ РОЗРОБЛЕННЯ ТА ПОСТАВЛЕННЯ НА ВИРОБНИЦТВО ОЗБРОЄННЯ, ВІЙСЬКОВОЇ І СПЕЦІАЛЬНОЇ ТЕХНІКИ

На сьогодні планування та організація робіт, пов’язаних із розробленням, виробництвом. експлуатацією та ремонтом озброєння, військової і спеціальної техніки (далі військова техніка), здійснюються центральними органами виконавчої влади, підприємствами, науковими установами і організаціями відповідно до вимог військових стандартів колишнього СРСР, що являють собою єдину систему розроблення та поставлення на виробництво військової техніки (далі система стандартів).

Системою стандартів урегульовано всі стадії життєвого циклу військової техніки, визначено організаційну структуру управління процесом її розроблення, виробництва, експлуатації та ремонту, склад його учасників та їх повноваження, процедуру прийняття рішень тощо.

Застосування системи стандартів в Україні послідовно запроваджувалося шляхом укладення угод з державами. що входили до складу СРСР, а також затвердження і введення в дію колишнім Держстандартом відповідних рекомендацій щодо такого застосування.

Разом з тим результати роботи Міноборони та інших центральних органів виконавчої влади із застосування системи стандартів вітчизняними підприємствами свідчать про необхідність її докорінної зміни або створення нової.

Аналіз причин виникнення проблеми

Нормативно-правова база, сформована на основі системи стандартів, не узгоджується з актами національного законодавства, не враховує перетворень, що сталися в економці, а також того фактору, що розроблення і виробництво військової техніки в Україні за замкнутим циклом не завжди доцільно або можливо. Так, в умовах СРСР стандарти, що були обов'язкові для виконання всіма міністерствами, відомствами, підприємствами, науковими установами і організаціями, визначали відповідні повноваження державних органів. Планування та контроль за розробленням і виробництвом військової техніки здійснювалися єдиним органом Військово-промисловою комісією при Раді Міністрів СРСР.

В Україні згідно із законодавством повноваження центральних органів законодавчої влади визначаються Конституцією і законами України. Відсутній єдиний орган з планування та контролю за розробленням і виробництвам військової техніки.

Системою стандартів передбачалося розроблення і виробництво військової техніки без залучення науково-технічної та виробничої кооперації з іншими державами. Науково-технічне супроводження таких процесів, а також авторський нагляд за військовою технікою забезпечувався цілісним комплексом спеціалізованих науково-дослідних організацій та підприємств. На даний час на території України функціонують розрізнені за спеціалізацією підприємства, наукові установи і організації, які спроможні переважно забезпечувати окремі стадії життєвого циклу військової техніки або розроблення і виробництво окремих складових частин, комплектувальних виробів і матеріалів. Крім того, виконання робіт із збільшення технічного ресурсу та продовження строків зберігання військової техніки, боєприпасів, потребує залучення розробників з Російської Федерації, що ускладнено багатьма факторами, зокрема економічними і фінансовими.

Системою стандартів також:

– не передбачено участь у супроводженні стадій життєвого циклу військової техніки суб’єктами господарської діяльності приватної форми власності;

– не визначено порядок забезпечення справності, технічної придатності та модернізації військової техніки іноземного походження, взяття її на озброєння;

– не приведено механізм розроблення і виробництва військової техніки у відповідність з вимогами Закону України „Про державне оборонне замовлення”;

– не проведено гармонізацію військових стандартів з державними стандартами, що застосовуються в інших сферах, але регулюють такі самі питання, з відповідними міжнародними, європейськими стандартами та стандартами країн членів НАТО.

Метою цієї доповіді є визначення шляхів, основних завдань і заходів щодо створення національної системи розроблення і поставлення на виробництво військової техніки.

Шляхи розв’язання проблеми, основні завдання та орієнтовні заходи

Систему розроблення і поставлення на виробництво військової техніки передбачається запровадити шляхом послідовного опрацювання і прийняття взаємо узгоджених актів законодавства, державних стандартів, технічних регламентів, актів центральних органів виконавчої влади, перелік яких наведений в табл. 1.

Таблиця 1

ПЛАН

заходів з реалізації Концепції створення національної системи розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки

Найменування (зміст) заходу	Відповідальні за виконання	Строк виконання	Результат, що очікується
1. Розроблення проектів законів України			
1.1.Розроблення проекту закону України щодо внесення змін до законів України „Про оборону України”, „Про Збройні Сили України”, „Про організації оборонного планування”	Міністерство оборони України Міністерство промислової політики України	Грудень 2010 року	Визначення повноважень органів державної влади, які приймають рішення про розроблення зразків озброєння, військової і спеціальної техніки, поставлення її на виробництво, експлуатацію, технічне обслуговування, продовження строку служби і строку зберігання, а також з інших питань щодо забезпечення життєвого циклу озброєння та військової техніки
1.2.Розроблення та супроводження проекту закону України „Про розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки”	Міністерство промислової політики України Міністерство оборони України	Грудень 2010 року	Врегулювання відносин, пов’язаних з провадженням господарської діяльності на всіх стадіях життєвого циклу озброєння і військової техніки, їх правового режиму, а також визначення прав і обов’язків учасників процесу їх створення
2. Розроблення проектів нормативно-правових актів Кабінету Міністрів України			
2.1.Розроблення проекту постанови Кабінету Міністрів України щодо внесення змін до постанови Кабінету Міністрів України від 3 серпня 2006 року N 1080 „Про затвердження Положення про Міністерство оборони України” (зі змінами) та внесення змін до Указу Президента України від 21 вересня 2006 року N 769/2006 „Про Положення про Генеральний штаб Збройних Сил України”	Міністерство оборони України	Червень 2010 року	Визначення функцій Міністерства оборони України щодо забезпечення справності та технічної придатності озброєння та військової техніки Збройних Сил України. Розподіл повноважень між Міністерством оборони України та Генеральним штабом Збройних Сил України з питань розроблення та поставлення на виробництво озброєння та військової техніки
2.2.Розроблення проекту постанови Кабінету	Міністерство оборони	Грудень 2010 року	Удосконалення функцій Міністерства оборони України щодо забезпечення

Найменування (зміст) заходу	Відповідальні за виконання	Строк виконання	Результат, що очікується
Міністрів України щодо внесення змін до постанови Кабінету Міністрів України від 13 квітня 2007 року N 624 „Про затвердження Порядку збільшення встановленого ресурсу та продовження строків служби і зберігання озброєння та військової техніки іноземного виробництва”	України		справності, технічної придатності і модернізації озброєння та військової техніки іноземного виробництва, які знаходяться на озброєнні Збройних Сил України
2.3. Розроблення проекту постанови Кабінету Міністрів України щодо внесення змін до постанови Кабінету Міністрів України від 19 січня 1998 року N 33 „Про покладення на Міністерство промислової політики функцій держзамовника робіт з технологічної підготовки виробництва для задоволення потреб оборони і національної безпеки”	Національне космічне агентство України Міністерство промислової політики України Міністерство оборони України	Грудень 2010 року	Покладення на Національне космічне агентство України функцій держзамовника робіт з підготовки виробництва та створення спеціальних технологій і матеріалів для виготовлення ракетно-реактивного озброєння
2.4. Розроблення проекту постанови Кабінету Міністрів України щодо визначення порядку організації робіт із стандартизації озброєння та військової техніки в України	Державний комітет України з питань технічного регулювання та споживчої політики Міністерство оборони України Міністерство промислової політики України	Протягом шести місяців після прийняття Закону України "Про розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки"	Встановлення порядку організації та проведення робіт зі стандартизації і уніфікації озброєння та військової техніки в процесі розроблення і поставлення на виробництво військової техніки відповідно до законів України „Про стандартизацію” і „Про розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки”. Розробляється на заміну постанови Кабінету Міністрів України від 19 серпня 1993 року N 662 „Про організацію робіт із стандартизації озброєння та військової техніки”
2.5. Розроблення проекту постанови Кабінету Міністрів України щодо визначення порядку здійснення технічного (гарантійного) та авторського нагляду за озброєнням та військовою технікою Збройних Сил України, зокрема озброєнням та військовою технікою іноземного	Міністерство оборони України Міністерство промислової політики України	Червень 2011 року	Визначення правових та організаційних засад планування та виконання робіт з технічного (гарантійного) та авторського нагляду за озброєнням та військовою технікою в умовах ринкової економіки

Найменування (зміст) заходу	Відповідальні за виконання	Строк виконання	Результат, що очікується
виробництва			
2.6.Розроблення проекту постанови Кабінету Міністрів України щодо внесення змін до постанови Кабінету Міністрів України від 23 квітня 2001 року N 392 „Про затвердження Положення про генерального конструктора із створення техніки для потреб оборони та безпеки держави” (зі змінами)	Міністерство промислової політики України Міністерство оборони України	Червень 2011 року	Удосконалення механізму призначення генеральних конструкторів та порядку їх взаємодії з державними замовниками озброєння та військової техніки
2.7.Розроблення проекту постанови Кабінету Міністрів України щодо затвердження основних умов постачання озброєння та військової техніки для потреб Збройних Сил України та інших військових формувань	Міністерство оборони України Міністерство промислової політики України	Листопад 2011 року	Врегулювання відповідно до чинного законодавства правових відносин між замовниками, постачальниками та споживачами озброєння та військової техніки з питань постачання, гарантійних обов’язків, пред’явлення та задоволення рекламацій. Розробляється на заміну „Основных условий поставки продукции для военных организаций” та „Основных условий поставки кораблей и судов для Министерства обороны”, затверджених відповідними постановами Ради Міністрів СРСР
3. Розроблення проектів нормативно-правових актів центральних органів виконавчої влади			
3.1.Розроблення проекту наказу щодо затвердження Положення про організації розроблення (модернізації) озброєння та військової техніки для потреб Збройних Сил України	Міністерство оборони України	Травень 2010 року	Визначення загального порядку організації робіт з розроблення (модернізації) озброєння та військової техніки та прийняття нового озброєння та військової техніки на озброєння (постачання, експлуатацію) Збройних Сил України, а також визначення функцій та повноважень основних учасників процесу розроблення (модернізації) цієї техніки
3.2.Розроблення проекту наказу щодо застосування нормативних документів НАТО та стандартів інших країн під час виконання дослідно-конструкторських робіт з розроблення (модернізації) озброєння та військової техніки в інтересах Збройних Сил України	Міністерство оборони України Міністерство промислової політики України	Вересень 2010 року	Визначення порядку застосування (впровадження) нормативних документів НАТО та стандартів інших країн під час виконання дослідно-конструкторських робіт з розроблення (модернізації) озброєння та військової техніки в інтересах Збройних Сил України
3.3.Розроблення проекту наказу щодо порядку застосування стандартів у сфері оборони та реєстрація його у Міністерстві юстиції України встановленим порядком	Міністерство оборони України Державний комітет України з питань технічного регулювання та споживчої	Грудень 2010 року	Встановлення порядку застосування технічних умов, стандартів організацій, галузевих стандартів СРСР, нормативних документів інших країн, що використовуються під час розроблення озброєння та військової техніки

Найменування (зміст) заходу	Відповідальні за виконання	Строк виконання	Результат, що очікується
	політики Міністерство промислової політики України		
3.4.Розроблення проекту наказу щодо порядку розроблення аванпроектів, узгодження та видання тактико-технічних завдань, розроблення, розгляду та затвердження ескізних і технічних проектів кораблів та суден Військово-Морських Сил Збройних Сил України	Міністерство оборони України Міністерство промислової політики України	Грудень 2010 року	Визначення порядку розроблення аванпроектів, узгодження та видання тактико-технічних завдань, розроблення, розгляду та затвердження ескізних і технічних проектів кораблів та суден Військово-Морських Сил Збройних Сил України. Розробляється на заміну „Положения о порядке разработки аванпроектов, согласования и выдачи тактико-технических заданий, разработки, рассмотрения и утверждения эскизных и технических проектов кораблей и судов ВМФ”, затвердженого наказом Міністра оборони СРСР
3.5.Розроблення проекту наказу з визначення у складі Міністерства оборони України органу з державного гарантування якості	Міністерство оборони України Міністерство промислової політики України	Червень 2011 року	Визначення в Міністерстві оборони України органу з державного гарантування якості
4. Розроблення проектів нормативних документів			
4.1.Перегляд міждержавних стандартів серії ГОСТ В 15 та розроблення на їх заміну відповідних національних стандартів* з питань розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки	Міністерство оборони України Державний комітет України з питань технічного регулювання та споживчої політики Міністерство промислової політики України	До 2015 року	Створення відповідно до законодавства України нормативної бази національної системи розроблення та поставлення на виробництво озброєння, військової і спеціальної техніки, зокрема з питань визначення: стадій життєвого циклу озброєння та військової техніки, порядку виконання науково-дослідних (аванпроектів) і дослідно-конструкторських робіт та їх складових частин, а також науково-дослідних робіт з розроблення комплектувальних виробів загально-технічного призначення, складу та правил оформлення експлуатаційної і ремонтної документації, гарантійних обов'язків, обмежувального переліку комплектувальних виробів і матеріалів, дозволених до використання у військовій техніці, вимог до підприємств, що розробляють та виробляють військову техніку, вимог до тактико-технічного (технічного) завдання на виконання науково-дослідних робіт, аванпроекту, дослідно-конструкторських робіт, порядку розроблення і виробництва матеріалів для озброєння та військової техніки, порядку підготовки програм забезпечення надійності, порядку складання звітної документації, порядку складання єдиного наскрізного плану створення зразка (системи, комплексу) і його складових частин, порядку випробування дослідних зразків озброєння та військової техніки, порядку проведення технічної експертизи, порядку постановлення на виробництво озброєння та військової

Найменування (зміст) заходу	Відповідальні за виконання	Строк виконання	Результат, що очікується
			техніки, порядку випуску бюлетенів для озброєння та військової техніки і проведення робіт за ними, порядку введення в експлуатацію серійних стаціонарних комплексів озброєння та військової техніки та інших стаціонарних об'єктів озброєння та військової техніки, порядку зняття озброєння та військової техніки з виробництва та її утилізації
5. Інші заходи			
5.1.Впровадження STANAG 4107	Міністерство оборони України Міністерство промислової політики України	Червень 2011 року	Впровадження в Міністерстві оборони України системи державного гарантування якості продукції військового призначення
5.2.Впровадження AQAP-2000	Міністерство оборони України Міністерство промислової політики України	Червень 2011 року	Впровадження в Міністерстві оборони України системи державного гарантування якості продукції військового призначення
5.3.Розроблення методичних рекомендацій щодо формування програм та методик випробувань озброєння та військової техніки при одиничному або дрібносерійному її виробництві	Міністерство оборони України	Грудень 2012 року	Встановлення порядку формування програм та методик випробувань озброєння та військової техніки в умовах обмежених обсягів його виробництва
5.4.Розроблення нормативних документів щодо використання імпортної елементної бази під час розроблення (модернізації), виробництва, ремонту та експлуатації озброєння та військової техніки	Міністерство промислової політики України Міністерство оборони України	Грудень 2012 року	Встановлення порядку використання імпортної елементної бази під час розроблення (модернізації) і виробництва озброєння та військової техніки виходячи з впровадження спрощеного порядку використання імпортної елементної бази
5.5.Розроблення проекту Плану робіт (заходів) щодо створення та впровадження системи інформаційної підтримки життєвого циклу озброєння та військової техніки на основі CALS-технологій	Міністерство оборони України Міністерство промислової політики України	Грудень 2012 року	Впровадження в Міністерстві оборони України системи інформаційної підтримки життєвого циклу озброєння та військової техніки

Очікувані результати

Реалізація зазначеного плану дасть змогу забезпечити створення національної системи розроблення та поставлення на виробництво військової техніки, що сприятиме ефективному управлінню такими процесами, узгодженості дій всіх їх учасників, прийняттю оптимальних технічних рішень, мінімізації витрат, державного бюджету, зменшенню строків її створення та взяття на озброєння.

к.т.н. Кувшинов О. В. (ВІТІ НТУУ „КПІ”)

МЕТОДОЛОГІЯ ОПЕРАТИВНОГО УПРАВЛІННЯ РАДІОРЕСУРСОМ ВІЙСЬКОВИХ СИСТЕМ РАДІОЗВ’ЯЗКУ

Однією з тенденцій розвитку тактики загальновійськового бою є широке застосування засобів радіоелектронної боротьби. Сучасні засоби радіоелектронного подавлення здатні з високою ефективністю та у короткий час подавити систему радіозв’язку, побудовану на традиційних принципах [1–4].

Враховуючі це, стає досить складним завдання забезпечення стійкого радіозв’язку в умовах активного радіоелектронного подавлення. Успішне його вирішення неможливо без застосування спеціальних технічних і організаційних заходів по забезпеченню оперативного управління радіоресурсом військових систем радіозв’язку (ВСРЗ). Під радіоресурсом розуміють (рис. 1) потенційну можливість певної кількості засобів радіозв’язку, об’єднаних в одну або декілька систем по обміну інформацією або енергією із заданою якістю у заданому частотному діапазоні з врахуванням їх технічних характеристик і просторово-часових координат. Надалі під оперативним управлінням радіоресурсом розумітимемо процес динамічної організації та корекції такої цілеспрямованої дії на елементи ВСРЗ (об’єкт управління), в результаті якого забезпечується максимальне значення показника ефективності функціонування ВСРЗ.

Рис. 1. Складові радіоресурсу

Стратегічним напрямом при вирішенні задачі оперативного управління радіоресурсом ВСРЗ є перехід від систем з жорсткою структурою до адаптивних систем [5, 6]. Застосування адаптації дозволяє в умовах мінімальної апріорної інформації досягти оптимальних параметрів системи. Відсутність єдиної методології, теоретичних основ і математичного апарату прикладного аналізу та синтезу систем управління радіоресурсом мереж зв’язку з динамічною топологією в умовах активної радіоелектронної протидії в значній мірі стримують створення сучасних ефективних систем цифрового радіозв’язку тактичного рівня з необхідними показниками якості інформаційного обміну.

Класифікація задач за циклом управління радіоресурсом ВСРЗ представлена на рис. 2.

Оцінка стану ВСРЗ. Раціональне оперативне управління радіоресурсом ВСРЗ потребує знання про стан каналу зв’язку. Методи контролю стану каналів можна класифікувати: за об’ємом – глобальний і локальний (зоновий), фіксований і адаптивний; за способом – тестовий, непрямий, кодовий, прямий вимір [7, 8].

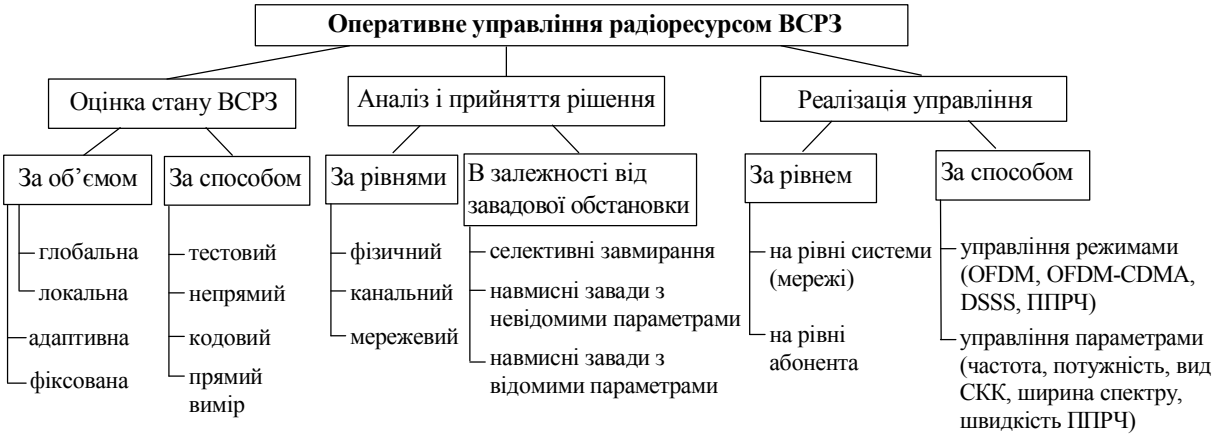


Рис. 2. Класифікація задач за циклом оперативного управління радіоресурсом ВСРЗ

Аналіз і прийняття рішення. Задачі оперативного управління радіоресурсом можуть вирішуватися на трьох рівнях моделі взаємодії відкритих систем: фізичному, канальному та мережевому. В залежності від завадової обстановки в процесі аналізу можуть бути визначені наступні сценарії радіоелектронної обстановки в каналі: тільки селективні завмирання, навмисні завади з невідомими параметрами, навмисні завади з відомими параметрами.

Реалізація управління. За рівнем реалізації оперативного управління радіоресурсом виділяють задачі управління на рівні мережі (верхній рівень) та на рівні окремих абонентів чи радіозасобів (нижній рівень). За способом реалізації розрізняють: управління режимами роботи радіозасобів; управління параметрами (значеннями параметрів) цих засобів у визначених режимах роботи.

Для ефективного функціонування ВСРЗ необхідно комплексне координування частотних, енергетичних, часових і просторових ресурсів радіоканалів з врахуванням характеристик комплексу зовнішніх умов їх реалізації. Це визначає доцільність спільного синтезу ВСРЗ і систем управління їх радіоресурсів.

Систему управління радіоресурсом подано як підсистему розподіленого ієрархічного адаптивного управління ВСРЗ (рис. 3). На рис. 3. $B_0(T)$, $B_з(T)$, $\mu(T)$ – вектори шуму, навмисних завад та селективних завмирань, що діють в каналі зв'язку (T – тривалість циклу управління).

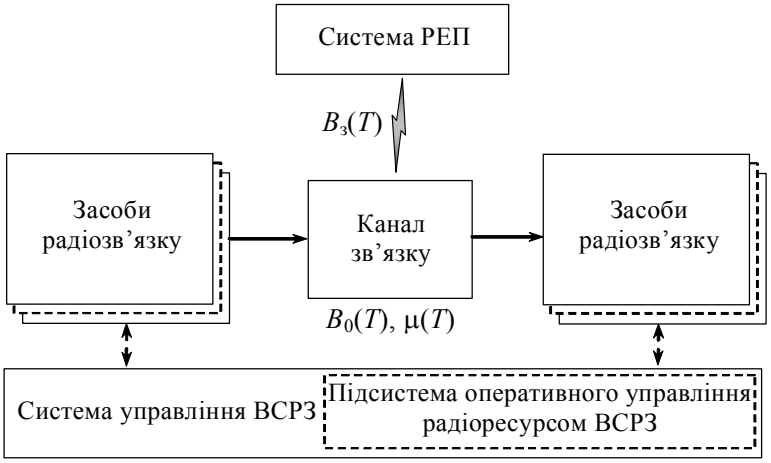


Рис. 3. Місце підсистеми оперативного управління радіоресурсом в структурі ВСРЗ

Структура підсистеми управління радіоресурсом ВСРЗ представлена на рис. 4, де $X(T)$ – вектор заданих впливів; $Y(T)$ – вектор вихідних впливів; $\Sigma(T)$ – вектор помилки (відхилення) параметрів системи від заданого значення; $H(T)$ – вектор оцінок параметрів каналу зв'язку та стану ВСРЗ; $U(T)$ – вектор оптимальних стратегій управління ВСРЗ; $W(T)$ – вектор керуючих впливів; $\Delta H(T)$ – вектор корекції параметрів і режимів роботи ВСРЗ.

До узагальнених функцій підсистеми управління радіоресурсом можна віднести: контроль за поточним станом об'єктів, що ґрунтується на зборі й інформаційній обробці контрольованих параметрів; визначення ступеня невідповідності значень поточних параметрів заданим; ухвалення рішення про зміни в ВСРЗ; виконання рішення; автоматичне стеження за основними параметрами системи для прогнозування їх змін і т.д.

Ієрархічна структура системи радіозв'язку, як різновиду адаптивної системи, що автоматично змінює структуру, алгоритми роботи і параметри радіоапаратури з метою забезпечення необхідного показника якості зв'язку при зміні зовнішніх умов однозначно визначають рівні управління її адаптацією. Розглянемо детальніше функції процедур адаптивного (оперативного) управління, що властиві даній системи (табл. 1).

На системному рівні процедури адаптації забезпечують управління прикладними процесами, терміналами, адміністративне управління мережею. На мережевому рівні процедури адаптації забезпечують вибір маршруту доставки повідомлень, управління

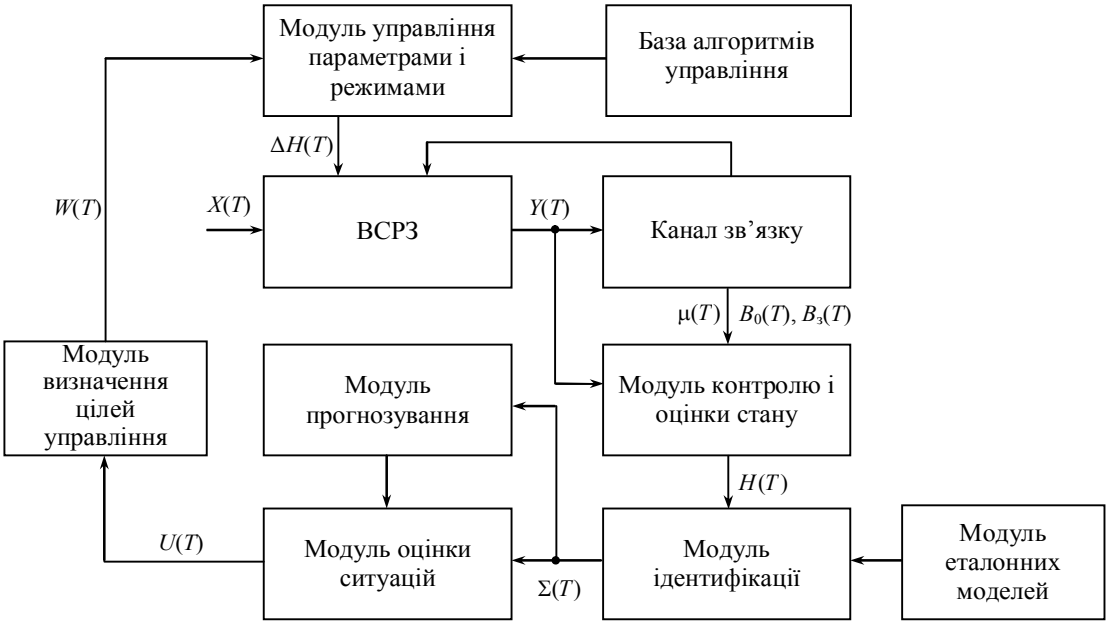


Рис. 4. Структура підсистеми управління радіоресурсом ВСРЗ

потоками повідомлень, протоколами і обміном даними, процедури конфігурації мережі. На рівні каналу зв'язку процедури адаптації забезпечують управління вибором робочої частоти, зондування середовища поширення радіохвиль і дослідження якості частотного каналу, спостереження за інтенсивністю використання частотного каналу, множинний доступ абонентів до ресурсу каналу.

Таблиця 1

Функції процедур адаптивного управління

Рівні адаптації	Функції процедур адаптивного управління	Робочий об'єкт
Рівень адаптації системи (прикладний)	Високорівневе управління системою Управління системою вибору частот Відновлення системи в надзвичайних ситуаціях	система
Рівень адаптації мережі (мережевий)	Маршрутизація повідомлень Адаптація маршрутів Управління потоками Управління протоколами Управління обміном даними Реконфігурація мережі	мережа
Рівень адаптації каналу (канальний)	Процедури вибору робочих частот Зондування середовища поширення радіохвиль Випробування якості каналів (оцінка каналу) Розподіл пропускної спроможності каналу	канал
Рівень адаптації фізичної передачі (фізичний)	Швидкість передачі даних Зміна виду модуляції Зміна завадостійкого кодування Зміна потужності передачі Адаптивне управління нулями діаграми спрямованості антени	фізична передача

На рівні фізичної передачі процедури адаптації забезпечують управління швидкістю передачі даних, видом модуляції, завадостійким кодуванням, управління потужністю передавача, типом і діаграмою спрямованості випромінювання антени [9, 10].

Розглянемо докладніше процедури різних рівнів адаптації, що мають відношення до пошуку рішення задачі підвищення ефективності функціонування ВСРЗ (окремих радіоліній).

Адаптивне управління на рівні каналу зв'язку забезпечує роботу каналу зв'язку радіолінії, тобто від пункту до пункту, включаючи управління вибором повного набору

робочих частот, проведення зондування середовища поширення радіохвиль, спостереження за станом виділених частотних каналів радіолінії.

На канальному рівні основна увага приділяється методиці проведення безпосередніх випробувань виділеного частотного робочого каналу – системі оцінки якості каналу зв'язку в реальному часі – Real-Time Channel Evaluation (RTCE). Процедура збору інформації RTCE – це автоматична технологія, що дозволяє приймачу проводити аналіз заданого списку робочих частот (сканування) з метою накопичення інформації, яка одержується за допомогою пасивних або активних методів контролю якості радіоканалу.

При підготовці заданих частотних каналів радіолінії до використання повинне виконуватися їх ранжирування з урахуванням отриманих оцінок якості, таких як рівень завад, ймовірність помилкового приймання, розбірливість мови. Таким чином, при тестуванні заданих частотних каналів окремої радіолінії, досліджуються характеристики тільки вибраних частотних каналів, передбачених до використання для зв'язку по даній радіолінії. Запропоноване рішення значно скорочує час отримання оцінок стану каналів і відповідної автоматичної настройки апаратури, а також підвищує точність оцінювання.

Отримані дані ранжирування використовуються не тільки для визначення ступеня готовності частотного каналу для передачі повідомлень, але і для визначення статистики зміни його якості, пропускної здатності або інтенсивності використання.

Розглянемо детальніше адаптивне управління, що використовуються в радіолінії на фізичному рівні. Дана процедура управляє параметрами сигналу, що передається по каналу зв'язку: швидкістю передачі, видом модуляції, параметрами завадостійкого коду, потужністю передачі, типом і діаграмою спрямованості антени.

Управління швидкістю передачі. При високій якості каналу зв'язку, швидкість передачі даних повинна бути встановлена максимально можливою. Проте за несприятливих умов для забезпечення необхідної надійності передачі даних в процесі адаптації швидкість передачі даних може бути знижена. Відповідно, адаптивна система автоматизованого управління апаратурою радіолінії повинна будуватися так, щоб спроби встановлення зв'язку починалися з максимальної швидкості передачі, а потім, якщо відношення кількості помилок на біт переданої інформації (ймовірність помилки), виявляється надмірно великим, система знижує швидкість передачі даних у спробі надійно закінчити процедуру передачі.

Управління видом модуляції. Вибір виду модуляції в складній радіоелектронній обстановці є критичним для радіозв'язку через нестаціонарність каналу зв'язку. Вид модуляції при зміні пропускної спроможності каналу повинен вибиратися оптимальним чином для забезпечення заданої ймовірності помилки. При зниженні якості каналу, тобто при зростанні контрольованої ймовірності помилок, для підвищення надійності демодуляції кратність модуляції може бути понижена, що також призводить до зниження загальної пропускної спроможності каналу передачі інформації.

Управління параметрами завадостійкого коду. Розглядаючи управління завадостійкістю кодування, відзначимо, що способи кодування з виправленням помилок забезпечують різні ступені надійності передачі даних і безпеки передачі. Залежно від стану каналу можуть бути вибрані ті або інші способи завадостійкого кодування. Адаптивне управління (за критерієм забезпечення заданої ймовірності помилки) структурою завадостійкістю коду дозволить забезпечити в конкретних умовах максимальну пропускну здатність каналу зв'язку.

Відзначимо, що для забезпечення високої швидкості і завадостійкості передачі інформації по радіолінії вибір швидкості передачі даних, видів модуляції і кодування повинен визначати оптимальний спосіб заповнення використовуваного сигнального простору. Тому вважається, що вибір всіх трьох вищевикладених способів управління сигнального рівня повинен бути взаємоузгодженим. Тоді єдина сигнально-кодова конструкція (СКК) забезпечить поліпшення загальної енергетичної і частотної ефективності використання радіоканалу [10]. Таким чином, управління швидкістю передачі інформації по радіолінії

забезпечується вибором узгодженої зі станом каналу сигнально-кодової конструкції, що забезпечує в заданих умовах необхідну завадостійкість передачі при високій спектральній ефективності.

Управління потужністю. Важливою є процедура адаптивного управління рівнем потужності канального сигналу. Техніка стеження за ефективністю потужності випромінювання дозволяє оцінити достатність її рівня для забезпечення заданої дальності і надійності радіозв'язку. Процедура адаптивного управління потужністю дозволяє понизити потужність випромінювання в умовах необхідності забезпечення роботи радіоліній і не встановлювати її рівень надмірно високим за добрих умов розповсюдження, тобто при забезпеченні прийнятного відношення сигнал/завада в заданій точці приймання. Адаптивне зниження потужності випромінювання є досить ефективним для системи з погляду електромагнітної сумісності, електромагнітної безпеки і розвідзахищеності.

Управління діаграмою спрямованості антени. Адаптивне управління діаграмою спрямованості антени також є ефективним способом підвищення якості радіозв'язку. Адаптивні антени відповідно до встановленої методики можуть бути оперативно перебудовані головним пелюстком діаграми спрямованості по заданим напрямом роботи, а нулями – по напрямах заважаючих випромінювань. Доцільність перестроювання діаграми спрямованості антени також визначається процедурою RTCE і величиною ймовірності помилкового приймання.

Підводячи підсумки виконаного аналізу способів адаптації, передбачених до використання, відзначимо, що для забезпечення надійної роботи радіоліній, відповідно до даних таблиці 1, найбільш ефективними виявляються:

на мережевому рівні – вибір маршруту доставки повідомлень;

на канальному рівні – процедури вибору робочих частот та оцінки якості каналів;

на фізичному рівні – процедури управління потужністю передачі, видом модуляції та завадостійкого коду.

Таким чином, актуальним напрямком підвищення ефективності функціонування сучасних військових систем радіозв'язку в умовах активної радіоелектронного протидії є комплексне координування частотних, енергетичних, часових і просторових ресурсів радіоканалів з врахуванням характеристик комплексу зовнішніх умов їх реалізації на принципах оперативного (адаптивного) управління. Оперативне управління радіоресурсом військової системи радіозв'язку повинно мати комплексний характер, тобто враховувати можливості фізичного, канального, мережевих рівнів.

ЛІТЕРАТУРА

1. *Романюк В. А.* Направления развития тактических сетей связи // Зв'язок. – 2001. – № 3. – С. 63 – 65.

2. *Баушев С. В., Передрий А. В.* Разработка перспективных систем связи вооруженных сил США и Объединенных вооруженных сил НАТО // Зарубежная радиоэлектроника. – 2000. – № 7. – С. 3 – 20.

3. *Кондратьев. А.* Перспективный комплекс РРТР и РЭВ сухопутных войск США „Профет" // Зарубежное военное обозрение. – 2008. – № 7. – С. 22 –28.

4. *Стрелецкий А.* Американский перспективный наземный комплекс ведения радиоэлектронной войны „Вулфпак" // Зарубежное военное обозрение. – 2002. – № 10. – С. 27 – 28.

5. *Фрадков А. Л.* Адаптивное управление в сложных системах: беспоисковые методы. – М.: Наука, 1990. – 296 с.

6. *Стеклов В. К.* та ін. Оптимізація та моделювання пристроїв і систем зв'язку : Підр. для вищ. навч. закл. – К.: Техніка, 2004. – 576 с.

7. *Коричнев Л. П., Королев В. Д.* Статистический контроль каналов связи. – М.: Радио и связь, 1989. – 240 с.

8. *Міночкін Д. А., Борисов І. В.* Метод контролю стану каналу зв'язку із селективними завмираннями // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2006. – Вип. 3. – С. 66 – 71.

9. *Шаров А. Н.* Автоматизированные сети радиосвязи. – Л.: ВАС, 1988. – 178 с.

10. *Григорьев В. А., Лагутенко О. И., Распаев Ю. А.* Сети и системы радиодоступа. – М.: Око-Трендз, 2005. – 384 с.

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

ІНТЕЛЕКТУАЛЬНІ МОБІЛЬНІ РАДІОМЕРЕЖІ

Існуючі та можливі загрози національній безпеці держави обумовлюють появу нових концепцій її забезпечення. Забезпечення військової безпеки передбачає готовність збройних сил (ЗС) держави до майбутніх війн чи збройних конфліктів. На сьогоднішній день в ЗС розвинених у військовому відношенні держав світу проводяться глибокі якісні перетворення, обумовлені бурхливим науково-технічним прогресом та інформаційною революцією [1 – 3].

Значна робота експертів та дослідників військового відомства США привела до появи великої кількості нових військових концепцій та теорій, спрямованих на підвищення ефективності дій американських ЗС. Однією з таких теорій стала концепція „мережецентричної війни” (*Network-Centric Warfare*, NCW), яка з'явилася в США в кінці 90-х років. До сьогоднішнього дня ця концепція не тільки завоювала своїх чисельних прихильників, але й була прийнята за основу діючих програм розвитку та удосконалення ЗС багатьох країн світу [3 – 6].

Наприклад, в Австралії здійснюється розробка та тестування перспективних засобів зв’язку та передачі даних, які повинні дозволити одному оператору здійснювати управління угрупованням робототехнічних засобів, призначених для вирішення розвідувальних задач. У Франції такі заходи реалізуються в рамках концепції під назвою „Інформаційно-центрична війна” (*Guerre Infocentre*), яка в більшій мірі акцентує увагу на інформаційних потоках, а не на самих мережах, як у ЗС США. Німеччина також працює над створенням перспективної системи оснащення та озброєння особового складу (*Infanterist der Zuknft*). Проводиться розробка перспективних засобів розвідки, персональних комп’ютерних систем, військових систем управління типу „тактичний інтернет” та ін. У Великобританії формується власна глобальна інформаційна структура, яка являє собою єдину інформаційно-управляючу мережу зі спеціалізованими системами забезпечення безпеки і яку планується використовувати для організації доступу до інформаційних ресурсів ЗС союзників (США, Канади та ін.) [4].

Засновники концепції „мережецентричної війни” представили її не як новий тип війни, а як новий підхід до організації та ведення бойових дій, шляхом створення єдиного інформаційно-комунікаційного простору на всьому театрі бойових дій. Модель „мережецентричної війни” представляється у вигляді розгалуженої мережі добре інформованих, але географічно рознесених сил (рис. 1).

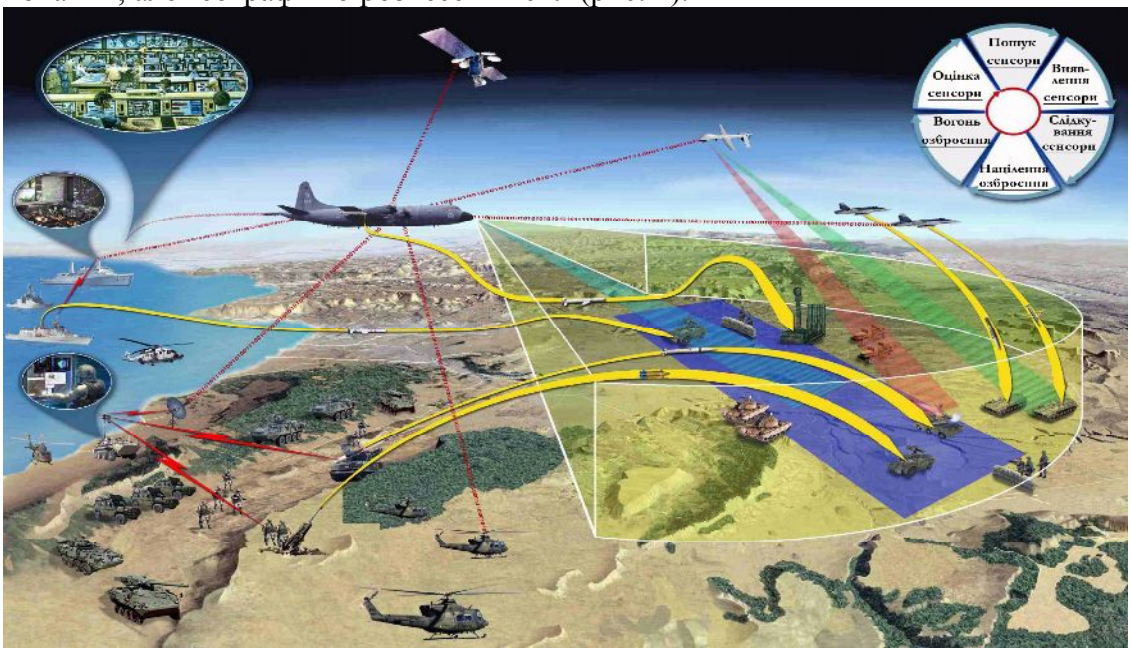


Рис. 1. Мережецентрична концепція ведення бойових дій

Головними компонентами цих сил є: високоефективна „інформаційна площина”, призначена для отримання всієї необхідної інформації, в тому числі від мережі сенсорів (засобів розвідки); високоточна зброя; високоефективна система управління та командування; надійна інформаційно-комунікаційна мережа для зв’язку джерел інформації (розвідки), органів управління та засобів ураження, що забезпечить доведення до учасників військових операцій достовірної та повної інформації про обстановку в режимі реального часу.

В цілому, зміст „мережі” чи „мережевого принципу” полягає в тому, що головним елементом всієї моделі управління військами є „обмін інформацією” – максимальне розширення форм і способів отримання цієї інформації, доступу до неї та її розподіл. Тому, враховуючи досягнення в області побудови тактичних систем зв’язку розвинених у військовому відношенні країн світу, в програмі розвитку військ зв’язку ЗС України до 2015 року передбачене створення багаторівневої мобільної компоненти (МК) мереж зв’язку військового призначення [7]. Інтенсивний розвиток інформаційних та телекомунікаційних технологій дозволив запропонувати у якості основи перспективної МК використання мобільних радіомереж (МР) – мереж радіозв’язку загального користування, що будуються за технологією MANET (*Mobile Ad-Hoc Networks*) [8, 9].

На рис. 2. зображено ієрархічну архітектуру перспективної МК, яка складається з мобільних радіомереж 4-х рівнів: 0-й – сенсорні мережі; 1-й – мобільні радіомережі низової ланки управління; 2-й – мережі мобільних базових станцій (МБС), що утворять опорну мережу; 3-й – повітряна мережа, яка може бути реалізована на безпілотних літальних апаратах (БЛА). В якості перспективного запропоновано введення 4-го рівня на базі систем супутникового зв’язку.

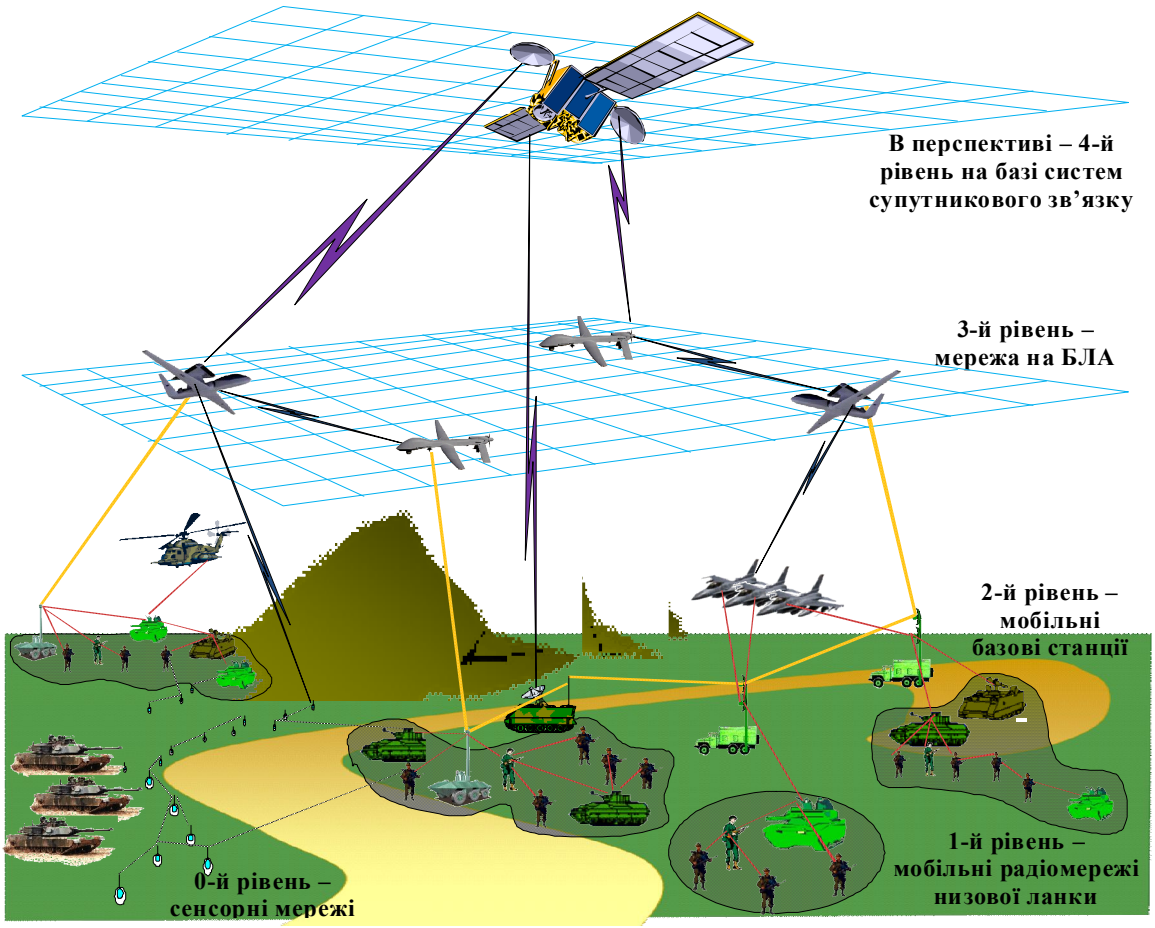


Рис. 2. Архітектура перспективної мобільної компоненти

В ролі джерел інформації в запропонованій архітектурі МК можуть виступати сенсорні мережі (0-й рівень), абоненти мобільних радіомереж низової ланки управління (1-й рівень) а також повітряна мережа на БЛА (3-й рівень). Від них інформація через радіоканали поступає на пункти управління, де обробляється і на її основі приймаються рішення з управління бойовими одиницями (солдат, танк, літак, БЛА, робототехнічний засіб і т.д.).

Під вузлом МР відповідного рівня МК розуміється термінал (сенсорний пристрій, переносний комп'ютер, робот, мобільна базова станція та ін.) оснащений радіомодемом, який одночасно виконує функції кінцевого пристрою та маршрутизатора. Кожному з рівнів перспективної МК характерна низка особливостей (таблиця 1), які необхідно враховувати при проектуванні та розробці протоколів і методів управління МР [8, 9]:

– динамічна топологія (вузли мобільні, канали радіозв’язку з обмеженою дальністю й пропускною спроможністю);

– значна розмірність мереж;

– неоднорідність елементів мережі (за мобільністю й рівнем продуктивності);

– колективний характер використання каналів зв'язку;

– обмежені потужність і час передачі абонентів, оснащених радіотерміналами з акумуляторними батареями;

– обмежена безпека.

Таблиця 1

Основні характеристики	**Сенсорні мережі – 0-й рівень**	**Мобільні радіомережі – 1-й рівень**	**Мережа МБС – 2-й рівень**	**Мережа на БЛА – 3-й рівень**
Розмірність	Сотні-тисячі	Сотні-тисячі	Десятки	Десятки
Принцип організації та побудови	Самоорганізація мережі, комутація пакетів, кожен вузол – маршрутизатор інформаційних повідомлень			
Мобільність	Низька	Висока	Низька	Дуже висока
Тип та спосіб управління	Розподілений, (ієрархічний), технологічний	Розподілений, технологічний	Зоновий, організаційно-технологічний	Зоновий, організаційно-технологічний
Способи розподілу радіоресурсу	Випадковий	Випадковий	Детермінований, гібридний	Детермінований
Потужність передавача терміналу; відстань зв’язку та швидкість передачі (залежать від частоти, потужності передавача, типу антени тощо)	Визначається типом сенсорів; (для наземних – мВт, сотні метрів >0.01 Мб/с)	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	Десятки Вт; десятки км; >20 Мб/с

У радіомережі простір, частота, код і час – чотири основні складові, які визначають розподіл загального ресурсу радіоканалу. Ефективне використання спектру радіочастот – одне з основних завдань під час управління МР. Недавно навіть було визначено нове поняття „когнитивне радіо” (*cognitive radio*) – нова технологія, що дозволяє використовувати спектр частот динамічним способом і володіє двома основними характеристиками (рис. 3) [10]:

– *здатність до пізнання* – визначає можливість збирати або вимірювати інформацію про радіосередовище. Причому ця можливість реалізується не тільки шляхом простого моніторингу потужності передачі в деяких смугах частот, а за рахунок використання більш складних технологій (наприклад, самонавчання й прийняття рішень) для збору відомостей про часові й просторові параметри мережі, а також для виключення взаємних перешкод між користувачами. Це дозволить визначити ту частину спектру, що не використовується під час функціонування мережі, а, отже, вибрати такі параметри передавача, які найточніше відповідають сформованій обстановці в мережі;

– *реконфігурованість* – визначає здатність вузла динамічно налаштовувати (програмувати) параметри прийомопередавача відповідно до параметрів радіосередовища. Тобто, прийомопередавач може бути запрограмований приймати й передавати сигнали на різних частотах, а також використовувати різні технології доступу до радіосередовища, які підтримуються його апаратними можливостями.

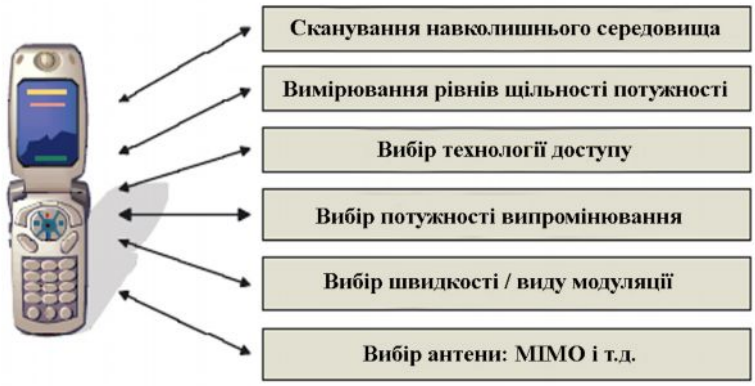


Рис. 3. Функції інтелектуальних засобів радіозв'язку з управління радіоресурсом

Крім управління радіоресурсом, особливості функціонування МР та специфіка завдань, які покладаються на них, вимагають вирішення низки інших задач управління, основними з яких є: управління маршрутизацією, топологією, потоками даних, безпекою та виконання підвищених вимог щодо забезпечення доставки великих обсягів інформації із заданою якістю [11, 12]. Крім того, функціонування МР відбуватиметься в умовах частої зміни обстановки (оперативної, тактичної, зі зв’язку, тощо), тому забезпечення стійкого, безперервного і прихованого управління мережею в цих умовах неможливе без ефективної системи управління, здатної приймати управляючі рішення в умовах невизначеності. Основними причинами невизначеності є:

– складність формалізованого опису МР та задач управління ними з врахуванням похибок при обчисленнях та вимірюваннях;

– нечіткість цілей функціонування та задач управління;

– нестаціонарність параметрів МР та системи управління ними (висока мобільність абонентів, зміна і непередбачуваність топології мережі);

– апріорна невизначеність обстановки та умов функціонування МР;

– наявність випадкових та навмисних впливів зовнішнього середовища (засоби знищення та радіоелектронного подавлення);

– викривлення інформації під час передачі в каналах радіозв’язку та ін.

Забезпечення здатності МР до самоорганізації, а також адаптації її елементів до різних умов функціонування вимагає розробки нових методів управління із залученням технологій обробки знань. Проблеми обробки та використання знань, як ефективного засобу аналізу погано формалізованих задач при апріорній неповноті та нечіткості вихідних даних були і залишаються головним предметом вивчення в теорії штучного інтелекту.

На сьогоднішній день системи управління інтенсивно розвиваються в напрямку їхньої інтелектуалізації, при цьому істотно змінюється технологія прийняття управлінських рішень. Інтелектуальні інформаційні системи (ІІС) поєднують можливості систем управління базами даних і технологію штучного інтелекту, завдяки чому зберігання управлінської інформації в них поєднується з обробкою й підготовкою її для використання при прийнятті рішень.

Тривалий час вважалося, що ІІС ефективні лише для вирішення так званих неформалізованих і погано формалізованих завдань, пов’язаних з необхідністю включення в алгоритм їхнього вирішення даних про навчання на реальному експериментальному матеріалі (наприклад, завдання розпізнавання образів). Однак поява принципово нового різновиду мереж зв’язку (мережі класу MANET) і, відповідно, завдань управління ними, пов’язаних з підтримкою необхідних режимів функціонування складних динамічних об’єктів

в умовах невизначеності, потребувала розвитку специфічних методів їхнього вирішення із залученням технології штучного інтелекту. Тому, останнім часом ІІС все ширше використовуються при вирішенні завдань у системах зв'язку й телекомунікацій: управління комутацією, маршрутизація, управління трафіком, розподіл каналів у рухомих системах радіозв'язку і т.д. [13].

Наведемо деякі доводи на користь того, що ІІС повинні стати найважливішою складовою частиною системи управління вузла мережі класу MANET:

– по-перше, головною проблемою при управлінні мережею MANET є необхідність вибору з безлічі можливих управлінських рішень в залежності від ситуації, яка склалася в мережі, а також вимог до передачі певного типу трафіка;

– по-друге, управління мережею вимагає обробки великого обсягу службової інформації про її стан, що використовується методами управління різних рівнів моделі OSI для прийняття відповідних рішень. Проблема одержання інформації з об'єктів (вузлів мережі), що функціонують у реальному масштабі часу, на сьогоднішній день вирішена (використання різних способів зондування мережі). Але це породило іншу проблему: як зменшити об'єм службової інформації до рівня, який дійсно необхідний для ухвалення рішення системою управління? У той же час слід зазначити, що втрата службової інформації, яка надходить від вузлів мережі, що працюють у реальному масштабі часу, може істотно позначитися на кінцевому рішенні, прийнятому системою управління;

– по-третє, нестача часу на прийняття рішень і проблема координації взаємодії методів управління, що виконують різні функції (потоками даних, управління маршрутизацією, топологією, енергоспоживанням, безпекою та ін.).

На рис. 4 зображена узагальнена модель інтелектуальної системи управління вузлом МР, елементом якої є підсистема управління потоками даних. Система управління має досить складну структуру, яка включає до свого складу низку функціонально-підлеглих підсистем. Ієрархія їхнього підпорядкування спричиняє декомпозицію вихідної мети управління на послідовність вкладених складових. Такий поділ передбачає багаторівневу організацію системи управління, яка володіє розвиненими інтелектуальними можливостями щодо аналізу й розпізнавання обстановки, формування стратегії доцільної поведінки, планування послідовності дій, а також синтезу управляючих впливів, спрямованих на задоволення вимог до обслуговування певних типів трафіка.

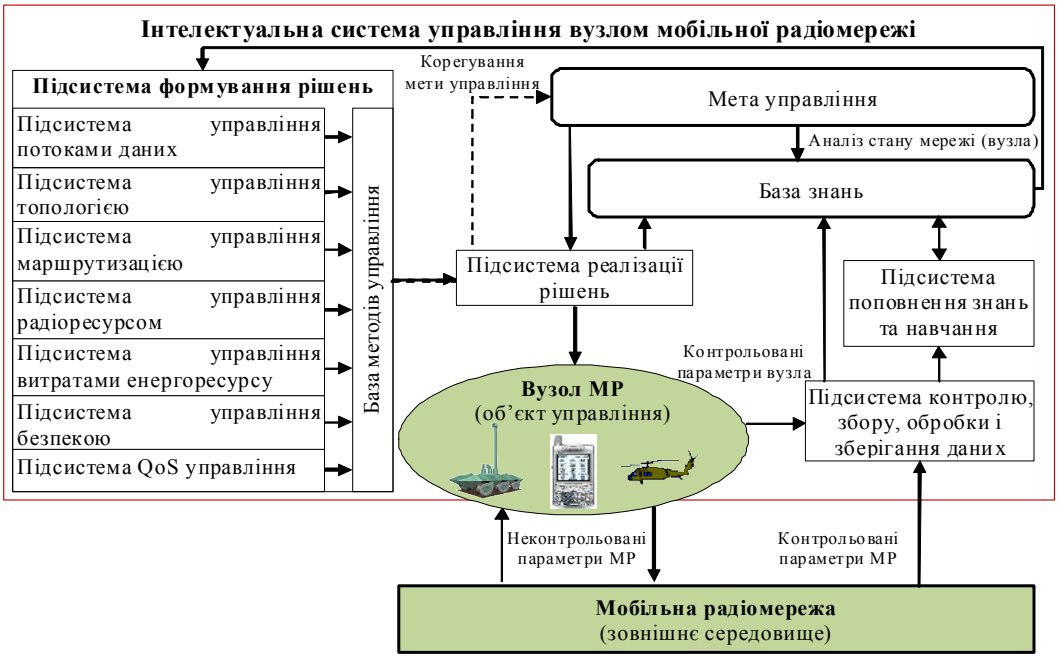


Рис. 4. Узагальнена модель інтелектуальної системи управління вузлом мобільної радіомережі

Важливо зазначити, що головна архітектурна особливість, яка відрізняє запропоновану інтелектуальну систему управління від побудованої за „традиційною” схемою, пов’язана з підключенням механізмів зберігання й обробки знань (блок „*база знань*”) для реалізації здатності виконувати необхідні функції в умовах невизначеності (неповноти інформації) при випадковому характері зовнішніх впливів. В базі знань міститься інформація про принципи побудови системи управління та мету її функціонування, специфіку використання різних методів управління, а також особливості функціонування підсистеми реалізації рішень та самого об’єкту управління. Крім того, до складу системи управління, у разі необхідності, може входити *підсистема поповнення знань та навчання*, яка забезпечує узагальнення накопиченого досвіду і, таким чином, поповнює базу новими знаннями.

Підсистема контролю, збору, обробки і зберігання даних призначена для вимірювання контрольованих параметрів мобільних вузлів та радіомережі в цілому. Різні функції (рівні) управління вимагають різного обсягу (кількості параметрів) і глибини збору інформації про стан мережі. Глибина збору *i*-м вузлом мережі звичайно визначається відстанню (площею при наявності системи позиціонування), яка задається кількістю ретрансляційних ділянок від даного вузла. Звичайно, знання повної інформації про мережу дозволяє приймати більш обґрунтовані рішення, однак приводить до значного зростання службового трафіка в умовах динаміки топології і вхідного навантаження.

Підсистема формування рішень побудована за принципом функціональності управління, який передбачає об’єднання функцій системи управління у відносно незалежні групи, що дозволяє здійснити декомпозицію управління мережею на підсистеми (що значно спрощує задачу розробки математичного забезпечення управління).

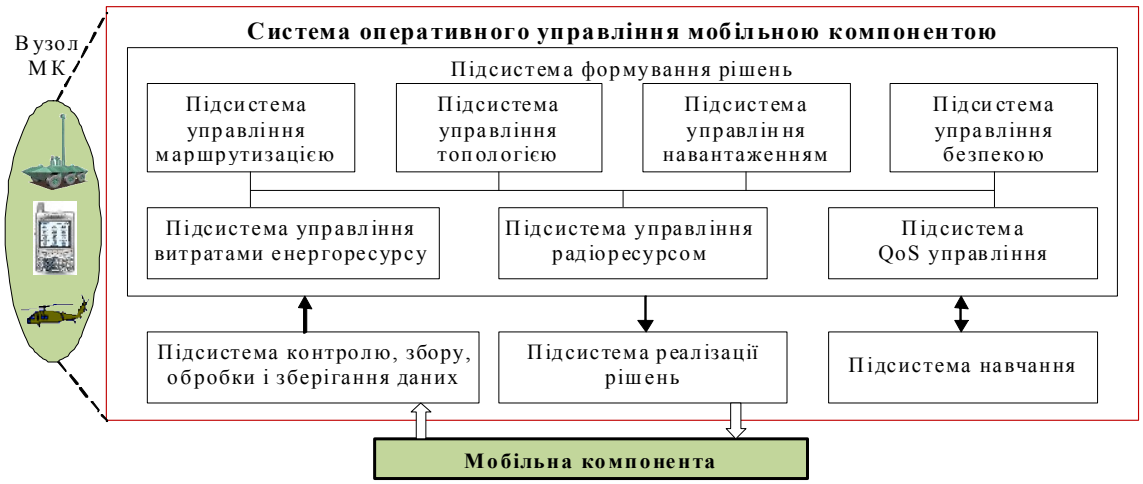


Рис. 5. Функціональна модель системи управління мобільною компонентою

За функціями задачі управління МК діляться на дві групи [11, 12]:

1) *спеціальні задачі управління* (наприклад, визначення маршрутів польоту БЛА й координація їхнього переміщення).

2) *універсальні задачі управління* – характерні для радіомереж всіх рівнів МК: управління топологією, управління маршрутизацією, управління навантаженням, управління радіоресурсом, управління енергоресурсом, управління безпекою. Однак, конкретна реалізація методів управління вузлом МР повинна враховувати призначення та особливості архітектури МК (розмірність, мобільність, продуктивність та ін.). Пропонується здійснювати вирішення універсальних задач управління вузлом МР за різними рівнями еталонної моделі взаємодії відкритих систем. Проведені дослідження показують відсутність єдиного методу управління вузлом МР, який забезпечує оптимізацію мережевих показників на кожному з рівнів моделі OSI, так як кожен з існуючих методів має свої межі ефективного застосування. У зв’язку з цим запропоновано ввести до складу підсистеми формування рішень вузлової системи управління (рис. 4) множину методів, які виконують відповідні функції на різних

рівнях моделі OSI. Множина цих методів утворює базу методів управління, яка взаємодіє з підсистемою реалізації рішень (містить знання про мету управління, методи її досягнення чи корегування) для координації взаємодії методів управління різних функціональних підсистем за рівнями моделі OSI з метою забезпечення оптимізації показників функціонування мережі.

Крім цього, для зменшення об'ємів службового трафіка виникає доцільність використання методами одного рівня моделі OSI службової інформації, отриманої на інших рівнях. Наприклад, якщо існуючі маршрути (мережевий рівень OSI) не відповідають вимогам до швидкості передачі інформації, то їх можна не перебудовувати (тобто не витрачати ресурси мережі на побудову нових маршрутів), а здійснити адаптацію швидкості та затримки передачі пакетів, використовуючи методи транспортного рівня моделі OSI. Тобто виникає задача інтеграції різних рівнів еталонної моделі OSI, вирішення якої також покладається на підсистему реалізації рішень. Основна складність інтеграції полягає у необхідності визначення параметрів, які будуть використовуватися між рівнями OSI. Організація елементів інтелектуальної системи управління мережею припускає використання сукупності моделей подання знань, інформаційної підтримки, опису контрольованого об'єкту і т.д. Головною відмінністю побудови інтелектуальної системи управління МР є використання методів і технологій штучного інтелекту, як основних засобів боротьби з невизначеністю зовнішнього середовища. Практичне втілення цієї концепції припускає вибіркове використання тих або інших технологій обробки знань залежно від специфіки розв'язуваних завдань і особливостей об'єкта управління. Найбільш перспективними для створення інтелектуальних систем управління представляються чотири технології [13]: експертних систем, асоціативної пам'яті, нечіткої логіки, нейронних мереж (таблиця 2). Основна ідея при цьому полягає в переході від строго формалізованих алгоритмів, які пропонують метод вирішення завдання, до логічного програмування з вказівкою на те, що потрібно вирішувати на базі знань, накопичених фахівцями в конкретних предметних областях.

Таблиця 2

Властивості інтелектуальних технологій

Властивість / Технологія	**Представлення знань**	**Формування початкових знань**	**Організація логічного висновку**	**Можливість поповнення**	**Пояснення прийнятих рішень**	**Спосіб реалізації та відносна швидкодія**
Експертних систем	В явному вигляді з допомогою продукційних правил та семантичних мереж	З допомогою експерта в інтерактивному режимі	Шляхом явного співставлення початкового запиту з категоріями багаторівневої класифікації, заданої ієрархією продукційних правил	Шляхом вимірювання продукційних правил, семантичних мереж та інших представлень	За рахунок аналізу активізованого ланцюга логічного виводу	Програмний, низька
Асоціативної пам'яті	В неявному вигляді, в формі гіперповерхні в багатомірному просторі ознак та архітектурі асоціативної пам'яті	Шляхом автоматичного формування асоціативних зв'язків за заданим алгоритмом	Шляхом проекції робочої точки гіперповерхні на осі вибраної поверхні координат	Шляхом вимірювання простору параметрів та форми відповідної гіперповерхні	Відсутнє, але може бути забезпечене шляхом введення додаткової координати з поясненням	Програмний, апаратний, висока
Нечіткої логіки	В напівприхованому вигляді з допомогою продукційних правил і функції приналежності	З допомогою експерта в інтерактивному режимі або в автоматичному режимі на основі вимірювання статистичних даних	Забезпечується шляхом виконання продукційних правил та вибраним методом обробки функцій приналежності	За рахунок зміни системи правил, форми та відносного розміщення функцій приналежності на базових осях	Відсутнє, але може бути забезпечена за рахунок аналізу додаткових правил	Програмний (висока), апаратний (низька)
Нейромережевих структур	В неявному вигляді в архітектурі мережі, параметрів нейронів та зв'язків	На прикладі навчальної вибірки з допомогою алгоритмічних процедур налаштування в автоматичному режимі	Забезпечується логікою роботи мережі	Шляхом зміни топології, структури і параметрів мережі	Відсутнє, але може бути організоване за рахунок введення додаткової пояснюючої нейромережі	Апаратний, висока

Основною відмінністю *технології експертних систем* є можливість роботи з формами явного представлення знань, включаючи продукційні правила, предикати та семантичні мережі. Яскраво виражена структурованість цих форм обумовлює можливість застосування формалізованих логічних методів для аналізу та перетворення знань, а також робити логічні висновки за сукупністю вихідних даних. Однак, формування початкових знань з допомогою експертів, що відбувається в інтерактивному режимі, спричиняє низьку швидкодію цієї технології і ускладнює її використання в системах управління динамічними об'єктами.

Технологія асоціативної пам'яті передбачає використання механізмів відновлення цілісних образів за їх окремими елементами і зводиться до роботи з багатомірними масивами пам'яті. Знання мають неявну форму представлення і задають класифікацію понять деякої предметної області у вигляді сукупності ознак, характерних кожній якісній категорії. Основна перевага такого підходу полягає у швидкодії систем обробки знань та в простоті програмного і апаратного виконання. Однак, проблеми виникають під час формування та збереження знань, які, з одного боку, повинні займати якомога менше пам'яті, а з іншого – забезпечувати задані показники якості управління.

Технологія нечіткої логіки орієнтована на обробку логіко-лінгвістичних моделей представлення знань. Моделі такого типу призначені для формалізації неточних, розмитих в змістовному відношенні тверджень і будуються з використанням узагальнених категорій, які задають класифікацію вихідних понять на рівні нечітких множин (функцій приналежності). Ефективність застосування нечітких моделей залежить від кількості термів для кожної лінгвістичної змінної та від виду функції приналежності, які визначаються експертами в конкретній області знань.

Технологія нейромережевих структур на сьогоднішній день є одним з перспективних підходів до організації обробки неявних форм представлення знань та побудови інтелектуальних систем управління. Вона передбачає формування однорідних структур, які складаються з множини взаємопов'язаних елементів із заданою характеристикою перетворення сигналів. Сукупність знань, які задаються в процесі навчання такої структури, визначається настройкою вагових коефіцієнтів міжелементних зв'язків. Перевагою нейромережевих структур є висока швидкодія, яка забезпечується паралельною обробкою інформації при їх апаратній реалізації, а також можливість отримання нової інформації в проблемній області в формі деякого прогнозу. До недоліків нейронних мереж можна віднести те, що знання про проблемну область подаються в спеціальному вигляді, який може суттєво відрізнятися від змістовної інтерпретації зв'язків елементів мережевої структури [14].

Як показують результати аналізу різних робіт стосовно розвитку методів обробки знань, однією з передових тенденцій в цій області є спроба інтеграції різних технологій з метою об'єднання характерних їм переваг. Так, наприклад, одночасне забезпечення високої функціональної гнучкості та швидкодії може досягатися шляхом комплексного застосування нечітких нейронних мереж. З одного боку, вони дозволяють розробляти та представляти моделі систем в формі правил нечітких продукцій, які характеризуються наочністю та простотою змістовної інтерпретації. З іншого боку, для побудови правил нечітких продукцій використовуються методи нейронних мереж, що є більш зручним та менш трудомістким процесом для системних аналітиків.

Таким чином, у найближчій перспективі необхідно говорити про створення „інтелектуальних мобільних радіомереж". Вже зараз в архітектурі вузла передбачається наявність баз даних і знань, електронної карти місцевості, підсистеми навчання (рис. 4), застосування технології розподілених інтелектуальних агентів і т.д. Введення ІІС у систему управління вузлом МР дозволить оптимізувати процес управління, мінімізувати помилки, пов'язані з ухваленням неправильного рішення з управління мережею, шляхом врахування ситуації в мережі, а також вимог до передачі трафіка. Крім того інтелектуалізація процесу управління вузлом МР дозволить мінімізувати помилки, викликані людським фактором у

процесі ініціалізації мережі, зменшити витрати часу на збір і аналіз службової інформації про стан мережі, а також скоротити обсяги цієї інформації.

В ході подальших досліджень доцільно проводити роботу над розробкою нових інтелектуальних методів управління за рівнями моделі OSI з використанням нечітких нейронних мереж, які характеризуються наочністю та простотою реалізації, що має особливе значення при використанні в малопотужних вузлах мобільної радіомережі.

ЛІТЕРАТУРА

1. Романченко І.С. Мережецентрична 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.
2. Малярчук М.В. Підходи до побудови перспективної системи зв'язку та автоматизованого управління військами в Збройних Силах Російської Федерації / Малярчук М.В., Колачов С.П., Люлін Д.В. // Збірник наукових праць ВІТІ НТУУ "КПІ". – 2009. – № 2. – С. 71 – 76.
3. Геоцентричний театр воєнних дій – нова концепція / [В.В. Опанюк, В.І. Снєцар, Б.Г. Бондарєв, С.Т. Кривоус] // Збірник наукових праць ЖВІ НАУ. – 2009. – № 2. – С. 44 – 53.
4. Борьба за информацию на основе информации [электронный ресурс] / А.Е. Кондратьев // Независимое военное обозрение – 2008. – Режим доступа к журналу:
http://nvo.ng.ru/concepts/2008-10-24/1_info.html.
5. Влияние концепции сетецентрической войны на характер современных операций [электронный ресурс] / М.М. Хамзатов // Военная мысль – 2006. – №7. – Режим доступа к журналу:
http://www.milresource.ru/Hamzatov-article-1.html.
6. Сетевые войны XXI века [электронный ресурс] / Б. Чельцов, С. Волков // Воздушно-космическая оборона. – Режим доступа к журналу:
http://army.lv/ru/Setevie-voyni-XXI-veka/787/4268.
7. Кравченко О.О. Пріоритетні напрямки розвитку системи зв'язку та автоматизації управління військами Збройних Сил України: збірник матеріалів IV науково-технічної конференції „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення] / – К.: ВІТІ НТУУ „КПІ", 2008. – С. 12 – 14.
8. Романюк В.А. Мережі MANET – основа побудови тактичних мереж зв'язку : збірник матеріалів IV Науково-практичного семінару ВІТІ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 15 – 28.
9. Міночкін А.І. Архітектура перспективної мобільної компоненти тактичних мереж зв'язку збройних сил України / Міночкін А.І., Романюк В.А. // Збірник наукових праць ВІТІ НТУУ "КПІ". – 2004. – № 5. – С. 107 – 115.
10. Akyildiz Ian F. CRAHNs: Cognitive radio ad hoc networks / Akyildiz Ian F., Lee Won-Yeol, Chowdhury Kaushik R. // Ad Hoc Networks. – №7, 2009. – pp. 810 – 836.
11. Міночкін А.І., Романюк В.А. Концепція управління мобільною компонентою мереж зв'язку військового призначення // Збірник наукових праць № 3. – К.: ВІТІ НТУУ "КПІ". – 2005. – С. 51 – 60.
12. Міночкін А.І., Романюк В.А., Скрипник Л.В. Управління мобільними радіомережами військового призначення – проблеми та шляхи рішення // Збірник наукових праць № 4. – К.: ВІТІ НТУУ "КПІ". – 2003. – С. 78 – 91.
13. Макаров И.М. Искусственный интеллект и интеллектуальные системы управления / И.М. Макаров, В.М. Лохин, С.В. Манько, М.П. Романов; [отв. ред. И.М. Макарова]; Отделение информ. технологий и вычислит. систем РАН. – М.: Наука, 2006. – 333 с.
14. Комашинский В.И. Нейронные сети и их применение в системах управления и связи / Комашинский В.И., Смирнов Д.А. / – М.: Горячая линия – Телеком, 2002. – 94 с.

д.т.н. Науменко М.І. (ДВОН МОУ)
к.т.н. Черних Ю.О. ДВОН МОУ)
к.пед.н. Приходько Ю.І. (ЦВСД НУОУ)

ПРОБЛЕМИ І НАПРЯМИ СУЧАСНОГО ЕТАПУ РОЗВИТКУ ВІЙСЬКОВОЇ ОСВІТИ

Сучасний світовий цивілізаційний процес визначається глобалізацією, інформатизацією, прогресуючим зростанням значущості гуманітарної сфери, високих інформаційних технологій, підвищенням ролі інтелектуального ресурсу та менеджменту, соціальних, науково-технічних і гуманітарних чинників економічного прогресу. Усі ці та інші сучасні цивілізаційні риси зумовлюють розвиток людини як головну мету, ключовий показник і основний важіль сучасного прогресу, викликають потребу в модернізації освіти, забезпеченні її пріоритетного розвитку. Освіта стає визначальним чинником політичної, соціально-економічної, культурної і наукової життєдіяльності суспільства, важливим стратегічним ресурсом зміцнення держави, її авторитету та конкурентоспроможності на міжнародній арені, забезпечення незалежності, національної оборони і національних інтересів країни, поліпшення добробуту людей [3].

Система військової освіти інтегрована в загальнодержавну систему освіти, побудована за видовим принципом, тісно поєднана з військовою наукою, базується на чинній загальній і відомчій нормативно-правовій базі і включає органи військового управління, мережу вищих військових навчальних закладів (ВВНЗ) та військових навчальних підрозділів вищих навчальних закладів (ВНП ВНЗ). Вона побудована на засадах безперервного ступеневого навчання офіцерських кадрів з урахуванням специфіки їх служби.

Основними принципами військово-освітньої діяльності є:

гуманізація та гуманітаризація навчального процесу, яка має спрямовуватись на формування критичності мислення, традицій відповідної предметної галузі знань, її військової, політичної, соціально-економічної основи, етичних і моральних аспектів, на підготовку випускників до практичної діяльності у військах, інших структурах Збройних Сил України;

спрямованість навчально-виховного процесу на гармонійний розвиток особистості кожного, хто навчається, на формування та розвиток компетенцій; органічне поєднання засвоєння військовими фахівцями світоглядних знань з формуванням здібностей самостійно аналізувати складні явища суспільного життя, творчо застосовувати діалектичний підхід у військово-професійній і суспільній діяльності;

єдність навчання та виховання, теоретичної і практичної підготовки, подолання відриву навчально-виховного процесу від реальних проблем розвитку суспільства, озброєння, військової техніки і військової служби;

інтеграція навчального процесу, наукової, науково-технічної діяльності, розвиток наукових шкіл ВВНЗ; спрямованість наукових досліджень на підвищення наукового рівня змісту навчальних дисциплін та удосконалення методик їх викладання;

підготовка фахівців на основі запровадження у навчально-виховний процес інноваційних, інформаційно-комунікаційних, комп'ютерних, модульних технологій навчання ;

рейтингова оцінка результатів діяльності тих, хто навчається, науково-педагогічних працівників кафедр, факультетів;

військово-професійна спрямованість нормативних навчальних дисциплін освітньо-професійних програм;

системний підхід до вивчення озброєння та військової техніки, застосування методів їх експлуатації і бойового застосування;

коригування змісту, організаційно-методичних засад освітнього процесу на основі всебічного вивчення національного досвіду та досвіду провідних країн світу;

управління якістю підготовки військових фахівців;

всебічність фінансового, матеріально-технічного та інформаційного забезпечення.

Водночас, суттєва зміна структури, чисельності Збройних Сил України, подальший розвиток воєнної стратегії, оперативного мистецтва потребують значних перетворень у системі військової освіти та організації підготовки військових фахівців [2]. Можна констатувати, що теперішній стан військової освіти, темпи та глибина перетворень не повною мірою задовольняють потребам Збройних Сил України та інших військових формувань.

Система військової освіти повинна забезпечувати підготовку військових фахівців з високим рівнем професіоналізму, компетентності, інтелектуального розвитку, загальної та військово-професійної культури, здатних з високою ефективністю виконувати поставлені завдання щодо оборони Вітчизни, розвитку власної творчої індивідуальності, наполегливого самостійного засвоєння нових знань протягом військової служби, прийняття оптимальних рішень в нестандартних умовах [1].

Розвиток системи військової освіти на теперішньому етапі стримується низкою таких основних причин:

падінням престижності та мотивації проходження військової служби, а також низьким рівнем соціального захисту військовослужбовців;

недостатнім рівнем управління військовою освітою, аналітичного та інформаційного супроводу реалізації проектів і прийнятих рішень;

незавершеністю оптимізації мережі ВВНЗ та ВНП ВНЗ, їх організаційно-штатних структур і чисельності особового складу;

неповною відповідністю змісту навчання військових фахівців досвіду бойової та оперативної підготовки військ (сил), їх застосуванню у миротворчих операціях, локальних конфліктах і війнах;

недостатнім досвідом військової служби на відповідних посадах у військах (силах) значної частини науково-педагогічних працівників ВВНЗ та ВНП ВНЗ;

недостатньою технологізацією та інформатизацією військової освіти;

недостатньою ефективністю інтеграційних процесів щодо військової освіти і науки;

застарілою навчально-матеріальною базою, відсутністю достатньої кількості сучасних навчально-тренувальних систем та комплексів;

недостатнім фінансовим забезпеченням системи військової освіти;

нормативно-правовою неврегульованістю механізму підготовки військових фахівців для військових формувань у навчальних закладах, які підпорядковані центральним органам виконавчої влади, що здійснюють керівництво іншими військовими формуваннями.

Системна робота щодо усунення зазначених причин має сприяти подальшому покращенню ефективності функціонування системи військової освіти.

Метою сучасних підходів щодо подальшого розвитку системи військової освіти, є приведення її кількісних та якісних показників у відповідність до структури, завдань і чисельності Збройних Сил. При цьому мають вирішуватися такі головні завдання:

створення організаційно-правових та економічних умов для повного задоволення потреб Збройних Сил у військових фахівцях з урахуванням раціонального використання ресурсів, що виділяються на їх підготовку;

визначення напрямів та шляхів підвищення професійного рівня підготовленості військових фахівців до виконання завдань за посадовим призначенням;

підвищення ефективності управління військовою освітою.

З урахуванням особливостей організації навчально-виховного процесу у ВВНЗ, ВНП ВНЗ, а також реальних економічних умов діяльності системи військової освіти, *основними шляхами і способами розв'язання зазначених вище проблем є:*

удосконалення відповідної нормативно-правової бази та економічних засад для задоволення потреб Збройних Сил та інших військових формувань у висококваліфікованих військових фахівцях;

запровадження ефективних механізмів підвищення престижу та соціального статусу учасників навчально-виховного процесу у ВВНЗ, ВНП ВНЗ та стимулювання їх професійного зростання;

створення механізмів раціонального використання коштів Державного бюджету України, що виділяються на підготовку військових фахівців;

підвищення ефективності системи управління підготовкою, перепідготовкою та підвищенням кваліфікації військових фахівців;

проведення подальшої оптимізації мережі військових навчальних закладів, їх організаційно-штатних структур і чисельності особового складу;

приведення обсягів замовлення на підготовку військових фахівців за всіма освітньо-кваліфікаційними рівнями у відповідність до реальних потреб Збройних Сил та інших військових формувань;

приведення діючого переліку напрямів, спеціальностей (спеціалізацій), за якими здійснюється підготовка військових фахівців, у відповідність до сучасних потреб Збройних Сил та інших військових формувань;

завершення розробки складових галузевих стандартів військової освіти у відповідних галузях знань;

приведення форм, методів, організації та змісту підготовки військових фахівців у відповідність до сучасних потреб Збройних Сил з урахуванням досвіду підготовки військ (сил), нових вимог щодо їх застосування, проведення миротворчих операцій та сумісних навчань з військовими частинами і підрозділами збройних сил іноземних країн;

посилення військово-практичної спрямованості навчання, забезпечення якісної підготовки випускників до служби в органах військового управління, військах (силах) з урахуванням переходу до комплектування Збройних Сил військовослужбовцями військової служби за контрактом та оснащення військ (сил) сучасними зразками озброєння і військової техніки;

забезпечення подальшої технологізації та інформатизації військової освіти;

вдосконалення системи професійно-психологічного відбору осіб, які вступають на навчання до військових навчальних закладів для підготовки на посади осіб офіцерського (сержантського, старшинського) складу у Збройних Силах та інших військових формуваннях;

подальший розвиток системи підготовки військових фахівців, що забезпечуватимуть безперервну освіту протягом їх військової служби;

запровадження механізму призначення на посади науково-педагогічних (педагогічних) працівників у ВВНЗ, ВНП ВНЗ кращих офіцерів з військ (сил) та ротаційних схем їх переміщення з урахуванням чередування служби на посадах у військах (силах) та у військових навчальних закладах;

вдосконалення системи підготовки та підвищення кваліфікації науково-педагогічних (педагогічних) працівників ВВНЗ, ВНП ВНЗ;

підвищення ефективності інтеграційних процесів щодо військової освіти і науки;

модернізація, розвиток навчально-матеріальної бази та забезпечення військових навчальних закладів сучасними зразками військової техніки та озброєння, засобами навчання, комп'ютерами, навчально-тренувальними системами і комплексами;

вдосконалення механізму підготовки військових фахівців у навчальних закладах, які підпорядковані іншим центральним органам виконавчої влади;

подальше поглиблення міжнародного співробітництва у галузі військової освіти.

Важливою передумовою успішного розв'язанні проблем військової освіти є підвищення рівня управління військовою освітою, покращення виховання в системі військової освіти, підвищення якості підготовки військових фахівців, рівня наукової і науково-технічної діяльності у ВВНЗ та ВНП ВНЗ, широке запровадження в навчальний процес інформаційних технологій, становлення та удосконалення матеріально-технічної бази

ВВНЗ і ВНП ВНЗ. Військова освіта має враховувати сучасні тенденції демократизації суспільства, зростання автономії військових навчальних закладів. Першочерговими завданнями є налагодження високопрофесійного наукового, аналітичного, інформаційного супроводу управлінських рішень, забезпечення якості та ефективності підготовки військових фахівців.

Підвищення рівня управління військовою освітою передбачає:

оптимізацію управлінських структур усіх рівнів на основі функціонального призначення;

перерозподіл функцій, повноважень між управлінськими структурами усіх рівнів і військовими навчальними закладами;

перехід до програмно-цільової моделі управління;

прозорість розроблення, експертизи, апробації, затвердження нормативно-правових документів і матеріалів;

створення системи моніторингу ефективності прийнятих управлінських рішень, їх впливу на якість підготовки військових фахівців;

впровадження новітніх інформативно-управлінських і комп'ютерних технологій;

демократизація процедур призначення та атестації керівників усіх рівнів;

зростання вимогливості щодо компетентності та кваліфікації управлінських кадрів.

Виховна робота в системі військової освіти – система організаційних, морально-психологічних, інформаційних, педагогічних, правових, культурно-просвітницьких та військово-соціальних заходів, спрямованих на формування, розвиток й саморозвиток у військових фахівців професійно необхідних психологічних якостей, моральної самосвідомості, що має забезпечити високу бойову та мобілізаційну готовність органів управління, з'єднань і частин, зміцнення військової дисципліни і правопорядку, згуртування військових колективів. Виховання в системі військової освіти є складовою національного виховання, органічною складовою освіти. та одним із головних її пріоритетів. Головна мета виховання – формування та розвиток особистості військового фахівця як найвищої соціальної цінності, забезпечення його прав і свобод, духовного та фізичного здоров'я, впровадження у військових колективах взаємовідносин, що базуються на військових статутах, законах, інших нормативно-правових актах, формування світогляду, громадянської позиції військових фахівців, найповніше розкриття їх здібностей в інтересах гармонійного розвитку громадян-патріотів, високопрофесійних військових спеціалістів, свідомих захисників Батьківщини.

Цілі виховання військових фахівців конкретизуються через систему виховних завдань, які об'єднуються в пріоритетні виховні напрями: національне (громадянське), розумове, військово-професійне, правове, культурологічне, моральне, фізичне, екологічне та ін. Ці напрями створюють стрункy систему, знаходяться у взаємозв'язку, доповнюють один одного, мають самостійне методологічне значення. У сукупності вони доповнюють систему національного виховання в нашому суспільстві.

Основні зусилля виховної роботи мають спрямовуватись на:

розкриття суті та характеру військово-професійної праці, формування у військових фахівців високих військово-професійних і морально-бойових якостей, розуміння їх значущості та відповідальності за захист своєї Вітчизни;

виховання особистості, яка усвідомлює свою належність до Українського народу, сучасної світової цивілізації, орієнтується в реаліях і перспективах соціокультурної динаміки, підготовлена до життя та праці в світі, що змінюється;

виховання поважного ставлення до національних святинь, державної мови, а також до історії та культури всіх корінних народів і національних меншин, які проживають в Україні, формування культури міжетнічних і міжособистісних відносин;

виховання людини демократичного світогляду, яка дотримується громадянських прав і свобод, з повагою ставиться до традицій культури, віросповідання та мови спілкування народів світу;

розвиток у військових фахівців творчих здібностей і навичок самостійного наукового пізнання, самоосвіти і самореалізації особистості;

забезпечення єдності навчання, виховання, розвитку та психологічної підготовки військових фахівців;

координація зусиль і вироблення поглядів щодо проблем виховання, визначення ролі органів виховної роботи усіх рівнів;

створення та вдосконалення педагогічних засобів, форм і методів виховання військових фахівців, узгодження дій державних і військових органів управління щодо цілеспрямованої підготовки молоді до військової служби.

Виховання в системі військової освіти має здійснюватися на всіх етапах навчання, носити систематичний, комплексний характер і забезпечувати всебічний розвиток, гармонійність і цілісність особистості, розвиток її здібностей, обдарувань, збагачення на цій основі інтелектуального потенціалу Збройних Сил України. Значне місце у процесі виховання військового фахівця повинно займати самовиховання як ефективний шлях самовдосконалення особистості.

Якість підготовки фахівців є важливою інтегральною характеристикою освітнього процесу ВВНЗ, ВНП ВНЗ, системною категорією, визначається ступенем обґрунтованості та дієздатності таких складових: мети навчання (для чого навчати), управлінських процедур (як управляти навчанням), змісту навчання (чого навчати), методів, засобів навчання та принципів організації процесу навчання (як навчати), а також має відповідати вимогам міжнародних стандартів. Якість військової освіти – показник її розвитку.

Основні шляхи підвищення якості військової освіти:

оптимізація переліку напрямів, спеціальностей і спеціалізації спеціальностей, за якими здійснюється підготовка військових фахівців;

розробка та впровадження нових державних, галузевих стандартів вищої освіти і стандартів вищої освіти ВВНЗ, ВНП ВНЗ на основі компетентнісного підходу;

приведення змісту соціально-гуманітарної, природничо-наукової, професійно-орієнтовної і військово-професійної підготовки військових фахівців у відповідність до завдань і функцій Збройних Сил України;

оптимізація мережі ВВНЗ, ВНП ВНЗ, забезпечення ступеневої і неперервної системи підготовки військових фахівців;

створення системи інтелектуального, професійно-психологічного та медико-фізіологічного конкурсного відбору талановитої молоді для вступу на навчання до військових навчальних закладів;

впровадження моделей неперервної військової освіти, які забезпечують кожному військовослужбовцю можливість формування індивідуальної освітньої траєкторії для подальшого професійного, кар’єрного та особистого росту.

активне використання науково обґрунтованих методів та засобів навчання і виховання, які забезпечують поєднання фундаментальної теоретичної підготовки військових фахівців з системою їх практичної підготовки, що орієнтована на воєнно-професійну діяльність військового фахівця за спеціальністю та спеціалізацією згідно з вимогами освітньо-кваліфікаційної характеристики випускника військового навчального закладу та освітньо-професійної програми;

впровадження інноваційних технологій, інформатизація навчального процесу, підвищення ролі самоконтролю знань, умінь, навичок тих, хто навчається, активне використання кредитно-модульної системи організації навчального процесу;

поєднання навчання та наукової роботи, підвищення ролі науки у ВВНЗ, ВНП ВНЗ як одного з основних факторів забезпечення високої якості підготовки військових фахівців, неперервного оновлення змісту військової освіти, підтримка провідних наукових шкіл;

створення єдиної системи оцінювання якості військової освіти, яка спрямована на створення механізмів об'єктивної оцінки якості військової освіти на всіх її рівнях;

введення прозорої системи обліку навчальної роботи того, хто навчається, і науково-педагогічних працівників;

оптимізація навчального навантаження науково-педагогічних працівників і курсантів;

розроблення та впровадження в практику науково обґрунтованих методик рейтингування результатів освітньої діяльності курсантів, навчальної, методичної, наукової та інших видів діяльності науково-педагогічних працівників, кафедр, факультетів ВВНЗ і ВНП ВНЗ;

повне забезпечення військових навчальних закладів сучасними засобами навчання й виховання, новими і модернізованими зразками озброєння та військової техніки, імітаційно-тренажерними засобами тощо;

Поєднання військової освіти і науки є умовою ефективного функціонування системи військової освіти, головним чинником її подальшого розвитку, що забезпечується:

розвитком військової освіти на основі досягнень науки і техніки, військової справи, коригуванням змісту, науково-методичного та дидактичного забезпечення підготовки військових фахівців;

інноваційною освітньою діяльністю на всіх рівнях управління;

створенням науково-інформаційного простору з використанням комунікаційно-інформаційних засобів;

спрямуванням фундаментальних, прикладних досліджень і розробок на створення та впровадження нових конкурентоздатних зразків техніки й озброєння, технологій і матеріалів;

розвитком різних форм наукової співпраці (у тому числі міжнародної) з установами і організаціями, що не входять до системи вищої військової освіти, для розв'язання складних наукових проблем, впровадження результатів наукових досліджень і розробок у військову практику;

залученням до навчально-виховного процесу провідних учених і науковців науково-дослідних установ і організацій;

організацією наукових, науково-практичних, науково-методичних семінарів, конференцій, проведення олімпіад, конкурсів на краще виконання науково-дослідних, курсових, дипломних (кваліфікаційних) та інших робіт учасників навчально-виховного процесу;

проведенням комплексних досліджень з проблем педагогіки і психології вищої військової школи, удосконалення технологій навчання, підвищення якості підготовки військових фахівців;

розширенням прав ВВНЗ, ВНП ВНЗ щодо самостійного використання позабюджетних коштів, направлення їх на розвиток науково-експериментальної і навчально-матеріальної бази, матеріальне стимулювання наукової діяльності наукових і науково-педагогічних кадрів.

Важливою складовою розвитку військової освіти є впровадження сучасних інформаційно-комунікаційних технологій, що забезпечують подальше вдосконалення навчально-виховного процесу, доступність і ефективність військової освіти, підготовку військових фахівців до діяльності в інформаційному суспільстві, умовах ведення бойових дій, участі у миротворчих операціях, що відповідають сучасним тенденціям розвитку військового мистецтва.

Це досягається шляхом: забезпечення поступової комп'ютеризації, інформатизації військової освіти, спрямованої на задоволення освітніх інформаційних і комунікаційних потреб учасників навчально-виховного процесу; запровадження дистанційного навчання із застосуванням у навчальному процесі та бібліотечній справі інформаційно-комунікаційних

технологій поряд з традиційними засобами; розроблення широкого спектру електронних підручників, дидактичних матеріалів, предметно-орієнтованих середовищ навчального та розвиваючого призначення, індивідуальних модульних навчальних програм різних рівнів складності, залежно від конкретних потреб.

Фінансове забезпечення військової освіти здійснюється в межах асигнувань, передбачених для Міністерства оборони України у бюджеті та за рахунок позабюджетних джерел. Основними джерелами фінансового забезпечення військової освіти є: кошти державного бюджету; кошти, отримані за рахунок: надання додаткових освітніх та інших послуг; кошти від здійснення економічної діяльності, регламентованої державою; кошти від оплати виконаних науковцями ВВНЗ, ВНП ВНЗ досліджень з договірних науково-дослідних і дослідно-конструкторських робіт; кошти від оплати підготовки студентів за контрактом і підготовки офіцерів запасу; кошти від оплати підготовки іноземних військових фахівців; гранти.

Основним напрямами становлення та удосконалення матеріально-технічної бази військових навчальних закладів є: забезпечення пріоритетної поставки до ВВНЗ, ВНП ВНЗ, навчальних центрів нових зразків озброєння та військової техніки, навчально-тренувальних комплексів, сучасної комп'ютерної техніки і засобів зв'язку; створення індустрії сучасних засобів навчання, що відповідають світовому науково-технічному рівню та є важливою передумовою реалізації ефективних стратегій досягнення цілей освіти, повне забезпечення ними ВВНЗ, ВНП ВНЗ; розробка типового навчально-лабораторного обладнання з відповідних навчальних дисциплін для ВВНЗ і ВНП ВНЗ; запровадження навчального, демонстраційного устаткування, сполученого з комп'ютерними системами для самостійного вивчення військовими фахівцями навчального матеріалу; створення у ВВНЗ, ВНП ВНЗ за відповідними напрямами наукових досліджень сучасної науково-експериментальної бази; забезпечення ВВНЗ, ВНП ВНЗ, курсів з перепідготовки і підвищення кваліфікації науково-педагогічних працівників ліцензованими програмними продуктами, створення електронних каталогів, забезпечення доступу до інформаційної бази наукових бібліотек провідних зарубіжних вищих навчальних закладів, електронного фонду навчальної літератури в мережі Інтернет; забезпечення редакційно-видавничих підрозділів ВВНЗ, ВНП ВНЗ сучасною поліграфічною технікою та необхідними витратними матеріалами.

Розглянуті проблеми і напрями сучасного етапу розвитку військової освіти передбачають вирішення низки системних, складних нормативно-правових, управлінських, структурно-організаційних, психолого-педагогічних, теоретико-методологічних, фінансово-економічних, матеріально-технічних та інших задач, в основу яких покладено принципи цілеспрямованості, системності, динамічності, адаптивності, еволюційності та поліфункціональності. Практична реалізація зазначених проблем і задач забезпечить подальший розвиток військової освіти у напрямі створення економічно доцільної, ефективної системи підготовки висококваліфікованих військових фахівців усіх рівнів за повним переліком спеціальностей та кваліфікацій, необхідних для Збройних Сил та інших військових формувань. При цьому зростуть самостійність і самодостатність військових фахівців, їх творча активність, що сприятиме виконанню поставлених перед ними завдань будь-якої складності та в будь-яких умовах; активізуються процеси національної самоідентифікації військових фахівців, їх авторитет у суспільстві, а також статус офіцера України у міжнародному цивільному та військовому середовищі.

ЛІТЕРАТУРА

1. *Воєнна доктрина* України: Затв. Указом Президента України від 15 червня 2004 р. // Офіційний вісник України. – 2004. – № 30. – Ст. 205.

2. *Державна програма* розвитку Збройних Сил України на 2006-2011 роки (Основні положення). – К.: МО України, 2005. – 40 с.

3. *Національна доктрина* розвитку освіти. Затверджена Указом Президента України від 17 квітня 2002 р., № 347/2002 // Професійно-технічна освіта. – 2002. – № 3. – С. 2 – 8.

к.т.н. Стрюк О.Ю. (ВІТІ НТУУ „КПІ”)

МЕТОД МАКСИМІЗАЦІЇ КОРИСНОСТІ MESH-РАДІОМЕРЕЖІ НА ОСНОВІ ПОКАЗНИКІВ СПРИЙНЯТТЯ ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ

Mesh-мережі – це новий перспективний принцип побудови широкосмугових радіомереж, відмінною особливістю якого є самоорганізація архітектури мережі, що забезпечує реалізацію наступних можливостей [1]:

– використання безпроводових транспортних каналів при побудові мережі за топологією „кожен з кожним”;

– масштабування мережі (зміна площі зони покриття і щільності інформаційного забезпечення) у режимі самоорганізації;

– стійкість мережі до втрати (відмови) окремих елементів;

– зменшення вартості розгортання мережі.

Незважаючи на великий потенціал mesh-мереж та наявні приклади практичного втілення mesh-технологій у стандартах побудови безпроводових мереж (для мереж масштабу Wireless Metropolitan Area Networks (WMAN) – 802.16j, Wireless Local Area Network (WLAN) – 802.11s, Wireless Personal Area Networks (WPAN) – 802.15.4), залишається ряд проблем, що перешкоджають їх широкому розповсюдженню. Одним з найбільш критичних факторів, які впливають на розвиток mesh-мереж, є складність забезпечення для кожного з користувачів mesh-мережі заданого рівня якості обслуговування (QoS, Quality of Service) – визначеної у рекомендації ITU – T P.800 як „сукупний ефект характеристик мережного сервісу, який визначає ступінь задоволеності споживача даного сервісу”. Забезпечення QoS у mesh-мережах потребує розробки і впровадження спеціалізованих механізмів і протоколів оперативного керування радіомережами [2 – 4].

Обґрунтування вибору сприйняття якості обслуговування як інтегрального показника якості обслуговування. Протягом останніх десяти років була розроблена концептуальна модель координаційної – крос-рівневої (cross-layer) архітектури систем оперативного керування радіомережами [5, 6]. Крос-рівнева архітектура побудови системи оперативного керування радіомережі передбачає координацію та інтеграцію рівнів еталонної взаємодії відкритих систем (OSI) за цілями і функціями керування та інтелектуалізацію процесів прийняття рішення. Основні труднощі при побудові координаційної архітектури керування радіомережею – це визначення необхідних параметрів, які будуть використовуватись між рівнями OSI та функціями керування, які дозволяють отримати користувальницьку та (або) мережеву, зонову оптимізацію [6].

Однією із прикладних задач мережного керування, пов’язаних із забезпеченням QoS, при вирішенні якої використовується крос-рівневий підхід, є задача максимізації корисності мережі (network utility maximization). Вперше задача максимізації корисності мережі сформульована у роботі F.Kelly [7]. Методи вирішення задачі максимізації корисності mesh-мереж запропоновані у роботах [8 – 10]. Задача максимізації корисності mesh-мережі, яка складається з E – ресурсних елементів, і в якій створено F – інформаційних потоків, полягає у пошуку такого вектору розподілу ресурсів mesh-мережі, який задовольняє (1)

$$\mathbf{x}^* = \arg \max_{\{x_f\} \in \Omega} \left(\sum_{f \in F} U_f\left(x_f\right) \right) \tag{1}$$

за умови

$$\mathbf{R} \times \mathbf{x} \le \mathbf{C}, \quad \mathbf{x} \ge 0,$$

де x_f – ресурси мережі, виділені інформаційному потоку f;

$U_f(\{x_f\})$ – значення функції корисності для інформаційного потоку f при виділенні йому x_f ресурсів мережі;

Ω – множина можливих варіантів розподілу ресурсів між інформаційними потоками у мережі;

$\mathbf{R} = \left(R_{ef}\right)_{|E|\times|F|}$ – матриця розподілу ресурсів елементів мережі між інформаційними потоками у мережі;

$\mathbf{x} = \left(x_f,\ f \in F\right)$ – вектор ресурсів, які виділяються інформаційним потокам.

$\mathbf{C} = (C_e, e \in E)$ – вектор місткостей ресурсних елементів мережі.

У якості інтегрального показника при оцінюванні оптимальності координаційного керування у радіомережі, безпосередньо пов'язаного з її основним призначенням – забезпеченням передавання інформації із заданою якістю, що враховує як вплив параметрів мережі, так і вплив прикладного програмного забезпечення, – може бути використане сприйняття користувачем якості інформаційної послуги [11].

Сприйняття якості обслуговування (PQoS – perceived quality of service) – це оцінка якості інформаційного сервісу з точки зору сприйняття користувачем як споживачем послуг даного сервісу. Рекомендація ITU-T P.830 встановлює для оцінювання якості сприйняття користувача п'ятибальну шкалу MOS (Mean Opinion Score – середнє значення експертних оцінок). Протягом останніх років були розроблені та пройшли міжнародну верифікацію методи об'єктивного оцінювання PQoS для більшості класів інформаційних служб. Наявність об'єктивних методів оцінювання PQoS дозволяє автоматизувати процедуру визначення PQoS як величини, залежної від широкого спектру показників мережі. Для кожної з функціонуючих у мережі інформаційних служб можуть бути визначені значення багатовимірного масиву значень PQoS – $\{q_i\}$, залежні від виділених ресурсів, параметрів мережі, з урахуванням функціональності прикладного програмного забезпечення (кінцевого абонентського обладнання), яке реалізовує дану послугу

$$\{q_i\} = F\left(\{R_i\},\{p\},\{E_i\}\right), \tag{2}$$

де q_i – значення PQoS за шкалою MOS для інформаційної служби i, $i \in 1,..,m$;

m – кількість інформаційних служб, які функціонують у мережі;

$\{R_i\}$ – множина значень ресурсів мережі, що виділені інформаційній службі i;

$\{p\}$ – множина показників, які характеризують мережу;

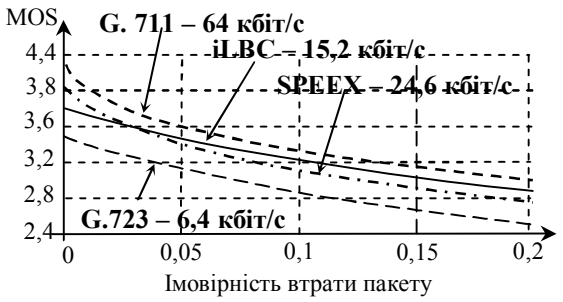
$\{E_i\}$ – множина факторів, що відображають вплив на PQoS особливостей реалізації прикладного програмного забезпечення, і (або) кінцевого абонентського обладнання.

На рис. 1 наведені залежності PQoS від:

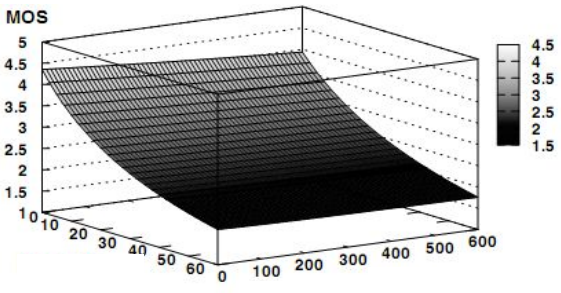
– ресурсів мережі - смуги пропускання;

– показників мережі – імовірність втрати пакету, затримка доставки пакетів;

– особливостей реалізації прикладного програмного забезпечення – тип і швидкість



а)



б)

Рис. 1. Залежність PQoS від:

а) імовірності втрати пакету для різних кодеків мови [12];

б) імовірності втрати пакету і затримки доставки пакетів для кодеку мови SPEEX (24,6 кбіт/с) [13]

інформаційного потоку, метод кодування.

У роботах [12, 14] доведена ефективність використання PQoS у якості показника при вирішенні задачі максимізації корисності мережі у зоні обслуговування базової станції радіомережі. Метою представленої роботи є розробка методу максимізації корисності mesh-радіомережі із використанням PQoS в якості цільової функції оптимізації.

Постановка задачі координаційної оптимізації для забезпечення максимізації корисності mesh-радіомережі на основі показників PQoS. При побудові mesh-радіомереж масштабу WMAN використовується структура mesh-мережі на основі ретрансляції. Дана структура стандартизована для побудови mesh-мереж у технології WiMAX – стандарт IEEE 802.16j [15], для технології LTE – розглядається як перспективний варіант [16]. Мережа складається з наступних мережних пристроїв: базова станція (БС), релейна станція (ретранслятор, РС), абонентська станція (АС). РС може функціонувати у прозорому або у непрозорому режимах. У прозорому режимі РС транслює лише дані і не транслює преамбули і поля керування. АС керується безпосередньо БС. При цьому АС логічно ніяк не взаємодіє з РС (не знає про її існування). У непрозорому режимі РС передає не лише дані, а й преамбулу, а також і всі керуючі повідомлення. По відношенню до АС релейна станція виглядає як БС, абонентська станція фізично і логічно з'єднана з РС. Релейні станції можуть бути стаціонарними, номадичними (пересувний ретранслятор) і мобільними.

Зв'язок між базовими станціями забезпечується із використанням надійних і високопродуктивних мережних технологій, здатних гарантувати необхідний рівень QoS. Основними причинами зменшення рівня QoS у mesh-радіомережах на основі РС є обмеженість радіоресурсу, нестабільність радіоліній і мобільність абонентів у зоні обслуговування БС і РС станцій. Найбільш вагомим ресурсом mesh-радіомережі є пропускна спроможність радіоінтерфейсів базових та релейних станцій [17], тому оптимізаційна задача, рішення якої пропонується, зосереджена на максимізації повного рівня PQoS у mesh-радіомережі за рахунок керування розподілом пропускної спроможності, кодування аудіовізуальних даних зі зміною швидкістю і з урахуванням рівня завадостійкості каналів між мережними пристроями. Вирішення запропонованої задачі забезпечує підвищення ефективності використання радіоресурсу mesh-мережі.

Початкові припущення. Оптимізаційна задача вирішується, виходячи із припущення про реалізацію в технології побудови радіомережі наступних методів забезпечення інформаційного обміну і керування мережею:

– релейні станції функціонують у непрозорому режимі, для зв'язку між елементами мережі використовується однаковий радіоінтерфейс, режим керування mesh-мережею централізований;

– наявність механізмів класифікації, маршрутизації та відокремленої обробки інформаційних потоків, керування чергами, планування передавання;

– детермінований доступ до радіоканалу з можливістю виділення кожному інформаційному потоку певного значення пропускної спроможності з дискретністю ΔR;

– наявність зворотного службового зв'язку між базовою станцією і мобільними абонентами з можливістю отримання інформації про рівень завадостійкості радіоканалу на приймальній стороні;

– можливість транскодування аудіовізуальних даних – зміни в реальному часі швидкості кодування та (або) формату представлення даних базовою станцією і абонентськими пристроями.

Аналіз наведених припущень показує, що всі зазначені механізми, крім транскодування, реалізовані в сучасних технологіях побудови mesh-радіомереж [15, 16]. Сучасні методи кодування аудіовізуальних даних передбачають можливість кодування зі змінною швидкістю без істотної зміни формату представлення даних, що створює умови для здійснення операції транскодування в реальному часі як у базових станціях, так і в абонентському обладнанні [18].

Вихідні дані. При вирішенні оптимізаційної задачі використовуються наступні вихідні дані: m- кількість РС у mesh-мережі; R – значення пропускної спроможності радіоінтерфейсів БС, РС, АС, біт\с; Δr – шаг зміни смуги пропускання, яка може виділятись БС або РС для інформаційних потоків – ресурсний елемент, біт\с; k – кількість інформаційних потоків, які конкурують за доступ; способи кодування інформації в інформаційних потоках; маршрути проходження інформаційних потоків у mesh-мережі; p_i – середня імовірність втрати пакету для кожного інформаційного потоку, $i \in 1,..,k$; масив значень PQoS по шкалі MOS в залежності від швидкості потоку імовірності втрати пакету для кожного з інформаційних потоків та обраного способу кодування (характеристик прикладної реалізації послуги)

$$\{q_i(r_i, p_i, E_i)\} = \{q_i(\Delta r, p_i, E_i),\ q_i(2\Delta r, p_i, E_i),\ \ldots,\ q_i(B_i\Delta r, P_i, E_i)\},$$

де $B_i = \lfloor R_i^{max}/\Delta r \rfloor$;

R_i^{max} – максимально необхідна смуга пропускання для інформаційного потоку i, біт\с.

Необхідно – знайти такий вектор розподілу пропускної спроможності між інформаційними потоками у mesh-мережі, при якому виконується

$$\mathbf{r}^* = \arg \max_{\{r_i\} \in \Omega} \left(\sum_{i=1}^{k} q_i\left(r_i, p_{i,}, E_i\right) \right) \tag{2}$$

за умови

$$\mathbf{\Delta R} \times \mathbf{r} \le \mathbf{C},$$

де $\mathbf{r}^* = \left(r_i, i = 1,...,k\right)$ – вектор розподілу пропускної спроможності між інформаційними потоками, який забезпечує вирішення задачі (2);

Ω – множина можливих значень вектору розподілу пропускної спроможності між k – інформаційними потоками, при дискретності зміни пропускної спроможності Δr;

$\mathbf{\Delta R} = \left(\Delta R_{ji}\right)_{|m+1| \times |k|}$ - матриця розподілу пропускної спроможності радіоінтерфейсів БС і РС mesh-мережі між інформаційними потоками;

$\mathbf{C} = (R_j, j = 1,...,m+1)$ – вектор пропускної спроможності радіоінтерфейсів БС і РС mesh-мережі.

Для вирішення оптимізаційної задачі (2) пропонується використовувати локально оптимальний („жадний” (greedy)) алгоритм. Вибір даного методу рішення обумовлений:

–множина пропускних спроможностей відповідає стандартному набору швидкостей передавання, і в силу цього є дискретною, компоненти рішення повинні відповідати цій дискретній множині;

– меншою обчислювальною складністю „жадних” алгоритмів у порівнянні із динамічним програмуванням, або пошуком аналітичного рішення.

Можливість використання „жадного” алгоритму для вирішення оптимізаційної задачі (2) обумовлена:

– адитивним характером цільової функції оптимізації;

– залежністю рішення про виділення частки пропускної спроможності, яке приймається в кожному із циклів, лише від величини нерозподіленої (вільної) пропускної спроможності;

– гарантуванням досягнення при використанні „жадних” алгоритмів Парето – оптимальності при характеристиках цільової функції і початкових обмеженнях, що відповідають сформульованій задачі оптимізації.

Для вирішення задачі (2) пропонується алгоритм, найближчим прототипом якого є алгоритм, запропонований у роботі [14]. Оригінальний алгоритм використовувався для вирішення задачі максимізації PQoS у сегменті «базова станція – мобільний абонент».

Алгоритм координаційної оптимізації для забезпечення максимізації корисності mesh-радіомережі на основі показників PQoS ініціалізується БС у випадку необхідності перерозподілу ресурсів mesh-мережі при початку (закінченні) сеансу зв’язку, або з заданою

періодичністю, яка, згідно умови стохастичної стійкості алгоритмів керування розподілом ресурсів мережі [19], має відповідати співвідношенню:

$$T_r \approx T_c < T_s, \tag{3}$$

де T_r – середній час, необхідний для здійснення розподілу ресурсів;

T_c – інтервал кореляції зміни параметрів мережі;

T_s – середня тривалість сеансів зв'язку.

