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

# V-й НАУКОВО-ПРАКТИЧНИЙ СЕМІНАР

## „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення”

**22 жовтня 2009 року**

**(Доповіді та тези доповідей)**

Київ – 2009

**ББК**
Ц4 (4Укр)39
П-768

У збірнику матеріалів п’ятого науково-практичного семінару 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. **Голь В. Д., Солодовник В. І.** Аспекти застосування атмосферних оптичних систем передачі для радіорелейного зв'язку…… 12
2. **Ільяшов О.А.** Полігауссовський розподіл структурних сигналів у телекомунікаційних мережах спеціального призначення…….. 22
3. **Кувшинов О. В.** Методи оперативного управління засобами завадозахисту військових систем радіозв'язку……..... 27
4. **Міночкін А.І., Романюк В.А.** Координація та інтелектуалізація рівнів OSI – нова парадігма управління мобільними радіомережами……... 31
5. **Науменко М. І.** Самоорганізація в системі підготовки військових фахівців…… 37
6. **Польщиков К.О.** Методи управління інтенсивністю потоків даних в мобільній радіомережі спеціального призначення…….. 41
7. **Приходько Ю. І.** Методологічні засади інноваційного розвитку військової освіти…… 48
8. **Слюсар В. І.** Метаматеріали в MIMO-антеннах……. 53


### (Тези доповідей)


1. **Ананьїн О. В.** Компенсація впливу завад в каналі радіоуправління системи радіозв'язку…….. 65
2. **Андреєв Б.М., Терещенко О.М.** Характеристики надійності елементів і мереж у системах зв'язку……... 66
3. **Ахтанін О. Г., Тарасюк Ю. М.** Обробка сигналів земних станцій на борту супутника ретранслятора з цифровою антенною решіткою…… 67
4. **Башкиров О. М.** Підвищення пропускної спроможності системи передачі даних про повітряну обстановку……... 68
5. **Бердников О. М.** Впровадження послуг *Triple Play* на телекомунікаційних мережах……... 69
6. **Берестов Д. С.** Визначення та формування профілів захищеності інформації в автоматизованих системах……. 70
7. **Бичков А. М., Нестеренко М. М.** Аналіз загроз безпеки інформації та методів протидії при використанні складних запитів у СУБД……..... 71
8. **Бовда Е. М.** Інформаційні технології в АСУ……... 72
9. **Богданов В. В.** Організаційно-технічні аспекти впровадження інфраструктури керування ключами в інформаційно-телекомунікаційних системах……. 74
10. **Богданов В. В., Маковецький О. М.** Методика вибору раціонального варіанта системи захисту інформації на основі експертних даних…… 76
11. **Богучарский В. В., Дідок Л. А.** Розвиток системи зв'язку та передачі даних в Збройних Силах України…… 78
12. **Богуш К. Ю.** Нормування форми сигналу для розпізнавання мови в інтелектуальних системах…….. 79
13. **Божко В. І.** Методологія архітектурної реалізації програмного забезпечення критичного застосування в системах що інтенсивно його використовують……..... 80
14. **Борисов І. В., Макарчук О. М.** Оцінка ефективності застосування сигнально-кодових конструкцій в каналах з навмисними завадами……..... 81
15. **Бугера М. Г., Сілко О. В.** Методика забезпечення автентичності навчальної звітності в об'єктно-орієнтованому навчальному середовищі…… 82

16. **Бурба О. І., Жилінський І. В.** Методика формування обрису автоматизованих систем на стадії розробки концепції…….. 83
17. **Бурячок В. Л., Кафтан В. О., Костюк Т. Я.** Класифікація об'єктів за методом кластерізації кількісних даних……... 84
18. **Вакуленко О. В., Гребеніченко А. Р.** Алгоритм вибору раціонального сценарію модернізації мережі доступу……. 85
19. **Вакуленко О. В., Липовий О. І.** Аналіз принципів побудови систем управління сучасними телекомунікаційними мережами в умовах надзвичайних ситуацій…... 87
20. **Вертегел С. Г., Тупкало В. Є.** Визначення рівня автоматизації завдань і функцій органів військового управління……. 89
21. **Ветлинський С. О, Раєвський В. М.** Узагальнена характеристика протоколів випадкового множинного доступу з контролем несучої…… 90
22. **Войтко Ю. М., Карпенко Б. О., Якорнов Є. А.** Визначення різниці різниць фаз в мікрохвильових фазових системах спеціального призначення…….. 92
23. **Восколович О. І.** Аналіз параметрів при проектуванні радіомодемів спеціального призначення з багаточастотними сигналами……..... 93
24. **Ган С.О.** Тендеції безпеки інформації в спеціальних інформаційно-комунікаційних системах…… 94
25. **Гахов С. О.** Методика оцінювання ефективності захисту інформації від несанкціонованого доступу в інформаційних системах спеціального призначення……. 95
26. **Генов М. С.** Комбіновані методи захисту поліграфічної продукції…….. 97
27. **Герасимов Б. М.,Шугалій Є. П.** Розподіл інформаційного ресурсу між робочими місцями оперативного персоналу органів управління військами……... 98
28. **Герасимов Б.М., Шугалій Є.П.** Методика синтезу структури органів управління військами по критерію оперативності…….. 99
29. **Гєлєсєв В. О., Карпенко Б. О., Якорнов Є. А.** Використання вагової міжкадрової обробки в системах спеціального призначення для сегментації рухомих об'єктів зображення……... 100
30. **Горбенко В. І., Заремський М. Й., Нищук А. М., Сілко О. В.** Процедура розподілу пам'яті автоматизованих комплексів спеціального призначення…… 101
31. **Горбенко В. І., Павлюк С. В., Ратанін Є. Г., Сілко О. В.** Процедура визначення параметрів матриці перемежіння в телекомунікаційних системах…… 102
32. **Горьков В. К.** Організація розробки технічного проекту інформаційних систем……..... 103
33. **Грохольський Я.М.** Гібридне кодування та винесене компандування…… 105
34. **Гулак Ю. С., Долгаленко О. В.** Удосконалення системи захисту об'єктів та підрозділів Збройних Сил від порушників…… 107
35. **Гулак Ю. С.** Питання захисту інформації при підготовці і в ході ведення оборонної операції Збройними Силами України…… 108
36. **Гурський Т. Г., Марченко А. О., Толюпа С. В.** Перспективні напрямки розвитку широкосмугових систем радіозв'язку…….. 109
37. **Дідик В. О., Натальченко О. О., Шевченко Л. Ю.** Забезпечення безпеки АСУ……... 110
38. **Драглюк О. В., Ліманська О. Л.** Децентралізовані однорангові мережі передачі даних ……..... 111
39. **Драчук О. В.** Використання технології внесення помилок для пошуку дефектів безпеки в програмних продуктах……. 112

40. **Дружинін С. В., Климович О. К., Захараш О. М.** Аналіз стратегій маршрутизації в телекомунікаційній мережі військового призначення……..... 113
....
41. **Дружинін С. В., Рвачова Н. В.** Методика визначення доступної для трафіку даних пропускної спроможності телекомунікаційної мережі……... 114
42. **Дружинін С. В., Янсонс Я. В., Шинкарьов М. М.** Імітаційна модель для визначення якості обслуговування в мережах IP телефонії……..... 115
43. **Єсаулов М.Ю.** Алгоритм об'єктивної кластеризації загроз безпеки…… 116
44. **Загребельний О. Ю., Біленький А. В.** Нечітка система управління доступом в мобільних радіомережах……..... 117
45. **Залогін С. М., Іванков Ю. М., Малишкін В. В., Тамаровський В. В.** Оцінка ефективності обчислювальної системи масового обслуговування спеціального призначення…… 118
46. **Замаруєва І. В., Бабіч О. М.** Методика виявлення ознак маніпулювання свідомістю в інформаційних текстових повідомленнях ЗМІ…… 119
47. **Заруднєв Д. І., Стейскал А. Б.** Математична модель дискретних повідомлень цифрових систем радіозв'язку…….. 120
48. **Захараш О. М.** Аналіз методів моделювання імовірнісно-часових характеристик мультисервісних мереж зв'язку…….. 122
49. **Звір В. Б.** Шляхи забезпечення ефективного функціонування телекомунікаційної мережі спеціального призначення ……. 123
50. **Звягінцев О. Г., Ладик О. І.** Моделювання системи стільникового зв'язку WCDMA…… 124
51. **Іваненко О. О.** Шляхи удосконалення волоконно-оптичної системи передачі…... 125
52. **Ільінов М. Д., Шафранський О. П., Шацький І. О.** Результати експериментального дослідження електричних характеристик низькопрофільних антен на циліндричній поверхні…….. 126
53. **Ільінов М. Д., Шацький І. О., Шафранський О. П.** Антена базової станції системи мобільного радіозв'язку…….. 128
54. **Ільницький С. В., Сілко О. В.** Аналіз існуючих підходів щодо синтезу системи дистанційного навчання, проблеми та шляхи їх вирішення……... 130
55. **Каравацький В. О.** Тенденції розвитку елементної бази засобів телекомунікацій, теорії електрозв'язку та антенно-фідерних пристроїв…….. 132
56. **Карловський І. В., Штаненко С. С.** Шляхи вдосконалення діагностики радіоелектронної апаратури військового призначення…… 133
57. **Карпенко Б. О., Лінчевська І. Л., Мазуренко О. В., Якорнов Е. А.** Дискретні антенні системи спеціального призначення з контрольним розділенням радіосигналів за відстанню……. 134
58. **Катін П. Ю., Кузавков В. В., Гунько Д. Ю.** Тестування програм обробки зображень з чисельною оцінкою ефективності для систем відео спостереження.... 135
59. **Коваленко А. О.** Удосконалений стеганографічний метод центрування значень колірних компонент……... 137
60. **Ковбаса Ю. В.** Аналіз стандартів технології CDMA……. 138
61. **Кокотов О. В., Шевченко А. С.** Модель загроз інформації в системах безпроводового зв'язку в умовах ведення інформаційної війни……..... 140
62. **Колос Ю. О., Манько О. В., Орищук І. О.** Характеристики та параметри телекомунікаційних мереж як засобу здійснення інформаційної боротьби……..... 141

63. **Колос Ю. О., Міхєєв Ю. І.** Технології використання засобів інформаційної боротьби в інформаційних мережах…….. 142
64. **Кондратюк А. Г.** Шляхи підвищення функціональної живучості напрямків телекомунікаційної мережі спеціального призначення…….. 143
65. **Кононова І. В., Петров А. В.** Аналіз можливостей IP-телефонії з погляду безпеки функціонування мережі…… 144
66. **Корнієнко О. О., Правило В. В.** Бездротові технології доступу до телекомунікаційних мереж……... 146
67. **Костина О. М.** Напрями розвитку засобів зв'язку і автоматизації в Збройних Силах України……. 147
68. **Коцюба В. П., Ніколаєнко Д. М.** Розвиток управління частин і підрозділів зв'язку та інформаційних систем в сучасних умовах…….. 148
69. **Коченовський Д. О.** Перспективи використання GRID технологій в сучасних телекомунікаціях ……... 149
70. **Кочетков О. В.** Підвищення завадо - стійкості пакетів повідомлень у цифрових лініях зв'язку рухомих об'єктів……. 150
71. **Круковський І. А., Перегуда О. М.** Методика оцінки якості програмного забезпечення……... 151
72. **Круковський І. А.** Розширені вимоги до реалізації OLAP у прикладних інформаційних системах……... 152
73. **Крупська М. В., Ладик О. І.** Удосконалення технології широкосмугового доступу CDMA……... 153
74. **Кувшинов О. В., Жук О. Г.** Методика управління режимами роботи засобів радіозв'язку в умовах навмисних завад……... 155
75. **Кузавков В. В.** Основи інформаційної війни……. 156
76. **Кулажський В. І., Кульчицький О. С.** Інформаційна безпека **с**истем планування та управління адміністративно-господарською діяльністю……. 158
77. **Куліков С. П., Комаров В. С., Олексіюк В. В., Демченко Р. М., Комаров Р. О.** Тенденції розвитку безпілотних літальних апаратів як елементу геоінформаційних систем……... 160
78. **Куляниця О. Й., Рябченко А. М.** Особливості опису широкосмугових радіосигналів…… 161
79. **Лаврут О. О.** Динамічна зміна режиму функціонування системи супутникового зв'язку за допомогою використання тензорного аналізу…… 163
80. **Ладик О. І., Головченко І. О.** Перспективи застосування технології MIMO……. 164
81. **Ладик О.І., Донець А.Ю., Завдовєєва О.С.** Застосування імітаційного моделювання процесів в середовищі GPSS…….. 165
82. **Ладик О. І., Муравйова О. Г.** Стандарт IPV6 у мобільних мережах…….. 166
83. **Липський О. А., Коваленко І. Г., Максименко Ю. Л., Васильченко В. В.** Аналіз впливу навмисних завад на радіорелейні лінії зв'язку при передачі IP трафіку……. 167
84. **Лисенко А. І., Валуйський С. В.** Підвищення стійкості мобільних радіомереж зв'язку за рахунок використання супутникових та псевдосупутникових систем... 168
85. **Лисенко О. І., Кірчу П. І.** Застосування адаптивної системи керування безпілотним літальним апаратом при створенні локальної мережі зв'язку спеціального призначення……. 169
86. **Лисенко О. І. Мірошниченко А. В.** Синхронізація базових станцій мережі мобільного зв'язку нового покоління…… 170
87. **Литвиненко Є. О., Помін А. Г.** Економічна доцільність побудови корпоративного CDMA…….. 171
88. **Літвін К.К., Літвін К.І., Шелепенко Ю.В.** Модифікація алгебраїчного декодера

в апаратурі передачі даних……. 173
89. **Літвін К. І., Літвін К. К., Шелепенко Ю. В.** Блокові сигнально-кодові конструкції каскадного типу……. 174
90. **Лук'янчук І. В.** Підвищення безпеки передачі інформації в системах радіозв'язку з використанням широкосмугових сигналів…….. 175
91. **Любарський С. В., Лазар Ю. В.**Оцінка ефективності застосування програмних прийомів шифрування інформації в додатках, розроблених на мовах високого рівня…….. 176
92. **Люлін Д. О., Іохов О. Ю., Кротов В. Д**. Перешкодостійкість DTMF сигналів при передачі коротких повідомлень в системах зв'язку ЗСУ……... 177
93. **Малигін М. М.** Модель оцінки рівня захищеності інформації в автоматизованих системах на базі теорії нечітких мір та нечітко-інтегрального обчислення…… 179
94. **Малюга А. В.** Методи та засоби контролю знань тих, хто навчається у системах дистанційного навчання……. 180
95. **Малярчук М. В., Слюсар В.І.** Попередня фільтрація OFDM сигналів в системі MIMO при додатковому стробуванні відліків АЦП……... 182
96. **Мацаєнко А. М., Цімура Ю. В., Шацький І. А.** Синфазні антенні решітки на низькопрофільних випромінювачах…….. 183
97. **Машков О. А., Шуренок А. В., Самчишин О. В.** Застосування інформаційної системи забезпечення функціональної стійкості системи радіомоніторингу……... 185
98. **Мєшков І. Н., Черкасова Ю. О., Висоцька Т. М., Нечушкін М. П.** Тенденції розвитку мереж рухомого радіозв'язку……. 186
99. **Микусь С. А., Романюк І. М.** Основні фактори, які впливають на процес організації зв'язку під час підготовки миротворчих операцій…… 187
100. **Микусь С. А.** Методика оцінки районів розгортання вузлів зв'язку пунктів управління з'єднання та військових частин……. 190
101. **Міцан І. Б.** Методичний підхід до оцінювання якості поліграфічної продукції спеціального призначення……. 192
102. **Могилевич Д. І., Правило В. В., Явіся В. С.** Стан та перспективи використання бездротових технологій в телекомунікаційних мережах……. 194
103. **Назаревич В. В.** Математична модель для управління територіально розподіленими підрозділами на основі геоінформаційних систем……... 196
104. **Настич Ю. Б., Бугера М. Г.** Розробка алгоритму шифрування інформації „APR" комбінованим методом на основі залишкових чисел…….. 197
105. **Наталенко П. П., Шелепенко Ю. В.** Перспективи і напрями розвитку інформаційно-телекомунікаційних систем……. 198
106. **Науменко Ю. Б.** Розширена модель захисту критичних систем управління на трьох рівнях інформаційної взаємодії……. 199
107. **Недайбіда Ю.П., Ляшенко В.Г., Ромащенко В. М., Шугалій О.О.** Модель контролю завантаження АСУ в реальному часі функціонування систем управління тактичної ланки ЗСУ…….. 200
108. **Носовськой Р. О., Горбенко В. І.** Структура і склад автоматизованої навчальної системи мови програмування асемблеру з елементами захисту інформації……... 202
109. **Овсянніков В. В., Паламарчук С. А., Паламарчук Н. А.** Вимоги щодо захисту інформації в автоматизованих системах рухомих засобів зв'язку…… 203
110. **Овчаров О. О.** Метод турбо кодування з повторенням для підвищення завадозахищеності багатоканальної програмованої радіостанції в умовах впливу навмисних завад…….. 204
111. **Ольшанський В. В., Бортнік Л. Л.** Задача розробки вдосконаленого методу

оцінки радіоканалу…….. 205
112. **Панченко А. Ю. Хусаінов П. В.** Вибір засобів візуалізації мережевого оточення об'єкта атаки…… 206
113. **Панченко І. В.** Дослідження фаззі-систем автоматичного регулювання потужності передавача при „Глибоких" завмираннях сигналу в адаптивному каналі радіозв'язку……. 207
114. **Пивовар С. О.** Методика оцінки якості обслуговування в IP мережах із застосуванням нечіткої логіки…… 209
115. **Пилипенко А. А.** Алгоритм підвищення точності наведення в цифрових антенних решітках з високою разрешаючою можливістю за допомогою кореляційної матриці…….. 210
116. **Півень С. О., Іванов Б. П.** Удосконалення зв'язку в Збройних Силах України.... 211
117. **Польщиков К.О., Здоренко Ю.М., Шкіцькій В.В.** Аналіз методів боротьби з перевантаженнями, що використовуються при передаванні TCP-трафіку в телекомунікаційних мережах……. 212
118. **Пономарьов Ю. В., Нетребко Р. В.** Моделювання як спосіб підвищення якості метрологічної підготовки майбутніх інженерів…… 213
119. **Правило В. В., Шарапанюк О. А.** Метод формування спектра шумоподібного сигналу……. 215
120. **Прищепа Т. О., Лисенко О. І.** Використання еволюційних структур для розв'язання задач синтезу та управління телекомунікаційними системами…… 216
121. **Прохорчук Ю. Ю., Макарчук О. М.** Послідовний аналіз статичних випробувань..... 218
.....
122. **Проценко М. М.** Методика вибору вейвлет-функції для обробки цифрових сигналів……... 219
123. **Радзівілов Г. Д., Бевзюк Б. М.** Методи оцінки факторів, що впливають на якість передачі у ВОСП зі спектральним розподілом каналів……... 220
124. **Радзівілов Г. Д., Труш О. В.** Оцінка динамічної точності системи фокусування станції лазерного запису……... 221
125. **Раєвський В. М.** Порівняльний аналіз кінцевих засобів проводового телефонного зв'язку…… 222
126. **Раєвський В. М., Тихонюк С. В.** Можливість застосування методу множинного доступу з контролем несучої та визначенням конфлікту в корпоративних радіомережах……... 223
127. **Різуненко А. О.** Метод зменшення ентропії значень коефіцієнтів трансформант зображень для побудови графічного компресора…….. 225
128. **Роговець М. А., Шуренок В. А., Дзюбчук Р. В.** Методика когнітивного аналізу інформаційно-аналітичної роботи……..... 226
129. **Розум І. Ю.** Відеозв'язок в перспективній системі зв'язку механізованої бригади……. 227
130. **Ролік О. І., Можаровський П. Ф., Покотило О. О.** Застосування агентського підходу до управління інформаційно-телекомунікаційною системою АСУ спеціального призначення……. 228
131. **Романов О. І., Нестеренко М. М.** Розвиток систем управління телекомунікаційними мережами на базі стандартів TMN…….. 230
132. **Рябцев В. В., Субач І. Ю.** Структура інтелектуальної системи управління якістю освіти та підготовки…… 231
133. **Савісько П. А.** Оперативно – тактичні принципи побудови 233

АСУВ……..
134. **Савісько П. А., Романюк І. М.** Особливості організації інформаційного процесу управління на основі нових (сучасних) інформаційних технологій…….. 235
135. **Самойлов І. В., Кокотов О. В.** Використання експертних парних порівнянь для побудови нечітких відношень інтервального типу в системах діагностики…… 237
136. **Сівківська А. П., Ладик О. І.** Розвиток технології четвертого покоління стільникового зв'язку …….... 238
137. **Сілко О. В.** Методика оцінки ефективності модульної побудови комплексів засобів автоматизації радіотехнічних підрозділів повітряних сил Збройних Сил України……. 239
138. **Слотвінська Л. І.** Захист поліграфічної продукції тисненням…….. 240
139. **Слюсар І. І., Слюсар В. І., Зінченко А. О.** Шляхи підвищення потенційних можливостей систем зв'язкуз цифровим діаграмо утворенням…… 241
140. **Слюсар В.І., Масесов М.О.** Вимірювання характеристик радіоканалів MIMO та МУЛЬТИ-MIMO в приймачах станцій спеціального призначення…… 242
141. **Слюсар В. І., Троцько О. О.** Оцінювання впливу ефекту допплера на пропускну спроможність телекомунікаційних систем з безпілотними літальними апаратами……. 243
142. **Сова О. Я., Жук О. В., Жук П. В.** Проблема управління потоками даних у мобільних радіомережах з динамічною топологією…… 244
143. **Солодовник В. І., Голь В. Д.** Цифрові мережі нового покоління на базі технології ***DWDM*** із застосуванням ***EDFA***–підсилювачів……. 246
144. **Степанов М. М., Уварова Т. В.** Використання геоінформаційного забезпечення для вирішення завдань з модернізації озброєння та військової техніки…….. 247
145. **Степанюк О. А.** Аналіз конкурентних технологій покоління 4G: LTE, MOBILE WIMAX…….. 248
146. **Стрюк О. Ю., Дядик Д. Ф.** Метод аналітичної оцінки ступеня стиску зображень…… 249
147. **Стрюк О. Ю.** Метод підвищення якості обслуговування абонентів базової станції радіомережі……. 250
148. **Субач І. Ю., Міщенко В. О., Симоненко О. А., Саєнко О. Г.** Моніторинг даних в інформаційних мережах…….. 252
149. **Субач І. Ю., Міщенко В. О., Саєнко О. Г.** Методологічні основи інтелектуального здобуття знань з систем моніторингу інформаційних мереж…... 253
150. **Сушин О. М., Шугалій Є. П.** Захист інформації від витоку технічними каналами…….. 254
151. **Твердохлібов В. В.** Напрями розвитку системи зв'язку сил спеціального призначення Збройних Сил України…… 255
152. **Терезюк О. Э., Шацький І. О.** Колінеарні антени……..... 256
153. **Тимченко О. М.** Основні принципи побудови та напрями розвитку автоматизованих систем управління Збройних Сил розвинених країн світу…… 258
154. **Ткаленко О. М.** Протокол MPLS – нова технологія для використання у мережах IP……..... 260
155. **Ткачов П. О.** Методи та способи захисту програмного забезпечення, яке розповсюджується на оптичних носіях інформації, від несанкціонованого використання, копіювання та тиражування……. 261
156. **Токовенко А. В., Ладик О. І.** Порівняльні властивості технології DECT ТА Wi-Fi…… 262

157. **Толюпа С. В., Мінакова М. В.** Реалізація інтелектуальних послуг на мультисервісних мережах нового покоління…… 263
158. **Фесьоха В. В., Хусаінов П. В.** Вимоги до мультиагентної системи аналізу мережевого трафіка…… 265
159. **Фігурна О. С.** WiMAX: безпровідна магістраль у майбутнє……..…. 266
160. **Фриз П. В., Рихальський О. Р.** Удосконалена система обслуговування космічних апаратів в умовах однопунктної технології управління…… 267
161. **Хусаінов П. В., Головко О. О.** Вибір способу представлення структури мережі в пам'яті ЕОМ…….…….…..... 269
162. **Цема В. Ф., Ладик О. І.** Функції тарифікації підсистеми IMS…….. 270
163. **Чумак В. К., Палій С.С.** Вплив перехресних завад в системі MIMO……... 271
164. **Чучмій А.В.,Гамалій Н.В.** Шляхи удосконалення інформаційної боротьби в Збройних Силах України…… 272
165. **Шевцов С. Ю.,Фесенко О. Д.** Протиріччя між логічною структурою і структурою інформаційних потоків в мережах SDH…….. 273
166. **Шевченко А. С., Артюх С. Г.** Аналіз загроз інформації в системі широкосмугового зв'язку стандарту IEEE 802.16 ……..... 274
167. **Шемендюк О. В., Хусаінов П. В.** Особливості пріоретизації повідомлень в різних умовах діяльності……..... 275
168. **Шестаков В. І., Гудзь С. М.** Формалізація задачі розподілу сил та засобів моніторингу мережі інтернет…… 276
169. **Шохін Б. П.**, **Кафтан В. О., Костюк Т. Я.** Інформаційно-пошукова підсистема в системі розвідки…….. 277
170. **Щербакова Т. П., Ладик О. І.** Інтелектуальні системи інформаційної безпеки.... 278
171. **Яблокова С.П., Куляниця О.Й., Кальчук І.А.** Матричний метод класифікації радіозасобів мереж зв'язку……... 279
172. **Явіся В.С., Войцеховський Ю.В.** Волоконно-оптичні систем передачі з дослідженням методів компенсації хроматичної дисперсії…… 280
173. **Явіся В. С., Корнієнко С. В.** Аналіз можливостей локальних обчислювальних мереж…….. 281
174. **Явіся В. С., Легкобит В. С.** Перспективи впровадження нових стандартів телекомунікаційного обладнання…….. 283
175. **Явіся В. С., Порох С. В.** Оцінка можливості впровадження додаткових послуг в телекомунікаційній мережі підприємства……..... 284
176. **Явіся В. С., Чередниченко О. Ю.** Перспективи використання технології *xDSL* в мережах загального користування…….…..... 285
177. **Явіся В. С., Шкоденко Ю. П.** Варіант розвитку мереж мобільного зв'язку……... 286

**Гуманітарна секція**

1. **Ананьїн В.О., Пучков О.О.** Роль військової освіти в формуванні особистості військового професіонала……. 287
2. **Бецько О.С.** Інформаційно-телекомунікаційні технології як засіб індивідуалізації навчання та формування особистості курсантів вищих військових навчальних закладів……... 289
3. **Волошина Н.М., Терещенко Т.П.** Сучасні аспекти військово-патріотичного виховання майбутніх фахівців телекомунікаційних систем та мереж спеціального призначення……. 291
4. **Гавриленко К.М.** Іноземна мова як засіб розвитку комунікативних здібностей

у курсантів вищого військового навчального закладу…….. 293
5. **Гнаткевич Л.О.** Проблеми формування національної технічної інтелегенції…... 294
6. **Гнатовська Л.Ю.** Телекоммунікаційні системи та формування особистості фахівця ……... 295
7. **Єфімова О.М.** Педагогічні підходи та вплив інформаційного суспільства на розвиток особистості у процесі навчання в ВТНЗ…….. 297
8. **Жицька С.А., Жицький К.О.** Роль іноземних мов у формуванні особистості військового фахівця…….. 299
9. **Зарівна О.Т., Гангал А.В., Хімай Н.І.** Підготовка військового професіонала в західній військовій школі…….. 301
10. **Лягіна І. А.** Культурна свідомість як чинник формування полілінгвокультурної компетенції студентів немовних вузів на заняттях з англійської мови…… 303
11. **Назаренко І. М.** Роль естетичного виховання у формуванні особистості майбутніх офіцерів……. 305
12. **Несин Ю. М.** Нові інформаційні технології та прийняття рішень…….. 306
13. **Романюк І. М., Микусь С. А.** Принципи кредитно-модульної технології навчання…….. 307
14. **Романюк І. М.** Модульні технології навчання як напрямок у досягненні відповідної якості вищої військової освіти……. 310
15. **Уваркіна О.В., Степаниця С.Л., Коваль А.М.** Інформаційна безпека як чинник захисту особистості в сучасних умовах…….. 312
16. **Шаблій О. С.** Сучасні проблеми формування особистості фахівця телекомунікаційних систем та систем зв’язку спеціального призначення в інформаційному суспільстві……. 314
17. **Шалова Н.С.** Формування особистості національної технічної інтелігенції в умовах сучасного суспільства……..... 315

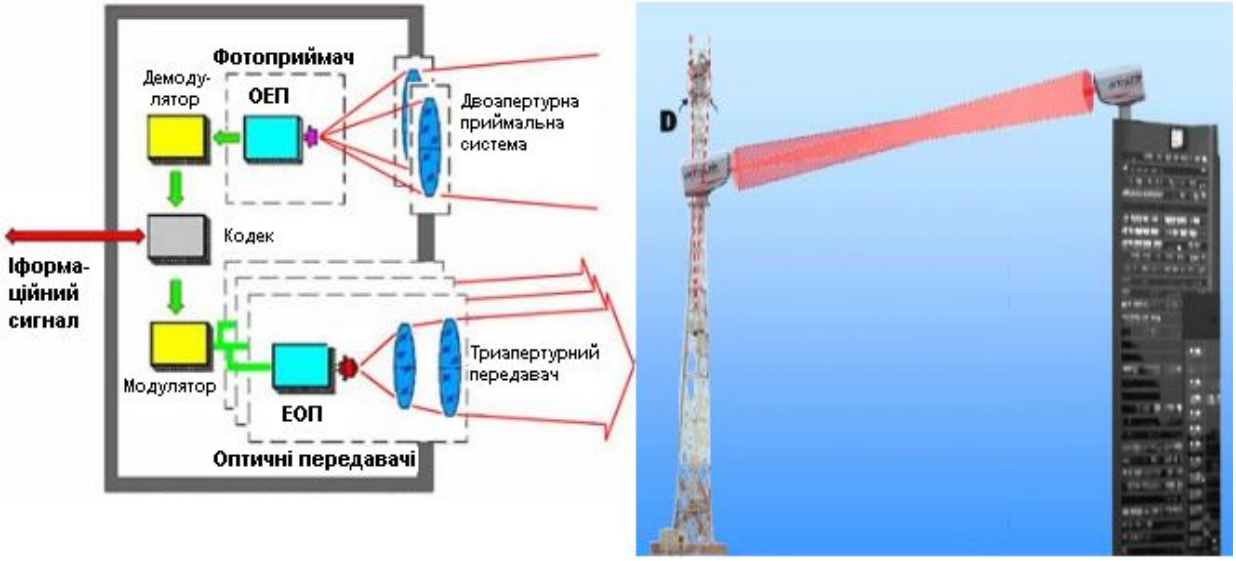
к.т.н. Голь В.Д. (ВІТІ НТУУ „КПІ”)
Солодовник В.І. (ВІТІ НТУУ „КПІ”)

# АСПЕКТИ ЗАСТОСУВАННЯ АТМОСФЕРНИХ ОПТИЧНИХ СИСТЕМ ПЕРЕДАЧІ ДЛЯ РАДІОРЕЛЕЙНОГО ЗВ’ЯЗКУ

Атмосферні (бездротові, відкриті) оптичні системи передачі (АОСП) призначені для передачі цифрових потоків даних через атмосферу в інфрачервоному оптичному діапазоні довжин хвиль. Сьогодні разом із стандартним терміном АОСП в літературі зустрічаються наступні назви, що вживаються для таких систем:

– АОЛ(П) – Атмосферна Оптична Лінія (Передачі);
– БОКЗ – Бездротовий Оптичний Канал Зв’язку;
– БОЛЗ – Бездротова Оптична Лінія Зв’язку;
– ЛАЛ – Лазерна Атмосферна Лінія.

Сама технологія передачі ґрунтується на передачі даних модульованим випромінюванням в інфрачервоній частині спектра через атмосферу. Оптична атмосферна система зв’язку між двома пунктами складається з двох спарених приймально-передавальних пристроїв (рис. 1 ,*а*), розташованих в межах прямої видимості на обох кінцях лінії і направлених один на одного (рис. 1 ,*б*). Передавачем служить напівпровідниковий лазерний діод (робочий діапазон довжин хвиль 810, 830 або 910 нм). У передавачі також знаходиться модулятор оптичного випромінювання сигналом, що передається. Модульований лазерний промінь колімірується оптичною системою і прямує у бік приймача. Як приймач використовується високочутливий фотодіод (робочий діапазон довжин хвиль 750 ... 950 нм). Випромінювання впливає на фотодіод, унаслідок чого регенерується початковий модульований сигнал. Далі, сигнал демодулюється і перетворюється в сигнали вихідного інтерфейсу. З обох сторін лінії використовується система лінз, з боку передавача – для отримання вузького, когерентного та спрямованого променя, а з боку приймача – для фокусування прийнятого випромінювання на фотодіод.




*а* *б*

Рис. 1. Пояснення роботи АОСП

Для організації дуплексного каналу передачі в кожному приймально-передавальному блоці встановлені модуль приймача і від одного до трьох модулів передавачів, які разом забезпечують прийом і передачу по паралельних променях. Все устаткування забезпечує

„прозору” трансляцію даних через себе і не вимагає додаткових мережевих пристроїв для конвертації або маршрутизації пакетів даних.

Основними перевагами використання АОСП в порівнянні з іншими бездротовими рішеннями є: висока конфіденційність зв’язку, невикористання радіодіапазону, відсутність необхідності в дозволах на використання радіочастотного спектра і відсутність принципових обмежень швидкості передачі.

**Організаційні переваги**

АОСП **не використовує радіодіапазон** і не створює перешкод в радіочастотному спектрі, внаслідок цього дане устаткування не потрапляє під дію Закону України про радіочастотний ресурс, оскільки під радіоустаткуванням маються на увазі системи, що працюють в діапазоні до 400 ГГц. Реальні частоти оптичних систем в тисячі разів вище встановленої межі. Установка оптичних систем не приводить до порушення роботи існуючих радіосистем і устаткування. Як результат застосування АОСП не потребує дозволів УДЦР і інших регулюючих органів. Робота устаткування не пов’язана з регулярними платежами за користування середовищем передачі, як це має місце у разі радіосистем. У містах, а особливо, в мегаполісах доступні частоти настільки щільно використовуються, що це очевидна перевага грає домінуючу роль. До того ж час, необхідний на підготовку і отримання документів для експлуатації радіосистем складає біля півроку, якщо взагалі вільний діапазон є в наявності.

АОСП вимагає **малий час для розгортання**. Оптичне устаткування вимагає мінімальних потужностей для роботи (десятки Вт), підключається, найчастіше, безпосередньо в порти стандартного мережевого або телекомунікаційного устаткування і не вимагає багато місця для розміщення.

**Технічні переваги**

АОСП **не чутлива до радіоперешкод**. Установка бездротових оптичних систем можлива навіть в зонах з високими перешкодами від радіоустаткування або промислового устаткування, де використання радіосистем проблематичне.

**Висока скритність та розвідзахищеність** тракту. Жодна бездротова технологія передачі не може запропонувати таку конфіденційність зв’язку. Перехопити сигнал можна тільки встановивши сканери-приймачі безпосередньо в промінь від передавачів. Практична складність виконання цієї операції, а також легка можливість визначення наявності стороннього приймача у проміні, роблять перехоплення практично неможливим. Наявність лазерних променів не можна визначити за допомогою різноманітних сканерів.

**Відсутнє** принципове **обмеження на швидкість передачі**. Атмосфера, як середовище розповсюдження оптичних сигналів, позбавлена низки явищ, які негативно впливають на процес розповсюдження і суттєво обмежують швидкість передачі. Це одна з ключових технічних переваг атмосферних оптичних систем зв’язку, яке викликало бурхливе зростання інтересу до технології серед виробників і потенційних замовників.

**Мінімальна затримка в тракті передачі та прозорий механізм передачі**. Системи АОСП є всього лише конверторами середовища передачі, тобто немає особливої різниці в протоколах передачі і т. п. Відсутність складних перетворень сигналу приводить до того, що затримка в тракті передачі, що вноситься оптичною системою, стає незначною.

Аналіз чинників, що визначають умови функціонування систем зв’язку і вищенаведених переваг АОСП, дозволяє сформулювати основні напрями їх впровадження [4]. АОСП можуть застосовуватися в наступних випадках:

– як абонентські лінії і лінії прив’язки (для військового зв’язку, в першу чергу, на лініях, які розгортаються поблизу з лінією зіткнення з супротивником);

– на внутрішньооб’єктових і сполучних лініях;

– для утворення сітки ліній в локальних обчислювальних мережах;

– як релейні вставки у ВОСП (наприклад, при подоланні водних перешкод і т. п.);

– для зв’язку між ретрансляторами на льотнопідйомних засобах (ЛПЗ);

– для зв’язку між ретрансляторами на ЛПЗ і космічних апаратах (КА);
– для зв’язку між ретрансляторами на КА;
– на лініях ЛПЗ (КА) – підводний об’єкт;
– для зв’язку між кораблями флоту (в першу чергу, військово-морських сил).

З іншого боку, в діапазоні, що використовують для роботи АОСП, необхідно враховувати цілий ряд чинників, які впливають на якість зв’язку. Основними з них є: погодні умови і вплив атмосфери.

**1. Погодні умови**

Особливі погодні умови, такі, як дощ, сніг, туман і т. д., можуть значно погіршити видимість і, таким, чином понизити ефективність використання діапазону інфрачервоного зв’язку. Такі умови мінливі, проте, загальні сезонні тенденції визначаються кліматичною зоною, широтою і іншими відомими географічними параметрами місцевості, де планується установка устаткування. Інші чинники, що погіршують видимість, це піщаний пил, міською смог і різні види аерозолів.

**2. Вплив атмосфери**

Різні чинники, такі, як вологість, атмосферний тиск і склад атмосфери (процентний зміст молекул кисню, азоту, вуглекислого газу і т. д.) мають вплив на працездатність атмосферного оптичного тракту не менш значний, чим сніг або туман. Наприклад, молекулярний склад атмосфери має істотне значення, оскільки молекули можуть створювати вузькі лінії або цілі смуги поглинання в робочому спектрі випромінювання системи, поглинаючи від енергії світла до 80 … 90 % і більше. Таким чином, за певних умов, атмосфера, залишаючись прозорою у видимому спектрі, в той же самий час може виявитися непрозорою в конкретній ділянці інфрачервоного спектра.

Крім того, в атмосфері спостерігаються турбулентні явища, які приводять до флуктуації показника заломлення середовища, коливанням світла і спотворенням сигналу, що приймається. Проте, не дивлячись на вказані проблеми, атмосферний оптичний зв’язок виявився цілком надійним на відстанях декількох кілометрів.

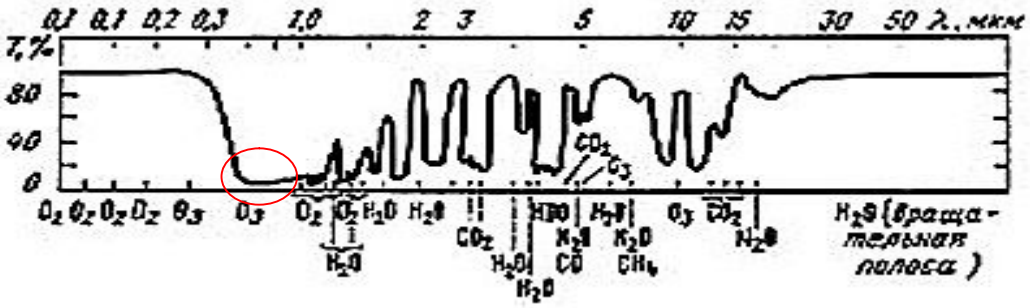
Атмосфера міст, насичена різними домішками і багата по газовому складу, помітно відрізняється по пропускних спроможностях від істотно чистішої атмосфери сільської місцевості. Також, помітно відрізняється склад атмосфери приморських зон від континентальних, субтропіків від арктичних зон. Крім того, склад атмосфери міняється в залежності від пори року. Облік всіх цих чинників дозволяє більш повно реалізувати можливості бездротових оптичних систем.

За чисто якісними ознаками вказані явища можна розділити на три основні групи: поглинання і розсіяння молекулами газів повітря, ослаблення на аерозолях (пил, дощ, сніг, туман) і флуктуації випромінювання на турбулентностях атмосфери. Стисло зупинимося на кожному з цих явищ.

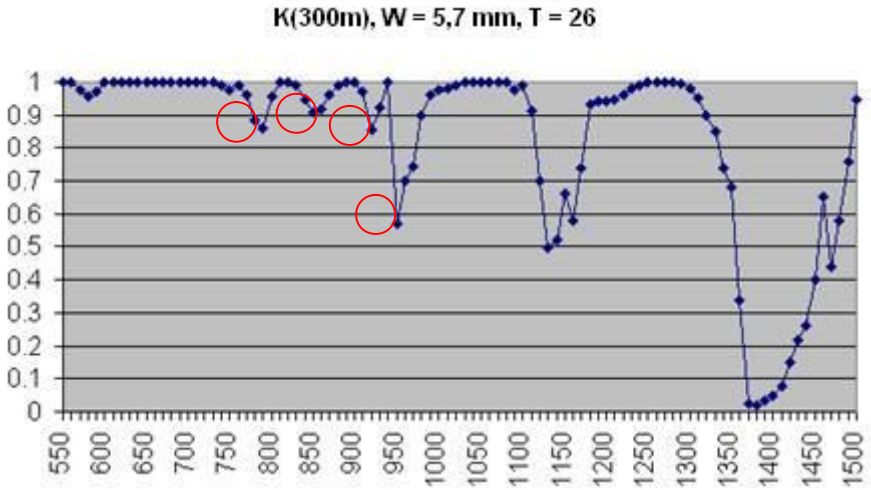
**Поглинання світлового потоку** видимого і інфрачервоного діапазонів визначається, перш за все, молекулярним поглинанням, украй нерівномірним за частотою. Воно максимальне на резонансних частотах молекул повітря, води, вуглекислого газу, озону і інших компонент атмосфери. На рис. 2 ,*а* приведений спектр поглинання сонячного випромінювання, кожна із зображених тут смуг поглинання, є результатом накладення і перекриття декількох смуг як одного і того ж газу, так і різних газів. У інших атмосферних умовах і інших регіонах подібні графіки розрізнятимуться із-за різного змісту водяної пари і інших компонент повітря. Є ділянки спектра, де поглинання незначне, вони називаються вікнами прозорості. Очевидно, що найбільш придатним для роботи АОСП є діапазон довжин хвиль трохи нижчий за 1 мкм. Проте при меншому кроці зміни довжини хвилі (рис. 2 ,*б*) і у вікнах прозорості існують цілі сукупності різних смуг поглинання.

Якщо довжина хвилі лазера відома, то поглинання його випромінювання може бути заздалегідь визначене для будь-яких реальних умов в атмосфері. Якщо лазерне випромінювання потрапляє в центр сильної лінії спектра, то воно поглинається атмосферою

на 100 % навіть на невеликій відстані. Тому для АОСП слід брати лазери з випромінюванням, що знаходиться на ділянках спектра атмосфери, зайнятих широкими вікнами прозорості або в проміжках між слабкими лініями поглинання, в мікровікнах прозорості. При цьому частота випромінювання повинна бути стабілізована з достатньо високою точністю, особливо якщо вона знаходиться на близькій відстані від лінії поглинання газів.




*а*.




*б*.

Рис. 2. Залежність поглинання $T_0$, % (*а*) та коефіцієнта передачі *K* (*б*) в атмосфері від довжини хвилі сонячного випромінювання

Крім молекулярного поглинання розповсюдженню променя заважає **молекулярне розсіяння** променистої енергії мікрозгустками молекул повітря, що мають різну щільність і різні показники заломлення. Ці неоднорідності в газовому середовищі вельми нестабільні і залежать від місцевих температурних умов, пори року і доби, а також від вмісту домішок в кожній конкретній мікрозоні атмосфери. Молекулярне розсіяння достатнє добре вивчено. Складені докладні таблиці коефіцієнтів розсіяння у видимій і інфрачервоній областях спектра, які забезпечують достатньо точний кількісний розрахунок втрат енергії випромінювання на заданій відстані [1–3]. Цей тип розсіяння не надає істотної шкоди АОСП на відміну від аерозольного розсіяння, яке буде розглянуто нижче.

Атмосфера є механічною сумішшю з газів, пари, крапель рідини і твердих частинок. У ній завжди в змінній кількості присутні пил, дим, кристали льоду. Тому атмосфера є аерозолем, склад якого безперервно змінюється із-за перемішування. Кажучи про **аерозольне розсіяння** загалом, мають на увазі аерозольне ослаблення, обумовлене не тільки розсіянням, але і поглинанням випромінювання частинками аерозоля. Всі типи атмосферних аерозолів можна об’єднати в наступні основні класи: хмари, тумани, серпанки, поморозь і опади – дощ або сніг. У хмарах і туманах найбільш вірогідне значення радіусу частинок складає 5 … 6 мкм, а в серпанках на 1 … 2 порядки менше.

Тому ослаблення мікронного випромінювання в серпанках нижче. При цьому теоретично і експериментально показано, що ослаблення сигналу при дощі і снігопаді менше, ніж при тумані (табл. 1).

*Таблиця 1*

**Ослаблення випромінювання в діапазоні 0,85 мкм залежно від погодних умов**

| Погодні умови | Затухання, дБ/км |
|---|---|
| Ясна погода | 0 … 3 |
| Слабкий дощ | 3 … 6 |
| Середній дощ | 6 … 22 |
| Сніг невеликої щільності | 6 … 26 |
| Легкий туман (серпанок) | 20 … 30 |
| Густий туман | 50 … 100 |

На рис. 3 приведені криві ослаблення лазерного сигналу в різних аерозолях.

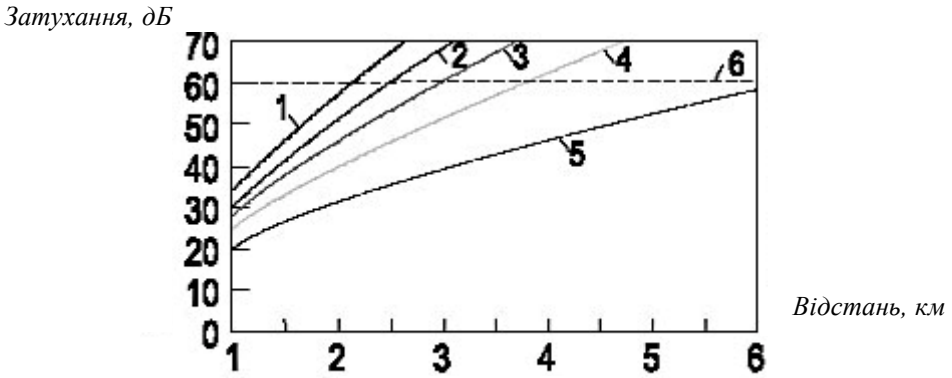



Рис. 3. Залежність ослаблення світла в аерозолях від відстані при різних метеофакторах:
1 – сніг середньої щільності; 2 – сильний дощ (40 мм/годину); 3 – сніг невеликої щільності;
4 – середній дощ (20 мм/годину); 5 – серпанок (МДВ = 2 км)

З табл. 1 і рис. 3 видно, що головними обмежувачами дальності АОСП є густий сніг і густий туман, для яких аерозольне ослаблення максимальне.

На розповсюдження лазерного променя сильний вплив надає також **турбулентність атмосфери**, тобто випадкові просторово-часові зміни показника заломлення, викликані переміщенням повітря, флуктуаціями його температури і щільності. Тому на світлові хвилі, що розповсюджуються в атмосфері, впливає не тільки поглинання, але і флуктуації потужності, що передається.

Турбулентність атмосфери приводить до спотворень хвильового фронту і, отже, до коливань і розширення лазерного пучка і перерозподілу енергії в його поперечному перетині. У площині приймальної антени це виявляється в хаотичному чергуванні темних і яскравих плям з частотою від доль герца до декількох кілогерц. При цьому іноді виникають завмирання сигналу (термін запозичений з радіозв’язку) і зв’язок стає нестійким. Завмирання найсильніше виявляється в ясну сонячну погоду, особливо в літні жаркі місяці, в години сходу і заходу сонця, при сильному вітрі. Наприклад, на рис. 4 показано дві крайні залежності вірогідності помилок BER для системи АОСП від дальності зв’язку при ясній погоді – одна в умовах сильної турбулентності атмосфери, інша в умовах слабкої. Звичайні значення BER лежать між цими кривими.

Найпростішим способом боротьби із завмираннями є збільшення розміру приймальної оптичної антени або використання декількох приймальних антен (до 8). При цьому відбувається усереднювання флуктуацій випромінювання, що приймається окремими елементами, і вирівнювання сигналу. Інший спосіб полягає в некогерентному складанні в одному каналі випромінювання декількох лазерів. При практичному використанні лазерів в системах атмосферного зв'язку необхідно враховувати сукупний вплив взаємодії випромінювання з атмосферою – що одночасно поглинає, розсіюючою і випадково неоднорідною середовищем. Цей вплив може змінюватися в надзвичайно широкому діапазоні. Тому для забезпечення працездатності АОСП на заданій дистанції з певним рівнем надійності (або доступності каналу) необхідно мати достатній динамічний запас енергетичного потенціалу.

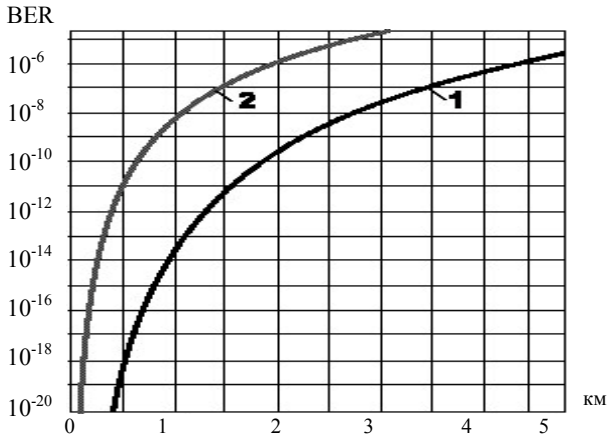



Рис. 4. Залежність вірогідності помилок BER від відстані при слабких завмираннях в атмосфері (крива 1) і сильних завмираннях (крива 2) для АОСП. Дощ, туман, сніг, серпанок відсутні

Чим більше запас потужності системи, тим менше погодні умови впливають на працездатність лінії. Розрахунок необхідного динамічного діапазону АОСП може бути проведений таким чином:

Найважливішим параметром оптичного тракту є енергетичний запас $P_е$ оптичного тракту:

$$P_е = P_{пер} - P_{пр}, \quad (1)$$

де: $P_{пер}$ – рівень потужності випромінювання передавача;

$P_{пр}$ – рівень потужності випромінювання на вході приймача.

Цей параметр для існуючих систем з інтерфейсом G.703/E1 може мати значення, представлені в таблиці 3.

*Таблиця 3*

**Енергетичний запас оптичного тракту деяких АОСП**

| Система | $P_{пер}$, дБм | $P_{пр}$, дБм | $P_е$, дБ |
|---|---|---|---|
| *SkyCell E*1-*T*6000 | 24,8 | – 60,0 | 84,8 |
| *SkyCell E*1-*T*4000 | 24,8 | – 45,0 | 69,8 |
| *SkyCell E*1-*T*338 | 20,0 | – 45,0 | 65,0 |
| *SkyCell E*1-*T*456 | 14,8 | – 45,0 | 59,8 |

Для нормальної роботи тракту необхідно, щоб виконувалася умова: $P_е > P_в$, т. т. енергетичний запас $P_е$ оптичного тракту повинен бути більше, ніж сумарні втрати в ньому. Сумарні втрати $P_в$ в тракті можна оцінити за формулою:

$$P_в = P_{опт} + P_{атм} + P_{впр}, \quad (2)$$

де: $P_{опт}$ – втрати оптичного узгодження;

$P_{атм}$ – втрати сигналу в атмосфері;

$P_{впр}$ – втрати в приймачі.

Зі всіх складових тільки величина $P_{впр}$ не залежить від відстані між оптичними блоками і для більшості систем знаходиться в діапазоні від 1 до 2 дБ. Дві інших величини, окрім прямої залежності від відстані, залежать від оптичної апертури, з якою розповсюджується промінь, розміру лінзи приймача (для $P_{опт}$), і від фізичних характеристик атмосфери (для $P_{атм}$).

У першому наближенні $P_{опт}$ можна визначити з простого співвідношення площі плями від променя на стороні приймача до площі лінзи цього приймача, тобто, це величина постійна для кожної конкретної дистанції:

$$P_{оп} 10\log\left(\frac{P_t}{P_r}\frac{D_r^2}{\theta^2 L^2}\right), \quad (3)$$

де $P_t$ – імпульсна потужність передавачів (Вт);

$P_r$ – чутливість приймача при співвідношенні сигнал/шум 10/1 (Вт);

$L$ – відстань від передавача до приймача (м);

$\theta$ – повний кут випромінювання передавача (рад);

$D_r$ – діаметр апертури оптичної системи приймача (м).

Природне бажання деяких виробників зменшити $P_{опт}$ шляхом зменшення повного кута випромінювання передавача. Проте, при дуже малих кутах випромінювання передавача системи стають чутливими до тремтіння атмосфери в жаркий період і до стабільності положення опор. Наприклад, при допустимому відході положення будівлі на кут в 1,5 хв (0,43 мрад) при зміні сезонів, і враховуючи, що допуск на точність позиціонування систем складає близько 30 секунд (0,15 мрад), на будівлі можна встановлювати системи з повним кутом випромінювання передавача тільки більше 1,16 мрад. Якщо для компенсації нестабільності опор можна застосувати системи автокорекції положення, то позбавитися від впливу тремтіння атмосфери можна тільки розширюючи промінь. Таким чином, оптимальна величина цього кута лежить в межах від 2 до 10 мрад. При дуже великому куті розбіжності різко збільшуються втрати $P_{опт}$.

Подивимося, яку величину $P_{атм}$ припускає типова оптична система на дистанції, наприклад, в 1,5 кілометра. Приймаючи кут випромінювання передавача в 2 мрад, як мінімально прийнятний і діаметр вхідної лінзи в 100 мм, використовуючи формулу (3) отримаємо $P_{опт}$ = 29,5 дБ. Тоді для $P_e$ = 60 дБ і $P_{впр}$ = 2 дБ:

$P_{атм} < P_e - P_{опт} - P_{впр} = 60 - 29{,}5 - 2 = 28{,}5$ дБ або: $P_{атм} < 28{,}5$ дБ/км.

Що ж означають величини $P_{атм}$ з практичної точки зору? Абсолютно очевидно, що чим більше допустима величина $P_{атм}$, тим більше суворі погодні умови може подолати оптична система. Проте, користувачам само це значення говорить тільки про можливості конкретної системи в порівнянні з іншими. В той же час, запас в 28,5 дБ на дистанції 1,5 км може бути малим для хорошої роботи тракту в Москві і цілком достатнім для Астрахані. Складність завдання полягає в тому, щоб з'ясувати відповідність цієї величини конкретним погодним умовам.

Вираз для $P_{атм}$ у загальному вигляді можна представити наступним чином:

$$P_{атм} = a \cdot L, \quad (4)$$

де: $L$ – відстань в км,

$a$ – питоме загасання сигналу в атмосфері дБ/км.

Проте, обчислення параметра $a$ і складає основну проблему, тому що в розрахунках необхідно враховувати хімічний склад атмосфери, наявність аерозолів, спектральні характеристики атмосфери. Необхідні спеціальні алгоритми для опису різного типу опадів (дощу, снігу, туману) і інших напівпрозорих середовищ (запорошені бурі, зміг). І все це з

урахуванням конкретного регіону, висот установки і ще величезного числа параметрів, що впливають на кінцеве значення *a*. Значення *a* лежать в дуже широкому діапазоні від 0,2 дБ/км (для відмінної погоди) до 350 дБ/км.

Вираз (4) надає лише уяву про фізичний сенс втрат сигналу в атмосфері, але не надає можливості для проведення розрахунків. Для виводу формули, яка придатна для реального розрахунку $P_{атм}$ доцільно розділити цю складову на дві частини. Перша описується законом Бугера-Ламберта-Бера, який визначає ослаблення монохроматичного світлового променя при його розповсюдженні у поглинаючому середовищі:

$$I(l) = I_0 e^{-k_\lambda l}, \tag{5}$$

де $I_0$ – інтенсивність оптичного сигналу на виході передавача;

$l$ –довжина оптичного тракту;

$k_\lambda$ – показник поглинання.

Показник поглинання $k_\lambda$ – коефіцієнт, що характеризує властивості атмосфери, як поглинаючої речовини, він залежний від довжини хвилі λ оптичного сигналу. Ця залежність називається спектром поглинання речовини, в даному випадку атмосфери. Для прогнозування значення $k_\lambda$ на практиці оцінюють параметр, що описує процес взаємодії оптичного випромінювання з атмосферою, а саме метеорологічну дальність видимості (МДВ) – *V*. Це відстань, на якій світло з довжиною хвилі 0,55 мкм ослабляється в 50 разів (на 17 дБ).

$$k_\lambda = \frac{4\pi}{\lambda V}. \tag{6}$$

Параметр *V* повинен враховувати відмінності погодних умов, як для різних географічних районів, так і для пори року і доби. Враховуючи (5) і (6), а також переходячи від абсолютних величин до відносних, можна отримати вираз для розрахунку величини загасання оптичного сигналу при його розповсюдженні в атмосфері (без урахування завмирань):

$$P_{атм} = 10\log e^{\frac{4\pi l}{\lambda V}}.$$

Відома також емпірична залежність [1], що оцінює параметри надійності зв'язку при використанні декількох лазерів, а також усереднюючий вплив апертури приймача зникнення когерентності на аерозолях атмосфери.

$$I = \frac{2{,}5\cdot 10^{-3} V}{2^N}\left(\frac{\theta L}{D_r}\right)^{\frac{3}{4}}, \tag{8}$$

де *N* – кількість лазерів, що передають.

Таким чином, використовуючи (7) і (8), отримуємо вираз для розрахунку величини загасання оптичного сигналу при його розповсюдженні в атмосфері з урахуванням завмирань:

$$P_{атм} = 10\log e^{\frac{4\pi l}{\lambda V}} + 10\log\left[\frac{2{,}5\cdot 10^{-3} V}{2^N}\left(\frac{\theta L}{D_r}\right)^{\frac{3}{4}}\right]. \tag{9}$$

Статистичним параметром погоди для конкретного географічного місця, що визначає надійність зв'язку, є частка часу за рік протягом якого МДВ менше заданої величини.

Обробка статистичних даних метеорологічних [4] спостережень дозволила встановити емпіричну залежність цього параметра від відстані. Співвідношення справедливе для МДВ менше 17 км:

$$W(L) = \alpha_i L^{b_i}, \tag{10}$$

де $W(L)$ – вірогідність настання погодних умов, при яких МДВ менше відстані L;

$L$ – відстань (км);

$a_i$, $b_i$ – константи для конкретної географічної крапки (наприклад, для Києва $a_i$ = 0,006, $b_i$ = 1,46).

З виразів (9) і (10) можна отримати співвідношення для визначення надійності зв'язку залежно від дальності і погодних умов для конкретної місцевості:

$$W = a_i V^{b_i} = a_i \left[ \frac{1{,}42 \dfrac{L}{1000}}{\log\left( \dfrac{P_t}{P_r} \dfrac{D^2{}_r}{\theta^2 L^2} \right) - \dfrac{2{,}5 \cdot 10^{-3} \cdot V}{2^N} \left( \dfrac{\theta L}{D_r} \right)^{\frac{3}{4}}} \right]^{b_i} . \qquad (11)$$

Отримані значення вірогідності зв'язку при різних відстанях для двох оптичних трактів приведені в табл. 4. З розрахунків виходить, що вірогідність безвідмовної роботи тракту довжиною до 3 км. при коефіцієнті помилки $10^{-6}$ – не нижче 0,993. Це вище за вимоги до радіорелейних ліній зв'язку, вірогідність безвідмовної роботи яких повинна бути не нижче 0,9925, що відповідає 0,75 % часу, протягом якого коефіцієнт помилки перевищує вказане значення.

*Таблиця 4*

**Вірогідність безвідмовної роботи траси АОСП при коефіцієнті помилки $10^{-6}$**

| Параметри системи | | | Довжина ділянки, км | Вірогідність зв'язку |
|---|---|---|---|---|
| № | Позначення | Значення | | |
| 1 | $P_{пер}$<br>$P_{чут}$<br>$D_{прм}$<br>$V_{пер}$ | 200 мВт<br>$5 \cdot 10^{-12}$ Вт<br>20 см<br>140 Мбіт/с | 0,5 | 0,99985 |
| | | | 1,0 | 0,99939 |
| | | | 2,0 | 0,99729 |
| | | | 3,0 | 0,99301 |
| 2 | $P_{пер}$<br>$P_{чут}$<br>$D_{прм}$<br>$V_{пер}$ | 100 мВт<br>$0{,}6 \cdot 10^{-12}$ Вт<br>10 см<br>8 Мбіт/с | 0,5 | 0,99988 |
| | | | 1,0 | 0,99955 |
| | | | 2,0 | 0,99818 |
| | | | 3,0 | 0,99564 |

Наприкінці декілька слів про такий дуже важливий аспект застосування АОСП, як безпека системи для обслуговуючого персоналу і взагалі для людини. У АОСП згідно з рекомендаціями МСЕ використовують лазерні випромінювачі виключно I та II класів.

До лазерів I класу відносять повністю безпечні лазери, вихідне коліміроване випромінювання яких не представляє небезпеки при опромінюванні очей і шкіри. Лазери II класу – це лазери, вихідне випромінювання яких представляє небезпеку (за певних умов) лише при опромінюванні очей людини колімірованим пучком. У табл. 5 приведені основні параметри лазерних випромінювачів, що характеризують їх безпеку для людини.

*Таблиця 5*

**Параметри лазерних випромінювачів, що характеризують їх безпеку**

| Вихідна потужність оптичного передавача | Клас | Довжина хвилі | Потужність у полі максимального опромінювання (при апертурі 7 мм) |
|---|---|---|---|
| 25 мВт | I | 810, 830 або 910 нм | 0,075 мВт |
| 35 мВт | I | 830 нм | 0,1 мВт |

| | | | |
|---|---|---|---|
| 100 мВт | II | 910 нм | 0,51 мВт |

**Висновки**

У даний час швидкості передачі комерційних АОСП складають від 2 до 622 Мбіт/с із застосуванням всіх поширених інтерфейсів локальних обчислювальних мереж і цифрових мереж передачі даних. Дослідні установки довели можливість передачі даних з ущільненням по довжині хвилі із швидкістю 10 Гбіт/с.

Перспективність використання АОСП для організації бездротового зв'язку визначається їх наступними перевагами:

– у жодній з країн не потрібна ліцензія на використання діапазону частот, який використовується в системах АОСП;

– практично стовідсоткова захищеність від перешкод радіодіапазону (перешкоди можуть впливати тільки безпосередньо на кінцеве обладнання);

– невеликий (порядка декілька годин) час розгортання;

– швидкість передачі даних може досягати декілька Гбіт/с;

– частота появи помилкових бітів (BER) від $10^{-9}$ до $10^{-8}$;

– менша, в порівнянні з іншими аналогічними по пропускній спроможності рішеннями, вартість.

Виходячи з вище наведених переваг, а також, враховуючи високий потенціал апаратних рішень, що застосовують в даних системах, з погляду їх модернізації і удосконалення, можна з упевненістю прогнозувати розширення спектра можливих застосувань АОСП. Очевидно, що не може залишитися в стороні від цього процесу і військовий зв'язок, особливо, зважаючи на такі, поза сумнівом, важливі для військового зв'язку переваги АОСП, як скритність і розвідзахищеність.

З іншого боку існує ще достатньо багато питань, що вимагають вирішення, перш ніж АОСП займуть гідне місце серед інших бездротових технологій. Отже, основні напрями розвитку АОСП можна сформулювати таким чином:

1. Вдосконалення елементної бази (розробка більш потужних джерел випромінювання, розробка фотоприймачів з більшою чутливістю, зниження вартості апаратних засобів АОСП і т.д.).

2. Оптимізація методів передачі і обробки сигналів в АОСП (вибір оптимальних методів модуляції і кодування оптичного сигналу, розрахунок оптимальної апертури оптичної системи передавача, розробка систем автоматичного регулювання потужності випромінювання і апертури передавача і т. д.).

3. Удосконалення методик проектування АОСП (розробка методик прогнозування дальності зв'язку АОСП, складання довідкових таблиць з даними для точного проектування АОСП в конкретних регіонах застосування і т. д.)

ЛІТЕРАТУРА

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

2. *Павлов Н.М.* Классификация аппаратуры и методика определения длины АОЛП. //Технологии и средства связи, специальный выпуск: Системы абонентского доступа, 2004. – С. 74 – 80.

3. *Милютин Е.* Современное состояние и перспективы атмосферных оптических линий связи. // Сети и телекоммуникации, № 6, 2003. – С. 14 – 20.

4. *Милинкис Б., Петров В.* Атмосферная лазерная связь. // Радиоэлектроника и телекоммуникации № 5 (18), 2001. – С. 44 – 48.

к.т.н. Ільяшов О.А. (в/ч А1906)

# ПОЛІГАУССОВСЬКИЙ РОЗПОДІЛ СТРУКТУРНИХ СИГНАЛІВ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Під час передавання інформації по радіоканалах зв'язку в телекомунікаційних мережах систем спеціального призначення корисні сигнали, як правило, спостерігаються на фоні адитивних зовнішніх і внутрішніх шумів природного походження, які за своїми властивостями близькі до гауссівських процесів. Однак з упровадженням багатоканальних асинхронних систем прихованого цифрового передавання інформації з кодовим розподілом сигналів ситуація змінюється. У смузі частот корисного сигналу може спостерігатися кінцева безліч сигналів-завад, які створюють аномальні викиди зі значною інтенсивністю і частотою появи. Тобто мають місце так звані структурні завади, що відрізняються від гауссівських сигналів. Аналогічна ситуація створюється у складній сигнальній обстановці, коли поряд з корисним приймається деяка кількість вузькосмугових сигналів. В цьому випадку використання гауссівських процесів при описі і аналізі сигналів на фоні структурних завад може привести до неадекватності їх фізичної та математичної моделі, що веде до появи похибок. У відомій літературі цій моделі сигналів приділяється визначена увага, однак кількість таких робіт значно менша ніж кількість публікацій, присвячених більш простій гауссівській моделі.

У зв'язку з цим виникає наукове завдання розробки деяких варіантів полігауссівської моделі структурних завад, що узагальнює гауссівську модель, і проведення аналізу їх статистичних властивостей, що визначає основну мету і зміст доповіді.