Алгоритм вирішення сформульованої задачі складається з двох основних етапів. На першому етапі для кожного інформаційного потоку визначається масив значень PQoS по шкалі MOS в залежності від швидкості інформаційного потоку, витрати ресурсів елементів мережі, через які проходить маршрут передавання даного потоку та імовірності втрати пакету на цьому маршруті. Оскільки під витратним ресурсом розуміється смуга пропускання радіоінтерфейсів БС та РС, то витрати ресурсів обчислюються за наступним виразами:

– для маршрутів, які проходять лише через РС

$$C = 2ny\Delta r; \tag{4}$$

– для маршрутів, які проходять через РС та БС

$$C = 2ny\Delta r + y\Delta r, \tag{5}$$

де n – кількість РС, через які проходить маршрут інформаційного потоку у mesh-мережі;

y – кількість ресурсних елементів, які виділяються інформаційному потоку, $y = \lfloor r_i / \Delta r \rfloor$.

Середня імовірність втрати пакету – p_i для маршруту передавання інформаційного потоку визначається наступним чином. Для маршрутів, які створюються, p_i визначається аналітичними методами, на основі інформації про імовірність виникнення помилки у радіоканалах, з яких складається маршрут. Для маршрутів, які вже існують, p_i може визначатись як аналітично, так і на основі статистичної інформації мережних протоколів (наприклад, RTP, SIP).

В кожному циклі другого етапу виконання алгоритму визначається інформаційний потік з максимальним значенням співвідношення „прирощення PQoS/ збільшення витрати ресурсів", детальне описання цієї складової наведено у [14]. В радіоінтерфейсах РС, через які проходить визначений потік, для нього виділяється частка пропускної спроможності $2y\Delta r$, у радіоінтерфейсі БС – $y\Delta r$.

Виконання алгоритму закінчується у випадку надання кожному з інформаційних потоків максимально необхідної смуги пропускання R_i^{max} (якщо mesh-мережа функціонує у недовантаженому режимі), або у випадку вичерпання ресурсів радіо інтерфейсів, через які проходять інформаційні потоки, для яких $r_i < R_i^{\max}$.

Результатами виконання алгоритму є вектор розподілу пропускної спроможності між інформаційними потоками, який забезпечує вирішення задачі (2), та матриця розподілу пропускної спроможності радіоінтерфейсів БС і РС mesh-мережі між інформаційними потоками.

Для експериментальної перевірки ефективності використання запропонованого методу із використанням системи комп'ютерної математики Matlab створена математична модель алгоритму максимізації корисності mesh-радіомережі на основі показників PQoS.

Результати математичного моделювання показують, що максимізація корисності мережі на основі показників PQoS дозволяє досягти 20 – 30 % переваги у порівнянні із значеннями PQoS, яких дозволяє досягти управління розподілом ресурсів мережі на основі пріоритетності аудіовізуального трафіку, і 5 – 10 % переваги у порівнянні із значеннями PQoS, яких дозволяє досягти управління розподілом ресурсів мережі на основі значень функції корисності.

Висновки. У доповіді доведена можливість і перспективність використання значення сприйняття якості обслуговування (PQoS) в якості показника в задачах мережного керування. Запропонований метод координаційної зонової оптимізації максимізації корисності mesh-радіомережі на основі показників PQoS. Запропонований метод відрізняється від відомих використанням у якості цільової функції оптимізації – PQoS, залежної від пропускної спроможності, рівня завадостійкості та способу реалізації інформаційної послуги. Результати, яких дозволяє досягти запропонований метод, перевищують результати стандартних та відомих перспективних методів забезпечення максимізації корисності mesh-радіомереж. Під час подальших досліджень передбачається розширення переліку ресурсів радіомережі, керування якими забезпечує вирішення задачі забезпечення максимізації корисності mesh-радіомережі, а також реалізація запропонованого методу у радіомережах зі структурою Ad Hoc.

ЛІТЕРАТУРА

1. *Бунин С.Г.* Перспективы беспроводных ячеистых сетей / С.Г. Бунин, А.И. Миночкин, В.А. Романюк // Зв'язок. – 2007. – № 5. – С. 20 – 24.
2. *Миночкин А.И.* Управление качеством обслуживания в мобильных радиосетях / *А.И. Миночкин, В.А. Романюк* // Зв'язок. – 2005. – № 8. – С. 17 – 23.
3. *Wireless quality of service : techniques, standards, and applications* / edited by M. Maode, M. K. Denko., Y. Zhang. - Auerbach Publications, 2009. – 372 p.
4. *Ganz A., Ganz Z., Wongthavarawat K.* Multimedia Wireless Networks: Technologies, Standards, and QoS. – Prentice Hall PTR, 2003. – 352 p.
5. *Adaptation and cross layer design in wireless networks* / edited by M. Ibnkahla. – CRC Press. – 2009. – 526 p.
6. *Романюк В.А.* Архітектура системи оперативного управління тактичними радіомережами / Романюк В.А. // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2009. – №3. – С. 70 – 76.
7. *Kelly F.* Charging and rate control for elastic traffic / F. Kelly // European Transactions on Telecommunications. – 1997. - №8 – P. 33 – 37.
8. *Xue Y.* Optimal Resource Allocation for Wireless Mesh Networks / Y.Xue, Y.Cui, K. Nahrstedt // Wireless Mesh Networks. Architectures and Protocols. – Springer. – 2008. – P. 143 – 166.
9. *Wang B.* QoS-aware fair rate allocation in wireless mesh networks / B. Wang, M. Mutka // Computer Communications. – 2008. – V. 31 – I. – 7. – P. 1276 – 1289.
10. *Dionysiou T.* Utility-based channel assignment and topology control in wireless mesh networks / T. Dionysiou,V.A. Siris, G. Stamatakis // World of Wireless Mobile and Multimedia Networks : 2010 IEEE International Symposium. – Montreal, 2010. – P. 1 – 9.
11. *Батлер Ю.В.* О качестве услуг в IP – сетях / Ю.В. Батлер, В.Ф. Михайлов // Зв'язок. – 2006. – №6. – С. 2 – 6.
12. *Jurca D.* Joint Network and Rate Allocation for Simultaneous Wireless Applications / D. Jurca, W. Kellerer, E. Steinbach, S. Khan, S. Thakolsri, P. Frossard // 2007 IEEE International Conference on Multimedia & Expo (ICME 2007), 2007. – P. 931 – 934.
13. *Valera M.* Quality assessment of interactive voice applications / M. Valera, A. da Silva, E. Souza, R. Leao, G. Rubino // Computer Networks, 2008 – №6(52). – 1179 – 1192 p.
14. *Стрюк О.Ю.* Метод розподілу пропускної спроможності базової станції радіомережі для підвищення інтегральної якості обслуговування абонентів / О.Ю. Стрюк // Збірник наукових праць ВІТІ НТУУ «КПІ». – 2009. – №3. – С. 89 – 99.
15. *Вишневский В.М.* Энциклопедия WiMAX. Путь к 4G / В.М. Вишневский, С.Л. Портной, И.В. Шахнович. – М.: Техносфера, 2009. – 472 с.
16. *Schoenen R.* Multihop Extensions to Cellular Networks – the Beneft of Relaying for LTE / R. Schoenen // Long Term Evolution: 3GPP LTE Radio and Cellular Technology. – CRC Press, 2009. – P. 266 – 303.
17. *Resource management in wireless networking* / edited by M. Cardei, I. Cardei, D-Z. Du– Springer, 2005. – 716 p.
18. *Multimedia Transcoding in Mobile and Wireless Networks* / edited by M. Ashraf, A. Ibrahim - IGI Global, 2009. – 439 p.
19. *Chiang M.* Stochastic network utility maximization / M. Chiang // European Transactions on Telecommunications. – 2008. – 00:1 – 22.

к.т.н. Субач І.Ю. (ВІТІ НТУУ „КПІ”)

НАПРЯМКИ ВДОСКОНАЛЕННЯ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

У теперішній час, у Збройних Силах України згідно з Програмою розвитку озброєння та військової техніки Збройних Сил України на період до 2015 року, завданнями начальника зв’язку Збройних Сил України щодо подальшого розвитку систем зв’язку та автоматизації, з метою підвищення ефективності прийняття рішень органами управління Збройних Сил України, створюється інформаційно-аналітичне забезпечення (ІАЗ) Збройних Сил України, що представляє собою сукупність інформаційних продуктів, ресурсів та послуг, що надаються керівному складу органів управління Збройних Сил (ЗС) України та система підтримки і прийняття рішень (СППР) їх управлінської діяльності. Основним призначенням ІАЗ є підтримка процесів прийняття рішень керівного складу ЗС України, інформаційні потреби якого задовольняються інформаційно-аналітичними підрозділами.

Аналіз показує, що сучасні вимоги до ІАЗ ЗС України можуть бути задоволеними перш за все шляхом впровадження нових інтелектуальних інформаційних технологій, які спеціально розвиваються для вирішення задач інформаційно-аналітичної системи ЗС України.

В якості прикладу можна навести інформаційно-аналітичну систему (ІАС) підтримки оборонного планування „Ресурс”, яка прийнята на озброєння та введена в експлуатацію наказом Міністра Оборони України від 22.08.06 р. № 498 та призначена для забезпечення своєчасного подання керівному складу Генерального штабу ЗС України достовірної інформації, необхідної для прийняття ефективних рішень при оборонному плануванні в ЗС України, а також проведення аналізу цієї інформації.

Проте, у теперішній час повною мірою проявляється тенденція як кількісних, так і якісних змін інформаційних потоків, які циркулюють в органах військового управління (ОВУ).

Тому, у відповідності до характеру змін інформаційних потоків, повинні змінюватися і технології обробки інформації.

Порівняльний аналіз вітчизняних та зарубіжних інтелектуальних технологій показує, що при автоматизації діяльності ОВУ переважає підхід, який полягає у забезпеченні максимальної інтенсивності використання інтуїтивного та асоціативного мислення посадових осіб та аналітиків ОВУ в процесі обробки інформації.

Основними пріоритетами підходу є: пріоритетність автоматизованих режимів, концентрація зусиль на вторинній обробці інформації, оснащення центрів обробки інформації ОВУ максимальним набором інформаційних технологій для обробки й аналізу інформації, а його основним недоліком, є залежність якості інформаційних та аналітичних відомостей від кваліфікації, досвіду та інтуїції аналітика.

Усі задачі, які вирішуються в ОВУ можна поділити на три класи.

До першого класу відносяться повністю формалізовані задачі, для яких є добре відомими методи рішення або можна розробити структуровані процедури їх відпрацювання.

Для другого класу задач є характерним застосування слабоструктурованих процедур прийняття рішень з неповною інформацією.

До третього класу відносяться задачі, які потребують застосування неструктурованих процедур відпрацювання рішень, які використовують інтуїтивні та практичні знання людини. Умови прийняття рішень у цьому класі задач характеризуються неповнотою інформації, а також нечіткістю цілей, що формулюються.

Отже різноманіття цілей і задач, що виникають у ході прийняття рішень посадовими особами ОВУ, їх складність та часові обмеження, які є характерними для багатьох задач, по

яким приймаються рішення, вимагають комп'ютерної підтримки цих процесів на основі розробки та застосування СППР.

Значний вклад у теорію підтримки прийняття рішень та побудови СППР внесли О.І. Ларичев, Г.С. Поспєлов, Е.А. Трахтенгерц – у Росії, Турбан Е., Аронсон Д.Е. – у Сполучених Штатах Америки, Глушков В.М., Ивахненко А.Г., Морозов А.А., Герасимов Б.М. – в Україні та інші провідні вчені.

Проте, незважаючи на інтенсивний розвиток СППР, як і раніше, у цій галузі залишається багато невирішених питань, які є зв'язаними з рішенням нових практичних задач на основі адекватних їм все більш складних моделей і методів.

Нерідко, в наслідок того, що у СППР головним джерелом інформації є людина, її дуже складно або взагалі неможливо формалізувати.

Дослідження показують, що ефективність роботи сучасних інтелектуальних систем, у першу чергу, визначається потужністю та адекватністю баз знань, котрі використовуються для відпрацювання рішень та рекомендацій.

У свою чергу, потужність бази знань у значній мірі визначається джерелами знань, їх якістю, а також технологіями добування та формування знань у ній.

На протязі багатьох років в якості основного джерела знань розглядалися експерти предметної області. Однак, усі сподівання на можливість створення баз знань тільки на основі експертних знань, в основному, не виправдалися

Саме відсутність надійних джерел знань та ефективних технологій добування та формування знань з них є однією з головних причин відносно слабкого промислового впровадження інтелектуальних систем.

У зв'язку з цим, виникла гостра необхідність в розробці методології формування знань у СППР, здатних моделювати та аналізувати різні види знань, що поступають з різнорідних джерел для вирішення складних слабоструктурованих і неструктурованих задач, а також спроможних до навчання та адаптування в умовах інтенсивних динамічних змін зовнішнього середовища та внутрішніх умов функціонування системи.

Аналіз вимог, які пред'являються до СППР та задач, які вони повинні вирішувати, а також характер предметної області, дозволяє сформулювати основні принципи побудови СППР: розподілений характер структури системи, адаптивність представлення знань та пошуку рішень, масштабуємість методів та алгоритмів обробки інформації, використання сучасних інформаційних технологій, ієрархічність структури системи та її бази даних і бази знань, відкритість модульної структури та інші.

Проведений аналіз робіт з проблематики проектування та розробки СППР показує, що у теперішній час найбільш перспективними напрямками підвищення ефективності СППР є: удосконалення методології побудови СППР, інтеграція сучасних інформаційних технологій для створення СППР, створення СППР, орієнтованих на динамічні предметні області та реальний масштаб часу, розробка методів формування знань у СППР.

Для ефективної реалізації її функцій необхідна єдина інтегрована система накопичення, обробки, аналізу та видачі різнорідної інформації, яка дозволить поєднати у єдине ціле усі розрізнені відомості, що поступають із різнорідних джерел.

Основними елементами даної системи повинні бути: інформаційна підсистема керівного складу, документальна підсистема, інформаційно-розрахункова підсистема, підсистема оперативної аналітичної обробки даних, підсистема інтелектуального аналізу даних, підсистема інтелектуального аналізу текстів, база знань, підсистема формування рішень (рекомендацій), інтегровані сховища і вітрини даних, підсистема збору, очищення та узгодження даних, підсистема адмініструванні та моніторингу змін даних і знань та інші.

Разом з тим, аналіз показує, що у теперішній час не існує єдиної методології побудови СППР, здатних моделювати та аналізувати різні види знань, що поступають з різнорідних джерел для вирішення складних слабоструктурованих і неструктурованих задач**.**

Тому, основним напрямком удосконалення СППР є розробка методології побудови СППР на основі системної інтеграції інтелектуальних технологій з традиційними методами пошуку рішень, яка полягає у поетапному рішенні задач проектування СППР, оптимальної організації її функціонування, а також реалізації та еволюціонування системи.

Важливою задачею забезпечення ефективного функціонування СППР є вирішення питань наповнення, довизначення та перевизначення знань.

У результаті проведених досліджень, запропонована методологія, яка дозволяє створювати СППР для вирішення складних слабоструктурованих і неструктурованих задач прийняття рішень в умовах невизначеності, здатних навчатися та адаптуватися до динамічних змін зовнішнього середовища і внутрішніх умов функціонування.

Важливим елементом даної методології є методи і алгоритми формування знань у СППР.

Для усунення недоліків традиційних стратегій наповнення бази знань та практичних методів добування знань від експертів, запропоновано використання технологій інтелектуального аналізу даних (ІАД).

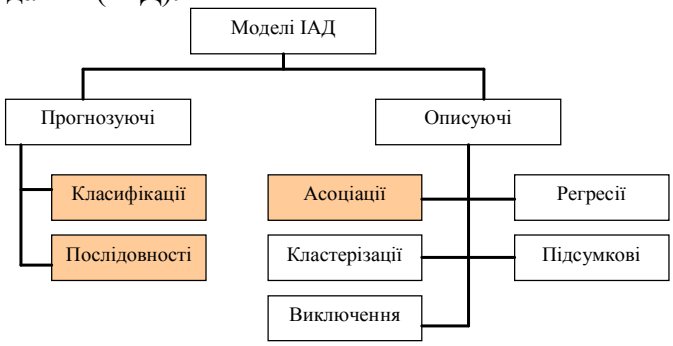


Рис. 1. Класифікація моделей ІАД

Проведений аналіз показує, що у теперішній час відсутні універсальні методи формування нових знань з інформації, яка знаходиться у базах даних (БД).

Основними недоліками існуючих методів є: великий простір пошуку, багаторазове сканування БД, значні часові витрати, відсутність врахування рівня впливу подій, що відбуваються, на ситуацію у цілому та інші.

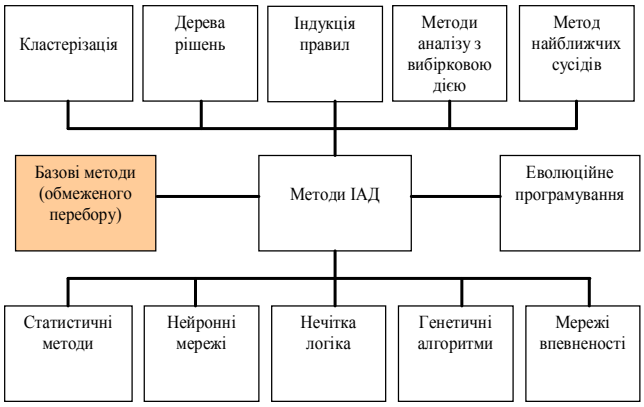


Рис. 2. Класифікація методів ІАД

Тому, другим перспективним напрямком удосконалення СППР є розвиток методів рішення задач ІАД, спрямованих на усунення протиріччя, яке виникає між характеристиками розглянутих методів та вимогами до них.

Таблиця 1

Порівняльна характеристика методів ІАД

Метод	Простота реалізації	Наочність	Наявність формальної теорії	Швидкість роботи	Складність предметної області	Спеціальна підготовка персоналу	Інтегрованість з БД та БЗ	Універсальність мови представлення знань
Базові (обмеженого перебору)	+	+	-	-	+	+	+	-
Дерева рішень	+	+	+/-	+	+/-	+	+/-	-
Індукція правил	+/-	+/-	+/-	+/-	+	+	+	-
Регресивні	+/-	+/-	+	+/-	-	-	-	-
Кластерізація	+/-	+	+	+/-	+/-	+	-	-
Аналіз з вибірковою дією	+/-	+/-	+/-	+/-	+/-	+	-	-
Мережі впевненості	+/-	+/-	+/-	+/-	+/-	+/-	-	-
Метод найближчих сусідів	+/-	+/-	+/-	+/-	+/-	+/-	+/-	-
Нейронні мережі	+/-	-	+/-	+/-	+/-	+	-	-
Генетичні алгоритми	+/-	+/-	+/-	-	+/-	+/-	+	-
Еволюційне програмування	-	+/	+/	-	+/-	+/-	+	+
Нечітка логіка	+/-	+	+/-	+/-	+	+	+	-

Умовні позначення в таблиці:

„+” – властивості методу задовольняють вимозі;

„+/–” – властивості методу задовольняють вимозі не у повній мірі;

„–” – властивості методу не задовольняють вимозі.

Важливим результатом досліджень є сукупність нових та удосконалених методів і алгоритмів формування знань зі сховищ структурованих даних СППР, які дозволяють: виявляти асоціації, що мають місце у тому випадку, коли декілька подій є зв’язаними одна з одною; знаходити закономірності у послідовностях подій, які відбуваються на об’єктах управління (ОУ), що, у свою чергу, дозволяє з певною мірою впевненості прогнозувати появу тих чи інших наступних подій для прийняття більш правильних, своєчасних та обґрунтованих рішень; формувати вирішальні правила, які дозволяють класифікувати об’єкти на відомі класи та інформація про які зберігається у сховищах даних СППР.

Крім того, для усунення недоліків, пов’язаних із значними часовими й інформаційними витратами та суб’єктивізмом під час квантування значень чисельних атрибутів запропонована сукупність зв’язаних методів формування нечітких асоціативних правил, в основу яких покладено теорію лінгвістичних термів та нечітких множин.

Для ефективного аналізу текстових документів запропоновано використання технологій інтелектуального аналізу текстів (ІАТ).

Однією з основних задач ІАТ є квазіреферування електронних документів.

Важливими задачами, які вирішують ОВУ під час інформаційно-аналітичної діяльності є пошук та аналіз електронних документів, що є релевантними до завдань, які ними вирішуються. Задача інформаційного пошуку полягає у знаходженні користувачем

інформації, яка є релевантною його інформаційній потребі. Вирішення цієї задачі полягає, як правило, у порівнянні запита користувача не з повним текстом документа, а з його пошуковим образом, який може складатися з множини інформативних фрагментів первинного електронного документу або квазіреферату та набору ключових слів.

Проведений аналіз показує, що у даний час існує ряд підходів щодо вирішення задачі індексування та квазіреферування електронних документів, але їм властиві недоліки, до яких можна віднести: складність реалізації для великої кількості електронних документів; неможливість побудови універсальної семантичної мережі чи тезаурусу; залучення великої кількості експертів, не адаптованість до спеціальних предметних областей та інші.

Тому запропоновано новий метод та алгоритм формування інформативних фрагментів з неструктурованих первинних електронних документів у сховищах даних СППР та виділення з них множини ключових слів. Метод дозволяє включати до масиву ключових слів тільки ті терми, які найбільш точно відображають зміст даного електронного документу. Він може бути основою для розробки ефективних технологій вирішення задач інтелектуального аналізу текстів, інформаційного пошуку, для автоматизованої реєстрації документів, що циркулюють в системі електронного документообігу органів управління ЗС України, а також аналізу неструктурованих електронних документів, які знаходяться у сховищі даних СППР.

Розроблені методи покладено в наукову основу методології формування знань у СППР.

Оцінка ефективності розроблених методів формування знань здійснювалася за загальноприйнятими показниками. Експериментальна перевірка показала ефективність розроблених методів.

Інтегральна оцінка ефективності розробленого математичного забезпечення здійснювалася на основі підходу, суть якого полягає у тому, що якість рішень представляється повністю залежною від степені їх обґрунтованості.

Під обґрунтованістю рішення розуміють степінь вірогідності доведеності всіх його положень. Обґрунтованість – якісна характеристика рішень, тому для її оцінки доцільно застосовувалися експертні міркування.

Отримані теоретичні результати були перевірені на практиці шляхом проведення спеціальних експериментів, методика організації яких полягала в наступному: було складено алгоритми підготовлення рішення СППР для слабоструктурованих функціональних задач; визначено переліки можливих варіантів алгоритмів, які відрізняються змістом операцій, що виконуються під час підготовлення рішення; проаналізовано інформацію, що використовується під час підготовлення рішення та оцінено обґрунтованість рішень, які приймаються.

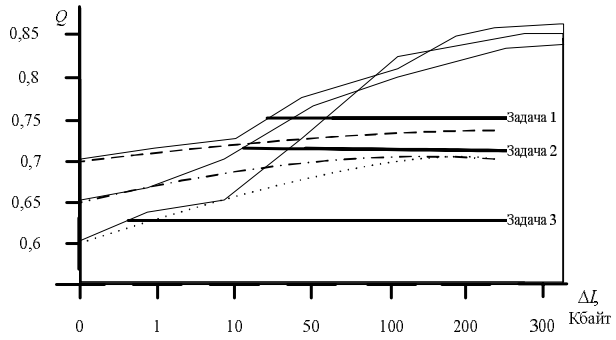


Рис. 3. Графік залежності обґрунтованості рішень від об’єму інформації

Дослідження показали, що застосування запропонованих методів приводить до збільшення степені обґрунтованості рішень, які приймаються в органах військового управління.

к.т.н. Ананьїн О.В. (НДІ ДПСУ)

ОРГАНІЗАЦІЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ В ПІДРОЗДІЛАХ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Європейський досвід свідчить, що технічна робота з документами іноді займає основний зміст діяльності сучасної державної установи чи організації. За результатами дослідження, що проводилися компанією Siemens Business Services в низці європейських установ (компаній), – 30 % робочого часу витрачається працівниками на пошук, відпрацювання та погодження документів, 6 % документів губляться, кожний внутрішній документ копіюється до 20 разів. Фахівцями Siemens Business Services встановлено, що при використанні електронного документообігу продуктивність праці персоналу зростає на 20 – 25 %, в процесі діяльності економиться великий відсоток часу, істотно збільшується оперативність при здійсненні документообміну, вартість архівного зберігання електронних документів на 80 % нижче, в порівнянні з їх паперовими копіями [1, с. 10].

Виходячи з вищеназваного, впровадження систем електронного документообігу в підрозділах управління всіх рівнів сучасних Збройних сил України, в управлінській діяльності яких оперативність прийняття рішень та їх здійснення є головною складовою – стає важливим напрямом підвищення оперативності їх управлінської діяльності.

Метою даної доповіді є: визначити цілі впровадження електронного документообігу в підрозділах управління всіх рівнів Збройних сил України та які можливості, й переваги над традиційним діловодством надає реалізація технологій електронного документообігу; які труднощі можуть виникнути в процесі їхньої реалізації; вказати, які існують на даний час, в Україні, перспективи впровадження систем електронного документообігу, що могли б знайти застосування в сучасних Збройних силах України.

Основними цілями впровадження електронного документообігу в підрозділах управління всіх рівнів Збройних сил України є: прискорення руху документів між головними підрозділами й підпорядкованими та зменшення витрати часу на опрацювання цих документів, що, в свою чергу, дозволить підвищити оперативність й ефективність їхньої управлінської діяльності.

Реалізація саме принципів електронного документообігу на базі новітніх інформаційних технологій за допомогою сучасного апаратного та програмного забезпечення, дасть можливість створити в підрозділах управління всіх рівнів Збройних сил України єдиний інформаційний простір електронного документообігу, інтегруючи в інформаційний вузол всі системи передавання та прийому електронних документів. Інтеграція здійснюється без зниження якості роботи із документами зі збереженням форм традиційного вітчизняного діловодства. Основа подібної інтеграції – надійне сховище електронних документів та взаємодіючої з ним системи передавання, прийому та регістрації електронної документації. Всі електронні документи повинні зберігатися в єдиному сховищі електронних документів, що дозволить забезпечити оптимальний пошук і вибір інформації при підготовці матеріалів. Такий архів електронних документів не відноситься до електронного документообігу, як такового, але робота з ним є його важливою складовою. Інтеграція такого архіву та взаємодіючих з ним систем електронного документообігу в єдиний інформаційний простір підрозділів управління всіх рівнів Збройних сил України дасть можливість зробити доступ до матеріалів та їх обробку більш оперативним та ефективним. Істотними перевагами електронного документообігу над традиційним діловодством, окрім оперативності та зручності, стануть ще, і можливість вміщення в електронний документ разом з текстом мультимедійних даних, використання при складанні документу заздалегідь заготовлених шаблонів, висока швидкість передачі даних, економія паперу, висока компактність архіву, можливість захисту документів від несанкціонованого доступу.

Однак революційні підходи до впровадження електронного документообігу можуть призвести до серйозних труднощів в організації управлінської функції вищих підрозділів над нижчими (підпорядкованими). Наприклад, без побудови якісної комплексної системи захисту інформації, розмежування доступу до документів може призвести до витоку службової інформації, відсутність якісного адміністрування в системі електронного документообігу може призвести до небажаних збоїв в її роботі. Крім того введення самого поняття електронного документообігу [2; 3] потребує розкриття та розуміння його суті в комплексі з такими поняттями, як електронне документування, електронний архів, архів електронних документів. Вкрай необхідне складання якісних методик по різним аспектам експлуатації електронного документообігу в управлінських підрозділах державних органів, в тому числі і в підрозділах управління всіх рівнів Збройних сил України.

За результатами наради на Державному підприємстві „Українські спеціальні системи" за участю Державної служби спеціального зв'язку та захисту інформації України і фірм-розробників систем електронного документообігу, – базовим стандартом електронного документообігу в Україні повинен стати міжнародний стандарт MoReq-2 [4]. На сьогодні MoReq-2 – має універсальний характер.

Цей стандарт є детально опрацьованим та апробованим на практиці, в європейських країнах, який визначає, яким функціональним вимогам повинна відповідати автоматизована система, щоб підтримувати будь-які регламентні роботи з документом. Стандарт MoReq-2 переконує, що базування такої системи має відбуватися на єдиній XML-схемі. Крім того, на додаток до XML-схем документів, визначених MoReq-2, можуть пропонуватися й інші, додаткові, національні XML-схеми, але які логічно та технологічно пов'язані зі схемами MoReq-2 [4]. За своїми функціями автоматизована система документообігу повинна підтримувати весь життєвий шлях документа – від його створення до знищення, або передавання в електронний архів, – забезпечувати діловодство, документообіг та архівне зберігання.

Таким чином, впровадження автоматизованої системи електронного документообігу в масштабі всіх Збройних сил України потребує виваженого, поетапного здійснення. Оскільки прискорене її впровадження може призвести до небажаних збоїв, не тільки в управляючих підрозділах, а разом, як наслідок, й у підпорядкованих підрозділах.

Таким чином перед розгортанням автоматизованої системи електронного документообігу в Збройних силах України необхідно виважено оцінити готовність матеріально-технічної, інформаційної та економічної бази всіх структурних підрозділів управлінської ланки Збройних сил України до переходу до здійснення управлінської діяльності із застосуванням якісно нових інформаційних технологій в сучасному діловодстві.

ЛІТЕРАТУРА

1. *Електронний документообіг* та діловодство. Рішення Microsoft в сфері документообігу для органів державної влади та місцевого самоврядування [Електронний ресурс]: інформаційний бюлетень Microsoft. – М., – 2003 – лютий – 78 с. Режим доступу: www. url. http:// www. Microsoft. com/Ukraine/Govermment/Newsletters/DocFlows/Default.mspx. – Назва з екрану.

2. *Про електронні* документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV/ Верховна рада України // Вісник Держ. ком. арх. України. – 2003. – Випуск 2 (14). – С. 15 – 22.

3. *Боркус В.М.* Системы документооборота: что стоит за терминологией? / В.М. Боркус. – М., 2005. – Режим доступу: www. url. http://www. Intertrust. ru/analytics/135. – Заголовок с экрана.

4. *Офіційний Веб-сайт* Державної служби спеціального зв'язку та захисту інформації України. – Режим доступу:http://www.dstszi.gov.ua.

к.т.н. Андреєв Б.М. (ВІТІ НТУУ „КПІ”)
Терещенко О.М. (ВІТІ НТУУ „КПІ”)

ОСОБЛИВОСТІ ВИМІРЮВАНЬ СИГНАЛІВ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Основним завданням методології вимірювань в сучасній техніці є розробка методик вимірювань фізичних величин, пов’язаних з роботою технічних засобів.

При нормальній експлуатації цифрових систем передачі необхідно враховувати вплив помилок, що виникають по різних причинах в системі. Основним параметром розрахунку тут виступає імовірність виникнення помилки p(t), яка є функцією часу і залежить від ряду чинників і значень параметрів, пов’язаних з різним впливом на систему. Прикладами такого впливу може служити інтерференція сигналів в радіочастотних системах передачі, алгоритмічний джіттер в системах *SDH* тощо [1].

Залежно від природи впливу на систему, характер функції p(t) може суттєво відрізнятися для різних систем. При проектуванні виконується розрахунок функції імовірності залежно від параметрів зовнішнього впливу на систему для визначення якісних параметрів роботи проектованої системи, визначення її стійкості до зовнішніх умов тощо. Перевірити результати розрахунків можна лише шляхом проведення експерименту або шляхом вимірювань на зразку, що досліджується. Проте, теоретична величина – функція імовірності виникнення помилки у системі – не може бути виміряна. Замість неї вимірюється параметр помилки по бітах – *BER*, який може бути представлений як:

$$BER = \frac{BITS_{err}}{BITS},$$

де $BITS_{err}$ – кількість бітів, уражених помилками; *BITS* – загальна кількість переданих бітів. Ця величина пов’язана з функцією імовірності виникнення помилки відношенням:

$BER = \int_{t1}^{t2} p(t)dt$, тобто є математичним очікуванням функції імовірності. За значенням математичного очікування функція імовірності може бути відновлена лише з певною мірою достовірності [2].

У описаному прикладі для того, щоб на підставі результатів можна було б відновити функцію імовірності без помилок, необхідно було б проводити вимірювання *BER* у нескінченно великому інтервалі, що практично неможливо. Таким чином, отримане значення завжди виявляється наближенням теоретичного і залежить від умов вимірювання, які визначаються методологією вимірювань, орієнтованою на мінімізацію помилки оцінки теоретичної величини.

Враховуючи, що розвиток засобів телекомунікацій дуже динамічний, розробка систем самодіагностики і їх відладка дещо відстають від розвитку самих засобів телекомунікацій. Таким чином, використання незалежних від устаткування систем контролю у ряді випадків являється єдино коректним рішенням. В результаті роль вимірювальної техніки у мережах телекомунікацій підвищується з розвитком нових технологій.

Вимірювальна техніка у сучасних мережах телекомунікацій відіграє важливу роль – налаштування і оптимізація мереж телекомунікацій, пошук несправностей і причин конфліктів, вирішення конфліктних ситуацій. Отже, основною рушійною силою розвитку вимірювальних технологій є ускладнення сучасних телекомунікаційних систем [3].

Розповсюджена думка про те, що цифрові телекомунікаційні системи кращі, надійніші, а тому вимагають у меншій мірі обслуговування при експлуатації, не вірна. Дійсно цифрові

технології забезпечують кращу якість зв'язку, менші експлуатаційні витрати, кращий контроль за ресурсом мережі. Вірно також, що добре відлагоджена, „доглянута" цифрова мережа вимагає у меншій мірі обслуговування. Проте також вірно, що „недоглянута" цифрова мережа деградує набагато швидше аналогової і вимагає при відновленні набагато більших витрат. Цифровим телекомунікаціям властивий так званий „пороговий ефект деградації", при якому погіршення параметрів не приводить довгий час до погіршення якості зв'язку. Досягнувши певного порогу параметри якості змінюються стрибкоподібно. Зазвичай, у цьому випадку достатньо складно відразу виділити причину порушення зв'язку, оскільки причини накопичуються протягом довгого часу, а відхилення від норми спостерігаються по декількох параметрах.

Використання сучасної вимірювальної техніки дає спеціалістам ключ до розуміння процесів, що відбуваються в мережі. У цьому випадку пошук конфліктних ситуацій і протиріч, „тонке налаштування" мережі допомагають добитися максимальної ефективності її роботи, а також зрозуміти принципи нової технології.

Ця роль вимірювальної техніки є новою у практиці вітчизняного зв'язку. До цих пір вимірювальна техніка служила для контролю роботи мережі і відповідності її вузлів вітчизняним стандартам. Для цього випадку застосовуються чіткі рекомендації стосовно методології вимірювань на мережах зв'язку (вказівки на прилад, методику і параметри вимірювань). На сьогодні процес стандартизації технології значно відстає від розвитку самих технологій. Чітких рекомендацій з використання вимірювальної техніки та експлуатаційної методології немає і в найближчому майбутньому не передбачається. Вимірювальна техніка використовується сучасними спеціалістами не лише для перевірки на відповідність стандартам (в першу чергу, міжнародним), але й для вивчення процесів, що протікають у мережі. Це дозволяє швидко освоювати нові технології.

Ще одна важлива особливість сучасної вимірювальної техніки для телекомунікацій полягає у тому, що з розвитком цифровізації телекомунікаційних мереж відбувається вищезгадана спеціалізація вимірювальної техніки. Ще 15 – 20 років тому для обслуговування аналогових телекомунікаційних мереж застосовувалася загальновимірювальна техніка (генератори, осцилографи, частотоміри тощо) або її модифікації з урахуванням параметрів телекомунікаційних систем.

Розвиток цифрових систем передачі і комутації призвів до того, що вимірювальна техніка для телекомунікацій стала високоспеціалізованою. Це означає, що її у більшості випадків неможливо використовувати в інших областях людської діяльності. Сучасні вимірювальні прилади для телекомунікацій, такі як аналізатори протоколів сигналізації, аналізатори цифрових систем передачі, вимірювальні прилади ВОЛЗ тощо, складають перелік спеціалізованої техніки, який до останнього часу недостатньо розглядався в технічній літературі.

ЛІТЕРАТУРА

1. *Немет* Э., Снайдер Г., Сибасс С., Хейн Т.Р. // Н50 UNIX: Руководство системного администратора. Для профессионалов / Пер. с англ. – СПб.: Питер; К.: Издательская группа BHV, 2002. – 928 с.: ил.

2. *Армстронг* (мл.), Джеймс // А83 Секреты UNIX: 2-е изд. / Пер. с англ. – М.: Издательский дом „Вильямс", 2001. – 1072 с.: ил.

3. *Олифер* В.Г., Олифер Н.А. // Компьютерные сети: технологии, протоколы. Учебник / – СПб.: Питер, 2000. – 672 с.

Архіпов В. В. (ВІТІ НТУУ „КПІ”)
к.т.н. Любарський С. В. (ВІТІ НТУУ „КПІ”)

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ВПЛИВУ НА ОБ’ЄКТ ІНФОРМАЦІЙНОЇ РОЗВІДКИ В МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Предметною областю дослідження являється мережева розвідка віддаленої корпоративної комп’ютерної мережі на основі впровадження мультиагентних систем у віддалений об’єкт атаки, збір інформаціїї про віддалений об’єкт майбутнього інформаційного впливу для аналізу та встановлення з ним з’єднання та отримання контролю, а також безпосередній інформаційний вплив.

Для встановлення з’єднання та отримання контролю над об’єктом атаки необхідно провести збір інформації про віддалену систему. Під час збору інформації про об’єкт інформаційного впливу передбачені наступні етапи: визначення мережевої топології, тип та версія операційної системи вузла, що атакується, а також доступність мережевих та інших сервісів.

Після аналізу віддаленого інформаційного об’єкту виявляються можливі шляхи з’єднання та встановлення контролю. Відповідно до технології з’єднання з віддаленим інформаційним вузлом залежить можливість проведення операцій інформаційного впливу. Запропоновано наступні технології інформаційного впливу:

- Мультиагент впроваджений у віддалений об’єкт інформаційного впливу працює скритно, маскуючись під звичайний стандартний процес, автономно запускаючись при завантаженні робочої станції, та встановивши зв'язок виконує відповідні покладені на нього функціональні задачі.

При встановленому з’єднанні по протоколу FTP (File Transport Protocol), за допомогою компонентів Indy у візуальному середовищі Borland Delphi7 (FTPClient, FTPServer), та набору їх опцій, дозвляє здійснювати наступний вплив на файлову систему віддаленого об’єкту атаки: видаляти, переглядати, змінювати, копіювати файли, а також визначати структуру та тип файлової системи.

Вплив через поштові протоколи SMTP та POP3 (набором компонентів Internet) дозволяє перехоплювати поштові повідомлення, отримувати журнал контактів листування, відправляти підроблені документи, отримати інформацію про можливу наявність поштового сервера.

При встановленому з’єднанні мультиагента із віддаленим центром управління за допомогою сокетів (компоненти SocketClient, SocketServer, та команди з’єднання Connect, Disconnect), можливо наступне:

1) вплив на апаратне забезпечення шляхом виконання команд відправляємих через сокети. Це надає можливість отримувати розвідувальну інформацію про обладнання віддаленого об’єкта розвідки, його обчислювальні можливості, потужність, тип маркування;

2) забезпечувати чи обмежувати роботу загальних та спеціальних служб. Можливість дистанційного відключення служб, що відповідають за систему безпеки, служби, що підтримують антивірусне програмне забезпечення, служба системи авторизації користувача у системі.

3) отримання зображення інтерфейсу віддаленого робочого стола, відправкою команди winlogScrean;

4) віддалена, скрита робота з реєстром, що дозволяє встановлювати підмінені ключі на відповідне, програмне забезпечення, видалення небажаної інформації, щодо присутності в системі, проведення дистуктивних дій.

Отже, після аналізу віддаленого об’єкту інформаційного впливу та встановлення відповідного з’єднання мультиагента та центру управління практично реалізувавши одну чи декілька технологій здійснити вплив на об’єкт атаки відповідно поставлених задач.

Барсюков С.В. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ СТАНДАРТУ 802.16e-2005 МЕРЕЖІ ШИРОКОСМУГОВОГО ДОСТУПУ НА ОСНОВІ ТЕХНОЛОГІЇ WiMAX

Мобільний WiMAX – технологія бездротових територіально розгалужених мереж широкосмугового доступу. Mobile WiMAX був розроблений в стандарті 802.16e-2005 і дозволив збільшити швидкість переміщення клієнтського устаткування більше 120 км/год. Ця технологія дозволяє паралельно передавати мову, мультимедійну інформацію і цифрові дані по одному каналу зв’язку. Мобільний WiMAX може забезпечити швидкість у десятки мегабіт за секунду для основних конфігурацій базових станцій. Характеристики мобільного WiMAX припускають взаємодію між ним і широкосмуговими провідними системами, включаючи цифрові абонентські лінії, що використовують технології xDSL. Важливою вимогою для успіху проекту є забезпечення послуг мобільного Інтернету.

Основними досягненнями мобільного режиму можна вважати нижче приведені чинники:

– стійкість до багатопроменевого розповсюдження сигналу і власних перешкод;

– масштабована пропускна спроможність каналу;

– технологія Time Division Duplex (TDD), яка дозволяє ефективно обробляти асиметричний трафік і спрощує управління складними системами антен за рахунок естафетної передачі сесії між каналами;

– технологія Hybrid-Automatic Repeat Request (H-ARQ), яка дозволяє зберігати стійке з’єднання при різкій зміні напряму руху клієнтського устаткування;

– розподіл частот, що виділяються, і використання субканалів при високому завантаженні дозволяє оптимізувати передачу даних з урахуванням сили сигналу клієнтського устаткування;

– управління енергозбереженням дозволяє оптимізувати витрати енергії на підтримку зв’язку портативних пристроїв в режимі очікування або простою;

– технологія Network-Optimized Hard Handoff (HHO), яка дозволяє до 50 мілісекунд і менше, скоротити час на перемикання клієнта між каналами;

– технологія Multicast and Broadcast Service (MBS), яка об’єднує функції DVB-H, MEDIAFLO і 3GPP E-UTRA для досягнення високої швидкості передачі даних з використанням одночастотної мережі, гнучкого розподілу радіочастот, низького споживання енергії портативними пристроями;

– технологія Smart Antenna, що підтримує субканали і естафетну передачу сесії між каналами, що дозволяє використовувати складні системи антен, включаючи формування діаграми спрямованості, просторово-часове маркування, просторове мультиплексування);

– технологія Fractional Frequency Reuse, яка для повторного задіювання частот з мінімальними втратами дозволяє контролювати накладення/перетин каналів;

– розмір фрейма в 5 мілісекунд створює оптимальний компроміс між надійністю передачі даних за рахунок використання малих пакетів і накладними витратами за рахунок збільшення числа пакетів (і, як наслідок, заголовків).

У результаті проведеного аналізу стандарту 802.16e-2005 мережі широкосмугового доступу на основі технології WiMAX показано, що мобільний тип доступу забезпечує безперервний сеанс зв’язку при русі пристрою з високою швидкістю (до 120 км/год) в зоні покриття бездротової мережі, гарантує передачу управління при переміщенні між секторами або базовими станціями та дозволяє всім застосуванням працювати безперервно. Для звичайних користувачів впровадження цієї технології буде означати можливість безпровідного високошвидкісного підключення до Інтернету віддалених приміських місць.

Нарощувана архітектура, висока продуктивність при передачі даних і низька, у порівнянні з іншими системами, вартість послуг, що використовують широкосмугові системи, роблять мобільний WiMAX лідером бездротових широкосмугових послуг.

Барсюков С.В. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ПЕРСПЕКТИВ ТЕХНОЛОГІЇ LTE

Досліджено аспекти впровадження та реалізації, а також технологічні особливості розгортання LTE-мереж, як значно більш вигідного проекту, ніж мережі третього покоління.

Поряд з підготовкою більшості країн до впровадження 3G-стандартів передачі даних в GSM-мережах, в світі вже почалося впровадження 4G – технології четвертого покоління, захищених і ефективних, призначених для обміну даними на надвисоких швидкостях. В результаті створено концепт, який враховує потреби споживача. Для мереж GSM, офіційно схваленим 4G-стандартом стане LTE , стандарт „довгостроковій еволюції”.

На сьогоднішній день існує дві основні 4G-технології: Mobile WiMAX і LTE. Єдиний конкурент мобільного WiMAX – стандарт LTE, що є розвитком існуючих мереж UMTS, в свою чергу, замінюють GSM. Впровадження LTE теоретично дозволить забезпечити швидкість передачі даних до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

Сьогодні LTE – найшвидша технологія передачі даних у бездротових мережах з усіх доступних. LTE це розвиток технології UMTS / HSxPA використовує OFDM (до клієнта), SC-FDMA (від клієнта) і MIMO і є дуже гнучким стандартом у плані використання частотного ресурсу. Його можна використовувати в будь-якому діапазоні частот з різною шириною смуги – від 1,25 до 20 МГц. Тому оператори, зможуть використовувати LTE на низьких частотах (700 МГц) для забезпечення щільного покриття території і переходити на високі частоти (2,5–3,5 ГГц) в окремих регіонах (містах та інших „гарячих точках”) для збільшення ємності мережі. Відмінною особливістю даної технології є можливість працювати з частотним (парним, FDD) і тимчасовим (непарною, TDD) поділом каналів, що дозволяє задіяти різні технології обладнання, що знаходиться в операторів. Використання антенних технологій MIMO дозволяє базової станції обслуговувати в 10 разів більше клієнтів, ніж дозволяла WCDMA.

Незважаючи на значні переваги технології LTE за всіма показниками, необхідно підкреслити, що ця технологія використовує метод OFDM. Це визначає підвищені вимоги до точності формування несучих частот. При використанні OFDM, як відомо, з’являється необхідність враховувати потужність міжканальних перешкод. Цей недолік практично можна компенсувати використанням фазорізностної модуляції високих порядків. Цей вид модуляції забезпечує інваріантність системи до стрибків фази і частоти сигналу.

Інтерес операторів зв’язку до технології LTE пов’язаний з тим, що розгортання LTE-мереж – значно більш вигідний проект, ніж мережі третього покоління. Технологія LTE являє собою наступний етап розвитку мобільних мереж GSM / CDMA / WCDMA / TD-SCDMA. LTE краще використовує частотний спектр, відрізняється підвищеною ємністю і меншими значеннями затримки. Мережі LTE можуть розгортатися як у нових, так і діючих частотних діапазонах. LTE має спрощену архітектуру платформи і є єдиною технологією, яка дозволяє застосовувати одну і ту ж платформу для парного і непарного спектра, за рахунок чого суттєво скорочуються витрати операторів. Для передачі великих обсягів інформації LTE підходить більше, ніж 3G, але LTE в Україні з’явиться не скоро.

Технологія LTE цілком підходить під характеристику „технологій завтрашнього дня ”. Швидка швидкість, масштабованість, стійкість до перешкод, пристосованість до складних умов передачі сигналу, все це чудово узгоджується з сучасними вимогами до мультисервісних мереж. Готовність використовувати цю технологію підтверджують оператори і виробники базових станцій і клієнтських терміналів. Питання „останньої милі” (в наших умовах – дуже важливе), є актуальним і чудово вирішується за допомогою LTE. Впровадження технології LTE дозволяє операторам зменшити капітальні та операційні витрати, знизити сукупну вартість володіння мережею, розширити свої можливості в області конвергенції послуг і технологій, підвищити доходи від надання послуг передачі даних.

к.т.н. Башкиров О.М. (ЦНДІ ОВТ ЗС України)

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ ДИВЕРСІЇ ПРОТИ КОМПЛЕКСІВ АВТОМАТИЗАЦІЇ

Новим явищем військового протистояння й ведення бойових дій будь-якими групами держав стає їх інформаційне протиборство, сутність якого полягає у зосередженні головних зусиль збройної боротьби не на фізичному знищенні конкретних одиниць зброї, а на руйнуванні інформаційних ресурсів Збройних сил ворога, руйнуванні або спотворенні системи управління ними, каналів обміну інформації, навігації і наведення, механізмів впливу на індивідуальну і суспільну свідомість. Досвід сучасних локальних війн та збройних конфліктів свідчить про значне зростання інформаційного фактору. В теоретичній частині доповіді формулюється поняття „інформаційно-диверсійна операція" та наводиться його визначення. Формулюються об'єкт ураження, вражаючі фактори, вражаюча дія інформаційно-диверсійної операції, а також її наслідки. В практичній частині доповіді аналізується можливість проведення інформаційно-диверсійної операції проти існуючих та перспективних спеціалізованих АСУ Збройних сил України. З цією метою аналізується структура типового комплексу засобів автоматизації, виявляються „вузькі" місця та звертається увага на конкретні засоби, які можуть застосовуватися як засоби негативного інформаційного впливу. Для проведення інформаційно-диверсійної операції пропонується використовувати типові технічні засоби комплексу, а за необхідністю й додаткові спеціальні. Наведемо приклад проведення інформаційної диверсії проти спеціалізованого комплексу автоматизованого управління засобами протиповітряної оборони та авіації, завдання якого – прискорити прийняття рішення на управління діями бойових засобів та підвищити якість прийняття рішення особами бойової обслуги. Типовий комплекс засобів автоматизації складається з таких основних компонентів: засоби обчислювальної техніки, відображення, в першу чергу автоматизовані робочі місця, апаратура передачі даних, а також деякі допоміжні і технологічні засоби, серед яких системи документування, тренажу, імітації. Особливістю проведення інформаційно-диверсійної операції є те, що втручання в роботу комплексу можливе не тільки з використанням суто „активних" засобів, але й таких, що ззовні є начебто „пасивними", як, наприклад, апаратура документування.

Крім того, в загальному вигляді аналізується типова структура математичного забезпечення та наводяться приклади можливих дій, що застосовують недоліки алгоритмів функціонування комплексів і можуть призвести до негативного впливу. Особливістю проведення інформаційно-диверсійної операції є те, що втручання в роботу комплексу можливе не тільки з використанням суто „активних" засобів впливу, але й таких, що є начебто пасивними, як вже згадані засоби документування. Можна привести приклади явного виведення комплексу з ладу. Наприклад, до складу системи передачі даних входять вбудовані засоби перевірки справності обладнання. Під час функціонального контролю ці засоби генерують тестову перевірочну інформацію та службові сигнали організації обміну. Застосування, вмикання засобів функціонального контролю під час реальної бойової роботи призводить до накладання на реальні дані і сигнали керування роботою прийомо-передавачів імітованих, що призводить до спотворення інформації. 1. Вже сьогодні існує особливий вид бойових дій: інформаційно-диверсійна операція. 2. Проведення інформаційно-диверсійної операції проти існуючих та перспективних спеціалізованих АСУ Збройних сил України або іншої держави можливе. 3. Потрібне проведення окремої НДР, а надалі й ДКР з проведенням натурних експериментів, щоб отримати певні деталі з оцінки можливостей окремих засобів для згаданої мети. 4. Вкрай потрібне організація науково-практичних спеціальних досліджень для отримання чіткого уявлення шляхів спотворення інформації в спеціалізованих комплексах засобів автоматизації управління Збройних сил, обґрунтування унеможливлення або розробки засобів зниження негативного впливу засобів інформаційно-диверсійного впливу.

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

РІШЕННЯ *Triple Play* НА БАЗІ ТЕХНОЛОГІЇ *ADSL2+*

Об’єднання послуг Інтернет – телебачення, *IP* – телефонії та передачі даних реалізує концепцію мереж *NGN (Next Generation Networks)*, в яких технологія *Triple Play* здійснює впровадження всіх трьох базових послуг в одному і тому ж телекомунікаційному просторі.

Рішення *Triple Play* полягає в одночасній підтримці обладнання широкосмугового доступу трьох типів послуг: доступ в Інтернет, *VoIP (Voice over IP* – система передачі голосу поверх *IP*) та *IPTV* (система передачі телебачення поверх *IP*).

В цьому випадку, персональний комп’ютер працює з протоколом *PPPoE*, а телеприставка *STB* (*Set Top Box/IP Set Top Box* – абонентський пристрій для цифрового телебачення) – з *DHCP* (*Dynamic Host Configuration Protocol* – протокол динамічної конфігурації вузла мережі).

Три послуги на одному порту реалізуються на одному *PVC* рис. 1, а далі розподіляються по *VLAN (Virtual LAN* – віртуальна локальна мережа). В одноканальному режимі *PVC*, кожному порту *ADSL* відповідає фіксований постійний віртуальний канал *PVC*, параметри *VPI (Virtual Path Identifier* – ідентифікатор віртуального шляху) та *VCI (Virtual Channel Identifier* – ідентифікатор віртуального каналу). Параметри віртуального каналу *PVC* порта *ADSL* повинні відповідати параметрам каналу *PVC* на стороні віддаленого модему. Якщо налаштування каналу *PVC* на стороні віддаленого модему змінились, то необхідно таким же чином змінити налаштування порту *ADSL*.

Для послуги *Triple Play* створюються три канали *VCI* для одного порта *ADSL* (перший для послуги Інтернет, другий для послуги *IPTV*, третій для послуги *VoIP*) і налаштовуються канали на розподілення трафіку в залежності від пріоритету. Це робиться з метою класифікації трафіку і розділення пакетів по їх пріоритетам на даному порту *ADSL*.

Так, як кожен порт *ADSL* підтримує до 8 каналів *VPI*, кожна плата *ADSL* підтримує до 128 каналів *VPI*, відповідно, загальна кількість каналів *VPI* для всіх портів не може перевищувати 128. Кожний канал *VPI* для порта *ADSL* повинен належати окремій мережі *VLAN*, іншими словами, декілька каналів *VPI* не повинні належати одній мережі *VLAN*. Значення *VPI* і *VCI* повинні відповідати налаштуванням віддаленого модему.

Таким чином, персональний комп’ютер працює через *PPPoE* – протокол, *STB* працює з *DHCP* – протоколом, а потік відео даних передається по *VLAN* багато адресної передачі.

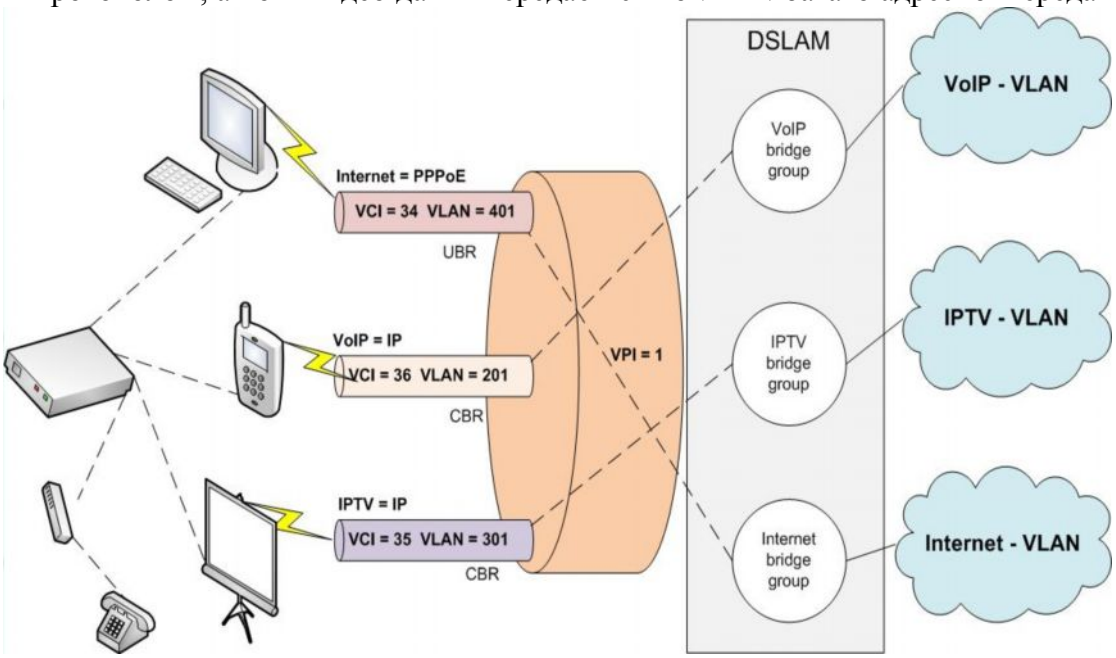


Рис. 1. Реалізація послуги *Triple Play* на абонентському порту

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

ПЛАНУВАННЯ ПРОЕКТІВ ТЕЛЕКОМУНІКАЦІЙНИХ ТРАНСПОРТНИХ МЕРЕЖ

Телекомунікаційна транспортна мережа (ТТМ) є основою будь-якої мережі зв'язку: магістральної, місцевої, мережі доступу. ТТМ − це універсальне неспеціалізоване середовище доставки інформаційних повідомлень у будь-якому форматі (чарунки *ATM*, пакети *Ethernet*, пакети *MPLS*, цикли *PDH* і тощо). ТТМ − базова мережа секцій передачі, мережевих трактів і типових універсальних каналів передачі на основі яких реалізуються можливості вторинних мереж зв'язку, що забезпечують спектр послуг через спеціалізовані користувальницькі інтерфейси для окремих видів послуг (телефонія, Інтернет, телебачення й т.д.) і інтегрованих послуг (В-ЦСИС − *N-ISDN*, Ш-ЦСИС − *B-ISDN*). При цьому ТТМ повинна бути повністю прозорою для користувальницьких послуг, це означає, що мережа планується з урахуванням тривалої перспективи (від 5 до 20 років) її розвитку й зміни; здійснюється облік спеціальних умов і вимог замовника (користувача) ТТМ; передбачається необхідний рівень експлуатації ТТМ і кадровий потенціал; визначається існуюче й перспективне навантаження ТТМ із підрозділом на види й обсяги надаваних послуг (канали, що комутуються, віртуальні канали, що комутуються, пакетна передача із заданою якістю й тощо); вибирається підходяще середовище передачі (оптичний, симетричний або коаксіальний кабель, радіотракти) і базові транспортні технології (*SDH*, *OTH*, *ATM*, *Ethernet*, *T-MPLS*); виконується обґрунтований вибір архітектури ТТМ; обґрунтовується використання методів підвищення надійності мережі через реалізацію захисту лінійних і групових трактів, резервування встаткування й тощо; розробляються схеми організації зв’язку, синхронізації й керування; розраховуються передаточні характеристики лінійних трактів; оптимізується використання обладнання й ліній; формується комплектація обраного обладнання й оцінка вартісних показників; оптимізується мережа по вартісних і якісних показниках при порівнянні як мінімум двох, трьох варіантів топологий, обладнання, лінійних споруджень і тощо.

Перелік цих принципів планування необхідно використовувати при наданні вимог і характеристик ТТМ, що проектується, які можна подати таким чином:

− мережа повинна забезпечувати пропускну здатність або базові швидкості передачі в *STM-N*, *OTUk* або хвильовими каналами λ_i;

− мережа повинна забезпечити перенос сумарного трафику в трактах магістралі (*VC*-12, *VC*-3, *VC*-4, *VC-X-CCAT*, *VC-X-VCAT*, *ODU*1, *ODU*2, *ODU*3, *Ethernet* на швидкості 100 або 1000 Мбіт/с);

− мережа повинна задовольняти заданим значенням надійності або коефіцієнта готовності;

− мережа повинна бути розширюваною, керованою і стійкою до ушкоджень, збоїв й тощо;

− у мережі повинне сполучатися встаткування різних вендерів.

Функціональні можливості ТТМ залежать від навантаження мережі, що визначається користувальницькими / трибними інтерфейсами; лінійними / агрегатними інтерфейсами різних видів передачі (наприклад, однохвильовий або многоволновой в оптичній мережі); операціями групування навантаження (*grooming*) в окремих блоках (VC-*X, ODUk*) або в зчіпці (*VC-X-CCAT*, VC-X-*VCAT*, *ODU-X-VCAT*); можливостями кросової цифрової й оптичної комутації; резервуванням з’єднань у лінійних й кільцевих топологий; резервуванням обладнання; обсягами обладнання й тощо.

Навантаження, що обумовлена при плануванні проекту ТТМ, створіть її сумарні ємності. Ці ємності необхідні для визначення можливостей лінійної передачі з урахуванням операцій захисту з’єднань і перспективи розвитку мережі.

Принципи й вимоги по плануванню й проектуванню ТТМ відбивають загальний підхід до процесу проектування мережі зв’язку.

д.т.н. Бессалов А. В. (ВІТІ НТУУ „КПІ”)
к.т.н. Кокотов О. В. (ВІТІ НТУУ „КПІ”)

КРИПТОСИСТЕМА НА ЕЛІПТИЧНИХ КРИВИХ ЕДВАРДСА НАД ПОЛЕМ ХАРАКТЕРИСТИКИ ДВА

Важливе місце серед алгоритмів несиметричного шифрування займає використання еліптичних кривих [1]. В останні роки в технології криптосистем на еліптичних кривих з'явився новий і досить перспективний напрямок – криві у формі Едвардса [2]. Для полів характеристики 2 в [3] вперше отримані повні формули додавання і подвоєння точок, придатні для будь-яких вхідних точок, включаючи зворотні точки, точки 2-го порядку й точку на нескінченності. Іншою не менш важливою перевагою цих кривих є рекордна швидкодія арифметики експоненціювання точок кривої [4].

Крива у формі Едвардса ізоморфна класичній несуперсингулярній кривій над полем F_2^m, що задається рівнянням

$$v^2 + uv = u^3 + au^2 + b, \quad b \neq 0, \ a,b \in F_2^m. \tag{1}$$

Заміною змінних

$$u = d_1(d_1^2 + d_1 + d_2)(x + y) / (xy + d_1(x + y)),$$

$$v = d_1(d_1^2 + d_1 + d_2)(x / (xy + d_1(x + y)) + d_1 + 1)$$

рівняння (1) приводиться до кривої у формі Едвардса

$$d_1(x + y) + d_2(x^2 + y^2) = xy + xy(x + y) + x^2y^2, \tag{2}$$

де d_1, d_2 – елементи F_2^m з $d_1 \neq 0$ і $d_2 \neq d_1^2 + d_1$. Коефіцієнти кривих (1) і (2) пов'язані співвідношеннями

$$a = d_1^2 + d_2 , \ b = d_1^4(d_1^4 + d_1^2 + d_2^2).$$

Важливою властивістю форми (2) рівняння кривої є його симетрія щодо змінних x і y. Звідси, зокрема, випливає, що якщо (x, y) – точка кривої, то і (y, x) – теж точка цієї кривої. Це дозволяє істотно спростити й прискорити обчислення на кривій.

Таким чином, застосування кривих у формі Едвардса дозволяє значно зменшити обчислювальну складність криптографічних перетворень і є перспективним напрямком в технології криптосистем на еліптичних кривих.

ЛІТЕРАТУРА

1. *Тилборг ван Х.К.А.* Основы криптологии. Профессиональное руководство и интекрактивный учебник. – М.: Мир, 2006, стр. 471, ил.

2. *Edwards, H. M.* A normal form for elliptic curves, Bulletin of the American Mathematical Society 44 (2007), 393{422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html. Citations in this document: x1.

3. *Bernstein D.J., Tanja Lange, Reza Rezaeian Farashahi.* Binary Edwards Curves. IST Programme under Contract IST{2002{507932 ECRYPT, 2008.

4. *Bernstein D.J.* Batch binary Edwards. Department of Computer Science (MC 152). The University of Illinois at Chicago, Chicago, IL 60607{7053.

Білан А.М. (НЦЗІ ВІТІ НТУУ ,,КПІ”)
Зеленко О.В. (НЦЗІ ВІТІ НТУУ ,,КПІ”)

МЕТОДИКИ ПІДВИЩЕННЯ ЯКОСТІ РОБОТИ ОПЕРАТОРА АСУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Діяльність операторів автоматизованих систем управління військового призначення (АСУ ВП) протікає в умовах, що висувають до них підвищенні вимоги. До таких умов відносяться [1]:

− наявність факторів ризику;
− ускладнення функцій оператора;
− сумісна діяльність, тобто виконання оператором двох і більше задач одночасно;
− переробка великих об’ємів і потоків інформації (перевантаження інформацією);
− неповнота інформації для прийняття рішення (сенсорний голод);
− виникнення екстремальних (аварійних) ситуацій;
− дефіцит часу на прийняття рішення та виконання необхідних дій;
− монотонність роботи в умовах очікування сигналу до дій;
− безперервність роботи та обмеження рухової системи людини-оператора на протязі тривалого часу та інші.

Особлива увага при цьому приділяється діяльності оператора в умовах потоку заявок, що потрапляють йому на обслуговування. Вибір цього виду операторської діяльності обумовлений наступними факторами:

− робота в умовах потоку заявок є найбільш розповсюдженим видом операторської діяльності в АСУ ВП;
− потік заявок і обумовлена ним черга на обслуговування здійснюють суттєвий вплив на психофізіологічний стан оператора (напруженість, втому) та показники якості його роботи.

Такими показниками є [2, 3]:

− вірогідність своєчасного прийняття рішення;
− вірогідність правильного (раціонального) прийняття рішення оператором;
− інтегральний критерій, що враховує вищевказані показники.

Потік заявок характеризується інтенсивністю їх надходження. За ступенем впливу інтенсивності вхідного потоку на перелічені показники, діяльність оператора АСУ ВП можна представити у вигляді чотирьох фаз його роботи [3]:

I. Мала інтенсивність вхідного потоку заявок, що надходять на обслуговування оператором. Даній фазі характерна відсутність напруженості у оператора, що призводить до зростання помилкових дій. Це пояснюється розслабленістю оператора в умовах очікування сигналів (монотонна діяльність), що може бути також наслідком пропуску заявок та несвоєчасного прийняття рішення.

II. При збільшенні темпу надходження інформації кількість помилкових дій оператора зменшується. Це досягається за рахунок мобілізації людини-оператора і концентрації уваги на виконанні своїх функцій.

III. При високій інтенсивності вхідного потоку показники якості діяльності оператора знову погіршуються, що обумовлено невідповідністю його перепускної спроможності інтенсивності надходження заявок. Це призводить до збільшення черги на обслуговування, в результаті чого виникає дефіцит часу на прийняття рішення, та різко зростає психофізіологічне навантаження людини-оператора.

IV. Подальше збільшення інтенсивності вхідного потоку заявок призводить до виникнення стресової ситуації та зриву діяльності оператора.

Розрахунок інтенсивності вхідних потоків інформації, що потрапляють на обслуговування операторів, здійснюється, як правило, тільки на етапі проектування

інженерно-психологічної взаємодії людини з технічними засобами автоматизації за загальними (усередненими) даними, тобто на одному з етапів проектування АСУ ВП в цілому. Це не дає змоги більш ефективно використовувати індивідуальні якості людини-оператора на етапі функціонування системи шляхом врахування негативних впливів вхідного потоку на показники якості його роботи.

Тому, пошук оптимального темпу роботи оператора АСУ ВП на протязі всього часу прийняття ним участі в процесі управління, при якому забезпечується необхідна (задана) якість його роботи та висока перепускна спроможність, остається на сьогоднішній день *актуальною* задачею, яка може мати рішення завдяки застосуванню адаптаційних інформаційних моделей (АІМ) на автоматизованих робочих місцях операторів АСУ ВП.

Застосування АІМ передбачає здійснення адаптаційної зміни складу та об'єму тієї інформації, що відображається на засобах візуалізації, при тому як моменти та інтенсивність її надходження залишаються випадковими процесами.

В даній доповіді пропонується розглянути можливість підвищення якості роботи оператора АСУ ВП за рахунок адаптаційної зміни інтенсивності вхідного потоку заявок до його індивідуальних психофізіологічних якостей на протязі всього часу прийняття ним участі в процесі управління.

В такому випадку, в склад системи управління крім основного контуру управління ,,комплекс технічних засобів (КТЗ) – інформаційна модель (ІМ) – оператор" повинен бути включений контур управління ІМ. Адаптивне управління інформаційною моделлю буде здійснюватися наступним чином:

− оцінюється поточний стан якості операторської діяльності;

− при розбіжності поточної та необхідної (заданої) якості його роботи формується сигнал управління ІМ;

− блок вибору засобу управління ІМ перевіряє причину виникнення такої розбіжності, оцінює можливі наслідки та здійснює зміну структури, параметрів ІМ або інтенсивності вхідного потоку заявок до тих пір, поки якість роботи оператора не досягне потрібного рівня.

Основним та найбільш трудомістким елементом схеми адаптивного управління ІМ є блок оцінки поточної якості. Оцінка якості потребує еталонів для визначення точності, безпомилковості і своєчасності дій оператора та ускладнена в технічній реалізації. Тому для прогнозування якості доцільно використовувати модель операторської діяльності. Подібна модель буде специфічною для кожного оператора, тому умовно можна назвати таку модель ,,паспортом" оператора АСУ ВП.

,,Паспортизація" оператора здійснюється шляхом спеціальних експериментів та статистичної обробки отриманих даних про вплив внутрішніх та зовнішніх факторів на якість діяльності конкретного оператора АСУ ВП. Важливою властивістю моделі (,,паспорта") оператора є те, що вона динамічна, тобто дозволяє в кожний поточний момент часу давати оцінку якості діяльності на основі об'єктивних даних про зовнішні та внутрішні фактори діяльності оператора.

Пропонується здійснювати добір та обробку статистичних даних про вплив інтенсивності вхідного потоку заявок, що потрапляють на обслуговування оператору АСУ ВП, на показники якості його роботи за допомогою наступних методик:

І. Методика збільшення ймовірності своєчасного доведення керуючих рішень об'єктам управління за рахунок створення динамічних пріоритетів вхідних заявок на обслуговування, сутність якої полягає в [4]:

− застосуванні не статичних, а динамічних пріоритетів для тих заявок, що надійшли на обслуговування оператору АСУ ВП та знаходяться у черзі;

− врахуванні прогнозованого часу їх очікування, обслуговування та доведення до об'єктів управління (ОУ) з метою недопущення перебування кожної із заявок у черзі більше деякого критичного значення.

Результатом застосування зазначеної методики є упорядкована черга заявок, що подаються на обслуговування оператору АСУ ВП, за максимальною вірогідністю своєчасного прийняття рішення з урахуванням пріоритетності їх обслуговування. Це дозволить збільшити ймовірність своєчасного прийняття рішення оператором АСУ ВП та ймовірність своєчасного доведення керуючих рішень ОУ за рахунок адаптаційної зміни часу очікування заявок у черзі до середнього часу обслуговування заявок оператором та перепускної спроможності телекомунікаційних напрямків.

II. Методика підвищення якості роботи оператора АСУ ВП за рахунок адаптаційної зміни інтенсивності вхідного потоку заявок на обслуговування, сутність якої полягає в [5]:

− доборі та обробці даних про вплив інтенсивності вхідного потоку заявок на показники якості роботи конкретного оператора АСУ ВП на протязі деякого часу з метою побудови відповідної експериментальної залежності;

− знаходженні інтервалу, в межах якого забезпечується відповідність поточної та необхідної (заданої) якості роботи оператора;

− визначенні оптимального значення інтенсивності вхідного потоку, при якому забезпечується найвища якість роботи оператора.

Результати застосування зазначеної методики є вихідними даними для останньої із методик.

III. Методика підвищення якості роботи оператора за рахунок адаптації вхідного потоку заявок на обслуговування до поточного часу робочої зміни, сутність якої полягає в [6]:

− врахуванні негативних впливів інтенсивності вхідного потоку заявок на показники якості роботи оператора АСУ ВП на протязі всього часу прийняття ним участі в процесі управління, тобто на протязі всієї його робочої зміни, бойового чергування тощо;

− доборі та обробці відповідних даних з метою побудови функціональної залежності якості роботи оператора від темпу його роботи за весь час робочої зміни;

− здійсненні адаптаційної зміни інтенсивності вхідного потоку заявок, що потрапляють на обслуговування оператору, у відповідності з отриманими даними.

Результатом застосування третьої методики є сторінка „паспорта” конкретного оператора АСУ ВП, що має дані про залежність якості його роботи від інтенсивності вхідного потоку заявок, що потрапляють йому на обслуговування. Кількість таких даних буде залежати від особливостей організації робочої зміни (в 2 зміни, в 3 зміни і т. д.).

Комплексне застосування зазначених методик дозволить підтримувати необхідну (задану) якість роботи конкретного оператора АСУ ВП на протязі всього часу прийняття ним участі в процесі управління.

ЛІТЕРАТУРА

1. *Забродин Ю.М., Ломов Б.Ф.* Психологические проблемы деятельности в особых условиях. − М.: Наука, 1985. − 362 с.

2. *Душков Б.А.*, *Королев А.В.*, *Смирнов Б.А.* Основы инженерной психологии. – М.: Академический Проект; Екатеринбург: Деловая книга, 2002. – 576 с.

3. *Зинченко В.П.* Введение в эргономику. − М.: „Советское радио”, 1974. − 352 с.

4. *Зеленко О.В., Колачов С.П.* Методика збільшення ймовірності своєчасного доведення керуючих рішень об’єктам управління за рахунок створення динамічних пріоритетів вхідних заявок на обслуговування // Труди академії. – Випуск № 66. – К.: НАОУ, 2005. — С. 51 – 57.

5. *Зеленко О.В., Колачов С.П.* Методика підвищення якості роботи оператора АСУ військового призначення за рахунок адаптаційної зміни інтенсивності вхідного потоку заявок на обслуговування // Зб. наукових праць. – Випуск № 2. – К.: ВІТІ НТУУ „КПІ”, 2006. – С 34 – 42.

6. *Зеленко О.В.* Методика підвищення якості роботи оператора за рахунок адаптації вхідного потоку заявок на обслуговування до поточного часу робочої зміни // Труди академії. – Випуск № 1 (88). – К.: НАОУ, 2009. – С. 43 – 49.

Біленький А.В. (ВІТІ НТУУ„КПІ”)
Процюк Ю.О. (ВІТІ НТУУ„КПІ”)
Філіпенко А.І. (ВІТІ НТУУ„КПІ”)

АНАЛІЗ НАДІЙНОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СПЕЦІАЛІЗОВАНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМ

У цей час питанням аналізу надійності приділяється особлива увага, як в Україні, так і за кордоном. На сьогоднішній день відсутній загальний розв’язок проблеми надійності програмного забезпечення та є багато приватних розв’язків рішень, що не враховують такі фактори, як інтенсивність внесення й усунення помилок у програмі, час розробки програмного забезпечення.

В області машинної обробки інформації існують ще й дві взаємозалежні проблеми: вартість обробки інформації та ненадійність програмного забезпечення, організуючого й виконуючого процес обробки інформації. При цьому перша проблема залежна від другої, тому що висока вартість проектування, тестування й супроводу програм обробки інформації визначається насамперед ненадійністю програмного забезпечення.

З розвитком комп'ютерної науки й комп’ютерної техніки розвиваються й технології створення програмного забезпечення, що вимагає розробки нових методів вирішення проблем надійності. У цей момент існує безліч моделей надійності:

– імітаційні (моделі, які імітують процеси появи помилок)

– статистичні (модель Миллса)

– експонентні (модель Шумана)

– евристичні та ін.

У цей час поставлене й вирішується завдання розробки підмножини моделей надійності спеціалізованого програмного забезпечення яке, на відміну від відомих, дозволяє ураховувати такі фактори як:

– структуру програмного забезпечення на основі блок-схем програм,

– параметри систем контролю програмного забезпечення (час, складність, повноту контролю і т.д.),

– параметри обслуговуючого персоналу,

– спільний облік надійних характеристик апаратури.

За основу взяті евристичні й імітаційні моделі.

У підчас проведеня аналізу надійності програмного забезпечення для спеціалізованих обчислювальних систем, повинна бути створена група моделей з урахуванням зазначених характеристик – створення засобів автоматизації аналізу надійності спеціалізованого програмного забезпечення, обґрунтоване використання програмних платформ та мов моделювання.

Тому пропонується розробка програмно-алгоритмічних засобів для проведення оцінки надійності програмного забезпечення на основі побудови моделі надійності програмного забезпечення, що дозволяє проводити розрахунки характеристик надійності програмного забезпечення (таких як, час наробітку до відмови, коефіцієнт готовності, імовірність відмови) та на основі цієї моделі прогнозувати зміну цих характеристик у часі.

ЛІТЕРАТУРА

1. *Майерс Г.* „Надійність ПО”, М.: Мир, 1981.

2. *Линаев В.В. „*Надійність ПО АСУ”, М.: Энергоиздат, 1981.

3. *Лисс В.А.* „Математичні моделі надійності програмного забезпечення розподілених систем”, М:. Звістки СпбГТУ „ЛЭТИ”, 2005.

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

ЗАСТОСУВАННЯ КРИТЕРІЮ РИЗИКУ ДЛЯ ОЦІНКИ ЗАХИЩЕНОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ

Автоматизовані системи (АС) різних класів займають важливе місце в інформаційній структурі сучасного суспільства. Виконуючи покладені на них функції по прийому, обробці, зберіганню та передачі інформації, вони забезпечують ефективне вирішення задач управління в органах державної влади, в банківській сфері, в сфері виробництва, по пошуку інформації різного характеру. Поряд з проблемами продуктивності, надійності і стійкості функціонування інформаційних систем, гостро постає проблема захисту інформації, що циркулює в них, від несанкціонованого доступу.

Питання оцінки ефективності і проектування системи захисту для АС зазвичай тісно взаємопов’язані, тому що в їх основі лежить єдиний математичний апарат рішення відповідної оптимізаційної задачі.

На сьогоднішній день для оцінки захищеності АС найбільш розповсюдженим на практиці підходом є застосування критерію ризику (потенційних втрат від загроз захищеності):

$$R(p) = \sum_{i=1}^{w} C_i p_i (1 - q_i) ,$$

де C_i – цінність ресурсу (наслідки втрати інформації) в разі здійснення загрози i-го виду;

p_i – ймовірність появи i-ої загрози;

q_i –ймовірність відбиття i-ої загрози;

w – кількість загроз, що діють на систему.

Процес оцінки ризиків складається з чотирьох етапів:

етапу ідентифікації і оцінки ресурсів;

етапу ідентифікації, оцінки загроз і уразливостей;

етапу оцінки захищеності АС;

етапу мінімізації ризиків.

Класифікація ресурсів визначається, як правило, в документі під назвою «Політика інформаційної безпеки». В переліку ресурсів обов’язково вказується тип ресурсу, серійний номер, відповідальний, місцезнаходження, носії інформації, дата вводу і контрольної перевірки. Для кожного інформаційного ресурсу встановлюється відповідний рівень конфіденційності, цілісності, доступності і спостережливості за багатобальною шкалою, наприклад, п’ятибальною. Рівень конфіденційності визначається ступінню важливості ресурсу і наслідками розголошення відповідної інформації, рівень цілісності ресурсу – ступінню пошкодження, фінансових втрат і можливістю відновлення, рівень доступності ресурсу – значенням максимального часу, на протязі якого недоступність ресурсу не впливає негативно на діяльність організації, рівень спостережливості – ступінню повноти, якості і контролю використання ресурсу з боку авторизованих користувачів. Середньоарифметичне значення рівнів конфіденційності, цілісності, доступності і спостережливості кожного ресурсу визначає важливість цього ресурсу.

Етап ідентифікації, оцінки загроз і уразливостей заключається в послідовному виконанні наступних кроків:

визначення загроз для ресурсів організації;

визначення уразливостей, завдяки яким можуть бути реалізовані дані загрози;

визначення існуючих захисних заходів;

визначення ймовірності реалізації загроз.

При цьому спочатку необхідно визначити потенційні загрози для кожного ресурсу, враховуючи місцезнаходження джерела загроз, природу його походження та характер прояву загрози. Далі, для кожного ресурсу слід визначити уразливості, пов’язані з загрозами, і

існуючі захисні заходи. Якщо $q_{ік}$ – ймовірність відбиття *і*-ої загрози *к*-м механізмом захисту, то ймовірність відбиття *і*-ої загрози буде

$$q_i = \prod_к q_{ік}.$$

Відповідно, ймовірність зламу системи захисту становитиме $\overline{q_i} = 1 - q_i$.

Насамкінець визначається ймовірність реалізації загрози. В табл. 1 приведені 7 рівнів реалізації загрози в залежності від їх можливої частоти (інтенсивності).

Таблиця 1

Рівні загрози

Характеристика загрози	Бальна оцінка	Ймовірнісна оцінка	Частота загрози
зневажливо мала	1	0-0,05	практично неможлива
дуже низька	2	0,05-0,2	2-3 рази на 5 років
низька	3	0,2-0,4	1 раз на рік
середня	4	0,4- 0,6	1 раз на півроку або рідше
висока	5	0,6- 0,8	1 раз на місяць або рідше
дуже висока	6	0,8- 0,95	декілька разів на місяць
найвища	7	0,95-1	декілька разів на день

Подібний підхід можна використати для визначення рівнів уразливості ресурсів, виходячи з їх важливості.

Якщо уразливість ресурсу найвища, то рівень реалізації загрози залишається на початковому рівні, тобто бальна оцінка загрози не зменшується. У випадку використання ефективних захисних механізмів рівень загрози знижується на 2–3 бали.

Остаточно рівень ризиків визначається як добуток важливості ресурсу і рівня реалізації загрози (табл. 2).

Таблиця 2

Рівні ризику

Важливість ресурсу	Рівень реалізації загрози						
	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	8	10	12	14
3	3	6	9	12	15	18	21
4	4	8	12	16	20	24	28
5	5	10	15	20	25	30	35

Можливо використання однієї з різновидностей табличної оцінки ризиків – з трибальною, чотирибальною і восьмибальною шкалою. В таблиці 2 приведені значення рівнів ризику за трибальною шкалою:

1) низький, якщо значення ризику знаходяться в межах 1– 4, при цьому припускається, що потенційні втрати мінімальні (до 10 %), вплив на функціонування АС, практично відсутній;

2) середній, якщо значення ризику знаходяться в межах 5 – 8, при цьому припускається, що потенційні втрати становлять до 20 %, є невеликий негативний вплив на діяльність організації. При необхідності можуть бути початі дії по керуванню даним ризиком;

3) високий – значення ризику знаходяться в межах 9 – 35, існують серйозні негативні наслідки для організації, необхідно почати відповідні дії по керуванню даним ризиком. В разі отримання високого ризику може бути прийняте рішення щодо нейтралізації загроз або зниження даного ризику до рівня припустимого шляхом застосування захисних заходів.

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

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Серед основних складових інтегральної безпеки інформаційно-комунікаційних систем таких як фізична безпека, безпека зв’язку, безпека програмного забезпечення, безпека даних, розробка і оцінка ефективності систем фізичного захисту (СФЗ) посідає особливе місце. СФЗ забезпечує захист будинків, приміщень, рухливих засобів, людей, а також апаратних засобів – комп’ютерів, носіїв інформації, мережного встаткування, кабельного господарства тощо.

Одним з базових припущень у питанні оцінки ефективності СФЗ є вимога кількісної оцінки способу, яким реалізована система захисту об’єкта. Існує достатньо багато комп’ютерних моделей для кількісного аналізу оцінки ефективності СФЗ. Кожна з них за міру ефективності приймає своєчасне виявлення порушника. Зрозумівши, наскільки добре СФЗ захищає ресурси об’єкта від загроз, можна визначити кількість ризику, що залишиться після її реалізації. Для цього використаємо наступне рівняння ризику:

$$R = P_A[1 - P_I]C ,$$

де R – ризик для об'єкта за умови одержання зловмисником доступу до важливих ресурсів; діапазон можливих значень 0 – 1, причому $R = 0$ означає повну відсутність ризику, а $R = 1$ – максимальний ризик. Ризик оцінюється за період часу від року до п’яти років;

P_A – імовірність нападу зловмисника на об'єкт протягом розглянутого періоду часу. Ця величина визначається досить складно, як правило, за допомогою експертних оцінок на підставі наявних даних про попередні напади. Значення даного параметра може змінюватися від 0 (відсутні шанси на проведення протиправних дій) до 1 (напад не підлягає сумніву). Іноді при обчисленні ризику припускають, що $P_A = 1$, тобто передбачається напад зловмисника на об’єкт;

P_I – імовірність того, що дії певного зловмисника будуть вчасно перервані силами реагування. Принцип своєчасного виявлення використовується при обчисленні цієї імовірності в межах від 0 (атака зловмисника визначена як успішна) до 1 (напад буде вчасно перерваний);

C – ціна наслідків. Ця величина в межах від 0 до 1 установлює ступінь важливості події, що відбулася. Це нормований фактор, що дозволяє порівнювати величину умовного ризику з усіма іншими видами ризику. Таблиця наслідків подій може бути організована таким чином, що буде охоплювати весь спектр збитків – від найбільш відчутних до незначних.

Оскільки ефективність системи залежить від рівня загрози, доцільно визначити відповідність між спектром загроз і вартістю СФЗ (значенням ризику) для різних варіантів побудови СФЗ. Додатковим інструментом, що може виявитися корисним в оцінці ризику, є матриця наслідків, в яку включаються імовірності нападу зловмисника і загроз. Кожний новий вдосконалений варіант СФЗ визначається своїм значенням ризику і відповідною вартістю системи, що дозволяє зробити необхідні висновки і прийняти правильне рішення.

Простим і зручним у використанні методом оцінки ефективності СФЗ на заданому шляху при певних загрозах і стані самої системи є модель EASI (Estimate of Adversary Sequence Interruption). Ця модель розраховує імовірність переривання дій порушника, виходячи з аналізу взаємодії процесів виявлення, затримки, реагування й передачі інформації. На вхід EASI подається функція виявлення у вигляді імовірності P_D для кожного датчика, встановленого на шляху руху порушника. Імовірність P_D є добутком імовірності виявлення датчиком незаконних або незвичайних дій порушника P_S, імовірності проходження сигналу тривоги до оператора, що робить оцінку тривоги, P_T і імовірності правильної оцінки цієї тривоги P_A.

Передача сигналу тривоги силам реагування подається на вхід EASI у вигляді

імовірності P_C. У більшості розроблених й впроваджених СФЗ імовірність успішного проходження цього сигналу дорівнює 0,95.

Важливими параметрами моделі є час затримки – час, потрібний порушникові для проходження певного шляху до мети і час реагування – час між моментом спрацьовування датчика й моментом появи на шляху порушника сил реагування в кількості, достатній для їхнього перехоплення. Звичайно, ці параметри вважають незалежними і нормально розподіленими.

На виході моделі EASI виходить оцінка ймовірності того, що сили реагування, у достатній кількості, перехоплять порушників у якійсь точці до того, як вони зроблять акт крадіжки або диверсії. Вихідним результатом є імовірність переривання P_I. Якщо на шляху порушника перебуває тільки один датчик, то $P_I = P_C P_D$. У випадку двох або більше датчиків необхідно розглядати виявлення порушника спочатку в першій точці, потім в другій і т. д.

Таким чином, першим кроком при використанні моделі EASI є визначення (вибір) послідовності дій порушника, наприклад, зламати (подолати) огородження, добігти до будівлі, відчинити двері, добігти до приміщення (критичної зони), відчинити двері в приміщення, вивести об'єкт з ладу. Далі по кожній дії порушника встановлюються час затримки *i*-м елементом – Ti , імовірність того, що елемент *i* виявить порушника P_{Di}, та час реагування сил охорони. В моделі EASI час затримки визначається як час, що залишається у порушника до досягнення цілі – T_R, а час реагування T_G вводиться як єдиний середній час зі стандартним відхиленням, що є сумою окремих компонентів:

– часу передачі сигналу тривоги операторові для оцінки;

– часу для оцінки сигналу тривоги;

– часу передачі сигналу тривоги силам реагування;

– часу, необхідного силам реагування для підготовки, одержання зброї, запуску автомобіля й т. п.;

часу руху сил реагування до цілі;

часу, необхідного силам реагування для заняття позицій тощо.

Модель EASI дозволяє показати вплив зміни параметрів фізичного захисту на певному маршруті на ефективність системи захисту і вибрати найбільш прийнятний варіант побудови. Модель легко реалізувати програмним шляхом в середовищі Microsoft Excel. Імовірність прибуття сил реагування до закінчення послідовності дій порушників вважається нормально розподіленою випадковою величиною $x = T_R - T_G$, яка апроксимується за допомогою вбудованої функції НОРМРАСП($\mu(x)$;0;σ_x^2;1) з математичним очікуванням $\mu(x) = \mu(T_R) - \mu(T_G)$ та середньоквадратичним відхиленням $\sigma_x^2 = \sigma^2(T_R) - \sigma^2(T_G)$.

Результати аналізу різних варіантів побудови СФЗ приведені в таблиці 1.

Таблиця 1

Аналіз СФЗ за допомогою моделі EASI

Час реагування, с		Час затримки, с		Характеристика засобів виявлення	Імовірність переривання P_I
Середнє значення	Стандартне відхилення	Середнє значення	Стандартне відхилення		
300	90	332	99,6	2 датчика, P_{Di}=0,9	0,48
300	90	332	99,6	3 датчика, P_{Di}=0,9	0,58
200	60	332	99,6	3 датчика, P_{Di}=0,9	0,83
300	90	452	135,6	3 датчика, P_{Di}=0,9	0,84

Отримані результати дозволяють визначити шляхи підвищення ефективності СФЗ. Так, для збільшення початкової імовірності переривання P_I = 0,48, можливі наступні заходи:

– встановлення додаткового датчика;

– зменшення часу реагування, наприклад, за рахунок переміщення сил охорони ближче до об'єкта захисту;

– збільшення часу затримки.

Саме два останніх заходи приводять до прийнятного значення P_I = 0,83–0,84.

Бугера М.Г. (ЦНДІ ОВТ ЗСУ)
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)

ЗАСТОСУВАННЯ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ В ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ ПІДРОЗДІЛАХ ЗБРОЙНИХ СИЛ УКРАЇНИ

Для інформаційно-аналітичних підрозділів Збройних Сил України характерним є застосування систем підтримки прийняття рішень, які орієнтовані на оперативний аналіз даних, виконання складних запитів, моделювання процесів предметної області, прогнозування, знаходження залежностей між даними. Для наочного подання багатовимірних даних, виконання аналітичних операцій над ними та оперативного створення аналітичних звітів застосовується технологія оперативної аналітичної обробки даних OLAP (On-Line Analytical Processing). Для Збройних Сил характерним є використання інформації яка містить просторову або географічну складову. У більшості OLAP-систем відсутня можливість роботи з картографічною інформацією, що значно зменшує ефективність комплексного аналізу територіально-розподілених даних.

Сучасні геоінформаційні системи військового призначення – це новий тип інтегрованих інформаційних систем, які дозволяють ефективно вирішувати задачі збору, накопичення, обробки і візуалізації геопросторової інформації для її аналізу, моделювання дій військ від окремого підрозділу до Збройних Сил у цілому. Геоінформаційні системи мають широкі можливості з інтеграції та аналізу різнорідних даних і виступають інструментом для рішення задач управління. Головна перевага геоінформаційних систем перед іншими інформаційними технологіями полягає у наборі засобів створення та об’єднання баз даних з можливостями їх графічного аналізу та наочної візуалізації у вигляді мап, графіків, діаграм, прямої прив’язки усіх атрибутивних та графічних даних.

Актуальною є проблема створення нового математичного та програмного забезпечення, яке дозволить застосувати геоінформаційні технології разом із сучасними засобами оперативної аналітичної обробки даних. Інтеграція геоінформаційних систем та OLAP-технологій забезпечить картографічну прив’язку аналітичних даних та динамічне формування і відображення картографічних шарів на основі аналітичної інформації. Динамічний зв’язок багатовимірних даних та електронної мапи значно розширює функціональність OLAP-системи, яка отримує додаткові можливості встановлення відповідності між результатами оперативного аналітичного моделювання та географічними об’єктами і наочного подання багатовимірних даних.

Для геоінформаційних систем доцільно розробити програмні засоби візуалізації даних, які можливо отримати з OLAP-системи або експертної системи. Експертна система забезпечує технологію оперативної підтримки управління.

На основі наведених міркувань пропонується розробити інтегровану інформаційну систему на основі експертної системи, геоінформаційної системи та баз даних. Експертна система виступає блоком управління для геоінформаційної системи, а геоінформаційна система – засобом картографічного представлення результатів логічного виводу для експертної системи або результатів оперативної аналітичної обробки інформації для OLAP-системи. Такий підхід забезпечить взаємний розвиток та розширення функціональних можливостей геоінформаційних технологій, OLAP-систем та експертних систем.

ЛІТЕРАТУРА

1. *Бугаевский Л. М.* Геоинформационные системы. / Л.М. Бугаевский, В.Я. Цветков. – М.: Златоуст, 2000. – 222 с.

2. *GIS* for Defense and Intelligence. – Режим доступу: http://www.esri.com/industries/defense/index.html.

3. *Digital* Topographic Support System (DTSS). – Режим доступу: www.globalsecurity.org/intell/systems/dtss.htm.

к.т.н. Бурячок В.Л. (в/ч А1906)
Бурячок Л.В. (КІСіТ)
Боголій С.М. (ВІТІ НТУУ „КПІ”)

ПОРІВНЯЛЬНЕ ОЦІНЮВАННЯ ПРОГРАМНИХ ЗАСОБІВ ОДНАКОВОГО ФУНКЦІОНАЛЬНОГО ПРИЗНАЧЕННЯ

Зважаючи на те, що останнім часом розвиток комп’ютерної техніки здебільшого зосереджений на розробці та поширенні персональних електронно-обчислювальних машин (ПЕОМ), спеціальне програмне забезпечення, яке використовувалося для великих ЕОМ – на даний час практично не застосовується. Для сучасних ПЕОМ бажано мати такі програмні засоби (ПЗ), які задовольняють новим вимогам до інтерфейсу, підтримують меню, розвитий HELP, іконіку тощо.

З метою якісного розв’язання нагальних завдань, наприклад, інформаційної та інформаційно-аналітичної діяльності, це потребує проведення сертифікації та порівняльного оцінювання ПЗ однакового функціонального призначення, а також вибору серед них такого, яке б відповідало заздалегідь сформованим технічним вимогам (ТВ). Математично дана задача може бути зведена до багатокритеріального оцінювання якості ПЗ по декількох часткових критеріях оптимальності [1, 2]. Одним із можливих шляхів її рішення є застосування методів експертних оцінок, які є визначальними при:

– вирішенні складних завдань оцінювання та вибору будь-яких об’єктів, в тому числі спеціального призначення;

– аналізі та прогнозуванні ситуацій з великою кількістю значимих факторів [3 – 5].

Останнім часом найбільш поширеним серед відомих методів експертного оцінювання є метод аналізу ієрархій (MAI), який поєднує в собі процедури багатокритеріального опису проблеми, синтезу різних міркувань, отримання пріоритетності функцій і критеріїв, а також знаходження альтернативних рішень. Його основне призначення – підтримка прийняття рішень за допомогою ієрархічної декомпозиції проблеми, що розглядається, на більш прості складові частини та подальше рейтингування обраних альтернатив на основі їх попарного порівняння [6].

Алгоритм проведення порівняльного оцінювання ПЗ однакового функціонального призначення одним експертом та прийняття, на підставі отриманих результатів, обґрунтованого рішення щодо вибору серед них найбільш раціональної альтернативи розглянемо на прикладі таких сучасних систем управління базами даних (СУБД), як *Oracle Enterprise Edition*, *DB2 ma Microsoft SQL Server*. В його основу покладемо основні постулати методу MAI, суть та специфічні особливості якого викладені нижче.

На першому кроці дослідником виділяється мета, наприклад, придбання найкращої СУБД серед сукупності подібних, що відповідає першому рівню ієрархії та визначаються вихідні дані, що необхідні для досягнення цієї мети: множина альтернативних СУБД, серед яких необхідно вибрати найкращу та множини притаманних ним функцій і критеріїв. В якості головних функцій, що характеризуватимуть якість обраних СУБД, в даному випадку пропонуємо зупинитись на функціях:

1) реалізації моделі даних і забезпечення взаємодії комп'ютерів у мережі (визначається критеріями підтримки: об’єктно-реляційної моделі даних та стандартних типів реляційних баз даних);

2) реалізації функціональних можливостей (визначається критеріями забезпечення: оптимізації запитів, підтримки мережевих протоколів, розподіленої обробки даних, зберігання/обробки мультемедійних і геопросторових даних та багатомірного аналізу інформації);

3) надійності (визначається критеріями можливості: відновлення після збоїв, резервного копіювання та відновлення змін та захисту від несанкціонованого доступу).

На другому кроці дослідником має бути виконана процедура попарного порівняння як функцій і критеріїв, що характеризують якість СУБД, так власне й самих СУБД за кожним критерієм окремо. При цьому слід враховувати, що значення критеріїв можуть бути задані як якісно – у вигляді показника переваги за певною вербально-числовою шкалою [6], так і кількісно – у вигляді тактико-технічних характеристик або сформованих технічних вимог. За результатами попарного порівняння будуються обернено симетричні матриці на другому (функції), третьому (критерії) та четвертому (СУБД) рівнях ієрархії.

На третьому кроці дослідником визначаються власні вектори та їх нормовані значення для матриць, сформованих на другому кроці дослідження.

На четвертому кроці дослідником мають бути визначенні глобальні пріоритети альтернативних СУБД, отримані на підставі суджень одного експерту. Їх максимальне числове значення дає підставу стверджувати про перевагу певного різновиду СУБД над іншими, що були обрані для оцінювання та порівняння. У запропонованому варіанті вищий пріоритет серед досліджуваних СУБД, як результат, належатиме *Oracle Enterprise Edition*.

На п'ятому кроці дослідником, з метою підтвердження або спростування рішення прийнятого на попередньому кроці, можуть бути виконані заходи по урахування суджень потенційних користувачів про важливість критеріїв (ТТХ) СУБД, які обрані для проведення їх оцінювання та порівняння. У запропонованому варіанті за таких умов найбільш функціональною та надійною при вирішенні завдань інформаційної діяльності може бути визнана СУБД *DB2* фірми *IBM*. Головними аргументами на її користь є: цілісність постачання розробником, можливість співпраці з усіма програмними платформами, здатність до функціонування в клієнт-серверному режимі тощо.

Як результат, запропонований алгоритм порівняльної оцінки ПЗ однакового функціонального призначення, задовольняючи головним вимогам наукового обґрунтування прийняття рішень, дає можливість:

– враховувати якісні характеристики в корисності ПЗ, а саме головні функції (критерії) та множинність цілей програмних засобів, а також можливий ефект від їх взаємодії;

– виключати застосування апарату регресійного аналізу;

– уникати необхідності пошуку функціональних залежностей корисності (важливості) кожної альтернативи від її часткових критеріїв;

– упорядковувати альтернативні варіанти, одержувати їхні вагові коефіцієнти та визначати їх місце в загальному переліку ПЗ, що порівнюються.

В перспективі зазначений алгоритм може бути використаним при створенні автоматизованих систем, спрямованих на забезпечення вирішення завдань інформаційної та інформаційно-аналітичної діяльності спеціалізованими підрозділами будь-якого підпорядкування.

ЛІТЕРАТУРА

1. *Тоценко В.Г.* Методы и системы поддержки принятия решений. / В. Г. Тоценко. – К.: Наук. думка, 2002. –381 с.

2. *Бешелев С.Д.* Экспертные оценки. / С.Д. Бешелев, Ф.Г. Гурвич. – М.: Наука, 1973. – 290 с.

3. *Самохвалов Ю.Я.* Экспертное оценивание. Методический аспект. / Ю.Я. Самохвалов, Е.М. Науменко. – К.: ДУИКТ, 2007. – 263 с.

4. *Мітрахович М.М.* Складні технічні системи. Системне математичне забезпечення проектних рішень. / М.М.Мітрахович. – К.: Нічлава, 1998. – 184 с.

5. *Брахман Т.Р.* Многокритериальность и выбор альтернативы в технике. / Т.Р. Брахман. – М.: Радио и связь, 1984. – 288 с.

6. *Саати Т.Л.* Принятие решений. Метод анализа иерархий. / Т.Л. Саати. – М.: Воениздат, 1993. – 216 с.

Бухал Д.А. (ЦНДІ ЗСУ)
Зеленко О.В. (ВІТІ НТУУ ,,КПІ")
Зіборєва О.Б. (ВІТІ НТУУ ,,КПІ")

ВПЛИВ ЯКОСТІ ОБСЛУГОВУВАННЯ ТРАФІКА ВІЙСЬКОВОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ НА СВОЄЧАСНІСТЬ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІННЯ

Найбільш важливим періодом ведення бойових дій (операції) є період відбиття удару засобів повітряного нападу, коли для прийняття рішення ще до оцінки замислу дій противника необхідно розпізнати мету його бойових дій, обрану стратегію, а по кожній групі цілей поставити бойові завдання за час не більше десятків секунд. Причому існуюча форма управління і постановки бойових завдань підлеглим підрозділам на сьогоднішній день залишається малоефективною – рішення приймається по планшетах, постановка завдань здійснюється голосом і т. д.

При сучасній інтенсивності змін повітряної обстановки та зовнішних інформаційних впливів на систему управління досягнення потрібної її ефективності стає проблематичним. Тому, виникає об'єктивне протиріччя між необхідністю своєчасного формування і передачі управлінської інформаціїї визначеного обсягу до підлеглих військ та неможливістю органів управління вчасно реалізувати задані функції управління.

Таке протиріччя вимушує звертати увагу не стільки на необхідність застосування автоматизованих систем управління (АСУ), скільки на розробку та вдосконалення відповідних алгоритмів обробки та доставки інформації з реалізацією новітніх принципів управління, що і підтверджує актуальність обраної теми.

В інтересах інформаційного забезпечення управління, в ході відбиття удару засобів повітряного нападу противника, будуть максимально застосовуватися різноманітні інформаційні системи (ІС) та АСУ військового призначення. Їх поєднання можливе за допомогою військової телекомунікаційної системи (ВТС) у єдине розподілене інформаційне середовище (ЄРІС), що у реальному масштабі часу може збільшити втрати повітряних угрупувань противника та змусити його відмовитись від виконання завдання. В ході активної фази відбиття удару це забезпечить: своєчасне отримання комплексної інформації щодо дій противника, відображення реальної повітряної обстановки та раціональний цілерозподіл, організацію взаємодії, скорочення циклу управління зброєю і військами.

При цьому, головний недолік полягає в тім, що при застосування ВТС у реальному масштабі часу інтенсивність інформаційного обміну може досягти критичного рівня (відмічається негативний вплив черг на передачу всього трафіка, тимчасово знижується швидкість передачі даних, виникають затримки у доставці пакетів та їх втрата тощо). В результаті це може призвести до зриву відбиття повітряного наступу противника, дезорганізації управління і недосягненню мети проведення бойових дій (операції).

Відповідно до архітектури ВТС, побудованих на протоколах TCP/IP, заявка на передачу інформації у випадку недостачі ресурсу, як правило, не відкидається, а ставиться в чергу на очікування, що буде впливати на ефективність ведення бойових дій підрозділів протиповітряної оборони (ППО). Тому, участь військ у відбитті повітряного наступу противника потребує не тільки тривіального збільшення швидкості передачі інформації, а і проведення спеціальної роботи по мінімізації затримок обслуговування пакетів та уникненню їх негативного впливу на параметри ВТС.

Тому, в доповіді пропонується розглянути можливість здійснення управління параметрами якості інформаційного обслуговування, підтримку її мінімального гарантованого рівня у стані перевантаження згідно угоді про трафік – Quality of Service (QoS), застосування якої дозволить зменшити негативний вплив конструктивних особливостей ВТС на своєчасність інформаційного забезпечення органів військового управління при проведенні бойових дій (операції).

Валюх А.І. (в/ч А1686)

МЕТОДИКА ПІДГОТОВКИ ДАНИХ ДЛЯ АНАЛІЗУ ФАКТІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Постійно зростаючий обсяг інформаційного навантаження вимагає від аналітичних підрозділів органів управління військами застосовувати сучасні, адаптовані до функціональних завдань за призначенням технології автоматизованої обробки даних.

Під час використання відомих методів аналізу інформаційних текстових повідомлень актуальним є завдання інтерпретації фактів у придатній для автоматизованої обробки формі.

З метою вирішення зазначеної проблеми пропонується методика підготовки даних для аналізу фактів, яка, на відміну від існуючих підходів, визначається тематичною спрямованістю процесів обробки інформації в системах спеціального призначення та дозволяє представити події повідомлень у структурованому вигляді.

Для попереднього аналізу даних у методиці використовується експертний реєстр (далі – реєстр), який містить моделі предметної галузі об'єктів, що досліджуються. Реєстр розробляється за тестовими даними групою експертів-аналітиків та складається зі зв'язних структур, що визначають властивості об'єктів спостереження для виявлення ознак у текстових повідомленнях за сформованими правилами – шаблонами. У записах реєстру також містяться перелік посилань на першоджерела повідомлень, в яких виявлені зазначені зразки об'єктів, та коментарі експертів, що не підлягають формалізації у вигляді правил.

Методика визначає такі етапи попередньої обробки інформаційних повідомлень вхідного потоку:

– *підготовка даних*. Повідомлення трансформується до придатної для аналізу форми (видаляються „стоп-слова", обробляються закінчення тощо) та перевіряється на наявність ознак предмета дослідження відповідно до образів зразків об'єктів реєстру;

– *нормалізація даних*. Формується новий формалізований документ зі створеними об'єктами дослідження та їхніми відносинами за виявленими ознаками;

– *верифікація даних*. Сформований документ аналізується на відповідність переданих знань у порівнянні з початковою формою інформаційного повідомлення. Визначається оцінка значимості інформації із прийняттям рішення щодо доцільності подальшої обробки повідомлення (перевіряється на подібність до раніше оброблених повідомлень);

– *завантаження даних*. Створений запис за шаблонною формою з визначеною класовою належністю завантажується до сховища даних для подальшого аналізу стандартними методами Data Mining. Вносяться відповідні зміни до реєстру.

Таким чином, впровадження методики в існуючий цикл обробки поточної інформації підвищить якість отриманих результатів за рахунок врахування максимальної кількості параметрів властивостей подій. Представлення початкових даних у структурованій формі зменшує загальний час всебічного аналізу фактів на виявлення скритих правил та спрощує процедури цільового пошуку інформації. Формалізована структура побудови реєстру та хронологічна зв'язність із подіями інформаційних повідомлень вхідного потоку – сприяє спадковому передаванню знань між експертами.

ЛІТЕРАТУРА

1. *Субач І.Ю.* Извлечение информативных фраз из первичных электронных документов в информационно-поисковых системах / Герасимов Б.М., Субач И.Ю., Сергеев О.Ю. // УСиМ. – 2006. – № 1. – С. 26 – 29.

2. *Субач І.Ю.* Моделі та методи інформаційного пошуку / Герасимов Б.М., Субач І.Ю. // Науково-технічна інформація. – 2004. – № 2. – С. 58 – 63.

3. *Субач І.Ю.* Обробка результатів пошуку в автоматизованих інформаційно-пошукових системах / Герасимов Б.М., Руденок О.А., Субач І.Ю. // Зб. наук. праць ВІ КНУ ім. Т.Г. Шевченка. – 2007. – Вип. № 7. – С. 102 – 109.

Венгеровська О.В. (ГШ ЗС України)
к.т.н. Раєвський В.М. (ВІТІ НТУУ „КПІ”)

ЗАБЕЗПЕЧЕННЯ ДЕКАМЕТРОВОГО РАДІОЗВ’ЯЗКУ ЧЕРЕЗ ВИНЕСЕНИЙ РЕТРАНСЛЯТОР ЯК ЕЛЕМЕНТ СТРИМУВАННЯ ВОЄННОГО КОНФЛІКТУ

Воєнна безпека виступає як критерій реалізації воєнної політики і характеризує стан реалізації національних інтересів держави у воєнній сфері та гарантії її захисту від воєнних загроз і збройної агресії [1 – 4].

Тому забезпечення воєнної безпеки України неможливо без підвищення ступеню як глобальної, так і регіональної стабільності, а також підтримання стану обороноздатності країни, при яких забезпечуються недопущення збройних конфліктів і відсіч можливої військової агресії [1 – 4].

В основу діяльності держави щодо забезпечення воєнної безпеки покладені головні концепції:

концепція співробітництва, яка передбачає активну співпрацю з усіма державами світу у напрямку забезпечення стратегічної стабільності і відвертання воєнних конфліктів виключно політичними, дипломатичними та економічними методами;

концепції стримування, за якою створюється воєнний потенціал України, здатний звести до мінімуму імовірність виникнення воєнного конфлікту за рахунок потенційної можливості нанесення агресору шкоди, при якій він втрачає стимули для нападу.

Проблема запобігання і стримування воєнного конфлікту існує майже з тих пір, коли з’явилася збройна боротьба.

В другій половінні XX-го століття на передній план міждержавних стосунків, поряд з силовим підходом, висувається запобігання і стримування. Враховуючи той факт, що рівень конфліктності в суспільстві не зменшується з часом, а руйнівна сила озброєнь зростає, проблема запобігання і стримування воєнних конфліктів трансформується сьогодні в окрему ціль і функцію держави [1 – 4].

Термін стримування частіше використовують по відношенню до суб’єкту воєнного конфлікту, тобто носія ворожих дій або агресії. Тому, коли говорять стримувати, то йдеться мова про зупинення ворожих намірів, або про те, щоб не дати проявитися ворожим діям, які ведуть до воєнного конфлікту, або про те, щоб придушити наміри до ворожих дій, або такі дії на самому початку.

Очевидно, що стримування є одним із засобів запобігання. Запобігання і стримування визначають єдиний шлях до недопущення воєнних конфліктів.

Таким чином, функція стримування – це вжиття адекватних (випереджувальних) заходів для попередження (призупинення) намірів агресора щодо застосування проти України воєнної сили [1 – 4].

Одним з шляхів стримування є демонстрація власної сили та могутності, або розгортання на суміжній території військових баз. Таким прикладом пострадянського суспільства можуть бути військові бази провідних країн світу в суміжних країнах, наприклад, Російської Федерації в багатьох республіках колишнього Декаметровий радіозв’язок, що був відкритий на початку минулого століття, не зважаючи на свою недосконаліть, використовується наразі цілою низкою підприємств і відомств. Як правило, такий радіозв’язок здійснюється безпосередньо між абонентами, при цьому, як відомо, протяжність одного інтервалу або „скачку” сягає близько 2000 км. Але радіозв’язок між станціями, що розташовані на відстані 100 – 500 км одна від одної забезпечується з великими труднощами. Низька надійність та завадостійкість обумовлені відомими властивостями розповсюдження радіохвиль. Так, при протяжності траси більше 1500 – 2000 км швидкість передачі може сягати до 200 Бод, то при трасі до 400 км швидкість передачі не перебільшує

100 Бод. Вказане пояснюється збільшенням кількості помилок через багатопроменеве розповсюдження радіохвиль [8].

Таким чином, забезпечити якісний декаметровий радіозв'язок на території з граничними розмірами до 2000 км є складною задачею (якою є територія України). Її рішення може бути забезпечено шляхом ускладнення обладнання для прийому більш завадостійких сигналів і різкого підвищення потужності передавача та використання нижньої частини діапазону що не завжди можливо реалізувати [8].

Вимоги підвищення надійності декаметрового радіозв'язку та розширення його функціональних можливостей ведуть до необхідності встановлення радіозв'язку через винесений з зони розташування кореспондентів ретранслятор, що розташований на відстані, близькій до оптимальної (1500 – 2000 км) та який буде відігравати роль центральної управляючої, розподільчої, регенераційної та контролюючої станції [8].

Аналіз застосування такої системи показує що надійність, завадостійкість та ефективність такої системи підвищується завдяки: переходу до більш протяжних ліній зв'язку, оптимальним умовам розповсюдження радіохвиль, переходу до більш широкого діапазону частот що підвищує можливості маневру частотами та зменшує рівень взаємних завад, зменшує потужності випромінювання задіяних засобів, централізованому розподілу частотного резерву та його економії, організації у складі ретранслятора системи прогнозування умов розповсюдження радіохвиль, поточному контролю якості радіозв'язку у всіх ланках системи радіозв'язку, оптимізації системи при постійно змінних умовах обстановки [8].