Для вивчення й аналізу загальних властивостей бігауссівськоого (полігауссівського) розподілу вважатиме, що є $m$-мірна випадкова величина, яка має полігауссівську щільність розподілу ймовірності:

$$f_{PN}(\mathbf{z}) = \sum_{k=1}^{n} q_k N_m(\boldsymbol{\mu}_k + \mathbf{s},\ \mathbf{G}_k), \tag{1}$$

де $G_k$ – невироджена матриця параметрів; $q_k \geq 0$, $\sum_{k=1}^{n} q_k = 1$ – вагові коефіцієнти; $\boldsymbol{s}$, $\boldsymbol{\mu}_k$ – вектори параметрів сигналу.

Далі обмежимося двома випадками: $\boldsymbol{\mu}_1 = -\boldsymbol{\mu}_2 = \boldsymbol{\mu}$, $\mathbf{G}_1 = \mathbf{G}_2 = \mathbf{G}$ і $\boldsymbol{\mu}_1 = -\boldsymbol{\mu}_2 = 0$, $\mathbf{G}_i = \sigma_i^2 \mathbf{G}_0$, при тому, що $i = 1{,}2$; $q_1 = q_2 = 0.5$.

У першому випадку розподіл (1) є бігауссівським і має вигляд:

$$f_{PN}(\mathbf{z}) = \frac{1}{2(2\pi)^{\frac{1}{2}m}|\mathbf{G}|^{\frac{1}{2}}}\left\{\exp\left[-\frac{1}{2}(\mathbf{z}-\boldsymbol{\mu}-\mathbf{s})^T\mathbf{G}^{-1}(\mathbf{z}-\boldsymbol{\mu}-\mathbf{s})\right]+\right.$$
$$\left.+\exp\left[-\frac{1}{2}(\mathbf{z}+\boldsymbol{\mu}-\mathbf{s})^T\mathbf{G}^{-1}(\mathbf{z}+\boldsymbol{\mu}-\mathbf{s})\right]\right\}\quad\frac{1}{(2\pi)^{\frac{1}{2}m}|\mathbf{G}|^{\frac{1}{2}}}\times$$
$$\times\exp\left[-\frac{1}{2}(\mathbf{z}-\mathbf{s})^T\mathbf{G}^{-1}(\mathbf{z}-\mathbf{s})-\frac{1}{2}\boldsymbol{\mu}^T\mathbf{G}^{-1}\boldsymbol{\mu}\right]ch(\mathbf{z}-\mathbf{s})^T\mathbf{G}^{-1}\boldsymbol{\mu}. \tag{2}$$

Математичне очікування й кореляційна матриця випадкового вектора з таким розподілом дорівнюють:

$$E(\boldsymbol{\zeta}) = \mathbf{s}, \qquad D(\zeta) = \mathbf{G} + \boldsymbol{\mu}\boldsymbol{\mu}^T . \tag{3}$$

При $\boldsymbol{\mu} \to 0$ розподіл (2) переходить у гауссівський, у іншому випадку він може помітно відрізнятися. На рис. 1 наведене сімейство одномірних бігауссівських щільностей розподілу для різних умов.

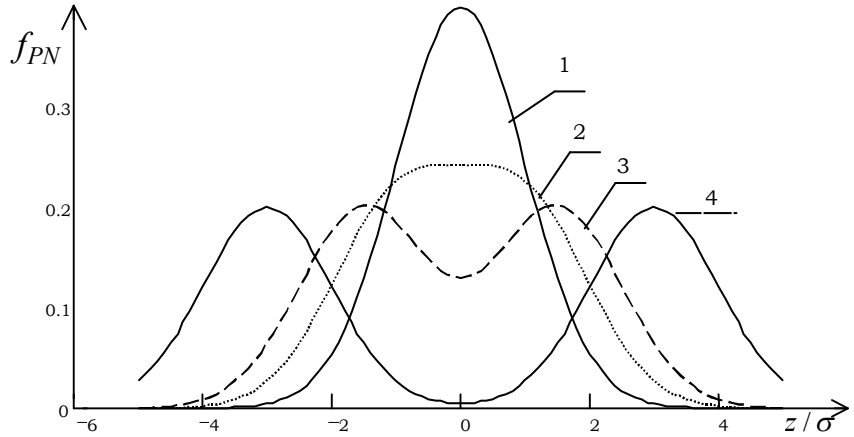



Рис.1. Полігауссівська щільність розподілу випадкової величини:1) $\boldsymbol{\mu}$ = 0 (гауссівська щільність розподілу); 2) $\boldsymbol{\mu}$ = 1 (унімодальна бігауссівська щільність розподілу); 3) $\boldsymbol{\mu}$ =1.5 (полігауссівська щільність розподілу з мало вираженими двома модами); 4) $\boldsymbol{\mu}$ = 3 (полігауссівська щільність розподілу із сильно вираженими двома модами).

У другому, із зазначених вище випадків, розподіл (1) записується у вигляді:

$$f_{PN}(\mathbf{z}) = \frac{1}{2(2\pi)^{\frac{1}{2}m}|\mathbf{G}_0|^{\frac{1}{2}}}\left\{\frac{1}{\sigma_1^m}\exp\left[-\frac{1}{2\sigma_1^2}(\mathbf{z}-\mathbf{s})^T\,\mathbf{G}_0^{-1}(\mathbf{z}-\mathbf{s})\right]+\right.$$

$$\left.+\frac{1}{\sigma_2^m}\exp\left[-\frac{1}{2\sigma_2^2}(\mathbf{z}-\mathbf{s})^T\,\mathbf{G}_0^{-1}(\mathbf{z}-\mathbf{s})\right]\right\}. \tag{4}$$

Математичне очікування й кореляційна матриця випадкового вектора з таким розподілом дорівнюють:

$$E(\boldsymbol{\zeta}) = \mathbf{s}, \qquad D(\boldsymbol{\zeta}) = \frac{1}{2}(\mathbf{G}_1 + \mathbf{G}_2) = \frac{\sigma_1^2 + \sigma_2^2}{2}\mathbf{G}_0 . \tag{5}$$

При виконанні умов $\sigma_1^2 >> \sigma_2^2$, „хвост” розподілу (4) виявляється товстим, що робить його відмінним від гауссівського.

Наявність таких „хвостів” дозволяє добре відбити факт наявності вимірів аномального характеру.

Отриманий вище вираз для розподілу (2) можна представити у вигляді

$$f_{PN}(z) = \int_{-\infty}^{\infty} f_{PN}(z/\gamma) f(\gamma) d\gamma , \tag{6}$$

де

$$f_{PN}(z/\gamma)=\frac{1}{(2\pi)^{\frac{1}{2}m}|\mathbf{G}|^{\frac{1}{2}}}\exp\left\{-\frac{1}{2}(z-\gamma\mu-s)^T\,\mathbf{G}^{-1}(z-\gamma\mu-s)\right\},$$

$$f(\gamma)=\frac{1}{2}\delta(\gamma-1)+\frac{1}{2}\delta(\gamma+1).$$

Тобто фактично від одного інтервалу спостережень до іншого середнє значення процесу *z(t) = s(t)* зазнає рівноімовірні перегони величиною $\pm\mu=const$. Усереднення гауссівського розподілу за цими випадковими стрибками і приводить до бігауссівського розподілу.

Наведемо інші передумови на користь переходу до бігауссівської щільності розподілу спостережень.

Нехай є сигнал

$$x(t)=X_0\cos(\omega_0 t+\varphi), \tag{7}$$

де $X_0$, $\omega_0$ – постійні величини; $\varphi$ – випадкова величина, що розподілена рівномірно на $[0,2\pi]$.

При фіксованому *t* випадкова величина має таку щільність розподілу:

$$f(x)=\begin{cases}\left[\pi\sqrt{X_0^2-x^2}\right]^{-1}, & -X_0<x<X_0.\\ 0, & |x|>X_0.\end{cases} \tag{8}$$

Аналіз умови (8) показує, що при $|x|\to X_0$ функція $f(x)$ необмежено зростає, тобто має два явно виражених максимуми. Якщо фаза має інший розподіл й амплітуда сигналу, будучи випадковою, розподілена в деякому інтервалі, то двогорбий характер щільності $f(x)$ не змінюється, сплески щільності розмиваються й стають обмеженими. Саме такими властивостями характеризується шумоподібний зв'язковий радіосигнал із частотною або фазовою модуляцією й постійною амплітудою, що у каналі зв'язку випадково змінюється в деяких межах.

Незважаючи на те, що наведені твердження мають якісній характер, вони переконливо свідчать на неадекватність гауссівської моделі шумоподібного зв'язкового сигналу й більшу перевагу бігауссівської моделі.

Як і для гауссівських процесів, теоретичний і практичний інтерес становлять одномірні характеристики обвідної й фази вузькосмугового бігауссівського сигналу:

$$\xi(t)=E(t)\cos[\omega_0 t-\varphi(t)]=E_c(t)\cos\omega_0 t+E_s(t)\sin\omega_0 t, \tag{9}$$

який при відомій величині $\omega_0$ повністю визначається квадратурними складовими $E_c(t)$ й $E_s(t)$. Якщо дані функції розглядаються у фіксований момент часу *t*, то разом вони утворять вектор $E^T=(E_c,E_s)$, щільність розподілу ймовірності якого задається формулою:

$$f_N(E) = \frac{1}{2\pi\sigma_\xi^2}\exp\left\{-\frac{1}{2\sigma_\xi^2}\left(E_c^2 + E_s^2\right)\right\}, \tag{10}$$

де $E_c = E(t)\cos\varphi(t)$, $E_s = E(t)\sin\varphi(t)$.

Для бігауссівського сигналу $\zeta(t) = P_c(t)\cos\omega_0 t + P_s(t)\sin\omega_0 t$, щільність розподілу сукупності квадратурної складової, розглянута в довільний момент часу, дорівнює:

$$f_{PN}(\mathbf{P}) = \frac{1}{4\pi\sigma_\zeta^2}\exp\left(-\frac{1}{\sigma_\zeta^2}\mu_0^2\right)\exp\left[-\frac{1}{2\sigma_\zeta^2}\left(P_c^2 + P_s^2\right)\right]ch\left[-\frac{1}{\sigma_\zeta^2}\mu_0(P_c + P_s)\right], \tag{11}$$

де $P_c = P(t)\cos\varphi(t)$, $P_s = P(t)\sin\varphi(t)$ .

Якщо, скориставшись (11), перейти від $P_c$, $P_s$ до $P$, $\varphi$, то одержимо:

$$f(P, \ ) = \frac{P}{4\pi\sigma_\zeta^2}\exp\left(-\frac{1}{\sigma_\zeta^2}P^2\right)\exp\left(-\frac{1}{2\sigma_\zeta^2}\mu^2\right)ch\left(-\frac{\sqrt{2}}{\sigma_\zeta^2}\mu_0 P\cos \ \right), \tag{12}$$

де $P \geq 0$, $-\pi \leq \ \leq \pi$.

Отриманий розподіл, на відміну від гауссівського, не описується у вигляді $f(P), f(\ )$, що вказує на певний статистичний зв'язок між випадковими величинами $P$ й $\varphi$.

Розподіл амплітуди $P$ можна надати в такому вигляді:

$$f(P) = \int_{-\pi}^{\pi} f(P, \ )d \ = \frac{1}{\sigma_\zeta^2}Pe^{-\frac{1}{2\sigma_\zeta^2}P^2}I_0\left(\frac{\sqrt{2}}{\sigma_\zeta^2}\mu_0 P\right), \quad P \geq 0. \tag{13}$$

Цей розподіл є законом Райса або узагальненим розподілом Релея. Параметр цього розподілу $\delta = \sqrt{2}\sigma_\zeta^{-1}\mu_0$ залежить від $\mu_0$ (центральний момент випадкової величини) і при $\mu_0 = 0$, як і слід було сподіватися, (13) переходить у розподіл Релея. Райсівський закон розподілу амплітуди бігауссівського процесу вказує на його більший ступінь "розмитості".

Вираз для розподілу фази може бути записаний у вигляді:

$$f(\varphi) = \int_0^\infty f(P,\varphi)dP = \frac{1}{4\pi\sigma_\zeta^2}e^{-\frac{1}{2\sigma_\zeta^2}\mu_0^2}\int_0^\infty P\exp\left(-\frac{1}{2\sigma_\zeta^2}P^2\right)ch\left(\frac{\sqrt{2}}{\sigma_\zeta^2}\mu_0 P\cos\varphi\right)dP \tag{14}$$

Відомо, що при спостереженні сигналів на фоні внутрішніх шумів найбільший інтерес становлять білі гауссівські процеси, що пояснюється наявністю широкосмугових шумоподібних сигналів спостереження.

На цей час шумоподібні сигнали в радіозв'язку займають смугу величиною до сотень мегагерців (у перспективі до одиниць гігагерців). За цих умов (при спостереженні сигналів на фоні надширокосмугових зв'язкових сигналів) безумовно становлять інтерес бігауссівські білі шуми.

Залежно від вибору параметрів багатомірної бігауссівської щільності розподілу спостережень функціонал білого бігауссівського шуму може бути різним.

Якщо обмежитися випадком бігауссівського розподілу вигляду (2) і перейти від багатомірного розподілу ймовірності до функціонала ймовірності, то у разі білого шуму можна одержати функціонал, що відрізняється від гауссівського:

$$f_{PN}[x(t)] = \frac{1}{2}h\left\{\exp\left[-\frac{1}{2}N_0\int_0^T\left(x(t)-\mu(t)-\sqrt{\varepsilon(\alpha)}S_0(t,\alpha)\right)^2 dt\right]+\right.$$

$$\left.+\exp\left[-\frac{1}{2}N_0\int_0^T\left(x(t)+\mu(t)-\sqrt{\varepsilon(\alpha)}S_0(t,\alpha)\right)^2 dt\right]\right\}; \qquad (15)$$

$$f_N[x(t)] = h\exp\left\{-\frac{1}{2}N_0\int_0^T\left[x(t)-\sqrt{\varepsilon(\alpha)}S_0(t,\alpha)\right]^2 dt\right\}. \qquad (16)$$

Оцінювання амплітуди $\varepsilon'$ можна провести за виразом [3]:

$$\varepsilon' = \int_0^T x(t)S_0(t,\alpha)dt - th\left\{\frac{2}{N_0}\int_0^T\left[x(t)-\varepsilon' S_0(t,\alpha)\right]\mu(t)dt\right\}\int_0^T \mu(t)S_0(t,\alpha)dt. \qquad (17)$$

За допомогою (17) досить просто будується ітераційна процедура одержання оцінки величини $\varepsilon'$.

Отже, наведені результати свідчать, що:

у реальних умовах під час передавання інформації спостережувальні процеси не завжди задовільно апроксимуються гауссівською моделлю. На практиці в таких ситуаціях, як правило, звертаються до методів кореляційної теорії, що приводить до відносно простих процедур обробки сигналів. Однак ці спрощення досягаються за рахунок певної втрати якості, що не завжди припустимо;

полігауссівські розподіли можуть бути полімодальними, а у разі шумоподібних сигналів засобів зв'язку – бімодальними;

полігауссівська модель сигналів є більше загальною в порівнянні з гауссівською (за певних умов полігауссівський розподіл спостережень переходить у гауссівський).

Тому, з методичних міркувань застосування полігауссівської моделі сигналів треба розглядати, порівнюючи його з добре відомим використанням гауссівської моделі;

алгоритми обробки сигналів, отримані в припущенні, що шум є гауссовим, виявляються в багатьох випадках неробастними. Це найчастіше є наслідком наявності аномальних вимірювань. За допомогою полігауссівської моделі можна задати розподіли з „товстими хвостами", фіксуючи тим самим факт наявності аномальних похибок вимірювань.

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

# МЕТОДИ ОПЕРАТИВНОГО УПРАВЛІННЯ ЗАСОБАМИ ЗАВАДОЗАХИСТУ ВІЙСЬКОВИХ СИСТЕМ РАДІОЗВ’ЯЗКУ

У сучасних умовах при забезпеченні безперервного і стійкого управління військами особливу актуальність має радіозв’язок, який у ряді випадків є фактично єдино можливим родом зв’язку.

Однією з тенденцій розвитку тактики загальновійськового бою є широке застосування засобів радіоелектронної боротьби [1–3]. В даний час створено значну кількість засобів радіоелектронного подавлення (РЕП), які можуть порушувати управління військами шляхом подавлення засобів зв’язку в різних діапазонах робочих частот (табл. 1).

*Таблиця 1*

**Характеристики сучасних станцій РЕП**

| № з/п | Найменування | Країна-виробник | Основні тактико-технічні характеристики |
|---|---|---|---|
| 1. | Р-330Т | Росія | Діапазон робочих частот: 30 – 100 МГц; потужність випромінювання передавача: 1 кВт; швидкість панорамного огляду частотного діапазону – до 7000 МГц/с; виявлення сигналів із ППРЧ – до 1000 стр/с; подавлення сигналів з ППРЧ – до 300 стр/с; на автомобільній базі; екіпаж – 4 чол |
| 2. | Комплекс „Вулфпак” | США | Діапазон робочих частот: 20 – 15 000 МГц; при віддаленні до 1 км забезпечує ефективне подавлення постановкою завади з рівнем потужності менше 10 Вт; забезпечує класифікацію й ідентифікацію (при швидкості ППРЧ 1400 і більше стрибків за секунду) сигналів всіх відомих РЕЗ; визначення менш ніж за 2 с місцезнаходження радіостанцій супротивника з круговою ймовірною помилкою не більше 10 м |
| 3. | „Проулер”, літак РЕБ | США | В радіусі близько 20 км створює завади з рівнем потужності більше 400 Вт, при цьому заважаючий сигнал власним приймальним пристроям не перевищує 1 Вт |
| 4. | Комплекс „Мошкара” | Росія | Діапазон – УКХ (30 – 100 МГц); на базі безпілотних літальних апаратів (БЛА); дальність дії – до 50 (100) км при прямій видимості; тривалість польоту – 2–3 год |
| 5. | Комплекс „Мошкарец” | Росія | Діапазон – УКХ (30 – 100 МГц); на базі БЛА; дальність дії – до 30 (60) км; забезпечує енергетичну перевагу передавача станції завад за рахунок підйому БЛА на висоту близько 1 км; локалізацію впливу в радіусі 5–10 км; одночасне подавлення незначною потужністю піддіапазону (30 – 110 МГц або 110 – 220 МГц); групове застосування БЛА дозволяє перекрити весь діапазон частот радіозв’язку. Для перекриття діапазону 30 – 1200 МГц необхідно 8 БЛА |

Засоби радіоелектронного подавлення здатні з високою ефективністю та у короткий час подавити систему радіозв’язку (СРЗ), побудовану на традиційних принципах. Враховуючи це, стає досить складним завдання забезпечення стійкого радіозв’язку в умовах впливу навмисних завад. Успішне її вирішення неможливо без застосування спеціальних технічних і організаційних заходів по забезпеченню завадозахищеності систем радіозв’язку.

Крім навмисних завад одним з факторів, що впливають на якість радіозв’язку, є завмирання сигналів, які виникають внаслідок багатопроменевого розповсюдження радіохвиль в каналі. При цьому завадова обстановка в каналі постійно змінюється.

Тому великого значення набуває *проблема* синтезу методів і методик оперативного управління засобами завадозахисту військової системи радіозв'язку в умовах активної радіоелектронної протидії та апріорної невизначеності щодо умов ведення зв'язку, сигнальної та завадової обстановки. Через економічні та частотно-ресурсні обмеження традиційні заходи завадозахисту, реалізовані в СРЗ, виявляються ефективними в обмеженому діапазоні можливих завадових ситуацій. Тому актуальним шляхом підвищення завадозахищеності військових систем радіозв'язку (ВСРЗ) є застосування всього комплексу заходів завадозахисту на принципах адаптивного управління (АУ).

Для розв'язання поставленої проблеми необхідно вирішити ряд часткових задач:

розробити математичні моделі СРЗ;

розробити методи контролю стану каналу зв'язку з селективними завмираннями і навмисними завадами;

розробити методи і методики оперативного управління засобами завадозахисту СРЗ.

Сучасні військові системи радіозв'язку являють собою складні системи з розподіленою багатозв'язною структурою. З урахуванням специфічних особливостей побудови й умов функціонування, важливим моментом при розробці структурної моделі СРЗ є її подання у вигляді глобальної керованої мережі радіозв'язку, що складається з множини локальних підмереж радіозв'язку і має в загальному випадку ймовірнісну ієрархічну структуру. Такий підхід відображає наявність реальних зв'язків між елементами СРЗ вищих і підлеглих пунктів управління і дозволяє зручніше формалізувати структуру СРЗ.

В якості математичного образу глобальної СРЗ введемо неорієнтований зважений стохастичний граф $G = G(\mathbf{V}, \mathbf{E})$, множину вершин якого $\mathbf{V} = \{V_i\}$ складають групи (опорні вузли зв'язку), а множину ребер (гілок) $\mathbf{E} = \{E_{ij}\}$ – напрями зв'язку між опорними вузлами зв'язку (ОВЗ), утворені за допомогою однієї або декількох радіоліній, що здійснюють передачу оперативних повідомлень між ними [4]. При цьому ОВЗ можуть виконувати функції відправників, одержувачів або ретрансляторів повідомлень.

Для функціонального опису СРЗ застосовується підхід, заснований на ієрархічній декомпозиції функціональної структури мереж, поведінка яких описується стохастичними диференціальними (або різницевими) рівняннями стану високої розмірності, на ряд взаємопов'язаних, але простіших функціональних структур, що характеризуються векторами стану набагато меншої розмірності.

Матричне різницеве кероване стохастичне рівняння стану СРЗ можна записати у вигляді

$$\mathbf{H}(k+1) = \mathbf{C}\mathbf{H}(k) + \mathbf{B}\mathbf{W}(k) + \Sigma(k), \tag{1}$$

де $\mathbf{H}(k)$ – стан системи на $k$-му кроці; $\mathbf{C}$ – матриця взаємодій опорних вузлів зв'язку; $\mathbf{W}(k) = \left\| \mathbf{W}_1(k), \ldots, \mathbf{W}_q(k), \ldots, \mathbf{W}_Q(k) \right\|^{\mathrm{T}}$ – складений вектор управлінь $(q = \overline{1, Q})$; $\mathbf{B}$ – матриця управлінь; $\Sigma(k)$ – складений вектор зовнішніх дій (завмирань та навмисних завад).

З урахуванням $Q$ підмереж, вираз (1) можна переписати

$$\begin{vmatrix} \mathbf{H}_1(k+1) \\ \vdots \\ \mathbf{H}_Q(k+1) \end{vmatrix} = \begin{vmatrix} \mathbf{I} & \cdots & \mathbf{C}_{1Q} \\ \vdots & & \vdots \\ \mathbf{C}_{Q1} & \cdots & \mathbf{I} \end{vmatrix} \cdot \begin{vmatrix} \mathbf{H}_1(k) \\ \vdots \\ \mathbf{H}_Q(k) \end{vmatrix} + \begin{vmatrix} \mathbf{B}_1 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & & \mathbf{B}_Q \end{vmatrix} \cdot \begin{vmatrix} \mathbf{W}_1(k) \\ \vdots \\ \mathbf{W}_Q(k) \end{vmatrix} + \begin{vmatrix} \sum_1(k) \\ \vdots \\ \sum_Q(k) \end{vmatrix}. \tag{2}$$

Адаптивна модель ВСРЗ дозволяє враховувати адаптивні властивості систем і засобів радіозв'язку, без яких неможливо успішне функціонування СРЗ в умовах випадкового характеру змін завадової обстановки. Мета адаптації залежно від сформованої обстановки в мережі полягає в досягненні екстремальних показників ефективності зв'язку

$$Q(U) \to \min_{U \in S}(\max) \to U^*,$$

де $S:\begin{cases} H(U) \geq 0; \\ G(U) = 0. \end{cases}$ – множина допустимих управлінь при заданих обмеженнях $H$ і $G$;

$U = (u_1, u_2, \ldots, u_n)$ – параметри адаптації.

В умовах протидії СРЗ і системи РЕП модель адаптивної системи радіозв'язку доцільно доповнити ігровим підходом, який враховує різноманіття і ефективність стратегій в умовах невизначеності (рис. 1). Для описання конфлікту застосовується модель нескінченно-крокової матричної гри із запізнюванням та помилками в інформованості сторін о діях супротивника. На рис. 1 $\mathbf{a} = (a_1, a_2, \ldots a_n)$ – вектор оптимальних стратегій СРЗ; $\mathbf{b} = (b_1, b_2, \ldots b_n)$ – вектор оптимальних стратегій системи РЕП; $\Delta t_{\text{СРЗ}}$ – час реакції системи радіозв'язку; $\Delta t_{\text{РЕП}}$ – час реакції системи РЕП.

Для реалізації адаптивного принципу управління потрібна максимальна кількість інформації про стан СРЗ. Тобто СРЗ повинна забезпечувати контроль характеристик каналу зв'язку та якості власного функціонування, передачу вимірювальної й керуючої інформації та динамічно змінювати свою структуру і параметри залежно від завадової обстановки.

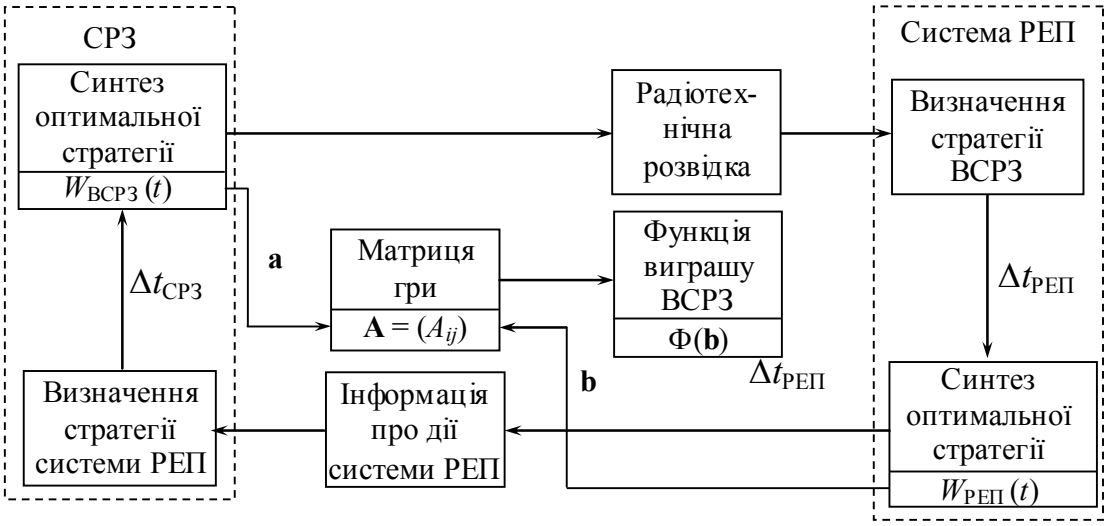



Рис. 1

На основі результатів контролю стану каналів зв'язку в залежності від завадової обстановки може здійснюватися оперативне управління засобами завадозахисту СРЗ. Залежно від наявності інформації про дії системи РЕП розрізняють наступні методи оперативного управління засобами завадозахисту: інваріантний, коли СРЗ не має інформації про дії системи РЕП; мінімаксний (ігровий) – коли СРЗ має можливість розпізнавати тільки факт впливу на неї системи РЕП; адаптивний – коли СРЗ має можливість розпізнавати поточну стратегію системи РЕП (вид і параметри завади).

При відсутності навмисних завад застосовуються адаптивні методи формування та обробки сигналів в залежності від рівня селективних завмирань сигналу в каналі. Параметрами радіозасобів, що оптимізуються, можуть бути кількість підканалів широкосмугового сигналу, потужність сигналу, вид модуляції, вид коригувального коду, тип та діаграма спрямованості антени, швидкість передачі інформації тощо.

В тому випадку коли СРЗ має можливість розпізнавати тільки факт впливу на неї системи РЕП ефективним виявляється мінімаксне управління засобами завадозахисту. Метод мінімаксного управління засобами завадозахисту можна представити як програмну зміну ВСРЗ своєї стратегії після встановлення факту зміни стратегії системою РЕП. При цьому у ВСРЗ виявляється й розпізнається факт впливу системи РЕП і здійснюється перехід до іншої стратегії завадозахисту, керуючись деяким правилом, що максимізує середній виграш за встановлений час. Наприклад, стратегіями СРЗ можуть бути зміна сигнально-кодової

конструкції, алгоритму перестроювання робочої частоти в режимі ППРЧ, вид коригувального коду тощо.

Метод адаптивного управління засобами завадозахисту являє собою ситуаційний вибір ВСРЗ найкращої стратегії на підставі розпізнавання стратегії, реалізованої системою РЕП.

У функціональній структурі військової системи радіозв'язку можна виділити два функціональних рівні, які перебувають між собою в ієрархічному підпорядкуванні.

На першому (нижньому) рівні вирішуються завдання контролю й управління окремими радіолініями або радіозасобами:

вибір радіозасобів, визначення оптимальних режимів їх роботи, утворення високочастотних трактів;

автоматичне входження у зв'язок, його ведення і відновлення;

оперативний контроль процесів передачі інформації радіоканалами.

Зазначені завдання вирішуються децентралізовано для кожного напрямку або лінії радіозв'язку (фізичний рівень).

Як параметр управління адаптивних радіоліній може використовуватися робоча частота, потужність радіосигналу, тип та діаграма спрямованості антени, швидкість передачі інформації, вид модуляції, вид завадостійкого коду, довжина кадру (пакету), швидкість та алгоритм перестроювання частоти в режимі ППРЧ тощо.

На другому (верхньому) рівні вирішуються завдання контролю й управління мережею радіозв'язку:

оперативний контроль і прогнозування умов ведення радіозв'язку (оцінка радіоелектронної обстановки);

оперативний аналіз інформаційної обстановки на мережі (оцінка станів інформаційних потоків);

маршрутизація;

розподіл частотних і енергетичних ресурсів.

Вирішення завдань другого рівня вимагає певної централізації (у розумному поєднанні з децентралізованими методами) контролю і управління радіозв'язком (канальний та мережевий рівень).

Для більш ефективного використання ресурсів ВСРЗ вирішення завдань першого і другого рівнів повинно проводитись комплексно.

Таким чином, актуальним напрямком підвищення завадозахищеності сучасних систем радіозв'язку в умовах активної радіоелектронного протидії є застосування всього комплексу засобів завадозахисту на принципах адаптивного управління. При цьому, адаптивне управління структурою і параметрами засобів завадозахисту системи радіозв'язку повинно мати комплексний характер, тобто враховувати можливості фізичного, канального, мережевого рівнів.

ЛІТЕРАТУРА

1. *Воробьев И. Н.* Вопросы теории и практики маневренной обороны // Военная мысль. – 1990. – № 9. – С. 34 – 40.

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

4. *Ливенцев С., Кувшинов А., Миночкин Д.* Синтез оптимальной иерархической структуры информационно-телекоммуникационной структуры // Збірник „Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. НТУУ „КПІ". – 2006. – Вип. 1 (12). – С. 162 – 169.

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

# КООРДИНАЦІЯ ТА ІНТЕЛЕКТУАЛІЗАЦІЯ РІВНІВ OSI – НОВА ПАРАДІГМА УПРАВЛІННЯ МОБИЛЬНИМИ РАДІОМЕРЕЖАМИ

Розглядається динамічна архітектура побудови мобільних радіомереж (МР) або MANET (Mobile Ad-Hoc Networks), що припускає відсутність базових станцій і фіксованих маршрутів передачі інформації. Вузли мобільні, повинні швидко адаптуватися до частих змін топології мережі та ефективно використати обмежені мережні ресурси [1].

Перспективна архітектура мобільна компонента (МК) тактичної ланки управління буде неоднорідною, ієрархічною та складатимуся з трьох основних рівнів: 1-й – мобільні радіомережі низової ланки управління (бойові радіомережі); 2-й – мережі мобільних базових станцій (МБС), що утворять опорну мережу; 3-й – повітряна мережа, яка може бути реалізована на безпілотних літальних апаратах [2]. Додатковий нульовий рівень можуть утворювати сенсорні мережі (мережі телеметрії). Створення кожного рівня мобільної компоненти передбачає поліпшення показників якості функціонування всієї системи зв’язку. Кожен рівень буде являти собою мережу типу MANET.

До основних особливостей цих мереж можна віднести: динамічну топологію, колективне використання радіоресурсу, нестабільність радіоканалів та наявність перешкод, обмеженість та неоднорідність ресурсів вузлів (пам’ять, продуктивність процесора, енергія батареї, мобільність), обмежену безпеку через широкомовну природу радіоканалу та ін. В таких умовах забезпечити інформаційний обмін із заданою якістю неможливо без ефективної системи управління мережею (СУМ), до якої пред’являються наступні основні вимоги: децентралізованість функціонування; виконання умов обслуговування різних типів трафіка за напрямками передачі (виконання користувальницької оптимізації); мінімізація службового трафіка, максимізація пропускної здатності зони мережі та інше (виконання мережевої або зонової оптимізації [3]).

Існуючі підходи до проектування телекомунікаційних мереж зв’язку припускають незалежність функцій управління за рівнями (рис. 1) еталонної моделі взаємодії відкритих систем (OSI) [4]. Тут стік протоколів кожного рівня працює незалежно (рис. 1а). Однак даний підхід не враховує особливості MANET і не дозволяє забезпечити оптимізацію показників ефективності на кожному рівні OSI (або в цілому) при різних умовах функціонування мережі та вимогах конкретного типу трафіка (наприклад, відео або мови) [5].

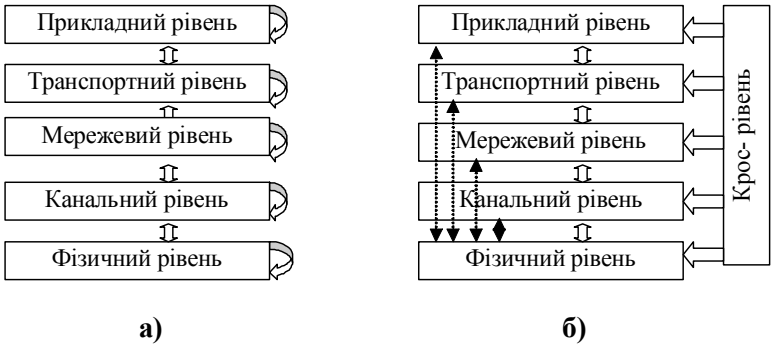



Рис. 1. Архітектура OSI (а) та координаційна (cross-level) архітектура (б)

При цьому необхідно відмитими, що досягання глобальної оптимізації при оперативному управлінні для всієї мобільної радіомережі неможливо внаслідок неможливості побудови відповідної моделі її функціонування, а також (що саме важливе)

неможливістю зібрати в реальному часі інформацію про стан мережі. Тому доцільно говорити про користувальницьку оптимізацію (задоволення користувальницьких вимог) між парами відправник-адресат при мінімізації витрат мережевих ресурсів (наприклад, мінімізація службового трафіка) [3].

Крім цього, проведені дослідження показують відсутність єдиного методу управління мережею, що забезпечує оптимізацію мережних показників на кожному з рівнів OSI [6 – 8]. Так, наприклад, на мережевому рівні моделі OSI: зондові методи маршрутизації ефективні при низькому трафіку та високої мобільності вузлів; табличні методи – при низької мобільності й значному навантаженню [6]. Методи управління доступом канального рівня OSI також мають свої границі ефективного застосування [7]. Крім цього, для зменшення службового трафіка виникає необхідність використання одним рівнем OSI службової інформації отриманої на іншому з рівнів. Наприклад, якщо існуючі маршрути (мережевий рівень OSI) не відповідають вимогам по 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 при відповідної можливості прикладного рівня OSI.

Метою доповіді є розгляд нової парадигми побудови системи керування МР, яка передбачає координацію та інтеграцію рівнів еталонної моделі OSI по цілях і функціях управління та інтелектуалізацію процесів прийняття рішення.

Основні труднощі інтеграції – це визначення необхідних параметрів, які будуть використатися між рівнями OSI (рис. 1б) та визначення методів прийняття рішення за рівнями OSI та функціями управління, які дозволять отримати користувальницьку та (або) мережеву, зонову оптимізацію [3].

На рис. 2 наведений приклад взаємодії рівнів OSI при передачі відеотрафіка з метою максимізації пропускної здатності при змінних канальних умовах [5]. На фізичному рівні, використовуючи адаптивну методи передачі, максимізується продуктивність каналу при різних умовах його функціонування. Це дозволяє збільшити продуктивність зони мережі (кожний вузол мережі може індивідуально встановлювати різну продуктивність каналів). Ґрунтуючись на інформації про стан каналів, протокол канального рівня призначає слоти, коди або частоти для кожного напрямку зв'язку. Канальний рівень, працюючи разом з мережевим рівнем, установлює множину маршрутів та розподіляє потоки для запобігання перевантаження. Знаходження загального оптимального рішення для призначення пропускної здатності потоків поширюється на інші рівні OSI. Транспортний рівень оптимізує планування темпу передачі. На закінчення, прикладний рівень визначає найбільше методи ефективного стиску даних.

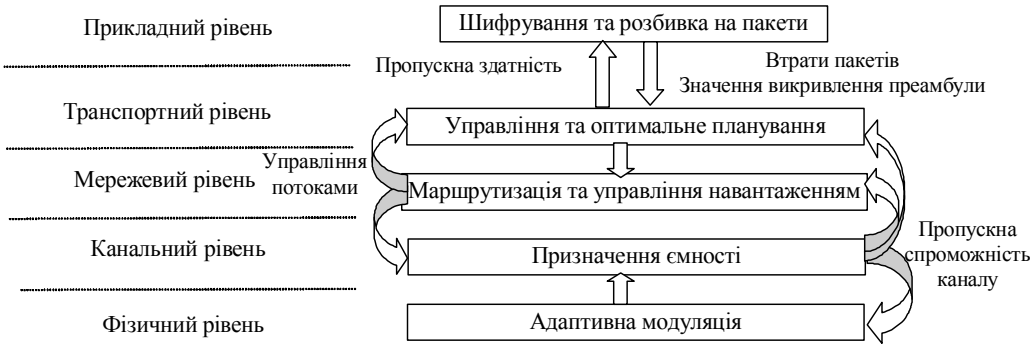



Рис. 2. Фрагмент координації рівнів OSI для зменшення затримки при передачі відеотрафіка

Розглянемо більш детально можливі варіанти параметрів координації.

Наприклад, *фізичний рівень* може характеризуватися наступним набором параметрів, що визначають якість каналу: співвідношення сигнал/шум (SINR, signal-to-interference-plus-

noise ratio), імовірність бітової помилки (BER, bit error rate), підтримувана швидкість передачі. Аналогічно мережевий і канальний рівень також характеризуються швидкістю передачі та прийнятною ємністю каналу.

*Канальний рівень*. На пропускну здатність радіоканалу впливає затухання, багатопроменеве поширення та взаємні перешкоди. Застосування адаптивної модуляції дозволяє поліпшити швидкість передачі даних за допомогою адаптації значень різних параметрів при змінних умовах радіоканалу. Дані параметри можуть включати модуляцію, кодування, потужність передачі, задану величину BER, символьну швидкість та комбінацію цих параметрів.

В [5] розглядається два можливих способи адаптації для підвищення пропускної здатності каналу:

1. Адаптація довжини пакета, обумовлена поточним значенням SINR і іншими параметрів каналу для оптимізації його пропускної здатності.
2. Оптимізація символьної швидкості та розмірності сузір'я при фіксованій довжині пакета.

Очевидно, що при збільшенні розміру пакета збільшується ймовірність його одержання з помилкою, тому пропускна здатність обмежується числом повторних передач. З іншого боку, малий розмір пакета приводить до збільшення частки службової інформації в загальному обсязі переданої інформації.

Оптимальна довжина пакета визначається виразом [5]

$$L = \frac{H}{2} + \frac{1}{2}\sqrt{H^2 - \frac{4bH}{\ln(1-P_e)}},$$

де $H$ – розмір заголовка пакета, $b$ – кількість біт на символ, $P_e$ – імовірність помилки символу, що залежить від типу модуляції та SINR. Загальні оптимальні довжина пакета та канальних параметрів визначаються виходячи з наступних правил.

Зона з високим рівнем SINR – коли затухання високе, максимальна символьна величина визначається відповідним розміром сузір'я, відповідно, оптимальна довжина пакета збільшується з поліпшенням якості каналу.

Зона з низьким рівнем SINR – величина помилки може додатково зменшуватися з передачами. Відповідно одне рішення – використати більший фактор кодування.

Після вибору оптимальних параметрів пропускна здатність межу двома вузлами визначається виразом

$$S = W \log_2(1 + SINR / \Gamma),$$

де $W$ – смуга каналу, Г – параметр, обумовлений при проектуванні каналу.

*Мережевий рівень* повинен побудувати маршрути передачі заданої якості та здійснювати їх підтримку. Однак більшість запропонованих методів маршрутизації досягають своєї ефективності при певних умовах функціонування мережі. Тому авторами запропонований новий інтелектуальний метод маршрутизації [8]. Суть методу полягає у ранжируванні цілей управління мережею в залежності від вимог до передачі певного типу трафіка та стану напрямку $a - b$ з метою забезпечення заданої якості обслуговування певних типів трафіка при різних умовах функціонування МР. Метод функціонує на етапах побудови та підтримання маршрутів. На відміну від існуючих методів зондової маршрутизації, розроблений метод маршрутизації передбачає (рис. 3): введення ієрархії процесу прийняття рішення з пошуку маршруту заданої якості, яка включає наступні етапи: вибір цільової функції управління маршрутами, типу маршрутизації, кількості маршрутів та способу зондування в мережі; інтелектуалізацію процесу прийняття рішень з вибору маршрутів передачі даних на основі використання апарата нечіткої логіки. Метод дозволяє скоротити об'єм службового трафіка на

20–30 % (завдяки врахуванню стану інформаційного напрямку та вимог до передачі різних типів трафіка).

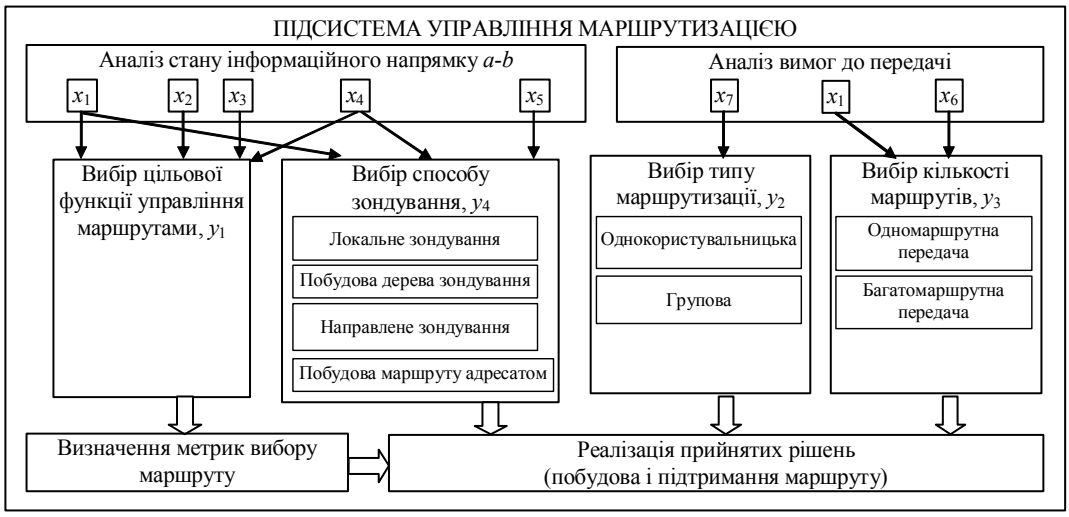



Рис. 3. Ієрархія прийняття рішень з побудови маршруту заданої якості (параметри стану напрямку *a* – *b*: $x_1$ – тип трафіка; $x_2$ – об'єм інформації; $x_3$ – залишкова ємність батарей; $x_4$ – розмір черг в проміжних вузлах; $x_5$ – мобільність мережі; $x_6$ – забезпечення безпеки інформації; $x_7$ – кількість адресатів)

*Управління топологією.* Пропонується введення додаткового підрівня мережевого рівня моделі OSI для управління топологією мережі за рахунок зміни потужності передачі та (або) діаграми спрямованості антени. Збільшення потужності передачі збільшує кількість „сусідніх" вузлів, однак розширює зону взаємних завад (проблема „прихованого термінала"), тем самим зменшує пропускну здатність радіоканалів зони та потребує більших витрат енергії батареї .

Задача пошуку топології відноситься до класу NP -повних, тому для отримання рішення в реальному часі запропонована база знань продукційного типу, яка дозволяє приймати близькі до оптимальних рішення [9].

Класифікація правил наведена в [9]. Кожна група правил призначена для здійснення користувальницької або системної оптимізації. Для усунення конфліктів серед правил запропоновані мета правила. Рішення по управлінню топологією можуть прийматися як кожним вузлом так і центром управління зоною мережі.

*Транспортний рівень.* Більшість відомих методів управління навантаженням на транспортному рівні реалізує „вікно перевантаження". Авторами запропоновано застосувати апарат нечіткої логіки за встановлення розміру „вікно перевантаження" [10]. Суть методу полягає в управлінні швидкістю передачі у вузлах шляхом вибору необхідного розміру вікна перевантаження в залежності від стану інформаційного напрямку між вузлами *a* та *b*, з метою реалізації користувальницької оптимізації. Новизна полягає в застосуванні множини різнорідних параметрів оцінки стану інформаційного напрямку $x_1$ … $x_6$ для прийняття рішення про розмір вікна перевантаження з використанням бази знань, побудованої на експертних даних. Метод дозволяє: скоротити об'єм службового трафіка на 20–25 %, шляхом встановлення нульового розміру вікна; попередити перевантаження напрямку передачі шляхом завчасного скорочення розміру вікна перевантаження; збільшити пропускну спроможність інформаційного напрямку на 15–25 % в залежності від швидкості переміщення вузлів, вхідного навантаження та кількості ретрансляцій.

*Прикладний рівень (міжрівнева інтеграція).* Для цього пропонується нова парадигма побудови системи управління – ввести базу методів управління та інтелектуальну надбудову над нею (систему прийняття рішень по управлінню), що координує функціонування множини методів управління по рівнях OSI з метою оптимізації показників функціонування мережі (рис. 4). База методів управління {МУ}={$МУ_ф$, $МУ_к$, $МУ_м$, $МУ_т$, $МУ_п$} містить

множину методів управління для кожного рівня OSI. Система прийняття рішень складається з бази знань (містить знання про об'єкт управління, знання про цілях функціонування та управління, знання про способи досягнення цілей), бази дані управління, блоку логічного висновку (БЛВ) і моделей ресурсів мережі [11].

Відмінність запропонованого підходу від існуючих – координація та інтеграція між рівнями OSI не тільки за різними параметрами, а за цілями управління, які визначають певний метод управління на кожному рівні моделі OSI.

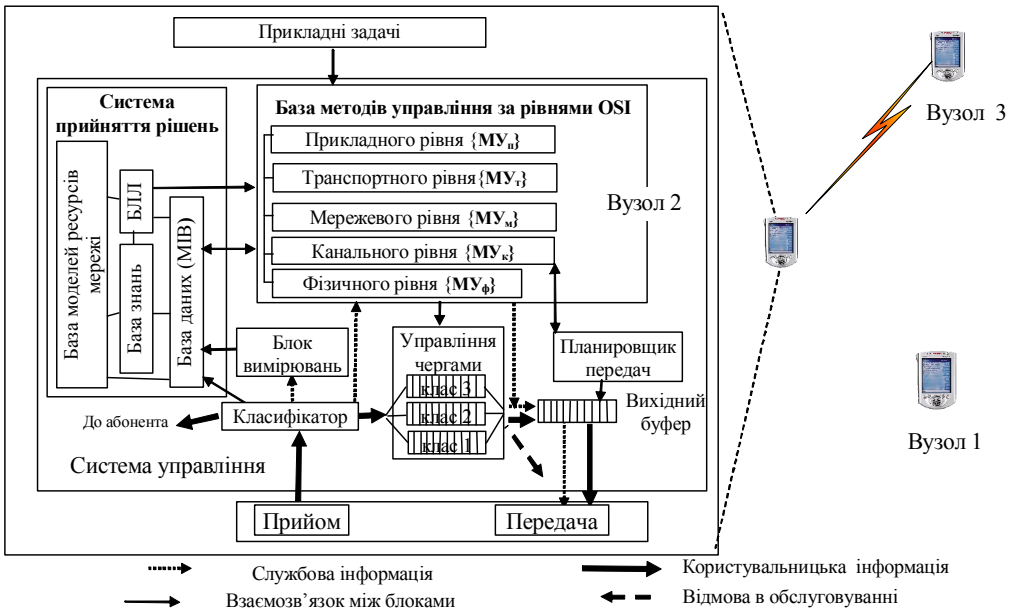



Рис. 4. Архітектура інтелектуальної системи управління вузла мережі

В умовах децентралізованого керування кожний вузол буде реалізовувати дві взаємозалежні групи цілей: користувальницькі цілі (досягнення заданої якості передачі) і мережеві (зонові) мети (оптимізація мережних або зонових показників ефективності). Завдання ухвалення рішення по управлінню МК (вибір $МУ_i^j$ $\forall$ $i$-х рівнів) зведена до завдання ієрархічного цільового динамічного оцінювання альтернатив при нечітких вихідних даних. Проведено декомпозицію глобальної мети управління мережею по функціях, кожна з яких ділиться на завдання й реалізується по рівнях OSI [11] (рис. 5).

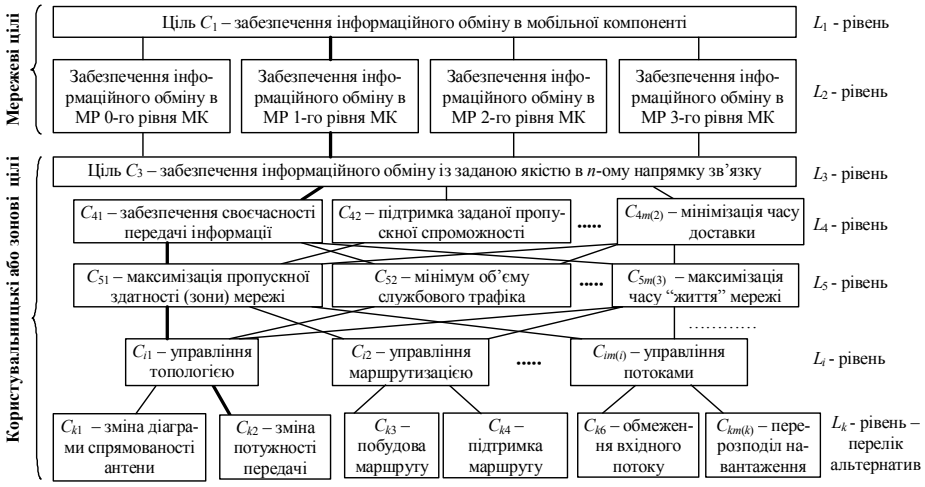



Рис. 5. Домінантна ієрархія процесу ухвалення рішення з управління МК

Запропоновано базу методів керування {МУ} для мереж тактичного рівня [12]. Мета – одержання вектора пріоритету елементів нижнього рівня ієрархії стосовно цілі – елементу першого рівня за допомогою методу аналізу ієрархій або методу згортки нечітких відносин.

Цільова структура управління МК: $ЦС \rightarrow H = \{C_1, R_{1m_{(1)}}\{C_{21}, C_{22}, \ldots, C_{2m_{(2)}}\}, R_{2m_{(2)}}\{C_{31}, C_{32}, \ldots, C_{3m_{(3)}}\}, \ldots, R_{km_{(k)}}\{C_{k1}, C_{k2}, \ldots, C_{km_{(k)}}\}\}$, де $C_1$ – основна ціль системи управління, $C_{im_{(i)}}$ – $m_{(i)}$-а підціль $i$-го рівня на цільовій структурі, $i$ =1…$k$, $R$ – множина відносин на підцілі структури. Запропонована побудова ієрархії процесу вибору альтернатив та порівняння рішень на кожному рівні ієрархії на основі нормалізації отриманих оцінок альтернатив (застосовуючи процедуру зважування методу аналізу ієрархій або метод згортки нечітких відносин).

Таким чином для виконання вимог до якості інформаційного обміну в мобільних радіомережах на напрямках зв'язку та зменшення службового трафіку в мережі пропонується:

1. Ввести координацію взаємодії між рівнями OSI за функціями управління.
2. На кожному рівні OSI ввести множину методів (протоколів) обміну, кожний з яких ефективний при певних умовах функціонування мережі.
3. Інтелектуалізувати процес прийняття рішення по вибору ефективного метода управління на кожному рівні OSI в залежності від стану (умов функціонування) мережі або напрямку та вимог типу трафіка.

ЛІТЕАТУРА


1. *Романюк В.А.* Мобильные радиосети – перспективы беспроводных технологий // Сети и телекоммуникации. – 2003. – № 12. – С. 62 – 68.
2. *Романюк В.А.* Мережі MANET – основа побудови тактичних мереж зв'язку // IV Науково-практичний семінар ВІТІ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення". – К.: ВІТІ НТУУ „КПІ". – 2007. – С. 15 – 28.
3. *Миночкин А.И., Романюк В.А.* Методология оперативного управления мобильными радиосетями // Зв'язок. – 2005. – № 2. – С. 53 – 58.
4. *Дымарский Я.С., Крутякова Н.П., Яновский Г.Г.* Управление сетями связи: принципы, протоколы, прикладные задачи. – М.: НТЦ „Мобильные коммуникации", 2003. – 384 с.
5. *Setton E., Yoo T., Zhu X., Gogdmith A., Girod B*. Cross-Layer Design of Ad-Hoc Networks for Real-Time Video Streaming // IEEE Wireless Communications, August 2005. – pp. 60 – 65.
6. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв'язок. – 2004. – № 2. – С. 46 – 50.
7. *Миночкин А.И., Романюк В.А.* Маршрутизация в мобильных радиосетях – проблема и пути решения // Зв'язок. – 2006. – № 7. – С. 49 – 55.
8. *Міночкін А.І., Романюк В.А., Сова О.Я.* Інтелектуальний метод маршрутизації в мобільних радіомережах // Збірник наукових праць № 1. – К.: ВІТІ НТУУ „КПІ".– 2009. – № 1. – С. 88 – 97.
9. *Миночкин А.И., Романюк В.А.* Управление топологией мобильной радиосети // Зв'язок. – 2003. – № 2. – С. 28 – 33.
10. *Міночкін А.І., Романюк В.А., Сова О.Я.* Багатопараметрична модель управління навантаженням в мережах MANET на основі нечіткої логіки // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2007. – № 2. – С. 137 – 149.
11. *Міночкін А.І., Романюк В.А.* Методи прийняття рішень системою управління мобільною радіомережею // Збірник наукових праць № 1. – К.: ВІТІ НТУУ „КПІ". – 2006. – С. 66 – 71.
12. *A. Minochkin, V. Romanyuk.* Control System of Mobile Ad-hoc Networks // In Proc. of International Conference Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET 2008), Lviv, 2008. – pp. 414 – 415.

д.т.н. Науменко М.І. (ДВОН МОУ)

# САМООРГАНІЗАЦІЯ В СИСТЕМІ ПІДГОТОВКИ ВІЙСЬКОВИХ ФАХІВЦІВ

Інноваційний розвиток військової освіти в Україні органічно пов'язаний із загальносвітовими тенденціями, характерними для XXI ст., становленням нашої держави та її інституцій. На початку третього тисячоліття можна впевнено констатувати, що освіта зайняла ключове місце в загальній стратегії розвитку сучасної світової цивілізації. Як відмічається в дослідженнях [4; 6, с. 11], освіта виступає в якості провідного механізму соціокультурної спадкоємності в розвитку суспільства; основи відтворення духовного потенціалу держави і розвитку індивідів, родової потреби, форми життя людини в суспільстві, що змінюється; механізму відтворення науки і культури; бази збереження історичної і національно-етнічної самоідентифікації народу; бази сучасної економіки; основи національної безпеки; головного механізму відтворення і розвитку суспільного інтелекту. Саме така освіта має стати провідним фактором соціально-економічного та суспільного прогресу держави. Як зазначає В.О. Кудін, – „у професійного спеціаліста будь-якого профілю має переважати прагнення творити і створювати, що відповідає справжньому покликанню людини у житті" [7, с.11]. Йдеться також про новий ціннісний підхід, щоб освіта у XXI столітті передбачала забезпечення неперервності у всіх ланках навчання, створення необхідних умов для доступу кожної людини до оволодіння новими знаннями, цінностями, відносинами, компетенціями і вміннями.

Водночас, на зміну лінійному уявленню про світ, що розвивається за стабільними і вічними законами, які уособлюють остаточну істину й змінюються під впливом людини, прийшло світорозуміння нестабільності самостворення й саморозвитку природних, суспільних, економічних та інших систем, альтернативних шляхів їхньої еволюції. „Як ці, так і інші питання, що стосуються майбутнього та перспектив розвитку складноорганізованих систем, вивчаються в руслі нового наукового напрямку – синергетики, яка, на наш погляд, може виступати в якості методологічної основи для прогностичної та управлінської діяльності в сучасному світі. Синергетика орієнтована на пошуки деяких універсальних законів еволюції і самоорганізації складних систем, законів еволюції відкритих нерівноважних систем будь-якої природи", – зазначають О.М. Князева та С.П. Курдюмов [5].

Як вважає Г. Хакен, принципи самоорганізації, що їх вивчає цей напрям науки, поширюються „від морфогенезу в біології, деяких аспектів функціонування мозку до флатера крила літака, від молекулярної фізики до космічних масштабів еволюції зірок, від м'язового напруження до спучування конструкції" [12, с. 16]. Можна стверджувати, що в даний момент саме синергетика є найзагальнішою теорією самоорганізації. Вона формулює найбільш загальні принципи самоорганізації, що діють на всіх структурних рівнях матерії, мовою математики описує механізми структурогенезису. В її рамках здатність до самоорганізації виступає як фундаментальна властивість усіх систем.

В основі синергетики лежать ідеї системності або цілісності світу і наукового знання, що його відображає, та загальності закономірностей розвитку всіх рівнів матеріальної і духовної організації, нелінійності чи багатоваріантності й необоротності, глибинного взаємозв'язку хаосу та порядку, кооперативної взаємодії окремих частин невпорядкованих систем певного типу (принцип синергетизму).

Синергетика як світобачення має значний гуманістичний та евристичний потенціал, оскільки її ідеї дають змогу виділити дещо спільне, взаємоподібне в процесах розвитку складних матеріальних і соціальних систем – як природних, так і економічних, політичних та ін. Це дає змогу прорахувати оптимальні для людей шляхи розгортання подій і, відповідно, отримати важелі управління процесами розвитку. Усвідомлення такого роду можливостей сприяє виживанню людей у непростій ситуації початку XXI ст. із загрозою безлічі катастроф:

ядерної, техногенної, екологічної, генетичної, біологічної, соціальної та ін. Саме синергетика дає надію на вирішення завдань, що виникли у зв'язку з цими загрозами, для виживання світової цивілізації.

У процесі розвитку синергетики прийшло розуміння того, що механізм розвитку, в основі якого лежить процес самоорганізації, чергування порядку та хаосу, є універсальним принципом світобудови, характерним для систем найрізноманітніших типів, у тому числі й для військово-освітньої.

Проблеми загальної інтерпретації розвитку освіти на засадах самоорганізації знайшли висвітлення в працях В.Г. Буданова [2], Л.Я. Зоріної [3], В.С. Лутая [8] та ін. Однак систематизованих досліджень з розвитку і трансформації військово-освітніх систем ще здійснено не було. Спробуємо й ми, зупинившись на принципах синергетичного підходу, відкритих в синергетиці, застосувати їх до розвитку військової освіти, щоб показати синергетизацію як сучасну тенденцію розвитку останньої.

Грунтуючись на викладених методологічних положеннях, наведемо аргументи на користь того, що військову освіту, як систему, можна досліджувати з позицій синергетичної методології. Ця система є:

– складноорганізованою;

– відкритою, тобто має джерела обміну енергією, інформацією із зовнішнім соціальним і культурним середовищем не тільки на межі системи, а й у кожній точці останньої;

– системою, що має потенціал самоорганізації і саморозвитку, тобто містить джерело, яке створює неоднорідність у системі (особистість майбутнього військового фахівця), і переборює дисипацію (розсіювання) цих неоднорідностей;

– нелінійною системою, тобто такою, що залежить від зовнішнього середовища і тому має не один, а велику кількість шляхів еволюції (процеси розвитку в цій системі відбуваються нерівномірно, можливі етапи надшвидкого розвитку, еволюція системи має незворотний характер);

– динамічною системою, тобто всередині її постійно відбуваються випадкові рухи, що забезпечують її нерівноважність, розвиток, самоорганізацію через нестійкість, випадковість стану.

Військова освіта, центром і головною метою якої є формування та розвиток особистості військового фахівця, еволюціонує шляхом самоорганізації, самостворення, де стимулюючий вплив можливий завдяки відповідно побудованому управлінню людьми з боку системи, тобто такому управлінню, яке враховує внутрішні тенденції та умови навколишнього середовища.

Застосування синергетичної моделі еволюції до аналізу проблем розвитку військової освіти дає можливість зрозуміти внутрішні механізми їх виникнення та еволюції, а також рівень взаємодії військової освіти з навколишнім середовищем. Обгрунтовуючи бачення механізму розвитку військової освіти з позицій синергетики, можна твердити, що з утворенням будь-якої освітньої системи у її функціонуванні мають місце як механізм онтогенезу (програма системи), так і механізм філогенезу (програма зміни системи), що на певних етапах еволюціїї приводять систему до розквіту чи занепаду. Програма становлення та розвитку освітніх систем поряд із соціальною (зовнішньою) організацією передбачає внутрішні механізми, здатні реагувати на набір флуктуацій, що виводять систему з рівноваги, на внутрішні умови акумулювання енергії, інформації, що й забезпечує освітнім системам здатність до розвитку, визначає стан-атрактор та підсумок її саомоорганізації.

Розглядаючи коротко ці нові методологічні принципи, відкриті в синергетиці, слід зазначити, що атрибутивною характеристикою для всіх складних відкритих систем є взаємодія двох протилежних понять: креативного, що створює певні структури, впорядковує хаос, і деструктивного, дисипативного (від лат. – „того, що розмиває"), спрямованого на ліквідацію будь-якої впорядкованості структури [3, с. 8; 5]. Саме взаємодія цих протилежних понять визначає створення, розвиток та ліквідацію всіх синергетичних систем.

Так, збільшення дії дисипативного джерела, вихід його за певні межі взаємодії з креативним призводять до нового знищення певної структури, до хаотичного стану даної системи. Проходження будь-якою синергетичною системою (чи її підсистемою) хаотичного етапу в своєму розвитку призводить до того, що подальший процес такого розвитку стає принципово недетермінованим, невизначеним, а тому й непередбачуваним, тобто виникають різні його варіанти, реалізуються різноманітні модифікації [11, с. 271], що характерне для розвитку військової освіти в Україні.

Розуміння військової освіти як системи відкритої та нелінійної передбачає нове ставлення до особистості майбутнього військового фахівця, що стає основою цієї системи.

Неповторність особистості постає одночасно і як постійне джерело стихійності та невпорядкованості, і як джерело розвитку. Свобода вибору, що є необхідним атрибутом кожної відкритої системи, не тільки дає можливість якнайповніше задовольняти освітні потреби у процесу навчання, а й стає засобом конструювання всієї системи, вихідним принципом її гуманізації.

В умовах свободи вибору якісно змінюються і зміст, і організація військово-освітньої діяльності. Реалізація принципу свободи вибору у військово-педагогічному процесі (ВПП) сприяє підвищенню його ефективності, розвиткові самостійності курсантів, допомогає вирішити проблему відчуженості їх від ВПП, оскільки:

– пізнання та вивчення значно активізуються, бо зумовлені вільним вибором курсанта;

– викладання набуває необхідної варіативності та диференційованості;

– суб’єкт навчання – курсант – стає реальною рушійною силою ВПП, співпрацює з викладачем;

– структура процесу навчання стає мобільнішою, змінюючись відповідно до обраного варіанта;

– методи навчання збагачуються самоосвітою, самовихованням, саморозвитком, загалом – самовдосконаленням особистості того, хто навчається;

– свобода вибору характеризує взаємозв’язок і взаємодію суб’єктів та інших компонентів ВПП.

Проблема формування єдиного Європейського освітнього простору відповідно до вимог Болонської декларації [1], перехід до двоциклової підготовки військових фахівців, на нашу думку, має суттєво змінити погляди на цей процес як мікросистему в межах системи більш вищого ієрархічного рівня – макросистеми. Йдеться про зміну підходів до функціональних, структурних та управлінських складових системи підготовки військових фахівців, кожна з яких включає такі компоненти: мету (проектування), комунікативний, змістовий, організаційний, аналітико-результативний, контрольний, коригувальний [9].

В якості основних елементів такої системи виступають суб’єкти та об’єкти діяльності (навчальні заклади, науково-педагогічні колективи, навчальні підрозділи), в якості системоутворюючих факторів – мета, зміст, способи, засоби і результат діяльності. Трансформація складових системи і її компонентів, їх відповідна адаптація до сучасних вимог має розв’язати низку протиріч, які постали на теперішній час, з одного боку, між вимогами Болонської декларації щодо рівнів, процесу та якості підготовки фахівців і системою підготовки військових фахівців, що склалася в нашій державі, а з іншого – протиріччями між вимогами європейської вищої освіти та організаційно-штатною структурою Збройних Сил України, спеціальностями підготовки спеціалістів, функціями та завданнями, які вони виконують.

Слід також пам’ятати, що мова йде про можливі варіанти адаптації системи військової освіти України до європейського освітнього простору, у якому, до речі, системи підготовки військових фахівців мають свої національні відмінності, які також не завжди відповідають зазначеним вимогам. Реальна, а не формальна реалізація вимог Болонської декларації потребує дослідження на засадах синергетики, аналізу, всебічного оперативно-тактичного та військово-економічного обґрунтування і лише на цій основі прийняття виваженого рішення.

Таким чином, синергетика як новий постнекласичний напрям міждисциплінарних досліджень процесів самоорганізації певним чином могла б у майбутньому виступити в ролі теоретико-методологічної основи подальшого вдосконалення військової освіти, а синергетизацію можна розглядати як тенденцію розвитку останньої. Методологічне й світоглядне значення синергетизації для військової освіти має стати предметом подальших досліджень і конструктивних дискусій.

ЛІТЕРАТУРА

1. *Болонський процес* у фактах і документах (Сорбонна-Болонья-Саламанка-Прага-Берлін) / Упорядники: Степко М.Ф., Болюбаш Я.Я., Шинкарук В.Д. та ін. – Тернопіль: Вид-во „Економічна думка”, ТАНГ, 2003. – 60 с.

2. *Буданов В.Г.* Трансдисциплинарное образование. Технология и принципы синергетики // Синергетическая парадигма. Многообразие поисков и подходов. – М: Прогресс-Традиция, 2000. – С. 52 – 78.

3. *Зорина Л.Я.* Отражение идей самоорганизации в содержании образования // Педагогика. – 1996. – № 4. – С. 105 – 109.