При застосуванні такого підходу для побудови системи зв'язку воєнної організації довільної країни з територіально обмеженою зоною декаметрового радіозв'язку, можливо розгортання зазначеного ретранслятора на суміжних територіях, що при розумній організації допоможе не тільки удосконалювати систему зв'язку, але і формувати позитивний імідж відповідної країни та забезпечувати струмування збройного конфлікту [5 – 7].

ЛІТЕРАТУРА

1. *Боевые действия* в Персидском заливе: Аналитический обзор. – М.: Воениздат, 1991. – 211 с.

2. *Васильев Г.* Военная операция „Буря в пустыне" //Зарубежное военное обозрение. 1991. – №3. – С. 3 – 20.

3. *Ващанин И.* Войны XXI века. //Зарубежное военное обозрение. 1998. – №3. – С. 17 – 25.

4. *Круглов В., Сосновский М.* О тенденциях развития современной вооруженной борьбы. //Военная мысль. – 1998. - №3. – С. 18 – 28.

5. *Непобедимый С.* Интеллектуализация оружия и оружие против интеллекта. //Военная мысль. – 2003. – №7. – С. 9 – 15.

6. *Березкин Г.* Уроки и выводы из войны в Ираке. //Военная мысль. – 2003. – №7. – С. 12 – 20.

7. Слипченко В.И. Безконтактные войны. –М.: Издат. Дом „Гранпресс" – 2003. – 257 с.

8. *Головин О.В., Чистяков Н.И., Шварц В.* Радиосвязь / Под ред. проф. О.В.Головина. – М.: Горячая линия – Телеком, 2001. – 288 с.

к.т.н. Волков О.В. (ВІТІ НТУУ ,,КПІ”)
Сидоркін П.Г. (ВІТІ НТУУ ,,КПІ”)
Страшна А.В. (ВІТІ НТУУ ,,КПІ”)

ПРОБЛЕМИ І ПЕРСПЕКТИВИ РЕАЛІЗАЦІЇ ТЕХНІЧНОГО І КРИПТОГРАФІЧНОГО ЗАХИСТУ

На сучасному етапі розвитку інформаційних технологій, коли постійно розширюються можливості іноземної розвідки і отримує все більше значення фактор раптовості, захист інформації стає все більш складною проблемою.

Одним з найважливіших технічних аспектів безпеки інформаційно-комунікаційних систем і мереж, наряду з радіоелектронним захистом і застосуванням захищених інформаційних технологій є технічний і криптографічний захист інформації (ТЗ і КТЗ – відповідно). В умовах, коли до систем захисту інформації (СЗІ) пред’являється багато різних, інколи протилежних вимог, актуальною представляється задача розробки інженерних методів вибору найкращого варіанта СЗІ з урахуванням усієї сукупності покажчиків якості.

Принциповими особливостями рішення задачі вибору раціонального варіанта СЗІ, що визначають метод її рішення є:

багатокритеріальність задачі вибору;

кількісний і якісний (нечіткий) опис показників якості СЗІ, що задаються у вигляді вимог;

вплив на вибір методу її рішення експертної інформації, що визначає перевагу того або іншого показника.

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 $Q = (q_1, ..., q_j, ..., q_m)$, виходячи з вибраного критерія переваги.

Як в класичній, так і в нечіткій постановці вибір методу рішення багатокритеріальної задачі визначається тим, в якому вигляді представлена експертна інформація про перевагу показників або їх важливість (табл.1).

Таблиця 1

Вибір методу нечіткої багатокритеріальної оптимізації

Експертна інформація про ступінь переваги чи важливості показників	**Метод рішення багатокритеріальної задачі**
Відсутня	Максимінний метод
Показники упорядковані по важливості	Лексикографічний метод
Визначені вагові коефіцієнти показників	Адитивний показник
	Мультиплікативний показник
	Максимінний показник

Якщо до СЗІ пред’являється n вимог: $C_1, C_2, ..., C_n$ $j = \overline{1, n}$, що мають однакову важливість, то правило для вибору найкращого варіанта може бути записано у вигляді перетину відповідних множин: $D = C_1 \cap C_2 \cap ... \cap C_n$ і вибору такого варіанту a^* з множини варіантів побудови СЗІ $A = \{a_1, a_2, ..., a_m\}$, що має найбільше значення функції приналежності $\mu_D(a^*) = \max\limits_{j=1,\,m} \mu_D(a_j)$.

У випадку, якщо вимоги C мають різну важливість, кожній з них приписується число $a_j \geq 0$ (чим важливіше вимога, тим більше a_j) і загальне правило вибору приймає вигляд $D = C_1^{a_1} \cap C_2^{a_2} \cap ... \cap C_n^{a_n}$.

Кращий варіант a^* знаходиться із співвідношення

$$\mu_D(a^*) = \max_{j=\overline{1,m}} \min_{i=\overline{1,n}} \mu_{c_i}(a_j).$$

В третьому випадку зважена оцінка *i*-го варіанта обчислюється за формулою $R_i = \sum_{j=1}^{n} W_j \cdot R_{ij}$ (R_{ij}; $i = \overline{1,m}$; $j = \overline{1,n}$ – оцінка відповідного варіанта, W_j – відносна важливість кожної вимоги). Оскільки в даному випадку R_{ij} і W_j є нечіткими числами, R_i визначається на основі принципу узагальнення двох нечітких чисел X і $У$: $\mu_z(z) = \sup_{z=x\cdot y} \min(\mu_x(x), \mu_\gamma(y))$.

Слід відмітити, що при виборі раціонального варіанта в якості вимог до СЗІ можуть бути використані якісні і кількісні показники нормативно-методичного і організаційного характеру, технічні характеристики, ступінь кваліфікації персоналу тощо, а кількість варіантів, що розглядаються, як правило, не більше п’яти.

Найбільш проблемними напрямами реалізації КГЗ є наступні:

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

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

3) збереження інформації (документів) на носіях в зашифрованому вигляді;

4) управління ключами з можливістю впровадження окремих елементів інфраструктури відкритих ключів;

5) вдосконалення алгоритмів апаратного шифрування і впровадження засобів програмного шифрування з можливістю використання сучасних засобів зв’язку;

6) дослідження статистичної безпеки КГ алгоритмів у сучасних і перспективних зразках ТСЗ.

Серед можливих напрямів вирішення цієї проблеми, на наш погляд, можна назвати наступні:

1) впровадження сучасних алгоритмів автоматизації обробки і розпізнавання інформації (від FormReader до нейронних і генетичних алгоритмів), представленої в різних формах;

2) 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;

3) застосування стеганографічних методів захисту при передачі зображень, мовних повідомлень і текстової інформації;

4) використання гібридних технологій шифрування, що поєднують можливості і переваги потокового і блочного шифрування;

5) дослідження можливостей впровадження в криптографічну апаратуру кращих світових алгоритмів потокового і блочного шифрування RC4 і AES-128, впровадження вітчизняного стандарту ЕЦП ДСТУ-4145-2002, що реалізується у групі точок еліптичних кривих;

6) 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.

Таким чином, серед можливих потенційних причин ненадійності систем технічного і криптографічного захисту особливої уваги заслуговують неправильне застосування криптографічних алгоритмів і 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.

к.т.н. Волобуєв А.П. (ЦНДІ ЗСУ)
Бондаренко О.Є. (ВІТІ НТУУ „КПІ”)

ПЕРЕВАГИ СИСТЕМ ЗВ’ЯЗКУ НА ОСНОВІ НАДВИСОТНИХ АЕРОПЛАТФОРМ

Сьогодні перед Збройними Силами України гостро стоїть проблема підвищення ефективності системи зв’язку і автоматизованого управління військами. Не останню роль у недостатній ефективності цієї системи відіграє відсутність в Україні власної системи супутникового зв’язку. На цьому фоні провідні місця починають займати технології, альтернативні супутниковому зв’язку. Одна з найбільш потужних альтернатив – це зв’язок за допомогою надвисотних аероплатформ (high altitude platform stations – HAPS). Абревіатура HAPS з’явилася як термін, що позначає стратосферні ретранслятори [1, 2]. Також HAPS – назва технології, що забезпечує послуги бездротового вузькосмугового і широкосмугового зв’язку. HAPS прагнуть надавати ці послуги користувачам, застосовуючи в якості аероплатформ як літаки (пілотовані і безпілотні) так і літальні апарати легше повітря (lighter-than-airships – LTA). Це аероплатформи багаторазового використання, які розміщуються в стратосфері на висотах від 20 до 30 км.

Міжнародний Союз Електрозв’язку (International Telecommunications Union – ITU) ще в 1998 році опублікував звіт під назвою „HAPS: слушна нагода скоротити інформаційний розрив”, який описує HAPS як нову технологію [3]. ITU описує HAPS як „довгоочікувану технологію, що може зробити революцію в індустрії телекомунікацій, це наступне покоління бездротових систем зв’язку, що може збільшити ефективність використання ресурсів радіочастотного спектра, демонструючи набагато більше можливостей, більш високу якість передачі та більш низький ризик операцій з модернізації устаткування в будь-який час”.

Враховуючи, що об’єм трафіка, який циркулює в каналах зв’язку, неухильно збільшуються, з’являється гостра необхідність у нарощуванні можливостей існуючих телекомунікаційних мереж. Але створення і виведення на орбіту супутників зв’язку – досить дороге заняття, і значного посилення супутникового угруповання у світі не відбувається. Це здебільшого пов’язано з тим, що останнім часом провідні країни світу розглядають концептуальні рішення іншого роду. В 1996 році рішенням заступника міністра оборони США по закупівлях озброєнь і технологій був сформований спеціальний підрозділ, що одержав найменування JAPO (Joint Aerostat Project Office) який призначений для організації розробок і випробувань зразків телекомунікаційних і розвідувальних засобів, розташовуваних на аеростатах. Власні програми Пентагона йдуть по двох напрямках. Перший – це створення невеликих дешевих дирижаблів і прив’язних аеростатів, другий – великих моделей, здатних залишатися в повітрі місяцями.

Про зацікавленість оборонних відомств провідних країн світу у створенні систем зв’язку на основі HAPS свідчить зокрема факт укладання контракту на $10 мільйонів у 2006 році компанії Lockheed Martin з Агентством перспективних оборонних наукових досліджень Міністерства оборони США (Defense Advanced Research Projects Agency – DARPA) на розробку досконалих матеріалів корпусів стратосферних LTA, та на $3,8 мільйонів у 2008 році міжнародної аерокосмічної компанії Boeing з DARPA, згідно якого Boeing прийме участь у першій фазі проекту „Стерв’ятник” по створенню нового типу літака з ультравеликою тривалістю польоту (ultra-long-endurance aircraft). Ця угода – частина проекту DARPA „Стерв’ятник”, спрямованого на створення літака, що зможе залишатися в польоті більш ніж 5 років і служити псевдосупутниковою системою. Літак має нести 500 кг корисного навантаження. Boeing буде працювати в команді з британською компанією QinetiQ Ltd [4].

Перебуваючи в геостаціонарному польоті, HAPS будуть забезпечувати послуги, еквівалентні супутниковим, такі як послуги регіональних систем спостереження за

поверхнею Землі та систем зв'язку з радіусом дії близько 500 км. HAPS, перебуваючи на висоті близько 25 км, здатні створити приблизно 700 – 1000 стовбурів ретрансляції в зоні покриття, тоді як негеостаціонарний супутник перебуваючи на висоті 500 км створить тільки 6 – 9 стовбурів.

Одна з головних причин, чому засновані на HAPS системи зв'язку надзвичайно цікаві, це їх характеристики втрат у вільному просторі. Наприклад, для HAPS, розташованих на висоті 25 км, втрати у вільному просторі порівняні з втратами на межі невеликого наземного стільника радіусом 2,5 км. А оператори супутникового зв'язку, маючи значні втрати у вільному просторі на відстанях у тисячі кілометрів, змушені просувати технології розвитку складних антенних систем і радіопристроїв, щоб гарантувати необхідну якість обслуговування. Іншою важливою перевагою HAPS систем перед супутниками є більш коротка затримка сигналу, що йде від HAPS до абонента на Землі. Наприклад, для низькоорбітального супутника, що перебуває на висоті 1400 км, однобічна затримка становить приблизно 5 мс, тоді як для HAPS, розташованої на висоті 25 км, ця затримка становить тільки 0,083 мс.

При цьому вартість HAPS системи оцінюється в 4 рази нижче вартості супутникової системи для геостаціонарних супутників і в 20 разів нижче ніж для низькоорбітальних супутників.

Аероплатформи не вимагають ракети – носія, тобто вони можуть рухатися самостійно на своїх двигунах або залишатися на місці, вони можуть здійснювати посадку на Землю, піддаватися відновленню і знову повертатися на місце. Як тільки платформа досягла робочої точки, вона може негайно почати забезпечувати зв'язок у межах зони покриття без необхідності розгортання глобальної інфраструктури або сузір'я платформ. Стратосфера забезпечує для абонентських станцій вільну лінію візування до платформи. Використовуючи невеликі антени і маючи низькі вимоги по живленню, HAPS враховують велике розмаїття абонентських терміналів, щоб відповідати практично будь-яким вимогам обслуговування.

На відміну від класичних LTA, для сучасних конструкторів з'явилася можливість захистити LTA від зенітного вогню різними видами легкої, але в той же час міцної броні. Такі види захисту були розроблені для штурмових літаків і вертольотів. Велике значення в захисті LTA може мати кевлар – штучне волокно з високою міцністю, що в 5 разів перевищує міцність сталі. Кевларові волокна та тканини мають більш високу міцність, ніж найбільш міцні сорти високоякісної сталі, але при цьому в 5,2 рази менш щільні, добре підходять для обшивання LTA та для захисту об'ємних газових балонів, що розташовуються усередині корпуса. Сполучення різних видів броні дозволяє зробити LTA дуже стійким до зенітного вогню. В цьому плані LTA має перевагу перед літаком. Оскільки підйомна сила створюється газом легше повітря, то навіть при серйозних ушкодженнях, LTA може залишатися в повітрі або здійснити посадку.

Таким чином, системи зв'язку на основі HAPS мають безсумнівні перспективи застосування у військовій сфері. Враховуючи значні фінансові витрати на створення систем супутникового зв'язку та фінансовий провал існуючих супутникових комерційних проектів, для України було б доцільним зосередити зусилля на створенні власної HAPS системи.

ЛІТЕРАТУРА

1. *Ільченко М.Ю.*, Кравчук С.О. Телекомунікаційні системи на основі висотних аероплатформ. – К.: НПП Видавництво „Наукова думка" НАН Украины, 2008. – 580 с.

2. *International* Telecommunication Union, Fixed Service Recommendation F.592 – 3, Vocabulary of terms for the fixed service, 1 – 10, Geneva, 2002.

3. *Tozer T.*, Grace D., Thompson J., Baynham P. UAVs and HAPs – potential convergence for military communications // Military Satellite Communications, IEE Colloquium on. – 2000. № 10 P. 1 – 6.

4. http://www.boeing.com/news/releases/2008/q2/080421d_nr.html.

Восколович О.І. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА АДАПТИВНОЇ ЗМІНИ ПАРАМЕТРІВ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ В КАНАЛАХ СИСТЕМИ MIMO

Для військових систем радіозв’язку (СРЗ) особливо актуальною задачею є підвищення пропускної здатності і завадозахищеності. Це обумовлено низкою причин, основними з яких є обмежений частотний ресурс та підвищення вимог до об’єму та швидкості передачі інформації радіозасобами [1]. Одним з напрямків підвищення ефективності засобів радіозв’язку є застосування методів просторової обробки сигналів у системах радіодоступу, зокрема технології „багато входів – багато виходів” (*Multiple-input multiple-output – MIMO*) [2]. У технології *MIMO* об’єднані просторово-часові методи прийому з використанням адаптивних антен і методи просторово-часового кодування і просторово-часового розділення сигналів. Підвищення ефективності системи передачі за рахунок узгодження форми переданих сигналів і виду модуляції з каналом зв’язку, в якому діють навмисні завади та селективні завмирання, без додаткового збільшення потужності передавача є досить актуальним завданням.

В умовах складної завадової обстановки ефективне функціонування СРЗ неможливе без застосування системи адаптації, основною задачею якої є формування на передаючій стороні оптимальних управляючих дій, що змінюють вид СКК [3]. За рахунок цього досягається значне збільшення швидкості передачі даних у власних каналах. Тому ефективність використання *MIMO* в сучасних системах радіозв’язку, значною мірою, залежить від вибору методів формування сигналу взалежності від завадової обстановки та дії завмирань у каналі зв’язку.

Тому метою роботи є розробка методики адаптивної зміни виду сигнально-кодових конструкцій у власних каналах системи *MIMO*.

Основна суть методики полягає у адаптивній зміні параметрів СКК, а саме виду модуляції, коректуючого і маніпуляційного кодів в заздалегідь визначених кращих власних каналах (найгірші канали відключаються, а потужність передавача, що на них затрачується, перерозподіляється між найкращими власними каналами що залишилися) при виконанні обмежень на якість ($P_{\text{пом}} \le P_{\text{пом доп}}$) і швидкість ($\nu_i \le \nu_{i\text{доп}}$) передачі інформації.

Для оцінки ефективності запропонованої методики було проведено імітаційне моделювання роботи системи *MIMO* при різному ступені глибини селективних завмирань сигналу в каналі зв’язку. Для побудови імітаційної моделі був застосований метод прямого імовірнісного моделювання, який полягає в генерації послідовності реалізацій вихідних випадкових процесів і функціональному перетворенні їх у відповідності зі структурою моделюємої системи і, нарешті, до статистичної обробки послідовності реалізацій на виході системи. Новизна запропонованої методики полягає у поєднанні процедури відкидання найгірших підканалів системи *MIMO*, уражених навмисними завадами і селективними завмираннями з процедурою вибору параметрів СКК для кожного паралельного каналу в залежності від завадової обстановки в каналі.

Таким чином запропонована методика дозволяє підвищити завадостійкість СРЗ при впливі навмисних завад та селективних завмирань на 12–17% у порівнянні з відомими.

ЛІТЕРАТУРА

1. *Вишневский В.М.* Широкополосные беспроводные сети передачи информации. / В. М. Вишневский, А. И. Ляхов, С. Л. Портной, И. В. Шахнович – М.: Техносфера, 2005. – 592 с.

2. *В. Слюсар.* Системы MIMO: принципы построения и обработка сигналов / Электроника: Наука, Технология, Бизнес. – 2005. – № 8. – С. 52 – 58.

3. *Бабич В. Д.* Завадостійкість каналів зв’язку: Навчальний посібник / В. Д. Бабич, О. В. Кувшинов, О. П. Лежнюк, С. П. Лівенцев – К.: КВІУЗ, 2001. – 150 с.

Гімпельс І.В. (ВІТІ НТУУ „КПІ”)

ЗАСТОСУВАННЯ SOFTSWITCH В МЕРЕЖАХ МОБІЛЬНОГО ЗВ’ЯЗКУ

Розглядається одна з областей застосування Softswitch в мережі мобільного зв’язку.

Як відомо, єдина мережа передачі даних між центральним вузлом комутації і базовими станціями істотно знижує витрати оператора за рахунок менших витрат на її будівництво і обслуговування, а також ефективнішого використання пропускної здатності з’єднувальних каналів. Така транспортна інфраструктура дозволяє надавати послуги передачі голосу і даних (а також факс і Internet), що логічно вписується в концепцію переходу до стандартів 2.5G і 3G. Планується інтеграція мереж мобільного зв’язку різних операторів (оператори мобільних мереж 2G, 2G+ і 3G) в транзитну мультисервісну мережу на базі обладнання Softswitch [1, 2].

Для побудови мережі мобільного зв’язку використовується принцип декомпозиції шлюзів, при якому логіка роботи мережі відділяється в центральному управляючому пристрої. Данне рішення забезпечує масштабованість мережі і простоту експлуатаційного управління. Крім того, шлюзи стають менш дорогими, що дозволяє встановлювати їх у великій кількості [3].

Використання Softswitch і сигнального шлюзу з підтримкою протоколу Sigtran (ЗКС № 7 поверх IP) дозволяє відмовитися від організації виділених каналів до мережі ЗКС №7, або послуг третіх компаній, які забезпечують транзит сигнального трафіку. Для оператора потрібний тільки звичайний канал доступу до Internet і він користується послугами мультисервісної мережі у разі необхідності. Крім того відновити дані в регістрі місцеположення (HLR) „домашньої” мережі при реєстрації, відключенні терміналу і т.д. Softswitch повністю контролює хід з’єднання. При втраті зв’язку з одним із шлюзів з’єднання з іншим шлюзом коректно завершується, система обліку фіксує реальний час з’єднання. Взаємодія з шлюзами інших операторів здійснюється з однієї IP-адреси (для них Softswitch виглядає як звичайний шлюз). Softswitch коректно взаємодіє з шлюзами різних виробників. І ще одна особливість полягає в тому, що він дозволяє вести облік з’єднань з корпоративними шлюзами [4, 5].

У зонових мережах зв’язку, у яких є сегмент транспортної мережі на базі технології комутації пакетів, устаткування Softswitch може використовуватись для забезпечення транзиту внутрізонового трафіку в межах телефонної зони або для транзиту голосового трафіку в місцевій мережі зв’язку. Крім того, при будівництві нових станцій комутації передача транзитного навантаження між ними може здійснюватися по мережі з комутацією пакетів. [6].

Отже, Softswitch не можна вважати простим набором програмних серверів. Він описує новий тип телекомунікаційної ідеології, заснованих на розподіленій і масштабованій архітектурі та відкритих стандартах. Softswitch може управляти будь-яким обладнанням, не залежно від того, на якій платформі функціонує його програмна система. Для нього немає переважних протоколів сигналізації, оскільки в його основу закладена взаємодія протоколів.

ЛІТЕРАТУРА

1. *Голышко А.* Какие мультисервисные сети выберет поколение NEXT // Мир связи. Connect. 2005. № 5.

2. *Андрианова Ю.* Мультисервисный доступ // Журнал „Сети”. 2003. № 23.

3. *Полунин А.* Операторские сети нового поколения // Журнал „Сети” 2005. № 6.

4. *Барсков А.* Alcatel 5020 Softswitch // „Сети и системы связи”. 2008. № 1.

5. *Айдарханов Д. М.* Программный коммутатор Softswitch в сетях IP-телефонии // „Мобильные системы”. 2006. № 12.

6. *Introduction to* the softswitch consortium // Softswitch consortium. 2009.

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

ЗАСТОСУВАННЯ ПЕРСПЕКТИВНИХ РАДІОЗАСОБІВ ТАКТИЧНОГО РІВНЯ

Радіозасоби тактичної ланки мають удосконалюватися у трьох загальних напрямах, а саме:

вдосконалення елементної бази та технологій виробництва;

впровадження цифрової обробки сигналів;

формування інтегрованого інформаційного простору на основі мобільних мереж, які адаптуються, що передбачає:

створення так званих самоконфігуруємих мереж;

застосування програмованих радіозасобів [1].

Реалізація вказаних напрямів пов’язана насамперед, із створенням нових радіозасобів тактичного рівня. При розробці таких засобів слід враховувати специфічні особливості умов їх застосування, які вимагають рішення складних системотехнічних, схемотехнічних та конструктивно-технологічних задач побудови радіоапаратури [2].

Значний якісний крок у розвитку досягнуто в радіостанціях 5-го покоління, до якого можна віднести нові радіостанції виробництва одеського заводу „Телекард-Прилад”: Р-002, Р-005, Р-030, а також радіорелейну станцію Р-450. Ці радіозасоби вже розпочали досить інтенсивно надходити у війська зв’язку Збройних Сил України.

Проте постає питання ефективності впровадження даних засобів на мережах військового зв’язку та аналізу можливих варіантів їх застосування. До позитивних сторін вказаних радіостанцій слід віднести підвищення завадостійкості за рахунок впровадження режиму псевдовипадкового перелаштування робочої частоти (ППРЧ), наявності технічного маскування мови (ТММ), підвищення, порівняно з попередніми поколіннями, швидкодії при перелаштуванні робочих частот та режимів роботи, наявності можливостей за адресним передаванням буквенно-цифрових коротких повідомлень або даних у вигляді файлів [3].

З іншого боку всі зазначені переваги даних радіозасобів можуть бути в повній мірі реалізовані тільки за умови виконання певних вимог, а саме:

зустрічної роботи виключно з аналогічними зразками радіостанцій для забезпечення режиму ППРЧ (в наслідок ексклюзивності реалізованих алгоритмів ППРЧ);

застосування їх у сукупності із інформаційною системою „Нарада” (у зв’язку з обмеженістю файлів, що передаються, обсягом 150 кбайт);

наявності кваліфікованого персоналу, здатного забезпечити грамотну експлуатацію та використання нових можливостей;

наявності додаткових пристроїв (обладнання) для забезпечення певних режимів роботи (для передачі файлів – терміналу, для заряджання акумуляторів – спеціального зарядного пристрою і т.д.);

розробки зрозумілих методик застосування.

У випадку незабезпечення таких вимог, реалізація всіх переваг аналізуємих радіозасобів не можлива.

ЛІТЕРАТУРА

1. *Н. Щербак*. Программируемые радиостанции – будущее тактической святи // Электроника: наука, технология, бизнес. – 2001. – № 5 – С. 16 – 19.

2. *Джон Кокс*. Адаптивная радиосвязь в зоне военных действий. – www.osp.ru/cw/2007/43/4521057/prinver.html.

3. *Л. Разгуляев*. Перспективные мобильные адаптивные сети передачи информации для СВ США // Зарубежное военное обозрение. – 2008 – № 1 – С. 35 – 39.

к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)
Якименко В.В. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМ ІДЕНТИФІКАЦІЇ БАЗОВОЇ СТАНЦІЇ В СТАНДАРТІ *GSM*

На сьогоднішній день використання пристроїв емуляції базової станції стандарту *GSM* дуже розвинуто, тому конфіденційність передачі інформації у мережах мобільного зв’язку не забезпечується. Злочинець, який має одну з таких систем, може безперешкодно дізнатися місце знаходження абонента та його номер, перехопити розмову або повідомлення яке посилається, переключати шифрування базової станції на свій емулятор. Відслідковувати базову станцію та відстань до неї та багато інших можливостей. Одною з таких систем є *SPYTEC* 3 000.

Для забезпечення безпеки зв’язку від таких систем використовується аутентифікація та ідентифікація абонента.

Аутентифікація – процедура перевірки дійсності абонента.

Ідентифікація – це процедура ототожнювання рухомої станції (абонентського радіотелефонного апарата), тобто процедура установки належності до одної із груп, що володіє певними властивостями та признаками. Ця процедура використовується для виявлення украдених, загублених та непрацюючих апаратів.

Однак існує проблема ототожнення базової станції, що може призводити до несанкціонованого доступу до мережі мобільного зв’язку таких емуляторів як *SPYTEC* 3 000.

Запропонований в доповіді алгоритм ідентифікації базової станції дає змогу ідентифікувати базову станцію, таким чином збільшити рівень безпеки інформації від систем прослуховування та моніторингу і забезпечити скритність та надійність передачі інформації.

Основні етапи запропонованого алгоритму наступні: після включення пересувної станції (мобільного апарата) відбувається аутентифікація абонента, по закінченню цього процесу пересувна станція посилає сигнал-запиту псевдовипадкову послідовність по радіоканалу на базову станцію. При прийомі такого сигналу базова станція розуміє, що в неї запитують процедуру ідентифікації, та здійснює додавання псевдовипадкової послідовності з *ID*-кодом даної базової станції.

Закодований сигнал (Кз) передається назад по радіоканалу на пересувну станцію. Після приймання сигналу в пересувній станції відбувається додавання прийнятого закодованого сигналу (Кз) з усіма *ID*-кодами дозволених базових станцій, які записані в *SIM*-карті (модуль ідентифікації абонента).

Після додавання вирахувана псевдо випадкова послідоввність порівнюється з тою що посилалась на базову станцію і якщо вони співпадають, то відбувається ідентифікація базової станції, а якщо ні то розрив з’єднання.

Отже запропонований алгоритм дає змогу покращити рівень захищеності систем мобільного зв’язку від несанкціонованого доступу до інформації, що передається у мережі мобільного зв’язку.

ЛІТЕРАТУРА

1. *Урядников Ф.Ю.* Надширокосмуговий зв’язок. Теорія і застосування / Ф.Ю. Урядников С.С. Аджемов.– М.: СОЛОН-Прес, 2005. – 368 с. (Серія „Бібліотека студента”).

2. *В.П. Іпатов, В.К. Орлів, І.М. Самойлов, В.Н. Смирнов*; під ред. В.П. Іпатова. Системи мобільного зв’язку: навчальний посібник для вузів – М.: Гаряча лінія Телеком, 2003.– 272 с.

3. *В.В. Крухмальов, Н.В. Гордієнко, А.Д. Моченов і ін*.; під. ред. В.Н. Гордієнко і В.В. – Крухмальова. Основи побудови телекомунікаційних систем і мереж: підручник для вузів – М.: Гаряча лінія Телеком, 2004. – 510 с.: мул.

4. http://www.alarm-gsm.ru.

5. http://www.edgemodem.ru.

к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)
Якименко В.В. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ БЕЗПЕКИ ЗВ’ЯЗКУ В РІЗНИХ СТАНДАРТАХ МОБІЛЬНОГО ЗВ’ЯЗКУ

Безпека зв’язку – здатність зв’язку зберігати в таємниці зміст переданих повідомлень і протистояти вводу фальшивої інформації.

Широке поширення та використання систем мобільного зв’язку в різних галузях дозволяє передавати будь яку інформацію, але виникає питання чи можливо передавати конфіденційну інформацію? Кожне інформаційне повідомлення сучасних комунікацій можуть прочитати та побачити багато хто, від приватних осіб до найпотужніших розвідок світу. В різних стандартах мобільного зв’язку безпека передачі конфіденційної інформації забезпечується по різному. В доповіді розглядаються декілька стандартів мобільного зв’язку *GSM*, *CDMA*, *DECT*. В стандарті *GSM* під безпекою зв’язку розуміється – виключення несанкціонованого використання системи і забезпечення таємності переговорів рухомих абонентів. Визначено наступні механізми безпеки в стандарті *GSM*:

– аутентифікація та ідентифікація абонента;
– таємність передачі даних;
– таємність напрямків з’єднання абонентів;
– таємність абонента.

В стандарті *CDMA* безпека зв’язку організується за допомогою кодування інформації. Код, що використовується, перетворює первинну комбінацію у шумоподібний широкосмуговий сигнал (ШПС) так, що його можна виділити знову, тільки маючи відповідний код на приймальній стороні. При цьому одночасно в широкій смузі частот можна передавати і приймати безліч сигналів, які не заважають один одному. Властивість цифрового зв’язку із шумоподібними сигналами – захищеність каналу зв’язку від перехоплення, перешкод і підслуховування. Саме тому дана технологія була розроблена і використовувалася для збройних сил США.

В стандарті *DECT* передбачено ряд функцій захисту, включаючи шифрування радіосигналу й ідентифікації портативних пристроїв зв’язку. Система ідентифікації пристроїв *DECT* дозволяє одному пристроєві зв’язку здійснювати доступ до декількох різних систем (наприклад, до базової станції звичайного домашнього телефону і до системи загального користування), а також одній базової станції забезпечувати доступ до різних систем зв’язку. При подібній організації кілька служб можуть спільно використовувати ту саму інфраструктуру зв’язку, що досить привабливо з економічної точки зору.

Розглянувши всі стандарти мобільного зв’язку та їх методи забезпечення безпеки зв’язку можна виділити один основний недолік – ні один з проаналізованих стандартів не дає 100 % безпеки зв’язку, оскільки не відбувається ідентифікація та аутентифікація базової станції, а лише самого абонента.

Таким чином на даний час використання мобільного зв’язку як засобу передачі конфіденційної інформації не є доцільним.

ЛІТЕРАТУРА

1. *Урядников Ф.Ю.* Надширокосмуговий зв’язок. Теорія і застосування / Ф.Ю. Урядников С.С. Аджемов.– М.: СОЛОН-Прес, 2005. – 368 с. (Серія „Бібліотека студента”).

2. *В.П. Іпатов, В.К. Орлів, І.М. Самойлов, В.Н. Смирнов*; під ред. В.П. Іпатова. Системи мобільного зв’язку: навчальний посібник для вузів – М.: Гаряча лінія Телеком, 2003.– 272 с.

3. *В.В. Крухмальов, Н.В. Гордієнко, А.Д. Моченов і ін.*; під. ред. В.Н. Гордієнко і В.В. – Крухмальова. Основи побудови телекомунікаційних систем і мереж: підручник для вузів – М.: Гаряча лінія Телеком, 2004. – 510 с.: мул.

4. http://www.alarm-gsm.ru.

5. http://www.edgemodem.ru.

к.т.н. Горбенко В.І. (ВІТІ НТТУ „КПІ”)
Заремський М.Й. (в/ч А1906)
Нищук А.М. (в/ч А1906)

МЕТОДИКА ВИБОРУ ФУНКЦІОНАЛЬНО ПОВНОГО НАБОРУ ЕЛЕМЕНТІВ ДЛЯ СИНТЕЗУ АВТОМАТИЗОВАНИХ КОМПЛЕКСІВ РАДІОМОНІТОРИНГУ

Автоматизований комплекс радіомоніторингу – складна дискретна система, яка вирішує функціональну задачу прийому, зберігання і обробки дискретних сигналів. Аналіз функціональної задачі показує, що не всі алгоритми чи їх фрагменти доцільно виконувати програмно. В процесі функціонування автоматизованого комплексу виникають пікові за продуктивністю інтервали. Тоді окремі фрагменти чи алгоритми в цілому потрібно реалізовувати апаратно.

Функціонально повними наборами елементів для апаратної реалізації (синтезу) є набори, які реалізують кон’юнкцію, диз’юнкцію, інверсію і включають запам’ятовуючі елементи, наприклад, тригери чи регістри зсуву. Найбільш сучасними функціонально повними наборами елементів є набори, які фізично реалізовані у чипах програмованих логічних інтегральних схем з вбудованою пам’яттю. Відкритими для спеціальних застосувань таких наборів є питання визначення їх потужності, тобто кількості різних типів логічних і запам’ятовуючих елементів, достатніх їх параметрів та програмування цих наборів.

У доповіді розглядається методика вибору функціонально повного набору елементів для синтезу автоматизованих комплексів радіомоніторингу заснована на блочному методі структурного синтезу академіка В.М.Глушкова, яка дозволяє встановити потужність і параметри такого набору.

В якості вихідних даних методики вибору функціонально повного набору елементів для синтезу автоматизованих комплексів радіомоніторингу пропонується використовувати часові та частотні характеристики алгоритмів та вимоги до автоматизованого комплексу.

Суть методики у визначенні чипів програмованих логічних інтегральних схем з вбудованою пам’яттю для реалізації блоків в залежності від часових та частотних характеристик алгоритмів вирішення функціональної задачі. До складу функціонально повного набору елементів на базі програмованих логічних інтегральних схем, виходячи з часових та частотних характеристик алгоритмів вирішення функціональної задачі, вимог до основних характеристик автоматизованого комплексу, повинні входити логічні та запам’ятовуючі елементи з часом затримки $t_з = 2 – 5$нс та вбудована пам’ять (оперативна та типу „флеш”) ємністю до 1 Мб. Це дозволить синтезувати комбінаційні схеми та схеми з пам’яттю (регістри, лічильники, суматори, демодулятори, декодери, контролери, пристрої управління, спеціалізовані пристрої обробки цифрових сигналів та інші) автоматизованого комплексу радіомоніторингу.

Наводиться алгоритм методики, який враховує часові та частотні характеристики алгоритмів вирішення функціональної задачі радіомоніторингу.

Таким чином, пропонується методика вибору функціонально повного набору елементів для синтезу автоматизованих комплексів радіомоніторингу з використанням програмованих логічних інтегральних схем із вбудованою пам’яттю, яка дозволяє встановити потужність і параметри такого набору та розглядається приклад практичного застосування методики.

ЛІТЕРАТУРА

1. *Вавилов Е.Н.* Синтез схем электронных цифровых машин. / Е.Н. Вавилов, Г.П. Портной. – М.: Сов. радио , 1963. – 440 с.

2. *Рембовский А.М.* Радиомониторинг: задачи, методы, средства. / А.М. Рембовский – СПб.: Горячая линия – телеком, 2006. – 492 с.

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

ПРОЦЕДУРИ КОНТРОЛЮ І УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ МЕРЕЖАМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

На сучасному етапі розвитку інформаційних технологій широкого застосування набрали інформаційні мережі.

Управління інформаційною мережею – це виконання функцій контролю, планування, виділення, впровадження, координування та моніторингу ресурсів мережі.

Міжнародна організація по стандартизації *ITU* в стандарті *M.3400* описала *FCAPS* модель, в якій зображені ключові функції адміністрування і управління мережами:

1. керування відмовами – виявлення, визначення й усунення наслідків збоїв і відмов у роботі мережі;
2. керування конфігурацією – полягає в конфігуруванні компонентів мережі, включаючи їх місце розташування, мережні адреси й ідентифікатори, керування параметрами мережних операційних систем, підтримка схеми мережі;
3. облік роботи мережі включає реєстрацію й керування ресурсами та обладнанням, що використовуються. Ця функція оперує такими поняттями – час використання й плата за ресурси;
4. керування продуктивністю служить для збору і надання статистики роботи мережі в реальному часі, мінімізації моментів перевантаження і вузьких місць мережі, виявлення складних тенденцій і планування ресурсів для майбутніх потреб ;
5. керування безпекою містить у собі контроль доступу, збереження цілісності даних і протоколювання подій. Функція містить процедури аутентифікації, перевірки привілеїв, підтримки ключів шифрування, керування повноваженнями. До цієї ж групи можна віднести важливі механізми надання та зберігання паролів, управління зовнішнім доступом, з’єднання з іншими мережами.

Функції реалізовані певним набором процедур.

У доповіді проведено аналіз та зроблено висновок, що на даному етапі розвитку інформаційної мережі ЗСУ в її склад відсутня жодна автоматизована підсистема контролю і управління мережею. Управління мережею здійснюється в ручному режимі, що викликає вплив людського фактора на саму мережу і призводить до приховування реального стану мережі від керівних органів. Були окремі спроби вбудувати підсистему контролю та управління в мережі, однак ці намагання не привели до бажаного результату з причин відсутності процедур контролю і управління інформаційною мережею.

На процедури контролю і управління в мережі ЗСУ накладаються додаткові вимоги. Так, наприклад, в сучасному стані економіки країни та недостатності коштів затрати на реалізацію цих процедур повинні бути мінімізовані. Цей факт аргументує застосування процедур контролю і управління з відкритим кодом. Ще одним аргументом за цей вид процедур є те, що жодна реалізація процедур не може задовольнити в повному обсязі вимоги інформаційних мереж спеціального призначення.

Таким чином нами проаналізовані розробки в сфері контролю і управління інформаційними мережами на основі програмних комплексів *Zabbix, Nagios, Zennos* і запропоновані механізми удосконалення рішень систем моніторингу і управління на базі процедур контролю і управління інформаційних мереж спеціального призначення.

ЛІТЕРАТУРА

1. *ITU-T* Recommendation M.3400: TMN management functions. - approved on 4 February 2000. Available from: <http://www.itu.int/rec/T-REC-M.3400/en>.
2. *Ed Wilson* Network monitoring and analysis. A protocol Approach to Troubleshooting, 2002. – 364 с.

к.т.н Горбенко В.І. (ВІТІ НТУУ „КПІ”)
Матковський Р.М. (ВІТІ НТУУ „КПІ”)

ЕЛЕМЕНТИ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В МОДУЛІ КОНТРОЛЬНОГО ОПИТУВАННЯ

Вищі військові навчальні заклади як і інші освітні установи України ведуть підготовку фахівців з використанням Болонської системи оцінювання і підготовки студентів.

Болонський процес передбачає як новий рівень підготовки курсантів (студентів) до занять так і новий спосіб оцінки знань навчаємих.

Впровадження Болонської системи викликає необхідність переходу від старої системи оцінки знань (5-ти бальної системи) до іншої – рейтингової. В основі цієї системи лежать кредитні модулі які кількісно характеризуються балами.

Для полегшення перевірки знань навчаємих і оцінки рівня їх знань створюються автоматизовані системи рейтингового оцінювання. Дані системи полегшують роботу викладача.

У доповіді розглядається підвищення безпеки автоматизованої рейтингової системи оцінки знань шляхом розробки і впровадження елементів захисту конфіденційної інформації. Захист конфіденційної інформації полягає як у розмежуванні доступу до неї так і у забезпечені її цілісності. [1]

До конфіденційної інформації, яка використовується у модулі контрольного опитування відносяться:

1. Відповіді до варіантів.
2. Індивідуальні бальні рейтинги навчаємих.
3. Процедури генерації варіантів контрольного опитування.

Досягнення мети здійснюється шляхом вирішення наступних задач:

– аналіз існуючих елементів захисту;
– вибір методів побудови елементів захисту;
– розробка блоку шифрування/дешифрування по паролю;
– програмна реалізація елементів захисту орієнтованих на рейтингову систему.

Об’єктом дослідження є процеси та алгоритми забезпечення безпеки інформації за допомогою комп’ютерних засобів. З урахуванням функціонального призначення системи контролю знань виділяємо наступні елементи системи:

1. Тестовий, до складу якого входять: база тестів і тестових завдань; блок перевірки ефективності тестів; блок аналізу показників ефективності тестів і корекції тестових завдань; редактор тестів.

2. Організації контролю знань, до складу якої входять: блок організації тестування; база результатів тестування.

Для забезпечення повного захисту конфіденційної інформації даного контрольного модулю захист повинен бути присутнім у всіх його елементах:

– тестовій – для забезпечення конфіденційності тестових варіантів, відповідей і унеможливить надання можливості редагування, видалення, додавання тестових завдань особам які не мають відповідних прав користувача.

– підсистеми організації контролю знань – для забезпечення зберігання результатів тестування у конфіденційності і унеможливлення їх підробки.

Таким чином для забезпечення адекватного оцінювання студентів (курсантів), безперебійну роботу модуля контрольного опитування потрібно в свою чергу забезпечити повний захист конфіденційної інформації.

ЛІТЕРАТУРА

1. Домарев В.В.. Защита информации и безопасность компьютерных систем. Эффективные методы и средства. – К.: видавництво „ДиаСофт”,1999. – 480 с.

к.т.н. Горбенко В.І. (ВІТІ НТУ „КПІ”)
к.т.н. Ніколаєв С.М. (в/ч А1906)
Ратанін Є.Г. (в/ч А1906)

МЕТОДИКА ВИЗНАЧЕННЯ ПРОТОКОЛІВ ПЕРЕДАЧІ ДАНИХ АВТОМАТИЗОВАНИМ КОМПЛЕКСОМ

Розвиток сучасних систем телекомунікацій відзначається появою нових та модернізацією існуючих систем зв’язку, які характеризуються впровадженням більш ефективних видів сигналів та протоколів обміну даними. Тому актуальними є прийом, обробка і зберігання інформації автоматизованим комплексом з мінімальною участю оператора при забезпеченні сумісності з вже наявними абонентськими засобами шляхом підтримки раніше використовуваних протоколів передачі даних.

Аналіз вітчизняних та зарубіжних науково-технічних джерел показує, що більшість існуючих методик визначення протоколів передач даних базуються на обчисленні автокореляційної функції періодичних двійкових послідовностей (бітових потоків) з метою визначення їхніх характерних особливостей.

Періодичність двійкових послідовностей проявляється в максимумах автокореляційної функції, які при вирішенні задачі визначення протоколів передачі даних, необхідно відрізнити від випадкових піків. Ця процедура потребує обчислення автокореляційної функції для великого обсягу двійкової послідовності (бітового потоку) і не дозволяє розрізнити протоколи передач, які мають однаковий період слідування.

У доповіді пропонується методика визначення протоколів передачі даних автоматизованим комплексом, яка дає змогу визначати протоколи передач і розпізнавати знакову синхронізацію на основі запропонованого вирішального правила та статистичної обробки.

В якості вихідних даних методики використовується двійкова послідовність (бітовий потік). Суть методики полягає у використанні вирішального правила для визначення знакової синхронізації і встановлення періоду, початку і кінця передачі на базі обробки набраної статистики. Результатом роботи методики є номер шаблону передачі, протокол передачі і позиція знакової синхронізації. Дана методика дозволяє визначати як існуючі з переліку протоколи так і сучасні, а також додатково розпізнавати позицію знакової синхронізації. Оцінка ефективності запропонованої методики була проведена на розробленій програмній моделі. У якості прототипу для порівняння була використана методика визначення протоколу за допомогою автокореляційної функції.

Таким чином, запропонована методика визначення протоколів передачі даних автоматизованим комплексом дозволяє підвищити ефективність роботи апаратури прийому-передачі даних автоматизованого комплексу радіомоніторингу та дає змогу автоматизувати роботу оператора у процесі вирішення функціональної задачі радіомоніторингу.

ЛІТЕРАТУРА

1. *Глазнев А.А.* Многостанционные системы радиоконтроля и определения местоположения источников радиоизлучения. / А.А. Глазнев, В.А. Козьмин, Г.В. Литвинов, И.А. Шадрин. – Спец. техника. Специальный выпуск. – М.: 2002. С.20 – 29.

2. *Рембовский А.М.* Радиомониторинг: задачи, методы, средства. / А.М. Рембовский– СПб.: Горячая линия – телеком, 2006. – 492 с.

3. *Р. Морелос-Сарагоса*. Исскуство помехоустойчивого кодирования. Методы, алгоритмы, применение. / Р. Морелос-Сарагоса. – М.: Техносфера, 2005. – 320 с.

4. *MIL* STD-188-110B. Interoperability and performance standards for data modems. – Department of defense USA, 2001. – 999 – 136 p.

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

ОЦІНКА НАДМІРНОСТІ ПРЕДСТАВЛЕННЯ ІНФОРМАЦІЇ ТЕКСТОВИХ ДОКУМЕНТІВ В ТЕХНІЧНИХ ЗАСОБАХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКАМИ

Удосконалювання керування військами і розвиток автоматизованих систем управління військами (АСУВ) супроводжується стійкою тенденцією збільшення обсягів циркулюючої та що зберігається інформації. З іншого боку, удосконалювання сучасного керування військами постійно вимагає зменшення часу на її збір, обробку і передачу в системах керування. Рішення цього протиріччя традиційно лежить у створенні нових більш досконалих технічних засобів АСУВ (комп'ютерів, засобів комунікації та інших).

Другий підхід удосконалювання інформаційного процесу в АСУВ підказується теорією інформації і полягає в збільшенні інформаційного навантаження на технічні засоби. Резерв для збільшення інформаційної ємності технічних пристроїв мається в самих даних як формалізованому представленні інформації: як показує досвід з точки зору інформація в технічних пристроях АСУ інформація кодується с надмірністю. Проблему усуненні цієї надмірності визначають як проблему стиску даних. Стиском даних прийнято називати процедуру перетворення послідовностей даних у більш короткі за рахунок усунення (скорочення) надмірності у вихідних послідовностях. При цьому мається на увазі обов'язкове існування зворотної процедури – процедури відновлення оригінальних вихідних послідовностей зі стиснутих. Природа надмірності даних в технічних засобах обчислювальної техніки пов'язана з дискретністю технічних пристроїв, надмірністю семіотичної системи подання інформації й з недосконалістю проектування структур даних.Дослідження подання інформації в ЕОМ штабів дозволяють виділити чотири види надмірності даних.

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

2. Ергодична надмірність. Пов'язана з кодуванням послідовних символів без обліку їхніх ергодичних властивостей.

3. Надмірність використання потужності коду ЕОМ.

4. Надмірність ланцюжків ідентичних символів.

Розробка методики кількісної оцінки цих видів надмірності дозволила досліджувати надмірність даних різних документах штабів в технічних пристроях ЕОМ. Була досліджена надмірність документів КШН по управлінню військами, звітні, довідкові. Результати показують, що в теоретично надмірність цих видив в відсотках становить: статистична надмірність – 4– 43 %; ергодична надмірність – 11 – 13%; надмірність використання потужності коду ЕОМ – 25 %; надмірність ланцюжків ідентичних символів – 5 – 8%. Скорочення надмірності даних – шлях підвищення інформаційної ємності технічних пристроїв АСУ за рахунок стиску даних. Для впровадження стиску даних в АСУВ необхідні ефективні методи СД, яки можуть бути реалізовані як програмно, так и апаратно технічними пристроями. В свою чергу, ефективність методів СД пов'язано з їх спрямованістю на усунення конкретні види надмірності.

Таким чином, результати кількісної оцінки надмірності показують на великий невикористаний резерв для компактного представлення текстових документів в обчислювальних системах: технічні пристрої в сучасний час зберігають у два з гаком рази меншу кількість інформації, чим вони могли б зберігати і передавати теоретично. Орієнтуючись на усунення конкретних видив надмірності, можуть бути розроблені ефективні методи стиску даних, що дозволять скорочувати обсяги текстових документів у технічних пристроях до 50 відсотків. Цим самим можливо збільшити швидкість передачі даних по каналах зв'язку, а також компактне збереження даних у базах даних.

Грабовський О.В. (ВІТІ НТУУ “КПІ”)
к.т.н. Любарський С.В. (ВІТІ НТУУ “КПІ”)

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМ ПЕРЕВІРКИ ЗНАНЬ

Важливим аспектом педагогічної діяльності являється оцінка викладачем знань навчаємих. З поміж існуючих систем перевірки знань варто виділити комп’ютерні, окільки вони характеризуються більшою рентабельністю та меншою, в порівнянні з традиційними формами, ціною освітніх послуг. А також проведення контролю знань у традиційній формі вимагає забагато аудиторного часу, якого сьогодні не вистачає у викладачів вузів, тому виникає необхідність в нових формах контролю та модифікації вже відомих. До однієї з таких форм контролю можна віднести перевірку знань з використанням комп’ютерних систем.

Окрім того звичайні комп’ютерні системи оцінки знань мають деякі недоліки, адже жодна зазделегіть підготовлена програмна система оцінки знань не може в точності відповідати рівню підготовленості конкретних навчаємих. Вони всі різні і тому, для ефективного оцінення необхідні програмні системи різного рівня складності. Ось чому в сучасних програмних системах оцінки знань моделюються адаптивні алгоритми, завдання яких підбирати складність системи до рівня підготовленості кожного навчаємого.

Одним із ключових моментів діагностики знань є не лише необхідність в оцінці знань навчаємих а ще й аналіз якості діагностичних матеріалів, що необхідно для адекватної оцінки знань.

Під якістю програмної системи оцінки знань розуміється сукупність властивостей, що визначають відповідність даної системи до її функціонального призначення та вимог, які до неї висуваються. До показників ефективності програмної системи оцінки знань варто віднести ті, які вказують на те чи задовольняє дана система вирішення функціональних завдань, її вартість розробки та використання, надійність та легкість експлуатації.

У визначенні ефективності програмної системи оцінки знань звертається увага на два ключові елементи – це число завдань в системі і рівень підготовленості студентів. Якщо з якої-небудь системи з великим числом завдань зробити оптимальний вибір меншого числа, то може утворитися система, яка не буде поступатися за своїми властивостями попередній. Систему з меншим числом завдань, у такому разі, можна назвати порівняно ефективнішою.

Окрім цього, ефективність системи можна оцінити, враховуючи відповідність рівня її складності до рівня підготовленості оцінюваних в даний момент

Ефективність системи також оцінюється з точки зору її диференціюючої здатності, яка тим вища, чим краще видні відмінності між визначеними балами навчаємих. Як один з можливих показників диференціюючої здатності можна використовувати дисперсію. Відношення більшої дисперсії до меншої при однаковому числі завдань з наступним множенням на сто може служити як один з показників ефективності системи з позиції його диференціюючої здатності.

Окрім того ефективний система не може складатися з неефективних завдань. З точки зору змісту ефективне завдання перевіряє важливий елемент змісту учбової дисципліни.

Отже, враховуючи усі вказані показники ефективності, пропонується така послідовність перевірки програмної системи оцінки знань:

– кількісний вимір показників оцінюваної системи;

– вимір ресурсів затрачених на впровадження системи;

– вимір ресурсів, що витрачаються на використання системи;

– порівняння скорочення витрат та економія, що досягається з іншою системою.

к.т.н. Грабчак В.І. (АСВ)
Грабчак З.М. (АСВ)

ОЦІНКА СКЛАДНОСТІ ФОРМУВАННЯ ТА ДЕКОДУВАННЯ КОДОГРАМ В УЗАГАЛЬНЕНИХ КАСКАДНИХ КОДАХ З АЛГЕБРОГЕОМЕТРИЧНИМИ КОДАМИ НА ЗОВНІШНІЙ СТУПЕНІ

В зв'язку зі збільшенням вимог до ефективності процесів управління, постійним зростанням об'єму і швидкості інформації, що передається (дискретних повідомлень), суттєво зросли вимоги і до вірогідності інформації, що передається (ймовірність помилки не вище $10^{-6} \div 10^{-9}$). Розробка та реалізація у вітчизняному виробництві методів і технічних засобів підвищення вірогідності інформації, що передається, є одним з першочергових напрямків Концепції розвитку зв'язку в Україні. Сферою реалізації методів і технічних засобів підвищення вірогідності інформації, що передається, є телекомунікаційні підсистеми Державної інтегрованої інформаційної системи, підсистеми зв'язку воєнного й урядового призначення, телекомунікаційні системи спеціального призначення.

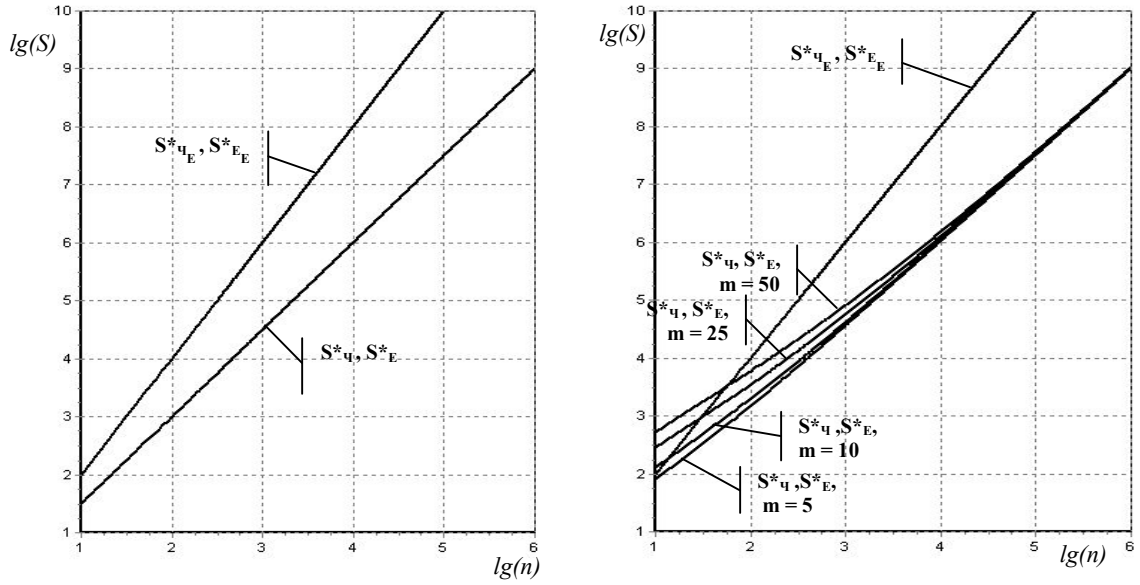
Одним із найбільш ефективних методів підвищення вірогідності інформації, що передається, є завадостійке кодування [1, 2]. При підвищених вимогах до вірогідності і низькому енергетичному відношенні сигнал/завада, наприклад, у системах мобільного і супутникового зв'язку, доцільно застосування каскадних кодів для зменшення складності реалізації декодерів [2, 3]. Відмінною особливістю каскадних схем кодування є кодування (декодування) інформації декількома складовими кодерами (декодерами).

Найбільш розповсюдженою схемою побудови каскадних кодів є схема з двома рівнями кодування. В якості зовнішнього коду, як правило, використовуються коди Ріда-Соломона. Ці коди найбільш широко розповсюджені, оскільки є кодами з максимально досяжною відстанню і відносно просто реалізуються. В якості внутрішнього коду можна вибрати один з багатьох різних кодів [2, 3].

Загальним класом каскадних кодів, які мають більш двох рівнів кодування, є узагальнені каскадні коди. Алгебраїчній теорії побудови узагальнених каскадних кодів, дослідженню складності їх реалізації присвячена монографія [4]. Узагальнені каскадні коди є однією з найбільш загальних схем каскадного кодування і є, в теоретичному плані, узагальненням більшості відомих каскадних кодових конструкцій (ітеріровані коди, каскадні коди і коди для локалізації помилок). Найбільший ефект каскадне кодування дозволяє одержати при використанні на зовнішній ступені алгеброгеометричних кодів [5, 6, 7]. В роботі [8] показано, що теорія їх побудови узагальнює більшість відомих алгебраїчних кодів, таких, наприклад, як великий клас циклічних кодів, у тому числі кодів Боуза-Чоудхурі-Хоквінгема, кодів Ріда-Соломона і їх узагальнень, альтернантних кодів, у тому числі кодів Гоппи, Сривестави та інших. Основна перевага методів алгеброгеометричного кодування полягає у побудові довгих недвійкових блокових кодів, які мають добрі асимптотичні властивості. У роботі [9] показано, що використання алгеброгеометричних кодів для передачі даних по дискретних каналах зв'язку дозволяє отримати суттєвий енергетичний виграш від кодування. Основним недоліком застосування алгеброгеометричних кодів є висока складність кодування і декодування кодограм. Для зменшення складності кодування і декодування кодограм пропонується використовувати узагальнені каскадні коди як метод практичної реалізації коду з великою довжиною і високою корегуючою здібністю.

Авторами проведені дослідження формування та декодування кодограм з використанням алгеброгеометричних кодів на зовнішньому каскаді узагальненого каскадного коду. Для оцінки часової та ємкісної складності алгоритмів формування кодового слова узагальненого каскадного коду сформульовані і доведені теореми, які визначають ємкісну і часову, та відповідно асимптотичу ємкісну і асимптотичу часову складності алгоритмів формування та декодування кодограм.

Проведений порівняльний аналіз часової і ємкісної складності реалізації алгоритмів формування кодограм в узагальнених каскадних кодах з алгеброгеометричними кодами на зовнішній ступені та еквівалентного двійкового лінійного блокового коду показав, що їх реалізація для коротких кодограм (декілька сотень біт) значно (на один - два порядки) простіша порівняно із традиційними кодовими конструкціями (рис.1).



а) формування кодограм б) декодування кодограм

Рис. 1. Залежності асимптотичної складності реалізації алгоритмів узагальненого каскадного коду

S^*_E, $S^*_ч$ – відповідно асимптотична ємкісна та часова складність реалізації алгоритмів узагальненого каскадного коду; $S^*_{ч_E}$, $S^*_{E_E}$ – відповідно асимптотична ємкісна та часова складність реалізації алгоритмів еквівалентного двійкового лінійного блокового коду; m – порядок узагальненого каскадного коду, n – довжина коду

Крім того, зростання цих складностей у межі при збільшенні розміру задачі (асимптотична складність) суттєво нижче, ніж у випадку використання традиційних кодових схем обробки інформації. Показано, що складність реалізації алгоритмів, що пропонуються зростає поліноміально від параметрів кодів, що використовуються.

При зміні порядку узагальненого каскадного коду складність реалізації алгоритмів декодування змінюється слабо, що практично не впливає на кінцевий вибір параметрів узагальненого каскадного коду.

ЛІТЕРАТУРА

1. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.

2. *Злотник Б. М.* Помехоустойчивые коды в системах святи / Б. М. Злотник. – М.: Радио и связь, 1989. – 232 с.

3. *Бернард Скляр*. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

4. *Блох Э.Л.,* Зяблов В.В. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. – М.: Связь, 1976. – 240 с.

5. *Гоппа В.Д.* Коды на алгебраических кривых. Докл. АН СССР / В.Д. Гоппа. – 1981. – Т.259, № 6. – С. 1289 – 1290.

6. *Гоппа В.Д.* Коды и информация. Успехи математических наук / В.Д. Гоппа. – 1984. –Т.30, вып. 1(235). – С. 77 – 120.

7. *Грабчак В.І.* Синтез каскадних кодів з алгеброгеометричними кодами на зовнішній ступені / В.І. Грабчак // Військово-технічний збірник. – Львів: ЛІСВ. – 2009. – Вип. 2. – С. 3 – 8.

8. *Науменко М.І.* Теоретичні основи та методи побудови алгебраїчних блокових кодів. Монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов. – Харків: ХУ ПС, 2005. – 267 с.

9. *Кузнецов А.А.* Энергетический выигрыш алгеброгеометрического кодирования / А.А. Кузнецов // Всеукр. меж вед. науч.-техн. сб. – Харьков: ХТУРЭ. – 2003. – Вып.134. – С. 218 – 222.

к.т.н. Грабчак В.І. (АСВ)
к.т.н. Пасько І.В. (Сумський державний університет)
Грабчак З.М. (АСВ)

КОДОВІ СХЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДОКАЗОВОЇ СТІЙКОСТІ НА ПРОСТОРОВИХ КРИВИХ

Перспективним напрямом у розвитку механізмів інтегрованого забезпечення достовірності і конфіденційності передачі повідомлень у системах передачі даних АСУВ є кодові схеми захисту інформації доказової стійкості [1 – 3]. Це криптографічні системи, побудова яких основана на маскуванні блокових алгебраїчних кодів зі швидкими алгоритмами декодування під випадковий код і зведенні задачі зламу криптографічної системи до теоретико-складної задачі декодування випадкового коду [3 – 6]. Їх практичне використання дозволяє реалізувати в одному пристрої методи канального кодування і спеціального перетворення даних.

Основна ідея, яка використовується при побудові кодових схем захисту інформації доказової стійкості, полягає у „маскуванні" алгебраїчних блокових кодів під коди загального положення (випадкові коди). У цих схемах для реалізації односторонньої функції спеціального перетворення даних використано важко вирішуване завдання декодування випадкового коду (коду загального положення).

На сьогоднішній день розглянуті приклади побудови кодових схем захисту інформації доказової стійкості Мак-Елліса та Нідеррайтера на основі кодів Боуза-Чоудхурі-Хоквінгема (БЧХ) і кодів Ріда-Соломона (підклас недвійкових кодів БЧХ). У [1] запропонований ефективний метод зламу схеми Мак-Елліса з кодом Ріда-Соломона.

Там же автором висувається припущення про потенційну вразливість схем, які побудовані на узагальнених кодах БЧХ. Крім того, процедури зламу схеми Мак-Елліса можуть бути легко трансформовані на схеми Нідеррайтера.

Стійкість кодових схем захисту інформації, побудованих на кодах Ріда-Соломона і кодах БЧХ, вважається недостатньою.

Одним із перспективних напрямів розвитку кодових схем захисту інформації доказової стійкості, спрямованих на підвищення стійкості, є використання алгеброгеометричних кодів [7]. Застосування кодів, побудованих по алгебраїчних кривих (алгеброгеометричних кодів) для формування кодових схем захисту інформації, дозволить отримати додатковий параметр маскування коду – вид алгебраїчної кривої [4], на основі якої будується перевірочна і породжувальна матриця коду.

Крім того, в роботі [8 – 9] показано, що використання алгеброгеометричних кодів для передачі повідомлень по дискретних каналах зв'язку дозволяє отримати значний енергетичний виграш від кодування.

Водночас проведені дослідження алгеброгеометричних кодів для плоских алгебраїчних кривих, заданих в проективному просторі P^2 однорідним незвідним рівнянням від трьох змінних.

Перспективним напрямом подальших досліджень для формування кодових схем захисту інформації доказової стійкості є використання алгеброгеометричних кодів на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних [10 – 11]. Застосування кодів, побудованих по просторових кривих, для формування кодової схеми дозволить отримати ще один додатковий параметр маскування коду – вид другої алгебраїчної кривої та підвищити енергетичний виграш від кодування [12].

Авторами розглянуті теоретичні питання побудови кодової схеми захисту інформації Мак-Елліса з використанням алгеброгеометричних кодів на просторових кривих, що задаються у проективному просторі P^3 сумісними рішеннями сукупності двох однорідних рівнянь від чотирьох змінних, розроблені практичні процедури їх формування та декодування, наведені алгоритми функціонування кодової схеми захисту інформації Мак-Елліса з алгеброгеометричними кодами на просторових кривих. Розглянутий практичний приклад реалізації процедур формування та декодування кодограм кодової схеми захисту інформації Мак-Елліса з алгеброгеометричними кодами на просторових кривих у вигляді послідовності кроків.

Показано, що варіюючи часткою виправляючої здатності коду, що доводиться на штучне внесення помилок – ρ, можна інтегровано (одним прийомом) забезпечити конфіденційність і достовірність передачі повідомлень – $0 > \rho > 1$, чи за умови $\rho = 0$ – режим забезпечення тільки достовірності (завадостійкого кодування), $\rho = 1$ – режим забезпечення тільки конфіденційності.

Перспективним напрямком подальших досліджень є визначення кількісних показників часової та ємкісної складності запропонованих процедур формування і декодування кодових схем захисту інформації Мак-Елліса з використання алгеброгеометричних кодів на просторових кривих.

ЛІТЕРАТУРА

1. *Сидельников В.М.* О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона / В.М. Сидельников, С.О. Шестаков // Дискретная математика. – 1992.– Т.4.№ 3.– С.57 – 63.

2. *Сидельников В.М.* Криптография и теория кодирования / В.М. Сидельников // Материалы конференции „Московский университет и развитие криптографии в России”. – М.: МГУ. – 2002. – 22 с.

3. *Онанченко Е.Л.* Исследование методов защиты информации, основанных на использовании алгебраических блоковых кодов / Е.Л. Онанченко, А.А. Кузнецов, В.Н.Лисенко, В.И. Грабчак, Р.В. Королев // Системи обробки інформації. – Харків: ХУ ПС. – 2007. – Вип. 7 (65). – С. 53 – 59.

4. *McEliece R.J. A* Public-Key Criptosystem Based on Algebraic Theory / R.J. McEliece // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, 1978. – P. 114 –116.

5. *Niederreiter H.*. Knapsack-Type Cryptosystems and Algebraic Coding Theory / H. Niederreiter // Probl. Control and Inform. Theorty. – 1986. –V.15. – P. 19 – 34.

6. *Rao T. R.* N. and Nam K. H. . Private-key algebraic-coded cryptosystem. Advances in Cryptology. / T. R. N. Rao, K. H. Nam // CRYPTO 86, New York. – NY: Springer. – PP. 35 – 48.

7. *Науменко М.І.* Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія / М.І. Науменко, Ю.В. Стасєв, О.О. Кузнецов. – Харків: ХУ ПС, 2005. – 267 с.

8. *Кузнецов А.А.* Энергетический выигрыш алгеброгеометрического кодирования / А.А. Кузнецов // Всеукр. меж вед. науч.-техн. сб. – Харків: ХТУРЭ, 2003. – Вып.134. – С. 218 – 222.

9. *Кузнецов А.А.* Энергетическая эффективность алгеброгеометрических кодов / А.А. Кузнецов // Электронное моделирование: Международный научно-теоретический журнал. – К: НАНУ, РАН, 2004. – №2. – С. 27 – 38.

10. *Ian Blake,* Chris Heegard, Tom Hoholdt, Victor K. W. Wei; Algebraic – Geometry Codes, IEEE Trans. Info. Theory. – October 1998.– vol. IT – 44.– PP. 2596 – 2618,

11. *Грабчак В.И.* Алгебраическое кодирование алгеброгеометрическими кодами на пространственных кривых / В.И. Грабчак, И.В. Пасько, Р.В. Королев, И.Е. Кужель // Системи обробки інформації. – Харків: ХУПС. – 2007. – Вип. 8 (66). – С.134 – 139.

12. *Кузнецов А.А.* Исследование помехоустойчивости передачи дискретных сообщений с использованием алгеброгеометрических кодов на пространственных кривых. / А.А. Кузнецов, В.И. Грабчак, И.В. Пасько // Системи управління, навігації та зв’язку. – К: ЦНДІНіУ. – 2007. – Вип. 3. – С.82 – 85.

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

ЙМОВІРНІСНИЙ ЗАХИСТ ВАГОМИХ РОЗРЯДІВ РІВНОМІРНИХ КОДІВ

Цифровий потік Е1 є базовим у формуванні потоків вищих ступенів ієрархії (Е2, Е3, Е4, …). Утворення Е1 стандартизовано рекомендаціями МСЕ-Т. Передача Е1 може здійснюватись по різних лініях зв’язку: кабельних, волоконно-оптичних, радіорелейних, супутникових, тропосферних. Рекомендаціями передбачається, що ймовірність помилок на одиничний елемент у цих лініях не повинна перевищувати $p \le 10^{-3}$, інакше апаратура переходить в аварійний режим функціонування з від’єднанням всіх каналів від абонентів.

Використання цифрових потоків Е1, Е2, … має тенденцію до розширення як у спеціалізованих системах, так і при побудові мереж загального використання. Для побудови польових варіантів цифрового зв’язку спеціалізованих структур доцільним є використання саме цифрового потоку Е1, який близький по канальній ємності до існуючих систем. Але при прогнозуванні використання таких систем зв’язку можливі варіанти ситуацій з погіршенням якісного стану ліній ($p > 10^{-3}$), зокрема, при радіоелектронному подавленні, що приведе до втрати зв’язків. Тому необхідна відповідна модернізація цифрової каналоутворюючої апаратури для роботи в таких умовах.

Першою реалізацією модернізації повинно бути підвищення границі аварійного стану до $p=10^{-2}$, а, можливо, і до $p=10^{-1}$ (що потребує додаткових досліджень). Для роботи в таких умовах повинен бути реалізований комплекс технічних заходів щодо підвищення вірогідності передачі цифрового потоку Е1. На лініях зв’язку високої якості ($p < 10^{-5}$) основним спотворювальним фактором у каналах ТЧ, яким відповідають основні цифрові канали (ОЦК) потоку Е1, є шуми квантування [1]. Вплив помилок у цифровому сигналі при таких умовах на спотворення сигналів незначний і він практично не враховується. Але із збільшенням ймовірності помилок p у цифровому сигналі кожного ОЦК вплив помилок стає зрівняним (за величиною дисперсії) із шумами квантування, а далі і значно інтенсивнішим.

Для кодування відліків (миттєвих значень) сигналів кожного ОЦК потоку Е1 (Європейський стандарт) використовується рівномірний симетричний код, в якому розряди мають різне вагове значення. Найбільший вплив на формування помилки декодування має другий розряд. Пропонується ймовірнісний захист цього розряду його трикратним повторенням в межах використовуваної кодової комбінації (у даному випадку із 8 елементів): він передається на стандартному місці та на місцях двох найменш вагомих розрядів (7-го і 8-го). При цьому дещо зростає шум квантування, але виграш за рахунок зменшення дисперсії помилок декодування компенсує це зростання і в цілому збільшує відношення сигнал/загальний шум.

На приймальній стороні реалізується мажоритарна обробка повторюваних розрядів за правилом більшості (два або три із трьох). Якщо ймовірність у каналі зв’язку p, то ймовірність помилкового прийому захищеного розряду $p_м$ визначається:

$$p_м = 3p^2(1-p)+p^3$$

Значення $p_м$ представлені у таблиці.

Таблиця

p	10^{-1}	10^{-2}	10^{-3}	10^{-4}
$p_м$	$2{,}8\cdot10^{-2}$	$2{,}98\cdot10^{-4}$	$2{,}998\cdot10^{-6}$	$3\cdot10^{-8}$

Як видно, при $p=10^{-2}$ отримуємо зниження ймовірності помилкового прийому захищеного розряду майже на два порядки.

Таким чином, при збільшенні ймовірностей помилок у цифровому потоці Е1 пропонується оригінальний алгоритм передачі та мажоритарна обробка найбільш вагомого розряду кодової комбінації кожного ОЦК, що збільшує відношення сигнал/сумарний шум.

ЛІТЕРАТУРА

1. *Джон К.* Беллами. Цифровая телефония: Пер. с англ. – М.: Эко-Трендз, 2004. – 640с.

Гупало А.Ю. (ЦНДІ ОВТ ЗС України)

ЕНЕРГЕТИЧНИЙ АНАЛІЗ СУКУПНОСТІ ЗАВАД В ЗОНІ ДІЇ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ПУНКТІВ УПРАВЛІННЯ ВІЙСЬКАМИ ТА ОЗБРОЄННЯМ

На теперішній час найбільш гостро виникає проблема ускладнення прийому сигналу різними радіоелектронними засобами (РЕЗ) пунктів управління (ПУ) військами та озброєнням в умовах дії сукупності завад, які характеризуються різними амплітудами, що перевищують у декілька порядків амплітуду сигналів, та терміном дії, що змінюється від наносекунд до декількох хвилин, часів, діб, місяців. При цьому проблема погіршується необхідністю враховувати взаємодію всіх РЕЗ між собою. Якщо розглянути всі фактори, що діють в зоні РЕЗ, то умови прийому сигналу можна характеризувати за допомогою енергетичного аналізу сукупності завад за їх амплітудою та довжиною наступним чином: вплив завади, коли є функціональне ураження РЕЗ, тобто її дія повністю припиняє роботу РЕЗ (завада типу ЕМІ від зброї електромагнітного імпульсу (ЕМІ) або окремих видів радіочастотної зброї, які створюють надпотужне електромагнітне поле, діє короткочасно, але з великою амплітудою, яка значно перевищує амплітуду сигналу) [1]; прийом сигналу, коли є тимчасове припинення роботу РЕЗ, тобто завада на деякий час припиняє прийом сигналу РЕЗ без його ураження (завада по типу прицільної активної завади (АЗ) діє більш триваліше ніж ЕМІ, але амплітуда її незначно перевищує амплітуду сигналу); прийом сигналу, коли є довгострокове погіршення роботи РЕЗ без його ураження, тобто завада на довгий час погіршує прийом сигналу РЕЗ (завада по типу інтермодуляційних перетворювань сигналу, що мають невелику амплітуду, але тривають значний період часу, тобто постійно [2].

Дані тези присвячені оцінці електромагнітної обстановки в зоні дії РЕЗ різного призначення за допомогою енергетичного аналізу дії сукупності завад. Вирішення задачі прийому сигналу плюс завада в РЕЗ за умовами дії сукупності завад дозволить контролювати прийом сигналу при функціонуванні РЕЗ ПУ.

Мета – визначення умов можливості енергетичного аналізу сукупності завад різної амплітуди та довжини в зоні дії РЕЗ різного призначення з ціллю контролю сигналу плюс завада в приймачах РЕЗ, для забезпечення інформаційної надійності систем РЕЗ.

Метод вирішення. Застосовуючи теорію математичного моделювання умов прийому сигналів РЕЗ (в радіолокації, радіонавігації, радіозв'язку) [2], визначаються межи амплітуд завад та довжини їх дії, з урахуванням амплітуд спектральної щільності потоку потужності за умовами існування вектору Умова-Пойнтинга та векторів напруженості електричних $\mathbf{E}_{max}$ і магнітних $\mathbf{H}_{max}$ полів в точці прийому з урахуванням хвильового опору вільного середовища для завади та сигналу одночасно.

Отримані результати. Підтверджено, що найбільш принциповим і важливим питанням можливості проведення енергетичного аналізу сукупності завад в зоні дії РЕЗ різного призначення є оцінка прийому сигналу плюс завада в приймачах РЕЗ за допомогою контролю амплітуд завад з перерахуванням характеристик електромагнітного поля завади з урахуванням характеристик антенно-фідерних трактів та преселекторів приймачів РЕЗ. Потужність сигналу плюс завада на виході антени знаходиться за умови узгодження розкриву антени та вільного середовища для РЕЗ різного призначення.

Реалізація такого енергетичного аналізу пов`язана з подоланням значних труднощів математичного та обчислювального характеру.

ЛІТЕРАТУРА:

1. Нетрадиційна зброя: Стан і основні тенденції розвитку. Захист від неї/За ред. О.П. Ковтуненка. – Київ: ЦНДІ ОВТ СЗ України, 2004, 220 с.

2. Радиотехнические системы: Учеб.для вузов по спец. „Радиотехника"/Ю.П. Гришин, В.П. Ипатов и др.; Под ред. Ю.М. Казаринова. – М.: Высшая школа, 1990.– 496 с.

к.т.н. Гурський Т. Г. (ВІТІ НТУУ „КПІ”)
к.т.н. Борисов І. В. (ВІТІ НТУУ „КПІ”)
Коротков В. С. (ВІТІ НТУУ „КПІ”)

ШЛЯХИ ПІДВИЩЕННЯ ПРИХОВАНОСТІ В СИСТЕМАХ РАДІОЗВ’ЯЗКУ З OFDM

В сучасних системах радіозв’язку (СРЗ) широко використовується один із методів формування широкосмугових сигналів – метод ортогонального частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). Основними перевагами даної технології є висока стійкість щодо частотно-селективних завмирань та висока спектральна ефективність.

Технологія OFDM знайшла широке застосування в стандартах IEEE 802.11, 802.16, Hiper LAN 2 [1, 2].

Суттєвим недоліком, що обмежує застосування ортогональної частотної модуляції у системах радіозв’язку спеціального призначення є нестійка робота в умовах впливу навмисних завад. Спектральна щільність потужності найпростіших шумових завад, навіть зосереджених по спектру, на прийомі після прямого перетворення Фур’є розмивається практично по всіх частотних підканалах, що або ускладнює, або й зовсім унеможливлює прийом OFDM-сигналу.

Як відомо завадозахищеність системи передачі визначається двома факторами – прихованістю і завадостійкістю. Доповідь присвячена вирішенню задачі підвищення прихованості передачі OFDM-сигналу. Під прихованістю системи передачі розуміють її здатність протистояти дії радіорозвідки [3]. Розрізняють енергетичну, структурну та інформаційну прихованість.

Для забезпечення інформаційної прихованості, спрямованої на утруднення несанкціонованого доступу до інформаційного змісту повідомлення, використовується засекречування (шифрування) повідомлень.

Основні методи підвищення енергетичної і структурної прихованості системи передачі:

1) робота з мінімально необхідною потужністю випромінювання, достатньою для забезпечення заданої якості зв’язку;

2) застосування оптимальних способів прийому сигналів;

3) застосування широкосмугових складних сигналів з великою базою.

Однією з головних проблем, пов’язаних з використанням OFDM-сигналів, є високий пік-фактор, що призводить до зниження прихованості. Виділяють чотири основних напрямки вирішення даної проблеми [1]. Перший та найпростіший – використання фазової маніпуляції сигналів у підканалах (двійкової фазової та квадратурної фазової маніпуляції). Недоліком його є невисока пропускна спроможність у порівнянні з використанням багатопозиційної квадратурної амплітудної маніпуляції.

Другий – амплітудне обмеження сигналу, що дозволяє суттєво знизити величину пік-фактора. Але при цьому виникають неконтрольовані спотворення сигналу, що призводить до погіршення якості зв’язку та зростання рівня позасмугового випромінювання. Виправляють ці недоліки за допомогою додаткової фільтрації, яка у свою чергу, знову призводить до збільшення пік-фактора.

Третім напрямком є додаткове кодування та введення надлишкових несучих, корекція параметрів яких дозволяє зменшити значення пік-фактора. При цьому погіршується спектральна ефективність, оскільки суттєве зменшення пік-фактора спостерігається тільки при швидкості кодування 1/2, тобто половина несучих частот використовується для корекції.

Четвертий напрямок – використання додаткових ортогональних (або неортогональних) перетворень, а також використання замість Фур’є-базису інших ортогональних базисів (Hadamard basis, wavelet-basis та ін.).

Недоліком підходів 2-4 є спотворення структури OFDM-сигналу, що призводить до того, що сигнал стає неінваріантним по відношенню до циклічних зсувів, тобто чутливим до багатопроменевості каналу.

Дослідження показують, що проблема зменшення пік-фактора повинна вирішуватись комплексно, з урахуванням характеристик якості та рівня позасмугового випромінювання [1].

Окремо виділимо напрямок підвищення прихованості OFDM-сигналу за допомогою його розширення псевдовипадковими послідовностями (ПВП), адже спектральна щільність потужності широкосмугового сигналу значно менша у порівнянні з простими сигналами. Таке поєднання використовується в стандарті MC-CDMA [4] (multi carrier CDMA – багаточастотне кодове розділення каналів) і дозволяє значно зменшити вплив навмисних завад.

MC-CDMA система має всі переваги CDMA і OFDM систем, тобто дозволяє боротися із багатопроменевістю й частотно-селективними завмираннями, однак платою за це є істотне зменшення швидкості передачі даних в порівнянні з OFDM.

Завадозахищеність в MC-CDMA системах забезпечується наступними факторами.

По-перше, зменшення впливу завад забезпечується ефектом ,,розмивання" завад по спектру за рахунок перемноження прийнятої суміші сигналу і завади з ПВП.

По-друге, завадостійкість приймання OFDM-сигналу значно підвищується за рахунок підвищення стійкості пілот-сигналів (пілот-несучих) щодо впливу завад, що забезпечує більш точну оцінку поточного стану каналу зв'язку. Знання передаточної характеристики каналу, в свою чергу, дозволяє застосувати режекцію частини спектра, ураженої завадою, з відключенням передачі корисної інформації у відповідних підканалах.

По-третє, якщо противник застосовує імітаційну заваду, яка в точності відтворює структуру сигналу, теоретично він не знає способу генерації ПВП. Тому така імітаційна завада хоч і буде створювати ефект внутрішньосистемних завад, проте внаслідок неортогональності ПВП, що генеруються постановником завад і засобами радіозв'язку, ефективність її значно зменшиться внаслідок узгодженої фільтрації після перемноження в кореляторі приймача СРЗ.

В [4] було досліджено різні ПВП: двійкові (коди Баркера, М-послідовності, послідовності Голда, послідовності Уолша, послідовності Шапіро-Рудіна й породжені на їх основі) і багатофазні (комплементарні послідовності Голея, послідовності Френка й Задова-Чу). Цей список можна розширити, включивши додатково до М-послідовностей інші двійкові послідовності типу Адамара, а також за рахунок багатофазних послідовностей Мілевського.

У результаті було встановлено, що найменший пік-фактор (до 3 дБ) в MC-CDMA системах демонструють ідеальні багатофазні послідовності Френка, Задова-Чу й Мілевського, що мають ідеальну автокореляцію, тоді як двійкові послідовності на основі послідовностей Шапіро-Рудіна забезпечують пік-фактор близько 6 дБ. Недоліком перерахованих вище ідеальних послідовностей є те, що обсяг їх алфавіту (число різних фаз) збільшується з ростом довжини послідовності.

Тому перспективним напрямком подальших досліджень є обґрунтований вибір раціональних ПВП та їх параметрів для розширення спектру OFDM-сигналу, що може додатково забезпечити зниження пік-фактора і, відповідно, підвищення прихованості.

ЛІТЕРАТУРА

1. *Новые алгоритмы формирования* и обработки сигналов в системах подвижной связи / Зубарев Ю. Б., Трофимов Ю. К., Шлома А. М. [и др.] // Электросвязь. – 2004. – № 3. – С. 11 – 13.

2. *Багатоканальні модеми*: Монографія / [Л. Н. Беркман, І. С. Щербина, О. І. Чумак, Л. В. Рудик]; під науковою редакцією С. Є. Захаренка. – К.: Зв'язок, 2006. – 149 с.

3. *Завадостійкість каналів зв'язку*: Навчальний посібник / [Бабич В. Д., Кувшинов О. В., Лежнюк О. П., Лівенцев С. П.]. – К.: КВІУЗ, 2001. – 150 с.

4. *OFDM and MC-CDMA* for broadband multi-user communications / [L. Hanzo, M. Munster, B. J. Choi, T. Keller]. – WLANs and Broadcating, John Wiley&Sons, Ltd., 2003. – 978 p.

к.в.н. Довбня С.Я. (ВІТІ НТУУ „КПІ”)

ОСОБЛИВОСТІ ПІДВИЩЕННЯ КВАЛІФІКАЦІЇ ФАХІВЦІВ В ГАЛУЗІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Важливою та невід’ємною складовою реалізації державної політики у сфері технічного захисту інформації є підготовка та підвищення кваліфікації фахівців у цей галузі [1].

На цей час в Україні створена та в цілому ефективно функціонує система підготовки, перепідготовки та підвищення кваліфікації в галузі інформаційної безпеки.

Система підготовки та перепідготовки фахівців із інформаційної безпеки, зокрема з технічного захисту інформації (ТЗІ), яка склалася у другій половині 70-х років, на сьогодні переживає трансформацію та модернізацію з урахуванням сучасних вимог, які висуваються до інформаційної безпеки у рамках Болонського процесу і як наслідок до рівня підготовки фахівців.

Підготовку спеціалістів в галузі (напрямі) „Інформаційна безпека” (ІБ) по 8 напрямам та спеціальностям здійснюють 28 вищих навчальних закладів, у тому числі і Військовий інститут телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут”. Для перепідготовки та підвищення кваліфікації фахівців функціонують 4 навчальних центри.

Особливістю існуючої системи підготовки фахівців за напрямом „Інформаційна безпека” на рівні „бакалавр” є підготовка фахівців однаково за всіма існуючими спеціальностями. Крім того, підготовка фахівців ведеться як за державним замовленням, так і на контрактній основі. Це обумовлює, що частина фахівців в подальшому буде працювати в державних структурах, а частина в недержавних.

Тобто підготовка спрямована на універсального фахівця за всіма напрямами захисту, який володів би організаційно-технічними і інженерно-технічними навичками, знав би засоби та технології захисту, міг би організовувати та забезпечувати комплексний захист інформації. В той же час, в органах державної влади, зокрема в збройних силах України, доцільно наряду з фахівцями-універсалами, мати фахівців за окремими напрямками захисту, що в силу їхньої спеціальної предметної підготовки краще ніж фахівець-універсал володіють методами, засобами та технологіями захисту інформації у відповідному напрямку.

Важливою ланкою у системі підготовки фахівців в галузі ТЗІ є підвищення кваліфікації. Програми перепідготовки та підвищення кваліфікації повинні мати практичну направленість та мати чітку мету та завдання. Підвищення кваліфікації може проводитися за наступними формами: семінар, конференція, курси. Базовою формою підвищення кваліфікації (з видачею відповідного свідоцтва загальнодержавного зразка) є курси.

Як свідчить практика підвищення кваліфікації, курси доцільно проводити у такій послідовності:

– уточнення мети та завдань підвищення кваліфікації фахівців;

– визначення рівня початкової підготовки слухачів та їх розподіл за напрямками підвищення кваліфікації ;

– уточнення розподілу годин між темами та видами занять за відповідними програмами, яки погоджено з Держспецзв’язку (орган державної влади, який сумісно з МОН України координує підготовку фахівців в галузі ІБ [2]);

– залучення для проведення занять на курсах провідних організацій та фахівців, що мають теоретичний та практичний досвід з конкретних питань ТЗІ, складання розкладу занять;

– визначення індивідуальних завдань підготовки кожному слухачу;

– проведення теоретичних та практичних занять на курсах, з дотриманням певних вимог: цільова аудиторія, використання навчальних засобів (нормативних документів та

літератури, зразків документів, вимірювальної техніки, засобів захисту інформації, тощо), перевірка засвоєння матеріалу та виконання індивідуальних завдань (рефератів), підведення підсумків проходження курсу.

На цей час, в системі навчання фахівців із ТЗІ не знайшли достатнього розвитку таки напрямки: перепідготовка кадрів та цільова підготовка з питань протидії технічним розвідкам (ПДТР), хоча вони в сучасних умовах набувають більшої актуальності.

Згідно з [3], підготовка з питань ПДТР потребує визначення реальних потреб органів державної влади у фахівцях, розвиток та вдосконалення системи підготовки (внесення змін до Переліку спеціальностей…(Табл.1.), визначення відповідних ВНЗ та форм навчання).

Таблиця 1

Зміни до Переліку напрямів та спеціальностей підготовки в Україні фахівців у сфері захисту інформації

Галузь знань	Напрям підготовки	Спеціальність
Навчання за освітньо-кваліфікаційним рівнем „бакалавр” (відповідно до постанови Кабінету Міністрів України від 13 грудня 2006 р. № 1719)		
1701 Інформаційна безпека	6.170101 Безпека інформаційних і комунікаційних систем	
	6.170102 Системи технічного захисту інформації	
	6.170103 Управління інформаційною безпекою	
	Протидія технічним розвідкам	
Навчання за освітньо-кваліфікаційними рівнями «спеціаліст» і «магістр» (Відповідно до постанови Кабінету Міністрів України від 24 травня 1997 р. № 507)		
16 Національна безпека	1601 Інформаційна безпека	160101 Захист інформації з обмеженим доступом та автоматизація її обробки (в комп’ютерних системах)
		160102 Захист інформації з обмеженим доступом та автоматизація її обробки
		160103 Системи захисту від несанкціонованого доступу
		160104 Адміністративний менеджмент в системах захисту інформації з обмеженим доступом
		160105 Захист інформації в комп’ютерних системах і мережах
		Захист об’єктів протидії від технічних розвідок

Розвиток системи перепідготовки кадрів дозволяє прискорити рішення кадрової проблеми за рахунок скорочення термінів навчання, також вносить внесок у рішенні ще однієї проблеми – працевлаштування, у першу чергу, звільнених у запас офіцерів, забезпечуючи їх перепрофілювання.

ЛІТЕРАТУРА

1. *Указ Президента* України від 27 вересня 1999 р. № 1229 „Положення про технічний захист інформації в Україні”.
2. *Закон України* „Про Державну службу спеціального зв’язку та захисту інформації України”.
3. *Постанова Кабінету* Міністрів України від 8 жовтня 1997 р. № 1126 „Концепція технічного захисту інформації в Україні”.

Драчук О.В. (ВІТІ НТУУ „КПІ”)

ВИЯВЛЕННЯ КОМП'ЮТЕРНИХ АТАК НА ОСНОВІ АНАЛІЗУ ПОВЕДІНКИ МЕРЕЖЕВИХ ОБ’ЄКТІВ

Методи виявлення програмних атак принято поділяти на методи виявлення аномалій і методи виявлення зловживань [1]. До другого типу методів відносяться більшість сучасних комерційних систем (*Cisco IPS*, *ISS RealSecure*, *NFR*) – вони використовують сигнатурні (експертні) методи виявлення [1, 2]. Існує ряд академічних праць в області виявлення аномалій, проте в промислових системах вони використовуються рідко і з певної обережністю, так як такі системи породжують велику кількість хибних спрацювань. Для експертних же систем основною проблемою є низька, близька до нуля, ефективність виявлення невідомих атак (адаптивність) [2]. Низька адаптивність до сьогоднішнього часу залишається проблемою, хоча такі переваги як низька обчислювальна складність і мала вартість розгортання визначають домінування таких систем в даній області.

Метою даного дослідження є розробка метода і експертної системи виявлення атак в розподіленій інформаційній системі (РІС) на основі спостереження за поведінкою об’єктів РІС, що дозволяє поєднати переваги двох підходів – виявлення аномалій і виявлення зловживань.

Суть задачі дослідження полягає в створенні моделі комп’ютерної атаки і метода автоматичного виявлення атаки на основі даної моделі, що дозволив би виявляти комп’ютерні атаки при спостереженні за поведінкою об’єктів РІС і їх взаємодією.

В рамках даного дослідження ставляться наступні задачі:

1. побудувати модель функціонування РІС, в рамках якої визначити таке поняття як атака;
2. виділити класи реальних атак, що розглядаються в рамках запропонованої моделі функціонування РІС;
3. розробити метод виявлення атак на РІС на основі інформації про поведінку об’єктів РІС;
4. розробити архітектуру системи виявлення атак для РІС на базі операційної системи *GNU/Linux.*

Таким чином, запропонований метод виявлення атак може бути використаний для побудови реальних систем захисту розподілених комп’ютерних систем з підтримкою загального доступу, де висока ймовірність появи нових реалізацій атак. Найбільша ефективність метода можлива в тих системах, де множина класів об’єктів (сервісів і програмного забезпечення) обмежена і не змінюється в часі істотним чином, що дозволяє використовувати моделі нормальної поведінки для виявлення атак.

Розвиток запропонованого метода, шляхом дослідження всіх відомих класів сучасних атак та оцінки можливості побудови граматики для кожного класа в термінах операцій доступа класа з обмеженим контентом фіксованої довжини, дозволить побудувати систему захисту розподіленої комп’ютерної системи, здатну виявляти не тільки будь-які атаки відповідного класа, але й передбачати розвиток траєкторії класа атаки до завершення самої атаки на початкових етапах її розвитку.

ЛІТЕРАТУРА

1. *Смелянский Р. Л., Гамаюнов Д. Ю.* „Современные некоммерческие средства обнаружения атак”. // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2002 г.

2. *Гамаюнов Д. Ю., Смелянский Р. Л.*, Модель поведения сетевых обьектов в распределенных вычислительных системах. // Журнал „Программирование”, 2007, № 4.

д.т.н. Єрохін В.Ф. (НЦЗІ ВІТІ НТУУ „КПІ”)
Черкасова Ю.О. (НЦЗІ ВІТІ НТУУ „КПІ”)

МЕТОДИКА ВИБОРУ СТРУКТУРИ ТА ДОВЖИНИ КОДОГРАМИ ДЛЯ ВИСОКОНАДІЙНОЇ ПЕРЕДАЧІ КОМАНД (КОРОТКИХ ПОВІДОМЛЕНЬ) У РАДІОМЕРЕЖАХ

Радіомережі, призначені для передачі команд (коротких повідомлень) – далі команд, мають особливості: кількість команд та довжина (об’єм) кодограм, які циркулюють у них, є відносно невеликими; потужності передавальних пристроїв, зазвичай, мінімальні. Внаслідок цього вимоги до вибору швидкості та виду надлишкового коду можуть суттєво відрізнятися від вимог до процедур кодування у традиційних каналах зв’язку.

Режим односторонньої передачі, який також має місце в таких радіомережах, характеризується певними особливостями, пов’язаними з відсутністю відомостей про факт прийому команди, її правильність і повноту. Тому для доведення команди із заданою достовірністю, як правило, вводиться суттєва надлишковість: багатократний повтор передачі інформації через деякі проміжки часу, дублювання передачі на різних частотах і одночасне використання завадостійких кодів.

В цілому проблема забезпечення якісної односторонньої передачі команд по радіоканалах обумовлена наступними чинниками:

1. Канал зв’язку – односторонній, тому оперативна адаптація структури кодограми (швидкості передачі, надлишковості, кількості повторних передач) неможлива через відсутність інформації про якість зв’язку.

2. Якість зв’язку радіоканалу може змінюватися у дуже широких межах. Імовірність помилки на біт $P_{\text{пом}}$ може відрізнятися на порядки – від 10^{-3} до 10^{-5} і навіть менше, до повної відсутності зв’язку на певній частоті, за різних причин – несприятливі умови для розповсюдження радіохвиль, наявність радіозавад і т.і.

3. Відлік часу у засобах передавання та приймання може відрізнятися на одиниці хвилин.

4. Очікувані вимоги до надійності доведення команд можуть сягати $P_{\text{к}} = 0{,}999$ і навіть більше.

Через вищевикладене для забезпечення вимог до завадостійкості та надійності доведення команд доведеться застосовувати кодування з нетипово великою надлишковістю, коли один інформаційний символ буде представлятися в каналі деякою кодовою послідовністю з декількох десятків символів. Тому за умови, що кількість різних команд може бути досить великою, використання найпростіших М-послідовностей не завжди доцільне.

Для досягнення максимальної завадостійкості кодограм важливо, щоб адресна та інформаційна частина мали однакову надлишковість.

Проте за умови обмеження на їх довжину не слід частину кодограми виділяти як адресну, а частину – як інформаційну. Найкращих результатів щодо завадостійкості очікується досягти за умови, коли у кодограмі не можна виділити окремо адресну та інформаційну частину. До того ж у такому випадку третій стороні буде набагато важче ідентифікувати зв’язок між кодограмами та їх адресатами, навіть без використання у лінії зв’язку криптографічних методів.

У кодограмах пропонується використовувати послідовності з хорошими взаємокореляційними властивостями: складені послідовності Касамі [1], послідовності бент-функцій (ПБФ) [1, 2], послідовності Камалетдінова [3] та об’єднання послідовностей Касамі та ПБФ [4], а конкретні значення довжин зазначених послідовностей визначати, виходячи з вимог до об’єму кодограми та завадостійкості передачі.

Основні параметри зазначених послідовностей розраховуються за наступними формулами: довжина $N = 2^{2m} - 1$ (m – ціле число); величина (об'єм) ансамблів $V = \sqrt{N+1} = 2^m$ (для послідовностей Касамі, ПБФ та Камалетдінова), $V_{\sum} = 2\sqrt{N+1} - 1 = = 2^{m+1} - 1$ (для об'єднань послідовностей Касамі та ПБФ, які існують тільки для m – парних [2]); максимальні значення взаємокореляційних сплесків $R = \sqrt{N+1} + 1 = = 2^m + 1$.

Щоб визначити загальну довжину кодограми (яка складається з деякої кількості однієї з вищезазначених послідовностей), необхідно для наборів послідовностей тої чи іншої довжини (N_1 = 15 біт, N_2 = 63 біта, N_3 = 255 біта, N_4 = 1023 біта, N_5 = 4095 біта – для послідовностей Касамі, ПБФ та Камалетдінова; N_1 = 15 біт, N_3 = 255 біт, N_5 = 4095 біт – для об'єднань послідовностей Касамі та ПБФ) розрахувати кількість відмінних комбінацій V^k, де k – кількість складових послідовностей у кодограмі.

Якщо одержана кількість недостатня, збільшити k. Якщо в подальшому результати аналізу завадозахищеності виявляються неприйнятними, збільшити N і повторити попередні розрахунки. Викладену процедуру повторювати циклічно, до виконання вимог до кількості відмінних комбінацій і завадозахищеності.

Аналіз проведених в якості прикладу розрахунків виявив, що:

1. Імовірності правильного прийому команд при передачі на однаковій кількості частот для кодограм із 4-х послідовностей довжиною N_1 = 15 біт та з однієї довжиною N_2 = 63 біта є досить близькими, якщо ймовірність помилки в каналі на символ не гірше за 10^{-1}.

2. Імовірність прийому команди, як і очікувалось, збільшується при збільшенні кількості частот, на яких здійснюється передача кодограми.

3. Для кодограм з довжиною послідовності N_1 = 15 біт поріг для прийняття хибної команди набагато менший, ніж для кодограм з довжиною послідовності N_2 = 63 біта і тому ймовірність прийому хибної команди для кодограм з меншою довжиною набагато більша. Ця різниця тим більша, чим гіршим за показником імовірність помилки є канал.

4. У каналах, які мають більшу імовірність помилку на біт, для отримання більшої ймовірності прийому команди необхідно вибирати менший поріг для прийняття рішення, але при цьому необхідно керуватися обмеженням на імовірність прийому хибної команди.

5. При виборі складових кодограм з більшою довжиною збільшується поріг для прийняття рішення щодо правильного прийому кодограми і покращуються показники передачі, але, очевидно, при цьому необхідно витратити більше часу на передачу такої кодограми.

Запропонований підхід дозволяє уникнути застосування складних надлишкових кодових конструкцій, які для малих швидкостей кодування (10^{-1} та менше) не мають суттєвих енергетичних виграшів у порівнянні з мажоритарним кодуванням, набагато складніші в реалізації, а в каналах з великою імовірністю помилки призводять до енергетичних програшів.

ЛІТЕРАТУРА

1. *Сарвате Д.В., Персли М.Б.* Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей // ТИИЭР, 1980, № 5.– С. 65 – 90.

2. *Камалетдинов Б.Ж.* Оптимальный ансамбль бинарных последовательностей на основе объединения ансамблей последовательностей Касами и бент-функций // Проблемы передачи информации. – М.: 1988, том XXIII, № 2.– С. 104 – 107.

3. *Камалетдинов Б.Ж.* Новые оптимальные ансамбли нелинейных двоичных последовательностей // Проблемы передачи информации.– М.: 1989, том XXV, № 3.– С. 107 – 110.

д.т.н. Жердєв М.К. (ВІТІ НТУУ „КПІ”)
Пистряк В. В. (ВІТІ НТУУ „КПІ”)

ОБГРУНТУВАННЯ НЕОБХІДНОСТІ УДОСКОНАЛЕННЯ МЕТОДІВ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ ЦИФРОВИХ ПРИСТРОЇВ ЗРАЗКІВ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Бойова готовність військ нерозривно пов’язана із забезпеченням ефективної експлуатації зразків озброєння. Витрати на їх експлуатацію на сьогоднішній день істотно перевищують первинну вартість.

У обстановці конверсії і скорочення витрат на оборону питання зниження витрат на експлуатацію і обслуговування радіоелектронної техніки достатньо актуальне як в мирний, так і у воєнний час. Його рішення направлене на зниження часу контролю технічного стану цифрових пристроїв радіоелектронних засобів озброєння при мінімально необхідних витратах на відновлення працездатності.

Аналіз стану і перспектив розвитку озброєння і військової техніки як в Україні так і за кордоном показує, що поліпшення тактико-технічних і експлуатаційних характеристик досягається схемним і конструктивним ускладненням радіоелектронної техніки, що приводить до зниження її надійності. Це протиріччя знімається покращенням ремонтопридатності за рахунок якісного діагностичного забезпечення (ДО), під яким слід розуміти комплекс взаємозв’язаних правил, методів, алгоритмів і засобів, що є необхідними для здійснення діагностування на всіх етапах життєвого циклу зразка озброєння.

Для вирішення задачі пошуку типових елементів заміни (ТЕЗ), що відмовили, можуть бути використані різні методи перевірки працездатності цифрових пристроїв.

Аналіз детермінованих методів показує, що їх використання для перевірки працездатності ТЕЗ безпосередньо на зразку озброєння ускладнене через тривалий час перевірки працездатності. Одночасне скорочення тривалості перевірки і довжини тестової послідовності неминуче призводить до істотного зниження достовірності діагностування.

Для вирішення проблеми генерації тестів останнім часом розроблена ціла низка імовірнісних методів діагностування, що використовують в якості тестових послідовностей випадкові або псевдовипадкові двійкові числа.

Однак, зазначені методи не дозволяють забезпечити виявлення дефектів із заданою достовірністю, що обумовлює їх низьку ефективність.

Підвищити достовірність діагностування дозволяє використання енергодинамічного методу (методу узагальненої контрольної точки), при використанні якого діагностичною інформацією є імпульси струму квазікороткого замикання, що виникають в ланцюгах живлення логічних елементів при їх перемиканнях. Висока достовірність діагностування при цьому досягається за рахунок того, що в якості узагальненої контрольної точки об’єкту діагностування використовується його ланцюгживлення, який є спільнимдля всіх елементів. Це дозволяє знімати діагностичну інформацію зі всіх логічних елементів без використання додаткових контрольних точок.

На теперішній час відпрацьовані лише питання детермінованого діагностування енергодинамічним методом, що не дозволяє використовувати його на зразках озброєння в умовах військової експлуатації.

Таким чином, подальший розвиток зазначеного методу з метою дослідження можливості використання псевдовипадкових тестових послідовностей при енергодинамічному діагностуванні є на сьогоднішній день актуальною науковою задачею.

Жилінський І.В. (ВІТІ НТУУ „КПІ”)
Тупкало В.Є. (в/ч А1906)

ПРОЕКТУВАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ЗВ’ЯЗКОМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Аналіз стану технічних засобів систем зв’язку спеціального призначення, темпи росту об’ємів інформації і потреб в зв’язку, а також вимоги до вирішення задач, які стоять перед ними, показують, що проблема підвищення ефективності функціонування системи, забезпечення надійним та якісним зв’язком загострюється і потребує термінового вирішення.

У теперішній час вирішення вищезгаданої проблеми пов’язують з удосконаленням системи зв’язку спеціального призначення (СЗСП). Але досягти успіху у підвищенні ефективності функціонування системи лише за рахунок впровадження нових засобів зв’язку без реалізації програми інформатизації, основаної на використанні новітніх інформаційних технологій, телекомунікаційних мереж нового покоління, неможливо, оскільки нормальне функціонування СЗСП з високими характеристиками стійкості, надійності, завадозахищеності, скритності та живучості, жорсткими часовими нормами проходження інформації не може здійснюватися без широкого використання автоматизованих систем управлінням зв’язком (АСУЗ).

Тому, вирішення даної проблеми необхідно здійснювати двома взаємозв’язаними шляхами: переоснащення СЗСП сучасними засобами зв’язку та впровадження АСУЗ СЗСП і процесів обробки інформації.

Такий стан зумовлює актуальність досліджень в напрямку проектування АСУЗ СЗСП, що представляє собою сукупність впорядкованих в часі взаємозв’язаних, об’єднаних в стадії та етапи робіт, виконання яких необхідне і достатнє для їхнього створення у відповідності із заданими вимогами.

В життєвому циклі будь-якої автоматизованої системи (АС) найбільш важливими є стадії передпроектного проектування (ПП) [1]. На цих стадіях визначаються вимоги до створюваної АС та формується технічне завдання на її створення. Характерними особливостями ПП є неповнота інформації, наявність кількох варіантів створення системи і необхідність вибору одного з них, неможливість експериментальної перевірки рішень і точного прогнозування їхніх наслідків, що значно підвищує ціну помилкових рішень.

На практиці у Збройних Силах України визначення вимог до АС полягає у створенні макетів (районів) системи в рамках адаптивного проектування [2]. Для визначеної організаційної структури створюються типові автоматизовані робочі місця (АРМ) посадових осіб на відповідних рівнях управління військами. Для кожного типового АРМ розробляється математичне та програмне забезпечення, яке відповідає оперативно-тактичним вимогам вирішуваних завдань. На основі аналізу функціонування створеного макету визначається перелік техніко-економічних вимог до створюваної АС.

У доповіді розглядається альтернативний макетуванню підхід формування технічних вимог до АСУЗ на основі технологічного прототипування, який покладено в основу відповідної методики. Визначено та формалізовано процедурну послідовність методики, в основі якої лежить механізм формування технологічного прототипу АСУЗ з подальшим визначення на його основі технічних вимог до системи в цілому.

ЛІТЕРАТУРА

1. *Мамиконов А.Г.* Проектирование АСУ: Учебник для спец. АСУ вузов / А.Г. Мамиконов. – М.: Высш. школа, 1987. – 303 с.

2. *Ситник В.Ф.* Системи підтримки прийняття рішень / В.Ф. Ситник, О.С. Олексюк, В.М. Гужва, С.П. Ріппа, В.М. Олейко. – К.: Техніка, 1995. – 162 с.

Жук О. Г. (ВІТІ НТУУ „КПІ”)

ВИБІР РЕЖИМУ РОБОТИ ЗАСОБІВ РАДІОЗВ’ЯЗКУ В СКЛАДНІЙ РАДІОЕЛЕКТРОННІЙ ОБСТАНОВЦІ

На якість військового радіозв’язку впливають завмирання сигналів, які виникають внаслідок багатопроменевого розповсюдження радіохвиль, та навмисні завади, що створюються системою радіоелектронного подавлення (РЕП) супротивника.

Крім того, суттєвою перешкодою для оптимального приймання сигналів є апріорна невизначеність характеристик каналу зв’язку. Враховуючі це, стає досить складним завдання забезпечення стійкого радіозв’язку в умовах складної радіоелектронної обстановки, яка постійно змінюється. Вирішити його можливо за вибору режиму роботи засобів радіозв’язку, що забезпечує задані характеристики системи.

Одним з шляхів підвищення ефективності функціонування ЗРЗ є використання широкосмугових сигналів (ШСС). Широкосмугові сигнали, на відміну від вузькосмугових, мають вищу завадозахищеність і протирозвідувальну захищеність.

У більшості широкосмугових систем застосовують ШСС, одержувані методом прямої послідовності (DSSS – Direct SSS). У таких системах розширення спектра здійснюється шляхом множення порівняно вузькосмугового первинного сигналу на широкосмуговий розширювальний сигнал. Серед методів формування ШСС широке практичне застосування одержав метод псевдовипадкового перестроювання робочої частоти (ППРЧ), при якому розширення спектра в межах заданої смуги частот здійснюється за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, невідомим постановнику завад. В сучасних системах радіозв’язку широко використовується один із методів формування широкосмугових сигналів – метод ортогонального частотного розділення з мультиплексуванням (Orthogonal Frequency Division Multiplexing – OFDM). Основними перевагами даного методу є відносно висока стійкість щодо частотно-селективних завмирань і вузькосмугових завад, а також висока спектральна ефективність. Але при наявності в каналі навмисних завад, особливо імітаційно-дезінформуючих, ефективність функціонування засобів радіозв’язку з OFDM значно знижується, іноді до повної втрати переданої інформації. Дослідження показали, що для різних сценаріїв радіоелектронної обстановки ефективними виявляються певні режими роботи ЗРЗ. Так для каналу зв’язку з селективними завмираннями та вузько смуговими завадами ефективним є режим OFDM.

Для випадку дії в каналі імітаційних завад доцільним є розширення OFDM-сигналу псевдовипадковими послідовностями (ПВП) дозволяє значно зменшити вплив навмисних завад.

По-перше, зменшення впливу завад забезпечується ефектом „розмивання” завад по спектру за рахунок перемноження прийнятої суміші сигналу і завади з ПВП. По-друге, завадостійкість приймання OFDM-сигналу значно підвищується за рахунок підвищення стійкості пілот-сигналів (пілот-несучих) щодо впливу завад, що забезпечує більш точну оцінку поточного стану каналу зв’язку. Знання передаточної характеристики каналу, в свою чергу, дозволяє застосувати режекцію частини спектра, ураженої завадою, з відключенням передачі корисної інформації по відповідних піднесучих. По-третє, якщо противник застосовує імітаційну заваду, яка в точності відтворює структуру сигналу, теоретично він не знає способу генерації ПВП. Тому така імітаційна завада хоч і буде створювати ефект внутрішньосистемних завад внаслідок неортогональності ПВП, що генеруються постановником завад і ЗРЗ, однак ефективність її значно зменшиться внаслідок узгодженої фільтрації після перемноження в кореляторі приймача .

Для ретрансльованих завад ефективним є режим ППРЧ. При цьому за рахунок вибору швидкості перестроювання частоти забезпечується можливість повністю позбавитись від ретрансльованих завад.

Результати імітаційного моделювання показують, що застосування адаптивної зміни режиму роботи засобу радіозв’язку дозволяє значно підвищити ефективність їх функціонування в умовах активного радіоелектронного подавлення.

Жук П.В. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ІСНУЮЧИХ ТЕЛЕКОМУНІКАЦІЙНИХ ПРОТОКОЛІВ ДЛЯ ПОБУДОВИ ПЕРСПЕКТИВНИХ МОБІЛЬНИХ РАДІОМЕРЕЖ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Як свідчать результати досліджень вітчизняних та закордонних військових аналітиків, сучасні війни та військові конфлікти характеризуються зростанням розосередженості бойових формувань на полі бою, а майбутні війни будуть характеризуватися ще більшим охопленням. Крім того було зроблено висновок про зниження залежності бойових формувань від централізованого тилового забезпечення, що дозволило підвищити їх мобільність та маневреність.