4. *Капица С.П., Курдюмов С.П.*, Малинецкий Г.Г. Синергетика и прогнозы будущего. – М.: Наука, 1997. – 285 с.

5. *Князева Е.Н., Курдюмов С.П.* Синергетика как новое мировидение: диалог с И. Пригожиным // Вопросы философии. – 1992. – № 12. – С. 3–20.

6. *Кремень В.Г.* Доповідь на ІІ Всеукраїнському з’їзді працівників освіти // Освіта України. – 2001. – 12 жовтня.

7. *Кудін В.О.* Освіта в інформаційному суспільстві. – К., 1998. – 151 с.

8. *Лутай В.С.* Синергетична парадигма як філософсько-методологічна основа формування світоглядів XXI століття // Філософія освіти XXI століття: проблеми і перспективи. Методологічний семінар: Збірник наукових праць. – Вип. 3 /За ред. В.П. Андрущенка. – К.: Знання, 2000. – С. 99 – 103.

9. *Науменко М.І. Приходько Ю.І.* Управління якістю військової освіти: теорія, методологія, практика // Наука і оборона. – К.: МО України. – 2009. – № 1. – С. 40 – 50.

10. *Пригожин И.И.* Природа, наука и новая рациональность //Философия и жизнь. – 1991. – № 7. – С. 11–15.

11. *Стенгерс И., Пригожин И.* Порядок из хаоса. – М.: Прогресс, 1986. – 431 с.

12. *Хакен Г.* Синергетика. – М.: Мир, 1980. – 246 с.

к.т.н. Польщиков К.О. (ВІТІ НТУУ „КПІ”)

# МЕТОДИ УПРАВЛІННЯ ІНТЕНСИВНІСТЮ ПОТОКІВ ДАНИХ В МОБІЛЬНІЙ РАДІОМЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Відомо, що сучасний бій характеризується швидкоплинністю, підвищеною маневреністю військ, застосуванням високоточної зброї, новими способами ведення бойових дій. Необхідне управління військовими силами і засобами можна здійснити лише шляхом забезпечення швидкого розгортання вузлів зв’язку, якісної доставки інформації на значних географічних територіях в умовах високої мобільності абонентів і деструктивних дій противника. На жаль, системи зв’язку, що використовуються зараз в Збройних Силах України мають ряд недоліків і не повною мірою задовольняють вказаним вище вимогам [1].

Останніми роками в середовищі учених і фахівців, що працюють в області мережних технологій, а також осіб і організацій, зацікавлених у використанні телекомунікаційних послуг, підвищений інтерес викликають мобільні радіомережі, які будуються на основі технології MANET (Mobile Ad-hoc Networks) [2, 3]. Специфіка мобільних радіомереж, перш за все, полягає:

1) у можливості доставки інформації в умовах випадкової, динамічної топології (взаємозамінюваність, мобільність всіх вузлів, відсутність фіксованих базових станцій, кожен вузол здатний функціонувати як маршрутизатор);

2) у реалізації децентралізованого управління елементами і процесами в мережі (самоорганізація мережі, автоматична адаптація до умов функціонування).

Перераховані вище можливості MANET, поза сумнівом, є перевагами цієї технології. Вони обумовлюють наявність у мобільних радіомереж таких важливих властивостей, як висока живучість і швидке розгортання. Першою властивістю мережі MANET володіють завдяки взаємозамінюваності всіх вузлів. Наявність другої властивості обумовлена можливістю автоматичної адаптації елементів мережі до умов функціонування.

Наявність вказаних переваг мобільних радіомереж виправдовує прагнення низки провідних країн світу застосувати технологію MANET для побудови телекомунікаційних мереж спеціального (військового) призначення [4]. Слід чекати, що в перспективі мобільні радіомережі спеціального призначення (МРСП) знайдуть гідне застосування і в армії нашої держави.

Необхідно відзначити, що абоненти МРСП мають можливість передачі по мережі різних видів трафіку, яка реалізується на основі застосування комутації пакетів. Інформаційні повідомлення, що передаються в MANET, утворюють мультимедійний трафік (мовні повідомлення, відео) і трафік даних (управляючі сигнали, текстові повідомлення, топографічні зображення, інша графічна і таблична інформація). Інтенсивність передачі інформації, ініційована роботою якої-небудь мультимедійної прикладної служби, є достатньо високою і близькою до постійного значення, тому такий вид трафіку часто іменують потоковим трафіком.

Для якісної передачі потокового трафіку необхідно мінімізувати затримку пакетів і її дисперсію (джиттер), при цьому допускаються незначні втрати пакетів [5 – 10]. При передачі даних, навпаки, затримки окремих пакетів на якість передачі даних не впливають, але при цьому потрібна гарантована безпомилкова доставка кожного пакету, тобто забезпечення вірогідності доставки даних при заданому рівні її оперативності. Доставка даних без помилок і втрат досягається за допомогою квитування (підтвердження приймачем успішно доставлених пакетів) і повторних передач втраченій інформації. Вказані процедури істотно ускладнюють процес передачі даних і збільшують час доставки повідомлень [11 – 12].

Відома велика кількість робіт, присвячених дослідженням, які спрямовані на забезпечення якісної передачі в MANET потокового трафіку [2, 3 – 16]. В той же час, мало уваги приділяється питанням задоволення вимог по доставці даних в мобільній радіомережі.

Одним з основних засобів, які можуть допомогти у вирішенні цих питань, є застосування в МРСП ефективного управління інтенсивністю потоків даних. Таким чином, викладені вище факти свідчать про актуальність наукових досліджень, що проводяться в рамках тематики даної доповіді.

Результати наукових досліджень показують, що наявність у мобільних радіомереж вищевикладених переваг не гарантує її абонентам високу якість доставки повідомлень. Доставка даних в МРСП істотно ускладнюється завдяки таким особливостям [16]:

1) короткочасністю існування з'єднань в результаті швидкої зміни мережної топології, викликаної мобільністю вузлів і впливом деструктивних чинників;

2) великими значеннями імовірності спотворення інформації, які викликані високим рівнем завад в радіоканалах;

3) великими значеннями імовірності втрати пакетів, обумовленої частими перевантаженнями мережі в результаті високої нестаціонарності її трафіку.

Це викликає необхідність пошуку ефективних засобів, застосування яких надасть можливість підвищити оперативність і забезпечити вірогідність доставки даних в МРСП.

Для задоволення вимог по доставці інформації в телекомунікаційних мережах розроблені методи, які іменуються методами забезпечення якості обслуговування користувачів (Quality of Service, QoS). Аналіз літератури [5 – 10] показав, що дані методи можна класифікувати, відповідно до схеми, зображеної на рис. 1.

Рис. 1. Класифікація методів забезпечення QoS в телекомунікаційних мережах

Все різноманіття відомих методів забезпечення QoS можна поділити на дві основні групи. До першої групи слід віднести методи збільшення кількості ресурсів мережі. Дані методи передбачають використання засобів, що збільшують пропускну спроможність фізичних каналів, наприклад, за рахунок застосування високошвидкісного середовища передачі або поліпшення характеристик сигналів.

Розробці методів, спрямованих на підвищення пропускної спроможності фізичних каналів, присвячена велика кількість плідних досліджень. Не випадково вважається, що найбільші успіхи в телекомунікаційній галузі пов'язані з прогресом саме технологій

фізичного і канального рівнів моделі взаємодії відкритих систем (Open System Interconnection, OSI). [17 – 24]. Але, як показує досвід, в сучасних умовах на практиці украй складно забезпечити високий рівень QoS в мережах тільки за рахунок збільшення їх фізичних ресурсів. Приведені вище аргументи свідчать про те, що для задоволення вимог абонентів по доставці інформації не достатньо піклуватися тільки про нарощування пропускної спроможності каналів, а необхідно вирішувати і інші не менш важливі завдання, пов'язані з її раціональним розподілом.

Потреба в одержанні послуг з необхідною якістю в умовах, коли можливості по передачі інформації обмежені дефіцитом пропускної спроможності каналів мережі, зумовила розробку методів, що відносяться в даній класифікації до другої групи. Методи раціонального розподілу обмежених мережних ресурсів в різних літературних джерелах трактуються як методи управління ресурсами або методи боротьби з перевантаженнями. Аналіз методів цієї групи показав, що переважна більшість методів, створених для раціонального розподілу мережних ресурсів, по суті, ґрунтуються на управлінні інтенсивністю інформаційних потоків.

У мобільних радіомережах для ефективної передачі потоків даних можна використовувати ряд існуючих методів управління трафіком, заснованих на зворотному зв'язку між джерелом і приймачем, наприклад, метод адаптивної зміни вікна прийому, метод Нагля, метод швидкої повторної передачі, багато методів управління оперативністю відправки підтверджень [7, 8, 10]. Певна частина методів в своїй основі використовує цікаві ідеї [12, 25 – 27], застосування яких могло б підвищити ефективність управління інтенсивністю потоків даних в мобільних радіомережах.

Проте запропонована реалізація цих ідей є неприйнятною, оскільки ґрунтуючись на евристичних алгоритмах і достатньо грубих, наближених моделях, вона не завжди сприяє прийняттю адекватних управляючих рішень. Тому для задоволення вимог по доставці даних в МРСП доцільно розробити нові теоретично обґрунтовані методи управління інтенсивністю потоків даних, засновані на адаптивній зміні: затримки відправки інформаційних сегментів в мережу, тайм-ауту повторної передачі та імовірності відкидання пакетів, що надходять у маршрутизатори.

Таким чином, з одного боку, з точки зору практики, потрібні технологічні рішення, що сприяють підвищенню оперативності і забезпеченню вірогідності доставки даних в МРСП, а з іншого боку, з погляду теорії, відчувається брак адекватних моделей і теоретично обґрунтованих методів ефективного управління інтенсивністю потоків даних, спрямованих на задоволення вказаних вимог. У зв'язку з цим актуальною є ***наукова проблема***, яка полягає в розробці теоретично обґрунтованих методів управління інтенсивністю потоків даних для підвищення оперативності і забезпечення вірогідності доставки даних в мобільних радіомережах спеціального призначення.

Важливим етапом вирішення поставленої проблеми є обґрунтування наукового апарату, застосування якого є доцільним для розробки ефективних методів управління інтенсивністю потоків даних в МРСП.

На характеристики процесу доставки конкретного повідомлення в МРСП впливають численні випадкові чинники, пов'язані з наявністю завад у радіоканалах, переміщенням вузлів, потребами абонентів в передачі інформації, характеристиками інформаційних потоків, працездатністю окремих вузлів, ураженням елементів мережі противником та ін. Зважаючи на наявність вказаних чинників складно адекватно оцінити поточний стан мережі, що характеризується ступенем завантаженості вузлів, наявністю доступної в мережі пропускної спроможності. Тим більше проблематично достовірно передбачити стан мережі в недалекому майбутньому.

Наприклад, відсутня можливість мати в своєму розпорядженні точні відомості про те, який проміжок часу пройде до отримання квитанції на тільки що відправлений пакет,

наскільки буде тривалим очікуваний сплеск інтенсивності трафіку і яких значень досягне при цьому черга пакетів в буфері маршрутизатора.

Адекватних моделей, здатних точно описати стан МРСП у будь-який момент часу, на жаль, не існує, а застосування наближених моделей в процесі управління ресурсами мережі не дає прийнятних результатів. Здавалося б, отримати точні відомості про поточний стан мережі можна, виміривши значення численних параметрів на всіх її ділянках.

Проте збір і доставка цієї інформації до вузлів, в яких здійснюється управління інтенсивністю потоків даних, по-перше, роблять архітектуру мережі більш складною, по-друге, створюють небажаний службовий трафік і, по-третє, обов'язково відбуваються з деякою затримкою, наявність якої сприяє частковій (або повній) втраті актуальності цієї інформації. Тому судити про ситуацію в мережі доводиться по значенням обмеженої кількості параметрів, які більшою мірою характеризують стан мережі не в даний час, а у минулому.

Таким чином, управління інтенсивністю потоків даних в МРСП відбувається в умовах наявності неповної, розмитої, неточної інформації про стан елементів цієї мережі в поточному часі і в майбутньому. Ефективним засобом управління в таких умовах є застосування систем нечіткого виводу [28 – 36].

Проте відомо, що класичним системам з нечіткою логікою, не здатним автоматично вивчатися, властивий істотний недолік, що полягає в тому, що набір нечітких правил, вигляд і параметри функцій приналежності, що описують вхідні і вихідні змінні системи, а також вид алгоритму нечіткого виводу, вибираються суб'єктивно експертом-людиною, тому вони можуть бути не достатньо адекватними дійсності [29]. Для усунення відміченого недоліку використовують апарат систем нейро-нечіткого виводу [28, 29]. Нечітка нейронна мережа – це багатошарова нейронна мережа, в якій шари виконують функції елементів системи нечіткого виводу.

Нейрони такої мережі характеризуються набором параметрів, налаштування яких здійснюється в процесі навчання, як в звичайних нейронних мережах [30]. Такі системи є, по суті, гібридними і об'єднують в собі переваги нейронних мереж і систем нечіткого виводу. З одного боку, вони дозволяють розробляти і представляти моделі систем у формі правил нечітких продукцій, що володіють наочністю і простотою змістовної інтерпретації. З іншого боку, для побудови правил нечітких продукцій використовуються методи нейронних мереж, що робить цей процес менш складним для дослідників [29]. Існує достатня кількість прикладів успішного використання систем нейро-нечіткого виводу в різних галузях науки і техніки [28 – 30].

Для вирішення завдання управління параметрами процесів, які або не піддаються, або піддаються з великими труднощами формалізованому опису, крім гібридних інтелектуальних систем успішно застосовуються системи, засновані на використанні ПІД-регуляторів. Системи, засновані на ПІД-регуляторах, відрізняються своєю простотою. При цьому застосування таких систем дозволяє здійснювати ефективне управління багатьма технічними процесами. Тому цілком виправданою є спроба застосувати системи, що ґрунтуються на нейро-нечіткому виводі і ПІД-регуляторах, для управління інтенсивністю потоків даних в МРСП.

В результаті декомпозиції поставленої проблеми було визначено наступні взаємопов'язані ***завдання дослідження***:

1) створення адекватних аналітичних і імітаційних моделей процесу доставки інформації в МРСП;

2) застосування отриманих моделей для дослідження особливостей і закономірностей процесу доставки інформації в МРСП з метою їх подальшого урахування при створенні нових методів управління інтенсивністю потоків даних;

3) розробка методів управління інтенсивністю потоків даних в МРСП з використанням систем нейро-нечіткого виводу;

4) розробка методів управління інтенсивністю потоків даних в мобільній радіомережі, що ґрунтуються на використанні ПІД-регуляторів;

5) оцінка ефективності управління інтенсивністю потоків даних, здійснюваного в МРСП відповідно до запропонованих методів, і розробка рекомендацій по їх практичному застосуванню.

В процесі вирішення сформульованих завдань одержано ряд наукових результатів. Основними результатами, що містять ***наукову новизну***, є:

1. Розвиток положень системного підходу до вирішення проблеми розробки теоретично обґрунтованих методів управління інтенсивністю потоків даних для підвищення оперативності і забезпечення вірогідності доставки даних в МРСП.

2. Методика моделювання доступної для трафіку даних пропускної спроможності мобільної радіомережі спеціального призначення.

3. Аналітична модель процесу доставки інформаційного повідомлення в МРСП.

4. Метод управління тайм-аутом повторної передачі в МРСП на основі застосування системи нейро-нечіткого виводу.

5. Метод управління затримкою відправки інформаційних сегментів в МРСП на основі застосування системи нейро-нечіткого виводу.

6. Метод управління імовірністю відкидання пакетів, що надходять до маршрутизаторів МРСП, на основі застосування системи нейро-нечіткого виводу.

7. Методи управління інтенсивністю потоків даних в МРСП на основі застосування ПІД-регуляторів.

Крім того, в результаті розв’язання наукової проблеми, одержано:

– модель процесу передачі в МРСП потокового трафіку, використання якої дозволяє імітувати зміну завантаженості мережних вузлів і дає можливість реалізувати методику моделювання доступної для трафіку даних пропускної спроможності мобільної радіомережі;

– аналітичну модель процесу передачі потокового трафіку в МРСП, застосування якої дозволяє обґрунтувати адекватність попередньої моделі;

– для оцінки ефективності управління інтенсивністю потоків даних в МРСП розроблено моделі процесу доставки даних, що імітують:

управління тайм-аутом повторної передачі, що здійснюється згідно з методом Джекобсона;

управління тайм-аутом повторної передачі, що здійснюється на основі застосування системи нейро-нічеткого виводу;

управління тайм-аутом повторної передачі, що здійснюється на основі застосування ПІД-регулятора;

управління вікном перевантаження, що здійснюється згідно з протоколом TCP Tahoe;

управління вікном перевантаження, що здійснюється згідно з протоколом TCP Reno;

управління затримкою відправки інформаційних сегментів, що здійснюється згідно з методом адаптивної швидкості;

управління затримкою відправки інформаційних сегментів, що здійснюється на основі застосування системи нейро-нечіткого виводу;

управління імовірністю відкидання пакетів, що надходять до маршрутизаторів, яке здійснюється відповідно до методу випадкового раннього виявлення перевантаження;

управління імовірністю відкидання пакетів, що надходять до маршрутизаторів, яке здійснюється на основі застосування системи нейро-нечіткого виводу;

управління імовірністю відкидання пакетів, що надходять до маршрутизаторів, яке здійснюється на основі застосування ПІД-регулятора.

Застосування вищезазначених результатів дослідження дозволяє в МРСП забезпечити вірогідну доставку даних і істотно підвищити її оперативність:

використання методів управління інтенсивністю потоків даних, що ґрунтуються на системах нейро-нечіткого виводу, дозволяє зменшити середній час доставки повідомлення на 15% – 21% у порівнянні з результатами застосування існуючих методів;

застосування ПІД-регуляторів для управління інтенсивністю потоків даних дає можливість у порівнянні з результатами використання існуючих методів зменшити середній час доставки повідомлення на 7% – 10%.

Таким чином, найбільш суттєво підвищити оперативність доставки даних в МРСП дозволяє практичне застосування методів управління інтенсивністю потоків даних, що ґрунтуються на системах нейро-нечіткого виводу. В той же час методи управління інтенсивністю потоків даних, що ґрунтуються на ПІД-регуляторах, відрізняються простотою реалізації, тому застосування їх на практиці може бути виправдано з економічних міркувань.

ЛІТЕРАТУРА

1. *Романюк В.А.* Напрямки розвитку тактичних систем зв'язку // II Науково-технічна конференція ВІТІ „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення". – К.: ВІТІ НТУУ „КПІ". – 2004. – С. 23 – 33.

2. *Basagni S., Conti M., Giordano S., Stojmenovic I.* Mobile Ad Hoc Networking. – IEEE Press, 2004. – 461 p.

3. *Романюк В.А.* Мобильные радиосети – перспективы беспроводных технологий // Сети и телекоммуникации. – 2003. – № 12. – С. 62 – 68.

4. *Миночкин А.И., Романюк В.А.* Методология оперативного управления мобильными радиосетями // Зв'язок. – 2005. – № 2. – С. 53 – 58.

5. *Вегеша Ш.* Качество обслуживания в сетях IP: Пер. с англ. – М.: Издательский дом „Вильямс", 2003. – 386 с.

6. *Столлингс В.* Современные компьютерные сети. 2-е изд. – СПб.: Питер, 2003. – 783 с.

7. *Кучерявый Е.А.* Управление трафиком и качество обслуживания в сети Интернет. – СПб.: Наука и техника, 2004. – 336 с.

8. *Таненбаум Э.* Компьютерные сети.: Пер. с англ. – СПб.: Питер, 2002. – 848 с.

9. *Паркер Т, Сиян К.* TCP/IP. Для профессионалов. 3-е изд. – СПб.: Питер, 2004. – 859 с.

10. *Куроуз Дж., Росс К.* Компьютерные сети. 2-е изд. – СПб.: Питер, 2004. – 765 с.

11. Математичні основи теорії телекомунікаційних систем / В.В.Поповський, С.О.Сабурова, В.Ф.Олійник, Ю.І.Лосєв, Д.В.Агеєв та ін.: За ред. В.В.Поповського. – Харків: ТОВ „Компанія СМІТ", – 2006. – 564 с.

12. *Польщиков К.О., Рвачова Н.В., Шкіцькій В.В.* Управління інтенсивністю передавання даних в інформаційних мережах, що здійснюється на транспортному рівні моделі OSI: методи, проблеми та шляхи удосконалення // Інформаційні інфраструктури та технології. – Полтава, 2009. – Вип. 1. – С. 55 – 58.

13. *Thompson D., Schult N., Mirhakkak M.* Dynamic Quality-of-Service for Mobile Ad Hoc Networks. – Boston: MobiHoc, 2000.

14. *Chun B.-G., Baker M.* Evaluation of Packet Scheduling Algorithm in Mobile Ad Hoc Networks // Mobile Computing and Communications Review, 2002.

15. *Xiao H., Chua K.C., Seah W.K.G.* A Quality of Service Model for Ad Hoc Wireless Networks. – FL USA, 2002.

16. *Миночкин А.И., Романюк В.А.* Управление качеством обслуживания в мобильных радиосетях // Зв'язок. – 2005. – № 8. – С. 17 – 23.

17. *Голышев В.Ю., Жуков Е.А.. Самариев И.Э., Слепов Д.Г.* Волоконно-оптические линии связи большой дальности // Успехи зарубежной радиоэлектроники. – 2004. – № 5-6. – С. 96 – 98.

18. *Поповский В.В., Григорьева Т.И.* Перспективы теории и практики телекоммуникаций // Радиотехника. Всеукр. межведомств. науч.-техн. сб. – 2002. – Вып. 128. – С. 4 – 10.

19. *Поповский В.В., Олейник В.Ф.* Накануне создания теории телекоммуникационных систем // Радиотехника. Всеукр. межведомств. науч.-техн. сб. – 2004. – Вып. 138. – С. 8 – 10.

20. *Поповский В.В.* Основные тенденции мирового развития телекоммуникаций // Радиотехника. Всеукр. межведомств. науч.-техн. сб. – 2001. – Вып. 123. – С. 4 – 8.

21. *Muqattash A., Krunz M.* CDMA-Based MAC Protocol for Wireless Ad Hoc Metworks // In Proceedings MOBIHOC'03, 2003.

22. *Tang K., Gerla M.* Random Access MAC for Efficient Broadcast Support in Ad Hoc Networks // In Proceedings WCNC'00, 2000.

23. *Jung E.-S., Vaidya N.H.* A Power Control MAC Protocol for Ad Hoc Networks // In Proceedings of MOBICOM'02, 2002.

24. *Deng J., Haas Z.* Dual Busy Tone Multiple Access (DTBMA): A New Medium Access Control for Packet Radio Networks // In Proceedings ICUPC, 1998.

25. *Floyd S. Jacobson V.* Random early detection gateways for congestion avoidance, IEEE/ACM Transactions on networking 1993 - 1(4), p.397 – 413.

26. *Rath H.K., Sahoo A., Karandikar A.* A Cross Layer Congestion Control Algorithm in Wireless Networks for TCP Reno-2 // IEEE Wireless Communications, August 2005.

27. *Alekseev I.V., Sokolov V.A.* ARTCP: Efficient Algorithm for Transport Protocol for Packet Switched Networks // Proc. Of PaCT'2001. – Springer-Verlag, 2001. – Vol. 2127. – P. 159 – 174.

28. *Рутковская Д., Пилиньский М., Рутковский Л.* Нейронные сети, генетические алгоритмы и нечеткие системы. – М.: Горячая линия – Телеком, 2006. – 452 с.

29. *Леоненков А.В.* Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург, 2003. – 703 с.

30. *Усков А.А., Кузьмин А.В.* Интеллектуальные технологии управления. Искусственные нейронные сети и нечеткая логика. – М.: Горячая линия – Телеком, 2004. – 143 с.

31. *Осовский С.* Нейронные сети для обработки информации. – М.: Финансы и статистика, 2002.

32. *Гостев В.И., Крайнев В.В., Скуртов В.Н.* Синтез цифровых регуляторов систем автоматического управления параметрами теплоэнергетических объектов. – К.: Радіоаматор, 2007. – 264 с.

33. *Кір'янов Д.В.* Вітростійкий підйом антенної щогли рухомих засобів радіозв'язку на основі САУ з нечітким регулятором // Телекомунікація-2005: Матеріали II Міжрегіональної науково-практичної конференції (25 жовтня 2005 р.). – Полтава: ПВІЗ, 2005. – С. 32 – 33.

34. *Гостев В.И.* Синтез нечетких регуляторов систем автоматического управления. – К.: Радіоаматор, 2005. – 708 с.

35. *Гостев В.И., Клюфас С.И., Захарчук О.В.* Синтез нечетких регуляторов следящих координаторов. Артиллерийское и стрелковое вооружение. – К.: НТЦ, 2003. – Вып. 7. – С. 41 – 47.

36. *Гостев В.И., Кунах Н.І., Науменко М.І.* Системи автоматичного регулювання потужності передавача в каналах радіозв'язку. – К.: Радіоаматор, 2007. – 332 с.

к.пед.н. Приходько Ю.І. (НУОУ)

# МЕТОДОЛОГІЧНІ ЗАСАДИ ІННОВАЦІЙНОГО РОЗВИТКУ ВІЙСЬКОВОЇ ОСВІТИ

Історичний досвід та спеціальні наукові дослідження [1, 2] красномовно свідчать, що саме від якісного стану системи освіти та її орієнтованості на інноваційний, науково-технологічний розвиток залежить не лише життєздатність будь-якої держави, але й її авторитет, значимість та лідерство в світовому співтоваристві. Невіддільною складовою загальнодержавної є система військової освіти.

Як відомо, визначальний вплив на систему військової освіти здійснюють соціально-економічні умови країни, військова політика держави, рівень розвитку освіти, науки, техніки, культури. В умовах науково-технічного прогресу продовжує зростати залежність системи військової освіти від воєнно-технічного та технологічного факторів. Стрімко зростає технічна оснащеність армії та флоту, з'являються нові засоби збройної боротьби, вдосконалюються способи бойових дій. Розвиток бойової техніки і озброєння відбувається на базі інформаційних технологій та систем, мікроелектроніки, автоматики, обчислювальної техніки, що передбачає розуміння майбутніми фахівцями різних рівнів надзвичайно складних процесів, що відбуваються в апаратурі, знання оптимальних умов її експлуатації та застосування. Сучасні зброя, техніка, тактика, оперативне мистецтво вимагають більш грунтовних теоретичних, загальнонаукових знань, військово-професійних умінь і навичок, високої морально-психологічної підготовки особового складу, що потребує постійного вдосконалення військово-педагогічного процесу [4, 5, 8].

Реформування національної системи освіти в Україні відзначається масштабністю та радикальністю, що повинно привести до якісно нового рівня її функціонування. При цьому йдеться не просто про окремі вдосконалення тих чи інших напрямків, а про зміну парадигмальних основ її розвитку. Якщо йти в реалізації цього процесу стихійним шляхом, то це може привести до механістичного, еклектичного поєднання ряду нових ідей і проектів з традиційною освітньою практикою що, в свою чергу, з одного боку, знецінить і дискредитує це починання, а з другого – призведе до наростання у військово-освітній сфері деструктивних явищ та процесів. Тому є необхідність здійснення інноваційних змін в системі військової освіти на основі розроблених і узгоджених в рамках єдиної парадигми світоглядних, концептуальних та методологічних засад.

Тобто, мова йде про характер інноваційного процесу у військовій освіті, про його суть, про співвідношення змінних та стабільних компонентів в освітньо-педагогічних процесах, про шляхи трансформації традиційного, усталеного в нове, незвідане. І пріоритетність цих процесів зрозуміла: адже без зв'язку з традицією немає новаторства та без використання досвіду минулого не можна побудувати майбутнє.

Як відмічається у передмові спеціального збірника [6, с.3], – „На жаль, ще не існує чіткої науково-теоретичної концепції педагогічної інновації в Україні, системи відбору та оцінювання тих чи інших нововведень; не визначена роль і місце закладів освіти інноваційного типу та педагогів-інноваторів у системі освіти. Це завдання найближчого майбутнього, які ставляться Міністерством освіти і науки та Академією педагогічних наук України перед науковцями і дослідниками". Але вже зараз можна говорити про те, що зроблено суттєві кроки в розв'язанні проблеми педагогічних інновацій, узагальнена сукупність яких може бути визначена поняттям „інноваційна педагогіка".

Звернемося до поняття „інноваційна діяльність". Саме поняття „інновація" походить від латинського – „оновлення, новизна, зміна". Новизна – це ідея, що є для конкретної особи новою. При цьому, як відмічає американський учений К. Роджерс: „Немає значення чи є ідея об'єктивно новою чи ні, ми визначаємо її в часі, який минув з її відкриття або першого використання". [Цит. за 6, с. 5]. Франц Брансуік визначає інновацію як нову ідею, або дію,

або адаптовану ідею, або ті, для яких настав час реалізації [там же, 6, с. 5]. В.Ф. Паламарчук визначає педагогічну інновацію як „результат творчого пошуку оригінальних, нестандартних рішень різноманітних педагогічних проблем” [7, с. 5], О.Я.Савченко – як процес створення, поширення у використанні нових засобів (нововведень) для розв’язання тих педагогічних проблем, які досі розв’язувались по-іншому [11], а Л.І. Даниленко, відмічаючи, що інноваційна освітня діяльність, передбачаючи розвиток творчого потенціалу педагога, стосується „не лише створення та поширення новизни, а й змін у способі діяльності, стилі мислення особистості”. При цьому, на думку автора, – „для педагога інноваційним є формування активної, ініціативної позиції учня; для керівника навчально-виховного закладу – розвиток творчих потенціальних можливостей кожного його учасника” [7 с. 11].

Рушійною силою, джерелом інноваційного розвитку військово-педагогічного процесу, що реалізується в системі військової освіти, є об’єктивно притаманні йому суперечності. Вони виражають специфіку військово-освітнього процесу, його багатоманітність і спонукають до інноваційної діяльності. Виділимо деякі групи суперечностей системи військової освіти як джерела її розвитку.

*По-перше,* це суперечності між вимогами до високої якості військової освіти і її реальним станом; між досягненнями сучасної науки, озброєння та військової техніки і ступенем відображення їх в системі військової освіти; між вдосконаленими способами бойових дій і методикою їх вивчення та інші. Головною умовою розв’язання цих суперечностей є глибоке розуміння та оперативна реалізація через систему інновацій вимог української держави до підготовки особового складу в сучасних умовах (вони викладені в керівних документах щодо будівництва та розвитку Збройних Сил України, в Концепції військової освіти України). *По-друге,* це суперечності процесу формування особистості майбутніх захисників Вітчизни в системі військової освіти: між цілісним характером формування особистості та мірою розвитку її окремих якостей, між прагненнями особистості та її реальними можливостями, між старими (тими, що склалися) і новими способами діяльності тощо. Головною умовою розв’язання суперечностей такої групи є допомога майбутнім військовим фахівцям в їх усвідомленні та розв’язанні. *По-третє,* суперечності, власне педагогічного характеру, між вихованням, навчанням, розвитком, психологічною підготовкою, самовихованням і самоосвітою, між навчально-виховними впливами суб’єктів освітнього процесу та рівнем підготовленості, вихованості фахівців і військових колективів, між характером сучасного бою та досягнутим рівнем його моделювання в військово-педагогичному процесі. Основними умовами їх розв’язання є піклування командирів та науково-педагогічного складу щодо військово-професійної спрямованості освітнього процесу; наближення процесу навчання особового складу до умов бойової обстановки; постійне підвищення рівня педагогічної культури і методичної майстерності; цілеспрямоване керівництво самовихованням і самоосвітою. *По-четверте*, це суперечності, що носять випадковий характер і були викликані суб’єктивними факторами – це різного роду відхилення від вимог військових статутів, інструкцій, відстала матеріально-технічна база, низька організація навчального процесу, недостатня психолого-педагогічна підготовка викладачів, офіцерів і т.ін. Шляхи подолання цієї групи суперечностей обумовлюються причинами їх виникнення та конкретними умовами, що характеризують стан справ у навчальному підрозділі. Головне тут – підвищення організованості, особистої відповідальності та педагогічної майстерності офіцерів-наставників, підвищення загальної культури тих, хто навчається.

Форми прояву та розв’язання суперечностей військово-педагогічного процесу в системі освіти багатоманітні. Але всі вони виступають для учасників інноваційних процесів у вигляді певних труднощів, подолання яких вимагають великої напруги, розумових і фізичних сил, творчого відношення до справи, спільних і зустрічних зусиль суб’єктів викладання та навчання. Але шляхом зняття одних суперечностей інноваційного процесу породжуються

інші, які знову розв'язуються та знову проявляються на новому якісному рівні. В цьому і полягає суть безперервного інноваційного розвитку військової освіти.

Зупинимося тепер на конкретних методологічних підходах щодо здійснення інновацій в системі військової освіти. У кожного з методологічних підходів є своя технологія, для побудови якої вимагається немало знань і творчості. Важливою тенденцією розвитку сучасного методологічного знання науки про освіту є те, що методологія все активніше проникає зі сфери наукових досліджень в галузі практики. Методологія педагогічної науки стає практично орієнтованою. Спеціалісти усіх структур освіти, що володіють методами і процедурами дослідження та перетворення освітньо-педагогічної реальності, більшою мірою вільні від помилок і хиб в своїй творчій роботі. А поєднання наукових інструментів з практикою управління розвитком педагогічних систем дозволяє раціоналізувати інноваційну діяльність в галузі освіти і самої науки, як її відображення [3]. Певні підходи до цього процесу знайшли відображення в науковій літературі [7, 9, 10, 12]. Критично-конструктивне їх переосмислення дозволяє сформулювати ряд методологічних вимог, яких слід дотримуватися при здійсненні інноваційних перетворень у військовій освіті. Вони зводяться до наступного.

*По-перше,* слід впевнитися в недосконалості, неефективності, застарілості тієї освітньо-педагогичної структури, чи типу управлінської, педагогічної діяльності, яку планується реформувати. При цьому ні „власне адміністративне передчуття", ні спонтанне бажання "щось обновити", ні мотиви смакових переваг не можуть бути достатніми підставами для початку реформаторської діяльності. Об'єктивною основою в цьому випадку є аналіз і оцінка освітньо-педагогічної системи за надійними критеріями, які і повинні виявити, доказати її недосконалість, застарілість чи неефективність. Такими показниками і критеріями, на нашу думку, можуть бути реальний розвиток курсантів, готовність їх до служби в Збройних Силах України, рівень освіти і вихованості, здоров'я і культури, життєвого благополуччя чи невлаштованості, міра самореалізації тощо.

Критеріальні засоби оцінки стану освітньо-педагогічних систем в сучасних умовах реалізуються шляхом педагогічної діагностики: контроль за якістю навчання з його різновидами: попереднім, поточним, періодичним, підсумковим, а також у відповідних термінах „моніторинг", „рейтинг", „експертиза", „інспекторська перевірка" тощо. Суттєвим для діагностики є уведення державних стандартіві освіти, компентентнісний підхід, який покладено в їх основу. Саме тоді, коли порівняльний аналіз буде свідчити не на користь стану справ відносно мінімального (чи оптимального) державного рівня знань, умінь і навичок, виникає потреба в новаціях. Логіка такого методологічного підходу очевидна та зрозуміла: не слід надмірно захоплюватися новаціями і реформувати те, що є продуктивним, що відповідає інтересам суспільства, диктується вимогами освітньо-педагогічного процесу. Тільки тоді, коли отримана достовірна картина застарілого, неефективного, нераціонального в освіті, чітко встановлені, описані та обгрунтовані межі цієї невідповідності, можна переходити до наступного етапу освітніх реформ.

*На другому етапі* проведення інновацій слід шляхом широкого, ретельного аналізу провести пошук передових педагогічних технологій, зразків освітніх рішень, що носять випереджувальний характер і можуть бути використані для моделювання новацій, що прийдуть на зміну застарілому та неефективному. При цьому слід відшукати передовий, прогресивний досвід як у вітчизняній, так і світовій практиці, знайти позитивні приклади, той „будівельний матеріал", з якого можна створити нові освітні конструкції. Доцільно звернутися при цьому до наукових розробок, де містяться творчі рішення учених та практиків. Зараз, наприклад, є дані щодо формування не лише бібліотечних, але й комп'ютерних центрів освітньо-педагогічних інновацій, а в перспективі передбачається створення Міжнародного банку педагогічних інновацій.

Важливо не тільки дізнатися та описати досвід, що має локальне, місцеве значення і часто пов'язаний з персональними носіями цього досвіду – професорами, викладачами чи

конкретними педагогічними колективами, що працюють в певних, цілком визначених, конкретних умовах. Важливо обгрунтувати можливість і необхідність переносу цього (в чомусь інноваційного, продуктивного досвіду) в нові умови, зробити його здобутком більш масової практики.

З наукознавства відомо, що залишаючись на емпірічному рівні, неможливо розраховувати на те, що той чи інший, навіть самий передовий і прогресивний досвід, може бути повтореним з таким же успіхом в інших умовах, в діяльності інших педагогів чи військово-педагогічних колективів. Тому недопустимо приймати управлінські рішення (а інколи цим страждають керівники військово-освітньої сфери старої формації, що хочуть враз „перелаштуватись" в новаторів) про негайне, безпосереднє і всезагальне поширення (або ще гірше –обов'язкове впровадження) того чи іншого досвіду. В нових умовах, в діяльності інших педагогів, інших педагогічних колективах цей досвід може не дати належного ефекту. Більш того, може виявитись, що він зовсім неприйнятний в цих умовах, а значить його застосування може призвести до результатів діаметрально протилежних до очікуваних. Адже ще К.Д. Ушинський відзначав, що переноситись в нові умови повинен не сам досвід як такий, навіть якщо він описаний самим детальним чином, а думка, ідея, що виведені із цього досвіду.

Трансформація практичного досвіду, фактів в абстраговане від суто місцевих умов прояву цього досвіду знання, що здатне побачити типове, регулярне та закономірне в явищах, веде до формування теоретичного знання в формі концепцій чи теорій.

Наступним, *третім кроком* в ланці перетворень освітніх систем є проектування інноваційної моделі оновлюваної освітньої системи від її ескізу до робочих проектів. Тобто створюється модель освітньої новації з конкретними, певним чином визначеними, властивостями, що відрізняють її від традиційного варіанту, на зміну якому вона пропонується.

У випадку масштабних реформ в системі військової освіти, а саме такий проект ми зараз реалізуємо, методологія освітньої діяльності передбачає фінансове, економічне, соціальне, організаційне, матеріальне, кадрове, просторове та часове обгрунтування новацій. Саме на стадії проектування закладаються задумані переваги перед попередніми моделями освітньо-педагогічної діяльності та дається всебічна характеристика кожного з компонентів новацій.

*Четвертим етапом* методології перетворення освітньої структури є практичне здійснення новацій, побудова алгоритму втілення їх у практику. Сутність цього в тому, що значні новації розкладаються на проектний етап та етап впровадження. Це вимагає персоніфікації завдань, в результаті чого повинно бути зрозуміло, хто за що відповідає, якими засобами його слід забезпечити, кому належать функції контролю та корекції, ходу перетворень, з кого слід запитати за невдачі чи заохотити за успіхи. Ця ж вимога передбачає опрацювання тих змін, які відбудуться в освітній, пізнавальній, керівній діяльності всіх тих, кого зачіпає новація після її втілення в життя. Особливу увагу при цьому слід звернути на інтенсивність і ефективність новацій, тобто які зміни в професійній діяльності кожної людини вона викличе, чи призводить це до більш оптимального використання робочого часу викладачів, курсантів, до кращого засвоєння навчального матеріалу та підвищення продуктивності військово-педагогічного процесу.

Проблема впровадження нового є однією з найскладніших в управлінні інноваційними процесами. Світова педагогічна практика містить багато прикладів опору навіть самим привабливим і цікавим новаціям. Дослідники виділяють психологічні фактори негативного відношення до новацій, серед яких вказують на стереотипи, які активно формуються при переході від старого до нового.

У контексті викладеного важливого значення набуває проблема підготовки науково-педагогічних кадрів на новій основі, яка передбачає формування військових педагогів з такими якостями, як відкритість до нового, тобто формування протилежного стереотипам і

шаблонним методам роботи, консерватизму, догматизму педагогічного мислення; рефлексивність самоусвідомлення себе як суб'єкта спілкування, суб'єкта пізнання, суб'єкта професійної діяльності, індивіда в цілому; комунікативність з усіма її різновидами (інформаційна, когнітивна, емоційна, креативна). Саме вони повинні виступати своєрідними педагогічними менеджерами, адже в їх розпорядженні тимчасово, чи на більший проміжок часу, поступає колектив курсантів, отже основним завданням військового педагога є забезпечення розвитку кожного учасника навчально-виховного процесу. Необхідною умовою цього є „розкріпачення" кожного педагога, переведення його праці та всього колективу в цілому в режим розвитку, в режим потреби запровадження авторських та запозичених інновацій.

Важливим тут є застосування методології узагальненого алгоритму процесу впровадження результатів досліджень в практику [3, 12].

З урахуванням викладеного вище його складовими доцільно виділити такі етапи і кроки: 1) аналіз практики для пошуку ділянок, що підлягають оновленню чи заміні; 2) моделювання власне новацій на основі аналізу досвіду та даних науки; 3) розробка критеріїв оцінки освітньо-педагогічної діяльності для замірів її покращення при впровадженні новацій; 4) розробка програми освоєння нового кращими педагогами; 5) навчання новаціям всіх; 6) плавний, поступовий, чи навпаки, різкий і швидкий, перехід на роботу за інноваційною системою; 7) моніторинг наслідків і корекція дій.

Застосування методології інноваційних перетворень має на меті надання реформаторському освітньому процесу наукового характеру, практичної спрямованості, запобігання втрат матеріальних та інтелектуальних ресурсів, сприяння підвищенню якості підготовки військових фахівців, ефективності функціонування системи військової освіти.

ЛІТЕРАТУРА

1. *Гершунский Б.С.* Философия образования для XXI века. – М.: Совершенство, 1998. – 608 с.

2. *Клімова Г.П.* Освіта і цивілізація. Харків: Право, 1996. – 128 с.

3. *Краевский В.В.* Методологическая рефлексия // Сов. педагогика. – 1982. – №2. – С. 25 – 28.

4. *Науменко М.І., Приходько Ю.І.* Методологічні аспекти військової освіти // Зб. наук. праць „Вісник Національної академії оборони України". – К.: МО України. – 2008. – № 3 (7). – С. 45 – 51.

5. *Науменко М.І. Приходько Ю.І.* Управління якістю військової освіти: теорія, методологія, практика // Наука і оборона. – К.: МО України. – 2009. – № 1. – С. 40 – 50.

6. *Наукове та методичне* забезпечення впровадження педагогічних інновацій. Збірник наукових праць / Ред. кол.: Л.І.Даниленко (відп. ред.) та ін. – Херсон: ЦНТЕІ,1999. – 254 с.

7. *Наукове проектування* інноваційних та альтернативних систем вищої освіти: Збірник матеріалів до Всеукраїнської науково-практичної конференції, 11–12 травня 2000 р. / В.П.Андрущенко (ред.) та ін. Інститут вищої освіти АПН України, Тернопільська академія народного господарства – Тернопіль: Економічна думка, 2000. – 224 с.

8. *Основні засади* розвитку вищої освіти України в контексті Болонського процесу (документи і матеріали) / За ред. В.Г. Кременя. – Тернопіль: Вид-во ТДПУ, 2004. – 147 с.

9. *Позінкевич Р.О.* Освіта в системі культури: Монографія. – Луцьк: Ред.-вид відділ "Вежа" Волинського державного університету ім. Лесі Українки, 2000. – 348 с.

10. *Романенко М.І.* Освіта як об'єкт соціально-філософського аналізу. – Дніпропетровськ: Промінь, 1998. – 254 с.

11 *Савченко О.Я.* Дидактика початкової школи. – К: Абрис, 1997. – 400 с.

12. *Степанов С.Ю.* Рефлексивная практика творческого развития человека и организации. – М: Наука, 2000. – 174 с.

д.т.н. Слюсар В.І.(ЦНДІ ОВТ)

# МЕТАМАТЕРІАЛИ В МІМО-АНТЕННАХ

Основною тенденцією розвитку електронних технологій вже багато років є їх мініатюризація, а попит на все більш компактні проекти – постійно зростає. Революційні зміни у виробництві напівпровідників і методології проектування мікроелектронних пристроїв сприяли досягненню дуже високих норм упаковки елементів і компактних розмірів виробів в цілому. Проте, в пристроях зв'язку розміри антен все ще залишаються приводом для нарікань. Технологія друкованих антен, яка була перспективною близько двох десятиріч тому, нині досягла своїх меж щодо скорочення габаритів надвисокочастотних (НВЧ) пристроїв. Тому пошук нетрадиційних підходів до реалізації мікрохвильової техніки останнім часом істотно активізувався, про що свідчить серія публікацій автора за технологіями електрично малих антен (ЕМА) [1 – 3]. Один з нових напрямів в розвитку теорії ЕМА пов'язаний з досягненнями в області створення метаматеріалів. Розглянемо основні результати в даній області стосовно завдання удосконалення техніки ЕМА систем МІМО.

## Історія і класифікація метаматеріалів

Одна з перших спроб реалізації концепції штучних електромагнітних матеріалів документально простежується в кінці XIX-го сторіччя, коли в 1898 р. Джагадіс Чандра Бозе (Jagadis Chandra Bose) провів перший мікрохвильовий експеримент з дослідження поляризаційних властивостей створених ним структур викривленої конфігурації. В 1914 р. Ліндман (Lindman) впливав на штучні середовища, що були множиною безладно орієнтованих маленьких дротів, скручених у спіраль і вкладених у фіксуюче середовище.

В 1946–48 рр. Уїнстон Кок (Winston E. Kock) вперше створив мікрохвильові лінзи, використовуючи провідні сфери, диски і періодично розташовані металеві смужки, що фактично утворили штучне середовище, яке демонструвало специфічний за величиною ефективний індекс заломлення. З тих пір складні штучні матеріали стали предметом вивчення для багатьох дослідників у всьому світі. Останніми роками нові поняття і концепції в синтезі метаматеріалів сприяли створенню структур, імітуючих електромагнітні властивості відомих речовин або маючих якісно нові функції.

Приставка „мета-" має грецьке походження і переводиться як „зовні", що дозволяє трактувати термін „метаматеріали" як структури, чиї ефективні електромагнітні властивості виходять за межі властивостей, утворюючих їх компонентів. Одна з перших згадок цього терміну відноситься до випуску новин 1999 року форуму промислової і прикладної фізики (FIAP) Американського фізичного співтовариства (APS), що анонсував в програмі засідання APS на березень 2000 р. серію докладів по секції „Метаматеріали". Серед включених в програму секції докладів фігурує виступ Роджера Уелсера (Rodger M. Walser) [4] з університету штату Техас в Аустіні, якого і вважають автором терміну „метаматеріал". Втім, практично одночасно з ним аналогічне поняття застосував Елі Яблоновіч (Eli Yablonovitch), чий доклад на згаданому форумі містив у назві слово „Meta-Materials".

Аналіз публікацій з різних аспектів технологій метаматеріалів дозволяє класифікувати все різноманіття штучних середовищ залежно від ефективних значень їх діелектричної (ε) і магнітної (μ) проникностей згідно класифікаційній діаграмі, представленій на рис. 1. На ній фігурують як штучні середовища, так і матеріали природного походження.

Майже всі природні речовини мають діелектричну постійну і магнітну проникність більше нуля. Суттєво, що у переважної більшості з них в найцікавіших для практичного використовування діапазонах частот ці параметри, як правило, взагалі більші або рівні одиниці. В закордонній літературі дані матеріали звичайно називають DPS (double positive, подвійні позитивні), підкреслюючи тим самим позитивність значень як ε, так і μ. На класифікаційній діаграмі рис. 1 цим природним матеріалам відповідає правий верхній

квадрант. DPS-середовища вважаються прозорими для електромагнітних хвиль, якщо внутрішні втрати в них (уявні складові діелектричної і магнітної проникностей) малі. В прозорих середовищах електромагнітні поля існують у формі електромагнітних хвиль, що розповсюджуються, хоча незначна частина їх енергії в тій чи іншій мірі піддається поглинанню.

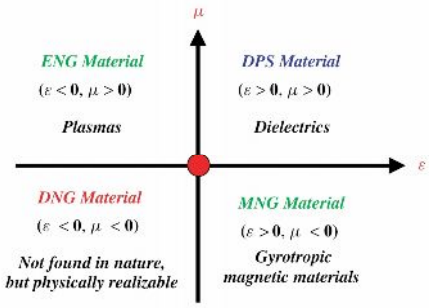



Рис. 1. Класифікація фізичних середовищ, залежно від знака величин діелектричної (ε) і магнітної (μ) проникностей

Матеріали, у яких негативний лише один з електромагнітних параметрів (ε або μ), на прийнятому за кордоном науковому жаргоні фігурують під назвою SNG (single negative, мононегативні). В таких середовищах електромагнітні хвилі не розповсюджуються і швидко затухають. З цієї причини відносно подібних матеріалів вважають, що вони непрозорі для випромінювання, якщо їх товщина більша за характерну експоненціальну довжину загасання електромагнітних хвиль. Залежно від того, який саме з параметрів приймає негативні значення, розрізняють два типи SNG-середовищ: так звані ENG (ε–негативні, для яких, як випливає з назви, ε<0 і μ>0) і MNG (μ–негативні, тобто такі, що мають параметри ε>0 і μ<0).

**Бінегативні середовища**

Останні кілька років були багаті подіями в області розвитку концепцій і рішення проблем створення метаматеріалів, що мають негативний коефіцієнт заломлення електромагнітних хвиль. Ефект негативного заломлення обумовлений одночасно негативними значеннями діелектричної постійної і магнітної проникності (ε <0, μ <0). Внаслідок негативних значень обох вказаних параметрів дані матеріали часто називають бінегативними середовищами (DNG, double negative). Донедавна цей клас матеріалів демонструвався тільки на основі штучних конструкцій, однак у 2006 р. було встановлено, що кристали $La_{2/3}Ca_{1/3}MnO_3$ мають негативний коефіцієнт заломлення електромагнітних хвиль у діапазоні 150 ГГц. Місце подібних середовищ на класифікаційній схемі відомих матеріалів може бути графічно представлено, як показано на рис. 1.

До розуміння фізики середовищ DNG сучасна наука підходила поволі і досить тривалий час. В результаті систематичних досліджень даного процесу за допомогою доступної літератури, у тому числі, в Інтернет, вдалося отримати деякі цікаві спостереження з історії даної області, які не слід розцінювати як спробу однозначних тверджень про пріоритет тих або інших відкриттів.

Перший етап на шляху формування сучасних уявлень про DNG пов’язують з розвитком теорії зворотних хвиль, одним з ключових понять якої стала негативна групова швидкість хвилі. Судячи з доступних в Інтернет публікацій, пальму першості в практичній постановці питання про існування хвиль з негативною груповою швидкістю слід віддати англійському фізику Артуру Шустеру (Franz Arthur Friedrich Schuster, 1851–1934). По суті, цей факт в своїй публікації [5] датованій 11 лютого 1904 р., відзначив англійський математик і гідродинамік Горацій Лемб (Horace Lamb, 1849 – 1934). За словами Г. Лемба, А. Шустер знайшов формальну можливість негативної групової швидкості електромагнітних хвиль, аналізуючи формулу з оптики, що стосується аномальної дисперсії світла. А. Шустер запропонував Г. Лембу перевірити гіпотезу про умови виникнення хвиль з негативною груповою швидкістю, що той і зробив з позитивним результатом, описаним в [5]. Таким чином, Г. Лемб з подачі

А. Шустера в 1904 р. вперше розглянув зворотні хвилі в механіці, що розповсюджується в одному і двох вимірах. Отримавши аргументацію Г. Лемба [5], в тому ж 1904 р. А. Шустер узагальнив цю теорію на оптичні явища, вперше показавши в своїй книзі [6], що зворотні електромагнітні хвилі можливі при негативній груповій швидкості, а також, що на межі двох середовищ в одному з яких розповсюджується пряма хвиля, а в іншому – зворотна, виникає негативне заломлення (рис. 2 [6]). Так, дякуючи А. Шустеру, вказівка на можливість негативного заломлення вперше з'явилася у фізичній літературі. Проте при цьому не деталізувалося, якими могли бути характерні властивості відповідного середовища у разі його існування.

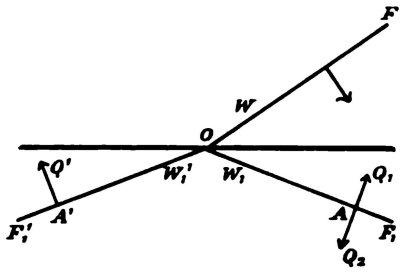



Fig. 179.

Рис. 2. Ілюстрація А. Шустера з книги [6], показує, що відхилення хвилі при вході в середовище з негативною груповою швидкістю відбувається на кут, більший кута падіння, убік, протилежний заломленню у звичайному середовищі ($WF$ – фронт падаючої хвилі, $W_1^{'}F_1^{'}$ – фронт заломленої хвилі у звичайному середовищі, $W_1F_1$ – фронт заломленої хвилі у середовищі з негативною груповою швидкістю)

Як водиться, роботи [5, 6] не стали унікальними у своєму роді. Висновки Г. Лемба і А. Шустера про те, що негативна групова швидкість можлива через аномальну дисперсію хвиль підтвердив в 1905 р. Фон Лауе (Max Theodor Felix von Laue, 1879 – 1960). В тому ж році Поклінгтон (H.C. Pocklington) в невеликій замітці ще раз показав, що в певному середовищі, де можлива зворотна хвиля, активізоване джерело коливань формує хвилю з груповою швидкістю, направленою від джерела, тоді як її фазова швидкість орієнтована йому назустріч.

В цілому ж, зважаючи на неочевидність практичного застосування зазначених ефектів, інтерес дослідників до них згас на кілька десятиріч, чітко визначивши рубіж між першим і другим етапами становлення теорії DNG.

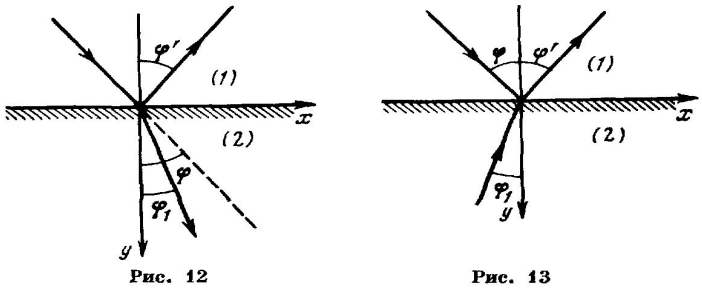



Рис. 12 Рис. 13

Рис. 3. Ілюстрації Л. Мандельштама з книги [7]: рис. 12 – заломлення променя у звичайному середовищі, рис. 13 – у середовищі, де групова швидкість хвиль негативна

З появою в 40-х роках НВЧ-пристроїв, що використовують зворотні хвилі, більшість з вже грунтовно забутих положень теорії зворотних хвиль знов з'явилася у полі зору фізиків. Формальним початком другого етапу становлення теорії DNG-середовищ можна вважати лекції з оптики Л.Мандельштама (1879–1944) [7], датовані 1944 р. В них, слідом за А. Шустером, був більш детально розглянутий ефект зворотного розповсюдження хвиль і незвичайний закон заломлення при падінні хвилі з вільного простору в середовище, де

групова і фазова швидкості хвиль направлені назустріч одна одній. При цьому заломлений промінь відхиляється у протилежну сторону від нормалі, ніж при падінні на звичайне середовище, в якому ці швидкості співпадають за напрямом (рис. 3).

Вивчення зворотних хвиль в 1940-і роки минулого століття сприяло не тільки освоєнню їх практичного використання у лампах і антенах зворотної хвилі, але і сплеску в 1950-і роки теоретичного інтересу до розповсюдження зворотних хвиль у лініях передачі. Прикладом тому є робота Г. Д. Малюжинця [8], опублікована в 1951 р. В статті [9] Сивухін Д.В. (1914 – 1986) першим відзначив, що фазова і групова швидкості хвилі будуть направлені протилежно в середовищі з одночасно негативними ε і μ, тобто, по суті, в середовищі DNG. У розвиток цієї ідеї в 1959 р. В.Е. Пафомов теоретично довів можливість виникнення зворотних хвиль в середовищі з одночасно негативними ε і μ. В тому ж в 1959 р. Р.А. Сілін знов звернувся до ілюстрації закону заломлення променя в середовищі з негативною дисперсією, розглядаючи кристали із зворотними хвилями.

Найбільш розвинену теорію речовин з негативним коефіцієнтом заломлення, що має одночасно негативні значення діелектричної і магнітної проникностей, запропонував в [10], як це визнано зарубіжними ученими радянський фізик Віктор Георгійович Веселаго (народився 13.06.1929 на Україні). У серії своїх публікацій в 1960-х роках, Веселаго В.Г. обґрунтував можливість існування фізичних середовищ з негативним коефіцієнтом заломлення, що мають властивості, парадоксальні з буденної точки зору. Основоположна його стаття [10] містила теоретичний опис властивостей середовища, в якому і ε, і μ були одночасно негативні, а також дослідження рішення рівнянь Максвела для цього випадку (в англійському перекладі тексту, опублікованому в 1968 р., помилково заявлено, що перші результати за цією темою були видані в 1964 р.). При інтерпретації рівнянь Максвела Веселаго вперше використовував як індекс заломлення n негативний квадратний корінь з добутку негативних величин εμ, що стало досить несподіваним логічним прийомом. Відзначаючи гіпотетичність відповідного середовища, Веселаго вказав на безперечний факт, що його існування не виключається рівняннями Максвела, і представив теоретичний аналіз процесу розповсюдження електромагнітних хвиль у подібних середовищах. З проведеного Веселаго аналізу виходило, що розповсюдження хвилі в середовищі з одночасно негативним ε, μ відрізняється від властивостей середовища з їх позитивними величинами.

Зокрема, в звичайних середовищах, коли $\varepsilon > 0$, $\mu > 0$, електромагнітна хвиля має правосторонню орієнтацію трійки векторів H, E, k, які характеризують магнітну, електричну компоненти поля і напрям хвильового вектора k. У разі DNG-середовищ через взаємно протилежну орієнтацію векторів фазової швидкості (хвильового вектора k) і вектора Умова-Пойтінга вектори E, H і k формують лівосторонню систему координат.

Негативна величина індексу заломлення змінює геометричну оптику лінз та інших об’єктів, утворених з DNG-матеріалів. Наприклад, фокусуюча лінза в цьому випадку стає розсіюючою, і навпаки, відхиляюча двоввігнута лінза, зроблена з DNG-середовища, діє як фокусуюча. Крім того, Веселаго першим довів, що звичайна плоскопаралельна пластина з $n=-1$ може виступати в ролі збираючої лінзи. В його роботі [10] передбачені такі електромагнітні ефекти, що відбуваються в DNG-матеріалах, як: реверсивні зміни допплерівського зсуву частоти і ефекту черенковської радіації, обернення світлового тиску на світлове тяжіння. Суттєво, що ці явища не були доказові і очевидні на момент розробки теорії Веселаго через брак фізичної реалізації відповідного метасередовища. На жаль, зусилля В.Г. Веселаго і його колег з отримання матеріалу з негативним заломленням на основі магнітного напівпровідника $CdCr_2Se_4$ виявилися марними через істотні технологічні труднощі, що супроводжували синтез даної речовини. Ця невдача, а також систематичний пресинг з боку директора Фізичного інституту ім. П.Н. Лебедєва Академії наук СРСР Д.В. Скобельціна, який звинувачував В.Г. Веселаго в заняттях псевдонаукою, надовго охолодили увагу дослідників до подібних проблем.

На рис. 4 стисло проілюстровано основні з розглянутих віх історії розвитку теорії DNG в рамках перших двох її етапів. Дана схема примітна тим, що під нею підписався і сам В.Г. Веселаго, тим самим виразивши свою згоду з публікаціями, які спростовували його пріоритет з низки ключових питань теорії DNG-середовищ.

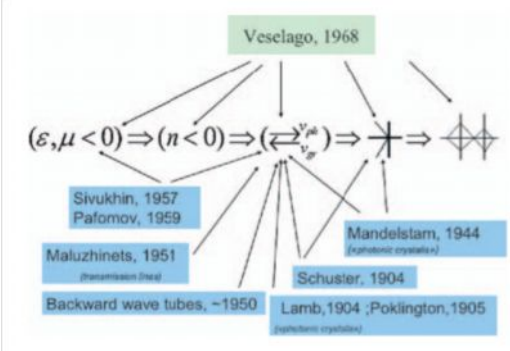



Рис. 4. Основні віхи перших двох етапів становлення теорії DNG

Проте, враховуючи значний внесок статті Веселаго [10] в теоретичне обґрунтування властивостей середовища з негативним заломленням, багато авторів іменують DNG-матеріали середовищем Веселаго (особливо у випадку ε=μ=–1 ), середовищем з негативною рефракцією або з негативним індексом заломлення (negative refractive index, NRI), а також „ліворукими” матеріалами (left-handed materials, LHM), зважаючи на відзначену в [10] лівобічну орієнтацію векторів електромагнітної хвилі.

Серед публікацій 1970-х років з теорії плоскопаралельних лінз, а також оптики DNG-середовищ необхідно відзначити роботи Р.А. Сіліна, в яких він описав оптичні властивості штучних діелектриків і дослідив особливості плоскопаралельної лінзи, виконаної з метаматеріала з негативним індексом заломлення.

Новим поштовхом до розвитку даного напряму і початком сучасного, третього етапу у формуванні теоретичних уявлень про DNG-середовища послужила публікація Джона Пендрі (Pendry) [11], в якій було запропоновано використовувати конкретні штучно створені матеріали особливої конструкції, які мають негативні ефективні значення діелектричної і магнітної проникностей. Пендрі запропонував масово використовувати структури з мініатюрних розрізних кільцевих рамок, виконуючих роль магнітних диполів, і прямолінійних відрізків дроту.

В основі цього підходу лежить той факт, що якщо дискретні розсіюючі елементи, складові середовища, мають розміри, менші, ніж довжина хвилі випромінювання, то даний композит, з погляду електродинаміки, можна розглядати як безперервний в обмеженій смузі частот.

Іншими словами, фізичне середовище буде безперервним в електромагнітному сенсі, якщо його властивості можуть бути описані усередненими параметрами, що змінюються у масштабі, набагато більшому, ніж розміри та інтервал утворюючих матеріал компонентів.

Дивно, що Пендрі був лише в одному кроці від лежачої на поверхні ідеї поєднання форм розглянутих їм різновидів елементарних антен (рис. 5), пізніше опублікованої Девідом Смітом разом з колегами з Каліфорнійського університету в Сан-Дієго і запатентованої патентом [12].

Саме таке очевидне поєднання структурних елементів, що виходило з публікації Пендрі, дозволило у 2000 р. дослідницькій групі Девіда Сміта створити перший матеріал, який мав у сантиметровому діапазоні електромагнітних хвиль (4,2 – 4,6 ГГц) негативний коефіцієнт заломлення.

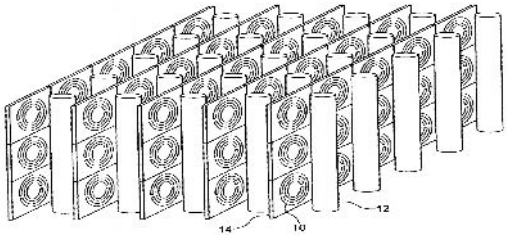



Рис. 5. Метаматеріал, запропонований в патенті [12], що вперше експериментально підтвердив ефект „ліворукості”

Цей штучний композитний матеріал складався з діелектричної основи, в якій розташовувалася множина мідних стрижнів і розрізних кілець, розташованих в строгому геометричному порядку. Стрижні, по суті, були антенами, що взаємодіяли з електричною компонентою електромагнітного поля, а розрізні кільця – антенами, реагуючими на магнітну складову. Основні розміри всіх елементів і відстань між ними були задані менше довжини хвилі, а вся система в цілому мала негативні ефективні значення ε і μ.

У роботі [13] був висловлений результат прямого виміру кута заломлення для призми, виготовленої з даного композиту. Експеримент, описаний в [13], переконливо показав що заломлення електромагнітної хвилі на межі вакууму і такого композитного середовища підкоряється закону Снелліуса з негативним значенням *n*. Тим самим можна вважати експериментально підтвердженими основні положення роботи [12]. Надалі ці експерименти були повторені незалежними групами дослідників з тим же позитивним результатом. Проте основними недоліками перших мета матеріалів, заснованих на використанні кільцевих і прямокутних SRR, є вузькосмуговість, високі рівні електромагнітних втрат, громіздкість і непрактичність для мікрохвильових технічних застосувань.

Для вирішення проблеми вузькосмуговості надалі було запропоновано багато варіантів магніточутливих елементів, що мають, зокрема форму грецької букви „омега”, спіралей. Суттєво, що проблема вузької смуги пропускання може до певної міри бути вирішена шляхом оптимізації геометричних розмірів SRR-резонаторів. Наприклад, для прямокутних SRR отримана ширина смуги пропускання 11,2 % у діапазоні частот 10,57 – 11,82 ГГц, що в 2,3 раз краще, ніж в первинному запропонованому варіанті. Для пошуку оптимальної комбінації геометричних параметрів використовувався вбудований в програмний пакет CST Microwave Studio (www.cst.com) НВЧ-оптимізатор.

Цілком очевидно, що надалі для оптимізації форми вказаних елементів доцільно використовувати генетичні алгоритми оптимізації, і відповідні роботи з’являться вже в найближчому майбутньому. Стосовно багаточастотних рішень є сенс використовувати замість розрізних кільцевих або квадратних рамок фрактальні рамки Серпінського, на основі ламаної Коха або інших фрактальних рішень. Аналогічні фрактальні конструкції слід задіяти і замість прямолінійних провідників.

Найбільш пристосованим для дослідження властивостей метаматеріалів із всіх пакетів моделювання антен на даний момент є пакет HFSS. З цієї причини моделювання електромагнітних властивостей нових метаматеріалів, використовуючих фрактальні елементи, доцільно проводити в програмній моделі HFSS.

Застосування DNG середовищ теоретично дозволяє підвищити роздільну здатність оптичних приладів, подолавши дифракційну межу. Використовуючи матеріали з $\varepsilon<0$ (і, по можливості $\mu<0$), можна за рахунок плазмонного резонансу підсилити ближні (неоднорідні) хвилі, відповідальні за перенесення інформації про деталі, розміром багато менше довжини хвилі. Ідеальним для цього є середовище Веселаго, що має $\varepsilon = \mu = -1$. Структури з одночасно негативними ε і μ мають цікаві, з погляду теорії, і корисні для практики властивості (розповсюдження зворотних електромагнітних хвиль, негативне заломлення, створення дійсного зображення плоскою пластинкою).