В таких умовах стало зрозуміло, що для організації взаємодії підрозділів в ході швидкоплинних бойових операцій необхідно використовувати досягнення в області новітніх інформаційних технологій, які б забезпечили безперервне та надійне управління і координацію дій тактичних угруповань військ, розміщених на значних географічних територіях [1]. В свою чергу, широке застосування передових інформаційних технологій у військово-промислових комплексах провідних держав світу призвело до суттєвих змін в принципах, формах і способах застосування військових формувань в ході збройного протиборства. У рамках створення теоретичної бази, що обґрунтовує основні принципи управління збройною боротьбою в інформаційну епоху, у США була розроблена концепція „мережецентричної війни” (*Network-Centric Warfare*, NCW) – концепція управління веденням бойових дій на основі єдиного інформаційно-комунікаційного простору [1]. Реалізація принципів нових „мережецентричних концепцій” та інтеграції систем управління, зв’язку, розвідки та ураження стає актуальним і пріоритетним напрямком реформування ЗС більшості країн світу, в тому числі і України. Враховуючи інтенсивний розвиток інформаційних та телекомунікаційних технологій а також досягнення в області побудови тактичних систем зв’язку розвинених у воєнному відношенні країн світу командування військ зв’язку ЗС України підкреслює необхідність проведення модернізації існуючої системи зв’язку та автоматизованого управління військами на основі бойового застосування новітніх інфокомунікаційних технологій. У зв’язку з цим, одним з актуальних завдань реформування ЗСУ на період до 2015 року є створення багаторівневої мобільної компоненти (МК) мереж зв’язку військового призначення, основу якої складатимуть мобільні радіомережі (МР) – мережі радіозв’язку загального користування, що будуються за технологією MANET (*Mobile Ad-Hoc Networks*) [2].

Однак, організація „мережевого принципу” управління військами вимагає вирішення низки задач як організаційного так і технічного характеру, першочерговими з яких є:

– створення інформаційно-комунікаційної мережі для зв’язку джерел інформації (розвідки), органів управління та засобів ураження, що забезпечить доведення до учасників військових операцій достовірної та повної інформації про обстановку в режимі реального часу;

– розробка програмованих засобів радіозв’язку, які матимуть можливість самоорганізації в мережу передачі даних без завчасно розгорнутої інфраструктури;

– розробка перспективних систем обробки, аналізу та розподілу інформації;

– стандартизація системи протоколів обміну даними.

В даний час швидкий ріст технологій в галузі телекомунікацій привів, з одного боку, до випереджального розвитку комерційних мереж, з іншого боку – необхідність скорочення бюджетних асигнувань на оборону вимагає впровадження цивільних технологій у військову сферу. Однак аналіз існуючих комерційних стандартів і протоколів показує, що їхнє безпосереднє застосування в системах військового зв'язку неможливе. Комерційні протоколи оптимізовані до стаціонарної інфраструктури і не можуть виконувати функції адресації, маршрутизації, передачі обслуговування з однієї зони в іншу в мережах з динамічною топологією, реалізують централізовані алгоритми управління і, крім цього, вносять значне

службове навантаження на мережу. Головна відмінність мереж військового призначення тактичного рівня – динамічна топологія, ненадійність, тимчасовість каналів, низька їх живучість. Під вузлом МР відповідного рівня МК розуміється термінал (сенсорний пристрій, переносний комп'ютер, робот, мобільна базова станція та ін.) оснащений радіомодемом, який одночасно виконує функції кінцевого пристрою та маршрутизатора. Вузли різних рівнів перспективної МК характеризуються різними значеннями мобільності, потужності передавачів та рівнем продуктивності, що необхідно враховувати при проектуванні та розробці протоколів і методів управління МР [3].

З метою виконання вимог до нового покоління систем зв'язку військового призначення доцільно провести аналіз та класифікацію існуючих протоколів (методів) управління мережами зв'язку, відповідно до рівнів еталонної моделі взаємодії відкритих систем (OSI).

Однією з проблем управління МР є ефективний розподіл радіоресурсу між множиною незалежно функціонуючих вузлів, що передбачає застосування відповідних методів доступу, які функціонують на *фізичному* та *канальному* рівнях моделі OSI. На сьогоднішній день існує велика кількість безпровідних локальних мереж цивільного призначення, при побудові яких використовуються протоколи *Bluetooth* (IEEE 802.15), *Wi-Fi* (IEEE 802.11), *WiMax* (IEEE 802.16), *Hiper*LAN2, тощо. Як показують результати проведеного аналізу, перевагу мають протоколи *Wi-Fi* (IEEE 802.11) та *WiMax* (IEEE 802.16) через можливість організації децентралізованого управління мережею та здатність підтримувати зв'язок з рухомими об'єктами (навіть при високих швидкостях). Дані протоколи після певної модифікації можуть бути застосовані в мобільних радіомережах і створювати основу для побудови мобільної компоненти тактичних мереж зв'язку ЗСУ [4]. На *мережевому* рівні моделі OSI вирішується проблема побудови топології МР (сукупність вузлів на місцевості і радіоканалів, які їх з'єднують у взаємному розташуванні). Це дасть змогу визначити потенційні можливості мережі з доставки даних між взаємодіючими вузлами, а вже на основі побудованої топології вирішується проблема пошуку маршрутів передачі заданої якості, шляхом використання відповідних методів маршрутизації (ММ). За способом побудови і підтримання маршрутів ММ діляться на три класи: таблично-орієнтовані (OSPF, OLSR, RIP, DSDV, ADV та ін.), зондові (DSR, AODV, SSR та ін.) та гібридні (ZRP, R-зоновий та ін.). Проведені дослідження показали, що таблично-орієнтовані методи маршрутизації ефективні при незначній динаміці мережевої топології, а зондові методи в більшій мірі відповідають особливостям функціонування мобільних радіомереж (мобільність вузлів та нестабільність радіоканалів). Тому в [5] запропоновано реалізувати так звану „активну" маршрутизацію, яка, на відміну від традиційних ММ, передбачає наступні підходи: функціонування в мережі множини (а не одного) методів маршрутизації; динамічне формування метрик вибору маршруту; управління топологією мережі як складовою частиною маршрутизації в МР; інтелектуалізацію процесів прийняття рішення з маршрутизації. На *транспортному* рівні моделі OSI здійснюється управління потоками даних – це процес узгодження характеристик потоків даних і характеристик засобів, які обслуговують ці потоки, що здійснюється шляхом встановлення таких значень параметрів відповідних мережевих елементів, при яких забезпечується доставка даних в мережі із заданою якістю обслуговування [6]. Основним протоколом, який функціонує на транспортному рівні є протокол TCP та його модифікації (TCP *Vegas*, TCP *Reno*, F-TCP, TCP-MEDX, C^{3}TCP та ін.). До основних недоліків існуючих методів управління потоками даних, які перешкоджають їх використанню в мережах з динамічною топологією, відносяться: повільна адаптація вікна перевантаження до частих змін топології МР; відсутність повної інформації про стан мережі; втрата сегмента розцінюється існуючими протоколами як така, що виникла внаслідок перевантаження; управління трафіком здійснюється, в основному, кінцевими вузлами. Враховуючи зазначені недоліки, у [6] запропоновано ввести координацію взаємодії методів різних рівнів моделі OSI, а також інтелектуалізувати процес управління потоками даних, що дозволить зменшити

витрати часу на збір і аналіз службової інформації про стан мережі, скоротити об'єми цієї інформації та мінімізувати помилки, пов'язані з ухваленням неправильного рішення з управління МР. На *прикладному* рівні моделі OSI вирішуються проблеми управління енергоресурсом, а також забезпечення необхідної якості обслуговування абонентів. Електроживлення більшості вузлів в МР здійснюється від батарей, тому в таких вузлах повинні бути реалізовані методи (методики) управління енергоресурсом, метою функціонування яких є мінімізація споживаної вузлами потужності. Управління енергоресурсом може бути реалізоване за різними функціями управління і рівнями еталонної моделі взаємодії відкритих систем (фізичному, канальному, мережевому, транспортному) методами управління потужністю передачі та методами збереження енергії батарей. Представником методів управління потужністю передачі є протокол PCM (*Power Control* MAC), який передбачає, що відправник передає запит на передачу, а приймач – згоду на прийом, з однаковою потужністю, але передача інформації і квитанції здійснюються з мінімальною потужністю, необхідною для безпомилкового прийому.

Представником методів збереження енергії батарей є децентралізований протокол PAMAS (*Power Aware Multiple-Access Protocol*), який реалізує пасивний режим між сусідніми вузлами (відключення вузла у випадку, коли пакет призначається не йому). Проведені дослідження показали, що застосування методів управління енергоресурсом дозволить збільшити час життя мережі в середньому в 1.5…2 рази і зменшити середню потужність передачі на один ретрансляційний відрізок на 15…20%. Синтез оптимального методу управління енергоресурсом буде визначатися характеристиками відповідного рівня мобільної компоненти та прийнятими рішеннями з реалізації інших функцій управління мережею. Іншою задачею управління МР на ***прикладному*** рівні є забезпечення передачі певних класів (типів) трафіка із заданою якістю обслуговування (QoS, *Quality of Service*). QoS-моделі, що використовуються в стаціонарних мережах не можуть бути використані в МР, виходячи з їх особливостей. Для МР запропоновано низку QoS-моделей управління (INSIGNIA, FQMM, iMAQ, SWAN, 2LQoS та ін.), більшість з яких передбачає управління якістю на певному рівні моделі OSI і реалізує найпростіші алгоритми резервування та адаптації ресурсів вузлів (каналів) до різних типів трафіка. Для управління якістю обслуговування в [7] запропоновано ввести в архітектуру системи управління МР відповідну підсистему, яка буде здійснювати координацію методів управління, що функціонують на різних рівнях моделі OSI. Таким чином, враховуючи рівень розвитку технологій в галузі цивільних телекомунікаційних систем, а також необхідність скорочення бюджетних асигнувань на оборону, одним із варіантів побудови перспективних тактичних мереж військового призначення є використання існуючих комерційних стандартів (протоколів, методів) та проведення наукових розробок для їх удосконалення з урахуванням унікальних характеристик військової інфраструктури, а також сучасних вимог до процесу управління військами та відповідних вимог до систем зв'язку тактичного рівня.

ЛІТЕРАТУРА

1. *Force Transformation* to Improve Mission Effectiveness: In Proceedings of Network-Centric Warfare Europe 2010 / K. – P. Steiglitz, 23 – 24 June, 2010, Brussels.

2. *Кравченко О.О.* Пріоритетні напрямки розвитку системи зв'язку та автоматизації управління військами Збройних Сил України: збірник матеріалів IV науково-технічної конференції [„Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ", 2008. – С.12 – 14.

3. *Романюк В.А.* Мережі MANET – основа побудови тактичних мереж зв'язку : збірник матеріалів IV Науково-практичного семінару ВІТІ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення"] / – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 15 – 28.

4. *Романюк В.А.* Методы множественного доступа в мобильных радиосетях / Романюк В.А., Миночкин А.И. // Зв'язок. – 2004. – № 2. – С. 35 – 39.

5. *Романюк В.А.* Активная маршрутизация в мобильных радиосетях / Романюк В.А. // Зв'язок. – 2002. – № 3.

6. *Сова О.Я.* Постановка проблеми управління потоками даних у мобільних радіомережах з динамічною топологією / Сова О.Я. // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2010. – № 1. – С. 92 – 100.

7. *Миночкин А.И.* Управление качеством обслуживания в мобильных радиосетях / Миночкин А.И., Романюк В.А. // Зв'язок. – 2005. – № 7. – С.54 – 58.

к.т.н. Загороднюк Ю.Г. (НЦЗІ ВІТІ НТУУ ,,КПІ")
Куцаєв В.В. (НЦЗІ ВІТІ НТУУ ,,КПІ")
Тамаровський В.В. (НЦЗІ ВІТІ НТУУ ,,КПІ")

ОДИН ІЗ МОЖЛИВИХ НАПРЯМКІВ СТВОРЕННЯ СИСТЕМИ НАВІГАЦІЇ НАЗЕМНИХ РУХОМИХ ОБ'ЄКТІВ

Сьогодні актуальні військові системи управління з геоінформаційними технологіями. Відомо, що у військових конфліктах та локальних війнах на Балканах, Африканському континенті, Грузії, Афганістані і т.д., в інтересах виконання військових задач активно використовувались географічні та просторові дані. Геоінформаційні системи (ГІС) можна розглядати як одну із основних складових систем підтримки і прийняття рішень (СППР). Досить широкого розповсюдження набирає поняття геоінформаційної системи підтримки та прийняття рішень в автоматизованій системі управління, основними завданнями якої є вирішення раціональних маршрутів руху підрозділів, точне визначення просторового положення рухомих об'єктів, вихід на задані точки маршрутів в найкоротший проміжок часу і т. д.

Основним джерелом інформації про географічне та просторове положення військових об'єктів є системи та комплекси навігації й орієнтації. Слід зазначити, що навігація успішно охопила космічний, повітряний, водний та наземний простори, проте можливості систем навігації (СН) наземних рухомих об'єктів (НРО) вкрай відстають від передових технологій, і не тільки в апаратному, але й у ідеологічному (моральному) розумінні. На протязі десятиріч системи навігації встановлювались лише на окремих та спеціальних машинах.

Найпоширенішими сучасними СН НРО провідних країн світу є системи, які об'єднують автономні системи навігації (АСН) та супутникові навігаційні системи (СНС). Такі системи називаються інтегрованими системами. Інтегровані навігаційні системи у поєднанні з елементами електронної картографії все частіше застосовуються у сучасних наземних рухомих об'єктах на гусеничному та колісному шасі, які виконують завдання як у складі основних підрозділів, так і автономно. Аналіз сучасних розробок в галузі навігаційного приладобудування вказує, що завдання створення інтегрованої СН для застосування на борту наземних об'єктів на базі автономної навігаційної системи та СНС і досі не вирішена в повному обсязі жодним виробником. Основою інтегрованої навігаційної системи повинна бути автономна система навігації, яка повинна задовольняти вимогам точності визначення основних навігаційних параметрів та вимогам надійності й розвідзахищеності її функціонування. Пропонується в якості основної в інтегрованій навігаційній системі застосовувати безплатформену інерціальну навігаційну систему (БІНС). Дана система володіє унікальними інформаційними можливостями, які реалізуються при високому ступені завадозахищеності, скритності та повної автономності виконання цільового завдання. БІНС відзначають також: простота конструкції; порівняно малі масогабаритні характеристики; порівняно малий час передстартової підготовки, а також широкі можливості модернізації на рівні програмного забезпечення. При цьому вартість виробництва БІНС у порівнянні із платформеними інерціальними навігаційними системами нижча на 25 %, а експлуатаційні витрати нижчі на 80 %, що в сукупності з перерахованими вище характеристиками обумовлює їх використання в якості ядра інформаційно-вимірювальних систем НРО.

Характерним недоліком інерціальних систем є той факт, що при тривалій автономній роботі накопичується похибка вихідної інформації. У якості коректорів навігаційної інформації пропонується використовувати СНС.

Пропонуємо варіант побудови інтегральної системи навігації наземних рухомих об'єктів, яка складається із автономної – безплатформенної інерціально–навігаційної системи та корегуючої – супутникової навігаційної системи. Дана інтегрована система є основною складовою геоінформаційної системи, яка служить для введення, накопичення, обробки та представлення просторових даних про наземні рухомі об'єкти.

Загребельний О.Ю. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ДОСТУПУ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ З РІЗНИМИ МЕРЕЖНИМИ АРХІТЕКТУРАМИ

Матеріальною основою наднадійного комунікаційного середовища, яке є неодмінною умовою ефективного функціонування комп’ютерних мереж в майбутніх „мережецентричних війнах” [1, 2], на тактичному рівні повинні стати перспективні мережі зв’язку – динамічні самоупорядковні мобільні радіомережі (МР) або MANET (Mobile Ad-Hoc Networks), які характеризуються високою динамікою топології, різноманітністю вузлів, децентралізованим управлінням тощо [3]. Всі вузли даної мережі мобільні, реалізують функції маршрутизатора та обмінюються інформацією безпосередньо між собою або застосовують ретрансляцію пакетів.

Однією із задач управління МР є ефективний розподіл радіоресурсу між множиною незалежно функціонуючих вузлів, що припускає застосування на канальному рівні відповідних методів доступу (МД). До МД у МР пред’являються наступні основні вимоги: децентралізоване функціонування, висока пропускна спроможність, мала затримка передачі, а також ряд додаткових: передача неоднорідного (дані, мова, відео) і пріоритетного трафіка, управління черговістю передач тощо [4]. На даний час для МР пропонується ряд МД. Однак, ефективність застосування того чи іншого МД залежить від характеристик конкретної МР (числа вузлів, пропускної здатності радіоканалів, мережевої архітектури – тобто, топології мережі) й умов її функціонування (динаміки зміни топології, навантаження, виду трафіка тощо). Тому, єдиного методу доступу в МР, що задовольняє усім вимогам, не існує [4] .

Забезпечити задану якість передачі пакетів на канальному рівні МР неможливо без ефективної системи управління, реалізованої на кожному вузлі мережі [5], при цьому ефективність використання радіоресурсу МР визначається не тільки індивідуальними характеристиками вузлів, а й можливостями усієї групи підключених до мережі засобів (вузлів) як єдиного цілого.

Таким чином, питання вивчення архітектури побудови МР є важливою і невід’ємною умовою вивчення можливостей „єдиного інформаційно-комунікаційного простору” в майбутніх „мережецентричних війнах” [1].

В доповіді представлений аналіз архітектур МР з точки зору їх впливу на вибір відповідних методів множинного доступу до радіоканалу в МР.

Одним з можливих підходів до вивчення мережної архітектури є таксономія мереж [1], що базується на таких поняттях, як „рівноцінність” („нерівноцінність”) і „однорідність” („неоднорідність”), а також поділ такої архітектури на централізовану, „за запитом”, однорангову (по типу „зграї”, „рою”) та на їх комбінацію.

При цьому підході можна припустити, що мережна архітектура рівноцінна, якщо усі підключені засоби ідентичні й втрата одного з них рівнозначна втраті іншого. І навпаки, архітектура мережі нерівноцінна, якщо один підключений засіб має велику цінність по відношенню до інших. Наприклад, втрата базової станції стільникової радіомережі набагато критичніше, ніж втрата одного контрольованого нею абонента. Отже, ця мережна архітектура нерівноцінна і будується навколо ключового вузла – стільникової базової станції.

Іншим критерієм оцінки може бути однорідність і неоднорідність мережної архітектури. Можна припустити, що мережна архітектура однорідна, якщо усі підключені вузли ідентичні, і неоднорідна – при неідентичності вузлів. Між двома цими поняттями є певний спектр станів (горизонтальна вісь).

Комбінуючи цей спектр з попереднім критерієм, можна отримати „трикутник можливостей”, тому що однорідна архітектура може бути як „цінно-симетричною” (рівноцінною), так і нерівноцінною (з ключовим „хабом”). Кожна з опцій цього трикутника відповідає мережній архітектурі. Можна виділити три типи основної мережної архітектури (рис. 1).

Тип *A* – централізована, тип *E* – архітектура мережі „за запитом”, тип *G* – зграєва архітектура (архітектура „рою”). В той же час найбільш реалістичними будуть варіанти *B*, *C*, *D*, *F*, комбінації основних трьох типів архітектури, що є, так звана змішана архітектура. В централізованих архітектурах зазвичай застосовуються МД з фіксованим закріпленням абонентів за радіоресурсом (ортогональні та квазіортогональні МД) або динамічні МД з централізованим управлінням (за вимогою) [6]. В МР з архітектурою „за запитом” застосовуються динамічні МД з централізованим управлінням (за вимогою) та децентралізовані з резервуванням.

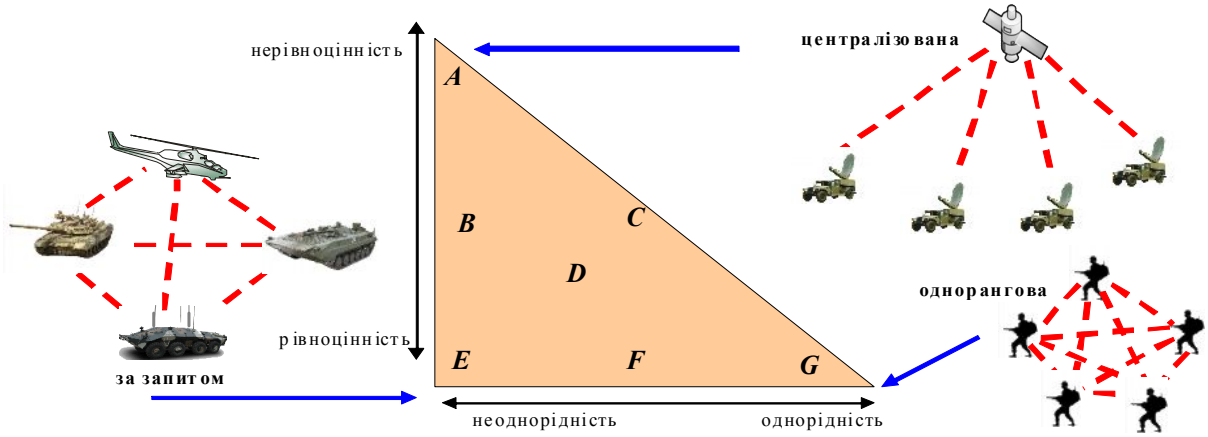


Рис. 1. Типи мережних архітектур у відповідності до „трукутника можливостей”

Найбільш складною, але в той же час і найбільш перспективною вважається мережна архітектура типу *G* – однорангова архітектура, що є комбінацією повністю рівноцінних і однорідних засобів (мережі бойових літаків, морських кораблів, бойових машин піхоти, танків, бійців тощо). Кожен з таких засобів має свій (хоча і з обмеженими можливостями) інформаційно-комунікаційний засіб. Для ефективного виконання завдання такі засоби повинні обмінюватися між собою інформацією, самоорганізовуватися і самосинхронізуватися. В зграєвій архітектурі доцільно застосовувати динамічні децентралізовані МД (випадкові або з резервуванням). Іноді „рій” ідентичних засобів доповнюється спеціальним центральним „хабом” (тип *C* – однорангова з вузлом, що управляє). В такій архітектурі доцільно застосовувати динамічні МД з централізованим управлінням (з опитуванням або з активним резервуванням) [6].

Однорангова архітектура властива і розвідувальним (сенсорним) мережам. Вона застосовується для організації обміну розвідувальною інформацією між окремими засобами і її розподілу в інтересах підготовки даних ситуаційної обізнаності та синхронізації дій. При такій побудові МР може застосовуватися керована (Orchestrated Swarming), ієрархічна (Hierarchical Swarming) і розподілена (Distributed Swarming) однорангова архітектура (рис. 2).

У змішаній архітектурі типу *F* (Mixed) використовується одночасно і однорангова архітектура, і архітектура мережі „за запитом”. Такий спосіб побудови мережі застосовується при використанні рівноцінних і неоднорідних засобів (у чомусь схожих, в чомусь різних). Наприклад, возимі та носимі інформаційно-комунікаційні засоби (далі – ІТЗ) тактичної ланки управління.

Можна виділити два підтипи змішаної архітектури типу *F*. Перший застосовується для об'єднання декількох типів неоднорідних, але рівноцінних засобів, наприклад, ІТЗ зразків, що розробляється за програмою „Перспективні бойові системи" армії США, – 14 комплексів, включаючи машини управління, гаубиці, міномети, БЛА, наземні роботизовані комплекси тощо. При такому об'єднанні ІТЗ однорангова архітектура застосовується, коли засоби об'єднуються для розподілу даних ситуаційної обізнаності (однорангова ієрархічна). Однорангова архітектура також може застосовуватися і серед перспективних наземних комплексів для виконання бойового завдання (однорангова розподілена), а між неоднорідними засобами може використовуватися і метод формування мережі „за запитом". В архітектурі типу *F* доцільно застосовувати динамічні децентралізовані МД з резервуванням. Широко застосовуються й інші типи архітектури, яку можна віднести до змішаних. Однорангова архітектура мережі з управляючим вузлом (тип *C* Hub-Swarm) – це результат об'єднання архітектури типу *G* і додавання „хаба" високої цінності для підсилення функціональних можливостей мережі, хоча сама архітектура і має особливості однорангової.

Наприклад, мобільні базові станції об'єднуються в мережу архітектури *G*, але додавання повітряного телекомунікаційного вузла дозволяє істотно підвищити ефективність мережі. При цьому літак виступає в якості центрального „хаба".

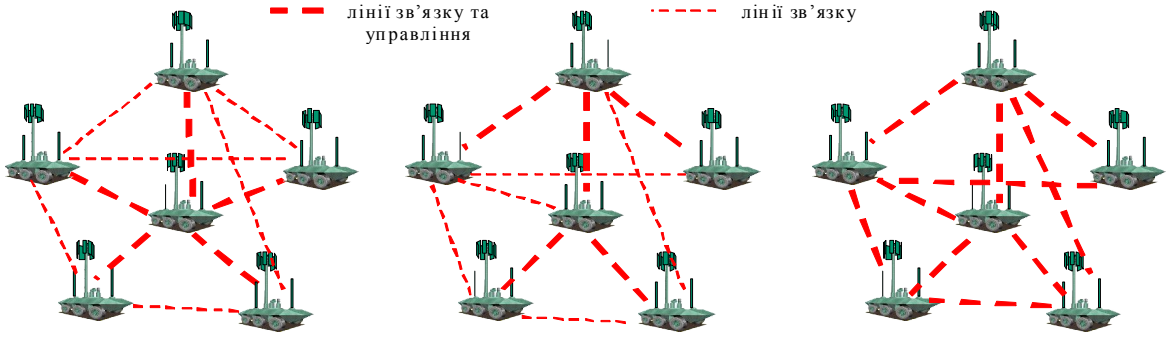


Рис. 2. Варіанти мережних однорангових архітектур

Архітектура мережі „за запитом" з центральним вузлом (тип *B* HubReqest) формується при додаванні до типу *E* високоцінного „хаба".

Останній і найскладніший варіант архітектури мережі – об'єднана (гібридна) мережа (тип *D* Joint). Такий тип об'єднує в собі всі наявні мережні архітектури і властивий в першу чергу операціям об'єднаних сил. Високоцінний „хаб" в такій об'єднаній архітектурі мережі виконуватиме завдання саме „хаба", тобто комутатора. Групи рівноцінних і рівнозначних ІТЗ об'єднуватимуться в мережу з одноранговою архітектурою і будуть використовувати децентралізовані гібридні МД та динамічні МД з резервуванням, прийнятні для неоднорідних мереж [6]. На практиці ж усі три основні типи архітектури мереж можуть бути об'єднані. Успіх сучасних і майбутніх військових операцій залежатиме в першу чергу від міри об'єднання усіх учасників операції (бойових дій) перспективними цифровими мережами в єдиний інформаційно-комунікаційний простір, що забезпечує ефективне управління підпорядкованими військами і силами.

Одним з основних і невід'ємних елементів методології дослідження мережевої архітектури, вживаної при реалізації МР перспективних сетецентрических концепцій, є їх класифікація і систематизація, що дозволяє визначати ключові вузли, тобто виявляти „центри тяжіння" МР.

В зв'язку з цим істотно зростає роль радіоелектронної боротьби і дезинформації як основних заходів організації протидії. Організація ж ефективної протидії вимагає знання

структури органів управління і архітектури МР супротивника для виявлення їх уразливих елементів, а також розуміння того, як супротивник використовує ці мережеві ресурси. В цих умовах найбільш перспективним є застосування гібридних Meta-MAC МД з управлінням на основі нечіткої логіки [6, 7].

В зв'язку з цим для вивчення перспективної мережної архітектури, вживаної при формуванні єдиного інформаційно-комунікаційного простору, а також для планування і організації заходів протидії є доцільним застосовувати спеціалізовану методологію з використанням теорії, що базується на визначенні центрів тяжіння МР і виявленні критично важливих уразливих елементів таких мереж, тому що кожен тип мереж має свої найуразливіші елементи і кожна архітектура вимагає свого підходу до вибору МД та організації і здійснення заходів протидії.

При цьому треба звернути увагу на те, що не можна змішувати поняття „центр тяжіння" і „критично важливі уразливі елементи", оскільки перший термін застосовується для усієї МР, а другий – саме для підготовки удару (дії) по першому.

В той же час необхідно враховувати, що архітектура перспективних МР залежно від ситуації постійно змінюється. Такі мережі можуть мати усі згадані архітектури. Певна архітектура може з'являтися і зникати після виконання поставленого бойового завдання, що, поза сумнівом, сприятиме підвищенню живучості МР. Запропонований підхід до класифікації і систематизації мережевої архітектури МР може застосовуватися при виборі (синтезі) необхідних методів доступу (мета-методу), при плануванні і організації заходів інформаційної протидії, дозволяє автономно в кожному вузлі мережі ідентифікувати ситуацію в каналі та керувати методами доступу на основі нечіткої бази знань, побудованої з використанням експертних знань. Вибір (синтез) необхідних методів доступу (мета-методу) буде визначатися параметрами МР (архітектурою, розмірністю, мобільністю, оснащеністю вузлів устаткуванням позиціювання, спрямованими антенами тощо), параметрами інформаційного навантаження й вимогами до його передачі.

Таким чином, в докладі представлений аналіз мережних архітектур МР, показаний характер впливу мережних архітектур МР на вибір відповідних МД, запропоновані найбільш прийнятні МД для кожного типу мережних архітектур, обґрунтовано застосування гібридних мета-методів доступу з управлінням на основі нечіткої логіки для об'єднаних (гібридних) мережних архітектур МР в умовах впливу засобів радіоелектронної боротьби.

ЛІТЕРАТУРА

1. *Кондратьев А.Е.* Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран // Военная мысль. – 2008. – № 12. – С. 63 – 74.

2. *Калистратов А.И.* К вопросу о сетецентрических действиях в вооруженной борьбе будущего // Военная мысль. – 2008. – № 12. – С. 22 – 30.

3. *Міночкін А.І., Романюк В.А.* Концепція управління мобільною компонентою мереж зв'язку військового призначення // Збірник наукових праць № 3. – К.: ВІТІ НТУУ „КПІ". – 2005. – С. 51 – 60.

4. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв'язок. – 2004. – № 2.

5. *Миночкин А.И., Романюк В.А.* Методология оперативного управления мобильными радиосетями // Зв'язок. – 2005. – № 2. – С. 53 – 58.

6. *Загребельний О.Ю.* Методи управління множинним доступом в мобільних радіомережах // Збірник наукових праць № 1. – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 41 – 50.

7. *Загребельний О.Ю.* Методика адаптивного управління доступом до радіоканалу в мобільних радіомережах // Збірник наукових праць № 2. – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 44 – 53.

к.т.н. Залогін С.М. (ВІТІ НТУУ ,,КПІ")
к.т.н. Колачов С.П. (ВІТІ НТУУ ,,КПІ")
Садиков О.І. (ВІТІ НТУУ,,КПІ")

ОБГРУНТУВАННЯ ТАКТИКО-ТЕХНІЧНИХ ВИМОГ ДО ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ПЕРЕВЕЗЕННЯМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Автоматизована система управління (АСУ) перевезеннями спеціального призначення є організаційно-технічною системою, що забезпечує вироблення рішень на основі автоматизації інформаційних процесів управління перевезеннями. АСУ реалізує інформаційну технологію у вигляді певної послідовності інформаційно зв'язаних функцій, завдань або процедур, що виконуються в автоматизованому (інтерактивному) або (та) автоматичному режимах.

У доповіді розглянута типова структура АСУ перевезень спеціального призначення, яка складається з **функціональних підсистем** (збору, аналізу, обробки інформації; підтримки прийняття рішення; планування перевезень; оперативного управління підпорядкованими підрозділами; забезпечення перевезень), **технологічних підсистем** (відображення інформації; геоінформаційна; електронного документообігу; інформаційно-довідкова; електронної пошти; відеоконференцзв'язку; управління функціонуванням; комплексна система захисту інформації; телекомунікаційна мережа; система автоматичної ідентифікації рухомого складу і великовантажних контейнерів), а також **технічних та програмних засобів комплексу засобів автоматизації**.

Сумісне функціонування різних підсистем комплексу засобів автоматизації повинно здійснюватися на базі локальної обчислювальної мережі (ЛОМ) відповідно до вимог керівних документів по стандартизації, наприклад, РД 50-680-88 (автоматизовані системи).

У доповіді пропонується, виходячи з організаційної структури перевезень, функціонування АСУ здійснювати територіально-розподіленою комутованою локальною IP-мережею з базовим програмним забезпеченням (ПЗ) для керування роботою апаратури та спеціального ПЗ для виконання функціональних та технологічних задач АСУ, в якій, з одного боку, група комп'ютерів повинна погоджено виконувати набір взаємозв'язаних завдань, обмінюючись даними в автоматичному режимі, з іншого боку, комп'ютерна мережа має бути засобом передачі інформації на великі відстані.

Пропонується представити IP-мережу у вигляді суми територіально відособлених типових IP-підмереж (сайтів), які відповідно повинні обслуговувати свої об'єкти. Сайти повинні обмінюватися IP-пакетами через глобальну мережу і утворювати віртуальну приватну мережу служби перевезень, для якої повинні виконуватися принципи системності, розвитку (відвертості), сумісності, стандартизації (уніфікації) і ефективності. Сайти повинні дозволяти здійснювати автоматизацію процесів управління перевезеннями за технологією Ethernet з допомогою однотипних комутованих ЛОМ на основі сервера (server based), які мають бути розміщені на територіально-розподілених об'єктах (управліннях) і об'єднані в одну обчислювальну мережу перевезень.

У складі типової комутованої ЛОМ повинні бути робочі станції, комутатор 3-го рівня (один або більше) (або комутатор та маршрутизатор), різні сервери: файл-сервер, принт-сервер, сервер додатків, поштовий сервер, факсі-сервер, комунікаційній сервер (Число серверів і робочих станцій визначається потребами роботи об'єкта (управління), де розміщується типова ЛОМ). Комутована ЛОМ повинна бути побудована за топологією розподіленої зірки. У вузлі зірки має бути розташований комутатор (або комутатор 3-го рівня). Якщо застосовуватиметься декілька комутаторів, то вони мають бути зв'язані між собою. Кожен комутатор має порти, до яких можуть бути приєднані невеликі локальні мережі та окремі робочі станції АРМ-ів, сервері. При цьому локальна мережа розділяється на

логічні сегменти, що дозволяє підвищити гнучкість і керованість мережі, безпеку даних і вирішити проблему масштабування локальної мережі. Так, при побудові мережі, як сукупності сегментів, кожен з них може бути адаптований до конкретних потреб робочої групи або відділу. Наприклад, в одному сегменті може виконуватися технологія Ethernet і ОС Unix, а в іншому – Token Ring. Разом з тим, у користувачів обох сегментів є можливість обмінюватися даними через комутатор (гнучкість ЛОМ підвищується). Встановлюючи різні логічні фільтри на комутаторі, можна контролювати доступ користувачів до ресурсів інших сегментів (безпека даних підвищується). При зниженні трафіку і підвищенні безпеки даних спрощується управління ЛОМ, оскільки проблеми дуже часто локалізуються усередині сегменту: сегменти утворюють логічні домени керування мережею.

Комутатор потрібно застосовувати так, щоб між логічними сегментами не було петель, тобто будувати за допомогою комутатора тільки деревовидні структури, які гарантують наявність єдиного шляху між будь-якими двома сегментами. Тоді кадри від кожної станції поступатимуть в комутатор завжди з одного і того ж порту, і комутатор зможе правильно вирішувати задачу вибору раціонального маршруту в мережі. Для підтримки *стійкого неблокуючого режиму* роботи комутатора, при якому комутатор передає кадри із швидкістю їх надходження протягом довільного проміжку часу, необхідно, щоб його продуктивність задовольняла умові [1]: $C_k = (\sum C_{pi})/2$, де C_k – продуктивність комутатора, C_{pi} – максимальна продуктивність протоколу. Для підтримки *миттєвого неблокуючого режиму* (кадри приймаються і обробляються комутатором від всіх своїх портів на максимальній швидкості протоколу) комутатор повинен володіти більшою власною продуктивністю: $C_k = \sum C_{pi}$.

Сайти типових IP-підмереж повинні бути об’єднані в одну обчислювальну мережу перевезень за допомогою однієї з найперспективніших транспортних технологій MPLS IGP [2], яка застосовується для прискорення просування пакетів мережевого рівня, наступних упродовж маршрутів, вибираних стандартними внутрішніми шлюзовими протоколами, наприклад, RIP, IS-IS, OSPF або MPLS TE [3], при якій шляхи комутації за мітками вибираються для вирішення завдань інжинірингу трафіку (TE) на основі модифікованих протоколів маршрутизації. Необхідно відзначити, що техніка MPLS TE не тільки дозволяє забезпечити раціональне завантаження всіх ресурсів глобальної мережі, але і створює хорошу основу для надання транспортних послуг з гарантованими параметрами QoS. Необхідно відзначити, що для забезпечення безпеки даних в мережах перевезень, без застосування технології шифрування, необхідно використовувати технології надійного розмежування трафіка, які реалізуються новим типом віртуальних приватних мереж – мережами MPLS VPN. Перевагою є те, що вище перелічені технології MPLS можуть співіснувати в одній мережі.

Таким чином, автоматизована система управління (АСУ) перевезеннями спеціального призначення, яка має територіально-розподілені типові IP- підмережі та які повинні бути об’єднані в одну обчислювальну мережу перевезень, повинна забезпечувати автоматизацію обміну командною, неформалізованою і табличною інформацією, а також формалізацію, редагування, контроль, обробку, реєстрацію, документування, зберігання і передачу різних видів оперативної інформації каналами АСУ прямими каналами зв'язку.

ЛІТЕРАТУРА

1. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2008 – 958 с.

2. *Олифер В.Г., Олифер Н.А.* Виртуальные частные сети на основе MPLS. – LAN/ Журнал сетевых решений, январь 2002.

3. *Олифер В.Г., Олифер Н.А.* MPLS на службе VPN. – LAN/ Журнал сетевых решений, март 2002.

Захараш О.М. (ВІТІ НТУУ „КПІ”)

ПЛАНУВАННЯ МЕРЕЖІ РАДІОДОСТУПУ CDMA 2000

Визначальним при проектуванні мережі рухомого радіозв’язку з кодовим розподілом каналів є планування радіомережі. Планування радіомережі являє собою ітераційний процес одним із кроків якого є синтез структури мережі. Процес планування здійснюється поступово, крок за кроком, і виливається в пропозиції стосовно побудови мережі радіозв’язку й аналізу її роботи.

На результати планування істотний вплив мають системні фактори, підсилюючи складність і неоднозначність розв’язку задачі синтезу мережі радіозв’язку, які можуть бути сформульовані як завдання пошуку такої мережі радіозв’язку s'', які задовольняють вихідним вимогам (обмеженням) і мають при цьому значення сукупності (вектора) показників якості $\overline{K}(s'')$, найкращим у якості безумовного критерію переваги: $\overline{K}(s'') \le \overline{K}(s')$.

Якщо виконується умова $\overline{K}(s'') \le \overline{K}(s')$, то кожен з показників якості оптимізованої мережі не гірше, ніж у вихідній мережі, у тому числі, щонайменше, один із цих показників якості краще, ніж у мережі s'. У даній постановці задача синтезу мережі відноситься до завдачі векторної (багатокритеріальної) оптимізації й полягає у виборі з декількох варіантів векторно-порівнянних розв’язків такого, при якому мережа має найкращі значення вектора показників якості $\overline{K}(s)$. Успішно розв’язати поставлене вище завдання синтезу мережі можна шляхом комбінації методів математичного синтезу, пов’язаного з істотною ідеалізацією мережі та евристичного синтезу. Слід зазначити, що методи векторного синтезу (оптимізації), засновані на безумовному критерії переваги, забезпечують відшукання „негіршого розв’язку”, а в математичному відношенні зводяться до мінімізації єдиного показника − апаратурного ресурсу мережі [1, 2].

У якості технічних основ для планування використовуються характеристики передбачуваних для використання стандартів, прийомопередаючого устаткування й антен, умови поширення радіохвиль, необхідна напруженість поля корисного сигналу, навантаження на одного абонента, припустиме блокування викликів і т.д. [3].

Планування мереж з кодовим розподілом каналів має відмінність,яка пов’язана з тим, що мережа працює в загальній для всіх базових станцій смузі частот. Отже, відпадає необхідність використовувати частотний кластер, що обумовлює архітектуру мережі й порядок розподілу частот за елементами мережі. Але з іншого боку, отримують особливу вагомість питання, які пов’язані з енергетичним балансом між елементами мережі, тому що від їхнього розв’язку залежать основні параметри стільникової мережі. Якісне проектування радіомережі повинно задовольняти очікувану щільність трафіку при мінімальній кількості встановленого радіоустаткування з урахуванням можливості збільшення пропускної здатності мережі при зростанні запитів на передачу трафіку [4]. Це завдання може вирішуватися за рахунок раціонального розташування базових станцій, потужності передавачів, висот антен і їх типів. Складність завдання не дозволяє знайти прямий розв’язок і має на увазі використання методу послідовних наближень.

ЛІТЕРАТУРА

1. *Качество услуг* мобильной связи. Оценка, контроль и управление / В.Ю. Бобков, П.В.Полынцев, В.И.Устюжанин; Под ред. проф. А.А. Гоголя. − М: Горячая линия − Телеком, 2006.

2. *Системы подвижной* связи / Под ред. А.М. Дедовского. − М.: Горячая линия − Телеком, 2006. − 536 с.

3. *GSM.GPRS and* EDGE Performance / *Timo Halonen, Javier Romero, Juan Melero.* − LTD: JOHN WILEY& SONS, 2002. − 585 p.

4. *3G CDMA* evolution − Enabling Broadband Wireless Access // Qualcomm. − 2005. − Sept.

к.т.н. Зінченко А.О. (НУОУ)
к.т.н. Жук О.В. (ВІТІ НТУУ „КПІ”)
Філіпов В.В. (НУОУ)

ПРОПОЗИЦІЇ ЩОДО РЕФОРМУВАННЯ ВУЗЛІВ ЗВ’ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Однією з найважливіших вимог, які висуваються до Збройних Сил України у теперішній час є їх якісне удосконалення для забезпечення високої бойової готовності та спроможності виконання бойових задач. Одним із шляхів такого якісного удосконалення є поліпшення функціонування системи управління та її найбільш складної частини – системи зв’язку. Головним призначенням системи зв’язку є забезпечення своєчасного проходження інформації між пунктами управління.

Система управління Збройних Сил України на сьогоднішній день переживає значні зміни та оновлення які, відповідно, не могли обминути і систему зв’язку Збройних Сил України. Кажучи про зміни, необхідно мати на увазі не тільки перехід до іншої організаційно-штатної структури органів управління, сил та засобів, які забезпечують зв’язок. В першу чергу слід сказати про зміну у підходах до організації зв’язку та перехід від аналогового до цифрового видів зв’язку.

Вузол зв’язку – найважливіший елемент системи зв’язку, який призначений для обміну усіма видами інформації та ведення переговорів у процесі управління військами (силами), тому питання щодо удосконалення структури вузлів зв’язку є найважливішими на шляху посилення готовності військ зв’язку до забезпечення потреб управління за будь-яких обставин. Крім того, задачі, що покладаються на вузли зв’язку пунктів управління, а також важливість цих елементів у складі системи зв’язку, визначають оперативність управління військами (силами), своєчасність, достовірність і прихованість передачі усіх видів інформації.

На теперішній час, наявними силами та засобами якісно вирішити питання забезпечення зв’язком посадових осіб пунктів управління практично неможливо, тому побудову структур вузлів зв’язку необхідно здійснювати виходячи з наступних принципів: відповідність їх оперативно-технічних можливостей потребам системи управління і зв’язку; структурна організованість; організаційно-технічна єдність вузлів зв’язку різного призначення; ешелонування сил і засобів вузлів зв’язку; сполучення централізованого і децентралізованого управління.

Виходячи із завдань, які стоять перед Збройними Силами України на сьогоднішньому етапі їх реформування, поняття вузол зв’язку пункту управління втрачає свою актуальність. На зміну йде нове формування – інформаційно-телекомунікаційний вузол, який забезпечить безперебійний обмін інформацією у єдиному інформаційному просторі та буде мати телекомунікаційну і інформаційну складові. На пунктах управління мають бути розгорнуті та функціонувати локальні інформаційні мережі, елементи регіональної інформаційної мережі, мережі абонентського доступу, внутрішні мережі. Створення інформаційно-телекомунікаційних вузлів зв’язку надасть можливість доступу посадовим особам пунктів управління до різних видів інформації у єдиному інформаційному просторі Збройних Сил України.

Таким чином інформаційно-телекомунікаційні вузли стаціонарних пунктів управління видів Збройних Сил України, армійських корпусів, оперативних командувань, територіальних управлінь будуть мати ідентичну структуру, та відрізнятися тільки кількістю обладнання (в залежності від кількості зв’язків та абонентів пунктів управління) і, відповідно – кількістю особового складу. В порівнянні з існуючими вузлами зв’язку та центрами АСУ будуть мати значно меншу кількість підрозділів, а отже – й меншу чисельність особового складу.

Зінченко А.О.(НУОУ)
к.ф.н. Пучков О. О. (ВІТІ НТУУ „КПІ”)
Ромащенко Р.А. (ВІТІ НТУУ „КПІ”)

ОЦІНКА МОЖЛИВОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ *FRAME RELAY* У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Автоматизовані системи управління можна розглядати у *функціональному* й *інформаційному* аспектах. Перший відбиває ієрархію вироблення управляючих впливів на різних рангах системи і характеризується структурою управління, що визначає взаємопідпорядкованість об’єктів і відображає конфігурацію і спрямованість зв’язків управління між об’єктами систем.

Окрім того, структура управління може містити відомості про те, де приймається те або інше рішення, яка інформація для цього збирається і звідки вона надходить, для яких об’єктів призначаються вироблені управляючі впливи і якого вони виду.

Інформаційний аспект управління відбиває процеси обміну управляючою або довідковою інформацією, що є необхідною для реалізації процесу змістовного функціонування системи.

Даний аспект характеризується структурою і функціонуванням інформаційної мережі, що забезпечує інформаційні зв’язки між об’єктами, тобто виконуючої функції збору, передачі, перетворення, збереження і розподілу інформації в інтересах управління.

На сьогодні найбільшого поширення у проводових телекомунікаційних мережах отримала технологія *Frame Relay*.

Оскільки перспективні автоматизовані системи управління (АСУ) спеціального призначення передбачать передачу інформації саме з використанням цієї технології, метою даної доповіді є оцінка можливості застосування технології *Frame Relay* у телекомунікаційних мережах спеціального призначення в умовах максимальної агресивності зовнішнього середовища, що передбачає постановку супротивником активних та пасивних завад, застосування зброї масового ураження та ін.

Слід зазначити, що технологія ретрансляції кадрів *Frame Relay* (*FR*) виникла завдяки потребі сполучення локальних мереж каналами глобальних мереж, поєднання територіально розрізнених локальних мереж корпорації в єдину швидкісну корпоративну мережу. *Frame Relay* можна розглядати і як спрощений варіант *X*.25 для надійних мереж та високих швидкостей передавання даних [1]. Головна відмінність цієї мережі від *X*.25 – це те, що корекцію помилок виконують не проміжні, а кінцеві вузли.

Завдяки зменшенню часу на опрацювання у проміжних вузлах затримка у вузлі *FR* становить близько 3 мс, тоді як аналогічне значення для *X*.25 – 50 мс. Швидкість передавання *FR* набуває різних значень – від 56 Кбіт/с до 1.544 Мбіт/с залежно від перепускної здатності та кількості залучених каналів. Технологія *FR* не накладає обмежень на максимальну швидкість передавання [2].

Аналогічно до *X*.25, технологія *FR* визначає тільки інтерфейс *UNI* (*User to Network Interface*) між вузлами комутації та кінцевими пристроями, не обмежуючи протоколів та архітектури магістральної мережі (вона може, наприклад, бути мережею *ATM* або *ISDN*) [3]. Для сполучення двох мереж FR визначено інтерфейс *NNI* (*Network to Network Interface*).

FR допускає змінну довжину кадру – від кількох до 2000 байт. Гнучка зміна довжини кадру дає змогу налаштовуватися до зміни навантаження. З іншого боку, вона призводить до змінної затримки у передаванні інформації та неможливості роботи з ізохронними потоками (відео- та аудіоінформація) [4].

Однак, оскільки *Frame Relay* є мережею з обходами, виникнення локальних перевантажень в одному або декількох інформаційних напрямках зв’язку може привести до загальномережевих перевантажень, і як наслідок цього, їх блокування в цілому [5]. Отже,

виникнення відмов комутаційних вузлів в обслуговуванні пакетів через збільшення інтенсивності вхідного потоку заявок приводить до зменшення функціональної живучості інформаційної мережі.

На сьогоднішній день використовується декілька методів спрямованих на вирішення зазначеного питання. Так, у розробках фірми *Cisco* головним засобом уникнення перевантажень є метод *Weighted Random Early Detection* (*WRED*), який полягає в тому, що в критичних пунктах мережі постійно відбувається вимірювання інтенсивності потоку і, якщо вона наближається до порогу перевантаження, деякі пакети відкидаються, зменшуючи таким способом навантаження [6]. Вибір пакетів залежить від їхнього пріоритету.

Однак, використання зазначених методів, даючи змогу уникнення локальних перевантажень на окремих вузлах комутації, може привести до глобальних (загальномережевих) перевантажень внаслідок додаткового збільшення (за рахунок відкинутих пакетів) інтенсивності потоку на визначеному інформаційному напрямку, намагання кінцевого вузла (точки входу в мережу) передати цей потік по іншим маршрутам, і як наслідок цього, загального зменшення перепускної спроможності мережі через розповсюдження переповнення вхідних буферів комутаційних вузлів [7 – 9]. В цьому випадку елементи мережі працюючи з повним навантаженням забезпечуватимуть передачу пакетів з незначною швидкістю.

Окрім того інформаційні напрямки, якими здійснюється передача пакетів з низькими пріоритетами, фактично втратять свою функціональну живучість через відкидання цих пакетів на комутаційних вузлах.

Таким чином, беручи до уваги те, що телекомунікаційні мережі спеціального призначення повинні функціонувати в умовах максимальної агресивності зовнішнього середовища, можна зробити висновок, що використання технології Frame Relay у АСУ спеціального призначення стає недоцільним через невиконання вимог по надійності та живучості [10].

ЛІТЕРАТУРА

1. *Баранец С*. Введение в сети с коммутацией пакетов // Компьютерное обозрение. 1996. № 16 (40).
2. *Кларк З*. *Frame Relay* становится общедоступньїм // *LAN Magazine*/*RE*. 1998. № 6.
3. *Крейнес А*. Пакет с нарочньїм // LAN Magazine. 1997. № 2.
4. *Мельников Д.* Frame Relay для профессионалов и не только // Сети. 1997. № 10.
5. *Парсонс Т., Бар Д.* Как стать победителем в гонке Frame Relay // LAN Magazine. 1996. № 5.
6. *Лайза Хендерсон,* Том Дженкинс, Frame Relay межсетевые взаимодействия, Москва, „Горячая линия – Телеком", 2000
7. *Буров Є*. Комп'ютерні мережі. 2-ге оновлене і доповн. вид. Львів: БаК, 2003. – 584 с
8. *Барабанов С,* Коростелин А., Крюков С. Компьютерньїе сети: вчера, сегодня, завтра //Компьютерпресс. 1997. №2, 3. С. 152 – 158, 158 – 162.
9. *Барсков А.Г., Фоминов О.С.* Передовьіе технологии: Layer 3 switching // Сети и системи связи. 1997. №8, 9.
10. *Колачов С. П.* Дослідження можливості використання технологій Frame Relay та АТМ у проводовій телекомунікаційній мережі спеціального призначення К.: Труди академії, 2008. – С. 125 – 132.

Ізофатов Д.О. (ВІТІ НТУУ „КПІ”)

МОДЕЛЮВАННЯ ПРОГНОЗУВАННЯ ТРАФІКУ В КОМП’ЮТЕРНІЙ МЕРЕЖІ

При проектуванні, запуску й експлуатації комп’ютерних мереж однією з основних проблем є задача забезпечення якості обслуговування (заданих рівнів затримок, втрат та ін.) при обробці потоку даних – трафіка, що є наслідком інформаційного обміну між системами.

Донедавна теоретичну базу для проектування систем розподілу інформації забезпечувала теорія телетрафіка, що є однією з галузей теорії масового обслуговування і з’явилася в результаті робіт А.К.Эрланга, Т.Энгсета, Г.О.Делла, К.Пальма, А.Я.Хінчіна та ін.

Однак, у 1993 році група американських дослідників W.Leland, M.Taqqu, W.Willinger та D.Wilson опублікували результати своєї нової роботи, що у корені змінила існуючі уявлення про процеси, що відбуваються в комп’ютерних мережах. Потоки в таких мережах не можна апроксимувати найпростішими і, як наслідок, вони вже мають зовсім іншу структуру, ніж прийнято в класичній теорії телетрафіка. Зокрема, було встановлено, що трафік такої мережі має так названу властивість „самоподоби”, тобто виглядає якісно однаково при майже будь-яких масштабах часової осі, має пам’ять (післядію), а також характеризується високою пачечністю (коефіцієнт пачечності (пачечність) для заданого потоку відповідає відношенню пікової інтенсивності процесу надходження заявок на обслуговування до його середнього значення).

В результаті теоретичний розрахунок параметрів системи розподілу інформації, призначеної для обробки комп’ютерного трафіка, по класичних формулах дає некоректні та невиправдано оптимістичні результати.

Більш того, звичні алгоритми обробки трафіка, створені для роботи з найпростішими потоками, виявляються недостатньо ефективними для потоків із самоподобою.

Метою даної роботи є розробка алгоритму та засобів для моделювання прогнозування трафіку в комп’ютерній мережі, яка включає в себе проектування експериментальної дослідницької комп’ютерної мережі та розробку програмного забезпечення для виконання функцій прогнозування трафіку та обчислення основних статистичних показників функціонування такої мережі.

В результаті виконання роботи був проведений аналіз існуючих методів розподілу пропускної здатності в каналах комп’ютерних мереж, на основі алгоритмів полісінга та шейпінга розроблений новий алгоритм забезпечення якості обслуговування, що реалізує принцип динамічного розподілу пропускної здатності за допомогою прогнозування, розроблена дослідницька комп’ютерна мережа та програмне забезпечення для проведення експерименту, проведено моделювання прогнозування трафіку в комп’ютерній мережі.

Аналіз самоподібного комп’ютерного трафіка та розрахунки щодо прогнозування його інтенсивної проводяться у середовищі відомого мережевого емулятора ns-2. Програмне забезпечення ns-2 має відкритий вихідний код та розповсюджується безкоштовно без обмежень на право використання, модифікації та розповсюдження. Ns-2 являє собою об’єктно-орієнтоване програмне забезпечення, ядро якого реалізоване на мові C++, а мова сценаріїв Otcl використовується в якості інтерпритатора. Експериментально показано, що запропонований механізм у випадку простого передбачувача дає помітний виграш (~ 8,5 %) у зменшенні втрат та збільшенні ефективності використання каналу при самоподібному трафіку в порівнянні із статичним способом розподілу пропускної здатності. При цьому якість прогнозу поліпшується на 58 %. Підвищення загальної ефективності системи обумовлено більш ефективним розподілом її ресурсів.

Результати, отримані в ході виконання даної роботи, можуть бути використані при розробці алгоритмів функціонування та програмного забезпечення вузлів комп’ютерних мереж з метою підвищення якості обслуговування й ефективності обробки трафіка, що має властивість самоподоби.

к.т.н. Ільїнов М.Д. (ВІТІ НТУУ„КПІ”)
Воробйов А.О. (ВІТІ НТУУ„КПІ”)

РОЗРАХУНОК ЗОВНІШНІХ ЕЛЕКТРИЧНИХ ХАРАКТЕРИСТИК ПОДВІЙНОЇ ЛІНІЙНОЇ АНТЕННОЇ РЕШІТКИ ВІБРАТОРНОГО ТИПУ

Незалежно від призначення системи мобільного радіозв’язку, її організаційно-технічної побудови, основним її елементом є базова (стаціонарна) станція (БС), а отже і її антенно-фідерний пристрій.

Відмінною особливістю антен БС системи мобільного радіозв’язку є те, що вони не тільки вносять вагомий вклад в енергетичний потенціал радіолінії, але й визначають організаційно-технічну схему побудови систем радіозв’язку в цілому.

В теперішній час широке розповсюдження отримали антени БС, виконані у вигляді синфазних антенних решіток (АР) різної конфігурації на випромінюючих елементах у вигляді симетричних вібраторів. Різновидом антен даного класу і являється подвійна лінійна АР вібраторного типу. Випромінюючий елемент такої АР представляє собою два симетричних вібратора рознесених в просторі на кут 180° над циліндричною поверхнею (трубою). Конструкція такого випромінюючого елемента показана на рис. 1, де позначено: h – висота вібратора над циліндричною поверхнею, $2a$ – діаметр циліндра, l – довжина плеча ВЕ, $r = h + a$.

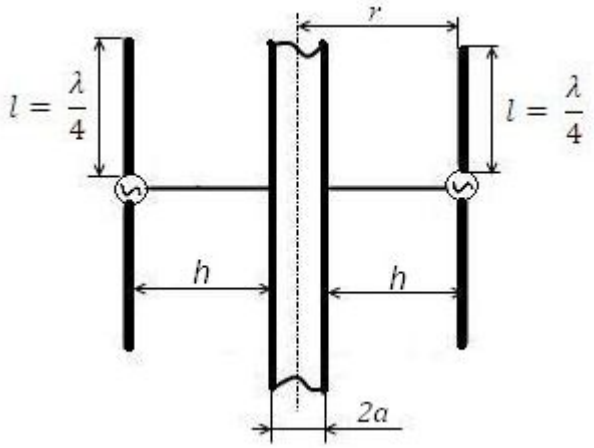


Рис. 1

В основу розрахунку зовнішніх характеристик випромінюючого елемента (ВЕ) покладена дифракційна задача про поле випромінювання симетричного вібратора над циліндричною поверхнею [1], а також теорія кільцевих АР [2]. Аналогічний вираз для розрахунку характеристик направленості (ХН) такого випромінювача має наступний вигляд:

$$f(\varphi,\theta) = f_0(\theta)\sum_{m=0}^{\infty}\left\{e^{i\Delta\psi m}\left(V_0 + 2\sum_{n=1}^{\infty} i^n V_n \cos[n(\varphi+\pi m)]\right)\right\}$$

де: $f_0(\theta) = \frac{\cos(kl\cos\theta)-\cos kl}{\sin\theta}$ – ХН симетричного вібратора у вільному просторі;

$$V_0 = I_0(kr\sin\theta) - \frac{I_0(ka\sin\theta)}{H_0^{(2)}(ka\sin\theta)} H_0^{(2)}(kr\sin\theta);$$

$$V_n = I_n(kr\sin\theta) - \frac{I_n(ka\sin\theta)}{H_n^{(2)}(ka\sin\theta)} H_n^{(2)}(kr\sin\theta);$$

$\Delta\psi$ – зсув фази між двома ВЕ;

a – радіус труби.

На рис. 2 представлені в азимутальній площині діаграми направленості (ДН) подвійної АР вібраторного типу для значень $\Delta\psi$ та h/λ.

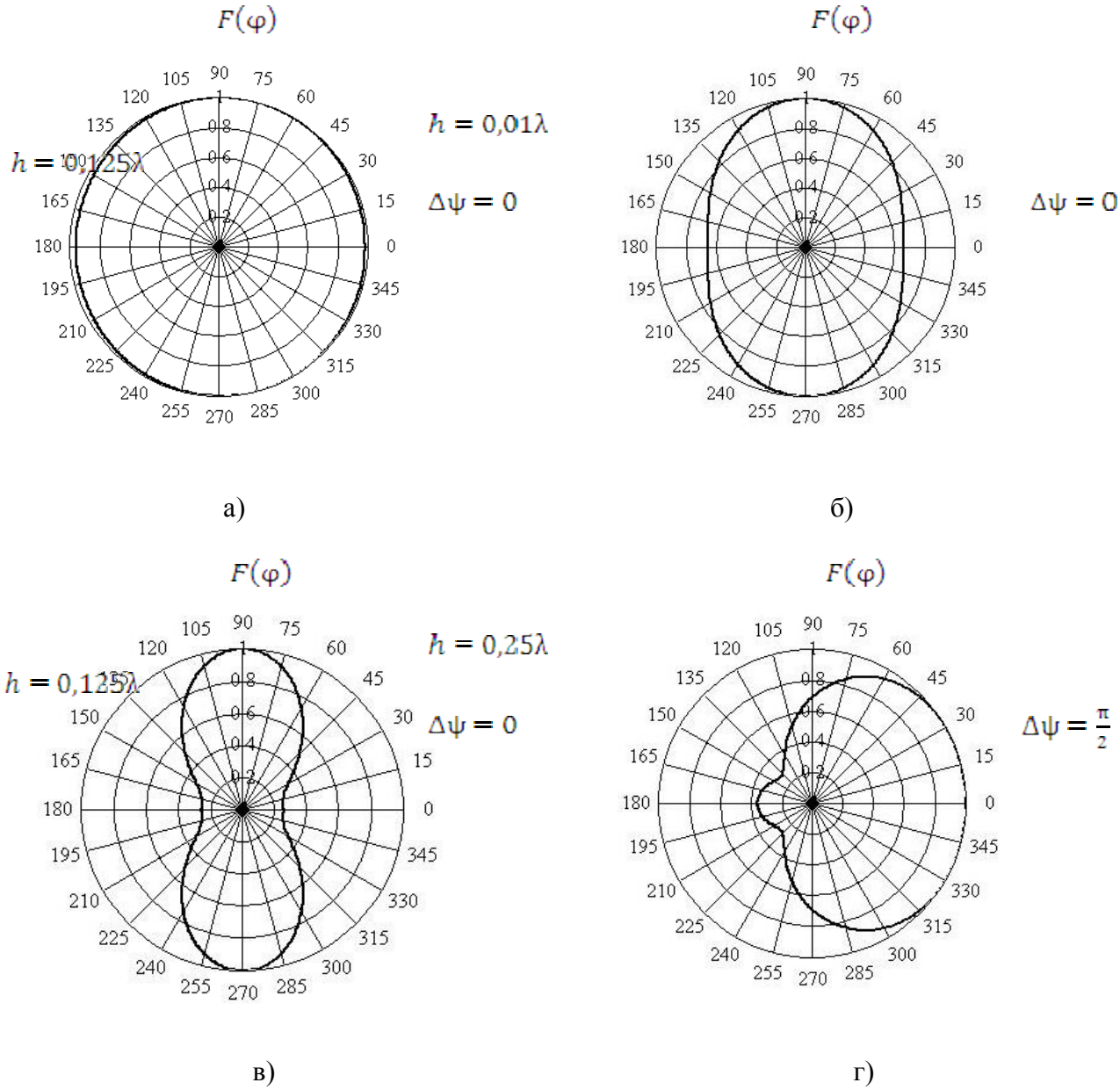


Рис. 2

Отримані результати наглядно демонструють широкі функціональні можливості за зовнішніми характеристиками випромінювачів у вигляді двох симетричних вібраторів над циліндричною поверхнею, тобто і АР на їх основі.

Таким чином, проведений аналіз зовнішніх характеристик подвійної лінійної антенної решітки вібраторного типу наглядно підкреслює важливість застосування подібних антен, дозволяючи формувати ненаправлене, квазінаправлене, двонаправлене та секторне випромінювання ДН в азимутальній площині, що значно полегшує задачу реалізації зони покриття відповідно з вимогами та особливостями конкретного регіону, при організації транкової чи мобільної системи радіозв'язку з рухомими об'єктами.

ЛІТЕРАТУРА

1. *Резников Г.Б.* Антенны летательных аппаратов / Резников Г.Б. – М.: Советское радио, 1967. – 415 с.
2. *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.

к.т.н. Ільїнов М. Д. (ВІТІ НТУУ „КПІ”)
Павлюк О. М. (ВІТІ НТУУ„КПІ”)

ЗОВНІШНІ ХАРАКТЕРИСТИКИ АНТЕН ГОРИЗОНТАЛЬНОЇ ПОЛЯРИЗАЦІЇ З НЕНАПРАВЛЕНИМ ВИПРОМІНЮВАННЯМ В АЗИМУТАЛЬНІЙ ПЛОЩИНІ

Впровадження цифрового телебачення в повсякденне життя, зокрема на початковому етапі, стало вимагати від виробників антенної техніки перегляд деяких фундаментальних положень в області як приймальних так і передаючих антен, це пов’язано з тим, що цифрове телебачення хоча й працює на одних частотах з аналоговим, але при цьому суттєво відрізняється від нього. По-перше, використання декомпресії в форматі *MPEG–4* дозволяє в десятки разів зменшити об’єм даних, завдяки чому в смузі одного аналогового каналу вміщується декілька цифрових. По-друге – при передачі цифрового сигналу (в стандартах *DVB–T* з модуляцією *OFDM*) для однакових зон покриття, порівняно з аналоговою передачею, енергетичний потенціал можливо зменшити на 20 дБ, тобто потужність передавача, наприклад, можна зменшити в 100 разів.

З цього короткого аналізу особливостей телевізійного цифрового мовлення можна зробити наступні важливі висновки щодо антенної техніки: по-перше, суттєво знижуються вимоги до телевізійних антен стосовно діапазонних властивостей; по-друге, реалізація передаючих телевізійних антен потребує зменшеного коефіцієнт підсилення і електричної міцності. Практично, це означає, що для прийому і передачі цифрового телевізійного мовлення можна використати антени відомих зразків. Але, при подальшому розвитку мереж цифрового телевізійного мовлення, антенну техніку слід модифікувати або переходити до нових принципів її компоновки.

На сучасному етапі розвитку антенної техніки телевізійного мовлення, в якості передаючих антен, які дозволяють формувати ненаправлене або секторне випромінювання з горизонтальною поляризацією, використовуються наступні типи антен. Класичним представником антен даного типу являється турнікетна антена (рис. 1а). На рис. 1 показана компоновка антен на основі напівхвильових вібраторів та їх діаграма направленості в азимутальній площині, а також практична реалізація у вигляді широкополосн1ё11

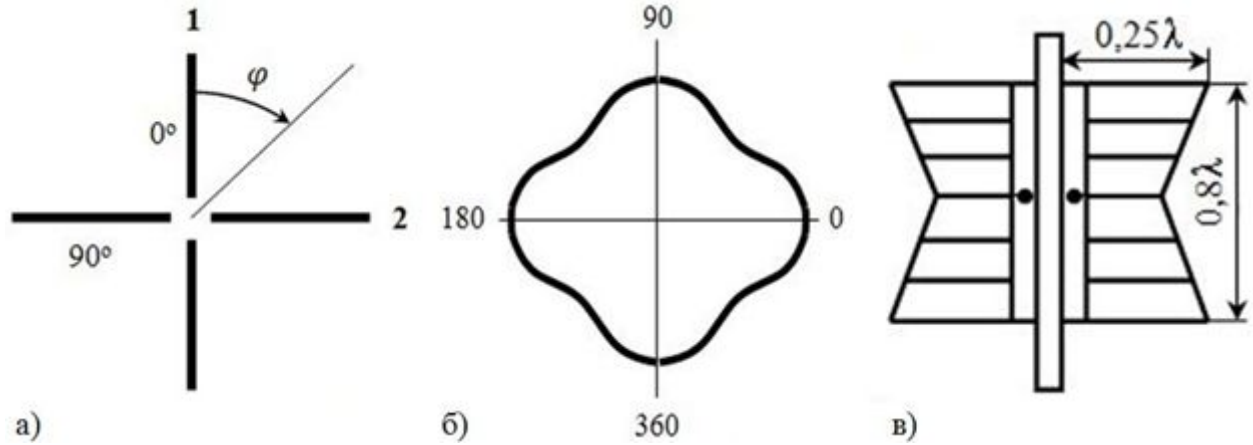


Рис. 1

На рис. 2 показано ряд технічних рішень (рис. 2а – кутова антена; рис. 2б – П-подібна; рис. 2в – П-подібна з ємкісним навантаженням; рис. 2г – кільцева), які можуть бути покладені в основу компоновки передаючих антен ди1циметрового діапазону

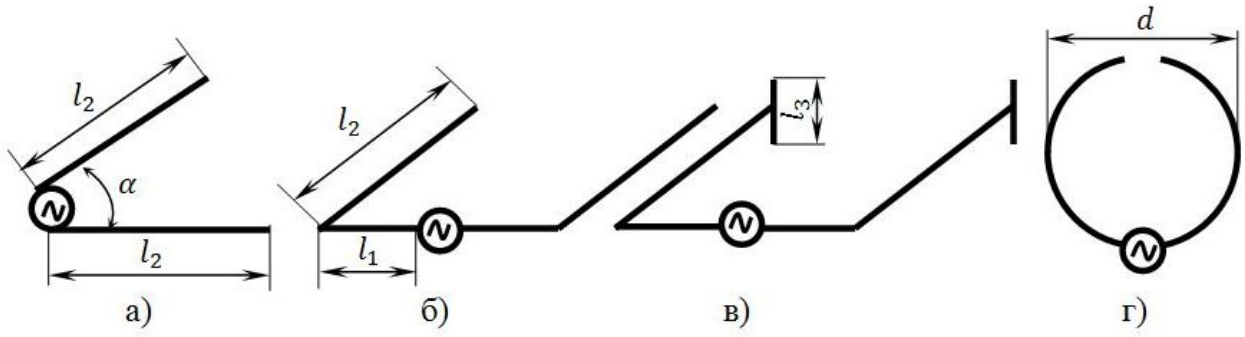


Рис. 2

Представлені технічні рішення являються модифікацією симетричного вібратора, що дозволяють отримати квазіненаправлене випромінювання в азимутальній площині і зменшити його розміри.

З метою підтвердження працездатності запропонованих технічних рішень та їх практичної реалізації, був проведений аналіз зовнішніх і внутрішніх електричних характеристик П-подібної антени для різних співвідношень l_1/l_2, з довжиною плеча симетричного вібратора $l = l_1 + l_2$.

На рис. 3 показано діаграми направленості П-подібної антени для різних співвідношень l_1/l_2. Аналіз електричних характеристик був проведений за допомогою програми „MMANA" – компютерне моделювання антен.

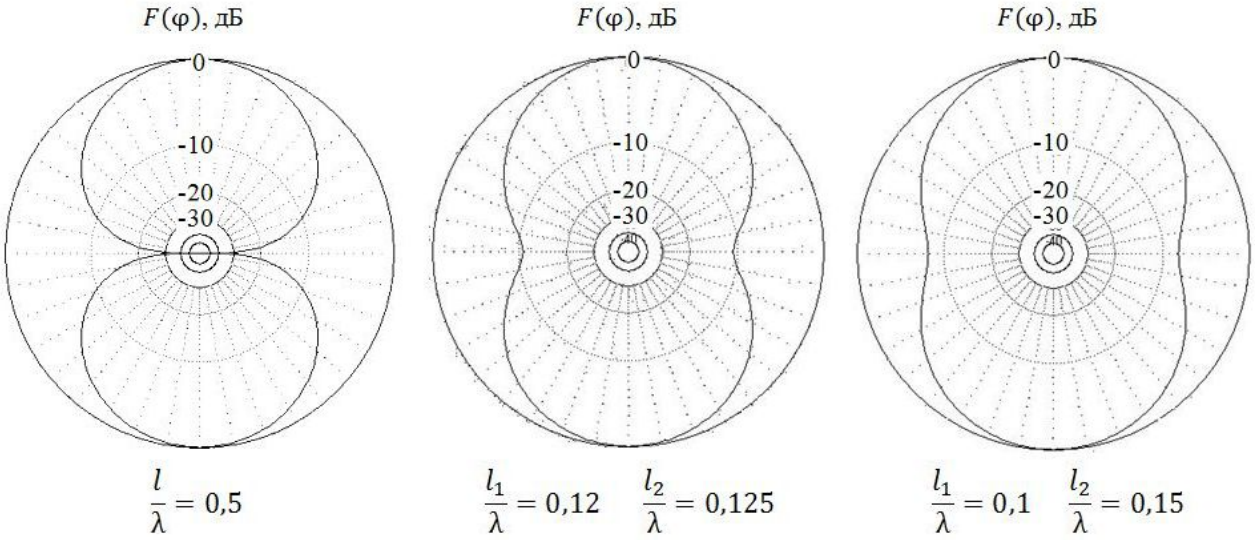


Рис. 3

Отримані результати наглядно показують, що П-подібний симетричний вібратор дозволяє в азимутальній площині формувати ненаправлене випромінювання з горизонтальною поляризацією і успішно може бути використаний в якості випромінюючого елемента в складі з антенною решіткою.

ЛІТЕРАТУРА

1. *Резников. Г. Б.* Самолетные антенны. – М., „Советское радио", 1962. – 455 с.
2. *MMANA* – компьютерное моделирование антен. – М., „РадиСофт", 2002. – 79 с.

к.т.н. Ільїнов М.Д. (ВІТІ НТУУ „КПІ”)
Шафранський О.П. (ВІТІ НТУУ „КПІ”)
Павлюк О.М. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ МЕТОДІВ РОЗРАХУНКІВ ЛІНІЙ РАДІОЗВ’ЯЗКУ З РУХОМИМИ ОБ’ЄКТАМИ

Розповсюдження радіохвиль на лініях зв’язку з рухомими об’єктами мають ряд особливостей котрі необхідно враховувати при їх проектуванні. При цьому характерні наступні явища: „втрати у вільному просторі”, поглинання, рефракція, дифракція, відбиття, багатопроменеве розповсюдження радіохвиль, допплерівський ефект, радіогоризонт та інші.

Моделювання впливів всіх факторів на поширення радіохвиль можна здійснити різними способами: детермінованими, статистичними і комбінованими.

Зазвичай, розрахунок здійснюється на основі різноманітних математичних моделей і методів, як правило емпіричних. Серед цих моделей, що знайшли широке застосування на практиці, найбільш поширені наступні: моделі прогнозування втрат: Альсбрука-Парсона, Окамури-Хата, Уолфіша-Ікегамі, Лі, Кся-Бертоні, Енглі, Бломквіста-Ладелла й ряд інших.

Проведемо короткий аналіз методів розрахунку ліній радіозв’язку з рухомими об’єктами, котрі зводяться до визначення множника ослаблення, тобто множника, що враховує особливості розповсюдження радіохвиль.

Найбільш проста та розповсюджена на практиці – *двопроменева модель розповсюдження радіохвиль над плоскою землею*

Модель дає змогу здійснити розрахунок напруженості поля E сигналу, що приймається антеною мобільної станції, з урахуванням впливу земної поверхні, як своєрідного екрану, при цьому розглядаються лише високо підняті, в порівняні з довжиною хвилі, антени рис. 1.

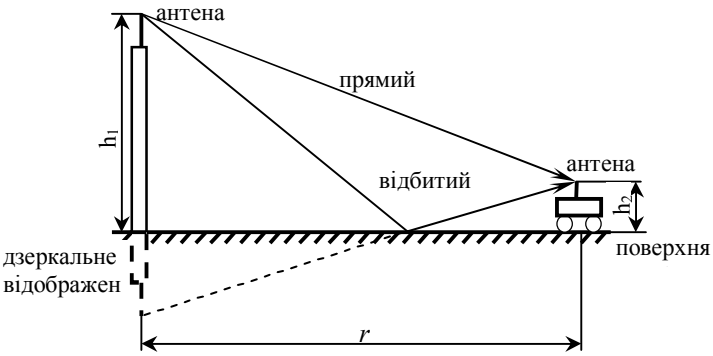


Рис. 1

В загальному випадку значення величина E є результатом взаємодії двох хвиль: прямої та відбитої, які розповсюджуються по прямому і відбитому напрямках. та розраховується за формулою:

$$E = \frac{\sqrt{30\,P_{A1}\,G_1}}{r}\sqrt{1 + R^2 + 2R\cos(k\Delta r - \varphi)},$$

де P_{A1} – потужність, що підводиться до антени БС;

G_1 – коефіцієнти підсилення антени БС; φ – різниця фаз між променями;

R – коефіцієнти відбиття (залежить від поляризації);

$\Delta r = \frac{2h_1h_1}{r}$ – геометрична різниця ходу хвиль;

r – відстань між передавачем та приймачем;

$F = \sqrt{1 + R^2 + 2R\cos(k\Delta r - \varphi)}$ – множник ослаблення.

Модель Альсбрука-Парсона дозволяє визначити основні втрати передачі в діапазоні (70 … 450) МГц у такий спосіб:

$$L = L_F + \left(\left(L_p - L_F \right)^2 + L_D{}^2 \right)^{1/2} + L_B + \gamma,$$

де: $L_F = (32{,}45 + 20\lg(f) + 20\lg(R))$ – втрати передачі у вільному просторі;

f – робоча частота, МГц; R – відстань між антенами БС та АС;

L_D – відстань дифракційні втрати, обумовлені характером місцевості;

L_p – втрати при поширені над плоскою землею;

Модель враховує втрати викликані наявністю міської забудови, дифракційні втрати, втрати передачі у вільному просторі. Недолік – обмежена смуга частот.

Модель Уолфіша-Ікегамі – визначає значення втрат передачі L_0, дБ за формулоюі:

$$L_0 = L_1 + L_2 + L_3,$$

де: $L_1 = 32{,}4 + 20\lg(Rf)$ – втрати при поширені у вільному просторі;

$L_2 = -16{,}9 - 10\lg(w) + 10\lg f(h_{d1} - h_2) + L_p$ – втрати за рахунок відбиття від будинків; L_3 – втрати за рахунок прилеглих будинків; $w = 10 \ldots 15$ *м* – ширина вулиці;

Ця модель визначає значення втрат передачі враховуючи втрати за рахунок відбиття від будинків, враховується ширена вулиці.

Модель Лі параметри моделі можуть бути просто скореговані за допомогою додаткових вимірів до конкретних умов поширення. Після проведення цієї процедури прогнозування рівня сигналу стає досить точним. Більше того, алгоритм прогнозування простий у застосуванні й легко обчислюється.

Дана модель дозволяє визначити потужність прийнятого сигналу в дБм що виражається співвідношенням:

$$P_{пер} = A - B\log(R) - n\log\left(\frac{f}{900}\right) + 10\log(\alpha),$$

де параметри A и B залежать від характеристик навколишнього середовища й були визначені статистично по вимірах у ряді міст. Для великих міст A = 55 ... 80, B = 30 ... 43. Для пригородів A = 54, B = 39. Множник n = 2 для пригородів і для діапазону f < 450 МГц; n = 3 для міст і для f < 450 МГц; – параметр, котрий враховує технічний фактор радіо лінії, а також вносить технічні характеристики антен базової – мобільної станції.

Модель Кся-Бертоні дозволяє врахувати ряд додаткових параметрів, пов’язаних з поверховістю будівель, шириною вулиць та ін. Дана модель являє собою дифракційну аналітичну модель, розроблену для розрахунків загасань на трасах систем рухомого радіозв’язку в міських та приміських зонах. На відміну від статистичної моделі вона дозволяє вести розрахунки в більш широкому діапазоні частот (до 2200 МГц).

Модель Кся-Бертоні дозволяє оцінити середній рівень втрат і в тих випадках, коли антена БС розташована на рівні дахів або нижче рівня дахів (такі прийоми використовують, коли необхідно „засвітити” обмежену локальну область.

Таким чином, розрахунок лінії радіозвязку з рухомими об’єктами є досить складною задачею. Зазвичай розрахунок здійснюється на основі складних емпіричних моделей і методів котрі детально описані в даній роботі.

ЛІТЕРАТУРА

1. *Міночкін А.І.* Перспективи побудови тактичних мереж зв’язку. Науково-практична конференція ВІТІ „Пріорітетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення” / Міночкін А.І., Романюк В.А. – К.: ВІТІ НТУУ „КПІ”, 2006.

2. *Бузов А.Л.* УКВ антенны для радиосвязи с подвижными объектами радиовещания и телевидения / Бузов А. Л. – М.: Радио и связь, 1997. – 350 с.

Іщенко О.М. (ЦНДІ ЗСУ)
Петросян І.А.(НЦЗІ ВІТІ НТУУ „КПІ”)

МОДЕЛЮВАННЯ КАНАЛІВ ЗВ'ЯЗКУ ДЛЯ HAPS СИСТЕМ

В світі активно набувають популярності HAPS (high altitude platform stations) системи зв’язку, тобто системи зв’язку на базі надвисотних аероплатформ. Відомо, що одним з основних питань при проектуванні систем зв’язку є забезпечення якості обслуговування відповідно до вимог користувачів. Ключовим моментом тут є якість каналу зв’язку. Як правило, канал зв’язку нестабільний, і щоб оцінити можливі втрати в каналі, необхідно розглянути всі фактори, що впливають на сигнал.

Можна виділити два підходи до моделювання каналів HAPS каналів зв’язку: геометричний та статистичний. Сутність геометричного підходу полягає в тому, що він використовує залежність між місцем розміщенням приймача (на Землі або на HAPS) та характеристиками каналу. При цьому фундаментальні параметри, що описують систему, це кут місця, висота платформи та віддалення користувача від проекції точки стояння платформи. Завдяки даному підходу можна розрахувати діаметр зони покриття та встановити залежність якості каналу від висоти платформи та кута місця.

Сутність статистичного підходу полягає у застосуванні статистичних характеристик каналу, наприклад функції щільності ймовірності огинаючої сигналу в каналі. Результати моделювання показують, що при зміні зони покриття, функція щільності ймовірності також буде змінюватись.

Моделювання HAPS каналів зв’язку доцільно проводити для частот до 10 ГГц і після 10 ГГц. Сьогодні в світі телекомунікаційні сервіси базуються на широкосмуговій цифровій передачі, і користувачі вимагають збільшення смуги частот. Розвиток моделей широкосмугових каналів став суттєвим для оцінки HAPS систем, тому що їх мета – надання саме широкосмугових сервісів.

Як показує аналіз, основними ефектами розповсюдження радіохвиль у HAPS системах зв’язку будуть: втрати у вільному просторі, багатопроменевість, гідрометеорні послаблення, поглинання газами, сцинтиляція [1, 2].

Для частот більших 10 ГГц ефектом багатопроменевості можна зневажити, а канал вважати вузькосмуговим. В даному випадку необхідно зосередитися на метеорологічних ефектах [2].

Із трьох частотних смуг, виділених для HAPS, смуга до 2,1 ГГц найбільш страждає від багатопроменевості.

HAPS системи, що працюють у смугах 27-31 і 47-49 ГГц, будуть суттєво страждати від гідрометеорних послаблень.

Поглинання газами серйозно ускладнюють використання смуги 57-64 ГГц для HAPS систем.

Сцинтиляція вище на високих частотах, при невеликих кутах місця. Вона також вище влітку чим узимку – хмарні умови роблять більшу сцинтиляцію, чим безхмарне небо.

Для кута місця у діапазоні 30-90º виявляється найкраща якість каналу, тому саме в цій зоні бажано розміщувати наземні станції.

Наведені вище дані доцільно використовувати при проектуванні HAPS систем зв’язку.

ЛІТЕРАТУРА

1. *International* Telecommunication Union, ITU-R Propagation Recommendation P.676 – 3: Attenuation by Atmospheric Gases, Geneva, 1997.

2. *International* Telecommunication Union, ITU-R Propagation Recommendation P.838: Specific Attenuation Model for Rain for Use in Prediction Methods, Geneva, 1992.

Кадет Н.П. (НАУ)
Зацаріцин О.О. (ЦНДІ ОВТ ЗС України)

ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БОРОТЬБИ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Новим явищем воєнного протистояння й ведення бойових дій будь-якими групами держав стає їх інформаційно-психологічне протиборство, сутність якого полягає в зосередженні головних зусиль збройної боротьби не на фізичному знищенні конкретних одиниць зброї, а на руйнуванні інформаційних ресурсів держави-ворога і її збройних сил, руйнуванні або спотворенні системи управління ними, каналів обміну інформацією, навігації і наведення, механізмів впливу на індивідуальну і суспільну свідомість. Нові концепції ведення війни передбачають комплексну боротьбу в трьох сферах: фізичній, ментальній і моральній. Досвід сучасних локальних війн свідчить про значне зростання ментального і морального факторів. Сучасні погляди на організацію та ведення інформаційної боротьби полягають у комплексному використанні різнорідних засобів для досягнення інформаційної переваги над противником. Інформаційна зброя, як і інформаційна боротьба, з розвитком суспільства та інформаційних технологій набули відповідних змін. Аналіз досвіду сучасних локальних війн та збройних конфліктів дозволяє визначити основні тенденції розвитку інформаційної зброї і, відповідно, форм і способів ведення інформаційної боротьби. Розвиток інформаційної зброї неминуче призведе до того, що в майбутньому виникнуть інформаційні війни, які будуть вестись у інформаційному просторі та в основному інформаційними засобами.

Таким чином, інформаційна боротьба змінює не тільки форми і способи ведення воєнних дій, змінюється зміст самого поняття війни, стираються межі між воєнним і мирним часом, змінюється поняття „театр воєнних дій", ще більш зрощуються воєнні і мирні технології. При комплексному використанні засобів C^4 та ISR формується інтегрована система C^4ISR. Мережа C^4ISR встановлює зв'язок у глобальних масштабах з гнучкими мережними службами, які здатні швидко перебудувати свою конфігурацію з метою створення необхідних умов для автоматизованого доступу єдиного користувача в жорстких умовах обміну інформацією й отримання гарантованих послуг. Ці служби будуть також забезпечувати функціонування гнучких командних структур, призначених для вирішення окремих пріоритетних короткотермінових задач, зокрема, для створення інтегрованої системи „датчик–система зброї" та її ефективного функціонування. Послуги системи C^4ISR концептуально відокремлені від структур, які передають інформацію про обстановку на полі бою користувачам у випадках, коли необхідно форсувати спільне планування й проведення єдиних операцій, а також операцій, які здійснюються коаліційними силами.

Інформаційна війна – це відносно нова сфера ведення спільних бойових дій, яка інтегрована в усі три сфери бойових можливостей, пов'язаних з інформаційною перевагою провідних країн світу. На найближчу перспективу передбачається: включення до мережі Інтернет учасників бойових дій на тактичному рівні; вдосконалення заходів забезпечення безпеки і надійності функціонування розподілу баз даних; розробка вдосконалених методів захисту інформації. Плани середньострокової перспективи передбачають вдосконалення: інформаційних каналів, які використовують переваги смуги пропускання ВЧ діапазону; ліній передач даних із засобами кодування для учасників бойових дій, які підключені до мережі „Інтернет" і забезпечені різними рівнями інформаційної безпеки; комплектів засобів планування й моделювання операцій в інформаційній війні.

Успішна розробка в рамках цих планів відповідних технологічних програм дозволить створити інформаційну систему, здатну своєчасно надавати користувачу необхідну інформацію, забезпечивши її безпеку і цілісність. Адаптована автоматизована комплексна інфраструктура інформаційної системи США і засоби захисту баз даних будуть сумісні з аналогічними системами і службами союзних сил.

Каравацький В.О. (в/ч А1906)
Яценко О.А. (ВІТІ НТУУ „КПІ”)

ОСНОВНІ ВИМОГИ ДО ПОБУДОВИ СУЧАСНОГО ЦЕНТРАЛЬНОГО ПУЛЬТА УПРАВЛІННЯ СТАЦІОНАРНОГО ВУЗЛА РАДІОЗВ’ЯЗКУ

Сучасний рівень розвитку збройної боротьби потребує постійного вдосконалення систем зв’язку військового призначення. При цьому невід’ємною складовою таких комплексних систем є засоби радіозв’язку та апаратура управління радіовузлів, до яких висуваються високі вимоги щодо надійності, ефективності, якості прийому, передачі та швидкості проходження інформації по елементах радіовузла, енергоспоживання тощо. При цьому важливу роль відіграє кваліфікація усіх спеціалістів радіовузла.

В зв’язку з цим при побудові сучасного центрального пульта управління стаціонарного вузла радіозв’язку потрібно враховувати деякі особливості [1, 2], а саме:

– місце розташування апаратної управління радіовузла (рівновіддалена від основних апаратних радіовузла);

– система життєзабезпечення (весь комплекс в цілому);

– система зв’язку радіовузла (лінії та канали проходження інформації);

– система управління радіовузлом (лінії управління та команд);

– система автоматизації радіовузла (обладнання засобами зв’язку та автоматизації спеціального призначення, автоматизованими робочими місцями (АРМ, ПЕОМ тощо).

Виходячи з цього переліку, а також в залежності від призначення радіовузла висуваються основні вимоги до пульта управління:

– відповідність вимогам ергономіки;

– використання модульно-блочного принципу побудови;

– забезпечення підключення апаратури як нового так і старого парку;

– можливість гарячої заміни блоків (без відключення всього пульта);

– наявність резервування ліній зв’язку;

– наявність резервування ліній управління (за необхідності);

– наявність засобів відображення оперативної інформації;

– наявність вбудованих засобів автоматизації з можливістю подальшої модернізації;

– наявність вбудованої системи контролю стану апаратури та каналів зв’язку;

– наявність не менше двох видів комутаційних засобів, один з яких може бути використаний вручну (або один засіб, який дозволяє проводити комутацію автоматичну (напівавтоматичну) та ручну);

– резервування системи електроживлення (обов’язково);

– наявність додаткових вторинних засобів електроживлення для спецапаратури, яка використовується на радіовузлі;

– наявність аварійно-захисних систем.

Наведені у доповіді положення у сукупності дають можливість повно та обґрунтовано визначити вимоги до сучасного центрального пульта управління стаціонарного вузла радіозв’язку та в спрощеному варіанті можуть бути використані при побудові систем управління польових вузлів зв’язку.

ЛІТЕРАТУРА

1. *Посібник офіцера* – зв’язківця / Під редакцією Д.Т. Примака – Київ: ВІТІ НТУУ „КПІ”, 2002. – 144 с.

2. *Лисенко І.В.* Організація та засоби зв’язку. – Ч. 1. організація та експлуатація засобів зв’язку тактичної ланки управління. – Житомир: ЖВІРЕ. – 1998. – 76 с.

Карловський І.В. (ВІТІ НТУУ „КПІ”)
Штаненко С.С. (ВІТІ НТУУ „КПІ”)

ЗАСТОСУВАННЯ НЕЙРОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

У даний час спостерігається могутнє зростання і розвиток телекомунікаційних засобів і систем, розширення спектра послуг, зростання числа компаній, що займаються проектуванням і експлуатацією мереж і систем телекомунікацій. Для досягнення глобальної доступності, реалізації вимог ринку інформаційних послуг, потрібна така архітектура мережі, яка б змогла поєднати існуюче устаткування з новітніми технологіями [1]. Нейронні мережі, розробка яких була почата ще в середині XX століття, можуть привести до нового витка інформатизації людства.

Теорія нейронних мереж (НМ) є напрямом науки, що активно розвивається. Основні перспективи використання цієї теорії пов’язані з рішенням складних практичних задач. Широкий круг завдань, які вирішуються нейронною мережею, не дозволяє в даний час створювати універсальні, могутні мережі, але дає можливість розробляти спеціалізовані НМ, що функціонують за різними алгоритмами [2].

Висока ефективність нейроінформаційних технологій при рішенні задач адаптивного управління може вже найближчим часом зробити їх незамінними при створенні нових поколінь мереж мобільного зв’язку та інших бездротових мереж (нейронних, сенсорних). Актуальність досліджень нейронних мереж підтверджується різноманіттям їх можливого застосування.

Представлення моделі телекомунікаційної мережі у вигляді нейромережевих ансамблів обумовлене рядом унікальних властивостей нейромережі це: паралельність розповсюдження активності по мережі, що забезпечує можливість функціонування мережі в масштабі часі, близькому до реального; агрегативна розподіленість – визначає здатність зберігання фрагментів знань в декількох вузлах мережі; асоціативність, тобто здатність НМ відновлювати інформацію, що зберігається в ній, за наявною частковою (фрагментарною) інформацією; здібність НМ до навчання і самонавчання, що є основною її „інтелектуальною” властивістю; надійність – вихід з ладу більше 10 % її елементів не приводить до відмов у роботі всієї мережі. Сукупність перерахованих властивостей НМ об’єктивно можуть служити основою для побудови нового покоління високоефективних телекомунікаційних систем як загального так і спеціального призначення.

Область застосування НМ у телекомунікаційних системах постійно розширюється, існує велика кількості напрямків її застосування: управління комутацією, маршрутизація, управління трафіком, розподіл каналів у рухомих системах радіозв’язку тощо. Перспективним напрямом є використання нейромережних алгоритмів у завданнях кодування і декодування інформації [3], про що свідчить досвід Західної Європи та США, де нейроінформаційні технології є достатню розповсюдженими.

У цих умовах поява на ринку України недорогих як багатофункціональних, так і орієнтованих на рішення конкретних завдань нейрочіпів та нейрокомп’ютерів буде сприяти швидкому переходу до чергового етапу розвитку телекомунікаційних систем – появи інтелектуальних телекомунікаційних систем.

ЛІТЕРАТУРА

1. *Стеклов В.К., Костік Б.Я., Беркман Л.Н.* Сучасні системи управління в телекомунікаціях. – К.: Техника, 2005. – 390 с.

2. *Комашинский В.И., Смирнов Д.А.* Нейронные сети и их применение в системах управления и связи. М.: Горячая линия – Телеком. 2002. – 94 с.

3. *Галушкин А. И.* Теория нейронных сетей. – М: ИПРЖР, 2000. – 416 с.

Кіруша К.С. (НТУУ ВІТІ „КПІ”)

КОНВЕРГЕНЦІЯ СТІЛЬНИКОВИХ МЕРЕЖ НА ОСНОВІ ТЕХНОЛОГІЇ NGN-SOFTSWITCH

Зараз існує ситуація, коли постійно з'являються нові технології мобільного радіодоступу, але при цьому є одна надзвичайно важлива проблема: наступний стандарт не сумісний з попереднім, тому побудова конвергентної мережі в якій широкий спектр послуг, включаючи передачу голосу і даних, надаватиметься на єдиній технологічній основі комутації пакетів є дуже важливим питанням. Телефонний зв'язок вже зараз є одним з багатьох додатків, доступних для IP. Розгортання технологій широкосмугового і безпровідного зв'язку тільки прискорить тенденцію загального переходу до вищезгаданого протоколу. Проаналізувавши принципи побудови кількох мереж стільникового зв’язку можна зробити висновок що найдоцільніше використовувати в якості мережі доступу мережу побудовану на основі технології WiMAX.

По замовчуванню обирається пріоритетна мережа доступу, покриття якою в даного оператора є найрозвиненішим. Через цю мережу Softswitch постійно відслідковує статус абонента. Коли абонент реєструється в мережі, йому автоматично надається сервісна точка доступу до всіх мереж доступу, передбачених його контрактом з оператором. Відповідно до того сервісу, який потрібний абоненту, тобто, відповідно до необхідного QoS, Softswitch обере оптимальну мережу.

Постає питання: яким чином відстежувати єдиний термінал? Проблемою є відсутність спільної платформи існуючих мереж доступу. Найкращим рішенням на даний час є відслідковування абонента по GSM-терміналу, так як відповідна мережа має найкраще покриття. Перехід до NGN пов’язаний із введенням в експлуатацію великої кількості нового обладнання, а це потребує істотних матеріальних затрат. Тому зрозуміло, що миттєвий перехід економічно невигідний. З цієї причини побудову конвергентної мережі пропонується проводити в 3 етапи.

Перший етап (встановлення функціональних модулів): заміна базових частин мереж доступу на єдину базову мережу, побудовану за технологією NGN-Softswitch; декомпозиція SoftSwitch; перехід до IP-мереж на транспортному рівні; HLR (Home Location Register), VLR (Visitor Location Register) – необхідні для процедури „хендоверу”; єдиний біллінг-сервер, який відповідає за тарифікацію всіх послуг для даного єдиного терміналу.

Другий етап: декомпозиція шлюза: розподіл функцій перетворення канальної інформації в пакетну та виділення і трансформації сигнальної інформації.

Третій етап: виділення точок доступу до мереж і єдиної точки доступу до сервісу; формування ідеології єдиного терміналу; керування сеансом зв’язку, виходячи з QoS.

Таким чином дана концепція переходу до NGN надає можливість побудови конвергентної мережі, яка дозволить без зміни її базової частини забезпечувати абоненту будь-які можливі послуги з відповідним QoS. Основоположним елементом архітектури конвергентної мережі є гнучкий програмний комутатор Softswitch. Softswitch є ідеологією мережі, носієм її інтелектуальних можливостей. В першу чергу, він керує обслуговуванням викликів, тобто встановленням з’єднань і роз’єднань, виконуючи функції Call Agent. Таким чином, Softswitch фактично залишається все тим же звичним комутаційним вузлом, тільки без цифрового комутаційного поля, кросу і т.д. Інший термін – контролер транспортного шлюзу MGC – є синонімом Softswitch і підкреслює той факт, що він керує транспортними шлюзами і шлюзами доступу по протоколу H.248.

к.т.н. Климович О.К. (ВІТІ НТУУ „КПІ”)
Саєнко О.Г. (ВІТІ НТУУ „КПІ”)
Данько В.О. (ВІТІ НТУУ „КПІ”)

МЕХАНІЗМИ РЕАЛІЗАЦІЇ СЕРВІСУ ЗАХИЩЕНИХ ВІРТУАЛЬНИХ МЕРЕЖ В КОМП’ЮТЕРНІЙ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Останнім часом при використанні комп’ютерних мереж військового призначення з’являються все нові завдання збереження конфіденційності, цілісності, доступності та захищеності інформації від зловмисників. Найбільш надійний захист інформації в автоматизованих системах та мережах різноманітних класів можливо забезпечити тільки за допомогою системного підходу та застосування комплексних систем захисту інформації. Він передбачає, що рішення завдання повинне досягатися за рахунок використання сукупності організаційних та організаційно-технічних заходів, а також криптографічних систем і засобів. Системний підхід орієнтований на створення комплексної системи захисту інформації та використання апаратно-програмних комплексів захисту інформації у мережах та системах.

Метою дослідження є проектування комп’ютерної мережі військового призначення за рахунок реалізації сервісу захищених віртуальних мереж. Розглядаються проблеми захисту сучасних локальних обчислювальних мереж, загрози їх безпеки, технології оцінки вразливостей систем і захисту від несанкціонованого доступу за допомогою застосування технології захищених віртуальних мереж [1-6]. Пропонується схемна реалізація технології захищених віртуальних мереж в комп’ютерній мережі військового призначення. Проводиться оцінка доцільності її використання.

За результатами розгляду комплексної системи захисту інформації в комп’ютерній мережі військового призначення та аналітичного огляду і вибору мережних технологій розроблена структура віртуальної приватної мережі, а також структури всіх підмереж, що входять до її складу. Проведений розрахунок кількості мереженого обладнання, вибору його типу і виробника, а також розглянутих принципів організації внутрішньомережної й міжмережної взаємодії, розроблена функціональна схема віртуальної приватної мережі. Опираючись на результати вибору апаратних засобів корпоративної мережі, наведено економічне обґрунтування.

Таким чином, розроблені пропозиції щодо можливих напрямків вдосконалення комплексної системи захисту інформації в комп’ютерній мережі військового призначення за рахунок реалізації сервісу захищених віртуальних мереж. Запропоновано рекомендації щодо захисту інформації в інформаційних системах, а також способи технічного захисту інформації з обмеженим доступом від витоку по технічних каналах витоку інформації.

ЛІТЕРАТУРА

1. Антонов В.М. Пермянов О.Ю. Комп’ютерні мережі військового призначення. – К.: „МК-Пресс”, 2005.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО „ТИД ДС”, 2001. – 688 с.

3. Завгородний В.И. Комплексная защита информации в компьютерных системах. – М.: Логос, 2001. – 264 с.

4. Норткат С., Новак Д. Обнаружение нарушений безопасности в сетях. 3-е изд. – М.: Издательский дом „Вильямс”, 2003. – 448 с.

5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.

6. Симонов С. Технологии и инструментарий для управления рисками // Jet Info. – М., 2003. – № 2 (117).– С. 7–17.

Коваленко А.О. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМИ ПОШУКУ КВАДРАТНИХ КОРНІВ В ПОЛЯХ ГАЛУА

Проблема пошуку коренів в раціональному полі чисел є однією з найбільш цікавих для науковців в області чисельних наук та криптографії зокрема. Ряд останніх стандартів криптографічної захисту інформації базується на основі перетворення в групі точок еліптичної кривої. Однією з центральних операцій в стандартизованих криптографічних примітивах є операція генерації випадкових точок кривої, і, як наслідок, операції пошуку коренів рівняння еліптичної кривої в полі цілих чисел. Обчислювальна складність цієї операції впливає на обчислювальну складність криптографічного перетворення в цілому. В даній роботі представлені результати досліджень обчислювальної складності алгоритмів пошуку коренів рівняння еліптичної кривої при генерації випадкових точок.

Розглянемо три варіанти генерації точок еліптичної кривої в полях Галуа зі стандарту ГОСТ Р 34.10-2001:

$$y^2=(x^3 + Ax + B) \bmod P \quad (1)$$

де A і B — коефіцієнти еліптичної кривої $A, B \in GF(p)$

Для отримання точки необхідно згенерувати випадково одну з будь-яких координат X або Y, а іншу отримати з рівняння 1. Враховуючи, що обчислення Y при відомому X більш простіше, то будемо генерувати саме X, а Y знаходити за формулою:

$$Y = \sqrt{x^3 + Ax + B} \bmod p$$

Було розглянуто 3 варіанти визначення числа Y, враховуючи, що вираз під коренем не може бути вищим за p^2.

Алгоритм 1.

1. $W = x^3 + Ax + B$;
2. Перевірити, чи виконується $Y = \sqrt{W}$, якщо так – „$Y = \sqrt{W}$”, вийти з циклу;
3. Якщо $W > (p-1)^2$, то „Y не існує” – вийти з алгоритму, інакше $W = W + p$ – іти на крок 2.

Алгоритм 2.

1. $W = x^3 + Ax + B$;
2. Перевірит, чи виконується $Y = \sqrt{W}$, якщо так – „$Y = \sqrt{W}$”, вийти за алгоритму;
3. Якщо $W > \left(\frac{p-1}{2}\right)^2$, то „$Y$ не існує” – вийти з алгоритму, інакше $W = W + p$ – іти на крок 2.

Алгоритм 3 (комбінований).

1. $W = x^3 + Ax + B$;
2. $Y = 1$;
3. Якщо виконується $Y^2 \bmod p = W$, то – ”$Y = \sqrt{W}$“ і вийти з алгоритму;
4. Якщо $Y > \left(\frac{p-1}{2}\right)$, то „$Y$ не існує” – вийти з алгоритму, інакше $Y++$, іти на крок 3.

На основі проведених дослідів при генерації точок вказаної еліптичної кривої довжиною від 14 до 22 біт можна зробити висновок, що серед представлених методів найбільш ефективним є третій алгоритм. На рис. 1–2 представлені порівняльні оцінки обчислювальної складності розглянутих алгоритмів.

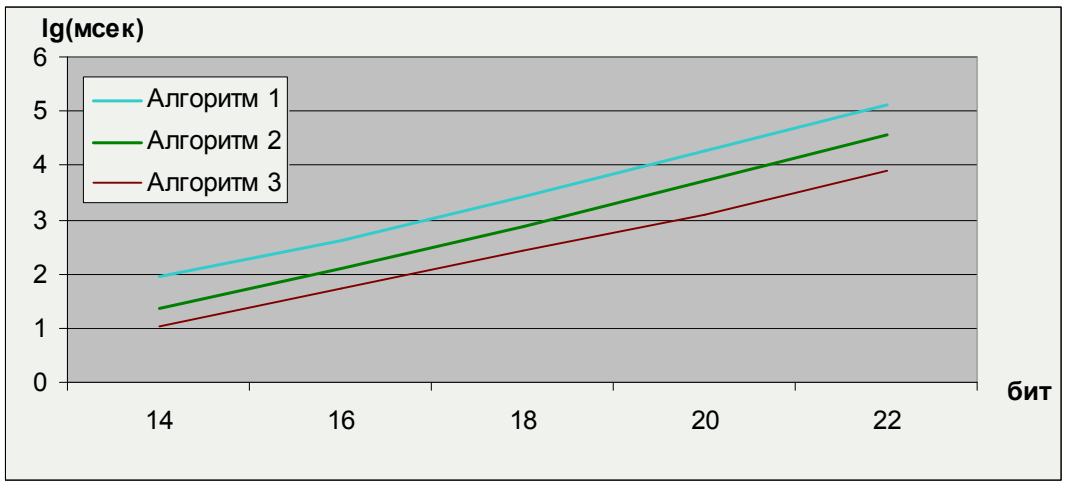


Рис. 1. Середній час генерації точки кривої кожним з алгоритмів для заданої довжини біт (логарифмічна залежність)

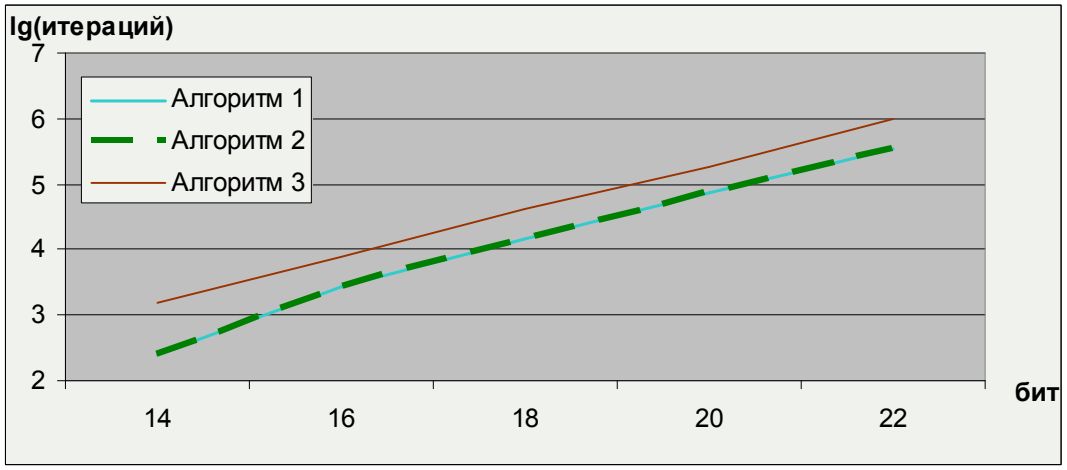


Рис. 2. Середня кількість ітерації кожного з алгоритмів при генерації однієї точки кривої заданої довжини біт (логарифмічна залежність)

Всі досліди та обчислення проводилися з використанням бібліотеки для роботи з великими числами Девіда Ірланда (David Ireland) з D.I. Management Services Pty Limited версії 2.1.0 від 23 серпня 2006. В якості обчислювальної машини було використано PC-сумісна ЕОМ на базі процесора Centrino T5670 с тактовою частотою 1.6 ГГц.

Крім того, було проведено дослідження, що дозволяють оцінити максимально ефективний спосіб підведення до квадрату по модулю великих чисел засобами даної бібліотеки. Найбільш ефективним виявились два методи:

1) використання функції ModExp – підведення до другого ступеню і взяття по модулю;

2) використання функції Sqr з наступним взяттям результату по заданому модулю.

Використання функцій множення за модулем, підведення до квадрату за модулем та множення числа само на себе виявились менш ефективними.

Таким чином, в даній роботі було розглянуто алгоритми генерації точок еліптичної кривої. Отримано комбінований спосіб перевірки, а також найбільш ефективний спосіб підведення до квадрату за модулем, що дозволяє скоротити обчислювальні затрати від 1.5 до 2 *O(log)* разів, що в свою чергу підвищує ефективність системи електронного цифрового підпису.

Коваленко І.Г. (ВІТІ НТУУ „КПІ”)

ЕНЕРГОЗБЕРІГАЮЧІ МЕТОДИ МНОЖИННОГО ДОСТУПУ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ

Перспективна мобільна компонента тактичних мереж зв’язку буде включати безпровідні сенсорні мережі (БСМ), що складаються з маленьких сенсорних вузлів з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних [1]. Основними елементами сенсорних вузлів є: датчики контролю зовнішнього середовища, мікрокомп’ютер, батареї, прийомопередавач.

Вузли БСМ повинні швидко адаптуватися до частих змін топології мережі, трафіка та ефективно використовувати обмежені мережеві ресурси. Продуктивність та ефективність БСМ прямо пропорційна механізмам множинного доступу (МД) до радіо ресурсів [2].

Методи МД в БСМ мобільної компоненти тактичних мереж зв’язку повинні відповідати наступним вимогам: децентралізоване функціонування, енергозберігання, великий час „життя” мережі, достатня пропускна здатність, малий час затримки передачі, мобільність, масштабування, адаптування до зміни щільності та кількості вузлів, протидія засобам радіоелектронної боротьбі (РЕБ), передача неоднорідного и пріоритетного трафіка, управління чергою передач тощо.

Характерними вимогами до БСМ є мінімізація витрат енергетичних ресурсів вузлів та максимізація часу „життя” мережі. Реалізації цих вимог заважають наступні фактори:

– пасивне прослуховування: на прослуховування та очікування прийму витрачається приблизно стільки ж енергоресурсів, скільки й на, безпосередньо, прийом пакетів;

– колізії, які передбачають додаткові передачі пакетів;

– „підслуховування”, коли вузли приймають пакети, які їм не адресовані;

– витрати протоколів більш високого рівня на передачу службової інформації, які в БСМ можуть досягати 70 % глобального трафіка [3];

– передача пакетів в час, коли вузол-адресат не готовий до прийому: при цьому здійснюються повторні передачі;

– розмір пакетів: з одного боку, при передачі пакетів малого розміру витрачається більше енергії на передачу службової інформації (заголовків пакетів тощо), з іншого – передача великих пакетів потребує більше енергії;

– флуктуації трафіка: різке збільшення глобального трафіку в мережі може призвести до значного збільшення кількості колізій.

Крім того, вимоги до методів МД з енергозберігання конкурують з вимогами продуктивності та ефективності передачі інформаційних потоків в мережі. Самим ефективним заходом зменшення використання енергоресурсу вузлів мережі це мінімізація кількості повторних передач пакетів та часу знаходження вузлів в режимі прослуховування каналу, що, автоматично, збільшує затримки доставки пакетів в мережі.

Сладність знаходження балансу між ефективністью енергозберігання та продуктивності передачі інформаційних потоків призвело до розробки ряду методів МД. Класифікація методів МД в БМС за напрямом реалізації енергозберігаючих функцій представлена на рис 1.

Методи МД без планування (випадкові) прості в реалізації, масштабовані та адаптовані до зміни топології мережі, але піддані всім вказаним вище факторам, що заважають ефективному енергозбереганню. Ці методи базуються на CSMA або CSMA/CA і використовуються в мережах невеликої розмірності без жорстких вимог з енергоефективності та продуктивності. Приклади:TEEM, UMAC, BMAC, PAMAS, CC-MAC, SIFT, AlertMAC, STEM, SynhWUF, TISER, RISER [4–6].

Методи з плануванням мінімізують вплив основних факторів, що заважають ефективному енергозбереганню, але більш складні в реалізації, потребують складних механізмів синхронізації вузлів, масштабування та адаптації до зміни топології мережі. Дані методи використовуються в мережах великої розмірності та інтенсивного трафіку. Приклади:

S-MAC, DMAC, T-MAC, E-MAC, LMAC, A-MAC, DSMAC, MS-MAC, PMAC, ADCA, LEACH, NAMA, LAMA, PAMA; EE TDMA MAC [4 – 6].