При розгляді ідеального метасередовища без втрат і частотної дисперсії мають місце істотне розширення смуги пропускання електрично малих антен (ЕМА) в порівнянні з межею Чу і більш низькі значення добротності, чим це слідує з його фундаментальної межі. Проте, перехід до реальних конструкцій метасередовищ з частотною дисперсійністю і втратами, приводить до катастрофічної деградації властивостей ідеальних антен з метаматеріалів. Тому основним завданням удосконалення метаструктур є синтез таких середовищ, які б мали мінімальні втрати і ледь помітні дисперсійні властивості.

На даному ж етапі основними напрямами застосування метаматеріалів в техніці антен є:

1) виготовлення підкладок в друкованих антенах для досягнення широкосмуговості і зменшення розмірів випромінювачів (MNG, DNG, CRLH);

2) компенсація реактивності ЕМА (ENG, DNG) в широкій смузі частот, у тому числі, перевищуючій фундаментальну межу Чу;

3) формування вузьких променів елементарними випромінювачами, зануреними в ENG або DNG середовища;

4) використання метаматеріалів для виготовлення антен поверхневої хвилі;

5) збільшення розв'язки між елементами антенних решіток, зокрема, MIMO-систем.

Розглянемо досягнуті при цьому результати докладніше, спираючись на характерні приклади конструктивного виконання відповідних метаантен.

**Метаматеріали в конструкціях друкованих антен**

Використання метаструктур як підкладки для друкованих мініатюризованих антен створює можливість подальшого скорочення розмірів випромінювачів, розширення їх смуги пропускання і підвищення ефективності випромінювання. Структура метаматеріалу, що утворює підкладку, може бути однорідною або композитною, утвореною з кількох типів середовищ. Так, у [14] описаний варіант використання однорідної MNG-підкладки, сформованої із занурених у діелектричну подушку розрізних квадратних рамок (рис. 6). Аналогічне рішення можливе і на основі DNG-середовища, в якому утворюючі елементи є осередками, приведеними на рис. 7.

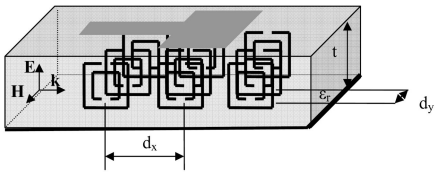



Рис. 6. Друкована антена з підкладкою з MNG [14]

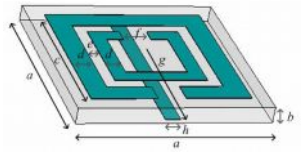


Рис. 7. Осередок DNG метаматеріалу

Серед композитних підкладок розповсюдження в антенах MIMO отримали структури, поєднуючі в собі правосторонні і лівосторонні сегменти. В числі привабливих властивостей таких гібридних рішень фахівці відзначають можливість реалізації в них частотно-регульованого коефіцієнта заломлення. Наприклад, в низькочастотному діапазоні композитний право-лівосторонній матеріал (CRLH Composite Right/Left-Handed) має негативний індекс заломлення, а при перевищенні деякої граничної частоти – позитивний. Підбором розмірів право- і лівосторонніх сегментів вдається регулювати резонансну частоту друкованої антени.

Одним з перших прикладів практичного використання метаматеріалів для серійного виготовлення друкованих антен є розробка фірмою Rayspan (http://www.rayspan.com) антенних решіток MIMO, використаних компанією Netgear в MIMO-маршрутизаторах WNR3500 і WNDR3300. Обидва маршрутизатори підтримують специфікації 802.11n Draft 2.0.

Деталі відповідних технічних рішень, що лягли в основу конструкції метаантен можна дізнатися з описів заявок фірми Rayspan на видачу американських патентів на винаходи [15], [16]. Суть їх полягає у використанні для виготовлення друкованої антени композитної структури CRLH на основі відрізка лінії передачі з негативним індексом заломлення, варіант якої приведений на рис. 8. Чисто зовні новий тип антен мало відрізняється від своїх друкованих прототипів, проте досягнуті результати розсіюють сумніви скептиків в перспективності подібних рішень. Зокрема на основі метаструктур вдалося помітно зменшити габарити випромінювачів антенних решіток MIMO, що дозволило понизити їх взаємний вплив. Електрична довжина печатної метаантени може бути зменшена до 0,1λ, що менше відомого обмеження в половину довжини хвилі. При цьому забезпечена робота в двох діапазонах частот (в районі 2,4 ГГц і 5,2 ГГц), а смуга пропускання антен збільшена на 15 %.

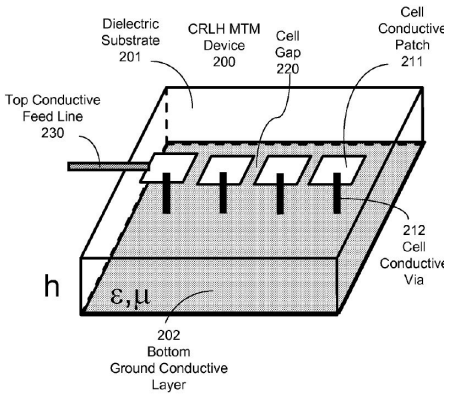



Рис. 8. CRLH –структура для антен MIMO

**Метаоболонки для ЕМА**

Згідно [17], основна ідея використання ENG-матеріалів в техніці електрично малих антен полягає в компенсації високої реактивної ємкості ЕМА-диполя індуктивністю оточуючої його ENG–оболонки. При цьому товщина метаоболонки може бути менше сотих часток довжини хвилі у вільному просторі, що не призводить до помітних загасань електромагнітного поля. Як приклад розглянемо описану в [17] ідею інтеграції ENG-обтікача з класичним монополем, розташованим над плоским екраном і підключеним до коаксіального фідера, причому сам монополь знаходиться усередині півсферичного ковпака з ENG-матеріалу (рис. 9).

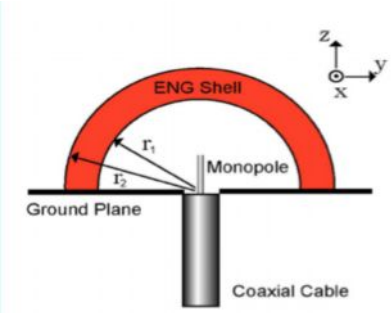



Рис. 9. Загальний вигляд конструкції ЕМА у складі монополя і ENG-оболонки [17]

Приведені в [17] результати моделювання свідчать, що у вказаній конструкції при резонансі відбувається збільшення випромінюваної монополем потужності, що становить у разі малих втрат 60 – 65 дБ порівняно з варіантом відсутності ENG-покриття. Сама по собі півсфера з ENG-матеріалу під впливом випромінювання монополя може розглядатися як електрично мала антена. Проте, цей елемент, через негативну діелектричну постійну діє як індуктивність, формуючи разом з ємнісним монополем LC-резонатор (рис. 10). Тому при фіксованій частоті резонансу із збільшенням модуля негативної діелектричної проникності ENG-середовища товщина оболонки повинна зменшуватися.

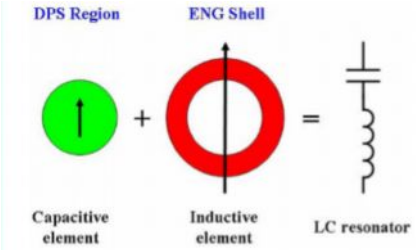


Рис. 10. Принцип компенсації реактивності ЕМА за допомогою метаоболонки [17].

Найважливішим висновком авторів [17] є твердження, що розглянута ЕМА, яка виконана з доступних метаматеріалів, має, тим не менш, виражені переваги над межею Чу. Зокрема, для використаних в розрахунках рівнів втрат і дисперсійності досягнута величина добротності Q в 1,583 рази перевищує межу Чу. Суттєво, що для ENG-матеріалу на резонансній частоті вдається добитися активного опору близько 50 Ом, майже нульової реактивності антени і ККД близько 98 – 99 %.

Аналогічна ідея може використовуватися і для випадку DNG-оболонок, які у порівнянні з ENG-покриттям дозволяють додатково зменшити розміри (товщину і радіус) оболонки. Пояснюється це тим, що використання середовища з $\mu<0$ еквівалентно внесенню ємності послідовно з ємністю диполя, що зменшує результуючу ємність ЕМА і вимагає меншої за величиною компенсуючої індуктивності.

Підтвердженням ефектів, описаних в [17], є експериментальні результати [18], отримані для електрично малого диполя, зануреного в плазмовий розряд у газі. В описаному експерименті плазма формувалася у вакуумній трубці з безперервним розрядом на постійному струмі. При цьому було зафіксовано більш, ніж 100-кратне підвищення напруженості електричного поля передаючої електрично малої антени ($l/\lambda << 10^{-3}$), зануреної в плазму, в порівнянні з таким же диполем, що знаходиться у вільному просторі. Дане явище легко може бути пояснено з урахуванням розглянутих електродинамічних властивостей вібратора в оболонці з ENG структури.

**Звуження діаграм випромінювання ЕМА**

До теперішнього часу отримано достатньо багато експериментальних підтверджень ефекту виникнення направлених властивостей випромінювання елементарного монополя, поміщеного в DNG-середовище. В роботі [19] описаний один з таких експериментів зі зняття діаграми спрямованості вібратора, розташованого усередині метаматеріала, утвореного з розрізних квадратних рамок (SRR) і друкованих провідників. Метаматеріал демонстрував в обмеженому просторовому секторі негативний коефіцієнт заломлення в діапазоні 10,3 – 10,8 ГГц. Загальний вигляд схеми відповідної експериментальної установки приведений
на рис. 11.

Метаматеріал (рис. 11) був сформований з двох типів друкованих плат квадратної форми (розміром 246×246 мм$^2$). На платах першого типу розташований масив з 48 паралельних провідників шириною 0,5 мм і завдовжки 238 мм, слідуючих з інтервалом 5 мм. Плати другого типу містили матрицю квадратних SRR-елементів (геометрія окремо взятого SRR приведена на рис. 12). На кожній такій платі розташовувалося 2304 (48×48) SRR з взаємною дистанцією 5 мм.

В збірному стеку метаструктури вказані плати розташовувалися почергово, паралельно одна одній, з взаємним інтервалом 2,5 мм. Загальна кількість плат з друкованими провідниками дорівнювала 49, а з квадратними рамками – 50. Чвертьхвильовий вібратор розміщувався паралельно друкованим провідникам усередині стека метасередовища над горизонтальним провідним екраном. Оцінка діаграм спрямованості проводилася шляхом обертання метаструктури навколо монополя.

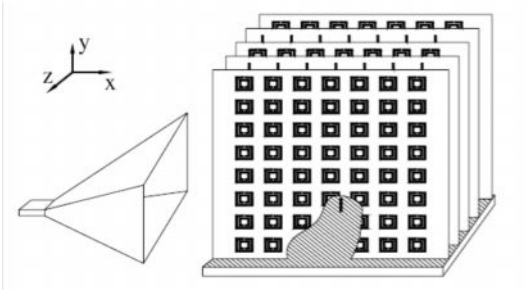



Рис. 11. Схема експерименту зі зняття діаграми спрямованості монополя, зануреного в DNG-середовище [19]

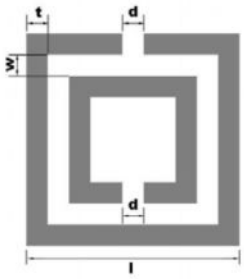



**Figure 1.** Single SRR with parameters $l = 3$ mm, $d = t = w = 0.3$ mm.

Рис. 12. Квадратний SRR, що використався для створення метасередовища [19], мав розміри l= 3 мм, d = t= w= 0,3 мм

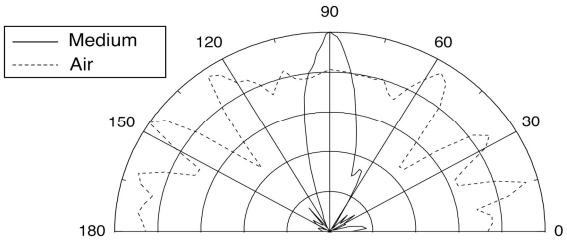



Рис. 13. Нормована діаграма спрямованості монополя в площині xz на частоті 10,6 ГГц [19]

Результати виміру діаграми спрямованості вібратора у площині, паралельній горизонтально розташованому екрану (x–z), приведені на рис. 13. Пунктирна лінія відповідає вільно розташованому у просторі вібратору а суцільна лінія – випадку занурення монополя в метасередовище.

Необхідно відзначити, що для всебічного вивчення ефекту звуження діаграм спрямованості вібратора в метасередовищі розглянутий в [19] експеримент слід було б доповнити оцінкою залежності ширини діаграми спрямованості монополя від габаритів метаоболонки. Це дозволило б отримати однозначну відповідь на припущення, що кутові розміри діаграми спрямованості вібратора, оточеного метасередовищем, визначаються площею його розгортки. Крім того, для подібних випромінюючих структур потребує додаткової перевірки виконання теореми взаємності передаючого і приймального режимів роботи. Оскільки розглянутий метаматеріал складений з гомогенних періодичних структур ряд дослідників висунули гіпотезу, що плоска хвиля в режимі прийому може бути направлена метаоболонкою під іншим кутом, ніж в режимі передачі. Приклад порушення теореми взаємності відносно обтічника антени, виготовленого з метаматериала, приведений в [20].

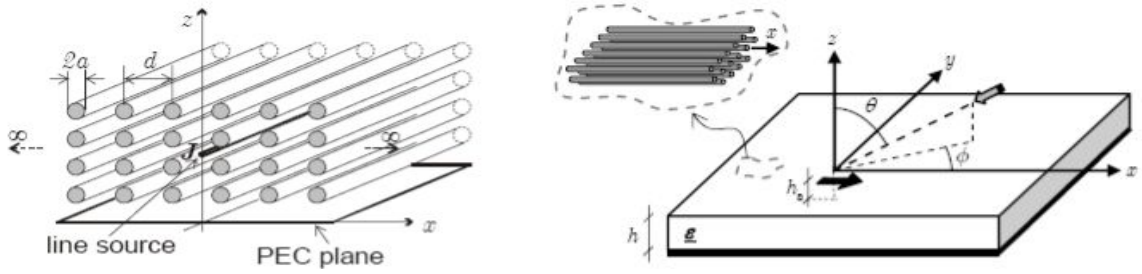


Рис. 14. Вібратор, вбудований в ENG-плиту [21]

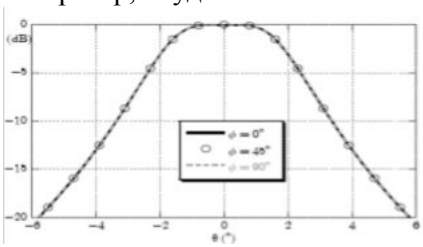


Рис. 15. Діаграма спрямованості вібратора у дротяній метаплиті [21]

Для звуження діаграми спрямованості елементарного випромінювача може застосовуватися також ENG-середовище. В [21] представлений огляд результатів дослідження особливостей діаграм випромінювання елементарного дротяного вібратора, вбудованого в метасередовище ENG-типу, яке утворене множиною паралельних провідників, розташованих над провідним екраном (рис. 14). Розрахунки поля в дальній області проводилися з допомогою методу моментів. Приклад різкого звуження діаграми спрямованості вібратора, зануреного в ENG-метасередовище, у разі його плазмової частоти 20 ГГц і частоти випромінювання 20,155 ГГц, приведений на рис. 15. Відповідне моделювання проводилося як для двовимірного, так і для тривимірного випадку. Висота метаструктури над екраном склала 60 мм, а джерело розташовувалося на відстані 30 мм від поверхні метапанелі.

На завершення слід зазначити, що аналіз відомих напрямів досліджень, що оформилися в даний час в теорії метаматеріалів, дозволяє спрогнозувати появу антенних конструкцій на основі активних і нелінійних метаструктур, теорію і технології яких ще належить розробити. Цілком імовірно, що в цей процес можуть бути залучені також хиральні метасередовища [22], матеріали з штучним магнітним і квадрупольним відгуком, метаматеріали з сильною просторовою дисперсією, за допомогою яких вже намагаються створювати оптичні прилади з розрізненням, перевищуючим дифракційну межу. Враховуючи успішний початок ери метаматеріалів в антенній техніці, що супроводжувався відкриттям цілої низки чудових ефектів, є підстави сподіватися, що розвиток цього технологічного напряму стане не менше вражаючим.

ЛІТЕРАТУРА

1. *Слюсар В. И.* Антенны PIFA для мобильных средств связи: многообразие конструкций. //Электроника: наука, технология, бизнес. – 2007. – № 1. – С. 64 – 74.

2. *Слюсар В. И.* Фрактальные антенны. Принципиально новый тип “ломаных” антенн. //Электроника: наука, технология, бизнес. – 2007. – №. 5. – С. 78 – 83; 2007. – №. 6. – С. 82 – 89.

3. *Слюсар В. И.* Синтез антенн на основе генетических алгоритмов. //Первая миля. Last mile (Приложение к журналу „Электроника: наука, технология, бизнес’). – 2008. – № 6. – С. 2 – 11.

4. *Rodger Walser.* Metamaterials: What are they and what are they good for? //2000 March Meeting of the American Physical Society. – March 20 – 24, 2000. – Minneapolis, Minnesota. – http://flux.aps.org/meetings/YR00/MAR00/abs/S9240.html.

5. *Horace Lamb*. On group velocity.//Proc. London Math. Soc. 1. – 1904. – Pp. 473–479, http://www.hep.princeton.edu/~mcdonald/examples/mechanics/lamb_plms_1_473_04.pdf.

6. *Arthur Schuster*. An Introduction to the Theory of Optics. – Edward Arnold, London. – 1904. – Pp. 313 – 318.

7. *Мандельштам Л.* Лекции по некоторым вопросам теории колебаний (1944 г.). Четвертая лекция. // В кн. Мандельштам Л. Лекции по оптике, теории относительности и квантовой механики. - М.: Наука, 1972. – С. 431 – 437.

8. *G. D. Malyuzhinets*. A note on the radiation principle.// Zhurnal Technicheskoi Fiziki, vol. 21, No. 8. - Pp. 940-942 (in Russian. English translation in Sov. Phys. Technical Physics), 1951.

9. *D.V. Sivukhin*, „The energy of electromagnetic waves in dispersive media," *Opt. Spektrosk.,* vol. 3, pp. 308-312, 1957.

10. *Веселаго В.Г.* Электродинамика веществ с одновременно отрицательными значениями ε и μ // Успехи физических наук. – 1967.– Т. 92. – № 7. – С. 517 – 526.

11. *J. B. Pendry, A. J. Holden*, D. J. Robbins, W. J. Stewart, Magnetism from conductors and enhanced nonlinear phenomena.// IEEE Trans. Microw. Theory Tech. – Vol. 47, No.11, 1999. – Pp. 2075 – 2084.

12. *Pat. USA* № 6791432B2. Int. $Cl^7$. H01P 7/08, H01Q 15/10. Left Handed Composite Media. //David Smith, Sheldon Schultz, Norman Kroll, Richard A. Shelby. – Filed Mar. 16, 2001. – Date of Patent: Sep. 14, 2004.

13. *R. A. Shelby, D. R. Smith*, S. Schultz. Experimental Verification of a Negative Index of Refraction. //Science. – 6 April 2001. – Vol. 292. – No. 5514, pp. 77 – 79. – http://people.ee.duke.edu/~drsmith/pubs_smith_group/Shelby_Science_(2001).pdf.

14. *A. Semichaevsky* and A. Akyurtlu. Homogenization of Metamaterial-Loaded Substrates and Superstrates for Antennas/ Progress In Electromagnetics Research, PIER 71, 129 – 147, 2007. – http://ceta.mit.edu/PIER/pier71/08.07021001.S.Akyurtlu.pdf.

15. *US Patent Application* Publ. No. 2008/0258993 Al. Int. Cl. H01Q 3/24, H01Q 1/38. Metamaterial Antenna Arrays with Radiation Pattern Shaping and Beam Switching.// Ajay Gummalla, Marin Stoytchev, Maha Achour, Gregory Poilasne. – Filed: Mar. 17, 2008. – Pub. Date: Oct. 23, 2008.

16. *US Patent* Application Publ. No. 2008/0048917 Al. Int. Cl H01Q 1/38, H01Q 9/04. Antennas Based on Metamaterial Structures.// Maha Achour, Ajay Gummalla, Marin Stoytchev. – Filed: Aug. 24, 2007. – Pub. Date: Feb. 28, 2008.

17. *Richard W. Ziolkowski,* and Aycan Erentok. Metamaterial-Based Efficient Electrically Small Antennas. IEEE Transactions on Antennas and Propagation, Vol. 54, No. 7, July 2006. – Pp. 2113 – 2130.

18. *Пахотин В.А.* Излучение электрически короткой антенны из ограниченного объема газоразрядной плазмы.// Письма в ЖТФ. – 2007, Том 33. – Вып. 8. – С. 22 – 29.

19. *Q. Sui , C. Li, L. L. Li*, and F. Li. Experimental Study of $\lambda/4$ Monopole Antennas in a Left-Handed Meta-Material.// Progress In Electromagnetics Research, PIER. – 2005. – No. 51. – Pp. 281–293. - http://ceta.mit.edu/PIER/pier51/16.0401122.Sui.LL.pdf.

20. *H. Cory, Y.J. Lee,* Y. Hao and C.G. Parini. Use of conjugate dielectric and metamaterial slabs as radomes. // IET Microw. Antennas Propag., Vol. 1, No. 1, February 2007. – Pp. 137 – 143.

21. *P. Burghignoli,* G. Lovat, F. Capolino, D. R. Jackson, and D. R. Wilton. Radiation from Elementary Sources in the Presence of Wire-Medium Slabs: Physical Mechanisms And Full-Wave Analysis. – http://www.elettromagnetismo.it/atti_rinem/2006S05A01.pdf.

22. *Lindell I.V.,* Sihvola A.H., Tretyakov S.A., Viitanen A.J. Electromagnetic waves in Chiral and Bi-Isotropic Media. – London: Artech House, 1994.

к.т.н. Ананьїн О.В.(НДІ ДПСУ)

# КОМПЕНСАЦІЯ ВПЛИВУ ЗАВАД В КАНАЛІ РАДІОУПРАВЛІННЯ СИСТЕМИ РАДІОЗВ'ЯЗКУ

В практиці застосування засобів радіозв'язку на якість прийому-передачі радіосигналів впливають різноманітні види завад. Це явище є суттєвою перешкодою для надійного передавання сигналів по каналах радіозв'язку. Актуальність проблеми обумовлена тим, що прийом-передача радіосигналів будь-якої потужності завжди відбувається під впливом зовнішніх та внутрішніх збуджуючих діянь (завад).

Одним із видів підвищення якості прийому-передачі сигналів по каналах радіозв'язку, з погляду теорії автоматичного управління, є забезпечення стійкого каналу радіоуправління (у вигляді одиничного зворотного зв'язку) [1]. Але у середовищі розповсюдження радіохвиль каналу радіоуправління теж діють завади. Це не тільки погіршує якість прийому-передачі сигналів в системі радіозв'язку, але, й може призвести до повного руйнування її роботи. Тому вплив завад у каналі радіоуправління необхідно знизити до мінімального рівня.

Метою даної статті було дослідження впливу завад на канал радіоуправління та запропоновано оптимальну модель цього каналу. Дослідження здійснено методом математичного моделювання в інтерактивній системі MATLAB [2]. Внаслідок цього отримано модель системи радіозв'язку з адаптивним каналом радіоуправління та компенсацією впливу завад на якість радіоприйому [3]. За критерії якості функціонування даного варіанта радіосистеми з каналом радіоуправління прийнято швидкодія та точність. Під швидкодією розуміється мінімальний час реакції системи на вплив зовнішніх збуджуючих діянь (завад), а під точністю – похибка розузгодження між сигналом, що потрапляє на радіоприймальний пристрій та опорним сигналом у пристрої порівняння, що знаходиться в радіоприймачі. При проведенні дослідження визначено що, навіть, при наявності незначних завад у середовищі розповсюдження радіохвиль каналу радіоуправління система практично непрацездатна (хоча і не втрачає стійкості) через значне погіршення якості прийнятого сигналу.

Пропонується такий ефективний захід, який дозволяє мінімально знизити вплив завад у каналі радіоуправління – це застосування блоку компенсації. Практично блок компенсації являє собою вимірювальний радіоприймач, що ідентифікує (вимірює) завади (збуджуючи діяння) в середовищі розповсюдження радіохвиль каналу радіоуправління. За умови протилежності величин сигналів в каналі радіоуправління та з виходу блока компенсації дотримується умова інваріантності динаміки системи завад у каналі радіоуправління.

Дослідження системи радіозв'язку з блоком компенсації завад (збуджуючих діянь) у середовищі розповсюдження радіохвиль каналу радіоуправління методом математичного моделювання показує, що блок компенсації забезпечує досить високу якість функціонування радіосистеми, яка характеризується похибками неузгодженості в перехідних і сталих режимах роботи. В даній радіосистемі з високою точністю відпрацьовується заданий рівень опорної напруги, якою оператор задає необхідну якість приймального радіосигналу на вході радіоприймача. Тому можна зробити висновок, що побудова каналів радіоуправління з блоком компенсації завад в системах радіозв'язку на базі розглянутої математичної моделі є доцільним та перспективним завданням.

ЛІТЕРАТУРА

1. *Дорф Р., Бишоп Р.* Современные системы управления. Перевод с английского – М.: Лаборатория базовых знаний. 2002 – 832 с.

2. *Дьяконов В., Круглов В.* Математические пакеты расширения MATLAB. Специальный справочник – СПб.: Питер. 2001 – 480 с.

3. *Кондрашов В.Е., Королёв С.Б.* MATLAB как система программирования научно-технических расчётов – М.: Мир. 2002 – 359 с.

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

# ХАРАКТЕРИСТИКИ НАДІЙНОСТІ ЕЛЕМЕНТІВ І МЕРЕЖ У СИСТЕМАХ ЗВ’ЯЗКУ

Сучасні телекомунікаційні мережі містять десятки мільйонів мережних і сотні мільйонів термінальних вузлів. При вирішенні завдань обміну даними, розподіленого керування, контролю параметрів і стану технічних й інших систем використовуються мережні технології. За цієї причини проблема надійності мереж стає усе більше актуальною. Перш ніж ставити питання про надійність мережі, визначаються деякі базові поняття. Надійність будь-якої системи визначається надійністю її елементів. Надійність елементів задається часом наробітку до відмови або ймовірністю відмови за обговорений період часу. Надійності різних елементів можуть мати значні розбіжності. У результаті, як усереднені значення надійності, так і розподіли ймовірності відмов різних мережних пристроїв можуть варіюватися у дуже широких межах. У багатьох випадках надійність і розподіли надійності визначаються емпірично. Необхідно наповнити зміст поняття надійності системи особливостями технологічної побудови системи зв’язку. Якщо вимога надійності визначити як працездатність всіх елементів, надійність мережі виявиться рівною нулю – завжди знайдеться несправний або відключений мережний або термінальний вузол. Якщо ж визначити надійність системи, як можливість комунікації між $N$ довільно обраних вузлів, то надійність мережі виявиться практично рівною одиниці. При цьому зовсім неясно, як вирішити проблему вибору цих вузлів. Якщо вузол, що представляє інтерес, не попадає в число обраних, рішення взагалі не має сенсу. Отже, обидва визначення неприйнятні. Насамперед, необхідно дати визначення відмови в мережі. Сучасна мережа – це складна система, що містить безліч зовнішніх пристроїв, ліній зв’язку, спеціалізовані процесори, запам’ятовувальні пристрої, програмне забезпечення тощо. Є велика кількість допоміжного устаткування, наприклад, джерела живлення й забезпечення життєдіяльності мережі. Тоді відмовою мережі необхідно вважати як локальні відмови мережного устаткування або обрив лінії передачі, так і вихід з ладу джерела живлення, зависання операційної системи, помилку в прикладній програмі або випадкове відключення джерела живлення. Однозначної відповіді на це питання немає, все залежить від умов функціонування мережі і тих завдань, які перед нею ставляться. Можна розділити відмови на катастрофічні та параметричні. Катастрофічні виникають у результаті миттєвої зміни одного або декількох компонентів, з яких побудована мережа (наприклад, обрив кабелю). Параметричні – наслідок зміни параметрів компонентів мережі із часом доти, поки значення одного з них не вийде за межі, що визначають нормальне функціонування. Вихід з ладу термінального вузла створює проблеми для користувача, інші абоненти мережі можуть цього й не помітити. Відмова магістрального маршрутизатора або транзитного вузла може вплинути на роботу цілого регіону. Звідси видно, що окремі вузли можуть по-різному впливати на роботу мережі в цілому**.** Крім того, вплив на надійність мережі може робити не тільки устаткування або операційна система, але й прикладні програми. На цьому список факторів, що впливають на надійність, не вичерпується. Якщо користувач не може одержати доступ до певного мережного ресурсу, це дуже часто пов’язано не з відмовою устаткування або програми, а просто з перевантаженням однієї з ділянок мережі на шляху до зазначеного ресурсу. Тут мається на увазі не тільки обмеження пропускної здатності, але й можливе збільшення затримки доставки, що досить критично у випадку, наприклад, IP-телефонії або відео-конференцій. Таким чином, параметри надійності часто залежать від вектора завантажень. Формулюючи завдання оцінки надійності, потрібно визначити, які з параметрів важливі: зв’язність, пропускна здатність, мінімізація затримок або інші, наприклад, пов’язані з вимогами замовника послуг. Після визначення необхідних параметрів і характеру обмежень на мережні ресурси можна отримати вирішення завдань керування надійністю сегментів мережі, порівняно слабко пов’язаних з іншими сегментами, тобто тих, що мають високий ступінь автономності.

Ахтанін О.Г. (ВІТІ ТУУ„КПІ”)
Тарасюк Ю.М. (ВІТІ ТУУ„КПІ”)

# ОБРОБКА СИГНАЛІВ ЗЕМНИХ СТАНЦІЙ НА БОРТУ СУПУТНИКА РЕТРАНСЛЯТОРА З ЦИФРОВОЮ АНТЕННОЮ РЕШІТКОЮ

Під час роботи через системи супутникового зв’язку кількох кореспондентів одночасно, на цифровій антенній решітки 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 цифрової антенної решітки 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, 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. 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.

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 цифрової антенної решітки знаходяться кілька кореспондентів, зазначені процедури надрозрізнення більш ефективні за умов достатнього відношення сигнал/шум.

ЛІТЕРАТУРА

1. *Варакин Л. Е.* Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.

2. *Помехоустойчивость* и эффективность систем передачи информации / Под ред. А. Г. Зюко. – М.: Радио и связь, 1985. – 272 с.

3. *Борисов В. И.* и др. Помехозащищенность систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000 – 384с.

4. *Джон Прокис*. Цифровая связь. Пер. с англ./Под.ред. Д.Д.Кловского. – М.: Радио и связь. 2000. – 800с.

к.т.н. Башкиров О.М.(ЦНДІ ОВТ ЗСУ)

# ПІДВИЩЕННЯ ПРОПУСКНОЇ СПРОМОЖНОСТІ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ ПРО ПОВІТРЯНУ ОБСТАНОВКУ

Розглядається процес обміну інформацією між пунктами обробки в інформаційній підсистемі, що здійснює обробку найбільш часто змінюваних даних: про радіолокаційну або повітряну обстановку. Ці дані передаються у виді кодограм, що мають фіксовану довжину. Існує кілька десятків типів стандартних кодограм. В складі кожної кодограми є службові, інформаційні та „порожні” розряди, які не використовуються або не містять ніякої інформації. Наявність порожніх розрядів пояснюється тим, що дані, які передаються в кодограмах, потребують для передачі різного числа розрядів, а довжина всіх кодограм фіксована, тому зайві розряди заповнюються „безінформаційними” даними. У будь-яких кодограмах стандартної довжини частина кодограми, яка не використовується взагалі та є „порожньою”, складає не менше 10%, а в деяких випадках пустує близько 60% переданих повідомлень. Темп видачі повідомлень різного типу неоднаковий і може змінюватися залежно від обстановки. Наприклад, перевірочні кодограми про стан каналу передаються з темпом дві кодограми за 10 с в кожний канал, повідомлення про радіолокаційну обстановку – з темпом одне у 10 с про кожний повітряний об’єкт, разові кодограми про ступінь бойової готовності або про бойові можливості бригад (полків) – у міру їхньої зміни.

Отже, завантаження каналу зв’язку визначається наявністю порожніх розрядів у переданих кодограмах різного типу й залежать від темпу їхньої видачі. З урахуванням темпу надходження кодограм різного типу математичне сподівання числа порожніх розрядів дорівнює близько 35%. Для визначення початку повідомлення в стандартних кодограмах використовується ознака початку повідомлення, що передує появі даних, які містять „корисну” інформацію. Внаслідок того, що довжина кодограм стандартна, ознака кінця повідомлення кодограми може бути відсутньою.

До особливостей „стандартних” кодограм про повітряну обстановку відносяться такі:

1. Наявність „порожніх” розрядів у повідомленні, які збільшують довжину повідомлення, а отже, час передачі кодограми та завантаження каналу передачі даних.
2. Наявність у повідомленні вторинної (дублюючої) інформації, що може бути отримана шляхом обробки первинної інформації безпосередньо на пункті обробки, що приймає повідомлення (наприклад, курс, швидкість руху і прискорення цілі і т.д.).
3. Наявність у повідомленні „повторних” даних – вже відомої одержувачеві інформації (наприклад, значення висоти польоту повітряного об’єкта, що не змінилося, і т.п.).

Всі перелічені вище особливості негативно впливають на ефективність системи передачі даних повітряного командування: збільшуючи надлишковість повідомлень, вони не збільшують кількості інформації, яка міститься в них, що призводить до зайвого завантаження каналів передачі даних.