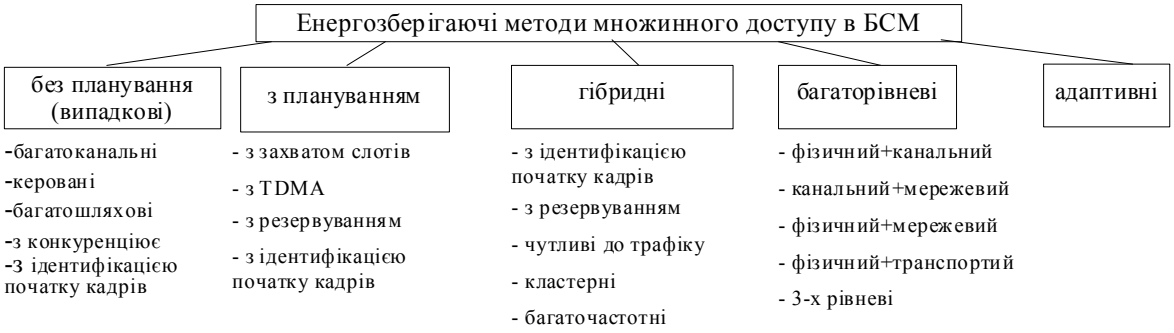


Рис.1 Класифікація методів доступу

Гібридні методи об'єднують переваги та зменшують вплив недоліків вищевказаних методів, більш складні в реалізації та ефективні для окремих типів топологій мереж. Приклади: ZMAC , GMAC, Wise MAC, TRAMA, HMAC, PARMAC, GANGS, MMSN, HyMAC, TMCP, Y-MAC[4-6].

В багаторівневих методах МД здійснюється взаємодія на різних рівнях моделі OSI, що дозволяє підтримувати баланс між енергозберіганням та продуктивністю мережі для підтримки QoS в залежності від характеристик інформаційних потоків. Приклади: MAC-CROSS, Q-MAC, EQ-MAC, CoCo.

Аналіз існуючих протоколів показав, що єдиного універсального методу МД для БСМ на даний час не існує. Результати моделювання для мереж різної розмірності, інтенсивності трафіку та його обсягу не дають однозначної переваги окремих методів [4]. Крім того, для мереж зв'язку тактичної ланки управління висуваються особливі вимоги зі стійкості, безпеки та прихованості. Розглянуті вище методи не відповідають цим вимогам і не можуть використовуватись для побудови БСМ тактичної ланки управління.

Тому актуальною є задача розробки нових методів МД в БСМ тактичної ланки управління, які повинні забезпечувати зберігання енергетичних ресурсів вузлів при забезпеченні заданої якості (QoS) передачі інформаційних потоків та адаптуватись до умов функціонування мережі. Дані методи пропонується розробляти з організацією взаємодії між вузлами БСМ на різних рівнях моделі OSI та використанням методів управління в умовах невизначеності [7].

ЛІТЕРАТУРА

1. *Міночкін А.І, Романюк В.А.,* Жук О.В. Перспективи розвитку тактичних сенсорних мереж // Збірник наукових праць № 4. – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 112 – 119.

2. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв'язок. – 2004. – № 2. – С. 46 – 50. http://viti.kpi.ua/Articles/rva/rva_2004_46.pdf.

3. *I. Rhee et al.,* „Z-MAC: a Hybrid MAC for Wireless Sensor Networks". ACM SenSys, San Diego, CA, Nov. 2005.

4. *Li De-liang* Peng Fei, „Energy-efficient MAC protocols for Wirel Sensor Networks", INFORMATION AND COMMUNICATIONS TECHNOLOGIES, Beihang University, Beijing,100083, 2009.

5. *Bashir Yahya,* Jalel Ben-Othman, „Towards a classification of energy aware MAC protocols for wireless sensor networks", „Wireless Communications and Mobile Computing", 2009, №9, pp 1572 – 1607.

6. *L.Chaari, L.Kamoun,* „Wireless sensors networks MAC protocols analysis, Journal of Telecommunications", volume 2, ISSUE 1, 2010.

7. *Герасимов Б.М.,* Дивидинюк М.М., Субач И.Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности. – Севастополь: СНИЯЭиП, 2004. – 320 с.

Ковбасюк Д.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаїнов П.В. (ВІТІ НТУУ „КПІ”)

МУЛЬТИАГЕНТНИЙ ПІДХІД ДО ВИЯВЛЕННЯ АТАК МЕРЕЖЕВОГО РІВНЯ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

У зв’язку з актуальністю питань інформаційної безпеки в сучасних розподілених комп’ютеризованих системах та мережах, а також розуміючи їх значний масштаб, важливим напрямком науково-практичних досліджень є розробка підходів до побудови систем виявлення атак (СВА).

Аналіз джерел свідчить, що найбільш ефективними СВА є ті, що використовують інтелектуальні алгоритми аналізу інформації. Крім того, такі системи мають бути масштабовані і пристосовані до різноманітних змін параметрів процесу, що спостерігається.

Виходячи з цього, пропонується результат дослідження мультиагентного підходу для побудови СВА, що має вигляд системи взаємодіючих агентів, які скоординовані загальною глобальною ціллю (стратегією), але достатньо автономних, щоб реалізувати свої завдання у рамках загальної стратегії. В якості засобів аналізу інформації використано комбінацію різних за архітектурою штучних нейронних мереж у складі: агента вузла, агента мережі, сервера централізованої обробки з інтерфейсом взаємодії з користувачем.

Агент вузла призначений для моніторингу подій безпеки вузла мережі з забезпеченням вирішення наступних завдань:

– моніторинг трафіку, що проходить через мережевий інтерфейс даного вузла;

– попередній аналіз інформації на виявлення аномальної діяльності, що не характерна для даного вузла мережі, за допомогою автономної штучної нейронної мережі (персептрон) з сигмоїдальною активаційною функцією, та навченою під аналіз діяльності конкретного вузла;

– передачу агрегованих даних до бази даних серверу обробки для подальшого аналізу.

Агент мережі призначений для виявлення подій безпеки на основі моніторингу вхідного і вихідного трафіку мережі та вирішення наступних завдань:

– моніторинг вхідного та вихідного трафіку мережі;

– аналіз даних моніторингу автономною нейронною мережею, завдання якої є виявлення аномальної діяльності, що не характерна для даної мережі. Архітектура нейронної мережі – трьохрівневий персептрон;

– аналіз трафіку на відповідність відомим сигнатурам атак за методом бінарного пошуку в базі сигнатур;

– передачу агрегованих даних у базу даних серверу обробки для подальшого аналізу.

Сервер обробки призначений для виявлення подій безпеки шляхом обробки первинних даних отриманих від агентів вузла та мережі. На сервер обробки покладаються такі завдання:

– аналіз первинних даних, отриманих від агентів на основі комбінації різних за архітектурою нейронних мереж (багатошаровий персептрон, рецеркулярна нейронна мережа);

– інтерфейс взаємодії з адміністратором безпеки, що реалізовує навчання нейронних мереж.

Таким чином, використання мультиагентної схеми побудови системи у поєднанні з позитивними рисами обробки даних на основі штучних нейронних мереж дозволяє:

– розподілення завдань моніторингу та обробки інформації між багатьма агентами системи;

– впровадити інтелектуальну обробку, що адаптується до зміни параметрів об’єкта спостереження;

– масштабованість;

– можливе виявлення раніше невідомих атак на основі аналізу аномальної діяльності за рахунок використання автономних штучних нейронних мереж на рівні агентів.

к.т.н. Козубцов І.М. (ВІТІ НТУУ „КПІ”)

МЕТОД ВІРТУАЛЬНО-ПІЗНАВАЛЬНОГО ПРЕДСТАВЛЕННЯ КУРСАНТАМ ЗВІТНИХ ЕТАПІВ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інтерактивні технології та методи навчання значно покращують навчально-виховний процес, полегшують формування умінь та навичок у курсантів. При їх впровадженні у життя, завжди з’являються численні перепони на шляху. Ось тому, значна частина педагогів, які застосовують застаріли заняття по шаблону або навіть після косметичного ремонту носять чисто інформативні, формальні заняття. Новатори ж, навпаки вимушені вирішувати складні проблеми, завчасно не знаючи кінцевого результату. Опрацюють студенти та курсанти матеріал дисципліни, чи ні? Чи справді вони набули необхідні знання, уміння і навички, сформували у собі значущі для сучасного життя цінності та компетентності [1]. З цими важливими проблемними питаннями оцінювання знань та умінь навчаючих, як з перепоною на шляху педагогічної діяльності, зустрічається кожен молодий педагог. Це пов’язано з відсутністю обґрунтованих підходів до розробки цікавого змістовно-логічного змісту дисципліни, стратегії оцінювання, яка тісно пов’язана з підготовкою і плануванням педагогом кожного заняття (уроку) не за шаблоном, а кожного разу вносити щось нове. Тільки так інтерактивні технології та методи навчання в змозі виконати функції навчання.

Тривалі спостереження за свідомістю курсантів дозволило встановити проблему, що на першому вступному занятті нової дисципліни курсанти не розуміють необхідності її вивчення. Це не пов’язано з небажанням вчитися, а з не розумінням структурно-логічної схеми навчання. На першому занятті викладачі припускаються помилки, починаючи його з розхвалювання дисципліни кафедри, її необхідності та важності поряд або над всіма. Такої ж участі без свідомого розуміння курсантами очікує структура та звітність навчальної дисципліни. Спроби вирішити ці протиріччя не досягли бажаного результату.

Автори дослідження поставили за мету для рішення цієї проблеми розробити метод віртуально-пізнавального представлення курсантам звітних етапів навчальної дисципліни. Метод забезпечить представлення у доступній формі зміст та структурно-логічну побудову звітних етапів для усвідомлення. Лише так можна досягти головної мети навчання [2]. Тільки усвідомленим навчанням курсант вивчить дисципліну і зможе застосовувати отримані в процесі навчання знання у вигляді умінь та навичок. А це і є критерієм адекватності запропонованого алгоритма в методі. В основу його положено – метод дидактичної гри.

Ці методи розвивають навчально-пізнавальну діяльність. Поєднання дидактичних ігор з електронно-обчислювальною технікою (ЕОТ) є зараз актуальними для існуючого суспільства. ЕОТ швидкими темпами впроваджується в усі галузі повсякденної діяльності людини, з динамікою збільшення обчислювальної можливості Це спонукає молоде і підростаюче покоління до її обов’язкового освоєння. Перше з чим ознайомлюється та навчається молодь є гра на ЕОМ. Згодом за допомогою викладача вони освоюють ЕОМ на рівні користувача. Граючи вони засвоюють будову, принцип роботи на ЕОТ та нові здобутки цифрової техніки. Тому в основі сучасної освіти має стати дидактична гра. Слід зазначити такі недоліки як: тривале користування ЕОТ без перерви, призводить до погіршення здоров’я. Це не стосується навчання запропонованого авторами методом [3 – 6].

Мета навчання в ході дидактичної ігри досягається за допомогою рішення різноманітних ігрових завдань [2, 6, 7]. Вивчаючи правила гри, курсанти дисциплінуються та швидко засвоюють складні на перший погляд основні поняття та визначення дисципліни. Встановлено, що дидактичні ігри активізують увагу і зацікавленість до пізнання. Це так необхідно курсантам при вивченні, складних у розумінні, військово-технічних дисциплін. Ігрові моменти заняття знімають напругу та перевтому курсантів.

Головною вимогою до застосування дидактичної гри є те, щоб навчальна мета не перетворилася просто в гру [6, 7]. Для цього слід управляти процесом гри. При правильних

коментарях викладач зможе керувати навчально-пізнавальною діяльністю, та поєднати її з позитивним мотиваційним і емоційним фоном гри.

Розглянемо метод віртуально-пізнавального представлення курсантам звітних етапів навчальної дисципліни. Якщо курсант не знає обсягу та структурно-логічного змісту дисципліни, то йому важко зорієнтуватися у контрольних точках звітності дисципліни. Особливо це стосується семестрових контрольних, модульних контролів дисципліни, передбачених навчальною та робочою програмою. Окрім звітності важливим елементом є критерії мінімально-максимального оцінювання знань курсантів викладачем. Це підтверджується дослідженнями [3 – 6].

Не слід виключати випадку, що курсант може бути відсутнім з причини виконання службових обов'язків (несення служби у добовому наряді, перебуванні у відрядженні) або по хворобі, тощо. Штатний розклад, який видається у навчальну групу містить лише інформацію: абревіатуру (шифр) дисципліни, номер теми та вид заняття. Модульні контролі та атестація у розкладі не відмічається, тому курсант їх не в змозі передбачити.

Першим етапом є вибір звітних етапів. Він є підготовчим. Підготовчий етап передує початком навчального семестру з вивченням нової навчальної дисципліни. Відповідальний за навчальну дисципліну на кафедрі, лектор, аналізує робочу програму навчальної дисципліни (РПНД) та виконує наступну послідовність робіт:

–виписує номери тем модульних контролів;

–контрольних робіт;

–лабораторних робіт;

–практичних робіт (які передбачають 100% звітність);

–інші розрахунково-графічні роботи;

–курсові роботи.

Ці дані записуються у тій же хронологічній послідовності, що вони є у РПНД. Всі вони повинні бути у відповідності до рейтингової системи оцінювання.

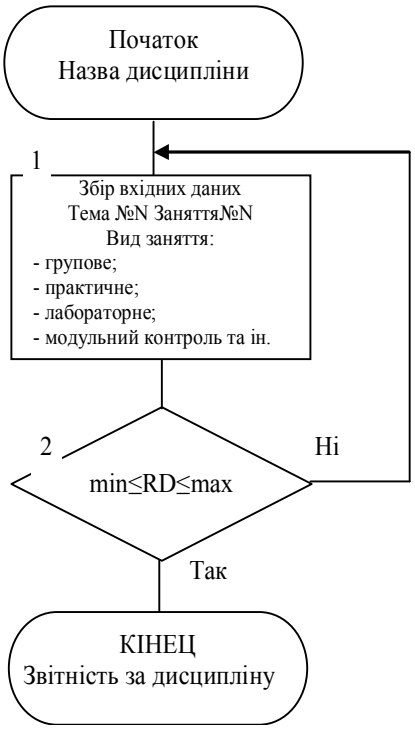


Рис. 1. Алгоритм структурно-логічного змісту навчальної дисципліни

На ***другому етапі*** вибір критеріїв оцінювання звітних етапів. Напроти звітних тем виставляється оціночний критерій *RD* в умовних балах, у тих, що передбачено рейтинговою системою оцінювання – Болонським процесом. Отримані вихідні дані об'єднуються в єдиний алгоритм представлення звітних під етапів навчальної дисципліни.

Тобто кожен звітний блок такого алгоритму завершується блоком порівняння й прийняття рішення. Блок представляє собою границю допустимих залікової оцінки значень.

Якщо курсант набирає наприклад за модуль оцінку нижче граничної або прохідної оцінки, то викладач приймає рішення про подальший допуск до навчання цього курсанта [2-6]. Рішення на перездачу приймається в залежності від рівня засвоєння знань та набуття практичних навичок курсантом.

Набравши базовий мінімум знань ($\min \le RD \le \max$) курсант має допуск до подальшого вивчення теми. Якщо курсант набирає ($0 \le RD \le \min$), то він може бути допущений до подальшого вивчення тем дисципліни, при умові обов'язкової перездачі її до початку екзаменаційної сесії. В усіх інших випадках надається курсантам час на перездачу до наступного заняття.

Третій етапі. Побудова алгоритму із прямими та зворотними зв'язками.

Підзвітні етапи кожного змістовного блоку згідно РПНД поєднуються лініями прямого та зворотного зв'язку. Побудований алгоритм повинен відповідати структурно-логічному змісту навчальної дисципліни (рис 1).

Четвертий етап. На першому лекційному занятті, лектору достатньо пояснити курсантам структурно-логічний зміст навчальної дисципліни, місце та роль її у подальшій життєдіяльності як офіцера.

ВИСНОВКИ

Тривалі спостереження за свідомістю курсантів дозволило, встановити, що курсанти на першому лекційному занятті нової дисципліни не розуміють необхідності її вивчення. Головним чинником проблеми є не усвідомленням структурно-логічного схеми навчання та вивчаючої дисципліни.

На наш погляд, це пов'язано з відсутністю обґрунтованих підходів до розробки структурно-логічного змісту дисципліни, стратегії оцінювання, яка тісно пов'язана з підготовкою і плануванням педагогом кожного заняття (уроку) не за шаблоном, а кожного разу вносити щось нове.

Ось тому на першому лекційному занятті викладачеві слід пояснити:

– структурно-логічний зміст дисципліни;

– місце її в системі підготовці фахівців з даного напряму спеціалізації;

– стратегію оцінювання знань, умінь та навичок [1];

– та звітність у вигляді алгоритму звітних етапів.

Представлення даного алгоритму у вигляді дидактичної гри найшвидше досягнеться мета навчання. Управляючи процесом дидактичної гри викладач природним чином активізує увагу стимулює навчально-пізнавальну діяльність при вивченні складних військово-технічних дисциплін, пов'язуючи її з позитивним мотиваційним і емоційним фоном гри.

ЛІТЕРАТУРА

1. *Козубцова Л.С., Козубцов М.К.,* Козубцов І.М. Аналіз необхідності переосмислювання існуючих підходів до оцінювання знань та умінь навчаючих у вищій школі. // Журнал. Известие науки. [Электронный ресурс]. – Режим доступа: http://www.inauka.ru/blogs/article96359.html.

2. *Козубцов І.М., Козубцова* Л.С. Розвиток логічного мислення, пізнавальної активності учнів. застосування різних форм навчання. // Журнал. Известие науки. [Электронный ресурс] – Режим доступа: http://www.inauka.ru/blogs/article91926.html.

3. *Козубцов И.Н.* Обучения электротехнических дисциплин методом виртуальной компьютерной игры. // Электротехнологии, электропривод и электрооборудование предприятий: сборник научных трудов II Всероссийской научно-технической конференции: в 2 т. Т. 2 / редкол.: В.А. Шабанов и др.– Уфа: Изд-во УГНТУ, 2009. – С. 107 – 110. – ISBN 978-5-7831-0867-9.

4. *Козубцов І.М.* Концепція самостійного навчання курсантів Сухопутних військ на навчально-тренувальних засобах методом гри на віртуальному комп'ютері. // Перспективи розвитку озброєння і військової техніки Сухопутних військ. Збірка тез доповідей Другої Всеукраїнської науково-технічної конференції (28 – 29 квітня 2009 р.). „ЛП". – Львів: ЛІСВ НУ „ЛП", 2009. – С. 77.

5. *Козубцов І.М.* Методологія навчання курсантів на телекомунікаційних навчально-тренувальних засобах в умовах фінансово-економічної кризи. // Журнал. „Наука и жизнь" [Электронный ресурс] – Режим доступа: http://www.nkj.ru/forum/forum15/topic12611/messages/message75075/#message75075.

6. *Козубцов І.М.,* Козубцова Л.С., Козубцов М.К. Метод ігрового проведення заліку та іспиту з радіотехнічних дисциплін. [Электронный ресурс] // Журнал. Известие науки. – Режим доступа: http://www.inauka.ru/blogs/article98182.html.

7. *Кроль В.М.* Психология и педагогика: Учеб. пособие для техн. вузов. – М.: Высш. шк., 2001. – 319 с.

к.т.н. Коцюба В.П. (ХУПС)
Станіщук А.Б. (ЦНДІ ОВТ ЗС України)

ОРГАНІЗАЦІЯ ЗАХИСТУ ОБ'ЄКТІВ ТА КОМПЛЕКСІВ ЗВ'ЯЗКУ ВІД ІНФОРМАЦІЙНОГО ВПЛИВУ

В доповіді розглядаються питання організації захисту від інформаційної диверсії проти АСУ ЗС України. На сьогодні новим явищем військового протистояння й ведення бойових дій будь-якими групами держав стає їх інформаційне протиборство, сутність якого полягає у зосередженні головних зусиль збройної боротьби не на фізичному знищенні конкретних одиниць зброї, а на руйнуванні інформаційних ресурсів держави-ворога і її збройних сил, руйнуванні або спотворенні системи управління ними, каналів обміну інформації, навігації і наведення, механізмів впливу на індивідуальну і суспільну свідомість. Сучасні погляди на організацію та ведення інформаційної боротьби полягають в комплексному використанні різнорідних сил для досягнення інформаційної переваги над противником. Варто відмітити, що тенденція зміни форм і способів інформаційної боротьби обумовлена розвитком інформаційної зброї. Теоретики відносять до цього виду зброї широкий спектр заходів і засобів інформаційного впливу на противника – від дезінформації й пропаганди до засобів радіоелектронної боротьби.

Таким чином, інформаційна боротьба змінює не тільки форми і способи ведення воєнних дій, змінюється зміст самого поняття війни, стираються грані між воєнним і мирним часом, пропадає стале сприйняття поняття „театр воєнних дій", ще більш зрощуються воєнні і мирні технології.

Розвинені країни світу приділяють велику увагу розробці інформаційної боротьби, а також системам комплексного захисту від неї. Кількість перспективних технологій, що знаходяться у розробці та у впровадженні, постійно зростає. В подальшому це може привести до беззаперечного панування на полі бою використанням небойових засобів. Визначення шляхів створення засобів інформаційного протиборства та інформаційного захисту в ЗС України потребує проведення додаткових наукових досліджень. Інформаційна боротьба є протиборчою стороною за завоювання переваги по кількості, якості і швидкості здобування інформації, її вчасному аналізу і застосуванню. Вона передбачає постійне вдосконалення інформаційних технологій з обов'язковим проведенням заходів по підвищенню їхнього захисту від впливу противника. Загальною стратегічною метою інформаційної боротьби є забезпечення переваги у вирішенні задач, що стоять, однією із сторін через досягнення переваги над протиборчою стороною на інформаційному рівні.

Метою інформаційної переваги є сприяння у розробці нових оперативних концепцій, які будуть забезпечувати оперативну перевагу в районі бойових дій. Для досягнення цієї мети створюється інтегрована система, яка включає найбільш важливі галузі бойових можливостей. До них відносяться: поінформованість про обстановку в районі бойових дій; ефективне використання сил; комплексна система засобів забезпечення (мережа C^4ISR). Провідні країни світу передбачають прискорити темпи вдосконалення організаційної структури мережі C^4ISR на тактичному рівні, в тому числі й вузлів мобільних користувачів. Визначена розробка низки вдосконалених методів захисту процесів збору й розподілу інформації. У більш віддаленому майбутньому, в період після 2010 року, еволюція оперативних концепцій і використання можливостей нових технологій забезпечать основу для повномасштабної розробки концепцій, передбачених комплексною програмою „Перспективна система збору й передачі інформації про хід бойових дій (ABIS)".

д.т.н. Кравчук С.О. (НТУУ „КПІ”)
Міночкін Д.А. (НТУУ „КПІ”)

ЗАСТОСУВАННЯ БАГАТОАНТЕННОЇ ТЕХНОЛОГІЇ MIMO В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ СПЕЦИФІКАЦІЙ LONG TERM EVOLUTION

Зростання пакетного мультимедійного трафіка в системах мобільного зв’язку вимагає більш надійної підтримки високих швидкостей передачі даних. У зв’язку з цим, великий інтерес викликає багатоагентна технологія MIMO (*Multiple Input-Multiple Output*), яка дозволяє формувати множину просторових слоїв, у яких множина потоків даних передається в певному частотно-часовому ресурсі. Це дає можливість збільшувати пропускну здатність каналу лінійно зі зростанням кількості антенних елементів на передавальній і приймальні сторонах. У своєму останньому релізі група стандартизації 3GPP визначила нову специфікацію мобільного зв’язку E-UTRA (*Enhance* – UMTS *Terrestrial Radio Access*), відомої як *Long Term Evolution* (LTE). Вона базується на технології мультиплексування з ортогональним розділенням частоти OFDM (*Orthogonal Frequency Division Multiplexing*) і підтримує бездротові широкосмугові послуги передачі даних зі швидкостями до 300 Мбіт/с у прямому каналі та до 75 Мбіт/с у зворотних каналах.

В LTE для збільшення пікової швидкості прямого каналу й середньої пропускної спроможності стільника широко використовується технологія MIMO, включаючи рознесення по передачі, однокористувальницьке MIMO SU-MIMO (*single user* MIMO), багатокористувальницьке MIMO MU-MIMO (*multiuser* MIMO), однорангове попереднє кодування зі зворотним зв’язком, а також спеціальне формування променів.

Різноманіття пропонованих підходів, складність розглянутих технологій і, особливо, їх комбінацій, вимагають їхньої аналітичної оцінки з єдиних позицій для прискорення розробки й впровадження LTE-Систем. Тому, аналіз різних технологій MIMO та підходів до їх реалізації, які пропонуються в рамках форму LTE-Advanced, є актуальним завданням на даному етапі розвитку систем мобільного зв’язку.

Схеми *однокористувальницького* MIMO визначені для конфігурацій з двома або чотирма передавальними антенами в прямому каналі, які підтримують передачу множини просторових слоїв (до чотирьох) до даного користувальницького обладнання. Схема *рознесення передачі* визначена для конфігурації із двома або чотирма передавальними антенами у зворотних каналах, та з двома передавальними антенами в прямому каналі. *Багатокористувальницькі* схеми MIMO дозволяють призначити різні просторові слої різним користувачам в одному частотно-часовому ресурсі і такий поділ підтримується при передачі як у прямому, так і у зворотному каналах. Схема *однорангового попереднього кодування* зі зворотним зв’язком використовується для поліпшення покриття при передачі даних з використанням однокористувальницького MIMO, ґрунтуючись на загальному опорному сигналі, індивідуальному для кожного стільника й введенні керуючого повідомлення з малою кількістю службової інформації. *Спеціальне формування променів* використовується для розширення покриття, коли абонентським терміналом підтримується демодуляція даних на основі спеціального опорного сигналу. У ході досліджень було проведено аналіз технічних особливостей зазначених технологій з урахуванням вимог висунутих LTE, представлений механізм встановлення зворотного зв’язку для поліпшення підтримки технологій MIMO у прямому каналі систем LTE, а також проаналізовані схеми MIMO, які пропонуються форумом LTE-Advanced. З допомогою системного моделювання було оцінено продуктивність прямого каналу LTE в режимі SU-MIMO за параметрами середньої пропускної спроможності стільника та пропускної спроможності на краю стільника. Результати моделювання для конфігурацій антен 2×2 та 4×4 показали зростання продуктивності системи в результаті введення просторового мультиплексування в LTE. Порівнюючи MIMO-SIC з SIMO-IRC спостерігається виграш за середньою пропускною спроможністю стільника в розмірі 14 % та 87% при застосуванні схем 2×2 та 4×4, відповідно.

к.т.н. Кривоножко Г.Є. (ВІТІ НТУУ „КПІ”)
к.т.н. Криховецький Г.Я. (ВІТІ НТУУ „КПІ”)
Срібний С.П. (ВІТІ НТУУ „КПІ”)

ШЛЯХИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ АВТОМАТИЗОВАНОГО УПРАВЛІННЯ ВІЙСЬКАМИ

В основі будь-якого управління [1], у тому числі й управління військами, лежать інформаційні процеси, які базуються на безперервному добуванні даних про супротивника, свої війська, умови ведення бойових дій; зборі інформації, її аналітичній обробці, збереженні та багатоцільовому використанні при проведенні оперативно-тактичних розрахунків, моделюванні й плануванні бойових дій, прийманні інформаційних, організаційних і оперативних рішень, постановці задач військам й контролі їхнього виконання [2].

Нові інформаційні технології мають на вказані процеси істотний вплив, забезпечуючи автоматизоване виконання більшого числа задач з більш високою якістю. Однак, обмежене фінансування розробок нових зразків озброєння й військової техніки дещо стримує запровадження новітніх технологій у практику військ [2].

В таких умовах раціональним шляхом підвищення ефективності автоматизованого управління військами є удосконалення системи управління Збройних Сил України через:

цифровізацію системи зв’язку;

загальну автоматизацію системи управління Збройних Сил України.

Стосовно цифровізації основними заходами визначено: прокладання волоконно-оптичних ліній зв’язку доступу; розгортання системи цифрового автоматичного зв’язку Збройних Сил України; створення системи закриття інформації на пунктах управління Збройних Сил України; створення польової компоненти системи зв’язку Збройних Сил України; створення системи супутникового зв’язку Збройних Сил України; створення комплексної системи захисту інформації на пунктах управління Збройних Сил України; створення системи сервісного обслуговування засобів зв’язку та автоматизації Збройних Сил України.

Впровадження цифрової системи зв’язку дасть можливість за рахунок різкого підняття якості управління знизити кількісний склад військ зв’язку.

В практиці управління військами виникла і постійно загострюється суперечність між зростанням обсягу інформації, що підлягає переробці при прийнятті керуючого рішення (на таку переробку потрібен час), і скорочення часу, що є на його прийняття.

На сьогоднішній день основним методом розв’язання цієї суперечності є автоматизація процесу управління військами на основі сучасної обчислювальної техніки і нових інформаційних технологій.

Оскільки своєчасне прийняття керуючих рішень (оперативність управління) та їх обґрунтованість (в граничному варіанті – оптимальність) самим безпосереднім чином впливають на ефективність управління військами та успіх бойових дій взагалі, комплексне вирішення цих питань можливе за рахунок загальної автоматизації системи управління Збройних Сил України.

Метою такої автоматизації [3] є досягнення якісно нового рівня системи управління для підвищення ефективності керівництва життєдіяльністю, розвитком, підготовкою і застосуванням Збройних Сил у мирний час та особливий період шляхом оптимізації організаційної та функціональної структур системи управління, інтенсивного впровадження нових інформаційних технологій управління, комплексної автоматизації всіх ланок і рівнів системи управління, процесів управління військами (силами), бойовими засобами (зброєю), удосконалення організації і методів роботи посадових осіб органів та пунктів управління.

Загальна автоматизація управління Збройних Сил України передбачає об’єднання на єдиних оперативно-стратегічних та системотехнічних принципах автоматизовані системи

управління стратегічної ланки, видів Збройних Сил, видів забезпечення, родів військ, об'єднань, з'єднань, частин і підрозділів та призначена для забезпечення і здійснення керівництва Збройними Силами України та іншими військовими формуваннями воєнної організації держави, управління військами (силами) та бойовими засобами (зброєю).

У зв'язку з цим загальна автоматизація системи управління Збройними Силами має за мету:

підвищення бойової готовності Збройних Сил;

підвищення ефективності використання та бойового застосування сил і засобів;

підвищення стійкості та оперативності управління військами (силами) в мирний та воєнний час;

зменшення працезатрат посадових осіб органів управління у всіх видах їх службової діяльності.

З метою виконання цих вимог, загальна автоматизація Збройних Сил України передбачає створення стаціонарно-мобільної системи яка б об'єднала на єдиних оперативно-тактичних, системотехнічних принципах комплекси засобів автоматизації пунктів управління стратегічної ланки управління, видів Збройних Сил, родів військ (спеціальних військ) та окремі системи автоматизації управління військами, розвідкою та зброєю, розроблених на основі загальної ідеології.

Така система призначається для забезпечення: автоматизованого керівництва Збройними Силами і управління військами (силами) в мирний та воєнний час, в перехідний період, при їх стратегічному розгортанні; автоматизованого керівництва будівництвом, забезпеченням і переозброєнням Збройних Сил, військовою наукою, підготовкою кадрів, резервів та комплектуванням військ; автоматизації вирішення завдань управління бойовим чергуванням, повсякденною діяльністю органів управління, установ Міністерства оборони, військ, об'єктів видів Збройних Сил і родів військ, відмобілізуванням та оперативним розгортанням військ, підготовкою і веденням бойових дій; взаємодії з системами управління Національної гвардії, Прикордонних військ, Служби безпеки, міністерств та відомств України.

Тобто, загальна автоматизація Збройних Сил України повинна бути реалізована у вигляді складної організаційно-технічної системи, що потребує виконання координованих робіт під загальним та постійним керівництвом Генерального конструктора, має базуватись на єдиних принципах та використовувати новітні інформаційні технології.

Таким чином, раціональні шляхи підвищення ефективності автоматизованого управління військами повинні базуватися на використанні існуючих зразків та їх модернізації та впровадженні нових інформаційних технологій.

Виконання заходів зі створення цифрової системи зв'язку та загальної автоматизації системи управління Збройних Сил України дасть можливість значно змінити та удосконалити систему управління Збройних Сил України; змінити структуру системи та військ зв'язку Збройних Сил України, пунктів управління Збройних Сил України.

ЛІТЕРАТУРА

1 *Глушков В.М.* Основы безбумажной информатики. – М.: Наука, 1987. – 552 с.

2 *Робочі матеріали* 1-го етапу НДР "Трикутник–НР". – К.: НЦЗІ ЗСУ, 2004. – 114 с., інв. 1188.

3 *В.Д. Кудрицький, Ю.І. Катков.* Основи організації систем автоматизації управління військами: Навчальний посібник. – К.: НАОУ, 2003.– Ч.1 – 172 с.

Кривцов І.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ СИСТЕМИ БЕЗПЕКИ МОДУЛЬНОГО ОБ’ЄКТНО-ОРІЄНТОВАНОГО СЕРЕДОВИЩА НАВЧАННЯ

Для аналізу ефективності системи безпеки модульного об’єктно-орієнтованого середовища навчання пропонується застосувати апарат математичної статистики. Математична статистика встановлює статистичні закономірності і забезпечує отримання науково обґрунтованих висновків про явища із даних спостережень та експериментів. Багато методів статистичного аналізу вийшли за рамки класичної математичної статистики, наприклад, група методів аналізу виживання (*Survival Analysis*). Ці методи дозволяють провести статистичний аналіз інформації, результатом якого виявлення найбільш вагомих факторів, які впливають на ефективність системи. Існує два типи інформацій, яку виявляють в цих методах: повна і неповна. Інформація, в якій немає даних про настання події, яка нас цікавить, має назву – неповна інформація (*censored*). Якщо є данні про настання цікавої для нас події, то інформація зветься повною (*complete*). Спостереження, які містять неповну інформацію, тобто такі величина спостереження – значення часу до здійснення критичної події, а час спостереження обмежений в часі, називаються цезорними. Застосування цензорних спостережень складає специфіку методу аналізу виживання. У методі досліджуються імовірностні характеристики інтервалів часу між послідовним виникненням критичних подій. Подібні дослідження отримали назву тривалість до моменту припинення (*time until failure*), які можливо визначити як інтервали часу між початком спостереження за об’єктом та моментом припинення, при якому об’єкт перестає відповідати визначеним для спостереження якостям. Побудова таблиць часу життя, розподіл виживання, оцінювання функції виживання за допомогою процедури Каплана-Мейєра відносяться до методів опису цензорних даних. Аналіз виживання містить регресійні моделі для оцінювання залежностей між багатомірними неперервними змінними зі значеннями, які аналогічні часу життя.

У доповіді пропонується дослідити ефективність застосування методики забезпечення автентичності навчальної звітності для об’єктно-орієнтованого середовища навчання за допомогою методу аналізу виживання.

Для досягнення поставленої мети вирішуються такі основні задачі:

– аналіз існуючих організаційних структур систем дистанційного навчання та загроз процесу дистанційного навчання, підходів до побудови підсистеми захисту навчальної звітності в системах дистанційного навчання;

– розробка методики забезпечення автентичності навчальної звітності в об’єктно-орієнтованому навчальному середовищі;

– оцінка ефективності системи безпеки з впровадженим програмним забезпеченням автентичності навчальної звітності.

Таким чином, для апробації зазначеної методики, пропонується обрати систему „Командирська підготовка”, яка реалізована в об’єктно-орієнтованому середовищі навчання *Moodle* та розгорнута в мережі кафедри № 21 ВІТІ НТУУ „КПІ”. Для оцінки ефективності впровадження програмних кодів методики забезпечення автентичності навчальної звітності пропонується застосувати модуль *Survival Analysis* з інтегрованого програмного пакета *Statistika 6.0*.

ЛІТЕРАТУРА

1. *Лалафян А.А.* STATISTICA 6. Статистический анализ данных. Учебник. / А.А. Лалафян – М.: ООО „Бином-Пресс”, 2008 г. – 512 с.

2. *Гороховський О.І.*, *Трояновська Т.І.* Аспекти створення, моделювання та практики автоматизованих систем дистанційного навчання // Автоматика 2006. – Вінниця, 2006. – С. 453.

к.т.н. Кувшинов О. В.(ВІТІ НТУУ „КПІ”)
Липський О. А. (ВІТІ НТУУ „КПІ”)

КОНТРОЛЬ КАНАЛУ ЗВ’ЯЗКУ ПРИ ПАКЕТНІЙ ПЕРЕДАЧІ ДАНИХ

При будівництві сучасних інформаційно-телекомунікаційних систем велика увага приділяється їх інтеграції в єдиний інформаційний простір. Аналіз створення сучасних мереж свідчить про те, що найбільш доцільним методом об’єднання окремих елементів та вузлів інформаційно-телекомунікаційних мережі є канали із комутацією пакетів. Проте, використання каналів із змінними параметрами, таких як, канали радіозв’язку, супутникового радіорелейного і тропосферного зв’язку вимагає їх контролю у відповідності до рекомендацій МСЭ-Т Y.1541 [1]. Дана рекомендація визначає основні характеристики мережі із передачі пакетів, такі як, середній час затримки пакету IPTD, процент втрачених пакетів IPLR і процент спотворених пакетів IPER.

Для адекватного представлення зазначених характеристик і контролю якості послуг в мережі доцільним буде опис зазначених характеристик на підставі послідовного критерію відношення ймовірностей. Ймовірність спотворення кадру P_{PSR} визначається за допомогою стаціонарних ланцюгів Маркова на підставі контролю наступних характеристик: n – загальна кількість кадрів по якій оцінюється радіорелейний канал; k – загальна кількість спотворених кадрів; v – кількість спотворених кадрів в серії; u – кількість правильно прийнятих кадрів в серії.

Задача оцінки каналу зв’язку полягає у перевірці статистичної гіпотези $H: p = P_{PSR\,\text{гр}}$ – канал не придатний до роботи, проти альтернативної гіпотези $\overline{H}: p = P_{PSR} < P_{PSR\,\text{гр}}, P_{PSR} > 0$ – канал придатний до роботи. Для перевірки гіпотез використовують критерій Неймана-Пірсона, який для марковських ланцюгів є найбільш потужним із всіх критеріїв при заданому значені помилки. Вказаний критерій для марковських ланцюгів приводить до нерівності [2]

$$\Lambda = \frac{W(n,k,v,u/P_{PSR})}{W(n,k,v,u/P_{PSR\,\text{гр}})} \geq \Lambda^*,$$

де $W(n,k,v,u/P_{PSR})$ – ймовірність появи вибірки із n кадрів, яка має k спотворених кадрів, $n-k$ не спотворених кадрів, v – серія із спотворених кадрів та u – серія вірно прийнятих кадрів. $\Lambda \geq \Lambda^*$ – нерівність що визначає критичну область для яких H відкидається.

Однак, використання дуже малих значень $P_{PSR\,\text{гр}}$ при незадовільній якості зв’язку приведе до значної затримки у визначені стану каналу зв’язку, використання великих значень $P_{PSR\,\text{гр}}$ приведе до недооцінки каналу зв’язку. Це потребує проведення попередньої оцінки каналу зв’язку із метою отримати значення $P_{PSR\,\text{гр}}$. Дана задача вирішується застосуванням математичного апарату на базі нечіткої логіки [3]. На підставі якої робиться висновок: канал зв’язку перебуває в дуже поганому стані, поганому, середньому, доброму і відмінному стані. У відповідності до визначеного стану обирається значення $P_{PSR\,\text{гр}}$.

Процедура контролю каналу зв’язку на підставі адаптивного вибору $P_{PSR\,\text{гр}}$ надасть можливість зменшити час контролю каналу зв’язку при незадовільній якості, та навпаки не дасть змоги зробити передчасний висновок про задовільний стан каналу зв’язку.

ЛІТЕРАТУРА

1. *МСЭ-Т* Y.1541 (02/2006). Требования к сетевым показателям качества для служб, основанных на протоколах IP. – Женева, 2007. – 44 с.

2. *Коричнев Л. П.* Статистический контроль каналов связи / Л.П. Коричнев, В.Д. Королёв. – М.: Радио и связь, – 1989. – 240 с.

3. *Гостев В. И.* Проектирование нечетких регуляторов для систем автоматического управления: монография / Гостев В.И. – Нежин: Аспект-Поліграф, 2010. – 416 с.

к.т.н. Кузавков В.В. (ВІТІ НТУУ „КПІ”)
Логінов М.В. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ОЦІНКИ РОЗПОВСЮДЖЕННЯ МОВНОГО СИГНАЛУ

Підслуховування, як і спостереження, буває безпосереднє та за допомогою технічних засобів. З огляду на малу потужність мовний сигнал людей, що розмовляють та значного згасання акустичної хвилі у середовищі розповсюдження безпосереднє підслуховування можливе на невеликій відстані (одиниці або, у кращому разі, за відсутності сторонніх звуків – десятки метрів). Тому для підслуховування застосовуються різні технічні засоби [4].

Постановка задачі.

При розповсюдженні мовного сигналу у вільному просторі і проходженні його крізь огороджувальну віконну конструкцію, знайти максимальну відстань r_{max}, від джерела мовного сигналу до мікрофону розміщеного за цією віконною конструкцією по відношенню до джерела, на якій абсолютний рівень звукового тиску мовного сигналу $L \geq L_{min}$.для розпізнавання його мікрофоном (рис. 1).

Умови задачі:

1. Відомий рівень мовного сигналу Ls, його частотна характеристика Lis та відстань r_0 від джерела розповсюдження на якій він вимірювався, при $r_0 < r_1$ де r_1 відстань від джерела мовного сигналу до віконної конструкції (у більшості випадків r_0=1 м);
2. Джерело мовного сигналу є одиничним і точковим;
3. Середовищем розповсюдження мовного сигналу є повітря;
4. Мовний сигнал розповсюджується від джерела крізь огороджувальну конструкцію до входу мікрофона під кутом 0°;
5. Віконна конструкція крізь яку проходить мовний сигнал є ідеальною (без щілин, тріщин тощо) з відомою частотною характеристикою звукоізоляції повітряного шуму R_i;
6. Мікрофон характеризується рівнем еквівалентного звукового тиску завад L_{enoise}, дБА, обумовленого власним шумом конденсаторного мікрофону відносно $p_0 = 2\ 10^{-5}$ Па.
7. Віконна конструкція, крізь яку проходить мовний сигнал і мікрофон розміщені у зоні дії прямого звуку (тобто на них падають лише прямі хвилі);
8. Прийом мовного сигналу мікрофоном здійснюється лише на фоні завад, обумовлених власним шумом мікрофону.

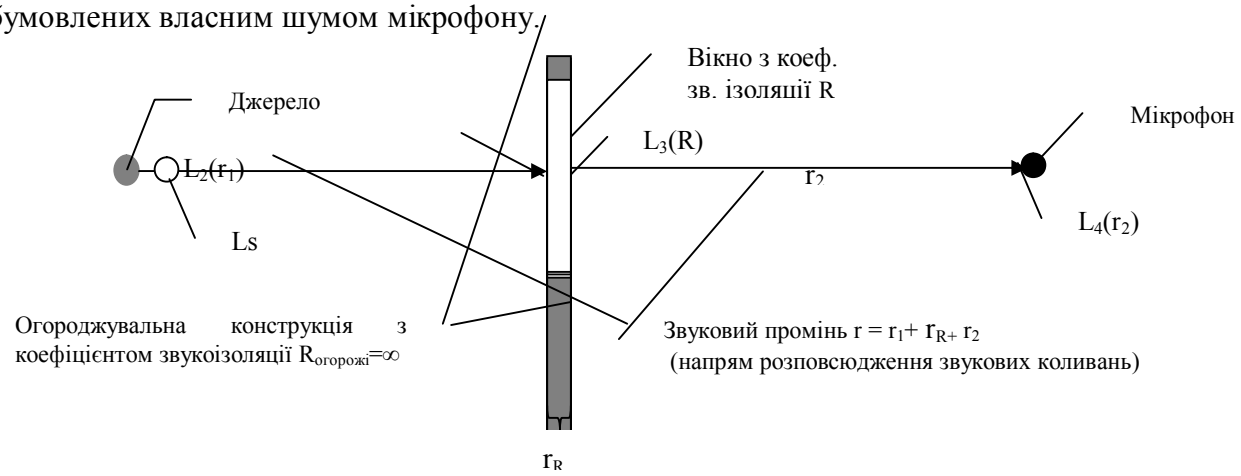


Рис. 1. Розповсюдження мовного сигналу від джерела до мікрофону крізь віконнуконструкцію

L_s – розрахункова точка з відомим значенням рівня мовного сигналу на відстані $r_0 = 1$ м від джерела;

$L_2(r_1)$ – розрахункова точка зі значенням рівня мовного сигналу на межі розподілу двох середовищ „повітря-скло”;

$L_3(R)$ – розрахункова точка зі значенням рівня мовного сигналу на межі розподілу двох середовищ „скло-повітря” (з урахуванням коефіцієнту звукоізоляції вікна);

$L_4(r_2)$ – розрахункова точка зі значенням рівня мовного сигналу на вході мікрофону;

r_1 – довжина звукового променю від джерела мовного сигналу до межі розподілу двох середовищ „повітря-скло” або відстань від джерела мовного сигалу до точки L_2;

r_2 – довжина звукового променю від межі розподілу двох середовищ „скло-повітря” до входу мікрофону або відстань від розрахункової точки L_3 до розрахункової точки L_4;

r_R – глибина віконної конструкції – є такою, яку можна не враховувати при розрахунках.

Для знаходження максимальної відстані r_{max} від джерела мовного сигналу до розрахункової точки $L_4(r_2)$ на вході мікрофона, в якій абсолютний рівень звукового тиску мовного сигналу $L = L_{min}$ необхідно:

1. Визначити мінімальний рівень мовного сигналу L_{min} який буде розпізнаватися мікрофоном за формулою [1]:

$$L_{min} = L_{enoise} + 12, \text{ дБ} \quad (1).$$

2. При відомих відстані r_0 від джерела до точки L_s та рівня мовного сигналу у цій точці, знайти рівень мовного сигналу на відстані r_1 в точці L_2, на межі розподілу 2-х середовищ „повітря-скло”, за формулою [3]:

$$L_2(r_1) = L_S - 10\lg(r_1^2/r_0^2), \text{ дБ} \quad (2),$$

де L_S – відомий рівень мовного сигналу на відстані r_0.

3. На підставі частотної характеристики ізоляції повітряного шуму даною віконною конструкцією R_i, за формулою 3 [2] розрахувати коефіцієнт звукоізоляції мовного сигналу R цієї віконної конструкції:

$$R = L_s - 10\lg \Sigma\, 10^{0,1(Lis - Ri)}, \text{ дБ}, \quad (3).$$

4. Обчислити значення рівня мовного сигналу у розрахунковій точці L_3, на межі розподілу 2-х середовищ „скло-повітря”. Так як різницею значень рівнів мовного сигналу у розрахункових точках L_2 та L_3 є коефіцієнт звукоізоляції мовного сигналу R [3], то:

$$L_3(R) = L_2(r_1) - R, \text{ дБ}. \quad (4).$$

– Якщо $L_3(R) < L_{min}$ – умова не виконується;

– Якщо $L_3(R) \geq L_{min}$ – умова виконуються, здійснюються заходи передбачені пунктом наступним пунктом.

5. Розрахувати максимальну відстань r_{max} від джерела МС до розрахункової точки L_4 на вході МК за формулою:

$$r_{max} = r_0' \; 10^{(L3 - Lmin) / 20}, \text{ м}, \quad (5),$$

де r_0' – відстань від джерела до розрахункової точки L_3 в якій виміряний рівень мовного сигналу.

Отже дані розрахунки, здійснені на підставі [1], [2], [3], можна використовувати у подальшому для побудови більш складних моделей розповсюдження мовного сигналу від джерела до приймача за наявності перешкод різного характеру, з метою оцінки технічного каналу витоку мовної інформації.

ЛІТЕРАТУРА

1. *ГОСТ 16123-88*. Микрофоны. Методы измерений электроакустических параметров.
2. *СНиП 23-03-2003*. Защита от шума.
3. *Техническая акустика транспортных машин* //Под. ред. Н.И. Иванова.//. – С.Пб.: Политехника, 1992.
4. *Торокин А.А*. Инженерно-техническая защита информации. – М.: „Гелиос АРВ”, 2005.

Линник А.І. (ВІТІ НТУУ „КПІ”)

ВПРОВАДЖЕННЯ ЧЕТВЕРТОГО ПОКОЛІННЯ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ

Серед існуючих телекомунікаційних засобів найстрімкіше розвиваються системи стільникового зв’язку, які спочатку розроблялися з метою забезпечення радіозв’язком великого числа рухомих абонентів з виходом в телефонну мережу загального користування. Зараз система стільникового зв’язку – це складна і гнучка технічна система. Вона може забезпечувати передачу мови та інших видів інформації, зокрема факсимільних повідомлень і комп’ютерних даних. Використання сучасної технології дозволяє забезпечити абонентам такої мережі високу якість мовних повідомлень і великий спектр додаткових послуг.

У стільниковому зв’язку зміна поколінь виражена набагато яскравіше, ніж, скажімо, в індустрії персональних комп’ютерів або іншої подібної техніки.

У мобільному світі все чітко:

– 1G (перше покоління) – це аналоговий зв’язок (стандарт NMT);

– 2G – покоління цифрового зв’язку з комутацією каналів (стандарти GSM і CDMA);

– третє покоління – 3G (стандарт UMTS) – передбачає разом з комутацією каналів і пакетну передачу даних;

– до сімейства 4G, як правило, відносять технології, які дозволяють передавати дані в стільникових мережах з швидкістю вище 100 Мбіт/с [1].

Четверте покоління пристроїв – це повноцінний мультимедійний „офіс в кишені”. Саме на це і направлені вимоги IMT-Advanced по забезпеченню такими системами швидкості до 100 Мбіт/с для мобільних і 1 Гбіт/с для фіксованих абонентів. Спочатку вони були сформульовані в рекомендації, зараз перебувають у стадії постійного уточнення. Це – можливість встановлювати голосові з’єднання, одночасно можливість для різних інформаційних сервісів – робота в Інтернеті, обміну великими масивами даних, проглядання ТБ-трансляцій (IPTV), відео за запитом і т.п. Тобто все те, що користувач має сьогодні у себе удома (в офісі). І все це – за дуже невеликі гроші [3].

Системи 4G можна визначити як технології, які увійдуть до пулу стандартів IMT-Advanced . На призначеному для користувача рівні їх будуть відрізняти:

– висока (від 100/1000 Мбіт/с для мобильних абонентів) швидкість. Це означає роботу одночасно з декількома мультимедійними потоками, різними за природою і вимогам до QoS;

– взаємна сумісність і активна взаємодія. Користувач не повинен відчувати ні перешкод від інших мереж, ні проблем з міжмережевою передачею даних.

На технологічному рівні системи 4G характеризуватимуться:

– повним переходом до модуляції OFDM;

– узгодженістю спільної роботи радіопротоколів фізичного рівня;

– високою гнучкістю при виборі частотних паюс, частотних діапазонів, адаптивною перебудовою методів модуляції;

– застосуванням найбільш довершених методів канального коректуючого кодування (каскадні коди, коди LDPC, і т.п.);

– опорні/базові мережі – повністю IP (з переходом до протоколів IPv6), з’явиться можливість інтеграції систем різних стандартів на базі єдиної NGN-мережі (наприклад, на основі технології MPLS), підтримка платформи IMS.

Всі перераховані технологічні особливості спираються на справді революційні досягнення останніх років у області мікроелектронної елементної бази. Це відноситься не тільки до функціональності самих прийомо-передавальних пристроїв. Адже самі по собі дані користувачу, як правило, не потрібні - йому потрібні засоби їх обробки. Кінцевий споживач хоче дивитися ТБ і відео, обмінюватися повідомленнями, прикріплюючи до них великі

файли, слухати музику, розмовляти і т.п. Для цього необхідна інтеграція мережевих пристроїв в ноут- і нетбуки, комп'ютери, смартфони і т.п. Більше того, мережі 4G без такого роду пристроїв просто даремні. Зараз ці пристрої по відношенню до масового користувача трохи дорогі. Але через три роки їх ціна неминуче впаде до вартості звичайного стільникового телефону. І тоді потреба на швидкісний мобільний контент стане глобальною і загальною [2].

Разом з революційними змінами у області мікроелектронної елементної бази відбуваються і не менш значущі зміни в супутньому програмному забезпеченні і створенні принципово нового інтерфейсу „людина – комп'ютер". Фахівці у області мобільного контента називають це заміною існуючого сьогодні інтерфейсу Web 2.0 на інтерфейс майбутнього Web 3.0.

Поняття мереж наступного, четвертого, покоління (4G) нерозривно пов'язане зі створенням універсальних мобільних мультимедійних мереж передачі інформації. Сьогодні дві групи технологій явно націлені на надання універсальних послуг зв'язку. Це WiMAX (як розвиток лінії IEEE 802) і технології стільникового зв'язку поколінь „супер 3G". Причому, кожна з них займає свою нішу на великому ринку бездротового зв'язку. Однак вимоги кінцевих користувачів до наданих послуг постійно підвищуються. Мобільні мережі повинні використовуватися не тільки для стільникового зв'язку, але й для передачі відео, мобільного ТБ, музики й роботи в Інтернеті з високими швидкостями і якістю передачі.

Мобільний WiMAX та LTE легко справляються зі збільшенням швидкості передачі даних. Однак, виникає інша глобальна проблема – сумісність. Для вирішення цієї проблеми необхідно узгоджувати протоколи роботи в стільниковому зв'язку. Наприклад, повинні співпадати тривалість кадрів і зони вихідних та вхідних каналів при одночасному дуплексі. Обов'язкова масштабованість по частотним смугам з однаковою для різних технологій кратністю [1].

Системи LTE – це революційне покращення 3G. LTE представляє перехід від системи CDMA до системи OFDMA, а також перехід до повністю IP-системи з комутацією пакетів. Тому впровадження цієї технології в існуючих мережах стільникового зв'язку значить необхідність нових радіочастотних ресурсів для отримання переваг для широкого канала. Крім того,для забезпечення зворотної сумісності необхідні абонентські пристрої, що працюють в двох режимах. Тому плавний перехід від системи 3G до LTE є проблемою.

Для операторів мобільного зв'язку, з точки зору інвестицій, WiMAX та LTE є рівноцінними. Однак, з точки зору ринкової конкуренції, WiMAX вже є сьогодні, а LTE потрібно чекати – це не вигідно. Тому ряд компаній мобільних мереж розгорнули та поширюють мережі WiMAX. В існуючих системах WiMAX перехід на стандарти наступних рівнів набагато простіший ніж з 3G на LTE. Тому для операторів WiMAX є перспективнішим ніж LTE.

Таким чином, на сьогоднішній день, телекомунікаційна мобільна мережа 4G має багато якісних переваг у порівнянні з існуючими в даний час стандартами стільникового зв'язку. Як стільникова телефонія дозволила бути на зв'язку завжди і скрізь, так і система 4G зможе забезпечити всіх і кожного надійним високошвидкісним доступом до різних мереж передачі даних.

ЛІТЕРАТУРА

1. *Вишневский В.М., Портной С.Л.,* Шахнович И.В. Энциклопедия WiMAX. Путь к 4G.М.: Техносфера, 2009. – 472 с.

2. *Вишневский В.М., Ляхов А.И.,* Портной С.Л., Шахнович И.В. Широкополосные беспроводные сети передачи информации. – М.: Техносфера, 2005.

3. *Шахнович И.* Широкополосная мобильность: IEEE 802.16e. Часть 1: MAC-уровень. – Электроника: НТВ, 2007, № 2, с. 18 – 27.

4. *Каранен Х.* и др. Сети UMTS. Архитектура, мобильность, сервисы. – М.: Техносфера. 2007, 460 с.

д.т.н. Лисенко О.І. (ІТС НТУУ «КПІ»)
Валуйський С.В. (ІТС НТУУ «КПІ»)

ПІДВИЩЕННЯ СТРУКТУРНОЇ НАДІЙНОСТІ БЕЗПРОВОДОВИХ ЕПІЗОДИЧНИХ МЕРЕЖ ІЗ ПОВІТРЯНИМИ РЕТРАНСЛЯТОРАМИ

Одним із шляхів підвищення структурної надійності (зв'язності) безпроводових епізодичних мереж (БЕМ) є застосування повітряних ретрансляторів (ПТ), в якості додаткових вузлів [1]. Оснащенні більш потужним радіоінтерфейсом, ПТ мають змогу з'єднатися з більшою кількістю вузлів, аніж наземні вузли, та значно підвищити таким чином структурну надійність мережі. Тому *метою* роботи є аналіз та розробка принципу оптимального розміщення ПТ в структурі БЕМ для підвищення її надійності.

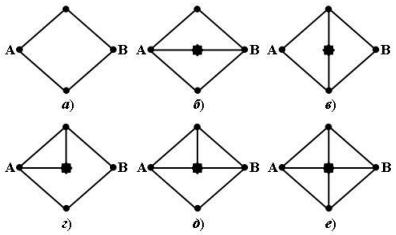


Рис.1. Приклади структури БЕМ (4 вузли та 1 ПТ)

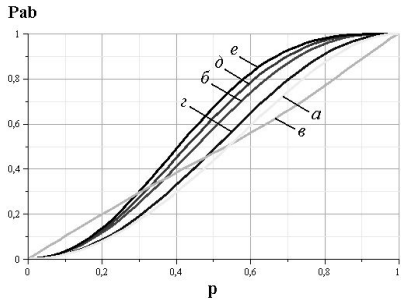


Рис.2. Залежність СЗ від надійності ребра

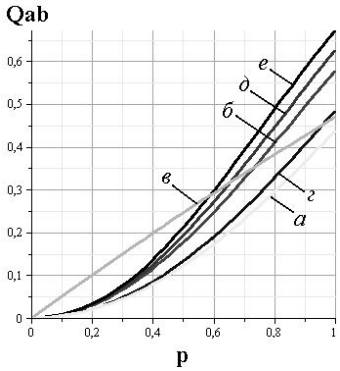


Рис.3. Залежність ІЗ від надійності ребра

Для знаходження оптимального принципу розміщення ПТ в БЕМ проаналізуємо наступні структури в напрямку вузлів АВ (рис.1). Для оцінки надійності будемо використовувати показники структурної зв'язності (СЗ) Pab, що враховує лише потенційну надійність мережі, та інформаційної зв'язності (ІЗ) Qab, що враховує ще й обмеження канального ресурсу. Використовуючи формули послідовного та паралельного з'єднання ненадійних елементів, а також метод розкладання Шеннона – Мура, отримаємо наступні графіки залежності СЗ і ІЗ від надійності ребра p (рис.2,3).

Аналізуючи ці графіки при надійності ребра, наприклад, 0,8, можемо бачити, що значення інформаційної зв'язності менші відповідних значень структурної зв'язності. Отже можна зробити висновок, що ймовірність зв'язності між вузлами мережі істотно залежить не тільки від надійності ліній зв'язку мережі, а й від ймовірності наявності в даний момент часу вільних канальних ресурсів.

Також аналізуючи вище вказані графіки можемо бачити, що більшу надійність мають структури (*е*), (*д*) і (*б*). Виходячи з цього можна зробити висновок, що для підвищення структурної надійності мережі ПТ слід розміщувати таким чином, щоб покрити (зв'язати) пару вузлів, в напрямку яких оцінюється надійність, та якомога більшу кількість інших вузлів мережі.

ЛІТЕРАТУРА

1. *Лисенко О.І., Валуйський С.В.* Метод оптимального управління топологією мережі безпілотних літальних апаратів за критерієм підвищення зв'язності безпроводових ad-hoc мереж // Системи управління, навігації та зв'язку. – 2010. – вип.2(14). – С. 218 – 224.

Литвин К.М. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМ СПРЯЖЕНИХ ГРАДІЄНТІВ В НЕЙРОННИХ МЕРЕЖАХ

Штучна нейронна мережа – це модель обробки інформації, працююча за тими ж принципами, за якими працюють біологічні нервові системи. Вперше дане поняття виникло при спробі змоделювати та систематизувати процеси мислення, протікаючі у мозку людини. Згодом, отримані системи почали застосовуватися у практичних цілях внаслідок їх специфічних можливостей і якостей. На відміну від обчислювальних структур, які використовуються в стандартних персональних комп’ютерах і мають один або декілька складних процесорів, нейронна мережа складається з великої кількості з’єднаних між собою простих процесорів. Кожен з цих процесорів має свою обмежену функцію, однак велика їх кількість, об’єднана в систему, здатна вирішувати складні завдання.

Специфіка побудови и функціонування надає даному типу структур наступні корисні властивості:

– адаптивне навчання. Можливість навчитися вирішенню задач на основі наданих для навчання даних або попереднього досвіду.

– робота в реальному часі. Обчислення в мережі можуть здійснюватися паралельно, при застосуванні відповідних апаратних умов.

– стійкість до ушкоджень. Часткове пошкодження мережі призводить до зменшення ефективності, але неушкоджені елементи залишаються в функціональному стані, що робить можливим подальше застосування деяких її можливостей.

– низьке енергоспоживання. Окремий обчислювальний процес в нейронних мережах потребує застосування відносно невеликої кількості простих процесорів, кожен з яких сам по собі потребує незначних енергетичних витрат.

Асоціативна пам’ять. Здатність нейронних мереж до виявлення взаємозв’язків між різними параметрами дає можливість виразити великий об’єм даних більш компактно, якщо вони мають спільні властивості.

Нейронні мережі не програмуються як традиційні моделі, але здатні до навчання. З біологічної точки зору, навчання полягає у специфічній настройці синоптичних зв’язків між нейронами. З технічної, навчання є процесом знаходження коефіцієнтів зв’язків між поєднаними у систему простими процесорами. В процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними та вихідними даними. Для навчання нейронних мереж створюються спеціальні алгоритми, що являють собою набір дій і інструкцій для спрямування роботи нейронної мережі в потрібному напрямку.

Існують сучасні алгоритми другого порядку, такі як метод спряжених градієнтів, які вирішують деякі задачі набагато швидше, ніж стандартний метод зворотного розповсюдження. Даний метод представляє собою варіант реалізації алгоритму лінійного пошуку, який працює наступним чином: обирається раціональний напрям руху по багатовимірній поверхні, найчастіше це напрям найкоротшого спуску. В цьому напряму проводиться лінія, і на ній знаходиться точка мінімуму. Потім алгоритм повторюється N кількість разів. При знаходженні точки мінімуму вздовж деякої прямої маємо похідну по цьому напряму рівну 0. Спряжений напрям обирається таким чином, щоб ця похідна і надалі залишалася рівною 0, при умові що поверхня має форму параболоїда. Якщо ця умова виконана, то для досягнення точки мінімуму достатньою буде M кількість епох, причому цей показник буде набагато меншим, ніж аналогічний при застосуванні методу зворотного розповсюдження, що означає суттєве збільшення швидкості навчання нейронної системи.

Таким чином на даний момент часу алгоритм спряжених градієнтів є одним з найефективніших методів навчання нейронних систем з точки зору швидкості навчання, незначного коефіцієнту помилок і відповідності вихідних даних, що значно поширює галузь його застосування і поліпшує якість роботи порівняно з алгоритмами першого порядку.

Лубенець А.А. (ВІТІ НТУУ ,,КПІ”)

ТЕЛЕФОНА МЕРЕЖА ЗВ’ЯЗКУ НА ПЛАТФОРМІ ASTERISK

Ключовою подією в історії телекомунікацій і інтернету стала поява технології передачі голосу по IP-мережі, тому за останні роки змінилося само поняття телефону. Використання VoIP сучасно, зручно, дешево, оскільки можна об’єднати видалені офіси, навіть не удаючись до послуг операторів телефонного зв’язку.

Asterisk є відкритою платформою марки Digium, що працює під різними операційними системами (Linux, Windows, FreeBSD, OS X) і дозволяє будувати і модифікувати телефонну станцію малих і середніх розмірів. Відкрита платформа означає ліцензійну програму з початковим текстом, не пов’язаним обмеженнями на подальшу модифікацію. Незважаючи на свою софтовость, Asterisk має усі функції класичної АТС, і навіть більше. Ось тільки деякі з них: центр обробки викликів, голосова пошта, можливість проведення конференцій, що у результаті робить його потужною і легко расширюваною платформою для створення телекомунікаційного сервісу будь-якого масштабу. Підтримуються практично усі популярні протоколи IP-телефонії (SIP, H.323, MGCP, Skinny/SCCP, Google Talk, Skype), власний IAX і деякі інші для роботи відео і факсу. Окрім обслуговування локальних клієнтів Asterisk уміє передавати голосовий трафік між серверами. Є модулі для сполучення з аналоговими (FXO/FXS) і цифровими (T1/E1) лініями.

Asterisk – це вільне програмне забезпечення з відкритим кодом (Open Source) для протоколів VoIP-телефонії (,,Voice over IP”). Платформа працює на операційних системах сімейства UNIX (FreeBSD і Solaris, наприклад), Linux (RedHat і Debian), і дає безліч можливостей для якісного зв’язку нового покоління. ,,Астеріском” є IAX (Inter-Asterisk EXchange), тоді як більшість продуктів IP-телефонії працює під SIP. ,,Астеріск” підтримує SIP, проте використовує його менш функціонально. Крім того, немає перевірених даних про тести роботи ,,Астеріска”, наприклад, під дуже великим числом користувачів.

Asterisk створений максимально гнучким таким чином, що ядро системи, що забезпечує внутрішній взаємозв’язок усередині централі, відокремлене від модулів протоколів, кодеків і апаратних інтерфейсів, які, у свою чергу, дозволяють використовувати не лише сьогоднішні технології і апаратні інтерфейси, але і ті, які тільки з’являться в майбутньому. Найбільша дивність усіх існуючих у світі традиційних телекомунікаційних стандартів – уявна нездатність різних виробників реалізувати їх однаково. Кожен виробник бажає досягти глобальної монополії, таким чином, концепція сумісності відходить на задній план в гонитві зайняти перше місце на ринку з новою ідеєю. ISDN-протоколи – класичний приклад цьому. Розгортання ISDN було хворобливим і дорогим підприємством, оскільки кожен виробник вирішив реалізувати його небагато по-своєму. ISDN міг би забезпечити появу масштабної загальнодоступної мережі передачі даних на 10 років раніше створення Інтернету.

Отже, потужність телефоної платформи Asterisk – у відкритості. За останні декілька років стало очевидним: стандарти міняються настільки нестримно, що не відставати від них допоможе тільки уміння швидко реагувати на нові напрями, що виникають в технології. Asterisk, через те що є системою з відкритим початковим кодом, ідеально підходить для такого типу швидкої розробки, який забезпечить відповідність так стандартам, що швидко змінюються. Asterisk не орієнтується на аналіз рентабельності або дослідження ринку. Вона розвивається у відповідь на усе, що, на думку співтовариства, є цікавим або необхідним. Телефонія з відкритим початковим кодом ставить телефонний зв’язок в один ряд з іншими інформаційними технологіями. Нарешті можна приступити до власне реалізації завдання по інтеграції електронної пошти, голоси, відео і усього, що тільки можна представити, по гнучких транспортних мережах (як дротяним, так і безпровідним) у відповідь на потреби користувача, а не по примсі монополій.

Лук'янчук І.В. (ВІТІ НТУУ „КПІ")

ОБРОБКА СИГНАЛІВ ЗЕМНИХ СТАНЦІЙ НА БОРТУ СУПУТНИКА РЕТРАНСЛЯТОРА З ЦИФРОВИМ ДІАГРАМО УТВОРЕННЯМ

Під час роботи через системи супутникового зв'язку ССЗ кількох кореспондентів одночасно, цифрова антенна решітка ЦАР [1] бортового ретранслятора необхідно формувати промені діаграми спрямованості антенної системи в їх напрямках. Рух ретранслятора обумовлює необхідність визначення та відслідковування оптимального напрямку прийому (передачі) та рівня потужності сигналу.

Тому пропонується визначити порядок роботи ЦАР в такому порядку:

– визначення кількості кореспондентів в зоні обслуговування супутника – ретранслятора;

– визначення кутових координат земних станцій;

– формування просторових каналів в напрямку на кожного кореспондента.

Для реалізації цих завдань, необхідно обробку сигналів можливо вести різними методами спектрального аналізу з високою розподільною здатністю.

Дослідження показали, що перевагу необхідно віддати методу Кейпона, MUSIC [2], та простору станів, що дозволяє не тільки оцінити кількість кореспондентів та напрямки приходу сигналів але і виміряти відносні рівні їх потужності.

Найбільш відомий метод Кейпона, якій спирається на формування зворотної кореляційної матриці [3].

Реалізація інших методів передбачає операцію розподілу власних значень кореляційної матриці на сигнальні та шумові (оцінка числа сигнальних власних значень еквівалентна оцінці кількості сигналів кореспондентів, що пеленгуються) характеристики [4,5,6].

За результатами досліджень встановлено, що поліпшення характеристик розрізнення при використанні методів пов'язаннях з обертанням кореляційної матриці істотно залежіть від відношення сигнал/шум прийнятих сигналів.

При багатосигнальному режиму прийому, коли в основному промені діаграми спрямованості ЦАР знаходяться кілька кореспондентів, зазначені процедури надрозрізнення більш ефективні за умов достатнього відношення сигнал/шум.

ЛІТЕРАТУРА

1. *Помехоустойчивость* и эффективность систем передачи информации / Под ред. А. Г.Зюко. – М.: Радио и связь, 1985. – 272 с.

2. *Банкет В. Л.,* Дорофеев В. М. Цифровые методы в спутниковой связи. – М.: Радио и связь, 1988. – 240 с.

3. *Гуткин Л. С.* Проектирование радиосистем и радиоустройств : Учебное пособие для вузов. – М.: Радио и связь, 1986. – 334 с.

4. *Сервинский Е. Г.* Оптимизация систем передачи дискретной информации. – М.: Связь, 1974. – 336 с.

5. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

6. *Spread Spectrum* Communication // M.K. Simon, J.K. Omura, R.A. Scholtz, B.K. Levitt. – V. 1. – Rockwille, M.D: Computer Science Press, 1985. – V. 1. – 402 p. –V. 2. – 358 p. – V. 3. – 423 p.

Лунькова Г.В.(АСВ)

СТВОРЕННЯ МОДЕЛІ ВІРТУАЛЬНОГО НАВЧАЛЬНОГО СЕРЕДОВИЩА АКАДЕМІЇ СУХОПУТНИХ ВІЙСЬК.

В умовах входження України у світовий освітній простір та становлення і розвитку сучасного глобального інформаційного суспільства, згідно з Національною доктриною розвитку освіти та Національною програмою інформатизації України основними пріоритетами розвитку системи освіти стають модернізація й підвищення якості освіти. Основою ефективної реалізації даних напрямків є, насамперед , удосконалювання сучасної педагогічної системи, адекватної потребам суспільства й функціонуючої на базі сучасних телекомунікаційних технологій та високоавтоматизованого інформаційного середовища. Підготовка офіцера вищого військового навчального закладу (ВВНЗ) має значні особливості обумовлені специфікою військового середовища та окреслені Державною програмою розвитку Збройних Сил України на 2006-2011 роки. Концепція розвитку військової освіти в Україні передбачає підготовку фахівців усіх рівнів та ланок військового управління з творчим мисленням, з високим рівнем професійної компетентності, здатних ефективно керувати особовим складом та бойовою технікою в екстремальних умовах сучасного бою. Все це потребує широкого використання комп'ютерних технологій в процесі навчання, що формує у майбутнього офіцера сучасний світогляд, вміння застосувати сучасні підходи і технологій в набутті знань та навичок.

Нововведення в освітньому середовищі Академії сухопутних військ (АСВ) впроваджуються з урахуванням вимог Болонського процесу до системи вищої освіти відповідно до концепції розвитку інформаційних технологій в АСВ. Мова йде про трансформацію навчального процесу у технологію навчання тобто адекватну зміну існуючої педагогічної системи в умовах розвитку засобів інформаційно-комунікаційних технологій. Основні елементи педагогічної системи, включаючи педагогічні завдання й педагогічні технології для їхнього вирішення, на сучасному етапі повинні розглядатися в додатку до педагогічного процесу в новому освітньому (інформаційному, інтерактивному, мультимедійному, інформаційно-освітньому) електронному середовищі.

В зв'язку з цим актуальним є аналіз, проектування та розвиток інформаційних освітніх систем, створення моделей та методів їх цілісного осягнення.

Розвиток інформаційно – навчального середовища АСВ на сучасному етапі розвитку освітнього середовища закладу відбувається в основному за рахунок впровадження авторських програмних продуктів, які являють собою найчастіше локальні розробки, спрямовані на вивчення окремих предметів або розділів дисциплін, які є незамінним засобом для активізації й інтенсифікації подачі навчального матеріалу під час аудиторних занять і для самостійної роботи курсантів. Викладач, використовуючи яку-небудь технологію (HTML, PowerPoint, Front Page) або просто створюючи електронний документ розробляє навчальний контент. На всіх факультетах Академії сухопутних військ розроблені електронні посібники по провідних дисциплінах. Як правило використовується технологія HTML (редактор Front Page), з'являються посібники на основі більш сучасних технологій (Flash анімація). Розроблений інтерактивний курс „Психологія" містить в собі комплекс навчальних модулів, словники, мультимедійні додатки та тестовий блок. Недоліком таких продуктів є неможливість відслідковувати й контролювати в часі процес навчання й успішність великої кількості курсантів. Відсутність зворотного зв'язку курсантів і викладача сильно знижує ефективність їхнього використання, недоліком таких продуктів є неможливість відслідковувати й контролювати в часі процес навчання й успішність великої кількості курсантів. Як правило, вони розроблені для створення занять з негайним зворотним зв'язком з курсантом, а не для зберігання інформації про навчальний процес за тривалий час. Таким чином для вирішення відзначеної проблеми необхідно вирішити комплекс задач пов'язаних з

трансформацією, адекватним вдосконаленням сучасного освітнього середовища на основі комп'ютерних технологій навчання.

Потенційні можливості для розв'язку вказаної проблеми і комплексу пов'язаних з нею задач надає об'єктно – орієнтоване програмування та відповідно побудова на його основі ефективного модульного об'єктно – орієнтованого навчального середовища .

На основі порівняльного аналізу засобів організації електронного навчання, тобто: авторських програмних продуктів (Authoring Packages), систем керування навчанням (Learning Management Systems – LMS), систем керування контентом (Content Management Systems – CMS), систем керування навчальним контентом (Learning Content Management Systems – LCMS, виявилось, що лідером серед відкритих програмних продуктів є модульне об'єктно-орієнтоване середовище управління навчанням – „Moodle". „Moodle" – це система керування вмістом сайту (Content Management System – CMS) або система керування курсами (Courses Management system – CMS), розроблюється на принципах Open Source під ліцензією GNU GPL, розповсюджується безкоштовно як Open Source-проект і дозволяє копіювати, використовувати і змінювати програмний код.

Аналіз проводився по критеріям: функціональність – наявність набору функцій різного рівня; надійність; стабільність; вартість; відсутність обмежень за кількістю ліцензій на слухачів (курсантів); наявність вбудованих засобів розробки та редагування навчального контенту; підтримка міжнародного стандарту SCORM; система перевірки та оцінки знань слухачів в режимі он-лайн; зручність та простота використання та навігації – інтуїтивно зрозуміла технологія навчання.

Крім базового функціонала, що вже став стандартним для будь-якого інформаційно – комунікативного середовища, Moodle підтримує безліч власних форм взаємодії, що виводять дистанційний навчальний процес зовсім на інший рівень ефективності. У їхньому числі: можливість створювати довільні, у тому числі й нечислові шкали оцінювання; оцінювання викладачами й однокурсниками за активність у форумі; збір і рецензування робіт у текстовому форматі, у вигляді довільних файлів і у вигляді довільної активності; глоссарії; бази даних (з форматом якій настроюється); wiki; тести Hot Potatoes (множинний вибір, коротка відповідь,чисельний, питання так/ні, вибір правильної відповіді з декількох варіантів відповідей, ессе); опитування; навчальні картки, запропоновані залежно від коректності рішення тесту в попередній картці (модуль „лекція"); семінари (учням пропонується спершу здати роботи, а потім оцінити роботи своїх колег за заданими критеріями).

Вся активність користувачів у системі фіксується й відображається у вигляді індивідуальних звітів про діяльності (портфоліо), у яких на одній сторінці можна бачити всі виконані завдання, здані роботи й отримані рецензії та оцінки за кожним курсом.

Таким чином інтеграція моделі віртуального навчального середовища АСВ (на основі об'єктно – орієнтованого середовище управління навчанням) в освітнє середовище Академії дозволяє взяти на себе такі організаційні задачі, як підтримка розробки навчального контенту; проведення атестаційних заходів і контроль успішності; підтримка спілкування викладачів та слухачів; підвищення кваліфікації викладачів, тобто вирішує завдання оптимізації навчання та приводить до якісної зміни навчального процесу навчального закладу.

ЛІТЕРАТУРА :

1. *Гамула І.* Особливості реформування системи вищої військової освіти відповідно до вимог Болонського процесу. // Вища освіта України. – 2006, – № 3 – С. 60 – 64.

2. *Ягупов В.В.* Теорія та методика військового навчання: Монографія. – К.: Тандем, 2000. – 532 с.

к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Шаціло П.В. (ВІТІ НТУУ „КПІ”)

ВИКОРИСТАННЯ ПАРАМЕТРИЧНИХ МОДЕЛЕЙ ITEM RESPONSE THEORY ДЛЯ РЕАЛІЗАЦІЇ АДАПТИВНИХ АЛГОРИТМІВ ОЦІНКИ ЗНАНЬ В КОМП'ЮТЕРНИХ СИСТЕМ НАВЧАННЯ

Ефективність управління процесом навчання, якість досягенння цільового призначення комп'ютерної системи навчання (КСН) прямопропорційно залежіть від організації зворотнього зв'язку між КСН і об'єктом навчання з метою визначення об'єктивної оцінки ступеня його підготовленості.

При вимірі рівня знань згідно класичної моделі тестування, для кожного навчаємого формується тест певної довжини з вибраних випадковим чином завдань тестового простору. При цьому тести відрізняються по ступеню складності, і підсумкова оцінка формується по числу правильних відповідей з урахуванням вагових коефіцієнтів завдань. Недоліком такої оцінки знань є недостатня об'єктивність у оцінці навчаємого. Для забезпечення максимальної інформативності результатів контролю необхідно, щоб середня складність тесту, яка пред'являється навчаємому, відповідала його гіпотетичному рівню підготовленості. Практично це можна здійснити за допомогою *адаптивного тестування*.

Під *адаптивним тестовим контролем* розуміють комп'ютеризовану систему науково обгрунтованої перевірки і оцінки результатів навчання, що має високу ефективність за рахунок оптимізації процедур генерації, пред'явлення і оцінки результатів виконання адаптивних тестів або адаптивних практичних завдань.

Проте побудувати адекватну модель тестування складно, оскільки рівень підготовленості (як параметр, що вимірюється) і рівень складності тестових завдань (як параметр завдання, що встановлюється при атестації навчаємого) мають різні метрики.

Пропонується використання параметричних моделей *Item Response Theory* (*IRT*) у програмній логіці КСН з метою вирішення наступних завдань педагогічного вимірювання: знаходження та оцінювання параметрів рівеня складності навчальних завдань δ та параметрів рівня знань навчаємих θ; знаходження ймовірності P правильної відповіді навчаємих будь-якого рівня підготовленості на завдання певного рівня складності.

Основною математичною моделлю *IRT* є однопараметрична логістична функція Раша, що має назву характеристичної кривої і яка має вигляд:

$$P_j = \frac{1}{1 + exp(\delta_j - \theta)}, \qquad (1)$$

де Pj − ймовірність правильної відповіді навчаємих будь-якого рівня підготовленості на завдання певного рівня складності під номером j; δj − рівень складності конкретного j-го завдання спроектованого тесту; θ − рівень знань навчаємого, латентна змінна;

Чим вище крутизна функції P, тим вужчий інтервал, на якому це завдання працює. Внаслідок цього пропонується поліпшення моделі Раша за рахунок уведення у вираз (1) другого параметра a_j. Параметр a_j надає інформацію про тестове завдання з точки зору оцінки його диференціюючої здатності на заданому інтервалі. Після уведення у вираз параметра a_j отримується двохпараметрична модель:

$$P_j = \frac{1}{1 + exp\, a_j(\delta_j - \theta)}. \qquad (2)$$

Емпіричні межі значень для параметра a_j − від мінус 2,80 до плюс 2,80. Можливо також додавання параметра C, що визначає ймовірність вгадування правильної відповіді (виконання правильної практичної дії).

Виникає проблема адекватної оцінки складності тестових завдань і початкового рівня знань навчаємих.

Початкова оцінка рівня знань навчаємого визначається по формулі:

$$\theta_i = ln\left(\frac{P_i}{q_i}\right), \tag{2}$$

де P_i − доля правильних відповідей *i*-го навчаємого, q_i − доля неправильних відповідей.

Аналогічно визначається початкова оцінка рівня складності завдання тесту:

$$\delta_i = ln\left(\frac{q_j}{P_j}\right), \tag{3}$$

де P_j − доля правильних відповідей на *j*-е завдання тесту , q_i − доля неправильних відповідей. Через дію різних випадкових чинників оцінки параметрів θ і δ, що отримані на декількох вибірках будуть, звичайно, розрізнятися. Якщо об'єм вибірки досить великий, то можна ставити питання про обчислення стійких значень параметрів θ і δ, які будуть найбільш ефективними оцінками і можуть бути прийняті у якості об'єктивних оцінок параметрів θ і δ.

При будь-якому проведенні процесу тестування результати обчислення $\widetilde{\theta}_i$-статистичних оцінок θ_i, і $\widetilde{\delta}_j$- статистичних оцінок δ_j будуть відрізнятися від існуючих точних значень. По своєму сенсу оцінки є певними функціями початкових випадкових значень елементів матриці відповідей A_{nk}, яка складається з N -рядків і K -стовбців і тому самі є випадковими величинами.

Таким чином, виникає питання про знаходження математичних очікувань і дисперсій цих випадкових величин. Необхідно, щоб математичне очікування відповідних оцінок співпадало з відповідними точними значеннями, а дисперсія оцінки була б мінімальною. Статистична оцінка рівня підготовленості і рівня ускладненості тестового завдання будуть незміщеними оцінками, якщо їх математичне очікування при будь-якому об'ємі вибірки навчаємих дорівнюватиме самому параметру, що оцінюється. На практиці, зазвичай, використовують асимптотично незміщену оцінку, математичне очікування якої прагне до істиного значення параметра, що оцінюється, при необмеженому збільшенні об'єму вибірки. Статистична оцінка є ефективною, якщо при заданій вибірці (вона має найменшу дисперсію D^* при неповній інформації), можливо отримати лише оцінку з $D>D^*$. Якщо відношення $D/D^* \rightarrow 1$ при збільшенні вибірки, то оцінка називається асимптотично ефективною. Статистична оцінка є спроможною, якщо незміщена оцінка не є ефективною, але при збільшенні об'єму вибірки її дисперсія зменшується. Незміщеність, ефективність і спроможність є незалежними властивостями, що характеризують оцінки з різних сторін. Завдання пошуку ефективних незміщених оцінок має особливо важливе значення при обробці результатів малих вибірок тих, хто підлягає тестуванню.

Для отримання оцінки параметрів δ і θ застосовуються метод моментів або метод найбільшої правдоподібності.

Отже, до переваг запропонованої адаптивної моделі тестування з використанням *IRT* можна віднести наявність безперервної шкали рівня підготовленості, що дозволяє співвідносити між собою результати по різним тестовим завданням.

Недоліком цієї моделі тестування є необхідність у калібровці, а саме, у емпірічному визначенні параметрів тестових завдань, що вимагає достатньо великої кількості експериментальних даних.

Таким чином, параметричні моделі доцільно застосовувати при средньо- і широкомасштабній оцінці знань навчаємих із використанням КСН.

Люлін Д.О. (ВІТІ НТУУ ,,КПІ”)
д.т.н. Єрохін В.Ф. (ВІТІ НТУУ ,,КПІ”)

БАГАТОЧАСТОТНІ ЦИФРОВІ СИГНАЛИ ДЛЯ КХ-РАДІОЛІНІЙ ЗА СТАНДАРТАМИ НАТО ТА ПІДХОДИ ДО ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ ЇХ ДЕМОДУЛЯЦІЇ

Вимоги до мінімальної конфігурації нових модемів для магістральних і тактичних ліній зв’язку, які дозволяють гарантувати здатність до взаємодії у системах військового зв’язку містяться у стандартах НАТО STANAG 4481, 4197, 4285, 4415, та MIL.STD 188.110. Ці модеми призначені для використання в системах зв’язку „абонент – абонент”, у каналах, що комутируються, загального користування (PSN), а також у спеціалізованих системах зв’язку середньо- і короткохвильового діапазону та ін. Аналіз таких вимог надає можливість пошуку шляхів їх модернізазії та подальшого розвитку.

Для забезпечення ортогональности окремих піднісівних багаточастотного сигналу у відповідності із вище згаданими стандартами НАТО та стандартами серії MIL.STD 188.110 використовується частотне рознесення.

Сигнал на виході модулятора складається з 39 ущільнених по частоті інформаційних каналів, кожний з яких модулюється за допомогою відносної чотирьохфазної модуляції (QDPSK). Наприклад, при технічній швидкості передачі 44,44 бод (тривалість інформаційної посилки τ =22,5 мс незалежно від швидкості даних на вході модему) частотний рознос між сусідніми піднісівними 39 тонового сигналу відповідно до MIL.STD 188.110 складає 56,25 Гц. Передача кожного сигнального елементу здійснюється за допомогою зміни фази частоти каналу відносно фази попереднього елементу.

Разом з тим, фазові співвідношення між окремими піднісівними є фіксованими. Очевидно, вибір цих співвідношень продиктований бажанням мінімізувати пік-фактор групового сигналу.

При формуванні OFDM-сигналів співвідношення між начальними фазами складових диктуються виняткова прагненням до їхньої ортогоналізації на тривалостях інформаційних посилок.

В обох зазначених випадках детермінований взаємозв’язок між початковими фазами піднісівних може бути використаний для поліпшення якості їх оцінки на прийомі. Для цього слід формувати опорні піднісівні коливання на прийомі від одного джерела, початковою фазою якого необхідно управляти за результатами спостережень у кожному з підканалів.

Для розв’язання завдання синтезу може бути застосована теорія оптимальної нелінійної фільтрації дискретно-безперервних Марковских процесів.

Додатковою перевагою пропонованого підходу є можливість застосування на вході демодулятора гребенчастого керованого фільтра, який забезпечить можливість адаптивного виключення з обробки підканалів, уражених перешкодами.

ЛІТЕРАТУРА

1. *STANAG* 4285, Characteristics of 1200/2400/3600 bits per second single tone modulators/demodulators for HF radio links; 1993.

2. *STANAG* 4415, Charateristics of a robust, non-hopping, serial tone modulator/demodulator for severely degraded HF radio links; 1999.

3. *MIL–STD–188–110B*, Military standard, interoperability and performance standards for data modems; 2000.

4. *STANAG* 4481, inimum technical equipment standards for NAVAL HF SHORE– TO– SHIP broadcast systems; 2002.

Мазниченко Ю.А. (ВІТІ НТУУ „КПІ”)
Панченко І.В. (ВІТІ НТУУ „КПІ”)
Васільєв А.Г. (ВІТІ НТУУ „КПІ”)

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ І ТЕНДЕНЦІЇ РОЗВИТКУ СИСТЕМ СУПУТНИКОВОГО ЗВ’ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЇ VSAT У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Основою сучасних систем управління військами є система зв’язку і передачі даних. При цьому вибір використовуваних засобів радіозв’язку для вирішення завдань організації системи управління безпосередньо залежить від умов організації зв’язку. Проте наявність основних принципів організації зв’язку, до яких належить, – стійкість, безперервність, скритність, надійність, глобальність, дозволяють, в більшості випадків формалізувати вимоги до технічних засобів радіозв’язку і передачі даних.

В той же час, сучасні телекомунікаційні технології пропонують користувачеві для вибору величезну кількість технологій і технічних засобів організації зв’язку в різних радіочастотних діапазонах. Актуальність вибору для збройних сил обумовлюється наявністю жорстких вимог до організації системи зв’язку, її відповідності сучасним умовам проведення військових операцій.

Розвиток військових супутникових систем зв’язку (ВССЗ) пов’язаний із збільшенням кількості мобільних абонентів, впровадженням автоматизованих мереж управління і збільшенням об’єму і різноманітності даних, що передаються по високошвидкісним каналам.

Основною перевагою ВССЗ, на думку представників військових відомств, є можливість управління космічними апаратами (КА) військового призначення в кризових ситуаціях без попереднього узгодження з комерційними операторами, висока міра завадозахищеності і функціональна пристосованість КА для вирішення завдань в інтересах збройних сил в складній радіоелектронній обстановці.

Розгляд досвіду створення ВССЗ провідних країн світу показав, що оптимальна архітектура сучасних ВССЗ повинна включати як супутники зв’язку військового призначення, так і канали, орендовані в комерційних системах супутникового зв’язку.

Надалі, за оцінками аналітиків, тенденція використання комерційних систем зв’язку в інтересах збройних сил неухильно розширюватиметься. Це пов’язано, передусім, з бюджетними обмеженнями, оскільки не кожна країна у змозі мати свою ВССЗ.

Іншою важливою причиною використання комерційних каналів зв’язку є випереджаючі темпи розвитку технологій комерційного зв’язку в порівнянні зі ВССЗ.

Однією з технологій, які використовуються для створення мереж супутникового зв’язку являється технологія VSAT (Very Small Aperture Terminal). Необхідно відмітити, що до основних переваг системи супутникового зв’язку VSAT відносяться: глобальний просторово-часовий рівень забезпечення зв’язку; малі габарити призначених для користувача терміналів і їх відносно невисока вартість, у тому числі і експлутаційна; можливість оперативної організації стаціонарного зв’язку у важкодоступних (віддалених) районах з високою мірою надійності.

В Україні розвиток VSAT технологій пішов дуже швидкими темпами, на даний час проектами VSAT мереж займається близько десяти операторів.

Оскільки Україна на даний момент не має свого орбітального угрупування доцільно використати досвід і технічні можливості цих операторів для забезпечення Збройних Сил України сучасними засобами телекомунікацій і зв’язку.

Виходячи з розглянутих матеріалів і результатів аналізу сучасного стану технічної реалізації технології VSAT, можливо зробити наступні висновки: застосування засобів зв’язку, що підтримують формати передачі даних які відповідають технології VSAT є перспективним для Збройних Сил України з точки зору уніфікації систем зв’язку по стандартах НАТО, вартості обладнання та можливості використання обладнання у майбутньому після запуску національного супутника зв’язку та мовлення.

к.т.н. Макарчук О. М. (ВІТІ НТУУ „КПІ”)

АВТОМАТИЗОВАНІ СИСТЕМИ УПРАВЛІННЯ НАВЧАЛЬНИМИ ЗАКЛАДАМИ: СТАН І ПЕРСПЕКТИВИ

Перспективним напрямком підвищення ефективності управління ВНЗ є впровадження автоматизованих систем управління (АСУ).

АСУ навчальними закладами можуть виконувати такі функції:

ведення баз облікових даних по педагогах, адміністративних працівниках, студентах, аудиторіях, матеріальному обладнанню;

складання навчального плану закладу освіти;

розрахунок навантаження по педагогах, предметах, на семестр, навчальний рік;

тарифікація навчального навантаження;

складання розкладу занять на семестр, навчальний рік;

забезпечення електронного документообігу закладу освіти;

отримання статистичних даних по студентах, педагогах;

формування різноманітних звітів ;

ведення електронної бібліотеки.

Використання засобів АСУ в організації та плануванні діяльності навчального закладу має певні переваги, а саме:

підвищення ефективності навчального процесу;

можливість управління з використанням результатів попередньої діяльності;

прийняття більш ефективних управлінських рішень;

підвищення об’єктивності в оцінці діяльності педагогів та учнів/студентів;

більш ефективне управління пізнавальною діяльністю учнів/студентів;

можливість прийняття більш виважених рішень, які стосуються підвищення результативності навчання;

оперативний доступ до організаційної інформації стосовно діяльності освітнього закладу;

економія як матеріальних, так і людських ресурсів.

Проведено порівняльний аналіз 3-х АСУ, поширених на українському ринку програмних продуктів:

– АСУ „ВНЗ” інформаційно-виробничої системи „Освіта” інституту прикладних інформаційних технологій Кібернетичного центру НАН України;

– АСУ „Політек” фірми „Політек-софт”;

– програмного комплексу „Альма – Матер” фірми „Direct-IT”.

Розглядається якість виконання основних функцій кожним з продуктів, переваги і недоліки, формулюються рекомендації по використанню і пропозиції по вдосконаленню.

Таким чином, за результатами аналізу можна визначити функціональні можливості кожного з перерахованих програмних продуктів і оцінити доцільність їх використання в конкретному ВНЗ.

ЛІТЕРАТУРА

1. *Лунячек В.Е.* Інформаційно-комунікаційні технології в управлінні загальноосвітнім навчальним закладом. – Харків: Основа, 2004. – 96 с

2. К. Т. Кузьма. Аналіз автоматизованих систем управління вищим закладом освіти. – Режим доступу: www.nbuv.gov.ua/portal/natural/Akpa/2008_12/12.pdf

3. *Програма* автоматизації ВНЗ АЛЬМА-МАТЕР. – Режим доступу:<http://www.alma-mater.org.ua>.

4. *ІВС Освіта* Міністерства освіти і науки України. – Режим доступу:<http://www.osvita.net>.

Макарчук О.М. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ МЕТОДІВ ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ В СИСТЕМАХ РАДІОЗВ’ЯЗКУ

У військових системах радіозв’язку завданню підвищення завадостійкості приділяється велика увага. Основними тенденціями розвитку й модернізації військових систем і засобів зв’язку провідних країн є: забезпечення їх високої мобільності, живучості, захищеності та пропускної спроможності; сумісності із мережами загального користування національних систем зв’язку, системами зв’язку й мережами інших військових формувань і партнерів по коаліції; стандартизація засобів і комплексів зв’язку; освоєння нових діапазонів частот.

За останні десятиліття засоби і методи підвищення завадозахищенності радіоелектронних засобів отримали могутній розвиток. Це пояснюється радіоелектронною обстановкою, що головним чином погіршується з кожним роком, проблемою електромагнітної сумісності радіоелектронних засобів (РЕЗ) і активізацією методів радіоелектронної боротьби (РЕБ), які включають в свій склад високоефективні постановники навмисних завад. Сучасні пристрої формування навмисних завад мають невеликі массогабаритні показники і можуть випромінювати в потрібному режимі і з необхідною потужністю будь-яку заваду.

Відмінності в типах завад пояснюється тим, що подавлятися може широкий спектр РЕЗ, що мають різні класи випромінювань. Завдання постановника завад (ПЗ) – створити на вході приймача подавлених РЕЗ неприпустимо низьке, для її нормального функціонування, відношення потужностей сигналу і завади+шум (ВСЗШ), для чого ПЗ випромінює у напрямі РЕЗ найбільш ефективний із його точки зору тип завади. Потрапляючи в смугу пропускання приймача РЕЗ завада змішується з корисним сигналом і маскує його, затрудняючи розпізнавання приймачем. Тому в радіоприймальних пристроях використовують різні. Наприклад, окрім оптимізації схем модуляторів – демодуляторів, до складу схем приймачів радіолокаційних станцій (РЛС) спеціально включені такі схемні рішення, які дозволяють проводити якісну селекцію робочого сигналу і більшості відомих типів завад.

В літературі відомі наступні методи підвищення завадостійкості в системах радіозв’язку:

селективні методи;

методи адаптивної просторової фільтрації;

метод кодової адаптації;

метод структурної адаптації;

завадостійке кодування

Слід відмітити, що кожен із перелічених методів має свої переваги та недоліки.

Селективні методів розраховані на використання оптимального прийому в умовах конкретного типу завад. Як критерій використовується, як правило, максимум відмінності сигналу і завади по частотних, тимчасових, просторових характеристиках, зокрема, відмінностей по ширині спектру, амплітудно-часової і спектральної огинаючої.

При реалізації методів адаптивної просторової фільтрації, як фізичне середовище використовується багатоелементна адаптивна антенна решітка. Як критерій при поділі сигналів і завад використовується розходження в напрямку приходу сигналів і завад. Розходження посилення адаптивною антенною решіткою в різних напрямках дозволяє збільшити ВСЗШ на прийомі. Адаптивність полягає в здатності адаптивної антенної решітки в результаті роботи спеціальних алгоритмів визначати азимут на заваду й змінювати свою діаграму спрямованості таким чином, щоб максимально послабити її вплив.

Основна перевага цих методів полягає в використанні просторового ресурсу та незалежності від типу завад.

Слід зазначити, що перспективним напрямком забезпечення завадозахищеності є структурна адаптація й параметрична (кодова) адаптація.

Метод кодової адаптації з використанням узагальнених каскадних кодів (УКК) для забезпечення завадозахищеності засобів радіозв'язку (ЗРЗ) із стрибкоподібною зміною частоти (СЗЧ) полягає в комплексному використанні адаптивної зміни структури кодека УКК залежно від зміни завадової обстановки. Ефект від впровадження цього методу полягає в збільшенні пропускної спроможності ЗРЗ із СЗЧ у середньому на 15 % і скороченні часу адаптації в умовах впливу навмисних завад на 12...24 %.

Метод структурної адаптації перспективних військових ЗРЗ на основі використання сигнально-кодових конструкцій (СКК) полягає в підвищенні на 16 – 27 % енергетичної ефективності систем рухомого радіозв'язку. СКК із багатопозиційною частотною маніпуляцією та блоковими циклічними кодами дозволяють збільшити енергетичну ефективність системи радіозв'язку на 2...5 дБ за рахунок зниження частотної ефективності при впливі різних видів навмисних завад.

Розглянуті методи орієнтовані на двійкові симетричні канали при середніх відношеннях сигнал-завада (ВСЗ).

Максимальні значення швидкості передачі інформації при заданій достовірності можна одержати шляхом використання завадостійкого кодування в поєднанні зі спектрально-ефективною модуляцією, а також технологіями розширення спектра. При використанні СКК забезпечується виграш по енергетичній і частотній ефективності для каналів із флуктуаційним шумом і завмираннями.

Крім оптимального приймання ефективним методом підвищення завадостійкості в цифрових системах радіозв'язку є завадостійке кодування, яке застосовується спільно з перемежінням символів в передаваємому повідомленні.

Показано, що при впливі оптимальної завади у відповідь на основний канал приймача з частотною модуляцією (ЧМ) максимальна ймовірність бітової помилки $P_{B\max} \approx G_0 / (eE_s)$, а при найгіршій шумовій завaді в частині смуги (ШЗЧС) $P_{B\max} \approx P_j / (eK_s P_s)$, де G_0 – спектральна щільність потужності шуму, e – основа натурального логарифму, E_s – енергія сигналу, K_s – коефіцієнт розширення спектру сигналу. Експоненційний характер залежності змінюється на лінійний, що різко знижує завадозахищеність ЗРЗ. Робочі характеристики ЗРЗ із СЗЧ в умовах таких завад можуть бути значно поліпшені за допомогою коригувальних кодів. В умовах найгірших завад у відповідь (ЗВ) застосування коду Хемінга дозволяє одержати енергетичний виграш близько 8 дБ при $P_{B\max} = 10^{-3}$ та 18 дБ при $P_{B\max} = 10^{-5}$. Аналогічні виграші виходять і у випадку впливу на ЗРЗ ШЗЧС. Так, застосування коду Голея забезпечує енергетичний виграш приблизно 25 дБ при $P_{B\max} = 10^{-3}$. Ще більші виграші в характеристиках завадозахищеності спостерігаються при використанні кодів БЧХ, Ріда-Соломона і узагальнених каскадних кодів (УКК).

Робочі характеристики ЗРЗ із СЗЧ в умовах таких завад можуть бути значно поліпшені за допомогою коригувальних кодів.

Тому для забезпечення завадозахищеності необхідно застосовувати ефективні коригувальні коди.

Всі перераховані методи підвищення завадостійкості можна віднести до сигнальних або фізичного рівня.

Таким чином проаналізувавши розглянуті методи підвищення завадостійкості в системах радіозв'язку можна сказати, що їх застосування залежить від безлічі зовнішніх і внутрішніх факторів, основними з яких є тип каналу, розповсюдження радіохвиль, структурно-функціональні властивості приймача.

к.т.н. Макарчук О.М. (ВІТІ НТУУ „КПІ”)
Микитюк А.В. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ХАРАКТЕРИСТИК СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Безумовним та загальновизнаним є той факт, що рівень розвитку держави та суспільства значною мірою залежить та визначається рівнем їх інформатизації.

Проводячи аналіз стану інформаційної безпеки різних відомств, організацій та фірм, можна прийти до висновку, що об’єктом захисту, який викликає найбільше занепокоєння і акумулює всі проблеми інформаційної безпеки є інформаційно-телекомунікаційні системи, що будуються на базі комп’ютерів.

Для того щоб звести до мінімуму витік інформації розробляються відповідні системи інформаційного захисту, які являють собою сукупність організаційних, інженерно-технічних заходів, засобів і методів технічного та криптографічного захисту інформації.

Склад системи захисту визначається на основі вивчення усіх інформаційних процесів та потоків системи телекомунікацій і, як наслідок, розробці такої моделі загроз, щоб забезпечити мінімізацію втрат.

Одним з напрямків захисту інформації в комп’ютерних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи задач:

– захист інформації від несанкціонованого доступу (НСД);

– захист інформації від витоку технічними каналами.

Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок, акустичні та оптичні канали та інші. Захист від НСД може здійснюватися в різних складових інформаційної системи:

– прикладне та системне програмне забезпечення;

– апаратна частина серверів та робочих станцій;

– комунікаційне обладнання та канали зв'язку;

– периметр інформаційної системи.

Для захисту інформації на рівні прикладного та системного ПЗ нами використовуються:

– системи розмежування доступу до інформації;

– системи ідентифікації та автентифікації;

– системи аудиту та моніторингу;

– системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

– апаратні ключі;

– системи сигналізації;

– засоби блокування пристроїв та інтерфейс вводу-виводу інформації;

Таким чином, розробка програмного середовища для моделювання системи захисту інформації від несанкціонованого доступу з використанням методів теорії масового обслуговування надасть можливість краще оцінити захищеність системи від впливу зловмисника.

ЛІТЕРАТУРА

1. *С.К. Варлатая, М.В. Шаханова.* Программно-аппаратная защита информации: учеб. пособие // – Владивосток: Изд-во ДВГТУ, 2007.

Мєшков І.Н. (НЦЗІ ВІТІ НТУУ „КПІ”)
Мусієнко В.А. (НЦЗІ ВІТІ НТУУ „КПІ”)
к.т.н. Кайдаш І.Н. (НЦЗІ ВІТІ НТУУ „КПІ”)

НАПРЯМКИ РОЗВИТКУ ЗАСОБІВ РАДІОЗВ’ЯЗКУ В ТАКТИЧНІЙ ЛАНЦІ УПРАВЛІННЯ

Сучасний рівень розвитку Збройних Сил України (ЗСУ), якісні зміни у способах і засобах ведення бойових дій поставили питання щодо вдосконалення системи управління в число найважливіших. Технічною основою системи управління ЗСУ, її невід’ємною складовою частиною є система зв’язку та автоматизації. Вона значною мірою визначає ступінь реалізації бойового потенціалу ЗСУ [1].

Система радіозв’язку є складовою частиною системи зв’язку відповідної ланки управління ЗС України. Найважливішу роль радіозв’язок відіграє в тактичній ланці управління (ТЛУ), і майже завжди залишається єдиним засобом управління військами. З впровадженням в практику управління військами автоматизованих систем управління (АСУ) зросли вимоги як до якості каналів радіозв’язку так і до системи радіозв’язку в цілому. До системи військового радіозв’язку в тактичній ланці управління пред’являються також високі вимоги щодо набору і якості послуг, які надаються абонентам. Для реалізації вимог до управління військами в сучасних умовах мережею військового радіозв’язку повинні забезпечуватися:

– автоматичний пошук радіоабонентів за цифровими адресними номерами, зокрема, в умовах їх переміщення та зміни структури мережі радіозв’язку;

– можливість організації автоматичного завадозахищеного адаптивного радіозв’язку між радіоабонентами через вузли радіодоступу;

– можливість обміну інформацією з абонентами систем зв’язку ланок управління, як мінімум, на інстанцію вверх і на інстанцію вниз;

– надання мобільним абонентам (і тим, що переміщаються), засекреченого радіотелефонного зв’язку і можливості передачі даних;

– сполучення зі стаціонарною державною мережею зв’язку по проводових і радіорелейних лініях через автоматичні центри комутації;

– пакетна комутація повідомлень, їх засекречування у групових і абонентських трактах;

– пріоритетність обслуговування вищого командування та можливість проведення конференцзв’язку;

– організація довідкової адресної служби та визначення адреси абонента за кодом, запрограмованим у абонентському терміналі;

– можливість створення ефективної багаторівневої системи автоматизованого управління радіозв’язком [2];

– автоматизація процесів призначення і розподілу частот.

В перспективних комплексах радіозв’язку необхідно використовувати схеми зв’язку, що забезпечують багатостанційний доступ чи повно доступне підключення великої кількості абонентів до обмеженого числа каналів зв’язку Такі системи можуть застосовуватися для організації групового зв’язку рухомих абонентів, а також індивідуальних переговорів. У такій радіосистемі кожному абоненту для зв’язку може бути наданий будь-який із вільних каналів. Усі канали об’єднані загальною системою управління, яка слідкує за каналами, що звільняються, й відразу надає їх наступним абонентам.

Аналіз сучасних систем та засобів радіозв’язку провідних фірм-виробників (Harris – США, Tadiran – Ізраїль, Codan – Австралія, ВАТ„ Концерн Сузір’я” – Росія та ін.) свідчить про те, що при створенні вітчизняних радіозасобів повинні виконуватись наступні вимоги:

– застосування єдиної базової радіостанції з вмонтованим діагностуванням, блочною конструкцією, відкритою (модульною) архітектурою;

– єдиний діапазон для КХ та УКХ радіозасобів;

– локальне та дистанційне управління радіозасобами;

– сучасна елементна база з експлуатаційними характеристиками, що відповідають світовим військовим стандартам;

– єдині способи аналого-цифрового та цифро-аналогового перетворення мови, засекречування інформації;

– підвищення пропускної спроможності систем і засобів радіозв'язку;

– можливість створення автоматизованих (автоматичних) радіоцентрів;

– підвищення надійності засобів і комплексів радіозв'язку;

– використання вдосконалених алгоритмів управління, інформаційного і програмного забезпечення;

– реалізація нових завадо- і розвідзахищених алгоритмів роботи засобів і комплексів радіозв'язку;

– створення уніфікованих перепрограмованих засобів радіозв'язку, в тому числі для взаємодії радіоцентрів ЗС України та з іншими зацікавленими відомствами;

– застосування компенсаторів завад і коригуючих кодів;

– сполучення з опорною мережею ЗС України, з мережами загального користування, комп'ютерними мережами;

– можливість попереднього настроювання не менше ніж на 100 симплексних або напівдуплексних каналів з кроком частот не більшим 10 Гц;

– режими ППРЧ;

– функціональна повнота – портативні, переносні та перевізні радіозасоби;

– автоматизація процесів встановлення, ведення та відновлення зв'язку;

– передавання інформації з комутацією пакетів;

– пріоритетність обслуговування абонентів;

– використання панелей управління з мінімальною кількістю органів управління;

– наявність вмонтованої апаратури навігації (GPS-приймач та ін.);

– зменшення енергоспоживання, маси та габаритів засобів радіозв'язку.

Висновки:

Задовольнити зростаючі вимоги до якості радіозв'язку в ЗС України в цілому і в тактичній ланці управління зокрема можливо тільки шляхом розробки та реалізації комплексної програми зі створення єдиного інформаційного простору ЗСУ, де система радіозв'язку буде представлена як його мобільний компонент. Очевидно, що для виконання сучасних вимог до радіозв'язку необхідні сучасні засоби і комплекси, які мають бути побудовані на єдиному базовому ряду уніфікованих програмно-технічних комплексів: стаціонарних, мобільних, переносних, портативних та ін., призначених для оснащення командних пунктів рівнів з'єднання, частина, підрозділ, командирські машини (командирів рот, взводів, відділень), окремих військовослужбовців.

ЛІТЕРАТУРА

1. *Малярчук М. В.* Проблеми і задачі воєнно-наукового супроводу процесу переозброєння військ зв'язку // ІІІ науково-практична конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. – К.: ВІТІ НТУУ „КПІ", 2006. – С. 10 – 15.

2.*Романюк В.А.* Архитектура системи оперативного управління тактичними радіомережами // Збірник наукових праць ВІТІ НТУУ „КПІ", №3, 2009.– С. 70 – 76.

к.в.н. Микусь С.А. (НУОУ)
Розум І.Ю. (НУОУ)

ПРОБЛЕМИ ВЗАЄМОСУМІСНОСТІ ІСНУЮЧИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З ТЕЛЕКОМУНІКАЦІЙНОЮ МЕРЕЖЕЮ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Існуючі телекомунікаційні системи спеціального призначення (ТКССП) базуються в основному на аналогових системах передавання. Силами і засобами зв'язку можуть розгортатися осі та рокади зв'язку, створюючи опорну мережу. Опорна мережа є некомутованою, з довгостроковою комутацією каналів і трактів на опорних вузлах зв'язку. На вузлах зв'язку здійснюється ручна оперативна і довгострокова комутація каналів та трактів. Канальний ресурс поділяється і закріплюється за кожним видом зв'язку. Канали тональної частоти, як правило, є різнорідними, створюються через опорні вузли зв'язку від одного пункту управління до іншого і закріплюються за інформаційними напрямками. Зазначені обставини обумовлюють низький ступінь використання каналів у телекомунікаційній системі спеціального призначення і необхідність розгортання (обладнання) на вузлах зв'язку декількох комутаційних засобів і абонентських мереж. Автоматична комутація, як правило, застосовується тільки для організації внутрішнього та режимного телефонного зв'язку на вузлах зв'язку. Для захисту інформації застосовується різнотипна апаратура засекречування із закріпленням її за каналами.

Технічна оснащеність існуючої ТКССП знаходиться на рівні розробок 60-70-х років. Значна кількість засобів зв'язку і автоматизації відпрацювала встановлений ресурс, є морально та фізично застарілою і потребує заміни. На сьогоднішній день розпочато модернізацію існуючих аналогових засобів зв'язку. Доля модернізованих цифрових РРС та ТРС складає біля 5% від їх загальної кількості, до того ж вони не працюють зустрічно з аналоговими станціями. Також тільки розпочато заміну апаратних польових вузлів зв'язку на цифрові комплексні апаратні зв'язку, які здатні у повній мірі використовувати ресурси магістралей, утворених цифровими РРС та ТРС. Тому для побудови польових опорних мереж зв'язку можливо використати у переважній більшості лише аналогові, малоканальні радіорелейні та тропосферні станції, які морально та фізично застаріли, ресурс електровакуумних приладів яких практично вичерпано, а також розгорнути обмежену кількість польових кабельних ліній невеликої канальної ємності. При цьому застосування аналогової апаратури з частотним розподілом каналів суттєво обмежить швидкість передавання даних в автоматизованих системах управління військами і не дасть можливості посадовим особам органів управління користуватися більшістю сучасних телекомунікаційних послуг.

Навіть стаціонарний компонент ТКССП не складає собою цілісної системи, являючись у переважній більшості лініями прив'язки вузлів зв'язку до магістральних ліній телекомунікаційних мереж загального користування (ТКМЗК). Також він має вкрай обмежені можливості щодо забезпечення управління внаслідок низької пропускної спроможності, використання застарілого аналогового обладнання, до того ж їх кількість поступово зменшується внаслідок зношення і відсутності коштів на їх ремонт. Тому навіть у мирний час 90% каналів зв'язку для забезпечення управління орендуються з ТКМЗК.

ТКМЗК, на відміну від телекомунікаційної системи спеціального призначення, має розгалужену, взаємопов'язану структуру великої канальної ємності, що дозволяє використовувати основні та резервні шляхи для надання каналів зв'язку. Вузли та центри електрозв'язку оснащені сучасними цифровими засобами зв'язку і автоматизації та базуються на цифрових методах передачі і обробки інформації.

Таким чином, на сьогоднішній день залишається невирішеною проблема сумісності застарілої аналогової ТКССП з сучасними цифровими засобами ТКМЗК.

д.т.н. Мохор В.В. (ІСЗЗІ НТУУ „КПІ”)
Цуркан В.В. (ІСЗЗІ НТУУ „КПІ”)

ВИКОРИСТАННЯ ПРОБІТ-МЕТОДУ ДЛЯ КІЛЬКІСНОГО ОЦІНЮВАННЯ РИЗИКУ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ

Наявність системи управління безпекою інформації є однією з ключових умов стратегічного розвитку будь-якої організації [1]. При цьому визначення вимог щодо розробки, впровадження, використання, моніторингу, аналізу, підтримки та покращення системи управління безпекою інформації повинно здійснюватися в контексті управління ризиком загроз безпеці інформації [2].

Одним із основних і найбільш складних етапів управління ризиком загроз безпеці інформації є аналіз, котрий поділяється на дві стадії:

– ідентифікація ризику *(Risk Identification);*

– оцінювання ризику *(Risk Estimation)*.

Задача оцінювання ризику загроз безпеці інформації у відповідності з [3] передбачає:

– визначення методу оцінювання ризику, який може бути

– якісним;

– кількісним;

– оцінку наслідків інцидентів безпеки інформації;

– визначення характеристик імовірності (випадковості) інцидентів безпеки інформації;

– обчислення рівня ризику.

Згідно [4 – 6], можна констатувати наявність істотних обмежень щодо використання відомих методів кількісного оцінювання ризику загроз безпеці інформації, в зв’язку з чим актуальним є пошук нових підходів, котрі забезпечують розв’язання задачі визначення ймовірності реалізації загрози безпеці інформації в умовах недостатності статистичних даних.

В цьому контексті перспективною вважається можливість застосування пробіт-методу, ідея котрого належить Ч. Бліссу [7].

Відомо [9], що пробіт-функція є математичною залежністю, котра пов’язує специфічні особливості негативного впливу на деякий об’єкт (у нашому випадку – інформаційний актив) із розміром можливих збитків. Вираз для визначення значень пробіт-функції в загальному випадку має наступний вид:

$$\Pr(D) = a + b\ln D + \gamma \ln \tau,$$

де a, b, γ – коефіцієнти, котрі характеризують ступінь уразливості інформаційного активу по відношенню до конкретної загрози або класу загроз; D – оцінка негативного впливу; τ – період часу від початку до кінця негативного впливу.

Для сфер, у яких можна знехтувати часовим періодом актуальності загрози, а саме це характерно для більшості випадків реалізації загроз безпеці інформації, використовується наступна форма представлення пробіт-функції:

$$\Pr(D) = a + b\ln D. \qquad (1)$$

При цьому розв’язок задачі визначення ймовірності реалізації загрози безпеці інформації для кожної пари (загроза, вразливість) виконується в два етапи:

1. Визначення значень елементів пробіт-функції $\Pr(D)$, котрі входять у праву частину виразу (1).

2. Обчислення значень пробіт-функції $\Pr(D)$ та визначення значення ймовірності реалізації загрози безпеці інформації по наступній формулі:

$$P = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\Pr(D)} e^{-\frac{x^2}{2}} dx.$$

Слід особливу увагу звернути на той факт, що у даному виразі немає емпіричних коефіцієнтів. Відповідно, проблема збору статистики у випадку використання пробіт-функції відсутня і, як наслідок, можливе використання відповідних графіків або таблиць на основі окремих досліджень параметрів (коефіцієнтів) a, b і D пробіт-функції.

В цілому, встановлення значень цих коефіцієнтів для кожної пари загроза/наслідки здійснюється в результаті проведення окремих досліджень.

Наприклад, такі дослідження проведені в ентомології, екології, токсикології, фармакології, радіобіології та інших областях біологічних і медичних наук. Відомі приклади таких досліджень в гідротехніці, будівельній механіці, пожежній безпеці та інших сферах, відмінних від безпеки інформації.

Разом з цим, аналіз та ідентифікація особливостей та характеристик, як загроз безпеці інформації, так і вразливостей, властивих різним інформаційним активам, є рекомендацією стандарту [3] і нормативною вимогою стандарту [2].

Наразі виконання таких досліджень для кожної організації та по кожному активу є практично невиконаним завданням, як в силу різноманітності умов і контексту їх функціонування, так і в силу динаміки цих умов у часі.

Використання підходу в основі котрого покладено знаходження значень пробіт-функції, забезпечує, по-перше, єдине методологічне підґрунтя урахування особливостей пар загроза/наслідки для різноманітних інформаційних активів, а, по-друге, дає можливість створити базу для рішення задачі кількісного оцінювання ризику загроз безпеці інформації.

ЛІТЕРАТУРА

1. *Про введення* в дію стандартів з управління інформаційною безпекою в банківській системі України [Електронний ресурс] / Проекти регуляторних актів Національного банку України// Національний банк України. Режим доступу: http://bank.gov.ua/B_zakon/Draft/ 02022010.htm. – Дата доступу: вересень 2009. – Назва з екрану.

2. *ISO/IEC 27001:2005*. Information technology. – Security techniques. – Information security management systems. – Requirements.

3. *ISO/IEC 27005:2005*. Information technology. – Security techniques. – Information Security Risk Management.

4. *Вишняков Я.Д.* Общая теория рисков: учеб. пособие для студ. высш. учеб. заведений / Я.Д. Вишняков, Н.Н. Радаев. – 2-е изд., испр. – М.: Издательский центр „Академия”, 2008. – 368 с.

5. *Буянов, В.П.* Рискология (управление рисками) [Текст] : учеб. пособие / В. П. Буянов, К. А. Кирсанов, Л. М. Михайлов. – 2-е изд., испр. и доп. – М. : Экзамен, 2003. – 382 с.

6. *Живетин В.Б.* Введение в анализ риска [Текст]: монография / *В.Б. Живетин*. – Казань: [б. и.], 1999. – 319 с.

7. *Bliss C. I.* The method of probits // Science. – 1934. – Vol. 79, No. 2037. – P. 38 – 39.

8. *Bliss C. I.* The method of probits – a correction // Science. – 1934. – Vol. 79, No. 2053. – P. 409-410.

9. *Белов П.Г.* Системный анализ и моделирование опасных процессов в техносфере: Учеб. пособие для студ. высш. учеб. заведений / Петр Григорьевич Белов. – М.: Издательский центр „Академия”, 2003. – 512 с.

к.т.н. Наталенко П.П. (ІССЗІ НТУУ „КПІ”)
к.т.н. Колачов С.П. (ВІТІ НТУУ „КПІ”)
Кисиленко П.П. (ВІТІ НТУУ „КПІ”)

БЕЗПЕКА СИСТЕМИ МАРШРУТИЗАЦІЇ В КОРПОРАТИВНІЙ МЕРЕЖІ

Сучасні корпоративні мережі ефективно використовують технологію Inernet (стек протоколів TCP/IP), яка в повному обсязі змінила нашу уяву про інформацію, форми її подання і доступу до неї. Широкий набір сервісних послуг (мережевих служб) e-mail,

Web (HTTP), FTP, відеоконференція, служба Telnet і їх використання по забезпеченню процесу управління силовими відомствами країни підсилює інтерес до впровадження як технології, так і спонукає розвиток напрямків забезпечення безпеки системи маршрутизації.

В доповіді наведено принципи побудови системи маршрутизації в корпоративній мережі на основі розділення її на автономні системи (АС) в межах яких використовуються протоколи динамічної внутрішньої маршрутизації (RIP, IGRP, OSPF), а між системами протокол зовнішньої маршрутизації BGP 4 [1].

Показано, що рекомендована до використання системи маршрутизації спроможна забезпечити необхідну якість передачі інформації і весь набір сервісних послуг.

На основі аналізу можливих атак на систему маршрутизації корпоративної мережі і механізмів її реалізації, а також наслідків їх дії, наведено основні шляхи забезпечення безпеки. Показано, що безпека і надійність системи маршрутизації залежить від можливості правильної відповіді на питання:

– чи є автономна система – відправитель повідомлення BGP дійсним, правомочним джерелом префіксу?

– чи відповідає атрибут AS PATH, отриманий в повідомленні BGP, дійсному шляху, який пройшло дане повідомлення в мережі?

В результаті аналізу шляхів забезпечення безпеки і надійності системи маршрутизації показано, що основним напрямом протидії трафіку від джерела з зфабрикованою адресою є фільтрація вхідного трафіку. Наведено конкретні варіанти реалізації системи маршрутизації в корпоративній мережі.

В роботі проведено аналіз ефективності застосування тунелювання, а також резервного тунелювання з метою забезпечення безпеки і надійності транспортування повідомлень в мережах.

Особлива увага приділена напрямам розвитку корпоративних засобів захисту у відповідності до корпоративних вимог з можливістю використання стандартних програм і апаратних засобів.

Висновки :

1. Рекомендовано до використання в корпоративних мережах фільтрацію вхідного трафіку і вилучення пакетів з можливою фальсифікацією мережевих адрес відправителів повідомлень.

2. Наведені конкретні методи застосування тунелювання з метою забезпечення безпеки системи маршрутизації в корпоративних мережах

ЛІТЕРАТУРА

1. *Науменко М.І., Стасев Ю.В., Рубан І.В.* „Технології комп’ютерних мереж в АСУ військами”. Харків: МОУ, 2004. – 458 с.

к.т.н. Наталенко П.П. (ІССЗІ НТУУ „КПІ”)
к.т.н. Шелепенко Ю.В.(ВІТІ НТУУ „КПІ”)
Білий О.С. (ІССЗІ НТУУ „КПІ”)

ТЕХНІЧНА РЕАЛІЗАЦІЯ СИСТЕМИ МАРШРУТИЗАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Рознесені підрозділи органів державного управління можуть підтримувати зв’язок через мережу Internet. На рис. 1 наведено варіант побудови корпоративної мережі. Корпоративна мережа розділена на автономні системи (АС) в середині яких піднято протоколи внутрішньої маршрутизації RIP v.2 і OSPF, а між АС – протоколи зовнішньої маршрутизації BGP v.4.

В роботі показано що вибір вказаних вище внутрішніх протоколів, а не базової модифікації протоколу EIGPR, обґрунтований наявністю у мережі обладнання різних виробників та наявністю у протоколі RIP v.2 захисту (паролів) таблиці маршрутів на базі алгоритму MD5. Крім того протокол OSPF забезпечує роботу абонентів в мережі через мережу Internet.

Показано, що зовнішній протокол BGP v.4 передбачає використання протоколів iBGP та eBGP, однак це веде до ускладненню конфігурації мережі та збільшенню розмирів таблиці маршрутизації [3].

Розглянути взаємодії протоколів внутрішньої (RIP v.2 і OSPF) і зовнішньої маршрутизації (BGP v.4).

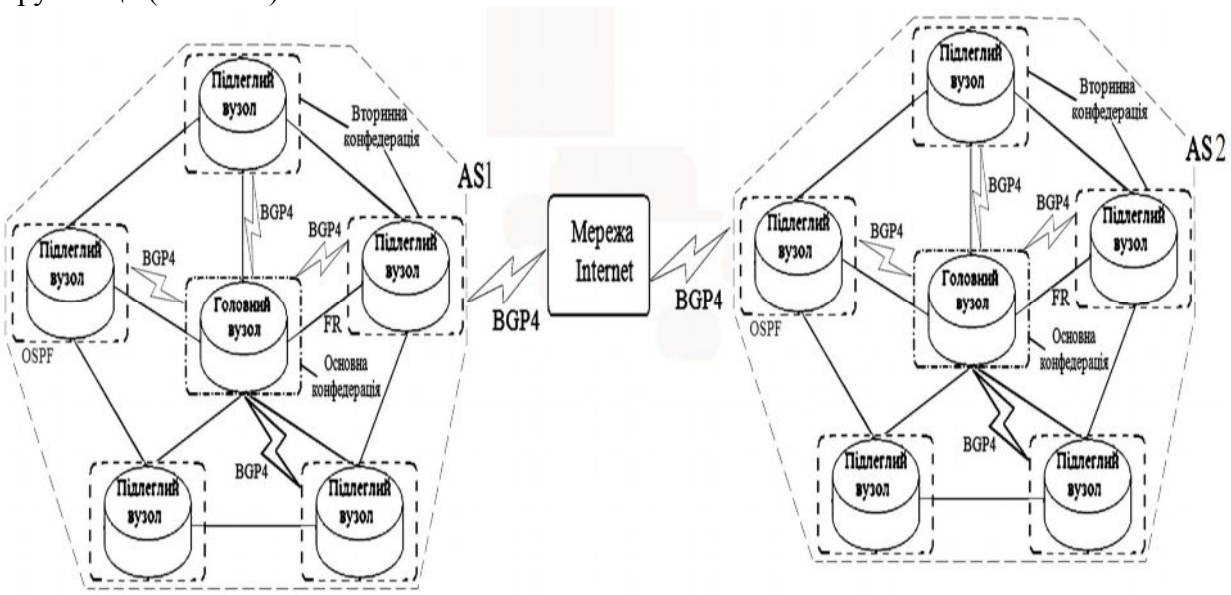


Рис. 1. Структура системи маршрутизації корпоративної мережі

В доповіді наведено варіанти технічної реалізації системи маршрутизації в мережі органів державного управління побудованої на обладнанні корпорації CISCO.

Використовуючи програмний продукт Packet Tracer v.5.1 [1], розроблений корпорацією CISCO, для емуляції мереж, сформовано захищену систему маршрутизації для корпоративної мережі.

Приклад технічної реалізації АС в середовищі імітаційного моделювання Packet Tracer v.5.1 наведено на рис 1.

Показано налаштування віртуального VLAN мереж в корпоративній мережі і маршрутизації між ними, а також проведення запуску протоколу покриваючого дерева STP [2].

Наведено конкретні файли конфігурації мережевих пристроїв (комутаторів і маршрутизаторів структури, приведеної на рис 2).

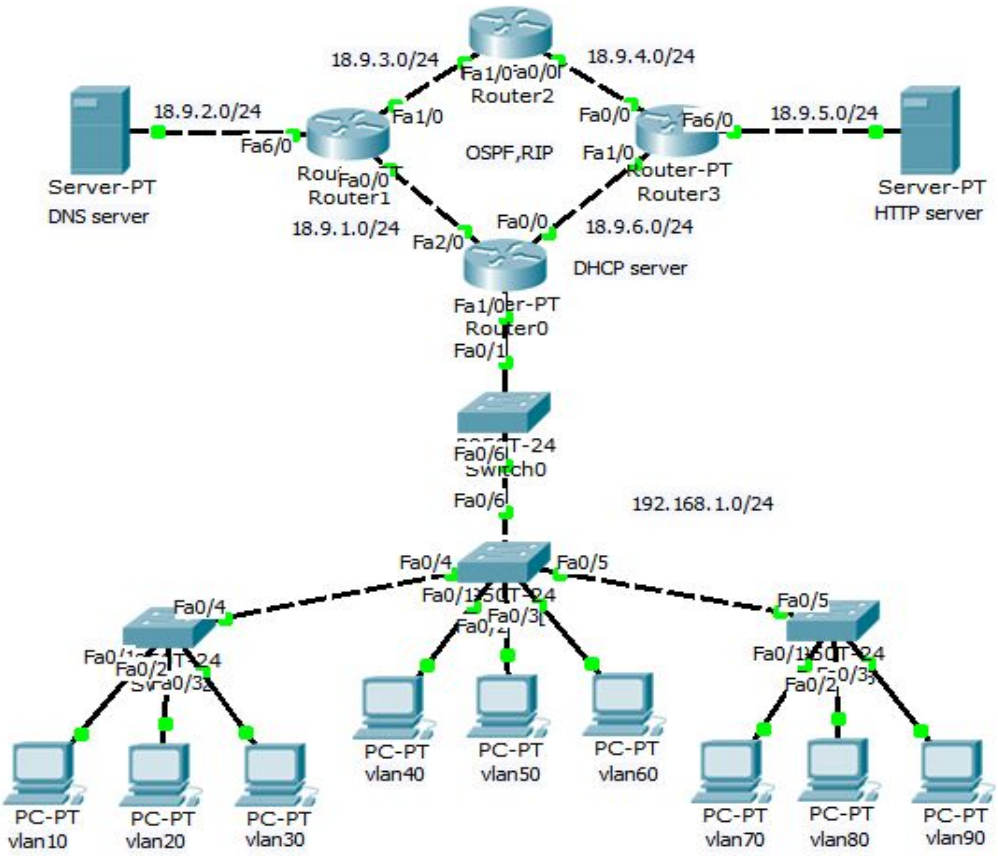


Рис. 2. Приклад технічної реалізації АС

Файли конфігурації мереживих пристроїв (комутатрів і маршрутизаторів структури) забезпечують скорочення часу на планування мережі і побудови системи маршрутизації органів державного управління.

Висновки :

1. Варіанти структур мереж і рекомендовані для них системи маршрутизації успішно можна використати при побудові системи маршрутизації в корпоративних мережах силових структур держави .

2. На базі аналізу структури системи маршрутизації показано що вона забезпечує скорочення часу доставки повідомлень не менше ніж на десять відсотків..

3. Розглянута структура та приклад технічної реалізації АС може використовуватися в мережах органів державного управління

ЛІТЕРАТУРА

1. Программа сетевой академии CISCO CCNA 3 і 4. Вспомагательное руководство. М : Вільямс. 2007. – 994с

2. Науменко М.І., Стасев Ю.В., Рубан І.В. „Технології комп'ютерних мереж в АСУ військами". Харків: МОУ, 2004. - 458 с.

3. Дж. Бони. Руководство по Cisco IOS.-СПб.: Питер, М.: Издательство „Русская Редакция".2008. – 782с.: ил.

Науменко Ю.Б. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ПРОЕКТУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ОБ’ЄКТНО-ОРІЄНТОВАНОГО ПІДХОДУ

Існуючі нормативні документи за оцінкою захищеності визначають гарантії безпеки, в яких проектування, розробка систем захисту інформації (СЗІ), розглядаються як основні вимоги безпеки. При високих вимогах безпеки, що пред’являються до систем захисту інформації (для систем державного призначення, банківських систем), в нормативних документах вимагається від розробників обов’язкова формалізація всіх етапів створення систем захисту інформації.

Завдання проектування системи захисту принципово відрізняється від завдань проектування інформаційних систем. Річ у тому, що проектування здійснюється з урахуванням статистичних даних про вже існуючі загрози. Однак в процесі функціонування системи захисту поле загроз може принципово змінитися. Зокрема, це пов’язано з тим, що багато загроз припускають знаходження зловмисниками помилок в реалізації системних засобів, які можуть бути невідомі на момент створення системи захисту, але мають бути враховані в процесі її функціонування.

Рівень захисту всієї системи визначається рівнем захисту ділянки технологічного ланцюга обробки інформації, який має найслабший захист. Тому, немає особливого сенсу докладати зусилля до підвищення рівня захисту інформації на одній ділянці інформаційної системи, якщо на іншому захист залишиться на нижчому рівні. Однак, як порівняти, рівні безпеки технологічних ділянок і визначити рівень безпеки системи в цілому, якщо оцінка захищеності проводиться за методиками, орієнтованими на різні типи інформаційних технологій, засоби і методи реалізації захисту і критерії оцінки?

Основним недоліком існуючих підходів до оцінки захищеності інформації є орієнтованість на певний тип інформаційних технологій або один з рівнів інформаційної взаємодії, на якій реалізуються функції захисту. При такому підході можна отримати адекватну оцінку захищеності інформації тільки для обмеженої галузі системи управління. Виникають складнощі проведення порівняльного оцінювання безпеки ділянок інформаційної системи, що використовують різні типи інформаційних технологій або різні рівні інформаційної взаємодії при реалізації функцій захисту, а також отримання комплексної оцінки захищеності інформації.

При проектуванні СЗІ доцільно використовувати об’єктно-орієнований підхід. Найважливішими характеристиками такого підходу є еволюційність, і перенесення акценту з процесу розробки на етапи аналізу і моделювання.

Важливою якістю об’єктного підходу є узгодженість моделей діяльності організації і моделей проектованої системи захисту від стадії формування вимог до стадії реалізації. Вимога узгодженості моделей виконується завдяки можливості застосування абстрагування, модульності, поліморфізму на всіх стадіях розробки. Моделі ранніх стадій можуть бути безпосередньо піддані порівнянню з моделями реалізації. За об’єктними моделями можна прослідкувати відображення реальної суті модельованої предметної галузі (організації) в об’єкти і класи інформаційної системи.

Побудувати систему з застосуванням об’єктно-орієнтованого підходу – означає, що необхідно проаналізувати проблему та знайти об’єкти, які охоплюються системою. Загальні характеристики, риси та поведінка цих об’єктів в подальшому моделюються та реалізуються як класи (або отримані із попередніх проектів, або бібліотеки класів третіх осіб), потім збираються разом, задля моделювання системи в середені комп’ютерного каркасу. Цей підхід, що ґрунтується на минулих зусиллях, дозволить створювати системи, сформовані з готових частин.

д.т.н. Науменко М.І.(ДВОН)
к.т.н. Шелепенко Ю.В.(ВІТІ НТУУ „КПІ”)
Кривенко С.С.(ВІТІ НТУУ „КПІ”)

АНАЛІЗ МОЖЛИВОСТЕЙ ВПРОВАДЖЕННЯ СИГНАЛЬНО КОДОВИХ КОНСТРУКЦІЙ

Існуючи методи підвищення ефективності системи передачі інформації полягають у застосуванні завадостійкого кодування безпосередньо в напівнеперервному каналі.

Наявність межсивольної інтерференції і фазових дрижань у реальних каналах зв’язку істотно знижує ефективність використання таких СКК і завадостійкість системи передачі в цілому навіть при досить якісному придушенні цих завад на прийом.

Спроби застосувати коди, оптимальні над кінцевим полем, в сполученні із ансамблями сигналів великих об’ємів із-за відсутності монотонного зв’язку між хеммінговою та евклідовою відстанями бажаного результату не дають. Тому теорія сигнально-кодових конструкцій (СКК), в основу котрої покладені методи завадостійкого кодування безпосередньо в напівнеперервному каналі, є об’єктом інтенсивних досліджень останнього десятиліття.

Теорія високошвидкісної передачі інформації по широкому класу реальних каналів зв’язку із межсимвольною інтерференцією, фазовими дрижаннями, негауссівськими адитивними завадами, змінними параметрами представлена в роботі [1].

Основний зміст доповіді присвячений розв’язанню науково-технічної проблеми підвищення швидкості передачі інформації до її теоретичних меж в широкому класі реальних каналів зв’язку із межсивольною інтерференцією (МСІ), фазовими дрижаннями (ФД), негауссівськими адитивними завадами на основі високоефективних СКК та адекватних їх методів оптимального декодування та адаптивного прийому.

Сформульована та розв’язана задача синтезу каскадних сферичних згорточних СКК для високошвидкісної передачі інформації в каналах із пам’яттю та фазовою не стаціонарністю. Показані складові частини й умови високоефективного формування згорточних СКК [2].

Структура узагальненого каскадного кодера показана на рис 1.

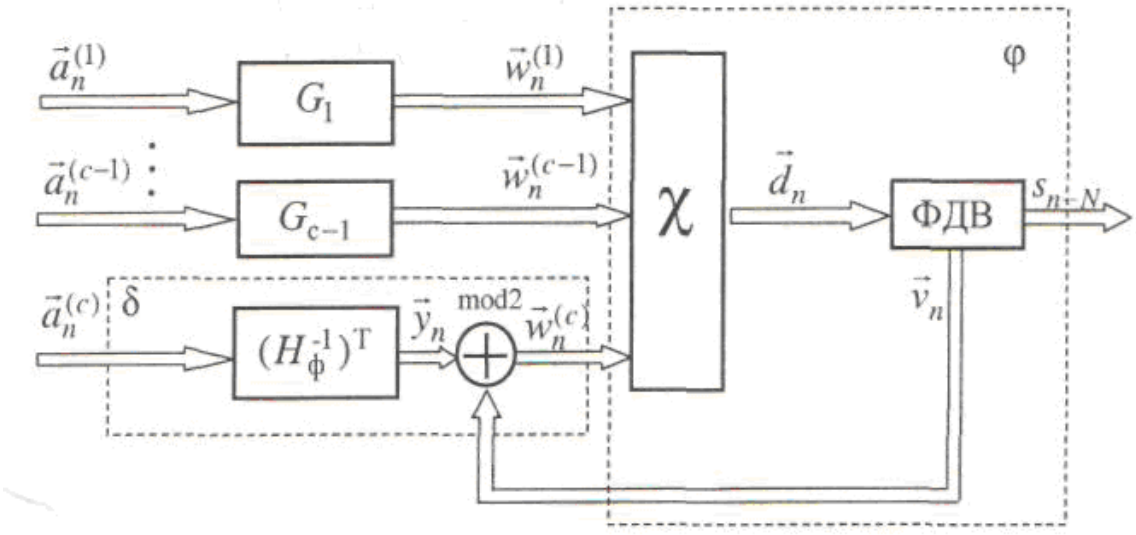


Рис. 1. Структурна схема узагальненого каскадного кодера

На рисунку $G_1,\ldots,G_{c-1}$ та кодер з оператором δ зовнішні згорточні кодери на входи якіх надходить напівнескінченні інформаційні послідовності

$$a_n^{(i)} = \left[a_1^{(i)}(n), a_2^{(i)}(n), \ldots, a_{k_i}^{(i)}(n)\right],$$

Формуючий декодер Вітербі (ФДВ), згідно [5], генерує з затримкою $N_з=N/2$ відповідну сигнально-кодову послідовність

$$\{S_{n-N}\} = \{(d_{n-N} - b_{n-N})\} \cdot \{h_{n-N}\},$$

де N розмірність сферичної СКК і * – символ математичної згортки.

Оператор внутрішнього кодування формує сферичні властивості СКК і забезпечує компенсацію МСІ. При цьому підвищення енергетичної ефективності гауссівського каналу із ФД складає 2,0…2,5 дБ. Оператор зовнішнього завадостійкого кодування збільшує дистанційні властивості СКК і створює енергетичний виграш (ЕВК) до 3…4 дБ. В цілому синтезовані СКК в разі їх оптимального декодування і фільтрації дозволяють в реальних негауссівських каналах із МСІ і ФД підвищити швидкість передачі інформації до 4.25 біт/вим (6 біт/с Гц) і досягти енергетичного виграшу до 6.5 дБ, що близько до пропускної спроможності ідеального гауссівського каналу.

Розглянути оптимальні методи і алгоритмі сумісного декодування та фазової синхронізації СКК в умовах неповної параметричної визначеності ФД, випадкових зрушень, негауссівських адитивних завад.

В роботі запропоновані технічні реалізації алгоритмів фазової синхронізації та корекції сигналів на базі каскадного кодера в послідовних цифрових модемах 5-го покоління [3,4].

Висновки:

1. Сигнально-кодові конструкції на основі інтегрованого застосування складних систем сигналів та перешкодостійких кодів є перспективним напрямком для досягнення необхідних показників завадостійкості, імітостійкості й скритності цифрових систем зв'язку.

2. Складність процедур кодування і декодування згорточних кодів нижча, ніж блочних кодів з аналогічними коригувальними властивостями. При фіксованій складності реалізації кодерів і декодерів згорточні коди можуть забезпечити меншу ймовірність помилкового декодування.

3. Переваги згорточних кодів визначаються, головним чином, простотою встановлення синхронізації, порівняльною легкістю й ефективністю виконання алгоритму „м'якого" декодування, а також можливістю більш повного узгодження коригуючих властивостей згорточних кодів із характеристиками реальних каналів зв'язку.

ЛІТЕРАТУРА

1. *Науменко М.І.* Високошвидкісна завадостійка передача інформації в каналах телекомунікаційних систем: Монографія. – К.: „Альтерпрес", 2003. – 220с.

2. *М.І. Науменко, Ю.В. Стасев, О.О. Кузнецов, С.П. Євсеев.* Теорія сигнально-кодових конструкцій: Монографія. – Х. : ХУПС, 2008. – 541с.

3. *Науменко М.І.* Рекомендации по реализации алгоритмов фазовой синхронизации и коррекции сигналов в последовательных цифровых модемах. – Л.: ВАС, 1986. – Кн. 3 – С. 3 – 5.

4. *Науменко М.І., Шелепенко Ю.В., Ткаченко В.В.* Использование микропроцессорных наборов для построения модемов: Тез. докл. – К.,1983. – 139 с.

5. *Наталенко П.П., Науменко Н.И., Ерко А.А.* Модифицированный алгоритм Витерби, оптимальный на классе негауссовых помех // XII межрегион. научн.-техн. семинар „Статистический синтез и анализ информационных систем": Тез. докл. – М.: ВЕТО РЭС им. А.С. Попова, 1992. – С. 89.

к.т.н. Недайбіда Ю.П. (ВІТІ НТУУ „КПІ”)
Ляшенко В.Г. (ВІТІ НТУУ „КПІ”)
Шугалій О.О. (ВІТІ НТУУ „КПІ”)

ПИТАННЯ СИСТЕМОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ АСУ НА СУЧАСНОМУ ЕТАПІ РОЗВИТКУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Будівництво і розвиток Збройних Сил України регламентується Державною програмою будівництва і розвитку Збройних Сил України, іншими нормативними документами, в тому числі Головною Програмою створення системи управління Збройних Сил України. Положення Програми визначають ідеологію управління, напрями розвитку систем, підсистем системи управління Збройних Сил України.

Одним з найважливіших завдань щодо вирішення проблеми організації і розвитку системи управління Збройними Силами, військами (силами) та бойовими засобами на цей час є розроблення і реалізація Програми створення Автоматизованої системи управління Збройних Сил України.

Автоматизована система управління Збройних Сил України (АСУ ЗС України) – інтегрована автоматизована система управління, об’єднує в своєму складі на єдиних оперативно-стратегічних і системотехнічних принципах автоматизовані системи (підсистеми) управління різних рівнів та функціонального призначення. Її функціонування організовується на основі єдиного інформаційного поля та інформаційно-розрахункового процесу із застосуванням єдиних форм та методів управління.

В Основних положеннях Програми викладені:

оперативно-стратегічні, оперативно-тактичні питання створення (призначення конкретної системи, підсистеми та елементів АСУ ЗС України, завдання, які вирішуються ними, галузь та ланки застосування, структура системи (органи, пункти управління, їх засоби автоматизації та зв’язку) управління її підсистем та елементів);

оперативні вимоги щодо бойової готовності, безперервності, стійкості, оперативності та скритності управління тощо;

системотехнічні питання побудови систем, підсистем АСУ ЗС України, в основу яких покладені такі положення, як відкритість, еволюційність, адаптованість, а також виконання вимог до організації єдиного технічного, інформаційного, лінгвістичного, математичного та програмного забезпечення, основні напрями уніфікації та стандартизації.

Системотехнічне забезпечення побудови АСУ ЗС України включає комплекс загальних заходів, спрямованих на розробку ідеології і технічної політики побудови АСУ ЗС України, її основних складових систем, підсистем та елементів, формування організаційно-методичного забезпечення їх створення, а також загальних питань з розроблення і взаємної ув’язки технічного, інформаційного, лінгвістичного, математичного, програмного, ергономічного, метрологічного, топогеодезичного забезпечення, життєзабезпечення та інших видів забезпечення систем зв’язку і автоматизації та пунктів управління.

Відзначимо, що положення Програми розроблялись в кінці минулого століття з урахуванням стану той час і прогнозу розвитку засобів нападу, зброї, джерел інформації, технологій упритул до 2000 року.

Поява на цей час новітніх засобів нападу, особливо високоточної зброї, потребує корінних змін в змісті та способах ведення бою, безперервної взаємодії різнорідних сил при його веденні. В результаті збільшення швидкостей та маневрених можливостей сучасних об’єктів нападу зросли просторові параметри бою, розширено області можливих атак противника. Зазначене приводить до наступних особливостей функціонування системи ЗС України, які суттєво ускладнюють створення системотехнічного забезпечення АСУ:

великі розміри і складність топологічної структури системи, яка може змінюватися в реальному часі;

можливість протікання в системі різнорідних потоків даних великої інтенсивності;

складність варіантів напрямків протікання і взаємодії потоків інформації і можливість зміни кількості каналів в реальному часі;

можливості зміни критеріїв і показників функціонування системи в цілому і її складових в реальному часі і т. ін.

При цьому, істотно зросли вимоги до якості управління в умовах жорсткого ліміту часу на прийняття рішення.

Враховуючи високу швидкоплинність, швидку зміну бойової обстановки, складність своєчасного отримання та обробки інформації про противника і стан своїх засобів, основні системотехнічні проблеми створення системи управління Збройних Сил України виникають при вирішенні таких задач:

виявлення об'єктів противника;

трасової обробки даних про цілі противника;

трасової обробки та вирішення задачі знищення ударного елементу в системах боротьби з високоточною зброєю;

виявлення маневруючих і неманевруючих цілей та оцінка їх характеристик;

визначення пріоритету цілей та вирішення задачі цілерозподілу;

визначення управління бойовими діями в реальному часі всіх частин, а в деяких випадках і безпосередньо підрозділами, що входять до складу системи;

забезпечення безпеки польотів винищувальної авіації тощо.

Відзначимо, що наявний стан розвитку інформаційних технологій дають можливість розробки нових і удосконалення існуючих методів, алгоритмів та відповідних засобів, здатних задовольнити вимоги до якості обробки інформації в сучасних умовах функціонування системи управління Збройних Сил України.

Тому системотехнічні проблеми створення АСУ залежать від можливостей якісного вирішенні задач вдосконалення та розробки методів та алгоритмів сумісної обробки різнотипної інформації від різнотипних інформаційних джерел, цілерозподілу в умовах масового нальоту, супроводу трас цілей і прийняття рішень на різних ланках управління в умовах дефіциту часу і недостатньої визначенні вихідних даних і т. ін.

Крім того, застосування сучасних досягнень в області інформаційних технологій дозволяє поліпшити вирішувати задач доповнення і перерозподілу функцій і задач управління між різними рівнями системи в реальному часі.

Впровадження АСУ дозволить вирішити наступні проблеми:

покращення якісних характеристик управління - готовності, безперервності, стійкості, оперативності, таємності, єдності та комплексності управління, зниження трудомісткості та підвищення якості вирішення завдань управління

скорочення часу, що витрачається на збирання, оброблення, передавання оперативної інформації та відображення її на автоматизованих робочих місцях оперативного складу;

скорочення часу, що витрачається на прийняття рішень і термінів доведення до підпорядкованих військ (сил) завдань, команд і сигналів і т. ін.

Висновки.

1. Нормативна база розвитку і впровадження АСУ потребує детального аналізу і перегляду з точки зору урахуванням можливостей наявних інформаційних технологій, сучасних засобів нападу і освітлення навколишнього середовища.

2. З урахуванням досягнень сучасних технологій, які спроможні створювати засоби і системи з характеристиками вищими по точності, скорості переробці інформації в процесах прийняття рішень, виконанні впливів управління ніж людина, системи різних рівнів управління Збройних Сил України повинні бути ергатичними з чіткім розподілом і виконанням функцій в інтересах цілей функціонування системи на кожному рівні.

к.т.н. Нестеренко М. М. (ВІТІ НТУУ „КПІ”)
Маньківській В. Б. (НТУУ „КПІ”)
Пасько С. П. (НТУУ „КПІ”)

ОЦІНКА ЧАСУ ЗАТРИМКИ ПОВІДОМЛЕНЬ В МЕРЕЖАХ *IP* ТА *MPLS*

Технологія *MPLS* (*Multiprotocol Label Switching*) − є багатопротокольною технологією з комутацією по мітках. Її поява пов’язана з пошуком способів побудови високошвидкісних *IP*-магістралей. Підвищення швидкості обробки пакетів, в порівнянні з технологією *IP*, досягається за рахунок заміни процесу маршрутизації *IP* пакетів на процес комутації, при проходженні даних через магістральну мережу провайдера.

Передача даних в технології *MPLS* забезпечує ізольованість мереж споживачів шляхом застосування тунелів для передачі клієнтського трафіку по внутрішній мережі провайдера. В результаті, маршрутизатори різних клієнтів не мають маршрутної інформації один про одного і тому не можуть обмінюватися пакетами, тобто досягається бажана ізоляція. При цьому для формування тунелів потрібні додаткові часові та обчислювальні ресурси.

Якщо не враховувати часові витрати на формування тунеля, то технологія *MPLS* завжди матиме перевагу над *IP* технологією. Однак, в реальних умовах експлуатації, постійно йде процес формування тунелів для передачі різних видів повідомлень і їх руйнування, якщо на протязі певного часу немає надходження пакетів, які пов’язані із відповідним тунелем. У даній роботі ставиться завдання аналізу „найгіршого” для *MPLS* випадку, при якому перед початком обміну інформацією між кінцевими пунктами є процес створення тунеля. А по закінченню обміну − тунель руйнується. При такій постановці задачі технологія *MPLS* матиме перевагу перед технологією *IP,* якщо час створення тунеля плюс час передачі повідомлення буде менше часу передачі повідомлення в дейтаграмному режимі.

Для порівняльної оцінки ефективності даних технологій пропонується використовувати сумарний час обробки пакетів на всіх вузлах мережі, від відправника до одержувача. Отримання чисельних значень часу обробки повідомлень вимагає побудови математичної моделі, яка б відображала, як особливості алгоритму функціонування мережі за тією або іншою технологією функціонування, так і часові витрати при вирішенні різних видів мережевих задач. У моделі процес передачі інформації з використанням технології *MPLS* формалізований наступним чином − обслуговування будь-якої заявки починається з формування тунеля. Якщо тунель вже існує, то проводиться корекція його параметрів для забезпечення заданої якості обслуговування. Частина заявок отримує відмову в обслуговуванні, якщо користувач не має достатніх має прав або відсутні ресурси в необхідному об’ємі. При чому, формування тунеля проводиться в три етапи: на основі стандартних протоколів маршрутизації, будується матриця маршрутів; у необхідному напрямку зв’язку створюється звичайний *LSP*-туннель без врахування обмежень на показники якості обслуговування; на основі *LSP*-туннеля, створюється *RSVP-TE*-туннель, який закріплює необхідний мережевий ресурс з метою забезпечення заданих вимог щодо якісті обслуговування.

В процесі моделювання процесу функціонування системи використовується ряд допущень:

− продуктивність вузлів і гілок на всіх ділянках мережі вважається незмінною в часі;

− довжина пакету не залежить від вигляду і типу інформації, яка передається та має постійне значення;

− не залежно від типу технології пакети повідомлень рухаються по одному і тому ж маршруту.

Таким чином, запропонована модель дозволить отримати області значень параметрів мережі, при яких дейтаграммний режим передачі інформації матиме перевагу перед технологією *MPLS* і навпаки.

к.т.н. Нестеренко М. М. (ВІТІ НТУУ „КПІ”)
Семеріч П.Ю. (ФІОТ НТУУ „КПІ”)

ОСНОВНІ ПІДХОДИ ЩОДО ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ КОНВЕРГЕНТНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Однією з основних стратегій розвитку сучасних телекомунікаційних мереж полягає в тому, щоб забезпечити, як умога більше сервісів абонентам використовуючи ресурси існуючих мереж. Тобто, об’єднання мереж різної природи, що мають різне комунікаційне обладнання та принципи побудови в єдину „віртуальну” транспортну базу для передачі інформаційних потоків. Конвергенція телекомунікаційних мереж обумовлена наступними факторами: економічним аспектом (створення та розгортання нових мереж вимагає значних матеріальних затрат); відсутністю універсальної мережевої технології, яка б виступала як транспортна основа для передачі всіх видів повідомлень; апробовані мережеві рішення є більш раціональними для побудови типових мереж, що функціонують в цілях організацій різного рівня.

Розподілений характер сучасних телекомунікаційних мереж робить неможливою підтримку її функціонування без інтегрованої системи управління. Це означає, що функції управління різнорідними пристроями повинні служити загальній меті обслуговування абонентів мережі із заданою якістю (*QoS*).

На даний час, існують рекомендації *ITU-T X.700* та близький до них стандарт *ISO 7498-4*, які ділять задачі системи управління на п’ять функціональних груп:

- управління конфігурацією мережі та ідентифікації її елементів;
- обробка помилок;
- аналіз продуктивності і надійності;
- управління безпекою;
- облік роботи мережі.

В свою чергу в склад базової архітектури управління мережами входять наступні основні елементи:

1. Система управління мережею.
2. Об’єкти управління.
3. Інформаційна база управління.
4. Протокол управління мережею.

Однак, виділення в системах управління типових груп функцій і розбиття цих функцій на рівні ще не дає відповіді з яких елементів вони складаються та яка архітектура зв’язків цих елементів. На практиці в системах управління використовується елементарна схема взаємодії агента із менеджером (рис. 1).

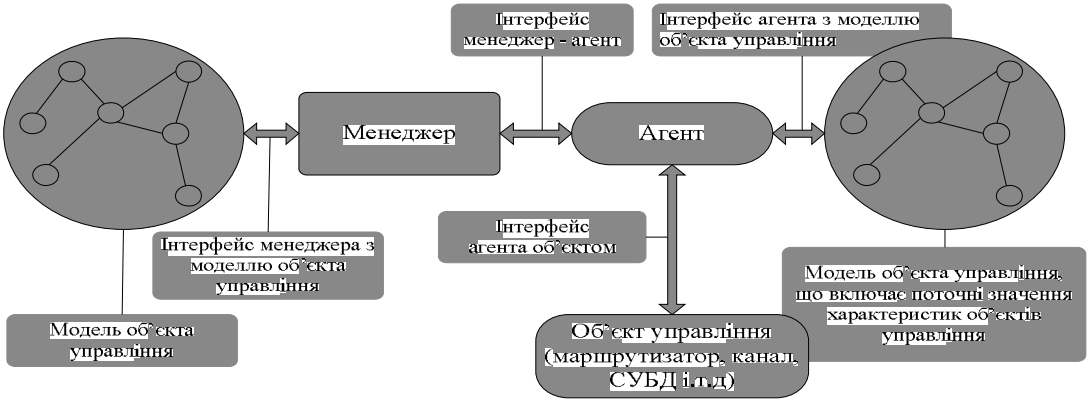


Рис. 1 Порядок взаємодії агента, менеджера та об’єктів управління

На основі цієї схеми можуть бути побудовані системи управління практично будь-якої складності із великою кількістю агентів і менеджерів різного типу.

При чому передача повідомлень управління може бути реалізована по тому ж каналу, по якому передаються дані користувача *inband* та управління *out-of-band*, тобто створення окремої мережі для системи управління. Проте спосіб *out-of-band* має переваги з точки зору надійності в випадку аварій і перевантажень в телекомунікаційній мережі та відповідає концепції *TMN*.

Також необхідно відмітити, що від вибір типу архітектури системи управління має величезний вплив на її продуктивність. Існує декілька типових архітектур побудови систем управління мережею:

- однорівнева архітектура;
- ієрархічна архітектура;
- комірчаста архітектура;
- платформна архітектура.

Однорангова побудова системи управління сьогодні вважається неефективною і застарілою тому, що не забезпечує необхідного рівня масштабованості по продуктивності та необхідного рівня надійності.

Набагато гнучкішою є ієрархічна побудова зв'язків між менеджерами, що дозволяє скоротити об'єми службової інформації, яка циркулює між рівнями системи управління, і як наслідок, приводить до набагато ефективнішої системи управління.

Комірчаста архітектура − це складна архітектура управління мережею, яка включає як ієрархічний підхід так і однорангову структуру на певних рівнях системи управління.

Платформна архітектура ґрунтується на єдиному прикладному програмному інтерфейсі, що універсальний та підтримується різними виробниками. В даному випадку розробники концентруються на специфіці додатків, оскільки сама платформа забезпечує необхідні базові засоби управління.

Тому при розробці та побудові систем управління для конвергентних мереж найбільш раціонально використовувати:

−схему управління „агент – менеджер". Дана схема дозволяє використовувати абстрактну модель управляючого ресурсу, а саме базу інформації управління. Це дозволяє стандартизувати дані, що використовуються в процесі управління. При чому, агент взаємодіє з об'єктом управління по нестандартному інтерфейсу, а із менеджером − по стандартному протоколу через мережу;

−багаторівневу ієрархічну або комірчасту структуру побудови системи управління, в залежності від складності мережі. Що, в свою чергу, дозволяє об'єднати розрізнені системи управління елементами мережі в єдину інтегровану систему;

−платформний підхід, так як платформа системи управління виконує для менеджерів роль операційної системи і забезпечує розробника менеджерів набором корисних системних викликів загальних для будь-якої системи управління;

−окрему мережу або виділені канали для передачі інформації, яка циркулює в системі управління, що дозволить підвищити її надійність.

В свою чергу сучасні системи управління телекомунікаційними мережами бути зорієнтованими на виконання всіх п'ять груп функцій, які визначаються стандартами *ISO/ITU-T* для систем управління об'єктами будь-якого типу.

Нечушкін М.П. (ВІТІ НТУУ „КПІ”)
Харченко Н.М. (ВІТІ НТУУ „КПІ”)

ВИЗНАЧЕННЯ ВАРІАНТА ПОБУДОВИ МОБІЛЬНОГО КОМПОНЕНТУ ПЕРСПЕКТИВНОЇ СИСТЕМИ ЗВ’ЯЗКУ ТА АВТОМАТИЗАЦІЇ ТАКТИЧНОЇ ЛАНКИ УПРАВЛІННЯ

Аналіз можливих варіантів структур мобільного компоненту систем зв’язку та інформатизації збройних сил провідних країн світу показав, що найбільш раціональним є його побудова на двох основоположних принципах. Перший – використання ліній прямого зв’язку між вузлами зв’язку пунктів управління і другий – використання мережі мобільних опорних (допоміжних) вузлів зв’язку з комплексним застосуванням радіорелейних, тропосферних та супутникових засобів зв’язку [1].

Базуючись на розробках цілої низки сучасних зразків техніки зв’язку, ТОВ „Телекарт-Прилад” (радіостанції, радіорелейні станції, засоби комутації та маршрутизації, кінцеве обладнання та ін.), апаратури засекреченого зв’язку, тропосферних цифрових станцій, сучасних зразків електронно-обчислювальної техніки та кінцевих термінальних пристроїв (телефонного, факсимільного зв’язку) можливе створення перспективного польового комплексу засобів зв’язку та автоматизації тактичної ланки управління.

Мобільний компонент системи зв’язку і автоматизації – частина системи зв’язку, розгорнута на основі мобільних елементів. Мобільний елемент системи зв’язку та автоматизації це елемент системи зв’язку та автоматизації, спроможний переміщуватися і забезпечувати зв’язок у нових районах у встановлені терміни або під час руху.

Варіантом мобільного компоненту системи зв’язку та автоматизації тактичної ланки управління ЗС України на найближчу перспективу може бути варіант, в складі якого присутні наступні елементи: інформаційно – телекомукаційні вузли (далі – ІТВ) пунктів управління; опорна, базова мережа зв’язку; лінії прямого зв’язку; лінії прив’язки; мережа управління системою зв’язку та автоматизації; мережа технічного забезпечення управління системи зв’язку і автоматизації; резерв сил і засобів зв’язку і автоматизації.

Інформаційно – телекомукаційні вузли пунктів управління є організаційно-технічними об’єднаннями сил, засобів зв’язку та автоматизації і призначені для забезпечення обміну і обробки інформації вирішення інформаційних, розрахункових та інших задач, обмін повідомленнями електронною поштою, надання доступу до серверів різного призначення для виконання завдань управління частинами (підрозділами) у ході бою.

В склад кожного ІТВ пунктів управління з’єднання можуть входити: 1-2 комплексних апаратних зв’язку, які можуть забезпечити створення цифрових мереж з інтеграцією послуг, що забезпечують передачу різних видів повідомлень (голосу, даних, відео та ін.); 1-2 радіостанції середньої потужності КХ (УКХ) діапазону; група командно-штабних машин (7-9 од.) з засобами зв’язку і автоматизації, обладнаними автоматизованими робочими місцями для службових осіб оперативного складу і призначена для забезпечення обміну всіма видами повідомлень на місці і в русі.

Опорна мережа зв’язку – елемент системи зв’язку, що включає опорні вузли зв’язку та з’єднувальні лінії зв’язку і є основою для забезпечення зв’язку в одній або декількох системах управління. Вона розгортається радіорелейними і кабельними лініями зв’язку і повинна мати можливість комутації каналів(трактів) на опорних вузлах зв’язку. Використовується для зв’язку зі старшим штабом.

Лінії прямого зв’язку розгортаються безпосередньо між ІТВ пунктів управління і абонентами. Роботу ліній прямого зв’язку забезпечують 1-2 радіостанції середньої потужності КХ (УКХ) діапазону.

Лінії прив’язки, це лінії зв’язку, що з’єднують ІТВ пунктів управління з опорним або допоміжним ІТВ.

Запропонований варіант мобільного компоненту системи зв'язку та автоматизації тактичної ланки управління ЗС України забезпечує:

створення каналів засобами прямого зв'язку, їх настройку, вимірювання, розподіл;

своєчасне встановлення додаткових зв'язків (каналів зв'язку) в умовах особливого періоду;

відновлення порушеного зв'язку, підтримання його у постійній готовності до передавання (приймання) сигналів бойового управління та інших видів повідомлень (документованих, телефонних, відеотелефонних);

захист інформації під час її обміну та обробки, вирішення інформаційних, розрахункових та інших задач;

приймання, передавання, обробку всіх видів вхідних, вихідних та транзитних повідомлень і доставку сигналів та документованих повідомлень адресатам, а також документовані, телефонні, відеотелефонні переговори службовим особам органів військового управління;

контроль за своєчасністю проходження сигналів бойового управління особливо важливої інформації, а також якість переговорів категорованим абонентам;

організацію і контроль оперативно-технічної, станційно-експлуатаційної, частотно-диспетчерської служб та служби єдиного часу.

В залежності від бойового складу з'єднання, частини, кількості бойових підрозділів, завдання, які вони вирішують, побудови бойового порядку та інших факторів, склад мобільного компоненту системи зв'язку та автоматизації може змінюватися. Так наприклад, збільшення підрозділів з'єднання спричинить до збільшення інформаційних напрямків, а зміни ширини смуги і глибини оборони приведе до зміни протяжності польових кабельних ліній, зміни дальності для радіо і радіорелейного зв'язку. Ці фактори враховуються при плануванні зв'язку [2].

Перспективна система зв'язку та автоматизації повинна швидко адаптуватися до частих змін топології й ефективно використовувати обмежені ресурси. У таких умовах забезпечити інформаційний обмін із заданою якістю неможливо без ефективної системи управління системою зв'язку та автоматизації. Функції системи управління системою зв'язку та автоматизації розподіляються по комплексних апаратних зв'язку.

Необхідно створювати розробки комплексу захисту інформації як на систему, так і на кожний її елемент та питання забезпечення взаємосумісності з існуючими системами та обладнанням, що використовується в стаціонарному компоненті системи зв'язку збройних сил та на телекомунікаційних мережах України.

Переозброєння частин (підрозділів) не потребує перегляду організаційно-штатних структур підрозділів зв'язку, суттєво підвищує вимоги до професійного рівня фахівців зв'язку та потребує їх перепідготовки і зміни програми бойової підготовки.

Цифровізація мобільного компоненту системи зв'язку та автоматизації тактичної ланки управління не виключає використання аналогових засобів, які можуть спільно працювати з цифровими. Виходячи з вищенаведеного, на підставі аналізу перспектив подальшого розвитку мобільного компоненту системи зв'язку та автоматизації тактичної ланки управління можна констатувати, що вона повинна реалізовуватись на використанні сучасних цифрових комутаційних систем військового призначення, управління якими має здійснюватися автоматично у реальному масштабі часу.

ЛІТЕРАТУРА

1. *Малярчук М.В.* Архітектура мобільного компоненту перспективної системи зв'язку і автоматизації тактичної ланки управління Збройних Сил України з використанням опорної мережі на радіорелейних станціях. //Збірник наукових праць ВІТІ НТУУ „КПІ", 2009. – С. 45 – 50.

2. *Стеценко О.О., Савков П.А., Ляхов М.О.* Основи військового управління. Частина 1. Основи управління військами: Навчальний посібник – К.: Ліра – К., 2009 – 160 с.

к.т.н. Овсянніков В.В. (ВІТІ НТУУ ,,КПІ”)
Місюра С.М. (ВІТІ НТУУ ,,КПІ”)

ПЕРСПЕКТИВИ РОЗВИТКУ СИСТЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

Розвиток комп’ютерних технологій призвів до масової практики автоматизованої обробки інформації в комп’ютерних мережах, в тому числі інформації персонального характеру. Виникла потреба додатково захисту інформаційних прав людини.

В Україні продовжується нормотворча робота у сфері правового регулювання конфіденційної інформації про особу. 1 червня 2010 року Верховна Рада України прийняла та 24 червня 2010 року Президент України підписав Закон України ,,Про захист персональних даних” від 01.06.2010 № 2297-VI (далі – Закон). Поява даного Закону обумовлено євроінтеграційними процесами України, зокрема, необхідністю виконання Україною вимог Євросоюзу, які містить спільна Угода за назвою ,,Матриця співробітництва”. Однією з умов даного документа є зобов’язання України ратифікувати й імплементувати Конвенцію Ради Європи від 28.01.1981 ETS № 108 ,,Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” (м. Страсбург) (далі – Конвенція). Таким чином, слідом за провідними демократичними країнами, Україна врегулювала правовідносини в сфері правового захисту персональної інформації про особу, і це, безсумнівно, позитивний факт. Зроблено черговий крок, спрямований на забезпечення гарантій прав та свобод людини, що є одним з основних ознак правової держави.

Необхідність прийняття цього Закону уже давно гостро стояла в усіх учасників інформаційного обміну персональними даними, що перш за все обумовлено тим, що стан нормативно-правової бази неефективно забезпечує захист прав людини щодо виконання положень статей 3, 32, 34 Конституції України стосовно персональних даних.

Актуальність дослідження полягає в тому, що даний Закон вступає в силу з 1 січня наступного року. Тобто власники чи розпорядники бази персональних даних, якими відповідно до Закону можуть бути підприємства, установи й організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи – підприємці, повинні до закінчення поточного року привести свою діяльність у відповідність до вимог положень Закону.

Для більш чіткого розуміння ситуації необхідно привести ряд інформаційних фактів:

1. Сучасні суспільні відносини характеризуються широким використанням персональних даних під час обігу інформації (соціального, фінансового, правоохоронного, науково-технічного та іншого характеру), товарів, послуг і капіталів, що вимагає не тільки вільний рух інформації про особу, забезпечення її надійного захисту у відповідності до основних прав і свобод людини.

2. Зміцнення міжнародного соціального, економічного та науково-технічного співробітництва, розвиток інформаційних мереж, зростання транскордонних потоків персональних даних, з одного боку, та зусилля, що вживаються державною владою щодо розвитку демократичних процесів з іншого, визначають актуальність і об’єктивну необхідність захисту прав і свобод громадян України у цій сфері.

3. Конституцією України визначено зміст основних прав людини, у тому числі стаття 32 гарантує недоторканість особистого життя, зокрема – щодо збирання інформації про особу. Зазначене право повинно бути конкретизовано Законами України встановленням технологій їх виконання. Бази персональних даних про своїх клієнтів сьогодні формує широке коло суб’єктів – фізичних та юридичних осіб: підприємства та торгівля, приватні лікарі, нотаріуси тощо. ,,Витік інформації” з цих баз даних наносить шкоду багатьом особам, що потребує термінового законодавчого врегулювання цих питань.

4. Україна спізнюється майже на чверть століття як з підписанням міжнародних угод, так й з впровадженням відповідних норм міжнародного прав. Лише у 2005 році підписано

Конвенцію, яку ратифіковано Законом України ,,Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних" від 06.07.2010 № 2438-VI. Європейське право охоплює майже два десятки загальноєвропейських конвенцій, директив та рекомендацій з питань захисту персональних даних, кожна країна ЄС видала свої базові нормативно-законодавчі акти, приймалися конкретні закони: щодо діяльності з персональними даними у медичній, статистичній, державній, журналістській, поліцейській та інших сферах. Аналогічні закони прийнято в багатьох країнах світу, у тому числі – в країнах СНД, зокрема в Росії.

5. Враховуючи необхідність застосування сучасних технологій при автоматизованій обробці інформації про особу, а також виникнення загрози для конкретної людини стосовно витоку та несанкціонованого використання персональних даних, багато європейських країн підписали згадану Конвенцію. Принципи, що містяться у Конвенції, уточнюються і розширюються в Директиві 95/46/ЕС Європейського парламенту і Ради від 24.10.1995 стосовно захисту фізичних осіб у питаннях обробки персональних даних і вільного обігу цих даних та в Директиві 97/66/ЕС Європейського парламенту і Ради від 15.12.1997 стосовно обробки персональних даних і захисту приватності у телекомунікаційному секторі.

Отже з прийняттям Закону можна сказати, що держава зробила перший, уже впевнений та відчутний крок до Євроінтеграції та розвитку свого інформаційного простору в частині одного із його найвагоміших сегментів ,,захисту прав людини під час автоматизації обробки її персональних даних". Але як кажуть, ,,важливо не зробити перший крок, а почати рух вперед". Для цього на виконання Закону необхідно вирішити ряд задач, низка яких може бути вирішена тільки **на державному рівні**, а саме:

1. Створити (або надати повноваження вже створеному) орган контролю за станом захисту персональних даних. Крім того, встановити чітку та прозору юридично-правову базу щодо забезпечення розгляду справ та відповідальності за несанкціонований доступ та використання персональних даних та/або порушень в частині забезпечення відповідного захисту.

2. Ввести в експлуатацію Державний реєстр баз персональних даних, прийняти регламент його функціонування та порядок реєстрації баз даних.

3. Розробити та запровадити загальнодержавну класифікацію відомостей, які відносяться до персональних даних та вимоги щодо їхнього захисту та автоматизованої обробки.

4. Розробити та запровадити вимоги щодо функціонального профілю захисту автоматизованих систем, в яких передбачається обробка та зберігання персональних даних.

В той же час уже зараз, відповідно до вимог положень Закону, **на рівні окремих організацій та установ (державної та недержавної форм власності)** необхідно виконати досить клопітку та важливу роботу, яка передбачає:

1. В рамках загальної класифікації інформації в ІТС визначити окремий клас ,,Персональні дані" та автоматизовані системи, в рамках яких вони обробляються.

2. Забезпечити відповідні юридично-правові та організаційно-розпорядчі заходи щодо визначення власника, розпорядника та основних вимог із захисту персональних даних, які надаються фізичними особами та/або накопичуються організаціями (угоди про використання персональних даних, реєстрація бази персональних даних в рамках єдиного Державного реєстру баз персональних даних).

3. Забезпечити захист персональних даних, які обробляються в автоматизованих системах, шляхом створення комплексної системи захисту інформації відповідно до Закону України ,,Про захист інформації в інформаційно-телекомунікаційних системах" та Закону ,,Про захист персональних даних" в обсягах встановлених профілем захисту відповідними підзаконними актами Адміністрації Держспецзв'язку України.

Осиченко О.Б. (ВІТІ НТУУ „КПІ”)
Мужеський К. К. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ПОБУДОВИ І ПЕРЕВІРКИ ПРОГРАМНОЇ МОДЕЛІ МЕРЕЖІ ЗА ДОПОМОГОЮ КОМАНД ОПЕРАЦІЙНОЇ СИСТЕМИ ТА ПЕРЕФЕРІЙНОГО ОБЛАДНАННЯ

Актуальність знаходження віддалених абонентів у побудованій захищеній корпоративній мережі, а особливо тих, що несанкціоновано намагаються під’єднатись до неї, набуває все більшого та перспективного розмаху в інформаційних технологіях. Фактично не існує на сьогоднішній час корпоративної мережі, що у своєму складі не містить активних вузлів з розумінням команд адміністраторів та їх виконання у вбудованій оболонці для представлення відповідних результатів та більш детального налаштування.

Тому однією із задач, при використанні структурованих кабельних систем і побудованих логічних програмних схем взаємодії мережі, є питання завчасного виявлення нових несанкціоновано під’єднаних користувачів мережі та їх своєчасного усунення, особливо для корпорацій-провайдерів глобальної мережі [1].

Аналіз існуючих літературних джерел, стосовно даної проблеми, показав, що відсутній чіткий опис методик тестів виявлення та перевірки кінцевих користувачів корпоративних мереж. Попередньо проаналізувавши шлях до серверів, що забезпечують розподіл доступу кожного кінцевого вузла мережі, здійснюється під’єднання до активних вузлів мережі з метою перевірки завчасно побудованої схеми роботи мережі на наявність нових вузлів [2].

Методологічним підходом для вирішення даної задачі є побудова тестової автоматизованої системи на основі застосування скриптів для аналізу взаємодії різнотипних вузлів з конкретною орієнтацією на команди активного мережевого обладнання визначеного виробника. З урахуванням різнотипності виробників активного мережевого обладнання доведеться аналізувати та використовувати команди, що сприймаються найбільш поширеними серед них, що ускладнює можливість універсальної розробки.

Головною проблемою є затрати великої кількості часу системним адміністратором на виконання команд уручну і відсутність чітких алгоритмів відслідковування цілі дослідження. Наприклад, досліджується шлях до кінцевого вузла системи, що під’єднаний до корпоративної мережі. При отриманні позитивної відповіді, тобто шляху, прослідковується через які активні вузли мережі зроблено під’єднання. Далі перевіряється наявність даного підключення на побудованій програмній моделі структурованої кабельної системи. Використання вузькоспеціалізованої спрямованості досліджень дозволяє перевірити ряд факторів, зокрема таких як: до якої зони імен серверів належить даний вузол, яку саме віртуальну мережу використовує, до яких портів активного мережевого обладнання під’єднаний, які види MAC-адрес записані до віртуальної мережі і чи взагалі він повинен бути включений до даної мережі чи підмережі, що дозволяє вцілому здійснювати доступ до глобальних ресурсів. Враховуючи, вищесказане, методика повинна передбачати наступну послідовність дій:

1. Перевірка фізичного під’єднання вузла за допомогою команд операційної системи.
2. Перевірка працездатності роботи сервера доменних імен за допомогою команд операційної системи та отримання його імені і режиму функціонування.
3. Отримання IP-адреси шлюза, що дозволяє доступ до віртуальної мережі корпоративної мережі.
4. Отримання імені та номера віртуальної мережі, до якої входить кінцевий вузол.
5. Отримання повного шляху під’єднання від сервера доменних імен до кінцевого вузла мережі, з вказанням IP-адрес активного мережевого обладнання.
6. Перевірка імені віртуальної корпоративної мережі до якої входить кінцевий користувач за допомогою команд активного мережевого обладнання.

7. Перегляд усіх активних портів мережевого обладнання, що використовуються в поточний момент часу.

8. Вивід наявної таблиці MAC-адрес активного мережевого обладнання.

9. За допомогою отриманих результатів в пунктах 2–8 здійснюється побудова програмної моделі мережі.

10. Програмна модель мережі повинна звірятись із реальною моделлю, що будується графічно при початковому проектуванні структурованої кабельної системи.

11. Робиться висновок про законність підключення кінцевого вузла.

12. Якщо вузол є несанкціоновано під'єднаним – здійснюється заборона доступу до ресурсів глобальної мережі.

13. На сервері виконується написання конфігураційних файлів по забороні доступу до ресурсів.

Науковою новизною даної методики є відсутність, на нинішній час, чіткого алгоритму дій адміністратора по перевірці під'єднаних вузлів. При частковій наявності таких алгоритмів у компаніях-провайдерах доступу до глобальної мережі, не враховано різноманітності команд активних мережевих пристроїв, що розглядається, як суттєва проблема для створення програмної моделі мережі. Тобто, на даний час не існує стандартизованої послідовності дій адміністраторів різних рівнів по відслідковуванню таких користувачів, а, отже, і не існує загальної концепції у перевірці доступу до ресурсів глобальної мережі.

Пропонується розробити і побудувати скрипт, який дозволяє прослідкувати число користувачів, яке використовується компанією, а також його реалізацію для покриття усієї корпоративної мережі, що дасть доволі цікаві знання, зокрема такі як побудова в реальному часі програмної моделі мережі з детальною прив'язкою вузлів до MAC-адрес, конкретного використання портів активного мережевого обладнання, пришвидшить доступ до конкретних зон імен серверів з прив'язкою до підмереж та скоротить часові затрати роботи адміністратора мережі по побудові власної програмної моделі мережі у реальному масштабі часу і перевірці користувачів. До даного скрипта повинні увійти команди найбільш поширених активних пристроїв мережі, які використовуються на нинішній час, що породжує нову проблему для подальших досліджень в області побудови структурованих кабельних систем. Окрім того, значним чином буде чітко зменшено трафік каналу для пришвидшення роботи користувачами, що реально є під'єднаними і оплачують доступ до ресурсів глобальної мережі. Розробка даного скрипту та його подальше впровадження дозволить стандартизувати дії адміністраторів мережі різного рівня, дасть можливість побудови однакової для всіх корпоративних мереж програмної моделі структурованих кабельних систем. Практичне виконання скрипта пропонується виконати мовою команд оболонки bash на основі операційних систем з відкритим кодом, тобто операційних систем сімейства Unix, при цьому розглядається можливість впровадження до скрипта команд такого активного мережевого обладнання, що розроблено наступними виробниками: Extreem, Catalyst, AsoTel, Planet, DLink та FoxGate. Дані розробники були обрані, як найбільш поширені серед тих, що зустрічаються на нинішній час. Окрім того, схожість інтерфейсів взаємодії даного обладнання значно полегшує напрямок розробки та дозволяє створити універсальні умови для виконання даного скрипта, проблема полягає лише в тому, що усі активні вузли мережі повинні розуміти команди адміністратора та мати вбудований інтерфейс з можливістю віддаленого під'єднання. Важливим є факт раціональності використання наявного активного мережевого обладнання, за допомогою розробленої програмної моделі адміністратор зможе швидше приймати рішення по розгортанню нових віртуальних мереж виходячи із фізичних обмежень використання мережевих апаратних засобів.

ЛІТЕРАТУРА

1. *GNU/Linux* Desktop Survival Guide by Graham Williams- August 2006 & Toorcon 8 – September 2008.
2. *Learning* Debian GNU/Linux, By Bill McCarty 1st Edition September 1999 1-56592-705-2, 360 pages.

Паламарчук Н.А. (ВІТІ НТУУ „КПІ”)

ПОРЯДОК ВВЕДЕННЯ ОБ’ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ В ДІЮ

Перелік та послідовність робіт при введенні об’єктів інформаційної діяльності в дію визначається низкою законів та інших нормативно-правових актів з технічного захисту інформації. Вимоги даних документів є обов’язковими для всіх суб’єктів інформаційної діяльності, незалежно від їх організаційно-правової форми та форми власності, якщо обробляється інформація з обмеженим доступом.

З метою перекриття всіх можливих каналів витоку інформації система захисту інформації створюється за комплексним принципом. Тобто, мова йтиме про комплексну систему захисту інформації (КСЗІ). До складу КСЗІ входять заходи та засоби, які реалізують способи, методи та механізми захисту інформації від:

– витоку технічними каналами (акустичних, вібраційних, оптичних, побічних електромагнітних випромінювань і наведень, акустоелектричних тощо);

– несанкціонованих дій та несанкціонованого доступу до інформації, застосування закладних пристроїв чи програм, використання комп’ютерних вірусів;

– спеціального впливу на інформацію з метою порушення цілісності інформації або руйнування системи захисту.

У створенні КСЗІ беруть участь: установа, яка є замовником створення КСЗІ; виконавець робіт зі створення КСЗІ; виконавець проведення випробувань щодо створення КСЗІ; виконавець проведення державної експертизи КСЗІ (атестації).

Роботи по створенню КСЗІ на ОІД впорядковані у часі, взаємопов’язані та об’єднані в окремі етапи. Їх зміст, результати та терміни виконання визначаються в технічному завданні на створення КСЗІ. В загальному, до основних етапів створення КСЗІ відносяться: організаційні роботи; виконання передпроектних робіт; розроблення та впровадження заходів із захисту інформації; випробування та державна експертиза КСЗІ (атестація). Кожний етап роботи завершується відпрацюванням організаційно-технічних документів, згідно переліку, визначеному в технічному завданні на створення КСЗІ.

В залежності від призначення об’єкту інформаційної діяльності та складу КСЗІ можуть виконуватися різні види робіт та випробувань, і залучатися виконавці проведення робіт, які мають відповідні ліцензії або дозвіл на провадження діяльності у сфері технічного захисту інформації. Крім того, випробування здійснюють виконавці (суб’єкти господарської діяльності), які мають необхідне технічне забезпечення для даного виду робіт.

По завершенню всіх визначених в технічному завданні етапів робіт та оформлення організаційно-технічних документів призначається виконавець державної експертизи комплексної системи захисту інформації на відповідність вимогам нормативних документів системи технічного захисту інформації. Після проведення якої надається атестат відповідності КСЗІ. Атестат відповідності комплексної системи захисту інформації вимогам нормативних документів системи технічного захисту інформації є підставою для введення об’єкта інформаційної діяльності в дію. При розробленні та прийманні на озброєння нових інформаційно-телекомунікаційних систем висуваються ті ж вимоги, що і до об’єктів інформаційної діяльності.Такий шлях достатньо затратний по термінам і тому не зовсім підходить для військових організацій. Пропонується змінити порядок введення в дію об’єктів інформаційної діяльності, інформаційно-телекомунікаційних систем, а також розподіляти окремі завдання по створенню комплексної системи захисту інформації та введенню об’єктів інформаційної діяльності (інформаційно-телекомунікаційних систем) в дію між різними підрозділами установи.

Сторонні ж організації залучати лише для проведення випробувань та експертизи комплексної системи захисту інформації, при чому, для нових зразків – лише на етапі прийому на озброєння.

Паламарчук С.А. (ВІТІ НТУУ „КПІ”)

ДОЦІЛЬНІСТЬ ЗАСТОСУВАННЯ ІНФРАСТРУКТУР ВІДКРИТИХ КЛЮЧІВ *PKI* ТА *SPKI* В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Політика безпеки, що розробляється для інформаційно-телекомунікаційних систем (ІТС) має організаційно-технологічну складову до якої відносяться процедури ідентифікації, автентифікації та авторизації. Дані процедури можливо реалізувати застосовуючи інфраструктури відкритих ключів *PKI* (*Public Key Infrastructure*) та *SPKI* (*Simple Public Key Infrastructure*). Інфраструктура відкритих ключів *PKI* надає три основних сервіса безпеки: автентифікацію (суб’єкта, джерела даних), цілісність та конфіденційність. Ці сервіси дають можливість суб’єктам підтверджувати, що вони дійсно ті, за кого себе видають, отримувати гарантії, що дані не були змінені, і бути впевненими, що дані, відправлені іншому суб’єктові, будуть прочитані тільки ним.

Прикладом *сертифікату відкритого ключа* є формат X.509, який являє собою структурований двійковий запис у форматі абстрактної синтаксичної нотації *ASN.1*. Сертифікат містить елементи даних, що супроводжуються цифровим підписом *видавця сертифікату*. У сертифікаті є десять основних полів: шість обов’язкових і чотири додаткових. Зміст обов’язкових полів сертифікату може варіюватися. До них відносяться: серійний номер сертифікату; ідентифікатор алгоритму підпису; ім’я видавця; період дії; відкритий ключ суб’єкта; ім’я суб’єкта сертифікату.

Не зважаючи на перераховані сервіси безпеки інфраструктура відкритих ключів *PKI* не забезпечує авторизацію користувача та захист комп’ютерних мереж (є базисом сервісів безпеки, але не замінює інші засоби та методи захисту).

Для Збройних Сил України (ЗС України) не завжди принциповими є процедури ідентифікації та автентифікації, цього не можливо сказати про процедуру авторизації, яка підтверджує повноваження посадової особи. Проста інфраструктура відкритих ключів *SPKI* саме і надає можливості підтвердження повноважень особи та делегування даних повноважень іншим.

Сертифікати *SPKI* (сертифікати авторизації) мають зручну для сприйняття форму, містять текст вільного формату, фотокартку або іншу інформацію. *Сертифікати авторизації*, за задумом авторів ідеї *SPKI*, повинні генеруватися будь-яким власником ключа, якому дозволено надавати або делегувати повноваження. Хоча *SPKI-сертифікати* мають багато загального з *сертифікатами відкритих ключів* X.509 (наприклад, поля ім’я видавця та період дії), синтаксис і семантика цих полів неоднакові. Крім того, кількість полів в сертифікатах цих двох типів не дозволяє їх еквівалентно відображати один на одного, а угоди про імена відрізняються повністю.

Робота над документами *простої інфраструктури відкритих ключів SPKI* завершена, проте на практиці в повному об’ємі не реалізована, попит на *SPKI-сертифікати* дуже невеликий.

Перевага вирішення безпеки на базі інфраструктури відкритих ключів заключається в створенні єдиної інфраструктури, котра здатна підтримувати багаточислені сервіси безпеки в складному великомасштабному середовищі з багатьма додатками.

Недоліки застосування інфраструктури відкритих ключів в ЗС України: необхідність взаємодії та функціональної сумісносності з зовнішніми користувачами, значні витрати на впровадження та підтримання функціонування інфраструктури відкритих ключів; структура сертифікату не повинна змінюватися, тому використання в данному вигляді не задовольняє ЗС України.

Таким чином, виникає необхідність в розробці стандартів відкритих ключів, які були б орієнтовані на потреби ЗС України (як для повсякденної діяльності так і під час ведення бойових дій).

к.т.н. Пашковський В.В. (НЦСВ АСВ)

ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ДІС В АЛГОРИТМАХ ДІЯЛЬНОСТІ ОПЕРАТОРІВ СТАНЦІЙ РТР В УМОВАХ НЕВИЗНАЧЕНОСТІ

Ефективність системи радіотехнічної розвідки це міра відповідності, що пов'язана з безпосереднім призначенням системи для виконання чітко окреслених завдань. Ефективність завжди є підґрунтям для отримання корисного ефекту, котрий називається виграшем.

Ефективність процесу розпізнавання залежить від наступних факторів: кількості джерел радіовипромінювання, серед яких проводиться розпізнавання; ступеню невизначеності радіовипромінювання, серед яких проводиться розпізнавання; точності виміру параметрів; меж вимірювання параметрів; алгоритму розпізнавання та вибору критерію прийняття рішення про належність вимірювання до визначеного типу РТЗ.

Для оцінки ефективності ДІС проаналізуємо основні характеристики алгоритму діяльності оператора станції, існуючого та з впровадженням довідково – інформаційної системи. Принцип проведення оцінки ефективності наступний. Для визначення основних характеристик алгоритмів необхідно знати складові частини алгоритмів діяльності, характеристики елементарних операцій, їх кількість, послідовність та вид об'єднання.

Враховуючи те, що характеристики існуючого алгоритму діяльності розраховані та представлені, далі переходимо до розрахунку ймовірнісно – часових характеристик алгоритму діяльності оператора з використанням результатів роботи довідково – інформаційної системи. Більшість ймовірнісно – часових характеристик операцій відомі, за виключенням операцій, що пов'язані з використанням довідково – інформаційної системи.

В результаті узагальнення сукупностей споріднених операцій граф значно зменшується, що дозволяє наглядно проаналізувати алгоритм діяльності оператора та ефективність запропонованого інформаційного забезпечення станції радіотехнічної розвідки. В таблиці приведено характеристики споріднених операцій для діючого алгоритму.

Необхідно використовуючи методику, що розглянута в попередніх працях, розрахувати характеристики нововведених операцій, та розрахувати загальні характеристики алгоритму діяльності оператора станції РТР у випадку невизначеності з використанням довідково – інформаційної системи.

Згідно з методикою першим кроком є формування множини операцій, характеристики яких невідомі, $Оп = \{Оп_1, Оп_2, ..., Оп_n\}$, де n – кількість операцій, в нашому випадку це операція $Оп_{15}$.

Вибираємо експертну групу, за відомими методами, в кількості 12 експертів.

Пропонуємо кожному експерту з експертної групи за кожною з елементарних операцій визначити мінімальний та максимальний час та імовірність безпомилкового виконання операцій, та записуємо отриману інформацію у вигляді. Отримаємо верхню та нижню межі основних характеристик на прикладі обробки інформації отриманої від одного експерта для 15 операції. Розбиваємо кожен з інтервалів характеристик операції поданих експертом на 26 проміжних значень та записуємо у вигляді.

Пропонуємо експерту вибрати значення рівня за кожною характеристикою та отримуємо нечіткі множини у нашому випадку А та В: А – нечітка множина – середній час виконання операції; експертне опитування за середнім часом виконання кожної операції; В – нечітка множина – імовірність безпомилкового виконання операції; експертне опитування з визначенням імовірності безпомилкового виконання операції.

Використовуючи отримані дані від експертів розраховуємо T_i, для кожного проміжного значення з виданого експертом діапазону:

Розраховуємо оцінку значень ймовірностей попадання оцінок з визначеного діапазону та розташовуємо їх в порядку зростання :

Підставляючи, отримані значення в систему рівнянь, враховуючи, що загальна кількість елементів у діапазоні характеристик рівна 26, підраховуємо ступінь належності елементів множині :

Вибираємо значення $t_{22,2}$ та $p_{0,9204}$ з визначеного експертом інтервалу характеристик операції, що мають ступінь належності рівний 1. Записуємо вибране значення до таблиці у відповідний рядок.

Повторюємо проведені пункти методики для решти експертів, заносимо отримані характеристики до таблиці, у відповідний рядок.

Розраховуємо ступінь узгодженості експертів.

Задавши ймовірність помилки $P_п$=0,05, за таблицею розподілу Стюдента визначимо величину t, якщо, в нашому випадку, число ступенів свободи дорівнює 12, t=2,16.

Розрахувавши дисперсію σ^2, переходимо до розрахунку величини Δ та визначення довірчого інтервалу та представляємо у вигляді

що виступатиме ступенем довіри до отриманих результатів.

Застосувавши методику визначення характеристик алгоритмів діяльності оператора, на основі обробки експертної інформації, отримали наступні характеристики нововведених операцій: $t_{оп\,15}$= 22,1; p_{15}= 0,92. Отримавши характеристики всіх елементарних операцій алгоритму перейдемо до розрахунку ймовірнісно – часових характеристик алгоритму вцілому використовуючи методи перетворення граф – схеми алгоритму.

Після проведення розрахунків отримуємо середній час та імовірність безпомилкового виконання алгоритму оператором в умовах невизначеності при використанні довідково – інформаційної системи. Проводячи аналогічні розрахунки для оператора з середнім рівнем кваліфікації та граничним часом виконання кожної операції отримали за нижньою границею $\bar{\tau}_{1-16} = 131{,}6\,(c)$ та за верхньою границею $\bar{\tau}_{1-16} = 195{,}1\,(c)$.

За рахунок впровадження довідково – інформаційної системи підвищили ймовірність правильного прийняття рішення оператором станції радіотехнічної розвідки у випадку виникнення ситуації невизначеності на 18,4%.

Порівнюючи часові характеристики алгоритму діяльності оператора у випадку виникнення ситуації невизначеності без використання ДІС та з використанням ДІС отримали виграш показнику оперативності в середньому на 8,7% (з 6,5% до 13,9%).

Отримані розрахункові результати доводять, що з впровадженням довідково – інформаційної системи до інформаційного забезпечення станції РТР вдається підвищити показники ефективності станції РТР: ймовірність правильного прийняття рішення про належність до визначеного типу РТЗ та час виконання алгоритму діяльності оператором.

Таким чином, мета роботи, що полягала у підвищенні ймовірності правильного прийняття рішення оператором станції РТР в умовах виникнення ситуації невизначеності, досягнута та всі часткові задачі виконані в повному обсязі.

Висновки. Представлена структурна схема розробленої довідково - інформаційної системи оператору станції РТР, що включає наступні основні частини: оновлений інтерфейс користувача; блок імітації появи РТЗ; розширену базу даних; блок формування та видачі повної інформації за типами визначеними системою розпізнавання станції РТР; блок редагування, уточнення та оновлення інформації, що наповняє БД ДІС.

Довідково – інформаційна система призначена для підвищення основних показників процесу прийняття рішення оператором, шляхом видачі повної інформації в структурованому вигляді на засоби відображення інформації станції РТР.

В результаті аналізу альтернативного алгоритму діяльності оператора станції РТР визначили, що впровадження ДІС дозволяє проводити розпізнавання типів джерел РТР за середній час виконання алгоритму діяльності оператором – 168 с забезпечуючи виграш на 8,7 (6,5 – 13,9)%, при цьому ймовірність правильного прийняття рішення оператором станції РТР підвищується до 0,58, що вище існуючого показника на 18,4%.

Пелих О.О. (ВІТІ НТУУ,,КПІ”)

НОВИЙ ПІДХІД ДО ПОБУДОВИ ТРАНСПОРТНОЇ МЕРЕЖІ МОБІЛЬНОГО ОПЕРАТОРА ЗВ’ЯЗКУ

Згідно з загальною статистикою, оператори часто відчувають труднощі, пов’язані зі зростанням вартості експлуатації транспортної мережі, що забезпечує трафік від мережі радіодоступу (Radio Access Network − RAN) до комутаційного центру мобільних послуг (Mobile services Switching Center − MSC). Адже будь-якого оператора постійно доводиться, з одного боку, нарощувати абонентську базу, а з іншого − надавати нові сервіси, що вимагає розвитку мережі. При цьому більшість операторів прагне як скоротити витрати на утримання інфраструктури, так і ,,запастися” ресурсами на випадок подальшого розвитку мережі та підготовку інфраструктури для розширення RAN і каналів зв’язку без принципової зміни самого транспорту. Ось чому еволюційний перехід до пакетної передачі даних, який не тільки неминучий, але і, безумовно, вигідний для оператора, краще за все робити, зберігаючи існуюче обладнання.

Багато каналів не є власністю оператора та орендуються у того чи іншого провайдера. Тому оператор прагне завантажити орендований канал максимально. Правда, в даному випадку збільшується ризик зниження якості послуг, що надаються, викликаний навантаженням на мережу, що може виявитися дуже критичним для підтримки іміджу оператора. Відповідно, баланс між якістю і низькою операційної вартістю утримання мережі залишається делікатним запитанням.

Перед кожним оператором постає проблема переходу на інші протоколи передачі даних, що дозволяють більш ефективно працювати в умовній підмережі 2G, оскільки вона буде присутня для тих базових станцій, які не має сенсу оновлювати відразу. Також транспортна мережа зможе передавати дані для мережі 2,5 G, що є у всіх операторів у центральних регіонах. І, нарешті, кожному операторові необхідно забезпечити оптимальну передачу даних для активно розвиваються мереж третього покоління (3G) і сервісів, що базуються на IP (4G) [1].

Тому, з огляду на тенденції в розвитку технологій передачі даних, логічно припустити, що будь-яка сучасна мережа повинна будуватися на базі архітектури IP, як найбільш універсального протоколу, надає можливість оптимально передавати трафік будь-якого типу. Зручно використовувати мережу, в якій як у центрі, так і у вузлах радіомережі використовуються мультисервісні шлюзи, наприклад Lucent PacketStar PSAX, Alcatel 7670 RSP MG , які займаються ,,упаковкою” трафіку в пакети і наступною передачею його з будь-якої існуючої транспортної мережі, здатної пропускати IP-трафік. Взагалі, впровадження подібних рішень виправдано у випадках, коли мова йде про орендовані канали, особливо якщо говорити про дорогі магістралі, такі як супутникові або радіорелейні. Це дозволяє значно заощаджувати на оренді.

Однак, виробляючи мультиплексування трафіку, мультисервісні граничні пристрої передають по одним і тим же каналам різні види трафіку: скажімо, одночасно можуть транспортуватися дані GSM (TDM), GPRS (TDM), CDMA 1xEV-DO, UMTS (ATM) або будь-які інші потоки, підтримувані конкретним кінцевим пристроєм.

Оскільки, транспортна мережа вирішує одразу кілька запитань: по-перше, оператор має повну утилізацію декількох потоків E1 і, наприклад, кілька запасних каналів, у той час як традиційна комутація каналів часто має на увазі наявність декількох частково використовуються E1 без можливості їх консолідації. По-друге, це оптимізація передачі даних різних типів одним пристроєм. Адже якщо канал GSM може досить успішно піддаватися стисненню, то стиснення голосових даних у мережі CDMA навряд чи принесе хоч якийсь помітний виграш. У той же час упаковка декількох потоків мультисервісними пристроями для передачі по одним і тим же каналам зв’язку дозволяє, зокрема, прибирати

паузи в розмові, а також утилізувати простої, коли по каналу TDM не передаються ніякі дані. За відомостями компанії Lucent, така технологія майже на 40 % збільшує ефективність існуючих каналів зв'язку в мережі сучасного оператора [3]. Ну а якщо говорити про подальшу підтримку нових протоколів, то, використовуючи подібну мережу, оператор орієнтується на IP-трафік і легко запровадить нові сервіси на базі протоколу IP MPLS.

Але не можна забувати і про ефективне застосування оптичних мереж SDH, що відрізняються високою надійністю за рахунок наявності ,,кілець" (які мають на увазі два способи руху трафіку), а також більш низькою вартістю експлуатації. Для передачі даних через SDH у багатьох виробників обладнання, серед яких Alcatel, Lucent, Cisco, існують пристрої, що підтримують специфікацію Ethernet-over-SDH. Дані рішення володіють відпрацьованими технологіями, що оптимізують передачу пакетного трафіку через SDH, серед них універсальна схема фреймінг (General Framing Procedure, G.7041). Обладнання з підтримкою згаданих технологій оптимізовано для побудови мультисервісних мереж, і його відносять до систем SDH наступного покоління (NG-SDH). При цьому економія від експлуатації мереж з мультиплексуванням трафіку через SDH зростає в міру збільшення кількості потоків E1, які необхідно передавати через цю мережу [2].

Також можна використовувати граничні мультисервісні пристрої та комутатори Ethernet-over-SDH одночасно. У даному випадку кільце SDH призначене для передачі трафіку від граничних пристроїв на MSC, а граничні пристрої агрегує потоки даних з тих базових станцій, до яких з тих чи інших причин невигідно прокладати оптичні канали зв'язку.

До того ж сучасні рішення для передачі даних від різних виробників агрегує потоки E1 на цифровому крос-конектори (DACS − Digital Access Cross Connect), після чого їх передача по SDH або іншої мережі може відбуватися в одній групі, іменованої Multi-Link Group. У результаті можна економити на IP-адресах, що виділяються базових станцій, так як всі пакети, призначені для однієї групи, будуть вступати на один і той же DACS, а потім пристрій сам займеться розподілом потоків даних між базовими станціями. Треба сказати, це не тільки спрощує схему самої мережі, але і зменшує кількість вузлів мережі, що вимагають адміністрування. Оператор отримує можливість знову ж таки нарощувати кількість базових станцій, підключених до одного крос-конектори, без внесення змін до інфраструктурних основну транспортну мережу [4].

Таким чином: в будь-якому випадку перехід від традиційної різнорідної структури транспортної мережі до уніфікованої IP-інфраструктурі приносить оператору кілька переваг. По-перше, це можливість планомірного розвитку мережі без модернізації обладнання, по-друге, збільшення пропускної спроможності транспортного сегмента за рахунок звільнення порожніх службових та інших додаткових таймслотов і, по-третє, мультиплексування різних типів даних для передачі по одній IP-мережі, що важливо в умовах стрімкого збільшення популярності мультимедійних послуг в мережах стільникових операторів третього покоління. Оператор як зберігає інвестиції в придбане раніше обладнання, так і отримує можливість розширення мережі, підтримуючи належний рівень QoS. А це в свою чергу має на увазі безболісне підключення нових абонентів і розширення кількості надаваних сервісів, що вимагають високошвидкісної передачі даних.

ЛІТЕРАТУРА

1. *Оліфер В.Р.* Нові технології і устаткування IP-мереж. – Спб.: БВХ – Санкт-Петербург, 2000.

2. *Ломовицький В.В.,* ,,Основы построения систем и сетей передачи информации". М.: Вильямс, 2005р. –382с.

3. *Катунин Г.П.,* „Телекоммуникационные системы и сети. Том 2", – М.: Горячая линия – Телеком, 2004 р. – 672с.

4. *Шмалько А. В.* „Цифровые сети святи", 2005. – 283 с.

д.т.н. Пермяков О.Ю. (ІІТ НУОУ)
Залужний Р.М. (ІІТ НУОУ)
Лаврінчук О.В. (ІІТ НУОУ)

ПРОБЛЕМА СИНТЕЗУ СТРУКТУРИ НАВІГАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОКРЕМИХ ГРУП СПОЖИВАЧІВ

Однією з характерних особливостей сучасного розвитку наземної складової глобальних навігаційних супутникових систем є ускладнення структури їх підсистем, включаючи компоненти як космічного так і наземного базування, що, в першу чергу, обумовлено зростанням вимог до навігаційного забезпечення окремих груп споживачів, розмірів зон обслуговування і розвитку методів формування диференціальної корегуючої інформації (ДКІ) і подальшої її передачі кінцевим споживачам в реальному масштабі часу. Це висуває ряд проблем, пов'язаних з науково-обґрунтованою побудовою структури наземної компоненти, ефективним формуванням складу підсистем передачі і обробки навігаційної інформації. Тому, актуальним є питання – постановка і вирішення задачі визначення кількісних показників, що будуть характеризувати вимоги щодо навігаційного забезпечення окремих груп споживачів та послідуючої побудови, на їх основі, процедур синтезу структури наземних функціональних доповнень, що дозволить враховувати особливості та динаміку функціонування зазначених споживачів. У зв'язку зі складністю вирішення задач синтезу структури відповідних систем найбільший ефект від їх застосування може бути досягнутий при дослідженні і аналізі великомасштабних і типових систем масового використання, що розгортаються в даний час на території України [1 – 4]. Важливим етапом є розробка структури системи, під час якої вибираються принципи побудови системи, визначаються перелік функцій і задач, які повинна виконувати система відповідно до вибраного принципу (функції обробки за допомогою спеціального програмного забезпечення навігаційної інформації, яка накопичується мережею контрольно-корегуючих станцій (ККС), формування на її основі ДКІ в реальному масштабі часу і передачі інформації кінцевому споживачу). В загальному вигляді, що стосується системи навігаційного забезпечення для обслуговування визначеної території, важливою її складовою є просторово розподілена система, що включає регіональні мережі ККС та центру обробки навігаційної інформації, при чому ККС розміщуються так, щоб своїми зонами обслуговування (зонами доступності) вони перекрили визначену частину території при мінімальній їх кількості. З урахуванням особливостей застосування за призначенням ЗСУ та інших силових відомств задача синтезу структури включає: обґрунтування кількісних показників, що характеризують вимоги до навігаційного забезпечення; визначення оптимального числа, розташування і варіантів побудови елементів системи; вибір заходів щодо забезпечення необхідної живучості системи.

Вирішення задачі синтезу структури системи пропонується проводити з урахуванням ряду військово-технічних вимог на двох рівнях опису: рівні функціональних завдань навігаційного забезпечення на визначеній території і рівні складових елементів структури системи з врахуванням просторового розташування споживачів та особливостей виконання ними завдань за призначенням.

ЛІТЕРАТУРА

1. *Верещак А.П., Пискорж В.В.,* Жалило А.А., Литвинов В.А., Волох К.Ф., Концепция создания системы навигационного обеспечения Украины, Космічна наука і технология. 1998. Т 4. – № 5/6. – С. 46 – 55.

2. *Концепція створення* та експлуатації системи координатно-часового та навігаційного забезпечення України з застосуванням глобальних навігаційних супутникових систем на 2006-2011 роки. – Національне космічне агентство України, 2006. – 31 с.

3. *Малевич М.Н., Коныщева Г.Н.,* Аналіз работы действующего фрагмента ПШДК СКНОУ // 3-й Международный радиоэлектронный форум „Прикладная радиоэлектроника. Состояние и перспективы развития", Харьков, Украина, 2008. – Т. 1, часть 1, – С. 333 – 336.

4. *Горб А.,* Экспериментальная оценка точности определения координат навигационным приемником в дифференциальном режиме // Сучасні досягнення геодезичної науки та виробництва. 2009. – С. 103 – 108.

д.т.н. Пермяков О.Ю. (НУОУ)
к.т.н. Савченко В.А. (НУОУ)

КОНЦЕПЦІЯ ПОБУДОВИ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ НА ОСНОВІ ГЕОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Побудова систем підтримки прийняття рішень на основі геоінформаційних технологій (СППР ГІС) є новим напрямком застосування інформаційних систем. Особливого значення ця проблема набуває у військовій справі, де у реальному часі обробляються величезні обсяги інформації а вимоги щодо оперативності та точності рішень є досить жорсткими. Такі системи є людино-машинними, в яких особи, що приймають рішення можуть використовувати дані, знання, об'єктивні та суб'єктивні моделі для вирішення слабо структурованих завдань в умовах невизначеності.

Геоінформаційні технології у даному контексті розглядяються не тільки як засіб представлення та візуалізації інформації про місцевість та її інфраструктуру, а набагато ширше – як загальна методологія подання будь-яких даних, які мають координатно-часову прив'язку і можуть бути застосовані для вирішення завдань управління військами.

Складність сучасних автоматизованих систем управління (АСУ) досягла сьогодні такого рівня, який перевищує можливості людини, задіяної в контурі управління. Це перевищення людських можливостей виявляється не тільки в обсягах інформації, що підлягає обробці, але і в рівні логічної складності, неможливості аналізу всіх взаємозв'язків і відносин.

Традиційні інформаційні системи, засновані на стандартній моделі „клієнт–сервер" і традиційних методах управління не забезпечують необхідної якості інформаційного аналізу і необхідної ефективності формування керуючих впливів в умовах недостатності апріорної інформації про зовнішнє середовище функціонування, великої кількості різноманітних чинників, нестаціонарного і суб'єктивного їх характеру, змінності цілей і критеріїв якості управління внаслідок деградації або цілеспрямованої реконфігурації системи.

Загальна концепція побудови СППР ГІС полягає у розробці нової інформаційної системи, яка б об'єднала ГІС та інші підсистеми АСУ у єдиний інформаційний комплекс (рис. 1). Проте проблема не обмежується необхідністю вирішення суто технічних аспектів поєднання декількох інформаційних мереж, оскільки нова система, більш складна та динамічна, лише ще більше завантажить роботою операторів, які при вирішенні завдань управління змушені будуть постійно звертатися до різноманітних підсистем, баз даних та засобів обробки. Таким чином, просте поєднання інформаційних систем не принесе очікуваного результату.

Значного зменшення обсягів роботи операторів можна досягти шляхом застосування в СППР ГІС засобів штучного інтелекту (ШІ). Необхідність застосування ШІ у такій системі обумовлюється наявністю в системі значних обсягів інформації та потребою вивільнення людини-оператора від рутинних операцій щодо її обробки шляхом автоматизованого вирішення певного кола завдань.

Одним з останніх досягнень у галузі штучного інтелекту розподілених мереж є мультиагентні системи (МАС), системоутворюючий ефект в яких досягається шляхом взаємодії великої кількості інтелектуальних агентів різноманітного призначення. Завдання таких агентів в СППР ГІС і полягатиме в аналізі, узгодженні, моделюванні окремих фактів і подій, інформація про які знаходиться в ГІС та АСУ.

Практична проблема побудови СППР ГІС на основі мультиагентного підходу обумовлює необхідність вирішення низки теоретичних проблем та задач.

Так, зокрема, існує необхідність розробки та обґрунтування загальної архітектури такої системи, визначення завдань та функцій її складових елементів з урахуванням впливу

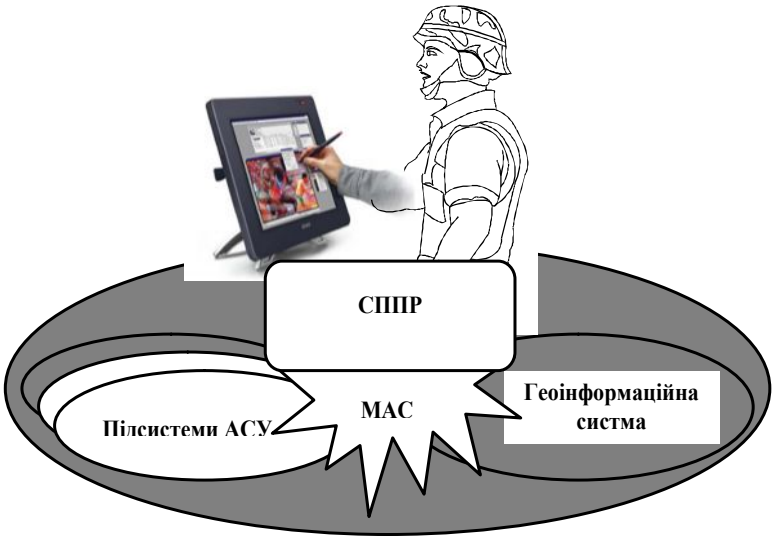


Рис. 1. Загальна структура системи підтримки прийняття рішень на основі геоінформаційних технологій

факторів середовища та технічних характеристик мереж.

Проблематиці побудови СППР різноманітного призначення присвячена велика кількість робіт вітчизняних та зарубіжних фахівців [1–5]. Проте у цих роботах не розглядаються системотехнічні аспекти побудови військових СППР ГІС, які мають суттєві відмінності від традиційних автоматизованих та інформаційних систем управління.

Тому у даний час існує необхідність дослідження моделей і методів побудови інтелектуальних СППР ГІС, а також засобів інтелектуалізованої обробки інформації в ГІС, заснованих на методах ШІ та інженерії знань.

Відповідно до запропонованої концепції для розробки методології побудови СППР ГІС необхідно вирішити наступні завдання:

вибір і обгрунтування інтелектуальних компонентів СППР ГІС;

дослідження математичних моделей інтелектуальних компонентів СППР ГІС, що забезпечують інтелектуальну інтеграцію у неоднорідному інформаційному середовищі;

розробка базової архітектури інтелектуальної СППР ГІС;

дослідження і розробка алгоритмів логічного виводу в архітектурі СППР ГІС;

створення проекту програмного комплексу для побудови СППР ГІС;

застосування розроблених методів і засобів для вирішення завдань інтелектуальної інтеграції в процесах управління військами.

Лише вирішення цих теоретичних завдань і дозволить побудувати СППР ГІС, як один з елементів інформаційних систем нового покоління.

ЛІТЕРАТУРА

1. *Информационно-управляющие* человеко-машинные системы: исследование, проектирование, испытания. Справочник. / Под общ. ред. А.И. Глубинского и В.Г. Евграфова // – М.: Машиностроение, 1993. – 528 с.

2. *Герасимов Б.М.* Системы поддержки принятия решений: проектирование, применение, оценка эффективности / Б.М. Герасимов, М.М. Дивизинюк, И.Ю. Субач // – Севастополь: Изд.центр СНИЯЭиП, 2004. – 320 с.

3. *Самардак А.С.* Геоинформационные системы / А.С. Самардак // – Владивосток: ДГУ, 2005. – 123 с.

4. *Интеллектуальные* системы поддержки принятия решений: Теория, синтез, эффективность / В.А. Тарасов, Б.М. Герасимов, И.А. Левин, В.А. Корнейчук // – К.: МАКНС, 2007. – 336 с.

5. *Пермяков О.Ю.* Інформаційні технології і сучасна збройна боротьба / О.Ю. Пермяков, А.І. Сбітнєв // – Луганськ: Знання, 2008. – 204 с.

к.т.н. Піддубний В.О.(РТФ НТУУ „КПІ”)
Корбут В.М.(РТФ НТУУ „КПІ”)
Піддубний В.В.(НТКУ)

ПОЛІПШЕННЯ ПРИЙОМУ СИГНАЛУ В МІСЦЯХ З ВАЖКОДОСТУПНИМ ПРОХОДЖЕННЯМ РАДІОХВИЛЬ

Дециметрові хвилі, в діапазоні яких працюють стільникові системи зв’язку NMT, GSM-900 та GSM-1800, сильно затухають при проходженні крізь перешкоди. Тому радіозв’язок в радіонепрозорих бетонних приміщеннях, в яких дуже часто розміщені кафе, офіси, різні контори та інше, нестійкий або взагалі відсутній. Забезпечення гарантованого зв’язку в таких випадках здійснюється ретрансляторами-репітерами, активними радіоподовжувачами (АРП). Використання АРП для багатьох користувачів не завжди можливе із-за їх вартості (500…700 у.о.). Однак в деяких випадках якісний зв’язок можна забезпечити за допомогою пасивних радіоподовжувачів (ПРП) [1], які складаються з двох антен, високопіднятої направленої та внутрішньої кругової, з’єднаних між собою коаксіальним кабелем. При работі в зонах гарантованого прийому замість високопіднятої направленої антени можна використовувати антену з круговою діаграмою спрямованості.

Розроблено декілька конструкцій ПРП, в яких використовуються дві антени з’єднані між собою фідером. Це – антени, взяті від радіостанції „Алтай” та модифіковані для діапазону частот стандарту GSM-900 (935-960 МГц), коаксіальні антени типу Sleeve antenna [2] або надширокосмугові, логоперіодичні антени типу ЛПА-900. Антени з’єднуються кабелями типу BELDEN H1000, 5D-FB PEEG, H155, RG-6/U чи RG-58.

Перша конструкція ПРП складається з двох ненаправлених антен від радіостанції „Алтай”. Як фідер використовується коаксіальний кабель 5D-FB PEEG довжиною 5 м (питомі втрати 0,2дБ/м). Одна з антен була розміщена в підвалі, в якому мобільна станція (МС) фіксувала повну відсутність зв’язку з базовою (БС), а друга – знадвору приміщення в точці максимального сигналу. Після монтажу ПРП в підвалі з’явився зв’язок з БС. Індикатор рівня сигналу телефонів Nokia 1100 чи Motorola SLVR показував 4 мітки. Стійкий зв’язок МС з БС забезпечувався на віддалі 1,5 -2 м від внутрішньої антени. Результати близькі до вказаних були отримані в другій конструкції ПРП (внутрішня і зовнішня антени коаксіального типу Sleeve antenna). Ефективність ПРП повністю залежить від типу з’єднувального кабеля. Найкращі результати отримані з кабелями типу BELDEN H1000, 5D-FB PEEG, H155. Дешеві кабелі типу RG-6/U та RG-58, виявилися практично не придатними для використання в ПРП. Заміна внутрішньої антени на антену типу ЛПА-900, розміщену в кутку приміщення, дозволила збільшити зону впевненого зв’язку в напрямку максимального випромінювання до 3 м. Індикатор вхідного сигналу мобільного телефону показав 5 міток.

При недостатньому сигналі необхідне ввімкнення в з’єднувальний кабель додаткових підсилювачів, наприклад, підсилювачів від активних телевізійних антен зі зміненою смугою пропускання, однак при цьому необхідно встановлювати подвійну кількість антен (окремі канали для прийому та передачі) або реверсивні підсилювачі. Структура АРП визначається конкретними умовами розповсюдження радіохвиль в точці прийому а її використання економічною доцільністю.

Таким чином використання РП, як активних так і пасивних, дозволяє збільшити напруженість електромагнітного поля в радіонепрозорому приміщенні до рівня достатнього для проведення стійкого зв’язку між МС та БС.

ЛІТЕРАТУРА

1. *Корсак В.Ф., Максименко Ю.Л., Микрюков А.С.,* Олейник В.Ф. Об использовании пассивных радиоудлинителей в сотовых системах связи. Материалы 10 Международной Крымской конференции „СВЧ-техника и телекоммуникационные технологии”.– Севастополь, 2001. – 253 – 254 с.

2. *К. Ротхаммель.* Антенны. Том 2.-Минск: Из-во „Наш город”, 2001. – 414 с.

Піскун С.Ж. (ІСЗЗІ НУТУ „КПІ”)

ЗАВАДОЗАХИЩЕНІСТЬ ТИПОВИХ АЛГОРИТМІВ ВХОДЖЕННЯ В СИНХРОНІЗМ ЛІНІЙ І СИСТЕМ ЗВ’ЯЗКУ З ПСЕВДОВИПАДКОВИМ ПЕРЕЛАШТУВАННЯМ РОБОЧОЇ ЧАСТОТИ

Одним із основних шляхів досягнення потрібної завадозахищеності ліній і систем радіозв’язку (РЗ) в умовах дії навмисних завад є застосування сигналів з псевдовипадковим перелаштуванням робочої частоти (ППРЧ). Незалежно від того, що радіозасоби з ППРЧ існують більше трьох десятиріч, процес удосконалення алгоритмів їх функціонування триває. Окрім того, доступ до опису цих алгоритмів залишається за зрозумілих причин обмеженим, що вимушує вирішувати завдання розробки вітчизняних варіантів.

Головним показником якості функціонування радіозасобів з ППРЧ є ступінь їх спроможності забезпечувати передачу інформації в умовах радіоелектронного придушення. Тому аналіз завадозахищеності системи синхронізації ліній і систем РЗ з ППРЧ, і в першу чергу, її складової - підсистеми, що забезпечує процес входження в синхронізм радіолінії з ППРЧ, залишається актуальною задачею. Завадозахищеність радіолінії з ППРЧ в цілому в першу чергу залежить від завадозахищеності цієї підсистеми, яка визначається алгоритмом входження в синхронізм, згідно з яким вона працює

Проте аналізувати завадозахищеність кожного з усієї досить великої множини відомих алгоритмів або навіть частини з них потреби немає. Достатньо розробити методичний апарат аналізу завадозахищеності для двох основних типових алгоритмів входження в синхронізм. Це пояснюється тим, що більшість відомих алгоритмів схожі за своїм принципом дії: синхронізація відбувається за рахунок співпадіння у часі неуражених завадами частот прийому і передачі, що використовуються для входження в синхронізм, і забезпечення подальшого правильного прийому синхрокадра цифрової інформації, що передається на цих частотах. Головна відміна між цими двома типовими алгоритмами міститься в тому, що для входження в синхронізм використовуються або тільки незначна фіксована частина частот (зазвичай від 4 до 32) із загальної кількості (128, 256 і навіть більше), призначених для роботи радіолінії в режимі передачі корисної інформації, або деяка частина з всіх робочіх частот, яка плинно, через фіксовані проміжки часу змінюється (оновлюється). Відрізняються алгоритми своїми взаємопов’язаними завадовими і часовими характеристиками.

На основі підходу, запропонованого в [1], розроблена методика розрахунку завадозахищеності входження в синхронізм, придатна для аналізу обох типів алгоритмів синхронізації. Розроблена методика дозволяє виконувати розрахунки для довільних значень вхідних даних, що характеризують завадову обстановку, канал зв’язку і власне сам алгоритм входження в синхронізм (структуру так званої синхропреамбули). Приведений приклад порівняльного аналізу. Розрахунки проводились для повільної ППРЧ та типової швидкості передачі інформації в радіоканалі 19,2 кбіт/с. Результати представлені у вигляді відповідних графіків.

Результати аналізу дають можливість за допомогою вибору певних значень характеристик алгоритму входження (включаючи структуру синхропреамбули) оптимізувати показники завадозахищеності – імовірність входження в синхронізм за відведений час, – як з метою скорочення часу входження, так і з метою покращення імовірності синхронізації.
Отримані результати і висновки можуть бути корисними при виборі структури типового алгоритму входження в синхронізм при розробці і удосконаленні (модернізації) вітчизняних радіозасобів для ліній і систем РЗ з ППРЧ.

ЛІТЕРАТУРА

1. *В.Г. Міщенко, В.Ф. Єрохін.* Методика оцінки завадозахищеності алгоритмів входження в синхронізм радіолінії зв’язку з псевдовипадковим перелаштуванням радіочастоти // Захист інформації, 2001. – № 2.

Погрібняченко А.І. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ МОЖЛИВОСТЕЙ СИСТЕМИ SDH ДРУГОГО ПОКОЛІННЯ – NG-SDH

Стрімкий розвиток інформаційних технологій та поява концепції мереж нового покоління (NGN) призвели до різкого росту проблем підприємств та галузей у високошвидкісних мережах передачі даних, трафік яких представляє собою пакети змінної довжини. Основна проблема при передачі даних через мережі SDH полягала у тому, що пакетну інформацію необхідно упаковувати у віртуальні контейнери, призначені для передачі TDM-трафіка. Оптимальним виходом з ситуації, що склалася стало створення концепції мереж SDH другого покоління – NG-SDH.

Переваги технології NG-SDH:

– одночасна передача TDM та Ethernet трафіка;

– швидкість до 10Гбіт/с (при використанні спектрального ущільнення – 40Гбіт/с);

– підтримка інтерфейсів Fast Ethernet 10/100 BaseT та Gigabit Ethernet 1000 BaseX;

– функція влаштованого комутатора другого рівня (switch layer 2) з підтримкою технології віртуальних локально обчислювальних мереж (VLAN);

– підтримка різних алгоритмів захисту передаваного трафіка: SNCP, MSP, MS-SPRing.

Для адаптації мереж SDH до мереж нового покоління, NG-SDH була побудована на основі декількох технологій: PoS, LAPS, ATM, GFP та інших.

Створені на основі синхронних мультиплексорів рівнів STM -1/4/16/64 мультисервісні транспортні платформи NG-SDH успішно вирішують задачу об’єднання трафіка з часовим розділенням каналів (TDM) і трафіка Ethernet з комутацією пакетів у агрегатні потоки зі швидкістю від 155Мбіт/с до 10Гбіт/с, а застосування технології SDH та спектрального ущільнення WDM дозволяє збільшити пропускну здатність трактів до 40Гбіт/с при теоретичній межі швидкості в декілька терабіт за секунду.

Основу NG-SDH складає інтелектуальна комутація (поєднання комутації каналів та пакетної комутації) та технологія передачі даних поверх SDH (EoS). Технологія EoS заснована на трьох стандартних засобах: віртуальній конкатенації (VCAT), загальній процедурі формування кадра (GFP) та механізму автоматичного регулювання полоси пропускання лінії (LCAS).

Віртуальна конкатенація логічно зв’язує індивідуальні контейнери в єдине з’єднання. Будь-яка кількість контейнерів будь-якого типу (VC-12, VC-3 або VC-4) можуть бути згруповані разом, утворюючи логічний канал. Це забезпечує кращу ступінь деталізації полоси та дозволяє ефективно використовувати пропускну здатність SDH.

Загальна процедура формування кадра (GFP) забезпечує формування асинхронного трафіку даних на основі кадрів змінної довжини до байт орієнтованого трафіку SDH з мінімальними затримками та збитковістю заголовків. Механізм автоматичного регулювання полоси пропускання лінії (LCAS) дозволяє реалізувати будь-які зміни пропускної здатності без припинення передачі даних.

Функція влаштованого комутатора другого рівня з підтримкою технології віртуальних локально-обчислювальних мереж дозволяє уникнути затрат на додаткове обладнання (повторювачі, комутатори) при об’єднанні окремих ЛОМ в єдину структуровану мережу передачі даних. Сучасні мультиплексори NG-SDH представляють собою мультисервісні транспортні платформи (MSTP), котрі здатні працювати на канальному рівні моделі OSI. При цьому на MSTP покладаються функції агрегації та комутації притаманні традиційним комутаторам.

Таким чином, заснована на технології NGN технологія NG-SDH призначена для надання послуг передачі даних та голосових сервісів, знімає цілий ряд обмежень існуючих при використанні технології SDH та дає можливість використовувати існуюче телекомунікаційне обладнання без значних витрат на модернізацію, саме у цьому і полягає її економічна та технологічна доцільність.

к.т.н. Правило В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Могилевич Д.І. (ВІТІ НТУУ „КПІ”)
к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)

ОСОБЛИВОСТІ TMN-ПЛАТФОРМ І СТРАТЕГІЇ ПЕРЕХОДУ НА АРХІТЕКТУРУ TMN

Донедавна системи управління телекомунікаційними мережами, що використовують архітектуру TMN (Telecommunication Management Network), будувалися в основному на індивідуальній основі, без використання платформ. Зараз ситуація змінилася. З’явилися багатофункціональні платформи TMN для додатків, що реалізують управління телекомунікаційними мережами, наприклад HP OV Telecom DM TMN, Digital Temip, Vertel TMN Manager Platform і Agent Platform, ISR Global Orbit і ін. Ці платформи, крім звичайних функцій, включають і ряд додаткових функцій і засобів, необхідних для побудови повноцінної системи TMN, а саме:

– засоби ведення довідкової системи, що зберігає інформацію про менеджерів і агентів, у тому числі й про місця їх дислокації у вузлах мережі. Довідкова система дозволяє їм автоматично знаходити один одного в мережі по не пов'язаних з місцем їх розташування іменам;

– засоби створення репозитарія − бази даних екземплярів керованих об’єктів. Репозитарій зберігає екземпляри об’єктів в ієрархічно впорядкованій формі, що відбиває підпорядкованість елементів у реальній мережі;

– засоби маршрутизації й фільтрації повідомлень протоколу керування CMIP, що циркулюють між агентами й менеджерами;

– засоби кореляційного аналізу потоку повідомлень для виявлення причинно-наслідкових відносин у керованій системі;

– інструментальні засоби розробки й налагодження індивідуальних класів керованих об’єктів на основі стандартних бібліотек класів типових елементів, за допомогою яких детально описуються родові характеристики всіх типових елементів телекомунікаційних мереж, так що розроблювач може або використовувати готовий опис елемента або доповнити його деякими індивідуальними атрибутами.

Розглядаючи процес переходу на архітектуру TMN, більшість аналітиків сходяться в думці в тому, що спостерігається суттєве зростання інтересу до TMN-продуктів у операторів і постачальників послуг.

Перехід до TMN різних компаній може носити як еволюційний, так і революційний характер. На швидкість впровадження TMN впливають два фактори: розмір компанії-оператора й динаміка розвитку самої мережі оператора.

Революційний характер переходу на TMN-архітектуру можуть дозволити собі невеликі оператори, які автоматизуючи свої системи, часто кардинально змінюють їх архітектуру та не мають ніяких „старих” систем управління.

Специфіка ринку телекомунікацій нашої країни характеризується динамічним розвитком, з одного боку, і не достатньо розвинутою системою управління − з іншого. Тому перспективи розвитку TMN у країнах СНД досить сприятливі.

ЛІТЕРАТУРА

1. Фокин В.Г. Управление телекоммуникационными сетями: Учебное пособие. – Н.: СибГУТИ, 2001. – 112 с.
2. TMForum GB929. Telecom applications map. Release 2.1, 2009.
3. ITU-T Recommendation M.3010 (02/2000). Principles for a telecommunications management network.

Прокопенко Є. М. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ХАРАКТЕРИСТИК ЗАСОБІВ РАДІОЕЛЕКТРОННОГО ПОДАВЛЕННЯ СИСТЕМ РАДІОЗВ’ЯЗКУ

Важливе місце в забезпеченні переваги в управлінні військами та зброєю в сучасних операціях (бойових діях) посідає радіоелектронна боротьба. Провідні держави світу приділяють велику увагу питанням розвитку систем та засобів радіоелектронної боротьби.

Сучасні засоби радіоелектронного подавлення (РЕП) здатні з високою ефективністю та у короткий час подавити систему радіозв’язку, побудовану на традиційних принципах.

В даний час створено значну кількість засобів РЕП, які дозволяють порушувати управління військами шляхом подавлення засобів зв’язку в різних діапазонах робочих частот з використанням всього комплексу навмисних завад.

Так американський наземний комплекс радіоелектронної боротьби для сухопутних військ „Вулфпак” за допомогою одного або декількох малогабаритних прийомо-передавальних пристроїв може здійснювати оптимальне подавлення ліній радіозв’язку спрямованими малопотужними завадами в результаті дії яких цифрові засоби радіозв’язку залишаються працездатними, але не забезпечують передачі корисної інформації.

Враховуючи 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 підвищення ефективності функціонування систем радіозв’язку в складній радіоелектронній обстановці.

Для подавлення військових систем радіозв’язку (ВСРЗ) можуть застосовуватися різні види організованих завад, що реалізуються у відповідних станціях завад. Все різноманіття варіантів подавлення радіозасобів визначається в основному шляхами, якими їх розробники прагнуть сконцентрувати обмежену потужність передавачів в певних частотних діапазонах, часових інтервалах та просторових секторах. Для подавлення засобів одного і того ж класу, але з використанням різних видів сигналів і способів їх обробки, застосовуються різні види завад. Тому виникає задача підвищення ефективності ВСРЗ, що функціонують в умовах впливу навмисних завад.

Все різноманіття завад, за частотно-часовими характеристиками, можна звести до шести основних різновидів: шумові, імпульсні, вузькосмугові (в граничному наближенні – синусоїдальні), внутрішньосистемні, ретрансльовані, імітаційні.

За допомогою імітаційного моделювання проведена оцінка ефективності впливу навмисних завад на характеристики військової системи радіозв’язку. Дослідження показали, що для різних режимів роботи засобів радіозв’язку ефективними виявляються певні види навмисних завад.

Проведений аналіз дозволяє зробити наступні висновки.

Найбільш універсальною і стійкою до різних способів підвищення завадостійкості, що застосовуються в ВСРЗ, є шумова загороджувальна завада. Потужність шумової завади може бути використана ефективніше за рахунок зосередження її в обмеженій смузі частот, значно меншій, ніж діапазон частот СРЗ, тобто за рахунок створення шумової завади в частині смуги. Для ефективного радіоелектронного подавлення ВСРЗ з псевдовипадковим перестроюванням робочої частоти доцільно використовувати прицільну за частотою заваду у відповідь (ретрансльовану заваду).

Особливу небезпеку для військових систем радіозв’язку з цифровою модуляцією представляють імітаційні (дезінформуючі) завади, при впливі яких система залишається працездатною, однак, не забезпечує передачі корисної інформації. В деяких випадках дезінформуючі завади можуть призводити до введення неправдивої інформації в ВСРЗ, викликати хибні режими роботи за рахунок впливу на системи тактової і циклової синхронізації приймача.

к.т.н. Радзівілов Г.Д. (ВІТІ НТУУ „КПІ”)
Мацаєнко А.М. (ВІТІ НТУУ „КПІ”)
Назарчук Б.О. (в/ч А1906)

АВТОМАТИЗАЦІЯ РОЗРОБКИ ПРОГРАМ РАДІОЗВ’ЯЗКУ

Основні показники ефективності систем радіозв’язку спеціального призначення закладаються під час планування. Одним із важливих етапів при плануванні та організації радіозв’язку є створення програми радіозв’язку. Програма радіозв’язку – це набір радіоданих, які необхідні для встановлення і ведення сеансу радіозв’язку [1]. Правильно створена програма радіозв’язку здатна забезпечити стійкий зв’язок в умовах дії засобів радіоелектронної боротьби противника, підвищити такі характеристики як оперативність, прихованість і безпека зв’язку.

Зазвичай (в мирний час), програма радіозв’язку створюється на довготривалий період (період роботи кореспондента) і перехід до роботи на інші програми здійснюється планово [2]. Тобто, наступна програма радіозв’язку розробляється заздалегідь. Оскільки системи радіозв’язку спеціального призначення повинні вирішувати відповідні завдання в особливих умовах функціонування, то терміни переходу роботи на інші програми радіозв’язку, а також створення цих програм, здійснюється в значно коротші терміни часу, ніж за умов повсякденної діяльності. При цьому неможливо заздалегідь передбачити умови роботи кореспондентів, які пов’язані зі зміною ситуації. Тому, за таких умов виникає обґрунтована необхідність у підвищенні ефективності процесу створення програми радіозв’язку в особливий період функціонування систем радіозв’язку спеціального призначення. Показником ефективності в даному випадку виступає оперативність розробки відповідних програм радіозв’язку.

В теперішній час розробка програм радіозв’язку здійснюється в ручному режимі, що знижує оперативність роботи систем радіозв’язку спеціального призначення та вимагає залучення значних людських і часових ресурсів [3].

Аналіз процесу створення програми радіозв’язку дає можливість зробити висновок, що деякі етапи створення програми можна автоматизувати. Це такі етапи як підбір позивних, коефіцієнтів, частот, оскільки на них витрачається найбільше ресурсів. В свою чергу, такий етап як призначення часу проведення сеансів зв’язку вимагає роботи відповідної посадової особи.

В доповіді зазначено, що такий стан зумовлює актуальність автоматизації розробки програм радіозв’язку при плануванні вирішення завдань системами радіозв’язку спеціального призначення. Вирішення даного завдання пропонується здійснювати двома взаємопов’язаними шляхами: створення баз даних позивних, коефіцієнтів, частот та програмного забезпечення для їх взаємозв’язку. Базу даних частот планується створити на основі існуючих прогнозів радіочастот для різних радіотрас, а бази позивних та коефіцієнтів для радіонапрямків створити внесенням до них всіх можливих варіантів їх формування. Це дасть можливість в умовах особливих режимів функціонування систем радіозв’язку спеціального призначення в короткі строки створювати програми радіозв’язку для кореспондентів, при цьому усуваючи можливість використання радіоданих, що використовуються в інших радіонапрямках.

ЛІТЕРАТУРА

1. *Посібник офіцера* – зв’язківця / Під редакцією Д.Т. Примака – Київ: ВІТІ НТУУ „КПІ”, 2002. – 144 с.

2. *Лисенко І.В.* Організація та засоби зв’язку. Ч. 1. організація та експлуатація засобів зв’язку тактичної ланки управління. – Житомир: ЖВІРЕ. 1998. – 76 с.

3. *Рудик В. В.* Актуальні проблеми та напрями розвитку системи зв’язку Збройних Сил України як складової частини системи управління військами (силами) / В. В. Рудик // Наука і оборона. – 2005. – № 2. – С. 22 – 28.

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

ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ АДАПТИВНИМИ АГОРИТМАМИ ФІЗИЧНОГО РІВНЯ

Однією з найбільш вагомих характеристик сучасних телекомунікаційних мереж є пропускна спроможність. І якщо зазначена характеристика у комерційних телекомунікаційних мережах відіграє основну роль як визначник якості послуг та в кінцевому результаті – їх вартості, то в мережах спеціального призначення (в системах зв’язку силових структур) мова може йти про виконання або невиконання поставлених задач. Зазначимо, що одним з основних родів зв’язку низових ланок управління силових структур, що використовується для побудови телекомунікаційних мереж, є радіозв’язок. Тут найбільш відомими виробниками якого є: Harris, Thales, Selex (Marconi), Tadiran, Rockwell, Rohde&Schwarz, Singars.

Зазвичай, для забезпечення заданої пропускної здатності за умови впливу зовнішніх факторів (більшою мірою ненавмисних у мирний час та навмисному впливі протидіючої сторони у особливий період) питання керування пропускною спроможністю між окремими вузлами мережі розглядаються за допомогою адаптивної маршрутизації потоків. При цьому не береться до уваги причина та величина зміни пропускної здатності (від деякого зменшення до повного припинення) між окремими вузлами телекомунікаційної мережі. Вона може бути зумовлена як безпосереднім навмисним впливом, наприклад, знищенням певних елементів мережі, так і, в більшій мірі, погіршенням завадової обстановки в районі розгортання елемента мережі зв’язку. Останнє може породжуватися великою кількістю різноманітних радіозасобів, які працюють в зоні розгортання телекомунікаційних мереж.

Разом з тим, останнім часом велика кількість наукових публікацій переконливо стверджує про можливість суттєвого підвищення пропускної спроможності телекомунікаційних мереж, які між окремими вузлами в протоколах випадкового множинного доступу запроваджують процедури розділяння конфліктів на фізичному рівні за різноманітних додаткових припущень (наприклад, про втрати заявок у вхідному потоці та при постановці в чергу джерела повторних викликів, про обслуговування тільки пар заявок, про обслуговування заявок різних випадкових довжин та ін.).

Також, з’явилось багато публікацій про методи синтезу алгоритмів когерентної демодуляції сигналів різних видів модуляцій (маніпуляцій) що спостерігається в адитивній суміші з синхронною або гетерохронною подібною завадою та білим шумом. Результати аналізу потенційної завадостійкості вказаних алгоритмів демодуляції характеризується тим, що при перевищенні миттєвої потужності заважаючого сигналу над корисним на певну величину, завадостійкість прийому корисного сигналу в умовах впливу подібної синхронної завади асимптотично наближається до завадостійкості прийому в каналі, в якому присутній лише білий шум. Тобто, за ідеального когерентного прийому і відсутності будь-яких викривлень сигналу та завади негативний вплив завади на завадостійкість прийому корисного сигналу, яка суттєво перебільшує за миттєвою потужністю корисний сигнал, зводиться до нуля.

Стало очевидним, що напрямки удосконалення систем зв’язку з випадковим множинним доступом, а саме: удосконалення протоколів випадкового множинного доступу на рівні доступу до середовища передачі та розділяння взаємозаважаючих сигналів на фізичному рівні взаємно доповнюють, збагачують можливості їх подальшого розвитку.

Таким чином можна констатувати, що з використанням адаптивних агоритмів фізичного рівня або іншими словами – в протоколах множинного доступу на рівні доступу до середовища передачі та розділянні взаємозаважаючих сигналів на фізичному рівні можна побудувати телекомунікаційні мережі зв’язку, в яких зміна завадової обстановки на елементах мережі не буде призводити до значного погіршення пропускної спроможності.

к.т.н. Раєвський В.М. (ВІТІ НТУУ „КПІ”)
Турянський К.М. (ВІТІ НТУУ „КПІ”)

SDR – ТЕХНОЛОГІЯ ЯК ПЕРСПЕКТИВНИЙ ШЛЯХ ПОБУДОВИ РАДІОЗАСОБІВ НОВОГО ПОКОЛІННЯ

Теорія побудови радіоприймальних засобів визначає, що приймач складається з загального та часткових трактів прийому радіосигналів. У загальному тракті обробляються всі класи випромінювання, у часткових трактах – тільки певного класу. До недавнього часу вказане яскраво підтверджувалось побудовою професійних засобів радіозв’язку. Так, радіоприймачі серії Р-155 (прийняті на озброєння в 1965 році) мали конструктивно окремо виконані блоки синтезатора частоти (1-0М), телефонних сигналів частотної та однополосної модуляції (4-0М), амплітудної модуляції та телеграфії (2-1М), частотної телеграфії (5-0М), телеграфних видодів (9-0М). Радіоприймачі серії Р-160 (прийняті на озброєння в 1978 році) також будувались подібним чином – конструктивні окремі блоки за видами сигналів, наприклад, блок формування телеграфних родів роботи (Б14-2), блок формування телефонних родів роботи (Б4-24) та ін. Вказане призводило до необхідності реалізовувати окремі блоки для кожного конкретного виду сигналу (класу випромінювання), що призводить до додаткових витрат, технічної складності радіозасобів та як наслідок незадовільної надійності. Стало зрозумілим, що надалі такий шлях неприйнятний.

Стрімкий розвиток обчислювальної техніки, починаючи з 80-х років минулого століття, дозволив будувати засоби радіозв’язку за принципово новим шляхом. Перші технічні роботи по цифровій обробці радіосигналів використовували аналогову техніку радіозв’язку попередніх поколінь в телефонний канал якої через відповідні узгоджуючі пристрої підключалась персональна електронно-обчислювальна машина, що дозволяло вести обмін данними (окремими короткими повідомленнями та файлами). Яскравим представником такого програмного забезпечення є програма MixWin.

Наступним етапом стало створення спеціалізованих цифрових процесорів обробки сигналів, які дозволяють майже на робочій частоті (без пониження частоти до проміжної) здійснювати обробку радіосигналу. Такий шлях веде до уніфікації радіозасобу, коли перелік режимів роботи та класів випромінювання, які він здатний обробляти, визначається не наявністю певних блоків, а тільки від відповідної версії програмного забезпечення. Такий шлях обрано провідними виробниками радіозасобів тактичної ланки управління – Harris, Selex, Tales, Tadiran, коли зміна програмного забезпечення змінює можливості радіостанції.

Більш бюджетним шляхом побудови новітніх радіозасобів є використання не спеціалізованих цифрових процесорів обробки сигналів, а потужностей персональних електронно-обчислювальних машин загального використання з спеціалізованим програмним забезпеченням. Такі радіозасоби отримали назву SDR-радіозасоби (Software Defined Radio – програмно визначене радіо), у яких програмне забезпечення використовується як для модуляції, так і для демодуляції радіосигналів. Мета такого підходу – створити систему, яка може приймати й передавати практично будь-які радіосигнали за допомогою програмного забезпечення, яке апріорі є гнучким і адаптивним. Наразі SDR широко застосовуються у військовому й стільниковому зв’язку, де в режимі реального часу потрібна підтримка різноманітних мінливих радіопротоколів. Можливості застосування SDR техніки досить різноманітні. Це може бути приймач, трансивер, панорамний аналізатор спектра або SDR тракт до вже наявної традиційної радіостанції, що помітно розширить можливості останніхо. Слід зазначити той факт, що комп’ютерні технології й програмне забезпечення швидко розвиваються, відповідно й Software Defined Radio здатне розвиватися разом з ними. Модернізувавши в черговий раз комп’ютер або проінсталювавши нову версію програми користувач отримує нові параметри й можливості SDR пристрою.

Враховуючи величезні можливості, які закладені в SDR, очевидно, у найближчому майбутньому ця технологія займе домінуюче положення в техніці радіозв’язку.

Розум І.Ю. (НУОУ)
к.в.н. Микусь С.А. (НУОУ)

ОРГАНІЗАЦІЙНІ ТА ТЕХНІЧНІ ЗАХОДИ ІЗ ЗАХИСТУ СИСТЕМ ЗВ'ЯЗКУ ТАКТИЧНОГО РІВНЯ

Розвиток системи зв'язку (СЗ) тактичного рівня в найближчі роки пропонується в умовах вкрай обмежених можливостей щодо фінансування розробок і закупівель техніки. Тому пошук науково обґрунтованих варіантів її побудови, застосування існуючих комплексів зв'язку і АУВ є першочерговим завданням.

Виходячи з оцінки показників стійкості організацію управління елементами бойового порядку в ході ведення бойових дій в тактичній ланці управління необхідно здійснювати в русі або з коротких зупинок (50 – 75% часу на добу); використовувати переважно модернізовані багатофункціональні командно-штабні машини та машини бойового управління, як наймобільніші елементи вузли зв'язку пунктів управління (ВЗ ПУ) та проведенням заходів із захисту СЗ від впливу засобів електронного придушення.

Так, організаційними заходами із захисту СЗ ТР від радіорозвідки противника вважати: виявлення і знищення постів радіоперехоплення, аналізу та пеленгування противника; встановлення режимів роботи радіоелектронних засобів відповідно до обстановки та завдань, які вирішуються; обмеження допуску посадових осіб до використання радіозасобів; навчання командирів (начальників) методам керування підрозділами за допомогою формалізованих документів, короткими сигналами і командами з дотриманням вимог СУВ; скорочення до мінімуму часу роботи радіозасобів на випромінювання; заборона допуску до роботи відритим текстом або за відкритими радіоканалами фахівців із зв'язку з явно вираженими дефектами мови, характерним почерком під час роботи на ключі; ведення радіообміну без застосування позивних і видачі квитанцій; виділення для роботи в найбільш важливих радіомережах (радіонапрямках) висококваліфікованих радіоспеціалістів; організацію суворого контролю за дотриманням дисципліни зв'язку і правил СУВ; створення помилкових радіомереж (за планом старшого штабу) з імітацією роботи в них стосовно до реально діючих радіомереж і радіонапрямків; забезпечення зв'язку проводовими і рухомими засобами, коли це дозволяють умови обстановки (у районах зосередження, на марші, в обороні).

Технічними заходами щодо захисту СЗ ТР від радіорозвідки вважати: роботу радіозасобів з мінімально необхідною потужністю і застосуванню спрямованих антен; настроювання радіозасобів без виходу в ефір (на еквіваленти антен); широке застосування апаратури лінійного шифрування і датчиків коду Морзе, що виключають індивідуальний почерк радистів при роботі на радіостанціях; роботу радіо і радіорелейних станцій у режимі „чергового прийому" за відсутністю навантаження; своєчасне усунення характерних ознак у роботі радіозасобів, обумовлених несправністю радіопередавачів, ліній дистанційного керування ними та прикінцевої апаратури.

Завдяки складної радіоелектронної обстановки на ПУ та під час здійснення її маршу рекомендовано зменшити вплив взаємних перешкод та забезпечення їх електромагнітною сумісністю (ЕМС). Так, організаційними заходами із забезпечення ЕМС радіоелектронних засобів (РЕЗ) доречно вважати: постійне вивчення, оцінка та прогнозування радіоелектронної обстановки на ВЗ ПУ і в смузі дій підрозділів; раціональний розподіл та призначення частот з урахуванням ролі та місця застосування РЕЗ; територіальне розгалуження РЕЗ, насамперед на ВЗ ПУ; правильний вибір позицій РЕЗ, які дозволяють використовувати антени направлених якостей; ретельне планування роботи РЕЗ з часу та режимам; виявлення джерел взаємоперешкод та ліквідування їх дій, які заважають; контроль за дотриманням режимів роботи РЕЗ та їх характеристиками; розміщення усіх РЕЗ у районах з великою щільністю пунктів управління.

Так, організаційними заходами захисту від навмисних радіоперешкод вважати: навчання особового складу діям в умовах навмисних перешкод; маневр виділеними в інтересах зв'язку частотами; виявлення і порушення роботи засобів РЕБ противника; створення дублюючих, прихованих, резервних радіомереж і радіонапрямків з використанням обхідних каналів зв'язку; продовження роботи в радіомережі, яка піддається перешкодам за наявністю інших каналів зв'язку, за якими ведеться радіообмін; одночасна передача повідомлень у декількох радіомережах; організацію зв'язку із застосуванням різних засобів радіо, радіорелейного і проводового зв'язку, а також сигнальними і рухомими засобами (так зване комплексне резервування ліній зв'язку); застосування переприймальних і ретрансляційних пунктів, у тому числі розміщених на льотно-піднімальних засобах; вибір прихованих трас для радіорелейних ліній зв'язку з використанням захисних властивостей місцевості; заміна районів розміщення ВЗ ПУ під час закидання передавачів перешкод одноразового використання.

Технічними заходами захисту СЗ від РЕБ вважати: застосування спрямованих антен; орієнтування антен, де напрямок мінімального прийому діаграми спрямованості збігається з напрямком отримання перешкоди; використання елементів завадо-захищеності в апаратурі прийому (звуження смуги частот, зміна зрушення частот); зміна тону під час прийому в режимі слухового телеграфу; зміна видів роботи і методів модуляції (маніпуляції), відведення від перешкоди незначним зміщенням частоти прийому.

Крім того, забезпечення стійкості СЗ під час пошкодження об'єктів атомної енергетики дозволяє рекомендувати: комплексне застосування засобів зв'язку різноманітних діапазонів; забезпечення зв'язку в КХ діапазоні земною хвилею із застосуванням ретрансляційних пунктів (РТП), а іоносферною волною – з використанням стаціонарних радіо або РТП в обхід збурених областей іоносфери; використанням верхньої ділянки КХ діапазону для забезпечення зв'язку на велику відстань; чіткою роботою частотно-диспечерської служби; використанням повітряних ПУ та повітряних ретрансляторів.

Так, для підвищення надійності, складової стійкості, СЗ необхідна: розробка та втілення у війська засобів зв'язку з високими характеристиками надійності, з пристроями автоматичного контролю за станом блоків апаратури та каналами зв'язку; скороченням часу перебування засобів зв'язку у ремонтних органах; резервуванням блоків, апаратури, апаратних та станцій на лініях зв'язку; комплексним застосуванням на напрямках зв'язку різноманітних засобів, зменшенням часу переключення зв'язку з відмовою каналу (лінії) на справний; професійним вишколом підрозділів зв'язку; суворим дотриманням правил технічної експлуатації засобів зв'язку.

Таким чином, організаційно-технічними заходами із захисту систем зв'язку тактичного рівня від впливу засобів електронного придушення, вважати: захист від радіорозвідки противника; виявлення та ліквідування засобів радіорозвідки та електронного придушення противника або придушення завадами ліній управління ними; створення прихованих та хибних вузлів і ліній зв'язку; застосування на напрямках засобів зв'язку різноманітних діапазонів; скорочення інтервалів на радіо, радіорелейних та тропосферних лініях; застосуванням адаптивних режимів роботи на важливих напрямках зв'язку; застосуванням завадозахищених методів ведення радіозв'язку; застосуванням завадозахищених методів модуляції; перехід на інші частоти з одночасною імітацією роботи на частоті яка придушується; маневр випромінюючою потужністю, режими робот з антенами; підготовка особового складу до забезпечення зв'язком в умовах сильних радіозавад.

Попереду уніфікація та мінімізація засобів та комплексів зв'язку з метою забезпечення необхідної гнучкості, яка направлена на: скорочення часу на виконання підрозділами зв'язку поставлених завдань; удосконаленням організаційно-технічної структури системи зв'язку та її елементів; підвищення оперативності роботи органів управління зв'язком.

к.т.н. Ролік О.І. (НТУУ „КПІ”)
Тимофєєва Ю.С. (НТУУ „КПІ”)

МЕТОД ФОРМУВАННЯ МАТРИЦІ НЕСПРАВНІСТЬ-СИМПТОМ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В наш час організації та підприємства для управління бізнес-процесами та процесами діяльності широко використовують автоматизовані системи на основі інформаційних та телекомунікаційних технологій (ІТ). Для ефективного управління ІТ-системою (ІТС) та раціонального використання ІТ-ресурсів розробляються та впроваджуються різноманітні системи управління ІТ-інфраструктурою [1].

Система управління ІТС повинна забезпечувати ефективне функціонування інформаційно-телекомунікаційної системи, моніторинг та аналіз станів її складових, ефективний перерозподіл ресурсів в разі виникнення несправностей, діагностування, локалізацію та швидке усунення несправностей і т.д. Підсистема управління усуненням несправностей виконує одні з найважливіших функцій, оскільки найменше порушення функціонування ІТС може спричинити простої в роботі організації або погіршення якості послуг, які надаються клієнтам, та викликати значні економічні витрати.

В статті [2] запропоновано алгоритм локалізації несправностей, який поєднує метод пасивного моніторингу, тобто збору симптомів, та тестових перевірок. На основі симптомів, що спостерігаються, виноситься рішення щодо наявності можливих несправностей. З цією метою для кожного з N класів, на які розбивається система, використовується матриця $Q_n = \left\| q_{n,ij}\left(c_{n,j} \mid f_{n,i}\right) \right\|$ несправність-симптом, елемент $q_{n,ij}\left(c_{n,j} \mid f_{n,i}\right)$ якої приймає значення:

$$q_{n,ij}\left(c_{n,j} \mid f_{n,i}\right) = \begin{cases} 1, \text{ якщо } j\text{-й симптом виникає} \\ \quad \text{при наявності } i\text{-ї несправності;} \\ 0, \text{ в іншому випадку.} \end{cases}$$

Формування даної матриці пропонується здійснювати наступним чином. Спочатку до матриці додаються усі симптоми, що породжуються усіма можливими несправностями. Далі проводиться мінімізація даної матриці з метою знаходження мінімальної підмножини симптомів, якої було б достатньо для вирізнення усіх можливих несправностей. Кожній несправності відповідає двійковий вектор, який відображає усі симптоми, що викликаються даною несправністю. Обирається пара несправностей з найменшою кодовою відстанню Хеммінга між відповідними векторам. Далі з усієї множини симптомів обирається той, що збільшує цю кодову відстань, саме він і залишається в матриці.

Таким чином, даний метод дозволяє зменшити розмір матриці Q_n, а значить, скоротити час пошуку можливих несправностей. Результативність мінімізації буде залежати від відсотка невзаємопов’язаних несправностей в системі.

ЛІТЕРАТУРА

1. *Теленик С.Ф.* Система управління інформаційно-телекомунікаційною системою корпоративної АСУ/ С.Ф. Теленик, О.І. Ролік, М.М. Букасов, Р.Л. Соколовський // Вісник НТУУ „КПІ”. Інформатика, управління та обчислювальна техніка. – 2006. –№ 45. – С. 112 –126.

2. *Ролик А.И.* Управление устранением неисправностей в ИТ-системах / А.И. Ролик, Ю.С. Тимофеева, Н.И. Турский // Вісник НТУУ „КПІ”. Інформатика, управління та обчислювальна техніка. – К.: „ВЕК+”, – 2008. – № 49. – С. 94 – 107.

Романенко В.П. (ІСЗЗІ НТУУ ,,КПІ”)

МОДЕЛЮВАННЯ ПРОЦЕСУ ГРУПОВОГО ПОШУКУ ДЕФЕКТІВ ПРИ РЕМОНТІ ВІЙСЬКОВОЇ ТЕХНІКИ ЗВ'ЯЗКУ

У практиці військового ремонту знаходять застосовування всі види групового пошуку: незалежний – при ремонті різних типів військової техніки зв’язку (ВТЗ) в універсальних апаратних технічного забезпечення (АТЗ), спільний – при ремонті об’єктів великої розмірності з просторово рознесеними елементами, зонний – при ремонті однотипної ВТЗ модульної конструкції в спеціалізованих АТЗ. Результати моделювання дозволяють кількісно оцінити показники якості діагностичного забезпечення різних видів групового пошуку і залежно від постановки завдання оптимізувати число ремонтників і параметри умовних алгоритмів діагностування (УАД).

Завдання при модернізації або створенні ремонтного органу зводиться до досягнення його максимальної пропускної спроможності при заданих обмеженнях на параметри в допустимих межах. Пропускна спроможність ремонтного органу визначається головним чином середнім часом відновлення ВТЗ $T_в$, яке, у свою чергу, залежить від часу діагностування об’єкту. Відомо, що до 60 – 80% $T_в$ витрачається на пошук дефектів, а решта 20 – 40% на усунення несправностей, перевірку працездатності на всіх режимах і, при необхідності, регулювання.

Отже, резерв підвищення ефективності роботи ремонтного органу полягає у вдосконаленні ремонтопридатності і діагностичного забезпечення ВТЗ на етапах її проектування і експлуатації [1 – 2]. Таким чином, виникає завдання здобуття в явному вигляді, дослідження і мінімізації функції $T_в$ від керованих змінних при заданих обмеженнях, які визначаються керівними документами, організаційно-штатною структурою ремонтного органу, реалізацією ремонту ВТЗ агрегатним методом, технологічним обладнанням спеціалізованих робочих місць АТЗ і пунктів технічного обслуговування та ремонту (ПТОР).

Залежно від умов функціонування ремонтного органу його цільова функція полягає в мирний час в забезпеченні заданого допустимого значення середнього часу відновлення ВТЗ $T_{во}$ при мінімальній вартості ремонту або у військовий час в мінімізації середнього часу відновлення $T_в$ при обмеженнях на ресурси.

З врахуванням приведених міркувань загальна графоаналітична модель процесу групового пошуку дефектів (незалежного, спільного, зонного) є сукупністю множини алгоритмів діагностування і функціональних залежностей їх параметрів та обмежень від керованих змінних, що дозволяє кількісно оцінити і максимально підвищити виробничі можливості військових ремонтних органів в заданих умовах функціонування.

Подальше узагальнення отриманих функціональних залежностей дозволить визначити в явному вигляді аналітичні вирази для кількісної оцінки показників якості діагностичного забезпечення групового пошуку дефектів будь-якого вигляду.

В доповіді узагальнюються отримані результати моделювання процесу пошуку дефектів, які доцільно використовувати при розробці діагностичного забезпечення ремонту існуючих та перспективних зразків ВТЗ в польових умовах екіпажами АТЗ.

ЛІТЕРАТУРА

1. *Давыдов П.С.* Техническая диагностика радиоэлектронных устройств и систем. – М.: Радио и связь, 1988. – 256 с.

2. *Розробка пропозицій* щодо удосконалення системи технічного обслуговування і ремонту техніки зв’язку і АСУ: Звіт про НДР „Дністер” / в/ч А-0375. – К., 2000. – 151 с.

д.т.н. Романюк В.А. (ВІТІ НТУУ„КПІ”)
Стемпковська Я.А. (ВІТІ НТУУ„КПІ”)

МЕТОДИ ПОКРИТТЯ ПОВЕРХНІ СЕНСОРНИМИ ВУЗЛАМИ

Безпровідні сенсорні мережі (БСМ) або *Wireless Sensor Network* (WSN) – розподілені мережі, що складаються з сенсорних вузлів, з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних.

Сенсорні вузли (СВ) є платформою, яка об’єднує можливості сенсорів (зовнішніх датчиків, які реєструють сукупність параметрів, – акустичних, вібраційних, радіаційних, хімічних, біологічних і т.п.) з мікрокомп’ютерами, об’єднаними в бездротову мережу.

Серед існуючих методів покриття поверхні території СВ, які використовують при детермінованому або випадковому розміщенні сенсорних вузлів в безпровідних сенсорних мережах, найбільш поширені – є *тріангуляційні методи* та *методи послідовного конструювання.* Виникає необхідність їх аналізу для подальшої розробки методик покриття території безпровідних сенсорних мереж за їх якісними характеристиками.

Тріангуляційні методи використовують, як у випадковому так і у детермінованому випадках розташування БСМ.

Процедура тріангуляції – передбачає побудову планарного графа, який отримують шляхом з’єднання сенсорів, з обов’язковою умовою відсутності можливості іншого з’єднання без порушення планарності (тобто без перетину з’єднань). Межа тріангуляції сенсорної мережі є опуклою оболонкою зони покриття, тому доцільно застосовувати: *Тріангуляцію Делоне, Метод Рапперта, Діаграма Вороного.* Тріангуляція дає кращий варіант апроксимації при максимальному розмірі мінімального кута у вихідних трикутниках.

Методи послідовного конструювання використовують у детермінованому випадку використовують кругові та кутові моделі, які найшли широке застосування у методах послідовного конструювання. Їх застосовують для пошуку оптимального розміщення СВ у багатокутниках з перешкодами. Вони дозволяють моделювати процеси територіального розподілу об’єктів в областях з перешкодами. Задача розміщення сенсорів зводиться до задачі покриття кругами, які є областю локації сенсора. Ці методи передбачають застосування:

– *блокового алгоритму*, який заснований на блоковій технології, раніше був використаний для вирішення завдань упаковки. Він дозволяє знаходити опорні, близькі до оптимальних, розв’язки завдання, щодо пошуку допустимого покриття.

– *гексагонального алгоритму*, який заснований на використанні гексагональних решіток, і, в більшості випадків, перевершує за ефективністю блоковий алгоритм, а також може використовуватися як декодер в багатопрохідних евристиках з метою поліпшення значення цільової функції.

Таким чином аналіз відповідних методів дозволяє провести їх класифікацію та розробити методику розгортання БСМ за її якісними характеристиками для забезпечення оптимального покриття території та виконання основних завдань БСМ: збору, передачі та збереження інформації.

ЛІТЕРАТУРА

1. *Міночкін А.І, Романюк В.А., Жук О.В.* Перспективи розвитку тактичних сенсорних мереж// Збірник наукових праць № 4. – К.: ВІТІ НТУУ „КПІ”. – 2007. – С. 112 – 119.

2. *Миночкин А.И., Романюк В.А*. Методология оперативного управления мобильными радиосетями // Зв‘язок. – 2005. – № 2. – С. 53 – 58.

3. *N. Bulusu, J. Heidemann, D. Estrin*, „GPS-less low cost outdoor localization for very small devices”, Technical report 00-729, Computer science department, University of Southern California, Apr. 2000.

Руденко С.Є. (ВІТІ НТУУ „КПІ”)

ПЕРСПЕКТИВА ВПРОВАДЖЕННЯ В ТЕХНОЛОГІЇ LTE В УКРАЇНІ

3GPP Long Term Evolution (LTE) – технологія побудови мереж безпровідного зв’язку на базі IP-технологій. Проект 3GPP являється стандартом по вдосконаленню технологій CDMA, UMTS, що дозволяє підвищувати ефективність, знизити затримки, розширити послуги, а також інтегруватися з вже існуючими протоколами.

Впровадження LTE забезпечить можливість створення високошвидкісних систем мобільного зв’язку, оптимізованих для пакетної передачі даних зі швидкістю 300 Мбіт/с на прийом і до 75 Мбіт/с на передачу. LTE краще використовує частотний спектр, відрізняється підвищеною ємністю і меншим часом затримки.

Радіус дії базової станції LTE може бути різним, залежно від потужності і частоти. В оптимальному варіанті – 5 км, при необхідності може досягати до 100 км при достатньому піднятті антени. Дзвінок чи сеанс передачі даних, ініційований в зоні покриття LTE, технічно може бути переданий без розриву в мережу 3G (W-CDMA), CDMA2000 чи в GSM/GPRS/EDGE.

Впровадження технології LTE дозволяє операторам зменшити капітальні і операційні витрати, загальну вартість володіння мережею, розширити свої можливості в області конвергенції послуг і технологій, підвищити доходи від надання послуг передачі даних. Мережа підтримує MBSFN (Multicast Broadcast Single Frequency Network), що дозволяє впроваджувати такі послуги, як мобільне ТВ як альтернативу DVB-H.

Можливості, які надає LTE:

– Висока пропускна спроможність мережі;

– Висока інтерактивність;

– Можливість передачі голосу по IP/IMS;

– Більш висока якість обслуговування;

– Більша кількість каналів мобільного ТВ і вища якість зображення;

– Гнучка мережа доступа.

Українські оператори („Київстар” і МТС) готові розвивати 4G-зв’язок на частотах покоління 3G. Частоти, на яких може будуватися LTE (0,7 – 0,8; 1,7 – 2,1; 2,6 ГГц), на сьогодні або зайняті, або їх використання обмежене законом. Прийняття закону про технологічну нейтральність (право оператора використовувати вже наявні в його розпорядженні частоти під нові технології) може вирішити це питання. Так, як радіочастотний ресурс розподіляється невеликими смугами частот по 1 – 3 МГц, то для розгортання повноцінних мереж GSM достатню було сумарної смуги частот 9,6 МГц. Проте для побудови мереж наступних поколінь такої смуги не достатньо, оскільки для 4G необхідно не менше 30 МГц, для високошвидкісної мережі LTE – 60 МГц, причому окрема смуга не повинна бути менше ніж 10 МГц. Крім того, якщо під LTE використати 1800-й діапазон, самі оператори визнають, що це призведе до погіршення якості GSM-зв’язку. Технології 2G/GSM ще не відпрацювали на повну, вони мають потенціал і будуть деякий час використовуватися. Потрібно також переорієнтувати абонентів на нову технологію. По даних он-лайн магазинів, близько 60 % телефонів, що продаються в Україні, можуть працювати в 3G (GPRS), а 40 % – в 2G-мережах.

Таким чином, технологія LTE може бути не впроваджена повністю, якщо це не буде економічно виправданим, або з’явиться більш цікава технологія в плані надання мобільного широкосмугового доступу. Вартість мереженого і абонентського обладнання, а також професійні послуги по будівництву мереж на сьогодні можливо не будуть виправдані при середньо українському доході від абонента. Це може вплинути на кінцеве рішення операторів по впровадженню технології. Компанії, які надають дані послуги, готові розпочати поставки обладнання в Україну, яке підтримує стандарт LTE, як тільки в нашій країні з’явиться відповідна інфраструктура.

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

АЛГОРИТМ АДАПТИВНОЇ ОБРОБКИ ІНФОРМАЦІЇ ПРО ДИНАМІЧНІ ОБ'ЄКТИ ПРОТИВНИКА В ПІДСИСТЕМАХ ЄДИНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ЗБРОЙНИМИ СИЛАМИ УКРАЇНИ

Точність оцінки координат і параметрів траєкторії динамічних об'єктів в процесі їх супроводження алгоритмом (фільтром) залежить від багатьох факторів, основними із яких є: помилки вимірювання координат місцезнаходження динамічних об'єктів в момент часу t_i; достатність статистики, тобто кількість вимірювань (кількість оглядів зони відповідальності джерела), які використовуються при обчисленнях; динамічні помилки, які обумовлені невідповідністю вибраної гіпотези руху динамічних об'єктів реальній траєкторії руху.

Відомі алгоритми супроводження динамічних об'єктів не задовольняють вимог інформаційного забезпечення по точності при автоматизації процесів збору, аналізу, обробки інформації та усвідомлення завдання в підсистемах ЄАСУ ЗС України.

Для підвищення точності оцінки координат і параметрів траєкторії руху динамічних об'єктів противника за умов їх маневру за швидкістю і напрямком пропонується для реалізації схема адаптивного алгоритму обробки інформації про динамічні об'єкти противника. В схемі пропонується використовувати два адаптивних фільтра послідовного згладжування Φ_1 і Φ_2, на вхід яких одночасно в кожному періоді обробки подається цифрова координатна інформація місцеположення динамічних об'єктів (обмірювані координати) і екстрапольовані координати. Адаптація (підстроювання) фільтрів здійснюється в кожному періоді обробки шляхом аналізу величин неузгодженості $(\Delta n_1, \Delta n_2)$ між координатами місцеположення об'єкту і їх екстрапольованим положенням і вибору, відповідних даним Δn_1 и Δn_2, коефіцієнтів згладжування.

В якості фільтру Φ_1 пропонується фільтр, налаштований на гіпотезу рівномірного і прямолінійного руху, а в якості другого фільтру Φ_2 пропонується фільтр, налаштований на гіпотезу руху динамічного об'єкту з постійною кутовою швидкістю.

Дані з фільтрів Φ_1 і Φ_2 поступають на вхід пристрою виявляча маневру . Основне призначення виявляча маневру - визначити характер руху і на підставі цього ухвалити рішення про те, які результати згладжування (Φ_1 або Φ_2) вважати координатами і параметрами динамічного об'єкту в даному періоді обробки. Рішення ухвалюється по величині згладженого значення. З виходу виявляча маневру результати згладжування і екстраполяції фільтру Φ_1 або Φ_2 записуються в базу даних, в якій відведений свій сектор для кожного датчика (джерела). Згладжені значення прямокутних координат датчика (джерела) перераховуються в систему координат пункту управління і в екстрапольовані полярні значення координат на наступний період обробки. Дані, записані у формулярі динамічного об'єкту, оновлюються на кожному черговому огляді зони відповідальності датчика (джерела).

Інформація про динамічного об'єкту, що формується у базі даних використовується для рішення функціональних задач підсистем ЄАСУ.

Адаптація алгоритму супроводження динамічного об'єкту реалізується як шляхом зміни коефіцієнтів згладжування фільтрів, так і комутацією результатів згладжування фільтрів Ф1 и Ф2 виявлячем маневру , що компенсує в алгоритмі вплив помилок на точність супроводження динамічного об'єкту.

Таким чином, адаптація алгоритму супроводження динамічного об'єкту реалізується як шляхом зміни коефіцієнтів згладжування фільтрів, так і комутацією результатів згладжування фільтрів Ф1 и Ф2 виявлячем маневру , що компенсує в алгоритмі вплив помилок на точність супроводження динамічного об'єкту.

Сакевич С. О. (ВІТІ НТУУ „КПІ”)

ТЕХНОЛОГІЯ БЕЗПРОВІДНОГО ДОСТУПУ WiMAX: СТАН І ПЕРСПЕКТИВИ

На даний час інфокомунікаційними послугами, які надаються в мережах зв’язку нового покоління, користується більш ніж 860 млн абонентів більш ніж у 200 країнах світу, при чому їх число збільшується на 15 млн кожного місяця. Відбувається перехід до сучасних технологій 3-го покоління – HSDPA, HSUPA, HSPA+ та 1xEV-DO, котрі дозволяють у декілька раз підвищити швидкість передачі даних. Тому стратегія розвитку безпровідного зв’язку з точки зору оператора повинна бути комерційно ефективною, яка дозволяє знижувати капітальні та операційні затрати при створенні мереж на нових технологіях.

Згідно тверджень зарубіжних експертів мобільний WiMAX (IEEE 802.16e) буде випереджати технологію LTE. Це пояснюється тим, що, по-перше, мобільний WiMAX, набагато раніше став об’єктом комерційної експлуатації, і це при тому, що об’єм інвестицій для переходу уже існуючих 3G-мереж в мережі LTE можна порівняти із затратами на розгортання WiMAX-мереж. Фактор часу стає головним при виборі технології 4G. І, по-друге, технології WiMAX та LTE будуть мати різне застосування. Більшість операторів схильні розвивати WiMAX на мережах фіксованого телефонного зв’язку в якості розширення технології DSL. Що ж стосується показників розвитку мереж WiMAX , то згідно даних WiMAX Forum, станом на вересень 2010 року було запущено в комерційну експлуатацію 625 мереж WiMAX у 188 країнах світу. Це значно вище показників минулого року(в квітні 2009 було запущено лише 470 мереж у 130 країнах). Також було зазначено, що вже початі досліди над новими послугами. Наприклад, у Тайвані була запущена зона на базі технології WiMAX для розповсюдження спортивних новин і даних про останні події в режимі реального часу. Жителям певних міст Китаю також надається безкоштовний доступ до Інтернету в метрополітені. В країнах Азіатсько-Тихоокеанського регіону уже забезпечується безшовний роумінг між мережами WiMAX та Wi-Fi.

На думку представників WiMAX Forum масштабного розгортання мереж LTE не буде до 2012 року, так як оператори мобільного зв’язку уже вклали значні кошти та засоби у будівництво мереж 3G. Саме чому і актуально порівнювати характеристики мереж 3G і WiMAX, але при цьому мережі WiMAX виграють завдяки швидкості надання послуг(10 Мбіт/с до абонента і 3 Мбіт/с від абонента проти 2 Мбіт/ та 1 Мбіт/с у 3G відповідно).

Технологію WiMAX можна назвати універсальною, яка підходить для вирішення багатьох задач. Підтвердження цьому є різноманіття операторів мереж WiMAX, в числі яких нові оператори, оператори кабельного ТВ, комунальні і промислові підприємства, оператори зв’язку і навіть оператори мереж GSM (наприклад оператори Orange Botswana і Mobilink у Пакистані використовують її для надання абонентам більш високі швидкості передачі).

За прогнозами консалтингової компанії Juniper Research, кількість абонентів у мережах WiMAX стандарту 802.16e до 2014 року досягне 50 млн.

Для захисту своїх позицій оператори WiMAX планують перейти із стандарту IEEE 802.16e до IEEE 802.16m (WiMAX 2), який по основних характеристиках ідентичний стандарту LTE. На виставці CEATEC IT, яка проходила в Японії наприкінці літа 2010 року, компанія Samsung провела першу публічну демонстрацію WiMAX 2, під час якої була зареєстрована швидкість передачі даних 330 Мбіт/с і велася пряма трансляція 3D HD-відео по безпровідній мережі. WiMAX 2 підтримує альянс комп’ютерних фірм, в числі яких Intel, Motorola і Samsung. Інститут повинен затвердити 802.16m в листопаді 2010 року, а на протязі 2011 – провести сертифікацію пристроїв.

Таким чином, WiMAX – нова перспективна ступінь розвитку бездротових технологій, яка гарантує простоту широкосмугового підключення і універсальність використання. WiMAX є альтернативою технологіям xDSL, привабливою для провайдерів завдяки можливості відносно простого, оперативного та гнучкого збільшення ємності мереж.

к.т.н. Сальник Ю.П. (НЦСВ АСВ)

ВДОСКОНАЛЕННЯ РОЗВІДУВАЛЬНОГО ЗАБЕЗПЕЧЕННЯ БОЙОВИХ ДІЙ СУХОПУТНИХ ВІЙСЬК

Досвід збройних конфліктів останнього десятиріччя свідчить про суттєве зростання частки завдань розвідувального забезпечення при веденні бойових дій.

Аналіз стану і можливостей розвідувальної техніки та озброєння, що є на озброєнні військових частин та підрозділів розвідки Сухопутних військ Збройних Сил України показує, що наявний парк засобів розвідки характеризується надмірною кількістю зразків застарілої техніки, яка вже не в змозі у повному обсязі забезпечити виконання завдань розвідки в сучасних умовах. У той же час, аналіз інформації про розвиток засобів ведення розвідки провідних країн світу свідчить про намагання останніх забезпечити постійну модернізацію існуючого парку техніки розвідки та створення нових зразків, які враховують останні досягнення науки і техніки у військовій сфері. Спостерігається чітка тенденція до створення комплексних засобів та техніки розвідки, збільшення їх кількості у тактичному ланцюзі із поступовим включенням кожного зразка ОВТ у систему здобування розвідувальної інформації.

Наприклад, бойова розвідувальна машина (БРМ), як основний засіб ведення військової розвідки, продовжує відігравати головну роль при здобуванні розвідувальної інформації у розвинених країнах. Більше того, в останні роки значно збільшилось коло завдань, що потребують вирішення. Класична схема компоновки розвідувального модуля БРМ засобами оптичної, оптико-електронної, радіотехнічної та радіоелектронної розвідки суто базового (на шасі) розташування доповнюється засобами повітряної розвідки (БпАК, зонди).

Однак, поряд з технічним переоснащенням, необхідне проведення організаційних заходів щодо переходу до ефективної системи розвідки (система розвідки включає розвідувальні органи, сили та засоби розвідки). Таким чином розвідувальне забезпечення є комплекс заходів, що виконуються системою розвідки з метою збору, обробки та аналізу розвідувальної інформації, розподілу розвідувальних даних для виконання конкретного бойового завдання. Мета розвідки може бути досягнута лише за умов дотримання всіх вимог до ведення розвідки за рахунок концентрації зусиль органів управління, наявних сил і засобів розвідки.

Розвідка як складова частина всебічного забезпечення, є основною складовою діяльності командирів і штабів усіх рівнів. Тому можливим шляхом вдосконалення системи розвідки є її розгляд як складової системи підтримки прийняття рішень (СППР) командиром. Такий підхід дозволить забезпечити оперативність обміну інформацією, інтерактивність у роботі із утримувачами розвідувальних відомостей, автоматизувати процеси розподілу, врахування, аналізу інформації, планування діяльності і таке інше.

До завдань такої підсистеми розвідки СППР можна віднести наступні:

1. Забезпечення ситуаційного розуміння обстановки на полі бою.

2. Забезпечення оперативності застосування засобів ураження (розвідки) у всьому районі впливу (ведення розвідки).

3. Безперервне ведення розвідки за будь-яких умов обстановки.

4. Цілеспрямованість ведення розвідки на отримання конкретного результату.

Таким чином, поєднання поступового технічного переоснащення частин та підрозділів розвідки Сухопутних військ Збройних Сил України із постійним проведенням організаційних заходів із переходу до ефективної системи розвідки, уточнення об’єму і змісту завдань є єдиним шляхом забезпечення виконання завдань розвідки в сучасних умовах в повному обсязі.

к.т.н. Самойлов І.В. (ВІТІ НТУУ „КПІ”)
Кокотова М.О. (НТУУ „КПІ”)

АНАЛІЗ ВИМОГ ДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОГНІТИВНИХ РАДІОСИСТЕМ

Швидке зростання потреб економіки у радіочастотному спектрі та обмеженість радіочастотного ресурсу потребує розробки нових підходів для їх використання. При цьому основними вимогами до таких підходів є гнучкість використання та динамічний доступ до радіочастотного спектру [1].

Когнітивні радіосистеми є одним з нових напрямків в області безпроводових технологій, який ґрунтується на використанні досягнень в області штучного інтелекту і динамічного управління використанням радіочастотного ресурсу (частотного спектру, часових та енергетичних характеристик). Основним завданням когнітивних радіосистем є забезпечення високої надійності зв'язку, ефективності використання радіочастотного ресурсу та забезпечення необхідного рівня інформаційної безпеки [2].

В доповіді розглянуті базові для когнітивних радіосистем поняття: цикл пізнання, когнітивне середовище, реконфігуруєма платформа. Розкриваються загальні принципи роботи когнітивних радіосистем, наводиться їх узагальнена схема. Надана класифікація когнітивних радіосистем за наступними ознаками:

за методами пізнання;

за функціональними параметрами;

за типом основних каналів управління (обміну інформацією);

за рівнем використання технологій штучного інтелекту.

З врахуванням здатності когнітивних радіосистем до самоорганізації, використання динамічного доступу до спектру, можливості впливати на експлуатаційне середовище, запропоновано їх уточнене визначення [3].

Наведені особливості функціонування когнітивних радіосистем як систем, що використовують штучний інтелект. Розглянуті поняття багатоагентної когнітивної радіосистеми та агента когнітивної радіосистеми. Розглянуті фактори, які підвищують вимоги до інформаційної безпеки когнітивних радіосистем.

На прикладі перспективного стандарту IEEE 802.22 розглянуті особливості технічної реалізації когнітивної радіосистеми [4, 5]. Стандарт IEEE 802.22 є першим стандартом для радіоінтерфейсу, який розроблений на принципах когнітивного радіо. Згідно з цим стандартом для роботи використовуються незайняті ділянки радіочастотного спектру в діапазоні частот відведеному для телевізійного мовлення. Розглянуті можливі загрози та вразливості для систем радіозв’язку, які побудовані за цім стандартом.

ЛІТЕРАТУРА

1. *J. Mitola III and G. Q. Maguire Jr.*, “Cognitive Radio: Making Software Radios More Personal,” IEEE Pers. Commun., vol. 6, no. 4, Aug. 1999, pp. 13 – 18.

2. *Mitola, J*. Cognitive radio: An integrated agent architecture for software defined radio. Ph.D. Dissertation, KTH, 2000.

3. *Гарбарчук В., Зинович З., Свиц А*. Кибернетический подход к проектированию систем защиты инфонрмации.- Киев, 2003, 659 с.

4. www. ieee802.org/22/

5. *Stevenson, C.; Chouinard, G.; Zhongding Lei; Wendong Hu; Shellhammer, S.; Caldwell, W.*; IEEE 802.22: The first cognitive radio wireless regional area network standard. Communications Magazine, IEEE. January 2009. Volume: 47, p. 130 – 138

к.т.н. Самойлов І.В. (ВІТІ НТУУ ,,КПІ”)
к.т.н. Толюпа С.В. (ДУІКТ)

ВИКОРИСТАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ТА НЕЙРОННОЇ МЕРЕЖІ ДЛЯ ВИДОБУВАННЯ НЕЧІТКИХ ВІДНОШЕНЬ З ЕКСПЕРИМЕНТАЛЬНИХ ДАНИХ

В умовах невизначеності для моделювання причинно-наслідкових зв’язків в системах діагностики зручно використовувати нечіткі відношення і композиційне правило виведення Заде [1]. Нечіткі відношення можуть бути видобуті з експериментальних даних. В цьому випадку вони інтерпретуються як ваги нечітких правил ЯКЩО „причини” ТО „наслідки”. Для видобування цих правил із даних традиційно використовуються нейронні мережі [2] або генетичні алгоритми [3]. Комбінація цих методів обумовила появу нейро-генетичних моделей видобування знань [4].

Недоліком нейро-мережевого підходу є те, що початкова нейро-нечітка мережа містить в собі всі можливі правила. Така мережа містить повнозв’язні шари нейронів, тобто структура моделі не є оптимальною.

При цьому конфігурація мережі вимагає, щоб число нечітких термів вхідних і вихідних змінних було строго фіксованим, що обмежує точність нечіткої моделі. Також до недоліків нейро-мережевого підходу слід додати можливість влучення в локальний екстремум. Принциповою перевагою нейронних мереж є здатність адаптивно навчатись по мірі появи нових даних. Перевагою генетичних алгоритмів є те, що вони дозволяють видобувати модель заданої структури. Недоліком генетичного алгоритму є те, що він погано пристосований для врахування нових даних, що надходять в навчальну вибірку.

Пропонується сумісне використання генетичного алгоритму та нейронної мережі для видобування нечітких правил ЯКЩО-ТО. Суть цього підходу полягає в тому, що генетичний алгоритм використовується для пошуку розв’язку в режимі off-line, а нейронна мережа використовується для уточнення розв’язку в режимі on-line.

При цьому, на відміну від [5], вектор керувальних змінних на етапі генетичного алгоритму відрізняється від вектора розв’язку на етапі нейронної настройки. На етапі генетичної оптимізації розв’язок має спрощену структуру і дозволяє грубо оцінити параметри функцій належності і ваг нечітких правил. Нейронна мережа використовується для уточнення розв’язку і його адаптивної корекції по мірі надходження нових експериментальних даних.

Крім того пропонується використовувати нейро-мережевий підхід для адаптації параметрів моделі до варіації значень вхідних даних, що зумовлені неточністю результатів вимірювань.

ЛІТЕРАТУРА

1. *Заде Л.* Понятие лингвистической переменной и её применение к принятию приближенных решений. – М.: Мир, 1976. – 167 с.

2. *Nauck D., Klawonn F., Kruse R.* Foundation of Neuro-Fuzzy Systems. – John Willey & Sons. – 1997. – 305 p.

3. *Ротштейн А. П.* Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. – Винница: УНІВЕРСУМ-Вінниця, 1999. – 320 с.

4. *Zhong N., Dong J., Liu Ch., Ohsuga S.* A hybrid model for rule discovery in data // Knowledge Based Systems. – 2001. – Vol. 14(7). – Pp. 397 – 412.

5. *Oh S. K., Pedricz W., Park H. S.* Rule-based multi-FNN identification with the aid of evolutionary fuzzy granulation // Knowledge Based Systems. – 2004. – Vol. 17(1). – Pp. 1 – 13.

д.т.н. Самохвалов Ю.Я. (ВІТІ НТУУ „КПІ”)
Коваленко І.М. (ВІТІ НТУУ „КПІ”)
Бурба О.І. (в/ч А1906)

МЕТОДИКА КОМПЛЕКСНОГО ФОРМУВАННЯ ВИМОГ ДО АВТОМАТИЗОВАНИХ СИСТЕМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В теперішній час створення автоматизованих систем спеціального призначення (АС СП) у Збройних Силах України здійснюється переважно в рамках адаптивного проектування [1]. Основним методом цього підходу є макетування системи. Згідно нього спочатку за результатами обстеження об’єкту автоматизації (ОА) формуються тільки загальні вимоги до АС СП. Відповідно до цих вимог будується макет системи на основі, як правило, мережевої технології. Потім за результатами дослідної експлуатації макету вимоги до системи уточнюються та доповнюються, а макет удосконалюється, доки його характеристики не будуть задовольняти вимогам замовника. При цьому, кількість ітерацій, а отже тривалість створення АС СП і її вартість, безпосередньо залежать від повноти та обґрунтованості початкових вимог до системи.

Аналіз існуючого методичного апарату формування вимог до АС СП показав, що на теперішній час він налічує тільки часткові методики [2]. Це, в свою чергу, не забезпечує достатню повноту і обґрунтованість вимог, що негативно впливає на процес побудови АС.

Таким чином, наведені положення ставлять у розряд актуальних завдання розробки методичного апарату комплексного формування повних та обґрунтованих вимог до АС СП, що визначає мету і основний зміст доповіді.

Згідно агрегативно-декомпозиційного підходу вимоги до АС СП можна розбити на два класи: тактико-технічні і техніко-економічні. Основним джерелом інформації для формування цих вимог є результати обстеження ОА, які включають відомості про його організаційну, функціональну та інформаційну структуру, оперативно-тактичні вимоги до вирішення завдань та їх характеристики.

Крім цих даних для забезпечення повноти та обґрунтованості вимог до АС СП необхідно в загальному вигляді представляти структуру, принципи побудови та функціонування, сукупність конструктивно-технологічних та технічних характеристик системи, тобто уявляти її обрис.

В доповіді визначена методика формування вимог до АС СП, згідно якої за результатами обстеження ОА будуються його функціонально-інформаційна модель та інформаційно-технологічна модель АС СП. Функціонально-інформаційна модель, яка будується на основі методології IDEF, відображає організаційно-функціональну ієрархічну структуру ОА та інформаційні зв’язки між його елементами. А інформаційно-технологічна модель є обрисом системи, який являє собою сукупність інформаційних технологій автоматизованої обробки інформації при вирішенні завдань в підрозділах ОА. Розроблені моделі дають можливість сформувати повні та обґрунтовані вимоги до АС СП.

Розглянута в доповіді методика комплексного формування вимог на основі побудованих моделей дає змогу структурувати цей процес та обґрунтувати перелік необхідних та достатніх вихідних даних, що забезпечує комплексне формування повних та обґрунтованих вимог до АС СП.

ЛІТЕРАТУРА

1. *Ситник В.Ф.* Системи підтримки прийняття рішень / В.Ф. Ситник, О.С. Олексюк, В.М. Гужва, С.П. Ріппа, В.М. Олейко. – К.: Техніка, 1995. – 162 с.

2. *Гриб Д.А.* Методологічний підхід до формування технічного обрису перспективних зразків озброєння та військової техніки / Д.А. Гриб, Б.О. Демідов, М.В. Науменко // Наука і оборона. – 2009. – № 4. – С. 30 – 34.

Сєткін В.В. (ЦНДІ ОВТ ЗС України)
Гамалій Н.В. (ЦНДІ ОВТ ЗС України)

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Сучасний розвиток інформаційних технологій накладає відбиток на вигляд, склад та порядок функціонування сучасних командних пунктів та пунктів управління усіх ланок. Засоби автоматизації в системі бойового управління все тісніше інтегруються із засобами зв'язку, а з переходом до цифрового зв'язку найближчим часом засоби зв'язку та автоматизації будуть єдиним цілим.

Зрозуміло, що інформація, яка циркулює в органах управління всіх ланок, має відповідний гриф секретності, а її обробка за допомогою автоматизованих систем (АС) висуває до них вимоги щодо захисту інформації від витоку технічними каналами.

З 70-х років минулого століття до цього часу для вирішення зазначеної проблеми широко використовуються дешевий метод активного радіотехнічного маскування (АРТМ) та електромагнітне екранування, яке має високу вартість реалізації. Інші методи захисту інформації через особливості та (або) складністю реалізації не знайшли широкого застосовування.

Існуючі методи відрізняються настільки серйозними недоліками, що застосування, наприклад, методу АРТМ стає в органах військового управління взагалі неможливим. Таким чином, зараз актуальним є питання забезпечення безпеки інформації в умовах постійного розвитку засобів зв'язку.

Аналіз проблеми витоку інформації технічними каналами показує, що більшість каналів втрачають свою інформативність при шифруванні даних периферійних пристроїв, накопичення інформації, даних, які циркулюють у комп'ютерної мережі і т.д. Однак дані, що транслюються у системі відображення інформації (як у аналоговому, так і у цифровому інтерфейсі), не можуть бути захищені за допомогою шифрування, оскільки це потребує зміни штатного алгоритму роботи засобів відображення інформації та складної апаратної модернізації як засобів відображення інформації, так і графічного адаптера АС.

Разом з цим небезпека витоку інформації в засобах відображення інформації пояснюється тим, що вони мають регулярний характер (період повторення та інші параметри інформаційного сигналу засобів відображення інформації стандартизовані та загальновідомі), а накопичення регулярних повторень, як відомо, підвищує відношення сигнал/шум пропорційно кількості накопичених повторень, що дозволяє збільшити дальність перехоплення побічних електромагнітних випромінювань та достовірність відновленої інформації.

З метою протидії витоку інформації через побічні електромагнітні випромінювання засобів відображення інформації пропонується параметричний метод захисту, який полягає у випадковій зміні часових параметрів інформаційного сигналу засобів відображення, ступінь зміни яких обмежується діапазоном відпрацювання системи синхронізації засобів відображення інформації та вимогами щодо збереження якості зображення, яке виводиться на екран засобів відображення.

Даний метод має низку переваг у порівнянні з існуючими методами:

побічні електромагнітні випромінювання засобів відображення інформації перестають бути регулярними, що усуває можливість їх накопичення;

спектральна щільність потужності випромінювань засобів відображення інформації розосереджується у широкому частотному діапазоні і випромінювання стає малопомітним на фоні природного шуму;

повністю виконуються вимоги електромагнітної сумісності радіоелектронних засобів.

к.т.н. Сілко О.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Шугалій Є.П. (УВМА)

МЕТОДИКА ДОСЛІДЖЕННЯ ФУНКЦІОНАЛЬНИХ ЗАЛЕЖНОСТЕЙ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ ТИПОВИХ ОБЧИСЛЮВАЛЬНИХ МОДУЛІВ ДЛЯ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ ВІД ЇХ ПАРАМЕТРІВ

Під типовим обчислювальним модулем (ТОМ) слід розуміти елемент автоматизованої системи управління (АСУ), який проводить обробку, збереження та видачу інформації, з оптимальними (раціональними) параметрами. Однією з основних задач під час конструювання та побудови АСУ є вибір параметрів ТОМ з метою оптимізації його техніко-економічних показників.

У публікаціях, які висвітлюють питання дослідження залежності показників складних технічних пристроїв від їх параметрів використовується великий набір методів обробки експериментальних даних. Найбільший розвиток отримали методи кореляційного та регресійного аналізу, які характеризуються високою достовірністю та простотою обчислення. Статистичний зв’язок між змінними вивчають методами кореляційного (встановлення наявності зв’язку між двома випадковими величинами та оцінка її тісноти) та регресійного (встановлення залежності між змінними) аналізів. Тому в подальшому для рішення поставленої задачі будемо використовувати метод кореляційно-регресійного аналізу. У доповіді наводиться методика, за допомогою якої можливо дослідити та узагальнити взаємозв’язки кореляційно пов’язаних змінних для задачі вибору параметрів типових обчислювальних модулів обробки, збереження та видачі інформації при розгортанні АСУ з використанням базово-модульного принципу побудови зразків АСУ. Представлено результати дослідження сукупності варіантів ТОМ. Параметрами, якими характеризуються варіанти ТОМ, є: ємність оперативної пам’яті (Мб), вартість модуля оперативної пам’яті (грн), тактова частота роботи процесора (ГГц), вартість процесора (грн.), вартість ТОМ (грн).

Формальна постановка задачі дослідження передбачає виявлення та вивчення функціональної залежності техніко-економічних показників типового обчислювального модуля від його параметрів. Вхідними даними виступають: сукупність зразків ТОМ $i = 1, \ldots, n$; параметри кожного зразка – швидкодія процесора x_{1i} $(i = \overline{1, n})$; об’єм оперативної пам’яті x_{2i} $(i = \overline{1, n})$; техніко-економічні показники ТОМ – вартість C_i $(i = \overline{1, n})$; час на виготовлення T_i $(i = \overline{1, n})$. Задача формулюється наступним чином: необхідно встановити функціональну залежність техніко-економічних показників C і T від параметрів ТОМ x_1, x_2. Запропоновано для спрощення проведення обчислення та виявлення зв’язку між параметрами поділити їх на факторні і результативні та замінити змінними (y, x_1, x_2, x_3, x_4): результативний параметр (y) – вартість ТОМ (грн.); факторні параметри: (x_1) – тактова частота роботи процесора (ГГц); (x_2) – ємність оперативної пам’яті (Мб); (x_3) – вартість процесора (грн); (x_4) – вартість модуля оперативної пам’яті (грн).

Знаходження рівняння регресії здійснено за допомогою пакета прикладного статистичного аналізу даних STATISTICA 6 компанії StatSoft. Отримані в процесі дослідження функціональні залежності техніко-економічних показників ТОМ від його параметрів дозволили вирішити низку прикладних задач, які виникають під час виробництва типових обчислювальних модулів, а саме:

– провести обчислення значень техніко-економічних показників ТОМ при конкретних значеннях параметрів;

– провести дослідження процесу оптимізації виробництва за показниками: вартість, темп випуску та надійність, шляхом раціонального вибору параметрів ТОМ.

к.т.н. Слотвінська Л. І. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ ВІДБИТКІВ З ЗАСВІДЧУВАЛЬНИХ ДРУКАРСЬКИХ ФОРМ

Для захисту спеціальної поліграфічної продукції на стадії заповнення використовують спеціальні засвідчувальні форми високого друку.

Виготовлення форм високого друку відбувається з використанням різних видів формних матеріалів. Відбитки з друкарських форм одержують, як правило, на готових зразках спеціальної поліграфічної продукції, надрукованих на різних видах друкарського паперу.

Найважливішими показниками паперу, що можуть впливати на якість відбитку є: маса 1 м^2, товщина, щільність, міцність, гладкість, пористість, білизна, непрозорість, відтінок.

Кожен вид друку має характерні особливості відбитків, які можна визначити візуально з допомогою оптичних збільшувальних пристроїв (лупа, мікроскоп) і за якими можна встановити вид формного матеріалу засвідчувальної друкарської форми.

Проведено аналіз відбитків за точністю передачі зображень з засвідчувальних друкарських форм, виготовлених з різних формних матеріалів – гумових, набірних полімерних та класичних фотополімерних друкарських форм.

Для одержання відбитків використовували різн види паперу – для документів, офсетний, не вибілений із вмістом великих частинок волокон деревини, офісний, двосторонній крейдований папір, крейдований картон. Визначали характерні особливості відбитків та вплив основних технічних показників паперу на якість відбитку.

Детально проаналізовано характер зображень на відбитках для кожного виду паперу, подібність та відмінності зображень, одержаних з однієї друкарської форми на різних видах паперу. Встановлено технічні показники паперу які найбільше впливають на точність передачі зображення на відбитку (таблиця 1).

Таблиця 1

Технічні показники паперу	Насиченість кольору відбитку	Гладкість країв зображення	Розподіл друкарської фарби	Спотворення зображення та тексту
Щільність	Змінюється насиченість кольору по площі зображення	Посіченість країв (пилкоподіб-ність)	Скупчення фарби в окремих місцях відбитку	Майже не впливає
Гладкість	Відбувається зміна насиченості фарби в певних частинах відбитку	Нерівні хвилясті краї	Погіршується рівномірний розподіл	Призводить до часткового спотворення за рахунок витіснення фарби
Пористість	Змінюється насиченість кольору	Значне посічення країв	Нерівномірний фарбовий шар за рахунок всмоктування фарби	Майже не впливає

Маса паперу, товщина, міцність, білизна, непрозорість, відтінок суттєво не впливають на якість відбитку. На основі проведених досліджень визначено характерні особливості відбитків для встановлення виду формного матеріалу засвідчувальної друкарської форми.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗС України)
Бондаренко М.В. (ТОВ „Пульсар")

ПОТЕНЦІЙНА ТОЧНІСТЬ ОЦІНКИ НАПРЯМКУ НА АБОНЕНТА ЦИФРОВОЮ АНТЕННОЮ РЕШІТКОЮ В УМОВАХ ДЖИТЕРУ АЦП

В результаті моделювання процедури пеленгації абонентів та джерел завад на етапі входження у зв'язок за допомогою лінійної цифрової антенної решітки (ЦАР) було виявлено, що дисперсія оцінки кутової координати приблизно дорівнює сумі дисперсій оцінок, спричинених адитивним шумом та джитером [1].

У доповіді пропонується модифікований вираз нижньої границі Крамера-Рао (НГКР) для лінійної еквідистантної решітки, який враховує наявність джитера АЦП.

Можна показати [2], що для такої решітки з комплексним виходом радіоприймального пристрою вираз для НГКР без урахування джитера АЦП має вигляд:

$$\sigma_\beta^2 \geq \frac{3}{2\nu^2\pi^2 N(N-1)^2}\frac{\lambda^2}{d^2\cos^2\beta}, \qquad (1)$$

де $\nu^2 = A^2/2\sigma_\eta^2$ – відношення сигнал/шум, A – амплітуда сигналу, σ_η^2 – дисперсія адитивного шуму, N – кількість елементів решітки, d – відстань між елементами, β – кут між напрямком на джерело сигналу та нормаллю до решітки, λ – довжина хвилі прийнятого електромагнітного випромінювання. Цей вираз не враховує джитер і призводить до надто оптимістичних оцінок точності, не відповідаючих результатам чисельного експерименту.

Можна показати, що у випадку малого джитеру відношення сигнал/шум у цифровому сигналі після дискретизації комплексного сигналу з виходу радіоприймального пристрою ЦАР має вигляд

$$\overline{\nu}^2 = A^2\left(A^2\omega^2\sigma_\tau^2 + 2\sigma_\eta^2\right)^{-1}, \qquad (2)$$

де ω – кругова частота сигналу на вході АЦП, σ_τ^2 — дисперсія джитеру.

Модифікуємо вираз (2) заміною ν^2 на $\overline{\nu}^2$ для урахування джитера. Отриманий вираз має вигляд

$$\sigma_\beta^2 \geq \frac{3\left(A^2\omega^2\sigma_\tau^2 + 2\sigma_\eta^2\right)}{2A^2\pi^2 N(N-1)^2}\frac{\lambda^2}{d^2\cos^2\beta}. \qquad (3)$$

Було проведене чисельне моделювання при різних співвідношеннях A, σ_τ^2 и σ_η^2. Оцінювання кута β здійснювалося шляхом максимізації функції правдоподібності перебиранням значення кута β. При $\sigma_\tau^2 = 0$ дисперсія оцінки задовольняла виразу (1). Результати моделювання показали, що вираз (3) може використовуватися в якості нижньої границі дисперсії оцінки кута β.

Перехід до $A \to \infty$ показує, що погрішності пеленгації, спричинені джитером, не можуть бути усунені підвищенням енергетики сигналу, що також підтверджує висновки з роботи [1]

$$\lim_{A\to\infty}\left(\frac{3\left(A^2\omega^2\sigma_\tau^2 + 2\sigma_\eta^2\right)}{2A^2\pi^2 N(N-1)^2}\frac{\lambda^2}{d^2\cos^2\beta}\right) = \frac{3\omega^2\sigma_\tau^2}{2\pi^2 N(N-1)^2}\frac{\lambda^2}{d^2\cos^2\beta}. \qquad (4)$$

ЛІТЕРАТУРА

1. *Слюсар В.И.* Влияние нестабильности такта АЦП на угловую точность линейной цифровой антенной решетки // Радиоэлектроника. – 1998. – том 41. – №6. – с.77– 80. (Изв.вузов)

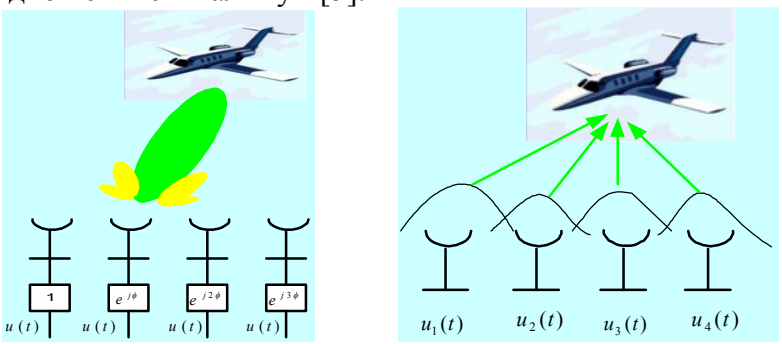
2. *Kay S.M.* Fundamentals of Statistical Signal Processing: Estimation Theory/ S.M. Kay – Prentice Hall, 1993. – 625 с.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗС України)
Зінченко А.О. (НУОУ)

ТЕХНОЛОГІЯ МУЛЬТИ-MIMO ЯК ЗАСІБ АПАРТНОГО ПОЄДНАННЯ СИСТЕМ ЗВ'ЯЗКУ ТА РАДІОЛОКАЦІЇ

Серед тенденцій розвитку інформаційних систем спеціального призначення заслуговує на увагу ідея створення багатофункціональних засобів, які поєднували б в межах однієї апаратної платформи вирішення завдань, традиційно притаманних окремим за призначенням радіотехнічним комплексам. Особливо ефективним таке поєднання можливе на основі використання цифрових антенних решіток (ЦАР), прикладом чого є запропонована в інтеграція [1, 2] засобів стільникового зв'язку та радіолокаційної розвідки.

Подальшим розвитком зазначеного напряму стали запропоновані в [3, 4] інтегровані системи радіолокаційної розвідки та зв'язку, що ґрунтуються на застосуванні технології MIMO та неортогональної частотної дискретної модуляції (N-OFDM) сигналів. Річ у тім, що останнім часом, для вирішення завдань радіозв'язку широке застосування знаходять системи MIMO. Також ведуться розробки для застосування MIMO-технології у галузі радіолокації. Відмінність між радіолокаційною станцією (РЛС) з традиційною системою цифрового діаграмоутворення та MIMO-радаром полягає у формуванні в режимі передачі не одного променя діаграми спрямованості, а кількох різних за частотою (рис. 1), що надає можливість за рахунок специфічної обробки цифрової суміші у процесорі приймального сегменту досягти виграшу у відношенні сигнал-шум [5].



а) б)

Рис. 1. Принцип радіолокації. а) традиційна система на основі ЦАР, б) MIMO – радар

MIMO радіолокація має значний потенціал для роботи із слабкими сигналами, покращення їх розрізнення, а також виявлення та придушення завад. Використання цього потенціалу надасть можливість збільшити ймовірність виявлення цілей в складних умовах інформаційної боротьби.

Апаратна реалізація систем зв'язку та радіолокації на основі технології MIMO принципово не відрізняється. Застосування пропонуємої інтегрованої MIMO-технології в апаратних рішеннях вузлових елементів тактичної „інформаційної решітки" дозволить реалізувати високу пропускну спроможність каналів зв'язку, своєчасно виявити засоби повітряного нападу противника, підвищить живучість мережі передавачів за рахунок своєчасного припинення роботи з випромінюванням, ускладнить противнику виявлення угруповання протиповітряної оборони (ППО) та надасть можливість здійснити засобам ППО ураження противника без підсвітки своїми РЛС.

Більш широким рівнем узагальнення розглянутого інтеграційного підходу є використання багатопозиційної системи MIMO-радіолокації у поєднанні з кооперативною передачею даних в розподілених MIMO-системах зв'язку на основі впровадження багатокористувальницьких алгоритмів MIMO-зв'язку (мульти-MIMO) у мережах мобільних

базових станцій. При цьому можливі гібридні системи, що поєднують у собі мульти-MIMO кластери та автономні MIMO-комплекси зв'язку і радіолокації.

Найбільш простим режимом функціонування інтегрованої мульти-MIMO системи є розподіл у часі виконання завдань передачі даних та радіолокації (наприклад, здійснення контролю повітряного простору на етапі входження у зв'язок). Найскладнішим випадком є одночасне вирішення радіолокаційних та зв'язкових задач з кооперативною передачею даних, коли кожна з станцій зв'язку одночасно працює з усіма зав'язаними у мережу базовими станціями.

Відправною точкою досліджень зазначених мульти-MIMO систем є математична формалізація їх відгуку. Складність математичного опису процесу функціонування інтегрованої системи радіолокації та зв'язку (ІСРЗ) залежить від типу ЦАР, які використовуються на мобільних станціях. Найпростішим є випадок застосування односекційних лінійних ЦАР, однак для вирішення локаційних завдань доцільно спиратись на використання плоских антенних решіток. Найбільш складним випадком є оснащення кожної з мобільних базових станцій ІСРЗ багатосекційними плоскими ЦАР. Суттєво, що використовуючи апарат блокових торцевих добутків матриць та добутку Хатрі-Рао [6, 7], всі зазначені випадки конструктивного виконання ЦАР можуть бути охоплені єдиним матричним виразом, що описує сукупність напруг сигналів по входах приймальних каналів ЦАР:

$U = P \cdot A + n$, де U - блоковий вектор комплексних напруг сигналів по виходах частотних фільтрів просторових каналів сукупності плоских ЦАР, P - сигнальна матриця, A – блоковий вектор амплітуд сигналів, n – блоковий вектор шумових напруг. Для кожного з випадків має використовуватись своя структура сигнальної матриці P та блокових векторів U і A.

В режимі зв'язку демодуляція сигналів може бути здійснена за виразом $\tilde{A} = \left(P^T P\right)^{-1} P^T U$ з урахуванням просторово-часового чи іншого з різновидів кодування MIMO-сигналів. В радіолокаційному режимі оцінюванню мають підлягати елементи сигнальної матриці P. Метою подальших досліджень є конкретизація запису сигнальної матриці та блокових векторів U і A, отримання відповідних оцінок параметрів сигналів та аналіз їхньої точності.

ЛІТЕРАТУРА

1. *Слюсар В. И., Тітов І.В., Карєв В.Г.* Концепція перспективної інформаційно-телекомунікаційної системи.// IV-а науково- практична конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення" (22 – 23 жовтня 2008, доповіді та тези доповідей). – Київ: ВІТІ НТУУ „КПІ", 2008. – С. 76 – 79.

2. *Патент України* № 56922 A. IPC8 G01S13/02, G01S13/06, G01S13/48, G01S13/74, G01S13/86, G01S13/87. Спосіб виявлення повітряних цілей за допомогою системи стільникового зв'язку // Слюсар В.І., Тітов І.В. – Заявка № 2002119018. – Дата пріоритету – 12.11.2002. – Опубл. 15.05.2003, Бюл. № 5/2003.

3. *Слюсар В.І., Зінченко А.О.* Інтегрована система зв'язку та радіолокаційної розвідки на основі технології MIMO. // 3-а Всеукраїнська науково-технічна конференція "Перспективи розвитку озброєння і військової техніки Сухопутних військ". – Львів, Академія Сухопутних військ імені Гетьмана Петра Сагайдачного. – 13 – 14 квітня 2010 р. – С. 150.

4. *Слюсар В.І., Зінченко А.О.* Технологія MIMO як основа інтегрованої системи зв'язку та радіолокаційної розвідки. //Шоста наукова конференція Харківського університету Повітряних Сил імені Івана Кожедуба „Новітні технології для захисту повітряного простору", 14 - 15 квітня 2010 року. – Харків: ХУПС. – 2010. – С. 108 – 109.

5. *Chun-Yang Chen.* Signal Processing Algorithms for MIMO Radar . – Pasadena, California, California Institute of Technology/ In Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy. – 2009.

6. *Слюсар В.И.* Обобщенные торцевые произведения матриц в моделях цифровых антенных решеток с неидентичными каналами.//Известия вузов. Сер. Радиоэлектроника. – 2003. – Том 46, № 10. – С. 9 – 17.

7. *Слюсар В.И.* Семейство торцевых произведений матриц и его свойства// Кибернетика и системный анализ. – 1999. – Том 35; № 3. – С. 379 – 384.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗС України)
Копієвська В.С. (ЦНДІ ОВТ ЗС України)

ОЦІНКА РІВНЯ КОМПЛЕКСНО-СПОЛУЧЕНОГО ВІДГУКУ СИГНАЛУ ПО ВИХОДУ ПЛОСКОЇ ЦИФРОВОЇ АНТЕННОЇ РЕШІТКИ

При використанні цифрових квадратурних демодуляторів OFDM сигналів у MIMO-приймачах з плоскою цифровою антенною решіткою (ЦАР) швидкість передачі даних обмежує наявність комплексно-сполученої складової (КСС) сигнального відгуку. Тому виникає потреба в оцінці рівня КСС, для чого в [1, 2] були запропоновані відповідні методи розрахунку. Однак їх розгляд був обмежений випадком лінійної ЦАР. В доповіді пропонується метод оцінки КСС по вихідним напругам плоскої ЦАР та наводиться нижня границя Крамера Рао (НГКР) для дисперсій незміщених оцінок амплітуд основної і комплексно-сполученої складових сигналів, що характеризує потенційну точність пропонованого методу. Розглянемо матричний запис відгуку плоскої ЦАР при впливі на неї гармонійного контрольного сигналу, обробка якого здійснюється шляхом синтезу цифрової діаграми спрямованості й формування частотних фільтрів по виходах вторинних прийомних каналів за допомогою швидкого перетворення Фур'є (ШПФ). Якщо вважати, що основному сигнальному відгуку у координатному просторі „напрямки приходу сигналу – частота" відповідають відомі кутові координати x, у джерела випромінювання та радіальна частота ω, то для КСС аналогічні параметри сигнального відгуку приймуть негативні значення: -x, -y і $-\omega$. Відповідний матричний вираз для вектора напруг сукупності сигнальних складових запишеться у вигляді:

$$\mathrm{U} = \mathrm{P} \cdot \mathrm{A} + \mathrm{n}, \qquad (1)$$

де $\mathrm{U}=\left[\dot{\mathrm{U}}_{11}\ \dot{\mathrm{U}}_{12}\ \cdots\ \dot{\mathrm{U}}_{\mathrm{rs}}\ \cdots\ \dot{\mathrm{U}}_{\mathrm{RS}}\right]^{\mathrm{T}}$ – вектор комплексних напруг сигналів по виходах S частотних фільтрів R×Z просторових каналів плоскої ЦАР, $\mathrm{P} = \mathrm{Q} \blacksquare \mathrm{V} \blacksquare \mathrm{F}$ – сигнальна матриця, ■ – символ добутку Хатрі- Рао [3],

$Q = \begin{bmatrix} Q_1(x) & Q_1(-x) \\ \vdots & \vdots \\ Q_R(x) & Q_R(x) \end{bmatrix}$ – матриця характеристик спрямованості (ХН) R просторових каналів ЦАР (первинних або вторинних) у першій координатній площині, причому у випадку виконання цифрового діаграмоутворення за допомогою операції просторового ШПФ маємо $Q_r(x) = [\sin(R[r-x])][\sin(r-x)]^{-1}$, $x = \pi \frac{d}{\lambda} sin\theta \cdot cos\varepsilon$, d_x – інтервал між антенними елементами еквідистантної антенної решітки, λ - довжина хвилі сигналу, θ – кут між напрямком на джерело сигналу й нормаллю до ЦАР у першій координатній площині,

$V = \begin{bmatrix} V_1(y) & V_1(-y) \\ \vdots & \vdots \\ V_Z(y) & V_Z(y) \end{bmatrix}$ – матриця ХН Z просторових каналів ЦАР (первинних або вторинних) у другій координатній площині, причому у випадку виконання цифрового діаграмоутворення за допомогою ШПФ $V_z(y) = [\sin(Z[z-y])][\sin(z-y)]^{-1}$, $y = \pi \frac{d}{\lambda} sin\theta \cdot sin\varepsilon$, d_y – інтервал між антенними елементами, ε – кут між напрямком на джерело сигналу й нормаллю до ЦАР у другій координатній площині,

$F = \begin{bmatrix} F_1(\omega) & F_1(-\omega) \\ \vdots & \vdots \\ F_S(\omega) & F_S(-\omega) \end{bmatrix}$ – матриця значень АЧХ S частотних фільтрів, синтезованих у результаті ШПФ, $F_s(\omega) = \left(\sin\frac{S}{2}\cdot\left[s\cdot\frac{2\pi}{S}-\omega\right]\right)\left(\sin\frac{1}{2}\left[s\cdot\frac{2\pi}{S}-\omega\right]\right)^{-1}$; $\mathrm{A} = \left[\dot{\mathrm{A}}_1\ \dot{\mathrm{A}}_2\right]^T$ – вектор комплексних амплітуд основної компоненти сигналу ($\dot{\mathrm{A}}_1$) і його КСС ($\dot{\mathrm{A}}_2$), n – вектор комплексних напруг шумів.

Варто звернути увагу, що в описі сигнального відгуку відсутні комбіновані добутки ХН і АЧХ, що залежать від параметрів основного й комплексно-сполученого відгуків, наприклад, $Q_r(-x)V_z(y)F_s(-\omega)$. Мають місце тільки комбінації цих характеристик як функцій параметрів лише однієї сигнальної компоненти: $Q_r(-x)V_z(-y)F_s(-\omega)$ або $Q_r(x)V_z(y)F_s(\omega)$. Синтез методу максимально правдоподібного оцінювання рівня КСС в умовах впливу гаусових некорельованих шумів полягає у мінімізації функціонала $\mathrm{L} = (\mathrm{U} - \mathrm{P}\cdot\mathrm{A})^*(\mathrm{U} - \mathrm{P}\cdot\mathrm{A})$, сформованого з вектору напруг (1). Сама оцінка максимальної правдоподібності вектора амплітуд сигнальних складових має відомий матричній запис $\tilde{A} = (P^T P)^{-1} P^T U$.

Нижня границя Крамера- Рао (НГКР) для дисперсій помилок оцінювання амплітудних складових σ_A^2 визначиться шляхом обернення інформаційної матриці Фішера, яка формується з математичних очікувань других похідних функціонала L по невідомому вектору А і в цьому випадку запишеться як $\mathrm{I} = (2\sigma^2)^{-1}(P^T P)$, де σ^2 – дисперсія шумів.

З огляду на матричну тотожність $(\mathrm{Q}\blacksquare V\blacksquare\mathrm{F})^{\mathrm{T}}(\mathrm{Q}\blacksquare V\blacksquare\mathrm{F}) = (\mathrm{Q}^{\mathrm{T}}\mathrm{Q})\circ(\mathrm{V}^{\mathrm{T}}\mathrm{V})\circ(\mathrm{F}^{\mathrm{T}}\mathrm{F})$ [4], де $\circ$ – символ по елементного добутку Адамара, співвідношення для НГКР можна одержати шляхом обернення інформаційної матриці I у вигляді $\sigma_A^2 = 2\sigma^2 diag\left(\left[(\mathrm{Q}^{\mathrm{T}}\mathrm{Q})\circ(\mathrm{V}^{\mathrm{T}}\mathrm{V})\circ(\mathrm{F}^{\mathrm{T}}\mathrm{F})\right]^{-1}\right)$, де $diag(H)$ – вектор, складений з діагональних елементів матриці Н,

$$(\mathrm{Q}^{\mathrm{T}}\mathrm{Q})\circ(\mathrm{V}^{\mathrm{T}}\mathrm{V})\circ(\mathrm{F}^{\mathrm{T}}\mathrm{F}) = \begin{bmatrix} \left[\sum_{r=1}^{R} Q_r^2(x)\right]\left[\sum_{z=1}^{Z} V_z^2(y)\right]\sum_{s=1}^{S} F_s^2(\omega) & D \\ D & \left[\sum_{r=1}^{R} Q_r^2(-x)\right]\left[\sum_{z=1}^{Z} V_z^2(-y)\right]\sum_{s=1}^{S} F_s^2(-\omega) \end{bmatrix},$$

$$D = \left[\sum_{r=1}^{R} Q_r(x)Q_r(-x)\right]\left[\sum_{z=1}^{Z} V_z(y)V_z(-y)\right]\sum_{s=1}^{S} F_s(\omega)F_s(-\omega).$$

Таким чином, проведені дослідження дозволили вперше одержати аналітичний запис НГКР для аналізу потенційної точності оцінювання основної та комплексно-сполученої сигнальних компонент по виходах приймальних каналів плоскої ЦАР системи MIMO.

ЛІТЕРАТУРА

1. *Слюсар В.И., Малярчук М.В., Копиевская В.С.* Метод расчета уровня комплексно-сопряженной составляющей сигнала в цифровой антенной решетке. // Сб. материалов 6-й Международной молодежной научно-технической конференции „Современные проблемы радиотехники и телекоммуникаций РТ-2010”, 19 – 24 апреля 2010 г., Севастополь, Украина. – С. 124.

2. *Слюсар В.И., Копиевская В.С.* Совместное оценивание основного и комплексно-сопряженного откликов сигнала по выходу линейной цифровой антенной решетки. // VI Международная научно-техническая конференция „Современные информационно-коммуникационные технологии” COMINFO’2010-Livadia. – 04 – 08 октября 2010. – Крым, Ялта, Ливадия.

3. *Слюсар В.И.* Обобщенные торцевые произведения матриц в моделях цифровых антенных решеток с неидентичными каналами. Радиоэлектроника. – 2003. – Том 46, № 10. – С. 9 – 17.

Слюсар В.І. (ЦНДІ ОВТ)
Троцько О.О. (ВІТІ НТУУ „КПІ”)
Копієвська В.С. (ЦНДІ ОВТ)

МЕТОДИ ВРАХУВАННЯ НЕЛІНІЙНОЇ ЧАСТОТНОЇ МОДУЛЯЦІЇ OFDM СИГНАЛІВ ПРИ ЗВ'ЯЗКУ З НАДЗВУКОВИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

У процесі зв'язку з високошвидкісними літальними апаратами, у тому числі безпілотними (БПЛА), при значних кутових швидкостях обертання лінії візування, що з'єднує в умовах прямої видимості (Line of Sight, LOS) точки прийому та передачі сигналів, високоточній демодуляції OFDM сигналів перешкоджає девіація частоти, обумовлена обертанням лінії візування за час накопичення сигналів при цифровому синтезі частотних фільтрів. Залежно від тривалості накопичення і швидкості цілі, вказана девіація може завадити прийому сигналу, і призвести до втрат інформації. У цьому випадку, як свідчить досвід вирішення радіолокаційних задач, гармонійна модель сигналів стає недієздатною, відбувається суттєва деформація форми спектру й обвідної відгуків частотних фільтрів, сформованих за допомогою операції швидкого перетворення Фур’є (ШПФ). Як наслідок традиційні методи демодуляції сигналів OFDM при вирішенні завдань зв’язку теж можуть втратити свою працездатність.

Тому при демодуляції OFDM сигналів виникає необхідність врахування не тільки допплерівських зрушень їхньої частоти, але й паразитної частотної модуляції, обумовленої зазначеним ефектом.

Метою роботи є дослідження впливу нелінійної допплерівської модуляції OFDM сигналів та розробка методів їхньої демодуляції з урахуванням нелінійного ефекту Допплера у системах зв'язку з високошвидкісними БПЛА.

Суть пропонованого варіанта обробки полягає в тім, що кожний з часових відліків прийнятого сигналу по виходу АЦП при квадратурній схемі прийому піддається фазовому довороту на величину $\exp(j\omega_0 R_s/c)$, знак комплексного аргументу якої протилежний знаку нелінійної зміни фази центральної несучої частоти прийнятого OFDM сигналу.

Якщо покласти, що в прийнятих сигналах в аргументі $p_s = \omega\Delta t(s-1) - \omega_0 R_s/c$ величина $\omega_0 R_s/c$ має негативний знак, то квадратурні складові U_s^c, U_s^s відліків напруг сигналів, прийнятих по виходу АЦП, у межах запропонованої процедури компенсації фази повинні бути піддані зважуванню за формулою:

$$U_s^c \cos\frac{\omega_0 R_s}{c} + U_s^s \sin\frac{\omega_0 R_s}{c} + j\left\{U_s^s \cos\frac{\omega_0 R_s}{c} - U_s^c \sin\frac{\omega_0 R_s}{c}\right\}. \qquad (1)$$

Внаслідок застосування фазового обернення (1) нескладно одержати скориговані відліки напруг сигналу, що в ідеалі будуть вільними від нелінійного фазового доданку:

$$\tilde{U}_s^s + jU_s^s = U_s^c \cos\frac{\omega_0 R_s}{c} + U_s^s \sin\frac{\omega_0 R_s}{c} + j\left\{U_s^s \cos\frac{\omega_0 R_s}{c} - U_s^c \sin\frac{\omega_0 R_s}{c}\right\} =$$
$$= a_m \exp\left[j(\omega\Delta t(s-1) - \omega_0 R_s/c + \varphi)\right]\exp\left[j(\omega_0 R_s/c)\right] =$$
$$= a_m \exp\left[j(\omega\Delta t(s-1)\varphi)\right].$$

Аналогічний підхід може бути використаний на прийомній стороні й при додатковому стробуванні відліків АЦП. Для цього в якості часових відліків напруг варто розглядати відгуки стробів, а в аргументі фазового виправлення, що компенсує нелінійне зрушення фази, використовувати величину $R_s = \sqrt{R_0^2 - 2VR_0(s-1)T\Delta t\cos\varepsilon + V^2T^2\Delta t^2(s-1)^2}$.

Розроблені методи компенсації враховують нелінійну девіацію частоти сигналів OFDM, що дозволить максимально мінімізувати похибки демодуляції й підвищить швидкість обміну даними з бортовою апаратурою БПЛА та інших надзвукових літальних об’єктів.

к.т.н. Сова О.Я. (ВІТІ НТУУ „КПІ”)

ІНТЕЛЕКТУАЛІЗАЦІЯ УПРАВЛІННЯ ПОТОКАМИ ДАНИХ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Одним з актуальних завдань реформування ЗСУ на період до 2015 року є створення багаторівневої мобільної компоненти (МК), основу якої складатимуть мобільні радіомережі (МР), що будуються за технологією MANET (*Mobile Ad-Hoc Networks*). До особливостей МР тактичної ланки управління відносяться: висока динаміка топології, значна розмірність, низька пропускна спроможність радіоканалу, неоднорідність вузлів та ін.

Особливості МР та специфіка завдань, які покладаються на них, вимагають виконання підвищених вимог щодо забезпечення доставки великих обсягів інформації із заданою якістю, а отже потребують застосування методів управління потоками даних (МУПД), які б забезпечили передачу цієї інформації в безпровідних мережах з динамічною топологією.

Так як функціонування МР відбуватиметься в умовах частої зміни обстановки (оперативної, тактичної, зі зв’язку, тощо), то рішення з управління потоками даних прийматимуться в умовах невизначеності, які спричинені складністю формалізованого опису МР та задач управління ними, нестаціонарністю параметрів МР та вузлової системи управління, апріорною невизначеністю обстановки та умов функціонування МР, наявністю випадкових та навмисних впливів зовнішнього середовища.

Крім того, забезпечення здатності МР до самоорганізації, а також адаптації її елементів до різних умов функціонування вимагає реалізації системи управління вузлом МР із залученням технологій обробки знань. На сьогоднішній день системи управління інтенсивно розвиваються в напрямку їхньої інтелектуалізації, а сучасні інтелектуальні інформаційні системи (ІІС) поєднують можливості систем управління базами даних і технологію штучного інтелекту, завдяки чому зберігання управлінської інформації в них ототожнюється з її обробкою й підготовкою для використання при прийнятті рішень. Враховуючи сказане, інтелектуалізація процесу прийняття рішень з управління потоками даних в МР військового призначення є актуальною на сьогоднішньому етапі реформування ЗС України. Організація елементів інтелектуальної системи управління припускає використання сукупності моделей подання знань, інформаційної підтримки, опису контрольованого об’єкту і т.д. Головною відмінністю побудови інтелектуальної системи управління вузлом МР є використання методів і технологій штучного інтелекту, як основних засобів боротьби з невизначеністю зовнішнього середовища. Практичне втілення цієї концепції припускає вибіркове використання тих або інших технологій обробки знань залежно від специфіки розв’язуваних завдань і особливостей об'єкта управління. Найбільш перспективними для створення інтелектуальних систем управління представляються чотири технології: експертних систем, асоціативної пам'яті, нечіткої логіки, нейронних мереж. Основна ідея при цьому полягає в переході від строго формалізованих алгоритмів, які пропонують метод вирішення завдання, до логічного програмування з вказівкою на те, що потрібно вирішувати на базі знань, накопичених в конкретних предметних областях. Як показують результати аналізу різних робіт стосовно розвитку методів обробки знань, однією з передових тенденцій в цій області є спроба інтеграції різних технологій з метою об’єднання характерних їм переваг. Так, наприклад, одночасне забезпечення високої функціональної гнучкості та швидкодії може досягатися шляхом комплексного застосування теорії нечітких множин та нейронних мереж. З одного боку, вони дозволяють розробляти та представляти моделі систем в формі правил нечітких продукцій, які характеризуються наочністю та простотою змістовної інтерпретації. З іншого боку, для побудови правил нечітких продукцій використовуються методи нейронних мереж, що є більш зручним та менш трудомістким процесом для системних аналітиків. Використання ІІС при розробці МУПД в МР дозволить зменшити витрати часу на збір і аналіз службової інформації про стан мережі, скоротити обсяги цієї інформації шляхом врахування ситуації, що склалася в мережі в певний момент часу.

к.т.н. Соколов В.В. (ВІТІ НТУУ „КПІ”)

ТЕХНОЛОГІЯ ПРОГРАМУВАННЯ АКТИВНИХ ДИНАМІЧНИХ СПОЛУК ОБ’ЄКТІВ

Технологія об’єктно-орієнтованого програмування (ООП) на сьогодні є домінуючою, вона реалізована практично в усіх сучасних мовах програмування. Створено багато інструментальних засобів автоматизації проектування програмного забезпечення (ПЗ) на основі ООП, які дозволяють побудувати об’єктну модель предметної області.

Але ООП не дає відповіді на запитання, як все ж таки з об’єктів побудувати програму. Великий обсяг допоміжного програмного коду, який забезпечує функціонування об’єктів, з’єднує об’єкти в єдину програму та примушує їх взаємодіяти, залишається поза межами об’єктно-орієнтованого проектування. Тому розробка технології програмування, яка б забезпечувала автоматизацію створення закінченого ПЗ, є актуальною проблемою.

Одним з підходів до створення ПЗ є побудова програми у вигляді активних динамічних сполук об’єктів, надалі його будемо називати АДС-технологією програмування.

Концепція АДС-технології базується на таких положеннях:

1. об’єкт є програмним модулем, який перетворює вхідні значення в вихідні значення;
2. об’єкт може отримувати управління для виконання перетворення вхідних значень в вихідні значення;
3. процес від початку зміни вхідних значень до закінчення обчислень всіх вихідних значень може виконуватись транзакційно, з відкатом змін або без відкату;
4. об’єкт може пасивно взаємодіяти з іншими об’єктами будь-яких класів шляхом читання значень їх властивостей;
5. об’єкт може активно взаємодіяти з іншими об’єктами будь-яких класів шляхом передавання їм управління (активації).

Основними принципами АДС-технології є такі:

1. сепарація інтерфейсу об’єкта – доступні зовні властивості об’єкта мають бути поділеними на вхідні дані (вхід) та вихідні результати (вихід);
2. внутрішня активність об’єкта – об’єкт повинен містити доступний зовні головний метод (ядро), який забезпечує обчислення значень виходу за заданими значеннями входу і здійснює контроль стану та інші дії всередині об’єкта;
3. транзакційність зміни об’єкта – об’єкт повинен забезпечувати транзакційність зміни значень його властивостей шляхом контролю відповідності значень на виході значенням на вході;
4. сполуки об’єктів – об’єкти повинні забезпечувати механізми пасивної або активної динамічної взаємодії з іншими об’єктами будь-яких класів шляхом запису у вхідні властивості об’єкта-приймача посилання на вихідні властивості об’єкта-джерела та посилання на його метод ядра (для активної взаємодії).

Реалізація принципу сепарації інтерфейсу об’єкта дозволяє більш конструктивно підходити до створення програм та є основою для створення сполук об’єктів.

Реалізація принципу внутрішньої активності об’єкта дозволяє отримати такий позитивний ефект:

- об’єкт стане більш функціональними та автономними;
- об’єкт отримає властивість активності, поєднуючи властивості структур даних та функцій;
- зменшаться витрати на використання об’єкта в декількох програмах;
- зменшиться кількість помилок.

Реалізація принципу транзакційності зміни об’єкта дозволяє контролювати стан об’єкта та коректність вхідних даних, а також зменшує кількість помилок, пов’язаних з використанням неадекватних вихідних значень об’єкта.

Найбільш суттєвим принципом АДС-технології є сполуки об’єктів. При цьому кожний об’єкт може бути:

– об’єктом-джерелом, якщо він містить тільки методи отримання адреси вихідних властивостей для сполучення з ним об’єктів-приймачів;

– об’єктом-приймачем, якщо він містить тільки конектори для сполучення з вихідними властивостями об’єктів-приймачів;

– транзитним об’єктом, якщо він виступає в ролі джерела та приймача.

Активна сполука дозволяє об’єкту-приймачу викликати методи ядра об’єктів-джерел для переведення їх в адекватний стан на всю глибину ланцюжка сполуки для отримання актуальних значень їх виходів.

Для створення сполук об’єктів використовуються функції синтезу сполук, які є ключовими елементами АДС-технології. Сигнатура функції синтезу визначає формулу сполуки, а тіло функції фактично містить знання про структуру сполуки. Основними артефактами програми, створеної за АДС-технологією, є сукупність описів класів об’єктів та функцій синтезу сполук. Якщо певний набір об’єктів-приймачів і об’єктів-джерел разом з функціями синтезу сполук оформити у вигляді класу об’єктів, то отримаємо унікальний різновид композитних об’єктів-сполук, які характеризуються справжнім поліморфізмом, тому що в різні моменти часу об’єкт може мати різну структуру сполуки.

Виходячи з цього, можна сформулювати таке бачення процесу програмування з використанням АДС-технології:

– об’єкти можуть створювати динамічні сполучення шляхом з’єднання вихідних властивостей одних об’єктів з вхідними властивостями інших об’єктів, а також отримувати можливість активації сполученого об’єкта;

– будь-яка програма може бути побудована у вигляді сполук об’єктів;

– процес розробки програми можна звести до розробки класів та синтезу сполук об’єктів; цей процес можна візуалізувати в інтегральному середовищі розробки;

– один об’єкт в різні моменти часу виконання програми може брати участь в різних сполуках, отже, з одних й тих самих об’єктів можна динамічно під час виконання програми синтезувати різні сполуки;

– сполуки об’єктів можна оформляти у вигляді класів сполук, які можуть з’єднуватися з іншими сполуками, утворюючи складні поліморфні конструкції;

– можливе створення інтерактивних програм, в яких користувачі самі синтезуватимуть потрібні сполуки для розв’язування своїх задач або використовуватимуть інтелектуальний інтерфейс для автоматичного синтезу потрібної сполуки за заданою постановкою задачі.

Таким чином, експерименти із застосування АДС-технології на мові *C++* довели можливість її використання в існуючих мовах програмування та її практичну ефективність.

Перспективними напрямами досліджень з розвитку АДС-технології є такі:

– розробка теоретичних основ проектування схем сполук об’єктів;

– створення мови опису схем сполук об’єктів для їх динамічного синтезу;

– розробка методу синтезу потрібної схеми сполуки за заданою постановкою задачі;

– дослідження шляхів створення програм з можливістю адаптації до умов експлуатації.

ЛІТЕРАТУРА

1. *Гради Буч*. Объектно-ориентированный анализ и проектирование с примерами приложений на C++. – М: Бином, 1998. – 560 с.

2. *Ирэ Пол*. Объектно-ориентированное программирование с использованием C++: Пер. с англ. – Киев: НИИПФ ДиаСофт Лтд, 1995. – 480 с.

3. *Фаронов В.В.* Программирование на языке C#. – СПб: Питер, 2007. – 240 с.

Солодовник В.І. (ВІТІ НТУУ „КПІ”)

ОБЛАСТІ ЗАСТОСУВАННЯ, ПЕРСПЕКТИВИ ТА ПРОБЛЕМИ ВПРОВАДЖЕННЯ БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖ

У сучасному динамічному світі часто виникає необхідність точного вимірювання параметрів середовищ, стану об’єктів, вивчення такого роду явищ, безпосередня участь і присутність людини в яких утруднена чи зовсім унеможливлюється через токсичність, жорсткі температурні режими або навіть загрозу життю. Для спрощення отримання відомостей з очевидним нехтуванням проблем важкодоступності та агресивності досліджуваних середовищ з поступовою відмовою від гомоцентричної моделі збору даних створені бездротові сенсорні мережі, розвиток яких відбувається швидкими темпами [1].

Бездротова сенсорна мережа (БСМ, *WSN − wireless sensor network*) − це бездротова система, що представляє собою розподілену мережу мініатюрних обчислювально-комунікаційних пристроїв з автономним джерелом живлення, здатну до самоорганізації та стійку до відмови окремих елементів. Вузли такої системи транслюють повідомлення одне через одного, забезпечуючи значну площу покриття при малій потужності передавача.

БСМ складаються з мотів, оснащених сенсорами і прийомопередавачами сигналів, що працюють у радіодіапазоні. Частіше за все використовуються датчики температури, тиску, вологості, місця розташування, освітленості, рівня вібрації, рідше − магнітоелектричні, хімічні, звукові. Набір застосовуваних датчиків залежить від функцій, виконуваних БСМ [2].

БСМ базуються на технології із трьох різних дослідницьких областей: сенсорне сприйняття, комунікації й комп'ютерна обробка. Напрямки використання БСМ обмежуються виключно людською фантазією, отож, перспективність та доцільність використання сенсорних мережних технологій очевидна. Наповнення навколишнього середовища гетерогенними сенсорами приведе до формування повноцінної *PAN* (*personal area network*) – „мережі персонального простору”. Це значить, що всі прилади, використовувані людьми, почнуть прозоро для людини взаємодіяти між собою. Області застосування БСМ розбиваються на три категорії: простір моніторингу, предмети моніторингу, моніторинг взаємодії предметів між собою та з навколишнім середовищем.

Ряд проблем БСМ: уніфікація механізмів й протоколів зв’язку між сенсорами, стандартизація устаткування та програмного забезпечення, вироблення методики збору датчиків після використання, дистанційне керування вузлами мережі, виявлення інформаційних шляхів до базової станції, здатність до самовідновлення у випадку виявлення помилок, підвищення надійності роботи в умовах екстремальних температур, високої вібрації й значного рівня радіочастотних перешкод, обмеженість ресурсів: швидкість обробки даних, обсяг пам'яті, пропускна здатність комунікацій, зниження вартості розгортання й супроводу вузлів БСМ [3]. Експоненційно зменшуючи розміри та вартість напівпровідникових пристроїв, дослідники використовуватимуть технологію сенсорних мереж для побудови сенсорів або датчиків, що вимірюють поля й сили у фізичному світі.

Висновки. БСМ можуть утворювати „інтелектуальне” середовище, здатне передбачати наші потреби й реагувати на поведінку людини, звільняючи від необхідності виконання рутинної, механічної роботи. Поєднання БСМ різного призначення забезпечить можливість формування більш цілісних інформаційних інфраструктур, що дозволить підвищити нашу продуктивність, збільшити безпеку, інформованість й ефективність у соціальному масштабі.

ЛІТЕРАТУРА

1. *Майская В. А.* Беспроводные сенсорные сети: малые системы – большие деньги. − Электроника: Наука, Технология, Бизнес № 2, 2005.

2. *Умнов А. Л., Головачев Д. А.,* Ковалев П. А., Шишалов И. С. Система сбора информации с узлов сенсорной сети. − Радиотехника. Нелинейный мир Т.2 № 4, 2005.

3. *Турута Е. Н., Мочалов В. А.* Проблемы проектирования отказоустойчивых сенсорных сетей // 2-я отраслевая НТК „Технологии информационного общества”. − М.:МТУСИ, 2008.

Сорока М.В. (ЦНДІ ОВТ ЗС України)

ВПЛИВ ІНФОРМАЦІЙНОЇ БОРОТЬБИ НА РОЗВИТОК АСУ

Вплив інформаційного протиборства на воєнне мистецтво останнім часом зростає. Розвинені країни світу приділяють велику увагу розробці інформаційної боротьби, а також системам комплексного захисту від неї. Кількість перспективних технологій, що знаходяться у розробці та у впровадженні, постійно зростає. В подальшому це може привести до беззаперечного панування на полі бою використанням небойових засобів. Визначення шляхів створення засобів інформаційного протиборства та інформаційного захисту в ЗС України потребує проведення додаткових наукових досліджень. Інформаційна боротьба є протиборчою стороною за завоювання переваги по кількості, якості і швидкості здобування інформації, її вчасному аналізу і застосуванню. Вона передбачає постійне вдосконалення інформаційних технологій з обов'язковим проведенням заходів по підвищенню їхнього захисту від впливу противника. Загальною стратегічною метою інформаційної боротьби є забезпечення переваги у вирішенні задач, що стоять, однією із сторін через досягнення переваги над протиборчою стороною на інформаційному рівні.

Оптимізація взаємовідносин різних цивілізацій, створення єдиного безпечного інформаційного простору в Україні, Європі та світі, а також освічення суспільства в галузі інформаційної безпеки, в тому числі, піклування про наявність достатніх і захищених інформаційних ресурсів і інформаційних потоків для підтримки життєдіяльності та життєздатності, стійкого функціонування і розвитку суспільства і держави та підтримання постійної готовності до адекватних дій в інформаційному протиборстві, ким би воно не було нав’язане, є частковими стратегічними цілями інформаційної боротьби.

Щодо досягнення часткових стратегічних цілей, вирішуються такі стратегічні завдання: прогнозування можливих негативних інформаційних дій на природу, людину, суспільство і державу; виявлення причинно-слідчих зв’язків фактору ризику і наслідків реалізації для суспільства і держави; прогнозування основних напрямків розвитку інформатизації в інтересах його безпеки; визначення співвідношення інформаційної дії інформатизації та безпеки природи, людини, групи, суспільства і держави; вироблення засобів протидії інформаційним небезпекам і загрозам, негативним інформаційним діям на індивідуальну та суспільну свідомість, психіку людей; забезпечення фізичної безпеки і нормального функціонування об’єктів інформаційних ресурсів; обмеження доступу до інформації, яка складає державну, воєнну, технологічну і комерційну таємницю. Відомо, що еволюція поглядів військових фахівців на зростаючу роль інформаційної боротьби призвела до появи нового явища – інформаційної війни, яка передбачає три стратегічні мети: у мирний час - електронне устрашіння; в загрозливий період - вибіркове і інтенсивне застосування електронних засобів проти інформаційних структур військового і громадянського призначення; під час військового конфлікту - масове застосування вогневих і електронних засобів по всім названим вище об'єктам. Суть цієї боротьби полягає в тому, щоб, скориставшись уразливими місцями системи управління, зв’язку, комп’ютерного забезпечення і розвідки противника, знизити ефективність їхньої роботи, в умовах дефіциту часу примусити противника до помилкових дій. Це дозволить своїм органам управління, використовуючи переваги в часі, випередити противника в оцінці стратегічної обстановки, прийнятті рішення, плануванні і в доведенні наказів до виконавців.

Варто відмітити, що тенденція зміни форм і способів інформаційної боротьби обумовлена розвитком інформаційної зброї. Теоретики відносять до цього виду зброї широкий спектр заходів і засобів інформаційного впливу на противника – від дезінформації й пропаганди до засобів радіоелектронної боротьби. Таким чином, інформаційна боротьба змінює не тільки форми і способи ведення воєнних дій, змінюється зміст самого поняття війни, стираються грані між воєнним і мирним часом, пропадає стале сприйняття поняття „театр воєнних дій”, ще більш зрощуються воєнні і мирні технології.

к.т.н. Субач І.Ю. (ВІТІ НТУУ „КПІ”)
Саєнко О.Г. (ВІТІ НТУУ „КПІ”)
Власенко О.В. (ВІТІ НТУУ „КПІ”)

РІШЕННЯ ЗАДАЧІ АНАЛІЗУ ДАНИХ ПРО ЗБОЇ В РОБОТІ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ШЛЯХОМ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ

Однією з основних задач, для якої використовуються методи інтелектуального аналізу даних (ІАД), є аналіз даних про аварії (збої) в роботі інформаційної мережі (ІМ). Останню можна розглядати як складну систему, що являє собою множину взаємозв’язаних компонентів (передавального обладнання, комутаторів тощо), кожний з яких може складатися з підкомпонентів.

У процесі функціонування вони можуть виробляти дані про помилки, які накопичуються в базі даних (БД) системи моніторингу ІМ. Аналіз показує, що записи БД, як правило, містять дату та час виникнення помилки, її джерело, а також код джерела, код помилки та, можливо, ваговий коефіцієнт, який характеризує ступінь її впливу на ситуацію в цілому. Обробка потоків даних про збої – складна задача, яку не можна розв’язувати вручну з огляду на наступні обставини:

великий розмір інформаційних мереж та різноманітність типів даних про аварії (збої), які виникають під час функціонування;

дефіцит часу на аналіз оператором даних про збій та прийняття рішення щодо його усунення;

динамічний характер розвитку інформаційних мереж, який впливає на характеристики послідовностей подій та не дає необхідного часу операторам для їх вивчення.

Таким чином, для аналізу збоїв у роботі інформаційної мережі доцільно застосовувати технології ІАД, предметом якого в цьому разі є послідовності помилок (збоїв) в роботі ІМ, які виникають одна за одною.

Знаходження закономірностей у послідовностях подій, які відбуваються в інформаційній мережі, представляє певний інтерес. При їх відшуканні можна з певною мірою впевненості прогнозувати появу подальших подій для прийняття більш своєчасних, обґрунтованих рішень.

Послідовністю називається упорядкована множина об’єктів, що містять транзакції БД. Для цього на цій множині задається відношення порядку. Транзакція БД містить певну послідовність, якщо об’єкти, що входять до неї, також входять у множину об’єктів транзакції зі збереженням відношення порядку. При цьому припускається, що між об’єктами послідовності можуть міститися інші об’єкти. Підтримкою послідовності є відношення кількості транзакцій, в яке входить послідовність, до загального числа транзакцій. Послідовність вважається частою, якщо її підтримка є не меншою, ніж задане користувачем значення. Таким чином, задача аналізу даних про збої в роботі ІМ зводиться до пошуку всіх частих послідовностей.

Для відомих методів рішення сформульованої задачі характерними недоліками є відсутність врахування рівня впливу подій, що відбуваються в ІМ, на ситуацію у цілому, а також значні часові витрати.

У доповіді розглядається методика рішення сформульованої задачі, яка дозволяє більш оперативно добувати нові знання про збої у функціонуванні ІМ, з урахуванням інформації про ступінь важливості подій, за рахунок уведення до їхнього опису вагових коефіцієнтів. Крім того, вона дозволяє скоротити об’єм обчислень шляхом відсіву неперспективних послідовностей-кандидатів. Це дозволяє отримати лінійну залежність часу роботи обчислювального алгоритму від кількості транзакцій, що містить БД системи моніторингу інформаційної мережі.

Танасієнко П. В.(ВІТІ НТУУ „КПІ”)
к.т.н. Нестеренко М. М.(ВІТІ НТУУ „КПІ”)

АНАЛІЗ ОСНОВНИХ ТИПІВ ВІРУСІВ В КОМП’ЮТЕРИЗОВАНИХ СИСТЕМАХ

Проблема безпеки інформації в період загальної інформатизації, широкого впровадження інформаційних технологій − одне із найгостріших питань сьогодення. Це пояснюється тим, що з кожним роком все збільшується число комп’ютерних злочинів, що може привести до підриву діяльності будь-якої організації. Тому питанням захисту інформації, аналізу основних методів та способів захисту інформаційних ресурсів та виявлення вразливих місць в комп’ютеризованих системах приділяється велика увага, як в нашій країні так і за кордоном.

На теперішній час основними джерелами загроз, які впливають як на цілісність так і на захищеність інформації, є комп’ютерні віруси. Основною властивістю комп’ютерних вірусів є саморозмноження. Тому процедура, що здійснює цю функцію, займає в алгоритмі вірусу центральне місце, всі інші функції (прояв, засоби маскування і т.д.) мають другорядне значення.

В свою чергу комп'ютерні віруси можна розділити на класи за деструктивно-класифікаційними ознаками, способами їх створення і знешкодження:

− за місцезнаходженням вірусів (файлові, бітові, файлово-бітові, пакетні, мережеві, віруси в структурі файлової системи, *WinWord*-віруси, *Windows*-віруси, *OS/2*-віруси, *Novell NetWare*-віруси, *BIOS*-віруси, *CD-ROM*-віруси);

− за способом зараження середовища перебування вірусів (резидентні, нерезидентні);

− за наслідками деструктивних дій вірусів (нешкідливі, не уразливі, уразливі, дуже уразливі);

− за особливостями алгоритму вірусу (*stealth*-віруси, *worm*-віруси, *companion*-віруси, *MtE*-віруси, *DIR*-віруси, *driver*-віруси, віруси-паразити, віруси-привиди, „троянські” програми, логічні бомби, комбіновані віруси та ін.);

− за способами знешкодження вірусів (знешкоджені однією антивірусною програмою (*AVO*-віруси) і знешкоджені кількома антивірусними програмами або *n*-комплектом антивірусів (*AVN*-віруси);

− за способом створення вірусів (створені ручними засобами розробки (*H*-віруси) і створені автоматизованими засобами розробки (*A*-віруси).

В таблиці 1.1 наведений процент найпоширеніших та найбільш шкідливих мережевих вірусів.

Таблиця 1.1

№ п/п	Назва шкідливої програми	Відсоток в загальному числі вірусних інцедентів
1.	*I-Worm.SoBig*	47,75%
2.	*I-Worm.Swen*	36,50%
3.	*I-Worm.Mimail*	6,50%
4.	*I-Worm.Klez*	2,52%
5.	*I-Worm.Lentin*	2,35%

Незважаючи на великі зусилля як теоретичного, так і практичного характеру щодо вирішення проблеми захисту інформації, його сучасний стан дуже далекий від будь-якого надійного розв’язання. Передові компанії світу, які займається забезпеченням безпеки комп’ютерних мереж і електронної пошти, звертають особливу увагу на розповсюдження комп’ютерних вірусів типу „троян”.

Згідно офіційної статистики за (2009 − 2010 роки) одну із перших позицій займають трояни сімейства *Trojan.Win32.Generic !BT* − троянська програма, призначена для зміни відповідностей доменних імен *IP*-адресами.

Другим у списку йде *Trojan-Spy.Win32.Zbot.gen*, відоме сімейство троянів для крадіжки даних. На третьому місці – *Trojan.Win32.Generic.pak. Cobra*, здатний вражати як 32-бітові, так і 64-бітні версії *Windows.*

Список із десяти найбільш популярних вірусів типу „троян" за серпень 2010 року наведено в таблиці 1.2.

Таблиця 1.2

№ п/п	Найбільш популярних вірусів типу „троян"	Статистики за 2009 − 2010 роки
1.	*Trojan.Win32.Generic!BT*	25.11%
2.	*Trojan-Spy.Win32.Zbot.gen*	4.23%
3.	*Trojan.Win32.Generic.pak!cobra*	3.61%
4.	*INF.Autorun (v)*	3.27%
5.	*Trojan.Win32.Generic!SB.0*	2.01%
6.	*BehavesLike.Win32.Malware (v)*	1.04%
7.	*Worm.Win32.Downad.Gen (v)*	0.96%
8.	*Trojan.Win32.Malware.a*	0.93%
9.	*Trojan.Win32.Meredrop*	0.92%
10.	*Exploit.PDF-JS.Gen (v)*	0.84%

В зв'язку з вище сказаним, комп'ютерні віруси типу „троян" потребують більш детального розгляду та удосконалення методів та способів їх виявлення та знешкодження.

Однією, з перспективних методик боротьби, що був запропонований американськими спеціалістами полягає в тому, щоб „маркувати" (помічати) трафік в реальному маштабі часу, в випадку виявлення аномальних явищ в мережі, а саме підвищене навантаження на апаратні ресурси або різкі скачки трафіку і.т.д.

Підвищене скупчення „маркованого трафіку" в тому чи іншому вузлі комп'ютерної мережі буде сигналом про небезпеку. Необхідно відмітити, хоча інноваційний антивірусний комплекс перебуває на ранній стадії розробки, але вже зараз він здатен виявляти деякі комп'ютерні віруси.

ЛІТЕРАТУРА

1. *Дибкова Л. М.* Інформатика та комп'ютерна техніка. − К.: Академвидав, 2007.
2. *Ярочкин В. И.* Безопасность информационных систем. − М., 2009.
3. *Chip*-Россия, № 5, 2002 – 12, 2003. − М.: *Vogel BURDA Communications*, 2009 – 2010.
4. *http://pcg.3dn.ru/news/gfi_v_avguste_trojany_prodolzhili_dominirovat_v_spiske_samykh_rasprostranennykh_ugroz/2010-09-07-21.*
5. *http://tsn.ua/nauka_it/borotisya-z-troyanami-budut-tsifrovi-murashki.html.*
6. *http://revolution.allbest.ru/programming/00013096_0.html.*
7. *http://ru.wikipedia.org/wiki.*
8. *http://www.securelist.com/ru/descriptions.*
9. *http://www.securitylab.ru/virus/1429.*
10. *http://www.softsoft.ru/search/9370/index.htm.*
11. *http://help-antivirus.ru/protectioninformation.*
12. *http://www.belvit.com/publ/10-1-0-143.*
13. *http://www.antivir.ru/main.phtml?/press-center/security&newser=0000001107267308.txt.*

Тимченко О.М. (ЦНДІ ОВТ ЗС України)
Іванов Б.П. (ЦНДІ ОВТ ЗС України)

ОЦІНКА ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ЗВ'ЯЗКУ І АВТОМАТИЗАЦІЇ УПРАВЛІННЯ

Розглядається методичний апарат оцінки ефективності систем зв'язку і автоматизації управління. Прогнози трансформування воєнних загроз України свідчать про потребу вдосконалення воєнно-технічної політики в забезпеченні національної безпеки держави. ЇЇ основним завданням на сьогодні є локалізація і воєнно-силова нейтралізація збройних конфліктів ще на ранній стадії. Для створення умов безпечного зв'язку та забезпечення захисту інформації в засобах зв'язку і автоматизації управління обов'язково передбачаються певні заходи безпеки, серед яких є організаційні та фізичні. Організаційні заходи є тією основою, що поєднує різні заходи захисту в єдину систему. На структуру і функціонування системи зв'язку впливають з одного боку вимоги до зв'язку, які ставляться системою управління військами, з іншого - параметри бойових дій, фізико-географічні умови бойових дій, можливості противника і т.ін. Тому система зв'язку і автоматизації управління повинна будуватися з урахуванням таких вимог:

1) бути завжди у високій бойовій готовності до забезпечення управління військами та зброєю;

2) мати необхідну стійкість, мобільність, перепускну здатність.

Оцінка ефективності складних систем, до яких відносяться системи зв'язку, є досить складним питанням. Існуючий методичний апарат дозволяє проводити оцінку окремо за декількома показниками, тому об'єктивно оцінити (порівняти) дві системи в цілому за ними досить важко. Це обумовлено тим, що складні системи є багатофункціональними і використання простих показників та критеріїв для оцінки їх ефективності часом просто неможливе. Виникає потреба у визначенні такого підходу щодо оцінки ефективності систем зв'язку, при якому використовувався б один комплексний показник.

Суть методу, який пропонується для оцінки ефективності систем зв'язку, полягає в наступному. Вибирається декілька показників ефективності, кожний з яких характеризує досліджувану систему з будь-якої конкретної сторони. Стосовно системи зв'язку в якості показників можуть бути використані: ймовірність передачі повідомлення, пропускна здатність, ймовірність виживання вузлів зв'язку, вартість експлуатації та утримання підрозділів та частин зв'язку та ін. Ступінь подрібнення залежить від можливої оцінки даної сторони показниками, які мають конкретний фізичний вимір. Якщо це зробити, тоді вводяться додаткові рівні, в результаті чого узагальнені показники утворюються за рахунок багаторазового згортання часткових показників. Щоб оцінити вплив сторін ефективності на комплексний показник, кожній стороні призначається певна "вага", так званий коефіцієнт відносної важливості. Тоді послідовність оцінки ефективності системи зв'язку така:

1. Вибрати показники оцінки ефективності системи зв'язку.
2. Визначити коефіцієнт відносної важливості кожного показника ефективності.
3. Оцінити найбільше значення показників і розрахувати їх значення для існуючої і перспективної систем.
4. Привести абсолютні значення показників до відносних. При цьому можливе отримання від'ємних значень, якщо показники перспективної системи погіршуються.
5. Скоректувати коефіцієнти відносної важливості і визначити їх суму.
6. Розрахувати коефіцієнт покращення для кожного показника і всієї системи в цілому.
7. Провести аналіз отриманих результатів.

Запропонований підхід може бути використаний для оцінки ефективності не тільки систем зв'язку і автоматизації управління, а будь-яких складних систем. Для цього лише необхідно визначитися з системою показників та порядком їх ранжування.

Тищенко М.Г.(НУОУ)

МАТЕМАТИЧНА ФОРМАЛІЗАЦІЯ ЗАДАЧІ РАЦІОНАЛЬНОГО ВИБОРУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПІДРОЗДІЛУ ДИСТАНЦІЙНОГО НАВЧАННЯ НА ПРИКЛАДІ ВИБОРУ СИСТЕМИ УПРАВЛІННЯ НАВЧАЛЬНИМ ПРОЦЕСОМ

На сучасному етапі побудови системи дистанційного навчання у Збройних Силах України, важливо зосередити зусилля на рішенні задач, які є пріоритетними у цьому складному процесі [1]. Одним з таких питань є методологія створення підрозділів дистанційного навчання (ДН), як елементів майбутньої єдиної системи дистанційного навчання Збройних Сил України. Ця методологія має включати до себе методичний апарат визначення структури та розподілу функцій підрозділу ДН, а також проектування його інформаційної системи, яка складається з програмного, апаратного та кадрового забезпечення.

Умовно задачу вибору програмного забезпечення для підрозділу ДН можна поділити на низьку часткових задач, а саме:

– вибір системи управління навчанням (*LMS – Learning Management System*);

– вибір авторських засобів розробки;

– вибір засобів web-комунікацій.

Розглянемо задачу раціонального вибору програмного забезпечення підрозділу дистанційного навчання на прикладі вибору системи управління навчальним процесом.

Нехай заданий граничний обсяг фінансування F^*.

Існує множина варіантів *LMS*:

$$V = \{v_n\}, \quad n = \overline{1, N}, \tag{1}$$

де N – кількість варіантів *LMS*, що розглядається.

Причому вартість будь-якого з цих варіантів не перевищує граничного обсягу фінансування:

$$F(v_n) \le F^*.$$

Також задана множина показників *LMS* які найповніше характеризуватиме її придатність для ПДН:

$$P = \{p_i\}, \quad i = \overline{1, I}, \tag{2}$$

Необхідно вибрати раціональний за усій сукупністю показників варіант:

$$v_n \in V, \quad \left| C(v_n) = \max_P, \right. \tag{3}$$

де $C(v_n)$ – інтегральний показник, що характеризує придатність n–го варіанту *LMS* для ПДН.

Ретельний аналіз виявив наявність значної кількості показників, що характеризують *LMS*. Причому, вони мають складні ієрархічні зв'язки. Таким чином сформульовану задачу слід розглядати як задачу багатокритеріального вибору на просторі альтернатив. Одним з найбільш поширених методів розв'язання даного класу задач є метод аналізу ієрархій (MAI) розроблений американським математиком Т. Сааті [2].

Він являє собою систематичну процедуру для ієрархічного подання елементів, що визначають сутність будь-якої проблеми. MAI передбачає декомпозицію проблеми на усе більш прості складові частини і подальшу обробку по парних порівняннях послідовностей суджень особи, що приймає рішення. У результаті може бути виражений відносний ступінь (інтенсивність) взаємодії елементів в ієрархії.

Ці судження потім виражаються чисельно. Метод аналізу ієрархій включає процедури синтезу множинних суджень, одержання пріоритетності критеріїв і знаходження альтернативних рішень.

Алгоритм розв'язання зазначеної задачі вибору раціонального варіанту *LMS* для ПДН матиме наступний вигляд.

1. Сформувати ієрархічну систему показників, які найповніше характеризуватиме придатність *LMS* для ПДН:

$$P = \left\langle (p_{ij}, r_{ij-1}, r_{ij+1}) \right\rangle, \quad i = \overline{1,I}, \quad j = \overline{1,J}, \tag{4}$$

де $r_{ij\pm1}$ – відношення порядку для показника p_{ij}, причому:

$r_{ij\pm1} = 1$, якщо показник зв'язаний відношенням порядку з показником верхнього (нижнього) рівня ієрархії, інакше $r_{ij\pm1} = 0$;

I – максимальна кількість показників, що характеризують *LMS* на 1 рівні ієрархічної моделі;

J – глибина (кількість рівнів) ієрархії.

Крім того, показник відрізняються між собою за важливістю.

2. Задати вектор відносної важливості показників:

$$\Omega = \{\omega_{ij}\}, \ \sum_{i=1}^{I} \omega_{ij} = 1.$$

3. Здійснити оцінку придатності усіх варіантів *LMS* із (1) для ПДН за всіма показниками із (3):

$$o_{ij}^{n} = o(v_n, p_{ij}).$$

4. Знайти інтегральні оцінки придатності усіх варіантів *LMS* із (1):

$$O_n = f(o_{ij}^{n}).$$

При застосування МАІ $O_n \equiv C(v_n)$.

5. Сформувати вектор раціональних рішень як лексикографічно упорядковану множину зважених за оцінками варіантів:

$$V_{\text{р}} = \left\{ \left\langle v_n, O_n \right\rangle \right\}. \tag{4}$$

Право остаточного вибору належить особі, що приймає рішення.

Таким чином задача раціонального вибору програмного забезпечення підрозділу дистанційного навчання є актуальним науковим завданням.

Вибір решти раціональних компонентів, які входять до складу програмного забезпечення підрозділу ДН, також можливо здійснювати за допомогою запропонованого методичного підходу.

ЛІТЕРАТУРА

1. *Сучасні* технології дистанційного навчання в системі підготовки військових фахівців: світовий та український досвід, місце та роль в навчально-виховному процесі Національної академії оборони України, перспективи впровадження дистанційного навчання в ЗСУ. Шифр „Дистанція" : Підсумковий звіт про НДР / О. Ю. Пермяков, В. В. Рябцев, Д. Д. Доляновський та ін. / НАОУ. – Київ, 2009 р. – 108 с.

2. *Саати Т.* Аналитическое планирование. Организация систем / Т. Саати, К. Кернс; Пер. с англ. – М. : Радио и связь, 1991. – 224 с.

к.т.н. Ткаленко О.М. (ДУІКТ)

ОРГАНІЗАЦІЯ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СИСТЕМ КОМУТАЦІЇ

Технічна експлуатація засобів зв'язку – це комплекс організаційно-технічних заходів і практичних дій обслуговуючого персоналу по збереженню системи, підтримки її в діючому стані і забезпеченню готовності до надійної роботи. Вплив на технічний стан пристроїв зв'язку мають: температура, вологість, режим використання, зношення, старіння, кваліфікація обслуговуючого персоналу та інше. Ефективне функціонування телефонного зв'язку з заданою якістю обслуговування абонентів забезпечується технічною експлуатацією всього комплексу споруд телефонної мережі, до якого відносяться: абонентські пристрої, таксофони, абонентські та з'єднувальні лінії, системи комутації, системи електроживлення, системи технічної експлуатації. Важливою функцією технічної експлуатації та технічного обслуговування є етап уведення в експлуатацію систем. Сучасні системи комутації дозволяють створювати комбіновані міські/міжміські, сільські, установчі АТС, забезпечуючи операторам зв'язку можливість вибору гнучкого та масштабного рішення для надання широкого спектру послуг зв'язку.

Організація технічного обслуговування для різних систем різна. Для електромеханічних систем – схемно-вмонтована з набором різних комбінацій сигналізації: оптичної та звукової. Для АТС з програмним управлінням система автоматизована на досить високому рівні. В сучасних системах для досягнення ефективності експлуатації практично всі процеси контролю за станом апаратури і діагностики несправностей – автоматизовані, тобто передбачені на етапі створення системи. Ці процеси складають 50% і більше ресурсу програмного забезпечення.

Основними задачами технічної експлуатації засобів зв'язку на міських та сільських телефонних мережах є: забезпечення безперервної і високоякісної роботи та ефективності використання засобів зв'язку; утримання обладнання і спорудження засобів зв'язку у межах норм і вимог нормативно-технічної документації; зниження трудових і матеріальних затрат на технічну експлуатацію; підвищення якості обслуговування абонентів шляхом удосконалення експлуатації і впровадження нової техніки.

Таким чином, експлуатацію пристроїв зв'язку можна розглядати як систему, яка складається з двох різних за призначенням частин: застосування (підготовка обладнання до роботи в заданому режимі; виконання обладнанням роботи по встановленню зв'язку і передачі інформації; контроль і вимірювання стану каналів (абонентських та з'єднувальних ліній), а також режимів роботи основного і допоміжного обладнання) та технічна експлуатація.

Задача експлуатаційного управління полягає в тому, щоб забезпечити нормальну роботу системи зв'язку, її адаптацію до змін як зовнішніх, так і внутрішніх умов, її розвиток у кількісному та якісному відношенні. Все це передбачає управління ресурсами, адміністративне управління, технічне обслуговування, введення нових ресурсів. Експлуатаційне управління охоплює, крім вузлів комутації, баз даних та пунктів сигналізації ЗКС№7, також і інші компоненти мережі зв'язку. Ріст мереж зв'язку потребує покращення системи технічної експлуатації, яка дозволяє скоротити чисельність обслуговуючого персоналу при збереженні високих експлуатаційно-технічних характеристик. Науково обґрунтована організація технічного обслуговування дозволяє підтримувати рівень технічної надійності апаратури з передбаченою можливістю підвищення її за рахунок запобігання частини відмов шляхом своєчасного виявлення пошкоджень, оскільки, головною метою всієї експлуатаційної діяльності на телефонних мережах є забезпечення безперервної роботи засобів і споруджень зв'язку з необхідною якістю.

к.т.н. Ткаченко А.Л. (ВІТІ НТУУ „КПІ”)
Мазниченко Ю.А. (ВІТІ НТУУ „КПІ”)
Панченко І.В. (ВІТІ НТУУ „КПІ”)

МОДЕЛЮВАННЯ НЕЧІТКОГО РЕГУЛЯТОРА ПРИ ВИХІДНИХ РОЗ’ЄДНАНИХ НА ВІДРІЗОК 1-2а ТРИКУТНИХ ФУНКЦІЯХ ПРИНАЛЕЖНОСТІ МОДИФІКОВАНИМ МЕТОДОМ

Актуальність технології − нечіткого моделювання обумовлена тенденцією збільшення складності 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.

За методикою проектування структурна схема нечітких регуляторів (НР) складається з трьох блоків: блоку формувача величин рівнів відсікання А і В (блок 1), блоку порівняння величин рівнів відсікання А і В і розрахунку вихідної змінної (блок 2) і блоку нормування вихідної змінної (блок 3).

На основі викладеної методики проектується нечіткий регулятор, в якому блок порівняння відрізняється простотою і, головне, може використовуватися з різними формувачами. Розроблені раніше методики проектування нечіткого регулятора мали змінну структуру (при A<B та при A>B), даний тип нечіткого регулятора звільнений від цього недоліку. Модифікований метод проектування НР полягає у суттєвому спрощенні виведення загальної формули для нечіткого виводу, що дозволяє значно спростити обчислення абсциси „центру тяжіння результуючої фігури”.

$$u_c = \frac{\int_0^1 u\mu(u)du}{\int_0^1 \mu(u)du} = \frac{\frac{A}{2}\times x_1^2 + \frac{B}{2}\times(1-x_2^2)}{A\times x_1 + B\times(1-x_2)}$$

За допомогою інтерактивної системи MATLAB проектуємо математичну модель нечіткого регулятора, яка використовує алгоритм Мамдані („мінімаксний” метод), як алгоритм нечіткого виводу, логіка роботи якого показана на рис. 1.

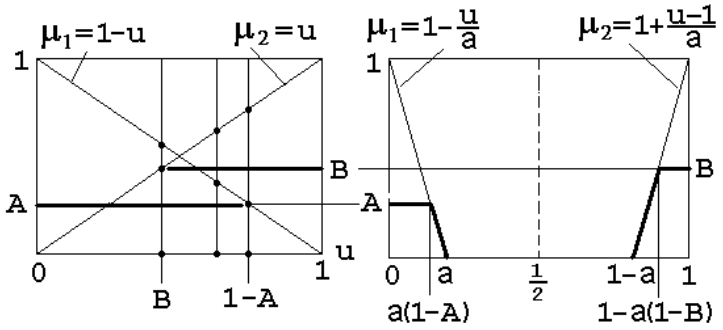


Рис. 1. Логіка роботи нечіткого регулятора для фіксованого моменту часу.

Таким чином викладені теоретичні положення і практична схема нечіткого регулятора з вихідними роз’єднаними на відрізок 1-2а трикутними функціями приналежності і вхідними трикутними функціями приналежності дають можливість використовувати такий регулятор в різних системах автоматичного управління, зокрема в електронних радіотехнічних системах, і шляхом настройки параметрів регулятора добиватися високої якості систем.

Ткачов П.О. (ВІТІ НТУУ „КПІ”)

ЗАХИСТ ІНФОРМАЦІЇ НА ОПТИЧНИХ НОСІЯХ ВІД НЕЛЕГАЛЬНОГО КОПІЮВАННЯ

У доповіді розглянуті методи та способи, які можуть бути використані для забезпечення захисту інформації, яке розповсюджується на оптичних носіях від нелегального копіювання. У роботі [1] наведені три методи реалізації такого захисту, які відбивають точку зору авторів на проблему у той час.

Метод 1. Захист інформації шляхом внесення змін у деякі управляючі службові сигнали, які записані на диск синхронно з основним потоком даних.

Метод 2. Захист інформації шляхом запису на попередньо підготовлений носій, поверхня якого містить низку дефектів, які не можна усунути фізично, та які заважають перезапису диску, але не заважають його зчитуванню.

Метод 3. Захист інформації, який базується на внесенні змін до файлової системи.

Наведені методи були всебічно проаналізовані та практично відпрацьовані. Як результат – була визнана їх не перспективність для практичного втілення, та був запропонований новий метод та різні способи його реалізації в залежності від типу оптичного носія.

Ідея полягає у наступному. Спочатку компакт-диски були призначені тільки для запису музики і тільки через певний проміжок часу були адаптовані для запису цифрового контенту довільної форми. Запис музики здійснюється двоканальним методом по 16 біт на канал із частотою 44,1 Кгц. Таким чином швидкість цифрового потоку при зчитуванні дорівнює 4x44100 = 176400 байт/сек. Довжина фізичного блоку даних або фрейму для формату CD-DA є 2352 байта. Якщо розділити 176400 на 2352, то отримуємо швидкість потоку даних 75 фреймів/сек. Адресація усіх фреймів у на диску здійснюється у форматі MM:SS:FF або MSF, де MM - хвилини (0-99), SS – секунди (0-59), FF – фрейми (0-74) . Адрес першого фрейму для інформаційної зони є 00/00/00. Зони Lead-In та Lead-Out теж мають свої визначені адреси у термінах MSF. Наприклад, останній фрейм у зоні Lead-In має адресу 99:59:74. Паралельно з адресацією у термінах MSF існує істотна адресація, де перший фрейм інформаційної області дорівнює 0, наступний 1 і так далі до 404849 номеру. Слід сказати, що між системами адресації існує взаємно однозначна залежність. Розмір інформаційної зони був обраний у 90 хвилин. Перший фрейм дорівнює 00/00/00, а останній 89/59/74. Або від – 150 до 404849. Зона Lead-In знаходиться у межах 90/00/00 – 99/59/74. Або від –45150 до – 151.

Для того щоб не можна було зробити точну копію компакт-диску, необхідною і достатньою умовою є умова, щоб копія хоч би на один біт відрізнялася від оригінала, та існував алгоритм, який міг би виявити таку різницю. Чисельні експерименти виявили, що для розташування інформації в інформаційній зоні використовується адресна зона, яка починається не з 00/00/00, а із 00/02/00 (це фрейм з адресом 0). Виявилось, що інформаційна зона з адресами фреймів від –150 до –1 (зона pre-gap) практично не використовується і не переноситься на копію. На CD-DA ця зона містить двохсекундну паузу перед початком першого музичного треку, а для CD-DATA функціональність цієї зони не визначена.

Таким чином, базі цього винаходу була розроблена система захисту програмного забезпечення, яке розташоване на компакт-дисках типу CD-DATA від несанкціонованого копіювання [2].

ЛІТЕРАТУРА

1. *Ткачев П.А.* Защита информации на компакт-дисках от нелегального копирования и тиражирования. /Ткачев П.А., Синицкий А.Н. // Безопасность информации. – № 4(14) – 2000.

2. *Pavel Tkachev.* Storage medium. United States Patent. Patent No US 7,567,981 B2. / Pavel Tkachev (Kyiv, UA), Alexander Sinitsky (Kyiv, UA). – July 28, 2009.

Труш О.В. (ВІТІ НТТУ „КПІ”)
Борисов О.В. (ВІТІ НТТУ „КПІ”)

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ РЕЗЕРВУВАННЯ ІНФОРМАЦІЇ В СИСТЕМАХ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ДАНИХ

Однією з основних умов ефективного функціонування розподілених комп’ютерних систем є забезпечення необхідного рівня збереження їх функціональних і інформаційних ресурсів. Різке збільшення об’ємів оброблюємих даних і необхідність їх сумісного використання великим числом споживачів приводять до необхідності вводити до складу комп’ютерних систем підсистеми розподіленого зберігання даних, які найчастіше будуються на устаткуванні мереж зберігання даних (МСД) (англ. SAN – Storage Area Network). Застосування методів розподіленого зберігання даних породжує ряд нових завдань забезпечення безпеки інформації, але одночасно і розширює можливості створення нових засобів і механізмів захисту. Зокрема, засоби розподіленого зберігання даних можуть бути ефективно застосовані для підвищення показників доступності і цілісності інформаційних ресурсів комп’ютерних систем різного призначення: інформаційних, управлінських, обчислювальних і контрольно-вимірювальних.

Класичні підходи до забезпечення високого збереження інформаційних масивів засновані на методах ідентичної або неідентичної надмірності, відповідно до яких, як правило, для конкретної системи вибирається ефективна стратегія резервування. Безумовною гідністю більшості класичних методів резервування є їх простота, недоліками – високий ступінь дублювання інформації, неефективне використання ємкості магнітних носіїв, у ряді випадків – незадовільний великий час відновлення системи.

Системи розподіленого зберігання даних відкривають можливості для широкого використання методів відновного резервування, які поєднують надмірність з введенням аналітичних залежностей між блоками даних, що представляють інформацію, яка зберігається. Пропонується трирівнева модель забезпечення безпеки резервування, яка опирається на технічні можливості сучасних МСД. Оскільки пропонований підхід орієнтований на широкий клас розподілених систем, то в загальному випадку найважливішою вимогою до системи буде максимізація коефіцієнта готовності; далі за умови забезпечення заданого рівня доступності – вимога гарантій якості інформації, зокрема цілісності, і лише при виконанні цієї умови – реалізація певної політики управління доступом, включаючи забезпечення таємності.

Таким чином, мінімальною вимогою до системи є забезпечення заданого рівня доступності функціональних і інформаційних ресурсів. Підсистема забезпечення доступності ресурсів утворює перший рівень моделі. Необхідними умовами його реалізації є введення в систему:

1) засобів контролю і діагностики стану ресурсів системи;

2) оперативних резервів і засобів відновлення системи;

3) механізмів оцінки досягнутих параметрів доступності, які мають зворотний зв’язок з механізмами відновлення. Пропонується інтерполяційний метод безпечного розміщення інформаційних масивів в МСД, який складається з k пристроїв зберігання.

Також розроблені узагальнені алгоритми прямого і зворотного перетворень, які реалізують запропонований метод. Головними особливостями запропонованих алгоритмів є:

− представлення n-бітових блоків масиву у вигляді елементів кінцевого поля $GF(2^n)$, використання операцій в полі $GF(2^n)$ для перетворення блоків масиву;

− застосування процедури обчислення до „пробних точок” полінома над полем $GF(2^n)$ для отримання представлень блоків даних, які підлягають розміщенню на засобах зберігання (перетворення A);

− використання схеми Руффіні – Горнера множення багаточленів над полем $GF(2^n)$;

− побудова інтерполяційного полінома по Лагранжу $GF(2^n)[X]$ та обчислення коефіцієнтів полінома для отримання представлень блоків даних, які складають початковий масив (перетворення A^{-1});

− ідентифікація засобів зберігання, на яких розміщуються перетворені блоки даних, елементами кода Грея порядку n з метою скорочення обчислювальної складності перетворень A і A^{-1}.

Інтерполяційні методи розміщення даних вимагають реалізації методів контролю якості інформації на всіх етапах перетворення і відновлення інформації. Поняття якості інформації – багатоаспектне, зазвичай його прийнято характеризувати термінами „достовірність", „збереження", „логічна несуперечність", „цілісність", „актуальність" і іншими, набір яких сильно залежить від наочної області. Часто ці показники формулюються замовником інтуїтивно або керуючись дуже загальними поняттями міжнародних стандартів ISO 9000, ISO 9001, ISO 17799 і не визначаються кількісно. Очевидною умовою досягнення більшості вимог є забезпечення цілісності даних. Рішення цієї задачі ретельно відпрацьоване на елементарному рівні, але в МСД з'являється складне завдання синтезу схеми контролю достовірності на базі елементарних методів (циклічні надмірні коди, криптографічні хеш-функції і ін.), яка додатково повинна задовольняти вельми жорстким вимогам ефективності. Підсистема забезпечення якості інформації формує другий рівень моделі. Необхідними компонентами підсистеми є:

1) механізми контролю системних умов, які забезпечують можливість досягнення заданого рівня якості;

2) виконавчі механізми (наприклад, схема забезпечення цілісності);

3) механізми підсумкової оцінки якості інформації, які мають зворотний зв'язок з регулюючими і старанними механізмами.

В окремих випадках до проектованої системи висуваються вимоги по захисту від несанкціонованих дій (НСД) по відношенню до інформації і забезпеченню секретності (конфіденційності) інформації. Ідеальною умовою функціонування системи є постійна можливість доступу будь-якого користувача до будь-якого ресурсу системи (зрозуміло, якщо доступ не заборонений по вимогам безпеки інформації). Тому разом із забезпеченням високої доступності необхідне і вирішення до деякої міри „зворотного" завдання – обмеження і запобігання небажаному доступу до інформаційних ресурсів. В цьому випадку додатково потрібна підсистема управління доступом, здатна реалізувати специфіковану власником системи (власником ресурсів) політику управління доступом.

Управління доступом в складному розподіленому середовищі, прикладом якого є системи розподіленого зберігання даних, вимагає деякої адекватної формалізованої моделі. Класичні суб'єктно-об'єктні моделі з багатьох причин виявляються незручні для завдання і опису правил доступу в цих умовах. Застосування яких-небудь моделей або їх комбінацій для кожної конкретної системи завжди залежить від наочної області і відповідних нею цілей забезпечення безпеки.

Таким чином, пропонований підхід може послужити основою розробки принципово нових методів забезпечення стійкості засобів захисту інформації в розподілених комп'ютерних системах при підвищених системних вимогах до функціональної і інформаційної безпеки.

ЛІТЕРАТУРА

1. *Кульба В.В., Ковальовський С.С., Шелков А.Б.* Достовірність і збереження інформації в АСУ. 2-е видавництво Серія „Інформаційні технології". – М.: СИНТЕГ, 2003. – 500 с.

2. *Запечников С.В.* Исследование и разработка алгоритмов обеспечения безопасности доступа к информации в сетях хранения данных. – М.: МИФИ, 2003. – 195 с.

3. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие для вузов. – М: Горячая линия –Телеком, 2004. – 280 с.

Фесьоха В.В. (ВІТІ НТУУ „КПІ”)

ТЕСТОВЕ ДОСЛІДЖЕННЯ СТІЙКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДО РУЙНІВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ, СПРЯМОВАНИХ НА ВИКОРИСТАННЯ ПОМИЛОК УПРАВЛІННЯ ПАМ’ЯТТЮ

Загальновизнано, що широкомасштабні програмні атаки створюють серйозну загрозу нашому суспільству, оскільки його благополуччя багато в чому залежить від надійного функціонування комп’ютерних систем (КС). Основною причиною існування загроз безпеці КС є помилки системних програмістів на етапах створення програмного забезпечення (ПЗ), оскільки на їх основі виникають вразливості ПЗ[1]. Існують два основних підходи (методи) до виявлення невідомих вразливостей, спричинених помилками управління пам’яттю[2]: статистичний аналіз (початкового або двійкового коду) потенційно вразливої програми; динамічний або тестовий аналіз потенційно вразливої програми.

Статистичний аналіз на практиці вимагає наявності початкового коду програми. При цьому основною процедурою є „ручний” перегляд початкового коду вразливої програми на предмет наявності вразливих кодових інструкцій. Під час статистичного аналізу програма, яка досліджується, не виконується. Під час динамічного (тестового) аналізу, навпаки, передбачається, що програма, яка досліджується, не виконується. Виявлення вразливостей при цьому здійснюється шляхом передачі програмі, яка досліджується, тестових повідомлень (руйнівних інформаційних впливів) і аналізу реакції поточної програми на ці повідомлення. Динамічний аналіз може виконуватись (і, як правило, виконується) і без доступу до початкового коду програми, яка досліджується, на відміну від статистичного аналізу.

Аналіз сучасних засобів тестового дослідження стійкості ПЗ до руйнівних інформаційних впливів на зміст оперативної пам’яті, таких як *Autodafe fuzzer*, *Sulley fuzzer Peach fuzzer*, показав недостатню їх розвинутість в аспекті застосування до з’ясування природи виявлених вразливостей (до пост–мортен аналізу об’єкта тестування), оскільки вони передбачають досить „вузький” підхід до процесу дослідження вразливостей на етапі, коли відбувається аварійне завершення виконання програми – „жертви”[2,3,4].

Доцільним напрямком підвищення стійкості ПЗ до руйнівних інформаційних впливів пропонується удосконалення динамічного аналізу захищеності ПЗ на основі технологій виявлення спроб використання помилок управління пам’яттю (*StackGuard*, рандомізації адресного простору (РАП), повного захисту від помилок управління пам’яттю) алгоритму РАП, який надасть змогу отримати детальну інформацію про цільову атаку, зокрема адресу враженого буфера та адресу точки виклику потенційно небезпечної зовнішньої функції, оскільки серед цих технологій захист від найширшого спектру атак при низьких накладних витратах забезпечує РАП. Більше того, на відміну від технології повного захисту від використання помилок управління пам’яттю, її застосування не стискається з проблемою забезпечення зворотної сумісності. Алгоритм РАП базується на спостереженні, що всі відомі способи використання помилок управління пам’яттю включають модифікацію деяких покажчиків, при чому нові значення цих покажчиків повинні міститись у повідомленні, що переносить атаку. На цій основі є доцільним застосування цього алгоритму, який передбачає дослідження адресного простору процес–жертви з метою ідентифікації його області, яка містить пошкоджений покажчик[5]. Запропонований алгоритм дозволить автоматично визначити розташування вразливих елементів двійкового коду цільового ПЗ та ідентифікувати вхідне повідомлення, через яке можна активізувати виявлену вразливість.

ЛІТЕРАТУРА

1. *Liang05automated*;
2. *Хогланд Г.*, Мак–Гроу Г. Взлом программного обеспечения: анализ и использование кода.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2005;
3. *Касперски К*. Фундаментальные основы хакерства. Искусство дизассемблирования.–М.: Солон, 2005;
4. *Buffer* Oerflows in 10 Easy Steps/ - SPI Labs, 2006;
5. *Канер С*. Тестирования программного обеспечения: Пер. с англ.- К.: ДиаСофт.

к.т.н. Хлапонін Ю.І. (ВІТІ НТУУ „КПІ”)
Мальцева І.Р. (ВІТІ НТУУ „КПІ”)

АНАЛІЗ СИСТЕМ УПРАВЛІННЯ ІДЕНТИФІКАЦІЙНИМИ ДАНИМИ КОРИСТУВАЧІВ ВИРОБНИЦТВА ПРОВІДНИХ СВІТОВИХ КОМПАНІЙ

Сьогодні практично будь-яка компанія чи державна організація в тій чи іншій мірі використовує інформаційні технології. Частіше за все ресурси корпоративної інформаційної системи є більш цінними активами, ніж будинки, обладнання чи ті ж самі комп’ютери, на яких зберігається інформація. Тому для захисту інформації від несанкціонованого доступу у великих і середніх компаніях з метою підвищення ефективності бізнес-процесів, забезпечення конфіденційності персональних даних і зниження витрат на управління ідентифікацією, необхідне впровадження спеціалізованих систем – Identity and Access Management (систем управління ідентифікаційними даними або СУІД). Практично всі визнані світові лідери в області IT готові запропонувати програмні засоби для управління ідентифікаційними даними як окремо, так і в складі комплексних рішень з управління доступом і IT-Інфраструктурою в цілому .

На думку аналітиків Gartner Group (див. 2009 Gartner UP MQ) Magic Quadrant for User Provisioning, рішення Oracle Identity Management є лідерами серед рішень подібного класу. Компанії Sun Microsystems, IBM Tivoli продовжують домінувати на ринку СУІД. Не відстають за лідерами також Novell і Courion. Замикають список компанії Microsoft, Hewlett Packard, BMC Software, Siemens, M-Tech і Beta Systems.

Oracle Identity Manager легко інтегрується з іншими засобами, що входять у сімейство продуктів Identity and Access Management (IAM), має потужні засоби рішення наступних завдань:

– управління ідентифікаційними даними користувачів і їхнім доступом до ресурсів;
– розробка нових адаптерів (конекторів) до цільових систем;
– моніторинг і аудит системи, у тому числі на певний момент часу в минулому.

Рішення **Sun Java System Identity Manager** добре себе зарекомендувало на ринку засобів класу Identity Management (IdM), і вже тривалий час удостоюється високих оцінок різних аналітичних агентств. У його основі лежить безагентна модель управління ресурсами (цільовими системами) і розподілене зберігання ідентифікаційних даних (атрибутів користувачів) без створення метакаталогів. Разом з тим при реалізації даної моделі не вдалося повністю відмовитися від центрального сховища (репозиторія), а також безагентного управління таким ресурсом, як, наприклад, служба каталогів Microsoft AD.

Корпорація **IBM** пропонує широкий спектр продуктів і рішень для управління безпекою. Вони дозволяють контролювати, адаптувати й адмініструвати ресурси й процеси для захисту інформаційних систем і одночасно забезпечувати відповідність постійно мінливим потребам бізнесу компанії.

Ринок рішень УІД у світі росте випереджальними темпами в порівнянні з показниками IT-ринку, як і ринок засобів забезпечення інформаційної безпеки (ІБ) у цілому. Згідно із прогнозом аналітичної групи IDC, в 2010 р. загальносвітовий обіг рішень на основі СУІД перевищить 5 млрд. дол. За результатами досліджень IDC, в провідних світових компаніях вже сьогодні на закупівлю програмного забезпечення УІД виділялося 30 % від загальних фінансових витрат на інформаційну безпеку (ІБ).

Проведений аналіз надає можливість керівництву компаній, організацій та державних установ зробити свій вибір на користь одного з виробників систем управління ідентифікаційними даними (СУІД). СУІД є не тільки необхідним інструментом ефективної організації управління інформаційними ресурсами та сприяє захисту та розвитку бізнесу, а й відповідає вимогам державних регуляторів щодо розмежування доступу в інформаційних системах органів державної влади .

к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)
Головко О.О. (ВІТІ НТУУ „КПІ”)

ОЦІНКА ОБ’ЄКТІВ ПРОГРАМНО-ІНІЦІЙОВАНИХ АТАК

Однією з можливих форм негативного інформаційного впливу на інформаційно-телекомунікаційну систему є створення умов для масової відмови обчислювальних процесів інформаційних служб, працюючих у складі її вузлів. Це досягається шляхом нав’язування обчислювальним процесам інформаційних служб, які виступають об’єктами атаки, спеціальної послідовності даних (вектор атаки) на основі використання засобів віддаленої міжпроцесної взаємодії.

Для ефективної реалізації інформаційного впливу суб’єкт атаки повинен мати відомості для визначення цілей програми атаки. Отримання таких відомостей є результатом перевірки працездатності (наявності) обчислювального процесу інформаційної служби на вузлах інформаційно-телекомунікаційної системи, а накладні витрати, які мають місце у ході перевірки, прийнято розглядати в межах етапу інформаційної підготовки атаки.

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. При цьому матриця накладних витрат при переході до перевірки наступного з множини об’єктів є відомою, наприклад, час переходу. У загальній постановці рішення задачі комівояжера є порядок перевірки всіх об’єктів з мінімальним значенням цільової функції. Всі варіанти „обходу” об’єктів визначаються повним перебором, але для практичного застосування це не є ефективним, враховуючи те, що знаходження оптимального варіанту перевірки об’єктів атаки здійснюється, як правило, в умовах часових обмежень.

Одним з можливих напрямків вирішення науково-практичної задачі планування перевірки об’єктів атаки полягає у введенні до задачі комівояжера та її цільової функції показника багатокритеріальної оцінки об’єкта атаки, яка формується на основі значень його кількісних та якісних характерних ознак. В подальшому цю оцінку будемо інтерпретувати як “показник важливості об’єкта атаки у складі інформаційно-телекомунікаційної мережі”. Схематичне представлення задачі – зважений неорієнтований граф, в якому вага ребра це показник часу переходу між перевірками об’єктів, вага вершини – важливість потенційного об’єкта атаки.

Доповідь присвячена висвітленню варіанта багатокритеріальної оцінки об’єкта атаки за кількісними та якісними критеріями на основні адитивного показника. До розгляду пропонуються наступні питання:

– вибір та обґрунтування характерних (класифікаційних) ознак;
– вибір та обґрунтування критеріїв оцінки;
– вимоги до процедури визначення ваги критеріїв оцінки експертним шляхом;
– вимоги до розробки алгоритмів визначення коефіцієнтів відповідності об’єкта атаки критеріям оцінки на основі аналізу наявних даних;
– вимоги до розробки алгоритмів обчислення багатокритеріальної оцінки об’єкта атаки.

При виборі сукупності характерних ознак об’єкту атаки акцентується увага на класифікації відомостей, які можуть бути отримані з загально доступних джерел. В загальному можна виділити такі групи відомостей: адміністративні(країна, провайдер, організація), технічні(доменне ім’я, програмне забезпечення та ін.).

Таким чином багатокритеріальна оцінка об’єкта програмно-ініційованих атак дозволить більш гнучко здійснювати пошук оптимального варіанту перевірки об’єктів, за рахунок врахування значення об’єкту для успішного здійснення впливу на інформаційні системи.

к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)
Гуреєв Ю.В. (ВІТІ НТУУ „КПІ”)

ОРГАНІЗАЦІЯ ПАРАЛЕЛЬНОГО ПОШУКУ ОБ’ЄКТІВ АТАКИ

Реалізація програмно-ініційованої атаки на обчислювальний процес інформаційної служби потребує отримання відомостей про його наявність (працездатність) у складі вузлів інформаційно-телекомунікаційної системи. Дані про наявність (працездатність) обчислювального процесу (об’єкт атаки) певного виду та версії є результатом спостереження передбаченої реакції на передачу йому деяких тестових даних. У контексті впровадження негативного впливу на інформаційно-телекомунікаційну систему інтерес представляє масовий характер реалізації програмно-ініційованих атак на множину обчислювальних процесів певної інформаційної служби, що обумовлює відповідну складність практичного вирішення задачі пошуку об’єктів атаки.

У загальному випадку постановка задачі пошуку об’єктів атаки відноситься до класу задач про комівояжера, базова ідея якої полягає у знаходженні оптимальної послідовності проходження (відвідування, перевірки) об’єктів будь-якої природи, керуючись результативним значенням цільової функції для кожного варіанта проходження з множини можливих. Схематична інтерпретація задачі – пересування маркера, який відповідає виконанню переходу, між вершинами (об’єкти) графу зі зваженими ребрами (перехід від об’єкта до об’єкта зі значеннями накладних витрат на виконання переходу). Обчислення цільової функції зводиться, як правило, до підсумовування ваг переходів. Передбачається існування зваженого переходу будь-якими двома вершинами графу, а також одноразове „відвідування” кожної вершини.

Пошук об’єктів атаки вимагає врахування наступних умов:

– можливі обмеження загального часу на виконання пошуку об’єктів атаки;

– значна кількість вузлів системи, які підлягають тестуванню на наявність обчислювального процесу – об’єкта атаки.

На практиці, як правило, дотримання обох умов при вирішенні задачі про комівояжера не може бути досягнуто: по-перше, значна кількість вершин графу обумовлює відповідну потужність множини варіантів їх проходження; по-друге, сума часових витрат на отримання значення цільової функції для всіх варіантів повного перебору значно перебільшує допустимий загальний час, що надається на пошук об’єктів атаки.

Одним з можливих шляхів практичного вирішення задачі є розподілення частин роботи щодо пошуку об’єктів атаки між кількома виконуючими пристроями та їх паралельне виконання. Центральним моментом організації паралельного пошуку об’єктів атаки є створення програмного забезпечення централізованого управління декількома виконуючими пристроями.

Таким чином, програмне забезпечення організації паралельного пошуку об’єктів атаки повинно відповідати наступним вимогам:

по-перше, можливість внесення змін в конфігурацію та/або вибору режиму роботи виконуючих пристроїв, що використовуються в програмному забезпеченні;

по-друге, наявність централізованого сховища даних для збереження первинної інформації яка надходить від виконуючих пристроїв в результаті пошуку з можливістю подальшої обробки;

по-третє, подальша обробка інформації зі сховища даних з використанням відповідних математичних методів;

четверте, інтерфейс користувача призначений для візуалізації роботи програмного забезпечення, централізованого управління роботою всіх взаємодіючих модулів, конфігурування виконуючих пристроїв, внесення змін в налаштування.

к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)
Редзюк Є.В. (ВІТІ НТУУ „КПІ”)

ІНФОРМАЦІЙНА МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ АДМІНІСТРАТОРА ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

Діяльність адміністратора безпеки локальної обчислювальної мережі (ЛОМ) в основному зводиться до вирішення наступних класів задач:

– моніторинг мережі і своєчасне виявлення недоліків, що стосуються топології мережі та підтримка в робочому стані мережевих пристроїв;

– визначення та усунення проблем, що стосуються роботи окремих вузлів мережі, зокрема серверів та функціонування їх програмного забезпечення;

– керування доступом до поділюваних ресурсів.

Об’єм інформації, який потрібно обробити адміністратору ЛОМ, значно перевищує допустимий об’єм, який він може обробити за відведений для прийняття рішення час. З цього випливає, що час реакції відповідної посадової особи на певну загрозу безпеці ЛОМ не дає змогу ефективно реагувати на події внаслідок значного інформаційного навантаження. Для зменшення цього навантаження на адміністратора та якомога швидшого реагування на різного типу події, повинне бути передбачене формування інформаційної моделі (ІМ).

Інформаційна модель – система сигналів, повідомлень, графічних об’єктів, елементів фізичної та/або логічної структури, що свідчать про динаміку об’єкта управління, умови зовнішнього середовища та стан самої системи управління [1].

Інформаційна модель об’єкта повинна бути представлена у вигляді інформації, що описує істотні для неї параметри та змінні, зв’язки між ними і дозволяє шляхом подачі на модель інформації про зміни вхідних величин моделювати можливі стани об’єкта.

Для побудови ІМ ЛОМ необхідно сформувати базу відомих порушень і подій із заздалегідь підготовленими варіантами для прийняття рішень при їх виявленні. Після ідентифікації порушень (подій) необхідно проводити пріотеризацію вхідної черги повідомлень згідно з умовами роботи користувача. В залежності від встановлених обмежень можливо отримати відповідні варіанти обробки подій, відомості про які надходять через чергу інформаційних повідомлень.

Враховуючи особливості роботи адміністратора ЛОМ, потрібно створити систему кодування повідомлень, але таким чином, щоб кількість символів у таблиці кодів була легко запам’ятовуваною і посадова особа мала можливість без труднощів її відтворювати.

Повинна мати місце ідеалізація об’єкта, сутність якої полягає у визначенні, які саме риси та властивості об’єкта є суттєвими для розв’язання поставленої задачі, впливають на результат рішення і мають бути відтвореними в моделі, а які риси та властивості є несуттєвими і при побудові моделі можуть не враховуватися. На основі цього необхідно розробити ергономічний дизайн інтерфейсу моделі [2], інформаційні елементи якого просто і змістовно відображали б динаміку стану робочого середовища адміністратора ЛОМ.

В доповіді пропонуються до розгляду основні принципи побудови інформаційної ІМ ЛОМ з урахуванням пріотеризації повідомлень про події та дотримання вимог ергономіки.

ЛІТЕРАТУРА:

1. *Козак Ю.А., Орлова Е.Ю., Кучерявый Д.Ю.* Принципы и методы создания информационных моделей в автоматизированных системах управления. //Тр. Одесск. политехн. ун–та: Научн. и практ. сб. по техн. и естетств. наукам – Одесса. – 2003. – 493 с.

2. *Введение* в эргономику, М., 1974; *Зинченко В. П., Мунипов В. М., Смолян Г. Л.*, Эргономические основы организации труда, М., 1974. – 645 с.

к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

АЛГОРИТМІЗАЦІЯ ЗАВДАНЬ ВПЛИВУ НА ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНУ СИСТЕМУ

Сучасне розуміння призначення, мети та завдань інформаційної боротьби у кіберпросторі ґрунтується на знанні механізмів впливу на роботу транскордонних інформаційно-телекомунікаційних систем (ІТС), загальними рисами яких є:

– дії, які виконуються з метою підготовки та реалізації впливу, мають суб’єктивну природу, що обумовлює їх спланований характер з елементами прийняття рішень;

– наявність недоліків системного та прикладного програмного забезпечення (ПЗ), які можуть бути використані для втручання в нормальну роботу обчислювальних процесів ІТС на основі віддаленої міжпроцесної взаємодії;

– масовий характер атакуючих дій, спрямованих на множину обчислювальних процесів ІТС, достатню для передбаченої втрати якості надання інформаційних послуг;

– централізоване управління програмними засобами реалізації впливу з метою координації окремих заходів за єдиним планом, особливо, при їх паралельному виконанні, враховуючи значну кількість ймовірних об’єктів атаки.

Типовий сценарій підготовки та реалізації впливу на ІТС з метою досягнення непрацездатності обчислювальних процесів інформаційних служб (ІС) включає:

1. дослідження ПЗ деякої ІС системи з метою виявлення його недоліків, які можуть бути використані для досягнення його непрацездатності шляхом нав’язування атакуючих даних її обчислювальному процесу.
2. розробка методики досягнення непрацездатності обчислювального процесу ІС шляхом віддаленого нав’язування йому атакуючих даних.
3. розробка програми атаки на основі методики використання недоліків ПЗ, а також алгоритмів пошуку, перевірки об’єктів атаки та оцінки ефективності впливу.
4. пошук об’єктів атаки – вразливих обчислювальних процесів.
5. перевірка об’єктів атаки.
6. застосування програми атаки – нав’язування атакуючих даних об’єктам атаки.
7. оцінка ефективності впливу – перевірка працездатності об’єктів атаки.

Центральним моментом практичної реалізації є застосування програми атаки, яка повинна забезпечувати базову функціональність 4 – 7 фази впливу, а також координацію дій з її іншими примірниками при паралельній роботі. Пошук об’єктів атаки полягає у передачі обчислювальним процесам ІТС тестових даних (запит) та отримання від них відповіді певного змісту, як реакції на обробку тестових даних (тестування). Аналіз відповіді дозволяє визначити тип, версію ПЗ та, як наслідок, дізнатись його недоліки. Необхідність перевірки об’єктів атаки викликана зменшенням з часом достовірності результатів їх пошуку, тобто відомих параметрів ймовірних об’єктів атаки. Існує низка причин „старіння” результатів пошуку, які обумовлюють необхідність нових ітерацій тестування об’єктів атаки. Оцінка ефективності впливу спрямована на отримання відомостей про результат застосування програми атаки відносно об’єкта атаки, як відношення між кількістю успішно атакованих та ймовірних об’єктів атаки.

У доповіді висвітлюються напрямки алгоритмізації практичної реалізації впливу на ІТС у вигляді відповідних часткових постановок задачі про комівояжера. Задача пошуку має на меті зменшення часових витрат при тестуванні обчислювальних процесів на основі розбиття області пошуку на підмножини об’єктів та їх паралельне тестування. Задача перевірки полягає у знаходженні найкращого варіанта тестування ймовірних об’єктів атаки з метою їх перевірки за умови дотримання обмежень на час та якість прийняття рішень щодо реалізації впливу. Задача оцінки ефективності впливу є частковим варіантом постановки попередньої задачі, відмінність – інверсна інтерпретація результатів тестування. Друга та третя задачі передбачають наявність апріорної інформації про ймовірні об’єкти атаки.

к.т.н. Чевардін В.Є. (ВІТІ НТУУ „КПІ”)
Коваленко А.О. (ВІТІ НТУУ „КПІ”)
Ізофатов Д.О. (ВІТІ НТУУ „КПІ”)

ПЕРСПЕКТИВИ РОЗВИТКУ НЕСИМЕТРИЧНИХ КРИПТОГРАФІЧНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

В сучасних умовах розвитку автоматизованих систем великих корпорацій та організацій, які надають інформаційно-телекомунікаційні послуги проблема безпеки інформації стає досить актуальна. Створення надійної системи безпеки інформації сьогодні без використання несиметричних криптографічних алгоритмів захисту інформації та автентифікації неможливо. Одним з перспективних напрямків розвитку систем захисту інформації є розробка сучасних методів несиметричного шифрування. Так поява методів несиметричного шифрування: RSA-перетворень – 1978 р. (Райвист, Шамир, Адельман), перетворень в групі точок ЕС – 1985 р. (Коблиць, Миллер), групі дивізорів точок НЕС – 1989 р. (Коблиць) сприяло активації досліджень в цієї галузі. Останні результати досліджень несиметричних криптоперетворень [1 – 8] показали суттєве зменшення розміру ключової інформації несиметричної криптосистеми за рахунок переходу до більш складних криптоперетворень в групі дивізорів точок гіпереліптичних кривих та групі точок еліптичних кривих. Перехід від абелевих груп цілих чисел до груп точок кривої та дивізорів точок гіпереліптичної кривої привів також до значного зросту обчислювальної складності криптоперетворень. Це обмежує їх використання в певній інформаційно-телекомунікаційній системі та ускладнює процедури оцінки їх криптографічної стійкості.

Відомо, що абелеву групу з початку отримували шляхом мультиплікативних або адитивних операцій над числами поля Галуа F_q, F_{2^m} (рис.1). Наступним кроком розвитку несиметричної криптографії було отримання абелевої групи шляхом додавання точок еліптичної кривої (рис.2). Сутність еліптичної кривої заключається в об’єднанні картежів елементів поля Галуа (X,Y – для афінних координат, X,Y,Z – для проективних) в групу, які є рішенням рівняння кривої E_p. Пізніше Коблиць запропанував замінити перетворення над групою точок кривої перетвореннями над групою дивізорів гіпереліптичної кривої (рис.3).

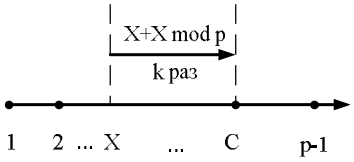


Рис. 1. Перетворення в групі цілих чисел над F_q

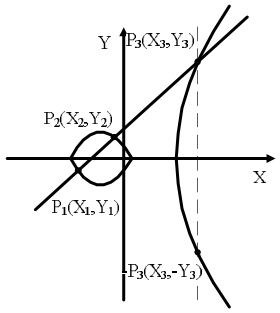


Рис. 2. Операції над групою точок несупресингулярної кривої $y^2 = x^3 + Ax + B$ над F_q

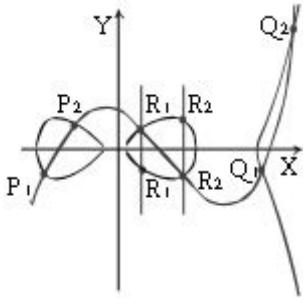


Рис. 3. Графічна інтерпретація операції додавання дивізорвів точок гіпереліптичної кривої над F_q

Аналітичні вирази перетворень над елементами відповідних груп наведені нижче.

Для перетворень в групі цілих чисел: $C_i = M_i * k_i \bmod p$, де C, M, k, p – великі числа. Для перетворень в групі точок еліптичної кривої $y^2 + a_1xy = x^3 + a_2x^2 + a_5 \bmod p$:

$x_3 = \frac{Y_2+Y_1}{X_2+X_1} + a_1\frac{Y_2+Y_1}{X_2+X_1} - a_2 - X_1 - X_2 \quad y_3 = \frac{Y_2+Y_1}{X_2+X_1}X_3 + \frac{Y_2+Y_1}{X_2+X_1}X_3X_1 + Y_1$. Для перетворень в

групі дивізорів точок гіпереліптичної кривої: $y^2 + h(x)y = f(x) \bmod p$: $D_1 + D_2 = \sum_{P_i \in C} m_i P_i + \sum_{P_i \in C} n_i P_i = (P_1 + P_2 - 2\infty) + (Q_1 + Q_2 - 2\infty) = R_1 + R_2 - 2\infty$, де D_1, D_2 – дивізори точок гіпереліптичної кривої другого роду, $P_1, P_2, Q_1, Q_2, R_1, R_2$ – точки гіпереліптичної кривої другого роду.

Порівняння обчислювальної складності криптоперетворень показало суттєвий зріст витрат на криптографічні перетворення в групі точок гіпереліптичних кривих. В зв'язку з чим сьогодні більшу увагу приділяють реалізації криптоперетворень в групі точок гіпереліптичних кривих першого роду (еліптичних кривих). Збільшення обчислювальної складності криптоперетворень є наслідком збільшення розміру абелевої групи, що виступає основою для побудови несиметричного криптографічного шифру. Доведення стійкості криптоперетворень в групі точок гіпереліптичних кривих є досить складним процесом, методики для цього сьогодні не існує. Одним перспективних шляхів створення методики оцінки криптографічної стійкості шифрів, побудованих на основі перетворень в групі точок гіпереліптичної кривої є подання криптографічних перетворень у вигляді функції від елементів поля Галуа. Для визначених вище перетворень відповідні функції можна визначити: $C = \varphi_{RSA}(X)$ – для шифру RSA, $C = \varphi_{EC}(X)$ – для шифру на основі перетворень в групі точок EC, $C = \varphi_{divHEC}(X)$ – для шифру на основі перетворень в групі дивізорів точок гіпереліптичної кривої, де *Y, X* – елементи поля Галуа.

Таким чином, характер функції φ буде визначати криптографічну стійкість певного криптоперетворення та обчислювальну складність, що дозволить визначати доцільність використання його в певній інформаційно-телекомунікаційній системі.

В результаті проведених досліджень було розроблено бібліотеку криптографічних функцій:

– множення та додавання великих чисел за модулем простого числа;

– множення та додавання поліномів за модулем примітивного поліному;

– множення та додавання точок гіпереліптичної кривої 1-го роду;

– визначення стійкості обраної гіпереліптичної кривої 1-го роду згідно ДСТУ 4145.

Отримана бібліотека криптографічних функцій дозволяє визначати обчислювальну складність функцій: $C = \varphi_{RSA}(X)$, $C = \varphi_{EC}(X)$, $C = \varphi_{divHEC}(X)$ та проводити дослідження властивостей криптографічних перетворень в групі точок гіпереліптичних кривих 1-го роду.

В подальшому планується провести дослідження структурних властивостей груп точок та дивізорів гіпереліптичних кривих 1,2 та 3 роду та криптографічних протоколів побудованих на основі криптоперетворень в групі дивізорів точок гіпереліптичної кривої.

ЛІТЕРАТУРА

1. *N.Kobliz.* Hyperelliptic cryptosystem. J. of Crypto., 1, 139 –150, 1989.
2. *G. Frey* and H.–G. Rück. A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves. Mathematics of Computation, 1994.
3. *P. Gaudry*. An Algorithm for Solving the Discrete Log Problem on Hyperelliptic curves. EUROCRYPT 2000, Berlin, Germany, Springer-Verlag, 2000. pp. 19 – 34.
4. *N. Theriault.* Index calculus for hypereleptic curves of small genus. – ASTRACRYPT' 03, Berlin, Springer Verlag, 2003.
5. *Tomas Wollinger*. Software and Haedware Implementation of Hyperelliptic Curve Cryptosystems. Dissertation for the Degree of Doctor-Ingenieur. Bouhum, Germany, May 2004.
6. *Tanja Lange,* Pradeep Kumar Mishra: SCA Resistant Parallel Explicit Formula for Addition and Doubling of Divisor in the Jacobian of Hyperelliptic Curves of Genues 2. INDOCRYPT 2005: 403 – 416.
7. *Tanja Lange:* Formula for Arithmetic on Genues 2 Hyperelliptic Curves. Appl. Algebra Eng. Commun. Comput. 15(5): 295–328 (2005).
8. *Jacobson, M.J.,* Scheidler, R., and Stein / Cryptographic protocols on real hyperalliptic curves. Adv. Math. Commun. 1,2 (2007), 197 – 221.

Чумак В.К. (ВІТІ НТУУ „КПІ”)
Бортнік Л.Л. (ВІТІ НТУУ „КПІ”)

ПЕРСПЕКТИВИ БОРОТЬБИ З НАВМИСНИМИ ЗАВАДАМИ В СИСТЕМАХ РАДІОЗВ’ЯЗКУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ MC-CDMA

В даний час технологія ортогонального частотного мультиплексування – OFDM (Orthogonal Frequency Division Multiplex*)* широко застосовується в мережах безпровідного доступу. Технологіяї OFDM має ряд переваг та недоліків. До основних переваг технології OFDM слід віднести стійкість до завмирань сигналу за умов багатопроменевості та високу спектральну ефективність. Багаточастотна структура групового сигналу зменшує чутливість системи передачі до імпульсних завад і дозволяє ефективно боротися із зосередженими за спектром завадами. Але технологія OFDM має і недоліки. Одним з важливим являється чутливість до навмисних завад [1].

Перспективним методом боротьби з навмисними завадами є розширення спектру за допомогою технології CDMA (Code Division Multiple Access), основними принципами якої являється розширення спектра в поєднанні з кодовим розділенням фізичних каналів за рахунок використання псевдовипадкових послідовностей (ПВП)

Своєрідне поєднання технологій OFDM та CDMA створює технологію MC-CDMA (Multi Carrier Code Division Multiple Access). При формуванні MC-CDMA систем кожен біт потоку сигналів відображається на всі піднесучі, а кожна піднесуча використовує своє постійне в часі фазове зміщення, яке вибирається відповідно до заданого закону кодування [2]. Ключова властивість системи MC-CDMA в тому, що всі чіпи, співставлені одному біту кода, передаються паралельно у вузькосмугових підканалах. Ця система володіє всіма перевагами OFDM та CDMA систем, та дозволяє боротися з частотно-селективними завмираннями і багатопроменевістю.

По-перше, зменшення впливу завад забезпечується ефектом ,,розмивання” завад по спектру за рахунок перемноження прийнятої суміші сигналу і завади з ПВП.

По-друге, завадостійкість приймання OFDM-сигналу значно підвищується за рахунок підвищення стійкості пілот-сигналів (пілот-несучих) щодо впливу завад, що забезпечує більш точну оцінку поточного стану каналу зв’язку. Знання передаточної характеристики каналу, в свою чергу, дозволяє застосувати режекцію частини спектра, ураженої завадою, з відключенням передачі корисної інформації по відповідних піднесучих.

По-третє, якщо противник застосовує імітаційну заваду, яка в точності відтворює структуру сигналу, теоретично він не знає способу генерації ПВП. Тому така імітаційна завада хоч і буде створювати ефект внутрішньосистемних завад внаслідок неортогональності ПВП, що генеруються постановником завад і засобами радіозв’язку (ЗРЗ), однак ефективність її значно зменшиться внаслідок узгодженої фільтрації після перемноження в кореляторі приймача системи радіозв’язку (СРЗ).

Важливу роль, також, відіграє вибір виду розширяючої послідовності. Для розширення спектра в системах MC-CDMA використовуються різні види розширяючих послідовностей: двійкові (послідовності Уолша, послідовності Шапіро-Рудіна, коди Баркера, *M*-послідовності, послідовності Адамара) та багатофазні (послідовності Френка та Задова-Чу, послідовності Мілевського, послідовності Голея).

Отже, перспективним напрямком вдосконалення технології OFDM в умовах навмисних завад являється додаткове розширення спектру сигналу за допомогою розширяючих послідовностей.

ЛІТЕРАТУРА

1 *Вишневский В.М.* Широкополосные беспроводные сети передачи информации. / Ляхов А.И., Портной С.Л., Шахнович И.В – М.: Техносфера, 2005. – 592 с.

2. *Волков Л.Н.* Системы цифровой радиосвязи: базовые методы и характеристики: Учебное пособие. / Немировский М.С., Шинаков Ю.С. – М: Эко-Трендз, 2005. – 392 с.

к.т.н. Шаціло П.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Любарський С.В. (ВІТІ НТУУ „КПІ”)

МЕТОДИКА ВИБОРУ МОДЕЛІ ПОДАННЯ ЗНАНЬ В ІНТЕЛЕКТУАЛЬНИХ НАВЧАЛЬНИХ СИСТЕМАХ

Одним з найбільш перспективних напрямків розвитку навчальних систем є розробка інтелектуальних навчальних систем (ІНС), заснованих на застосуванні методів і засобів штучного інтелекту.

Центральним елементом архітектури ІНС є база знань, основою якої є модель подання і обробки знань, що впливає на методи отримання знань, вимоги до знань, можливості і властивості ІНС.

Завдання вибору моделі подання знань в ІНС відноситься до класу завдань нечіткої багатокритеріальної оптимізації.

Тобто, існує безліч *m* моделей подання знань (МПЗ). Деяка *j*-а властивість *i*-го варіанту МПЗ характеризується величиною *j*-го часткового показника q_{ij}; $i=\overline{1, m}$; $j=\overline{1, n}$. Тоді МПЗ при *i*-тому варіанті реалізації характеризується вектором $\overline{Q_i} = \left| q_{i1,\dots}\ q_{ij,\dots}\ q_{in} \right|$. Завдання багатокритеріальної оптимізації зводиться до того, щоб з безлічі *m* варіантів МПЗ вибрати такий варіант i_0, який має найкраще значення вектора $\overline{Q_i}$, тобто

$$i_0 = \arg opt Q_i \quad (1)$$
$$i=\overline{1, m}$$

Для вирішення багатокритерійного завдання вибору необхідно виразити значення часткових показників q_{ij} в зручній кількісній формі. Практика показує, що найдоцільніше як кількісні, так і якісні показники привести до вигляду, коли їх значення змінюються від нуля до одиниці, тобто $0 \le q_{ij} \le 1$ для $i=\overline{1, m}$; $j=\overline{1, n}$. При цьому кількісні показники нормуються відносно оптимальних значень, а якісні представляються у вигляді функцій приналежності заданому рівню якості. Першим кроком рішення задачі є визначення важливості показників. Для цього пропонується використати метод власних векторів Уэя [1].

Метод грунтується на даних матриці парних порівнянь $A = \left\| a_{jk} \right\|$, $a_{jk} \in \{-1, 0, 1\}$, де a_{jk} = -1 означає перевагу показника q_k над показником q_j, a_{jk} = 0 − рівноцінність q_k і q_j, a_{jk} = 1 − перевага показника q_j над q_k.

Зважаючи на незручність роботи з негативними числами матрицю попарних порівнянь можна представити як ненегативну матрицю $A^+ = \left\| a_{jk} \right\|$, $a_{jk} \in \{0, 1, 2\}$, де числа $\{0, 1, 2\}$ мають вищезазначений сенс.

Склавши числа по кожному з рядків матриці, матимемо числові характеристики важливості показників, а розділивши їх на загальну суму, отримаємо коефіцієнти важливості показників.

$$\omega_j = \frac{\sum_{k=1}^{n} a^+_{lk}}{\sum_{j}^{n} \sum_{k}^{n} a^+_{jk}} \quad (2)$$

На другому кроці рішення задачі експертим методом визначаються значення часткових показників q_{ij} для усіх даних моделей подання знань.

Нарешті, на третьому, завершальному кроці вибирається раціональний варіант МПЗ одним з можливих методів нечіткої багатокритеріальної оптимізації.

Зокрема, пропонується застосовати *лексикографічний метод* як найбільш простий в реалізації і вимагаючий мінімальної експертної інформації про міру переваги показників.

Застосування методу зводиться до наступних операцій.

1. Упорядковуються показники по важливості

$$q_1 > q_2 > \ldots q_j > \ldots > q_n; \quad j = \overline{1, n} \tag{3}$$

2. За згодою особи, що приймає рішення, для кожного показника призначається величина допустимої поступки $\Delta q_j; \quad j = \overline{1, m}$, у межах якої розглянуті альтернативи вважаються практично рівноцінними.

3. Для першого по важливості показника q_1 формується множина π_1 „практично рівноцінних" альтернатив, які задовольнять умові

$$\max \quad q_1(\overline{X_i}) - q_1(\overline{X_k}) \le \Delta q_1 \tag{4}$$

$$i = \overline{1, S} \qquad k \ne I_o^{(1)}$$

$$i = I_o^{(1)}$$

4. Якщо множина π_1 містить тільки один варіант, то він і є найкращим. Якщо множина π_1 містить більш за один варіант, то належіть перейти до розгляду множини π_1 по показнику q_1.

5. Для другого показника q_2 формується множина π_2 варіантів з множини π_1, які задовольняють умові

$$\max q_2(\overline{X_i}) - q_1(\overline{X_k}) \le \Delta q_2 \tag{5}$$

$$i \in \pi_1 \qquad k \ne I_o^{(1)}$$

$$i = I_o^{(2)} \qquad k \ne I_o^{(2)}$$

6. Якщо множина π_2 містить тільки один варіант, то він і вважається найкращим; якщо більше 1 - розглядаємо ці варіанти по показнику q_3 і так далі.

7. Якщо усі показники послідовно розглянуті і в результаті отримана множина $\pi = \pi_1 \times \pi_2 \times \ldots \times \pi_m$, що містить більш за одну альтернативу, то можна застосувати два підходи:

– зменшити величину допустимої поступки Δq_j, починаючи з першого по важливості показника і повторити усі кроки рішення;

– надати особі, що приймає рішення, остаточний вибір кращого варіанту.

Отже, завдання вибору моделі подання знань в ІНС є одним з центральних завдань етапу проектування подібних систем. Раціональний вибір МПЗ залежіть не тільки від обґрунтованості показників якості МПЗ, а і від ефективного вирішиення завдання нечіткої багатокритеріальної оптимізації. Запропонована методика дозволяє урахувати якісні та кількісні показники МПЗ і на підставі лексикографічного методу обрайти найкращий варіант моделі подання знань у інтелектуальній навчальній системі.

ЛІТЕРАТУРА.

1. *Анохин А.М., Глотов В.А., Павельев В.В.* Методы определения коэффициентов важности критериев. // Автоматика и телемеханика – 1997 -№ 8 – с. 3 – 35.

Шацький І. О. (ВІТІ НТУУ „КПІ”)
Залужний О. В. (ВІТІ НТУУ „КПІ”)
Терезюк О. Е. (ВІТІ НТУУ „КПІ”)

РОЗРАХУНОК КОЕФІЦІЄНТА НАПРАВЛЕНОЇ ДІЇ НИЗЬКОПРОФІЛЬНОГО ВИПРОМІНЮВАЧА НАД ЦИЛІНДРИЧНОЮ ПОВЕРХНЕЮ

На теперішній час широкого застосування набув відносно новий тип антен – низько профільні, відомі також як мікрополоскові антенні пристрої. Відмінною особливістю даного класу антен є їх високі масо-габаритні показники, простота виготовлення, велика стабільність параметрів і міцність конструкції. Низькопрофільні антени (НПА) дають змогу працювати як з лінійною так і з круговою поляризацією поля. Даний тип антен широко застосовується на літальних апаратах (літаках, ракетах і т. д.), як самостійна антена так і в якості випромінюючого елемента різного типу антенних решіток, в абонентських комплектах систем радіозв’язку з рухомими об’єктами (наприклад, в системах сотового зв’язку). Конструктивно НПА являє собою дві металеві пластини рознесених між собою на відстань $d << \lambda$, де λ – довжина хвилі, одна з яких виконує функцію екрана, друга, певних розмірів (рис. 1а), є випромінюючим елементом (ВЕ). В просторі між пластинами розміщується вузол збудження електромагнітних хвиль [1]. На практиці найбільш широкого застосування набули НПА з простою формою верхньої пластини: прямокутною, квадратною та круговою. За рахунок введення діелектричного матеріалу в простір між пластинами, розмір випромінювача можна зменшити в $\sqrt{\varepsilon'}$ раз, де ε' – відносна діелектрична проникність високочастотного діелектрика. Таким чином НПА є компактним, малогабаритним, не виступаючим за межі екрана випромінювачем електромагнітного поля.

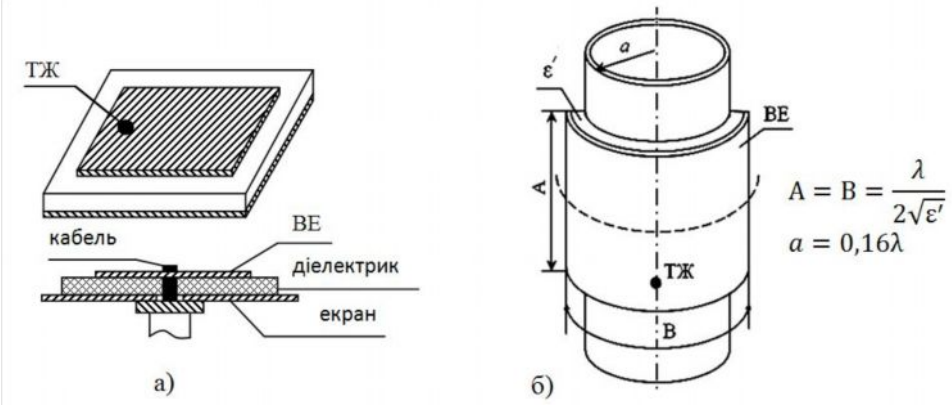


Рис. 1

Одним із нових напрямків розвитку техніки НПА є використання в їхній конструкції циліндричних екранів, що еквівалентно розміщенню низькопрофільного випромінювача над циліндричною поверхнею (рис. 1б). Застосування НПА з циліндричним екраном дозволяє створювати антени як з ненаправленою так і секторною характеристикою направленості (ХН) в азимутальній площині [2].

Однією з найважливіших зовнішніх характеристик будь-якої антени є її коефіцієнт підсилення G, що одночасно враховує як коефіцієнт корисної дії (ККД) антени та виграш по потужності за рахунок направленості випромінювання, так і завадостійкість антени якщо вона працює в режимі прийому:

$$G = \eta_A D \ , \tag{1}$$

де: η_A – ККД антени; D – коефіцієнт направленої дії (КНД).

Розрахунок коефіцієнта підсилення за виразом (1), при відомій ХН, зводиться до розрахунку КНД та ККД. Точний розрахунок останнього є досить складною задачею. Проте ККД більшості антен УКХ діапазону, до яких і належить, власне, НПА, досить високий

($\eta_A > 0{,}9$) і при наближених розрахунках може бути прийнятим рівним одиниці [3]. Таким чином для визначення коефіцієнта підсилення НПА достатньо здійснити розрахунок її КНД.

КНД, наряду з ХН, дає змогу охарактеризувати направлені властивості антени. Якщо ХН дозволяє оцінити, в яких напрямках антена створює більшу чи меншу напруженість поля, то КНД дає змогу визначити енергетичний ефект, що пов'язаний із застосуванням тієї чи іншої направленої антени. Під КНД розуміють відношення потужності випромінювання ненаправленої (ізотропної) до направленої (реальної) антен, що на однаковій відстані в даному напрямку створюють однакову напруженість поля. Розрахунок КНД, зазвичай, здійснюється по відомому полю чи ХН в дальній зоні.

Вираз для ХН НПА з циліндричним екраном і квадратною формою верхньої пластини, для випадку вертикальної поляризації поля має наступний вигляд:

$$f(\varphi,\ \theta) = \frac{\cos\left(\dfrac{\pi}{2\sqrt{\varepsilon'}}\right)}{\sin\theta}\sum_{n=0}^{\infty}\left[\varepsilon_n i^n \frac{\cos n\varphi}{\mathrm{H}_0^2\left(\dfrac{ka}{\sqrt{\varepsilon'}}\sin\theta\right)}\frac{\sin\left(n\dfrac{\pi}{2}\right)}{n\dfrac{\pi}{2}}\right],\ \varepsilon_n = \begin{cases}1, & \text{при } n=0\\ 2, & \text{при } n\neq 0\end{cases}. \qquad (2)$$

При значеннях θ близьких до $(0;\ \pi)$ перший член ряду (2) прямує до нескінченності, що унеможливлює розрахунок КНД. Розклад в степеневий ряд виразу (2) та застосування відповідного асимптотичного співвідношення при $\theta \to (0;\ \pi)$ вирішує дану проблему. На рис. 2 подано теоретично розраховані діаграми направленості в меридіальній площині та КНД низькопрофільного випромінювача з циліндричним екраном для двох значень параметра ε'.

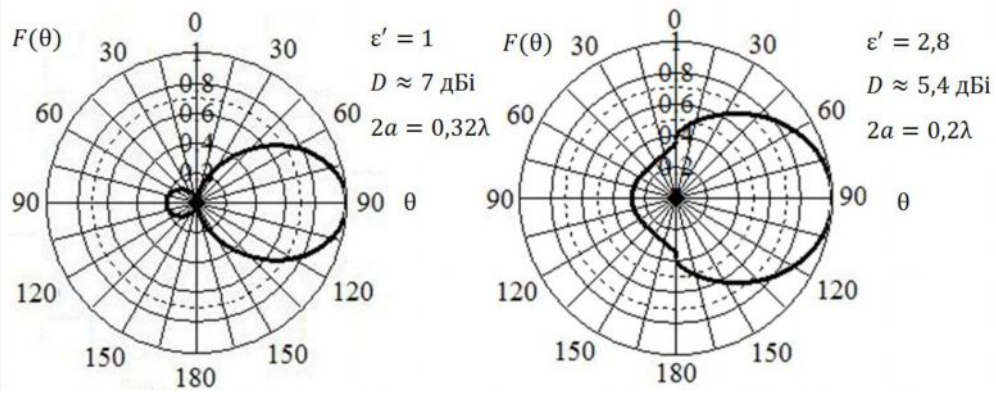


Рис. 2

При збільшені параметра ε' значення КНД поступово зменшується, що пояснюється розширенням ширини діаграми направленості яв в меридіальній так і в азимутальній площинах за рахунок зменшення поперечних розмірів (діаметра циліндра) антени. Зокрема, при відсутності діелектрика $(\varepsilon' = 1)$ маємо $D \approx 7$ дБі, ширина сектора в меридіальній площині становить 66°, в азимутальній – 120°. При цьому поперечні розміри такої НПА рівні $2a = 0{,}32\lambda$ від довжини хвилі. Наприклад, для GSM-900 ($\lambda_{ср} = 315$ мм) $2a \approx 100$ мм.

Таким чином, побудова антенних решіток на основі низькопрофільних випромінювачів з циліндричним екраном дає змогу не лише в широких межах формувати необхідні ХН, але й забезпечити із застосуванням лише одного низькопрофільного ВЕ величину КНД близько 7 дБі. З метою ж подальшого збільшення D необхідно будувати антенні решітки на їх основі.

ЛІТЕРАТУРА

1. *Ломан В. И., Ильинов М. Д.* Микрополосковые антенные устройства. – М: ж. Зарубежная радиоэлектроника – № 10, 1981. – С. 99 – 115.

2. *Сборник* трудов VIII Международной научно-технической конференции "Повышения качества, надежности и долговечности технических систем и технологических процессов".– г. Хургада (Египет). – ХНУ, 2009. – 197 с.

3. *Ямайкин В. Е., Кишкунов В. К.* Антенные устройства. – Минск, 1965. – 529 с.

д.т.н. Шворов С.А. (ВІТІ НТТУ ,,КПІ”)
к.пед.н. Лукін В.Є. (ВІ КНУ)

МЕТОДИЧНІ ЗАСАДИ ПЛАНУВАННЯ ТА ПРОВЕДЕННЯ ЗАНЯТЬ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНИХ ЗАСОБІВ ДИСТАНЦІЙНОГО НАВЧАННЯ

На даний час особлива увага у вищих навчальних закладах приділяється побудові та використанню інтелектуальних засобів дистанційного навчання (ІЗДН). При використанні таких засобів у навчальному процесі забезпечується досягнення необхідного рівня підготовки студентів (курсантів) до виконання навчальних завдань (НЗ) при мінімальних витратах матеріальних засобів і коштів. Незважаючи на досить велику кількість публікацій, присвячених питанням побудови та використання ІЗДН в процесі навчання [1-4], у даний час не в повній мірі розроблені методичні засади планування та організації навчання з використанням перспективних ІЗДН.

Виходячи з того, що початковий рівень підготовки студентів (курсантів) з виконання типових НЗ різний, доводиться розв’язувати задачу мінімального розподілу часу й фінансових витрат на відпрацювання кожного типу операцій НЗ для досягнення необхідного рівня підготовки у виконанні всього НЗ.

Методика планування та організації навчання з використанням ІЗДН включає наступні основні етапи:

1. Формулюються цілі навчання та завдання, що необхідно відпрацювати.

2. Визначаються необхідні прогнозовані рівні підготовки студентів з виконання основних типів операцій НЗ.

3. Здійснюється формування оптимального плану інтенсивної підготовки.

4. Забезпечується відпрацювання основних типів операцій НЗ за оптимальним планом інтенсивної підготовки.

5. В процесі навчання, якщо рівень підготовки не відповідає прогнозованому, забезпечується корегування плану інтенсивної підготовки. При цьому у процесі навчання здійснюється адаптивна зміна кількості запланованих НЗ, тобто забезпечується корегування часових витрат, необхідних для досягнення прогнозованого рівня підготовки, в залежності від фактичного рівня навченості студентів (курсантів) з виконання типових операцій.

З цією метою через певні часові інтервали забезпечується реєстрація фактичного рівня підготовки з виконання кожного типу операції і всього НЗ.

Одночасно проводиться порівняння фактичного й необхідного рівнів підготовки (P і $P_т$). Якщо умова

$$P \geq P_T \tag{1}$$

виконується, то відпрацювання НЗ даного типу може бути закінчене, оскільки студенти (курсанти) досягли необхідного рівня підготовки з виконання НЗ. У решті випадків проводиться перевірка наступної умови:

$$| P_i^{*} — P_i | \leq \Delta P_i , (i = 1, ..., n), \tag{2}$$

де ΔP_i — величина гранично допустимої помилки в реалізації студентами i- го типу операції навчальних завдань.

При виконанні умови (2) передбачається, що фактичні показники рівнів підготовки студентів (курсантів) $P_1 , …, P_n$ зі встановленим ступенем точності (ΔP_i, $i=\overline{1, n}$) відповідають прогнозованим рівням $P_1^{*}, ..., P_n^{*}$.

Отже, відпрацювання типових операцій НЗ продовжується відповідно до наперед встановлених часових інтервалів T_1, ..., T_n.

Якщо умова (2) не виконується, то виникає необхідність в поетапному корегуванні процесу організації та проведення занять, тобто в реалізації в ІЗДН адаптивного управління процесом навчання.

Саме тому, на п'ятому етапі організації та проведення тренування необхідно відкорегувати (адаптувати) часові характеристики відпрацювання типових операцій T_1, ..., T_n, прогнозовані рівні P_1^*, ..., P_n^*, а також необхідний рівень P_T у зв'язку зі зміною фактичного рівня підготовки (P).

Іншими словами, як тільки в процесі заняття не виконуються умови (1) і (2), то, що очевидно, необхідно скорегувати показники P_1^*, ..., P_n^*. Цей простий цикл адаптивного управління процесом навчання є нижнім рівнем адаптації, процесу організації та проведення заняття. На даному рівні забезпечується адаптивна зміна кількості НЗ залежно від рівня підготовки студентів (курсантів) з виконання кожного типу операцій.

Основною метою адаптивного управління процесом навчання є мінімізація часу підготовки студентів (курсантів) до необхідних прогнозованих рівнів з виконання основних типів операцій НЗ.

Якщо нижня межа адаптації процесу організації та проведення заняття є недостатньо ефективною, тобто умови (1) і (2) постійно не виконуються, то доцільно, виходячи з фактичного рівня підготовки, скорегувати цілі навчання (Z_T), а потім і відповідні показники P_1^*, ..., P_n^*; T_1, ..., T_n. Даний цикл адаптивного управління належить до верхнього рівня адаптації процесів організації й проведення заняття.

Для розв'язання даного завдання доцільно використовувати метод оптимального розподілу вимог до рівня підготовки студентів (курсантів) з виконання типових операцій НЗ та методи штучного інтелекту [5-8].

Таким чином, розглянуті методичні засади планування та проведення занять з використанням інтелектуальних засобів дистанційного навчання спрямовані на вирішення практичної проблеми - досягнення необхідного рівня підготовки студентів (курсантів) до виконання навчальних завдань (НЗ) при мінімальних витратах часу і коштів.

ЛІТЕРАТУРА

1. *Машбиц Е.И.* Психолого-педагогические проблемы компьютеризации обучения. – М.: Педагогика, 1988. – 192 с.

2. *Петрушин В.А.* Интеллектуальные обучающие системы: архитектура и методы реализации (обзор) // Техническая кибернетика, вып. № 2. – К: ИК, 1993. – С. 164 – 189.

3. *Искусственный* интеллект. - В 3 кн. Кн. 1. Системы общения и экспертные системи: Справочник. – М.: Радио и связь, 1990. – 464 с.

4. *Искусственный* интеллект. - В 3 кн. Кн. 2. Модели и методы: Справочник. - М.: Радио и связь,1990. – 304 с.

5. *Герасимов Б.М.,* Тарасов В.А., Токарев И.В. Человеко-машинные системы принятия решений с элементами искусственного интеллекта. – К.: Наукова думка, 1993. – 184 с.

6. *Перспективы развития* вычислительной техники: Справ. пособие. Кн.2. Интеллектуализация ЭВМ. – М.: Высш. шк., 1989. – 159 с.

7. *Фабри Д.М.,* Лупинетти А.А. Имитационное моделирование и искусственный интеллект в системах обучения персонала УВД // ТИИЭР, т. 77, вип. № 11, 1989. – С. 189 – 193.

8. *Герасимов Б.М.,* Оксінюк О.Г., Шворов С.А. Проектування та застосування експертно-навчальних систем: Монографія.- К.: Вид-но Європ. Ун-ту, 2008. – 263 с.

Шевченко А. С. (ВІТІ НТУУ ,,КПІ”)

УЗАГАЛЬНЕНА МОДЕЛЬ ПОРУШНИКА БЕЗПЕКИ ІНФОРМАЦІЙНИХ АКТИВІВ БЕЗПРОВОДОВИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ВІДОМЧОГО ПРИЗНАЧЕННЯ В ІНФОРМАЦІЙНІЙ БОРОТЬБІ

Стрімкий розвиток безпроводових інформаційно-комунікаційних систем (БпІКС) дозволяє надавати користувачам все ширший спектр послуг та сервісів. Але поява нових сервісів однозначно призводить до загострення інформаційної безпеки у зв’язку з появою нових вразливостей.

З впровадженням концепції ведення інформаційних війн особливо загострили питання забезпечення безпеки інформації, що передається БпІКС відомчого призначення в умовах інформаційної боротьби. Відповідно до моделі загроз інформації для БпІКС відомчого призначення, що функціонують під час інформаційного конфлікту, приведеній в роботі [1], побудуємо модель порушника інформаційних активів.

Для інформації, яка передається БпІКС в умовах інформаційної боротьби, основними атаками порушника є: застосування засобів радіоелектронного придушення (РЕП); використання засобів деструктивної дії (зброя вогневої поразки, ядерна зброя і зброя, основана на нетрадиційних принципах фізичного впливу); проникнення в систему; порушення системи управління БпІКС; порушення системи захисту БпІКС; зняття інформації по технічних каналах витоку інформації (ТКВІ) та побічних електромагнітних випромінюваннях і наводках (ПЕМВН). Вказані атаки порушник може наносити, для реалізації переваги в інформаційному просторі, як в комплексі, так і окремо.

Основними і найбільш розповсюдженими засобами для реалізації порушником атаки на БпІКС є застосування станцій (комплексів) РЕП. Комплекс РЕП структурно складається із станції радіо/радіотехнічної розвідки (РРТР), станції постановника завад (ПЗ) та станції управління. Після перехоплення радіосигналу, розпізнавання його параметрів та пеленгування джерела випромінювання, станція РРТР отриману інформацію передає на станцію управління комплексу РЕП, яка в свою чергу подає команду на станцію ПЗ чи здійснює цілевказівку засобам деструктивного впливу.

В залежності від особливостей тактичного застосування комплексів РЕП та їх тактико-технічних характеристик модель порушника необхідно розбити на зони дії порушника: ефективності наземних і повітряних засобів РЕП; неефективності наземних засобів РЕП і ефективності повітряних засобів РЕП; ближня зона.

З урахуванням можливостей реалізації порушником перерахованих атак представимо схематично модель порушника (рис. 1). Модель порушника відображає формалізований опис порушника, перелік реалізуємих атак та засобів їх реалізації.

Для реалізації атак: проникнення в систему, порушення системи управління БпІКС; порушення системи захисту БпІКС; зняття інформації по ТКВІ та через ПЕМВН, порушнику необхідно знаходитись в ближній зоні БпІКС. Передувати реалізації останніх трьох атак, майже завжди, має проникнення в систему (подолання технічних системи захисту периметра і охорони). На рисунку дані атаки порушника обособлені і позначені від 1 до 4. Радіус ближньої зони залежить від технічних характеристик БпІКС з урахуванням технічних можливостей устаткування порушника. Атаки застосування РЕП та деструктивного впливу реалізуються також і в ближній зоні.

Прикладом порушника, набір можливостей реалізації атак якого максимально наближений до набору атак порушника, представленого на моделі порушника, є комплекс розвідки і радіоелектронної війни ,,Профєт” (Prophet). Даний комплекс був розроблений в рамках концепції ,,Єдиного інформаційного простору розвідки” ЗС США і прийнятий на озброєння для тактичної ланки управління (ТЛУ). Даний комплекс призначений для ведення радіо- і радіотехнічної розвідки, спеціальної технічної розвідки, а також радіоелектронної

війни. В якості платформи для повітряної підсистеми використовується гелікоптер ЕН-60, а в подальшому планується використання і тактичних безпілотних літальних апаратів (БЛА) RQ-5 Hunter і RQ-7A Shadow 200. Наземна підсистема комплексу „Профєт" AN/MLQ-40(V)3 виконує сканування в діапазоні 20 МГц – 2 ГГц та відображає дані радіоелектронної обстановки на площі 150×120 км, формує базу даних джерел радіоелектронного випромінювання.

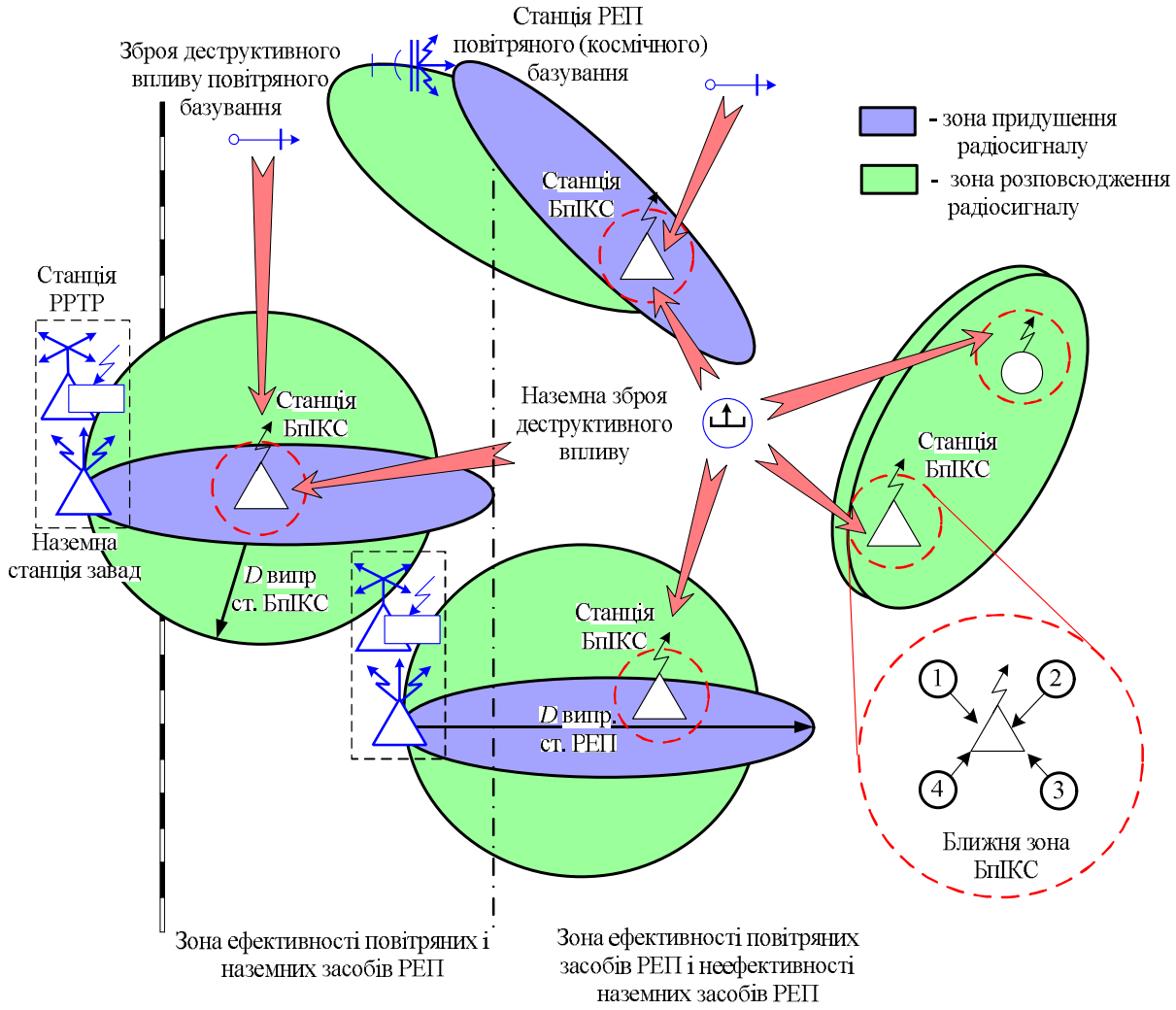


Рис. 1. Узагальнена модель порушника інформаційної безпеки БпІКС відомчого призначення в умовах інформаційної боротьби

Представлена модель порушника інформації, що передається засобами БпІКС, об'єднує всі атаки порушників, деструктивний вплив яких протягом довгого часу розглядався окремо (РЕП, засоби деструктивного впливу, ТКВІ, тощо). Приведена модель порушника, адекватна сучасним концепціям ведення інформаційної боротьби та їх реалізації. Підтвердженням цього є склад комплексу „Профєт". На відміну від комплексів РЕП, він має в своєму складі станції спеціальної технічної розвідки. Це дає зрозуміти, що відбувається реальний перехід від радіоелектронної боротьби до комплексних інформаційних протиборств. Таким чином, протидією на реалізацію комплексних атак має стати комплексний захист власних БпІКС.

ЛІТЕРАТУРА

1. *Кокотов О.В.* Модель загроз інформації в системах безпроводового зв'язку в умовах ведення інформаційної війни / Кокотов О.В., Шевченко А.С. V науково-практичний семінар „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення". – К.: ВІТІ НТУУ„КПІ". – 2009. – С. 140.

к.т.н. Юденок І.С. (НУОУ)
Білько Н.Ю. (ЦНДІ ОВТ ЗС України)
Лобанова М.М. (ЦНДІ ОВТ ЗС України)

ВИМОГИ ДО ПЕРСПЕКТИВНОЇ СИСТЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

В доповіді розглядаються проблеми розвитку перспективної система інформаційного забезпечення ЗС України. З цією метою формулюються вимоги до системи зв'язку та інформатизації ЗСУ, яка повинна забезпечувати: використання взаємносумісних протоколів, інтерфейсів; прийом, ретрансляцію, розподіл потоків інформації, що циркулюватимуть в створюваній Єдиній автоматизованій системі управління ЗСУ та управління ними; скритність та стійкість управління військами (силами) в будь-яких умовах оперативної обстановки завдяки використанню сучасних телекомунікаційних засобів; застосування у військовій сфері готових комерційних стандартів і апаратно-програмних засобів. Використання сучасних технологій надасть змогу інтегровано використовувати універсальні мережі зв'язку й інформаційно-телекомунікаційні мережі. Сучасні цифрові технології нададуть не тільки можливість обміну інформацією, але й можливість резервування інформаційно-телекомунікаційних мереж за рахунок каналів, що надаються для універсальних мереж зв'язку. Можливість такої взаємозаміни досягається використанням загальноприйнятих міжнародних стандартних інтерфейсів, протоколів, стиків та технологій. Обладнані такими апаратними засобами стаціонарні і мобільні вузли зв'язку набудуть можливості швидкої адаптації до роботи з існуючими системами й мережами зв'язку і телекомунікаційними мережами загального користування, мережами зв'язку інших силових структур, а також з системами зв'язку та телекомунікації інших країн світу. Створення загального інформаційно-телекомунікаційного простору надасть можливість оптимального використання ресурсів апаратури каналоутворення та комунікації, швидкої зміни топології мереж та легкого пристосування системи до роботи в будь-яких умовах при веденні будь-якого виду бойових дій.

Перспективна система зв'язку та передачі даних, яка буде складатись з ліній прямого зв'язку і мережі зв'язку загального користування, повинна задовольняти такі вимоги: 1. Необхідну стійкість функціонування системи зв'язку в умовах високої динамічності бойової обстановки, інтенсивної протидії противника різноманітними засобами РЕБ і вогневого ураження, перш за все за рахунок високого ступеня зв'язності елементів системи та високої структурної скритності. 2. Необхідну пропускну здатність за рахунок більш ефективного використання частотно-часового ресурсу, що досягається сполученням прямих зв'язків і застосуванням спільного ресурсу універсальної мережі зв'язку. 3. Покращяння характеристик електромагнітної сумісності на вузлах зв'язку пунктів управління і підвищення розвідзахищеності системи шляхом зниження потужностей випромінюючих засобів та зменшення їх кількості, а також за рахунок винесення випромінюючих засобів за границі пунктів управління. 4. Максимальне використання ресурсів групових трактів передачі даних та зв'язку, розгорнутих на інформаційно-телекомунікаційних вузлах зв'язку, побудованих з використанням сучасних технологій. 5. Забезпечення мобільності та живучості універсальної мережі зв'язку за рахунок зв'язності інформаційно-телекомунікаційних вузлів зв'язку між собою радіорелейними лініями зв'язку. 6. Інтеграцію функцій комутації та каналоутворення для різношвидкісних потоків.

З метою створення єдиної інформаційно-технічної системи інформаційного забезпечення Збройних Сил, підвищення її стійкості та оперативності, забезпечення прийняття та своєчасного доведення рішень до посадових осіб органів та пунктів управління в реальному масштабі часу пропонується варіант структури сучасної системи інформаційного забезпечення ЗС України.

к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
к.т.н. Могилевич Д.І. (ВІТІ НТУУ „КПІ”)
к.т.н. Правило В.В. (ВІТІ НТУУ „КПІ”)

МЕТОДИ ЗАПОБІГАННЯ ВЗАЄМНІЙ ІНТЕРФЕРЕНЦІЇ НА БАЗОВИХ СТАНЦІЯХ СИСТЕМ ШИРОКОСМУГОВОГО БЕЗПРОВІДНОГО ДОСТУПУ

Досить суттєво інтерференція на базовій станції (БС) виявляється в несприятливому впливі радіосигналу, що випромінюється передавачем одного каналу, на приймач сусіднього каналу БС. Якщо центральні частоти цих сусідніх каналів розташовані досить близько одна від одної так, що їх частотні спектри перекриваються, і антени розташованіпоблизу одна від одної, то міжканальна інтерференція може перевищувати допустимі норми.

Рівень інтерференції на сусідніх частотних каналах залежить не лише від параметрів приймально-передаючого пристрою, але і від характеристик антен. В умовах, коли повністю виключити інтерференцію між сусідніми частотними каналами неможливо, вживання антен з параметрами, що забезпечують придушення такої інтерференції, а також територіальне рознесення антен, дозволяє забезпечити нормальну роботу багатосекторної БС в умовах обмеженості частотного ресурсу. Проте антени в антенних системах розташовуються досить близько одна від одної, що означає фактичну відсутність територіального рознесення. Ця обставина в даному випадку повинна компенсуватися забезпеченням необхідного частотного і/або часового рознесення.

Частотне рознесення реалізується в системах Frequency Division Duplex (FDD), де канали прийому Uplink (UL) і передачі Downlink (DL) рознесені по частоті (зазвичай на 100 Мгц). Тобто рівень інтерференції в FDD системах не залежить від територіального рознесення антен сусідніх секторів БС і, крім того, системі FDD не потрібна часова синхронізація каналів.

Якщо для антенної системи не виконуються вимоги ні частотного, ні територіального рознесення, то можлива реалізація механізму синхронізації частотних каналів, що вживається в системах Time Division Duplex (TDD), та який полягає в синхронізації за часом циклів передачі і прийому фреймів. В даному випадку фрейми передачі і прийому не перетинаються в часі і відповідно канали не створюють інтерференцію один одному навіть у випадку, якщо вони збігаються по частоті.

Для випадку, коли зазначені методи територіального, частотного та часового рознесення каналів не забезпечують запобігання взаємній інтерференції, пропонується використовувати так звані „інтелектуальні антени”, що фактично являють собою фазовані антенні решітки, які спроможні синтезувати голчатий промінь діаграми спрямованості для кожного абонента в момент його обслуговування. Таке рішення, окрім зменшення взаємної інтерференції, дає змогу підвищити потужність сигналу DL на 12 дБ, а сигналу UL на 6 дБ, і тим самим збільшити дальність обслуговування абонентів на декілька кілометрів та підвищити швидкість передачі даних шляхом зміни рівня квадратурно-амплітудної модуляції QAM, наприклад з QAM-16 на QAM-64.

У підсумку вибір методу запобігання взаємній інтерференції на базових станціях для визначеної системи широкосмугового безпровідного доступу залежить від наявного частотного ресурсу, кількості каналів та можливих варіантів розташування антен з урахуванням особливостей їх конструкції.

ЛІТЕРАТУРА

1. EN 302 085: European Norm – Fixed Radio systems; Multipoint Antennas; Antennas for MultiPoint fixed radio systems operating in the range 3 to 11 GHz.

2. IEEE 802.16e 2005 and IEEE 802.16-2004/Cor1 –2005. IEEE standard for Local and metropolitan area networks. Part 16: Air Interface for Fixed Broadband Wireless Access Systems. Amendment 2.