Для зменшення завантаження каналів передачі даних у радіолокаційній системі пропонуються три способи.

Реалізація нового алгоритму вимушує розділити всі дані на дві категорії. До першої варто віднести дані, які необхідно видавати постійно, а до другої – дані, передача яких потрібна тільки після їхнього оновлення. Наприклад, дані про координати повітряної цілі змінюються дуже часто, дані про параметри руху цілі (швидкість, курс, прискорення) змінюються порівняно рідко, а дані про ознаку державної належності, номери цілі, типи цілі змінюються дуже рідко або ж взагалі не міняються протягом усього польоту.

Новий спосіб передачі даних дозволяє збільшити пропускну спроможність системи передачі даних про повітряну обстановку на 30-40 %.

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

# ВПРОВАДЖЕННЯ ПОСЛУГ *Triple Play* НА ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Об’єднання послуг Інтернет – телебачення, *IP* – телефонії та передачі даних реалізує концепцію мереж *NGN (Next Generation Networks)*, в яких технологія *Triple Play* здійснює впровдження 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*).

З активним розвитком нових послуг на мережі ВАТ „Укртелеком” почали великими темпами збільшуватись об’єми *IP* – трафіка, що призвело до необхідності значного розширення можливостей магістральної мережі. І щоб забезпечити відповідну гарантовану швидкість і надійність передачі голосу, даних і відео в межах всієї країни, в Укртелекомі було прийняте рішення побудувати другу чергу національної оптичної магістралі. При цьому було вирішено зробити ставку не на розвиток існуючої *SDH*– мережі *(Synchronous Digital Hierarchy – синхронна цифрова ієрархія)*, а на інвестування в передову технологію *DWDM (Dense Wave Division Multiplexing* – технологія ущільненого хвильового мультиплексування*)*, яка забезпечить високу пропускну здатність, гнучкість і надійність для розвитку нових мультимедійних послуг.

В основу проекту нової магістральної оптичної мережі закладені три основні задачі:

– побудувати високошвидкісну, надійну і легко масштабовану телекомунікаційну транспортну *DWDM* – мережу по всій Україні;

– нова транспортна мережа повинна забезпечувати надання абонентам сучасних мультимедійних послуг *Triple Play* (передача голосу, відео і даних);

– послуги, які будуть надаватись абонентам повинні бути високої якості в незалежності від географічного розташування абонента на території України.

Друга черга магістральної мережі ВАТ „Укртелеком” побудована на базі обладнання *Cisco*. В проекті використані новітні розробки, які забезпечують транспорт до 32 – х оптичних трактів по одній парі оптичних волокон з пропускною здатністю 10 Гбіт/с. Загальна ємність магістральної мережі може бути збільшена до 320 Гбіт/с в одній оптично волоконній парі без переривання надання послуг. Нова мережа об’єднала 52 вузла по всій країні. Топологія мережі складається з восьми оптичних сегментів, які об’єднують обласні центри України і АР Крим. Магістральна мережа побудована з використанням технології *ROADM (Recofigurable Optical Add-Drop Multiplexer* – реконфігуровані модульні мультиплексори виводу – вводу*)*, яка переналаштовує оптичні мультиплексори виводу/вводу, які не тільки мінімізують номенклатуру компонентів, які використовуються в мережі, але і ефективні в налаштуванні та експлуатації і дозволяють легко добавляти нові оптичні тракти без зупинки мережі. Використана в проекті мультисервісна транспортна платформа *Cisco ONS 15454 MSTP* має високу масштабованість і можливість гнучкої підтримки в любій точці міської і регіональної мережі послуг любого типу: традиційна телефонна мережа загального користування – ТмЗК, передача голосу, даних, відео, зберігання даних тощо. Ця платформа може налаштовуватись на підтримку мереж *DWDM* з різними топологіями: крапка – крапка, кільце, багато кілець. Вона включає переналаштовані мультиплексори оптичного виводу/вводу (*ROADM*), які дозволяють термінувати, пропускати, передавати та приймати різні потоки *DWDM* на різних довжинах хвиль (як в діапазоні *C*, так і в діапазоні *L*).

На сьогоднішній день компанія „Укретелеком” один із небагатьох телекомунікаційних операторів, яка має велику аудиторію потенційних користувачів послуг *Triple Play* на всій території країни, так як вже сьогодні абонентська база споживачів широкосмугового доступу в Інтернет складає понад 651 тисячу абонентів. На початок 2009 року послуга *Triple Play*

знаходилась в тестовому режимі, однак перші результати перебільшили очікування, і вже зараз компанія „Укртелеком” готова до комерційного запуску цих сервісів.

Берестов Д.С. (НАОУ)

# ВИЗНАЧЕННЯ ТА ФОРМУВАННЯ ПРОФІЛІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Інформаційні ресурси держави чи суспільства в цілому, а також окремих організацій та фізичних осіб являють собою певну цінність, мають відповідне матеріальне вираження і вимагають захисту від різних впливів, що приводять до зниження цінності інформаційних ресурсів. Базовою основою для захисту цих інформаційних ресурсів служить система нормативних документів [1–4], одним з основних понять яких е функціональний профіль захищеності автоматизованої системи.

Функціональний профіль захищеності – це мінімально необхідний перелік послуг, що може забезпечити система захисту інформації (СЗІ), щоб задовольнити певним вимогам до необхідного рівня захищеності інформації. На даний час у нормативних документах по захисту інформації визначено 90 профілів до яких перераховані вимоги до механізмів і засобів захисту, що необхідні для їх реалізації [4].

При розробці автоматизованих систем (АС) одною із проблем є вибір найбільш придатного для них профілю. оскільки в нормативних документах по цьому питанню даються лише загальні міркування [3]. Вибір необхідного профілю для АС є складною задачею тому, що наявність такої кількості профілів має на увазі й істотне розходження в захищаемих АС. Для полегшення процесу установлення відповідності вимог до СЗІ з характеристиками АС уводиться класифікація АС [3].

Хоча класифікація АС і полегшує процес вибору придатного профілю, усе-таки цей процес поки залишається дуже складнім, потребує високої кваліфікації і точності. Також в процесі формування нового профілю виникає ряд труднощів, пов’язаних з постановкою задачі забезпечення захисту і завданням вимог до системи захисту інформації , а також обґрунтованим вибором той чи іншої послуги та визначенням глибини її деталізації.

Список профілів, представлений у [3], визначено експертним шляхом розробниками документів [1-4]. Однак зовсім ясно, що може існувати деяка формальна (можливо, не взаємно однозначна) відповідність між характеристиками АС і відповідним їй профілем, що могло б бути теоретичним обґрунтуванням існування зазначеного довідника.

Але для практичної реалізації зазначеного у [3] списку профілів необхідний розвиток розглянутої в [5] формалізації та подальші дослідження з метою розробки можливої низки профілів захищеності інформації з урахуванням властивостей певного переліку послуг та характеристик захищаємих АС.

ЛІТЕРАТУРА

1. *Загальні положення* щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-99, ДСТСЗІ СБ України, Київ, 1999.

2. *Термінологія в* галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-003-99, ДСТСЗІ СБ України, Київ, 1999.

3. *Критерії оцінки* захищеності інформації в комп’ютерних системах від несанкціонованого доступу. – НД ТЗІ 2.5-004-99, ДСТСЗІ СБ України, Київ, 1999.

4. *Класифікація автоматизованих* систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – НД ТЗІ 2.5. – 005 – 99, ДСТСЗІ СБ України, Київ, 1999.

5. *Антонюк А.О., Берестов Д.С., Пустовіт С.М.* Методика формалізованого визначення профілю захищеності інформації в автоматизованих системах // Науково-технічний журнал „Захист інформації”. – 2004. – №3(20). – КМУЦА. – С.20 – 24.

Бичков А.М. (ВІТІ НТУУ „КПІ”)
к.т.н. Нестеренко М.М. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ ТА МЕТОДІВ ПРОТИДІЇ ПРИ ВИКОРИСТАННІ СКЛАДНИХ ЗАПИТІВ У СУБД

Сьогодні бази даних виступають основною складовою практично будь-яких додатків, які дають можливість надання різноманітного динамічного вмісту даних. Оскільки в таких базах даних може зберігатися дуже важлива і конфіденційна (комерційна) інформація, треба приділяти багато уваги захисту цієї інформації.

Бази даних стосовно управління розділяють на централізовані та розподілені. У централізованих базах даних простіше вирішуються проблеми захисту інформації від навмисних загроз, підтримання актуальності й несуперечливості даних. Перевагою розподілених баз даних, за умови дублювання даних, є їх висока захищеність від стихійних лих, аварій, збоїв технічних засобів та людських факторів.

При побудові захисту баз даних необхідно враховувати ряд специфічних загроз безпеки інформації, пов’язаних з концентрацією в базах даних великої кількості різноманітної інформації, а також з можливістю використання складних запитів обробки даних. До таких загроз можна віднести:

1) інференцію;
2) агрегування;
3) комбінацію дозволених запитів для отримання закритих даних.

Розкривши їхню суть, визначимо наступні методи протидії таким загрозам:

1) блокування відповіді при неправильному числі запитів;
2) перекручення відповіді шляхом округлення та іншої навмисної корекції даних;
3) поділ баз даних на групи;
4) випадковий вибір запису для обробки;
5) контекстно-орієнтований захист;
6) контроль надходження запитів.

Провівши аналіз методів протидії загроз, дійшли до висновку, що найбільш ефективними є останні два методи:

– контекстно-орієнтований захист полягає в призначенні атрибутів доступу (читання, вставка, видалення, відновлення, управління і т. д.) елементів бази даних (записам, полям, групам полів) в залежності від попередніх запитів користувача, що не дозволяє зловмисникові простежити безліч запитів;

– контроль надходження запитів передбачає контроль наявності „підозрілих” запитів або комбінації запитів. Аналіз подібних спроб дозволяє виявити можливі канали отримання несанкціонованого доступу до закритих даних.

Потрібно зауважити, що для повного рішення проблеми захисту даних, адміністратор безпеки повинен мати можливість проводити моніторинг дій користувачів. Тому для підвищення ефективності його роботи є доцільним розробка програмних продуктів аналізу інформаційних загроз у розподілених базах даних, за допомогою якого буде проводитися відстеження та аналіз різних аспектів несанкціонованого доступу або використання подібних комерційних програмних додатків.

ЛІТЕРАТУРА

1. *Сабанов А.* Безопасность баз данных. Connect! Мир Связи. Бизнес-практикум. Апрель 2006 г.

2. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. Наука и Техника, Санкт-Петербург. – 2004. – 384 с.

3. *Смирнов С.Н.* Безопасность систем баз даннях. Учебное пособие. – Гелиос АРВ, – 2007. – 352 с.

к.т.н. Бовда Е.М. (ВІТІ НТУУ „КПІ”)

# ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В АСУ

Складність сучасного військового управління, різке зростання його ролі в результатах збройного протиборства обумовлює підвищення уваги до автоматизації управління військами (силами) та інтелектуальної підтримки роботи комплексів засобів автоматизації (КЗА).

Сучасні автоматизовані системи повинні включати наступні підсистеми:

1) підсистему розвідки (наземну, морську, повітряну, космічну компоненти);

2) пункти управління;

3) підсистему зв’язку;

4) підсистему навігації.

Такі системи дозволять отримувати різнорідну інформацію про обстановку і використовувати її для якісного планування бойових дій та управління військами (силами).

Розробка, удосконалення АСУ Збройних Сил України спрямована на підвищення ефективності управління військами (силами) та відноситься до розряду складних проблем. Одним із основних напрямків її рішення є впровадження в систему управління ЗСУ новітніх інформаційних технологій, що орієнтовані на безпосередню участь посадових осіб органів управління (ОУ) в процесі оброблення інформації. Це дасть змогу максимально приблизити посадових осіб ОУ до інформаційних ресурсів, а також до самого процесу розв’язування інформаційно-управлінських задач.

Застосування новітніх інформаційних технологій забезпечить наступні можливості в організації процесу управління в ЗСУ:

1. Інтелектуальну підтримку діяльності посадових осіб органів управління. Дані технології можуть забезпечити:

а) автоматизацію процесів обробки документальної інформації, що характерно для діяльності ОУ;

б) автоматизацію обробки графічної, аудіо і відеоінформації;

в) виявлення можливих варіантів взаємодії об’єктів і на основі цього здійснення діяльності по організації розпізнавання й аналізу ситуацій, що складуються;

г) прогнозування процесів розвитку ситуацій;

д) генерацію раціональних варіантів рішень на основі бази знань.

2. Роботу посадових осіб у режимі маніпулювання даними та знаннями.

3. Наскрізну інформаційно-інтелектуальну підтримку процесу вироблення рішення на всіх етапах управління від постановки задачі до прийняття рішення.

4. Впровадження та активне застосування „Електронного документообігу” в ОУ, що значно прискорить всі процеси управління.

5. Інтерактивний режим рішення задач управління з можливістю для посадових осіб впливати на цей процес та здійснення перетворення змісту інформації в разі потреби.

6. Інтерпретація інформації (у тому числі неповної і суперечливої інформації) завдяки використанню бази знань.

7. Візуалізація (девізуалізація) інформації, що представляється посадовій особі органу управління, при різних формах і способах її перетворення, що значно покращує сприйняття ситуацій.

8. Інформаційний супровід процесу вирішення задач.

9. Геоінформаційне забезпечення процесів управління з елементами моделювання.

10. Комплексний захист всіх рівнів управління завдяки створенню системи захисту.

11. Взаємодія як по вертикалі так по горизонталі з усіма АСУ видів та родів військ.

Впровадження новітніх інформаційних технологій обумовлює перехід від централізованої до децентралізованої обробки даних (на вищих ланках управління можливо

використання комбінованої (розподіленої) обробки даних), в якій вирішальна роль належить ПЕОМ (на основі ПЕОМ створюються АРМ посадових осіб ОУ). Відповідно змінюється технологія роботи посадової особи, де вона інтегруючись у людино-машинний комплекс виступає вже оператором, але продовжує виконувати функції прийняття рішень. З іншого боку, АРМ оператора виконує функції розв'язування певного класу задач. Все це разом змінює методи професійної діяльності посадових осіб, психологічні аспекти його роботи, а в майбутньому може сприяти створенню умов для зміни структури ОУ та переходу до іншого принципу управління.

На ПЕОМ можливо використання великої кількості програм, що дасть змогу задовольнити різноманітні потреби посадових осіб щодо обробки текстової інформації, роботи з базами даних і базами знань (БД, БЗн), виконання розрахунків (ІРС), роботи в локальній мережі ПЕОМ, організація відеоконференцій тощо.

Все це разом з урахуванням професійних знань і практичних навичок посадової особи надасть змогу вибрати методику розв'язування задачі, маніпулювати даними для розрахунків, проаналізувати одержані на ПЕОМ результати розрахунків і прийняти найраціональніше в даній ситуації рішення.

Створення локальних мереж ПЕОМ, в яких ефективно поєднуються можливості ПЕОМ для персональної обробки даних з перевагами розподіленої обробки даних, що забезпечують колективне використання загальних інформаційних ресурсів надає певні переваги для управління військами (силами).

Незважаючи на постійні зміни в засобах і способах боротьби, бойові дії носять і будуть носити загальновійськовий характер, про що свідчить досвід локальних війн і військових конфліктів. У зв'язку з цим автоматизація повинна розвиватися на загальновійськовій основі. Саме загальновійськові АСУ можуть об'єднати окремі видові (родові) угрупування військ (сил) в єдину систему. Складовими частинами („вертикальними стволами") загальновійськової АСУ повинні стати підсистеми управління силами авіації, ППО, ВМС, РЕБ, розвідки, а також технічним, тиловим забезпеченням та інші. Деякі з них будуть мати вертикальні зв'язки до стратегічного рівня.

Основними тенденціями розвитку АСУ будуть:

1. створення інтегрованого банку даних ЗСУ, як сукупності технічних і програмних засобів та інтегрованих у єдиний інформаційний простір баз даних, призначених для інформаційно-аналітичної та програмно-технічної підтримки функціонування єдиної системи інформаційно-аналітичного забезпечення діяльності керівного складу ЗС України;
2. розробка комплексу аналітичної обробки інформації та підтримки прийняття рішень;
3. формування бази знань, як сукупності програмних засобів, що забезпечують пошук, зберігання, перетворення та запис у пам'ять ЕОМ складно структурованих інформаційних одиниць (знань);
4. розробка, впровадження та подальший розвиток загального та спеціального програмно-математичного забезпечення інформаційно-аналітичної діяльності ЗС України;
5. створення комплексної системи захисту інформації;
6. подальше удосконалення інформаційно-телекомунікаційної мережі ЗС України;
7. удосконалення нормативно-правової бази створення і функціонування системи інформаційно-аналітичного забезпечення ЗС України;
8. впровадження системи підготовки кадрів та удосконалення структури інформаційно-аналітичних підрозділів ЗС України;
9. організація взаємодії з АСУ інших структур державних органів управління.

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

# ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ ІНФРАСТРУКТУРИ КЕРУВАННЯ КЛЮЧАМИ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Бурхливий розвиток новітніх інформаційних технологій та інтенсивне впровадження інформаційно-телекомунікаційних систем (ІТС) різко активізували проблему забезпечення їх інформаційної безпеки, цілісності і конфіденційності повідомлень, які передаються. Практичне вирішення цієї проблеми базується на застосуванні криптографічних засобів захисту, що використовують спеціальні (ключові) дані. Крім вибору належної для ІТС криптографічної системи (криптографічного алгоритму), одночасно постає задача надійного керування ключовою інформацією.

Керування ключами – інформаційний процес, що включає генерацію ключів, їх зберігання і розподіл.

В симетричній криптосистемі відправник і одержувач використовують один і той же секретний ключ. Процес розподілу і доставки секретних ключів для учасників інформаційного обміну в симетричних криптосистемах має достатньо складний характер. Асиметрична криптосистема передбачає використання двох ключів – відкритого і секретного. Оскільки з відкритого ключа практично неможливо отримати секретний, відкритий ключ можна поширювати вільно всім учасникам інформаційного обміну, забезпечивши його цілісність та справжність. Таким чином, вирішуються дві головні проблеми симетричної криптографії – через розповсюдження усього *SN* ключів і відкритість каналу їх поширення. З найбільш розповсюджених асиметричних алгоритмів найбільшу складність криптоаналізу можна забезпечити при використанні перетворень в групі точок еліптичних кривих.

Захищений обмін повідомленнями, надійна їх ідентифікація, цілісність і конфіденційність базуються на створенні в ІТС спеціальної інфраструктури керування ключами – набором служб безпеки, центрів сертифікації й інших реєстраційних центрів, що виконують вищеназвані функції щодо виготовлення, видачі, відновлення, скасування і поширення ключів.

Розподіл ключів – самий відповідальний процес в керуванні ключами. До нього пред’являються наступні дві вимоги:

1) оперативність і точність розподілу ключів;

2) прихованість розподілу ключів.

Розподіл ключів між учасниками інформаційного обміну в ІТС може реалізовуватися наступними способами:

1) створенням одного (головного) або декількох центрів розподілу ключів (головного і підпорядкованих);

2) прямим обміном ключами між абонентами ІТС.

В обох випадках повинна бути гарантована дійсність сеансу зв’язку, яку можна забезпечити використовуючи механізм запиту – відповіді або механізм відмітки часу (рис. 1).

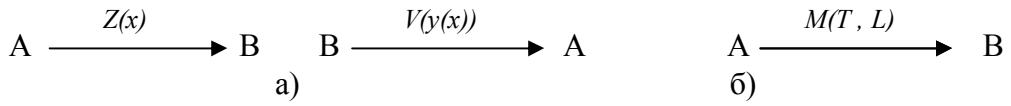



Рис. 1. Варіанти встановлення дійсності сеансу зв’язку:
а) через механізм „запит – відповідь”; б) через механізм відмітки часу

У випадку реалізації механізму „запит – відповідь” абонент А відправляє абоненту В повідомлення *Z(x)*, в яке включений випадковий елемент *x*. Отримавши запит, абонент В

перетворює випадковий елемент $x$ на новий елемент з відомою функцією $y(x)$, включає його в повідомлення $V$, яке відправляє абоненту А. Після отримання відповіді $V(y(x))$ абонент А може бути впевненим в тому, що сеанс є дійсним. В іншому випадку абонент А відправляє абоненту В повідомлення $M(T, L)$, в яке включається час відправки повідомлення $T$ (відмітка часу) і допустимий інтервал затримки $L$ (термін дії повідомлення).

При розподілі секретних ключів з участю центра розподілу ключів (ЦРК), як правило, здійснюється попередня його взаємодія з учасниками інформаційного обміну ІТС через спеціально організовані служби. При цьому відповідальність за підтвердження дійсності учасників обміну і розподілені ключі несе ЦРК і відповідні служби.

В окремих випадках, наприклад, для роботи в мережі TCP/IP розподіл секретних ключів за участю ЦРК може здійснюватись відповідно до встановлених протоколів автентифікації і розподілу ключів, основаних на застосуванні відомих алгоритмів симетричної криптографії. При цьому учасники інформаційного обміну повинні мати відповідні унікальні ідентифікатори.

Для реалізації процесу управління ключовою інформацією на ЦРК ІТС може застосовуватись окрема програма або програмно-апаратна система, що запускається безпосередньо перед передачею документів.

В якості прикладу реалізації інфраструктури відкритих ключів можна привести вітчизняний комплекс програмних засобів „Тайфун-РКІq, що орієнтований на ГОСТ 28147-89, ГОСТ 34.310 та ДСТУ 4145. Комплекс забезпечує генерацію і розподіл необхідних ключових компонентів для всіх абонентів, а також виконання відповідних криптографічних перетворень – шифрування, автентифікацію і цифровий підпис електронних документів. До складу комплексу входять програмні засоби автоматизованих робочих місць (АРМ) головного і регіонального центрів сертифікації ключів, програмні засоби АРМ центра реєстрації та програмні засоби генерації ключів і обслуговування сертифікатів користувачів. Програмні засоби комплекса функціонують на IBM-сумісних комп’ютерах в операційних системах Windows 2000/XP/2003/Vista.

Іншим способом розподілу ключів є прямий, тобто без ЦРК, обмін сеансовими ключами між користувачами мережі. Для його реалізації можливі два шляхи:

1) використання криптосистеми з відкритим ключем для шифрування і передачі секретного ключа симетричної криптосистеми;

2) використання системи відкритого розподілу ключів, зокрема Діффі – Хелмана.

Схема передачі зашифрованого на ключі $Ks$ повідомлення $M$ від сторони А на сторону В з використанням відкритого і секретного ключів має наступний вид:

1. А: $Ks$, $E_{KS}(M)$, $EK_B(Ks)$.
2. А → В: $E_{KS}(M)$, $EK_B(Ks)$.
3. В: $DK_B(EK_S) = Ks$, $DK_S(Ks(M)) = M$.

Даний спосіб допускає можливість використання процедури автентифікації за допомогою алгоритму ЕЦП.

Інший напрям – прямого обміну відкритими ключами дозволяє використовувати незахищені канали зв’язку.

Генерація і розподіл ключів для асиметричних криптосистем з відкритими ключами є більш складнішими, оскільки ці ключі повинні бути великими простими числами (більше 256 біт) і сформовані в спеціальному Центрі сертифікації відкритих ключів, функції якого може виконувати ЦРК. В той же час, багаточисельні дослідження показали, що криптосистеми на основі еліптичних кривих переважають інші системи з відкритим ключем за двома важливими параметрами: ступенем захищеності в розрахунку на кожний біт ключа і швидкодією в разі програмної і апаратної реалізації. Так, у вітчизняному стандарті ДСТУ 4145 використовуються ключі, що мають максимальну довжину 431 біт, а в стандарті ГОСТ 34.310 – 1024 біта.

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

# МЕТОДИКА ВИБОРУ РАЦІОНАЛЬНОГО ВАРІАНТА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ ЕКСПЕРТНИХ ДАНИХ

На сучасному етапі розвитку інформаційних технологій, коли постійно розширюються можливості іноземної розвідки і отримує все більше значення фактор раптовості, підвищені вимоги пред’являються до систем захисту інформації (СЗІ), які повинні забезпечити надійне збереження в таємниці від зловмисника змісту інформації, що обробляється, її цілісність, доступність та оперативність. В умовах, коли до СЗІ пред’являється багато різних, інколи протилежних вимог, вибір найкращих варіантів для реалізації є складною задачею. Виходячи з цього, актуальною представляється задача розробки інженерних методів вибору найкращого варіанта СЗІ з урахуванням не одного, а 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.

Аналіз літератури показує, що всі численні методи рішення багатокритеріальних задач можна звести до трьох груп методів:

– метод головного показника;

– метод результуючого показника;

– лексикографічні методи (методи послідовних поступок).

Метод головного показника заснований на переводі всіх показників якості, окрім якого-небудь одного, що називається головним, в розряд обмежень типу рівностей і нерівностей. Надамо головному показнику номер $q_1(S)$. Тоді задача зводиться до однокритеріальної задачі вибору системи $S \in M_s$, що володіє найкращим значенням показника $q_1(S)$ за наявності відповідних обмежень.

Метод результуючого показника якості заснований на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу часткових показників якості $q_1,...,q_m$ на результуючу якість виконання системою її функцій. Оцінки такого впливу даються групою фахівців – експертів, що мають досвід розробки подібних систем.

Найбільше застосування серед результуючих показників якості отримали адитивний, мультиплікативний і мінімаксний показники.

Адитивний показник якості є сумою зважених нормованих часткових показників, в той час як мультиплікативний утворюється шляхом перемножування часткових показників з урахуванням їх вагових коефіцієнтів. У ряді випадків вид результуючої цільової функції достатньо важко обгрунтувати або застосувати. В подібних випадках можливим простим шляхом рішення задачі є застосування максимінного показника. Максимінний показник забезпечує найкраще (найбільше) значення найгіршого (найменшого) з часткових показників якості.

Суть лексикографічного методу полягає у впорядкуванні всіх показників по важливості, наприклад $q_1(S) > q_2(S) > ... > q_m(S)$ і виділенні множини альтернатив з

найкращою оцінкою за найважливішим показником. Якщо така альтернатива єдина, то вона вважається найкращою; якщо їх декілька, то з їх підмножини виділяються ті, які мають кращу оцінку по іншому показнику і т.д.

Принциповою особливістю задачі вибору раціонального варіанта СЗІ є переважно якісний характер показників, що трактуються як вимоги, які задаються до СЗІ. У зв'язку з цим методи багатокритеріальної оптимізації повинні формулюватися в нечіткій постановці, коли показники якості розглядаються як функції приналежності заданому рівню якості СЗІ.

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 за важливістю | лексикографічний метод |
| визначені вагові коефіцієнти показників | адитивний показник |
| | мультиплікативний показник |
| | максимінний показник |

Використовуючи рекомендації по вибору методу рішення, надалі можуть бути розглянуті наступні рішення задачі багатокритеріальної оптимізації СЗІ в нечіткій постановці: а) при рівній важливості вимог; б) при різній важливості вимог; в) по адитивному критерію; г)лексикографічним методом.

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 варіанта $a^*$ з множини варіантів побудови СЗІ $A = \{a_1, a_2, ..., a_m\}$, що має найбільше значення функції приналежності $\mu_D(a^*) = \max\limits_{j=\overline{1,m}} \mu_D(a_j)$.

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 $R_i = \sum\limits_{j=1}^{n} W_j \cdot R_{ij}$ ($R_{ij}; i = \overline{1,m}; j = \overline{1,n}$ – 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 $У$ : $\mu_z(z) = \sup\limits_{z=x \cdot y} \min(\mu_x(x), \mu_\gamma(y))$.

Значення відповідної функції приналежності інтерпретується як характеристика ступеня того, наскільки варіант $a_i$ є кращим.

На завершення слід відмітити, що при виборі раціонального варіантf 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.

к.т.н. Богучарский В.В. (ЦНДІ ОВТ ЗСУ)
Дідок Л.А. (ЦНДІ ОВТ ЗСУ)

# РОЗВИТОК СИСТЕМИ ЗВ'ЯЗКУ ТА ПЕРЕДАЧІ ДАНИХ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Система зв'язку та передачі даних в ЗС України становить сукупність організаційно-технічних комплексів засобів зв'язку та автоматизації органів і пунктів управління, об'єднаних інформаційно-телекомунікаційною мережею, а також органів автоматизації та інформатизації, призначених для забезпечення інформаційно-телекомунікаційних функцій управління мережею та роботи пунктів управління в автоматизованому і неавтоматизованому режимах з наданням доступу до необхідних сервисів (послуг). Система повинна включати до себе такі основні компоненти:

– цифрові мережі та лінії прямого зв'язку, основу яких повинні складати цифрові засоби зв'язку;

– цифрові мережі зв'язку колективного користування, основу яких повинні складати універсальні вузли зв'язку загального користування з цифровими засобами радіодоступу, каналоутворення і комутації;

– стаціонарні військові лінії зв'язку;

– орендовані мережі зв'язку загального користування.

Така система зв'язку та передачі даних забезпечить: використання взаємосумісних протоколів, інтерфейсів; прийом, ретрансляцію, розподіл потоків інформації, що циркулюватимуть в створюваній Єдиній автоматизованій системі управління Збройних Сил України та управління ними;скритність та стійкість управління військами (силами) у будь-яких умовах оперативної обстановки завдяки використанню сучасних телекомунікаційних засобів; застосування готових комерційних стандартів і апаратно-програмних засобів.

Використання сучасних технологій надасть змогу інтегровано використовувати універсальні мережі зв'язку й інформаційно-телекомунікаційні мережі. Перспективна система зв'язку та передачі даних, яка буде складатись з ліній прямого зв'язку і мережі зв'язку загального користування, дозволить забезпечити:

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 узагальнення ресурсу універсальної мережі зв'язку (УМЗ).

3. Покращання характеристик електромагнітної сумісності на вузлах зв'язку пунктів управління і підвищення розвідзахищеності системи внаслідок 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 вузлах зв'язку.

5. Забезпечення мобільності та живучості УМЗ за рахунок зв'язності ІТВЗ радіорелейними лініями зв'язку.

6. Інтеграцію функцій комутації та каналоутворення для абонентських різношвидкісних потоків. З метою створення єдиної інформаційно-технічної системи зв'язку, збору, обробки і розподілу інформації, для забезпечення управління Збройними Силами, для підвищення його стійкості та оперативності, забезпечення прийняття та доведення рішень посадовими особами органів та пунктів управління в реальному масштабі часу, необхідно вибрати найбільш раціональний варіант рішення щодо складу та структури технічних засобів.

Богуш К.Ю. (ІСЗЗІ НТУУ „КПІ”)

# НОРМУВАННЯ ФОРМИ СИГНАЛУ ДЛЯ РОЗПІЗНАВАННЯ МОВИ В ІНТЕЛЕКТУАЛЬНИХ СИСТЕМАХ

Розпізнавання мови є важливим елементом розвитку інтелектуальних систем. Для мов слов’янської групи задача розпізнавання злитого мовлення ще не вирішена. Також, перенесення систем машинного розпізнавання, що добре зарекомендували себе на Заході, на слов’янські мови сполучений зі значними труднощами, і такі системи не можуть бути застосовані для розпізнавання російської чи української мов. Одним із завдань, що виникає при розпізнаванні мови – це розпізнавання не тільки від різних джерел, але й для різних каналів передачі з різною швидкістю передавання.

Пояснюється це тим, що однакові звуки від одного джерела дещо відрізняються за формою (статистичний розкид), крім того форма сигналу того самого звуку від одного джерела змінюється зі зміною швидкості передачі мови. У цей час є різні стандарти передачі мови (1,2 кбіт/с, 2,4 кбіт/с, 4,8 кбіт/с, 8 кбіт/с, 16 кбіт/с, 32 кбіт/с, 64 кбіт/с тощо). Тоді, природно, виникає завдання побудови нормуючої функції за допомогою якої можна було б виконувати автоматичне розпізнавання мовних сигналів від різних джерел і для різних швидкостей передачі. З цією метою в роботі пропонується побудова таблиці (матриці) для автоматичного розпізнавання мови, що відбивала б зазначені аргументи (обставини).

Після побудови матриці, пропонований у роботі алгоритм на основі перебору й порівняння зі зразком дозволить виконувати автоматичне розпізнавання в реальному часі (динамічний алгоритм). Таким чином, для побудови елементів матриці аналізуються форми сигналів (звуків, складів, звукосполучень і слів) від різних джерел мовного сигналу й на різних швидкостях. Як приклад, на рис. 1 приводяться форми звукових сигналів голосних і приголосних звуків чоловічих і жіночих голосів, а також вимовлених папугою, які записані із різними швидкостями (1200 біт/с (вокодерне перетворення), 128 кбіт/с (ІКМ), 353 кбіт/с (ІКМ)), для яких будується статистична функція як елемент таблиці 1. Інструментом для дослідження форми сигналу є система математичного моделювання MATLAB, за допомогою якої виконується спектральний аналіз і вейвлет-перетворення.

Приклад матриці для визначення нормуючої функції

*Таблиця 1*

| Джерело\частота дискретизації, кГц, швидкість сигналу, кбіт/с | 2,4 кбіт/с | 8 кГц, 128 кбіт/с | 22 кГц, 353 кбіт/с |
|---|---|---|---|
| папуга | $f(\alpha_{11})$ | $f(\alpha_{12})$ | $f(\alpha_{13})$ |
| чоловік | $f(\alpha_{21})$ | $f(\alpha_{22})$ | $f(\alpha_{23})$ |
| жінка | $f(\alpha_{31})$ | $f(\alpha_{32})$ | $f(\alpha_{33})$ |

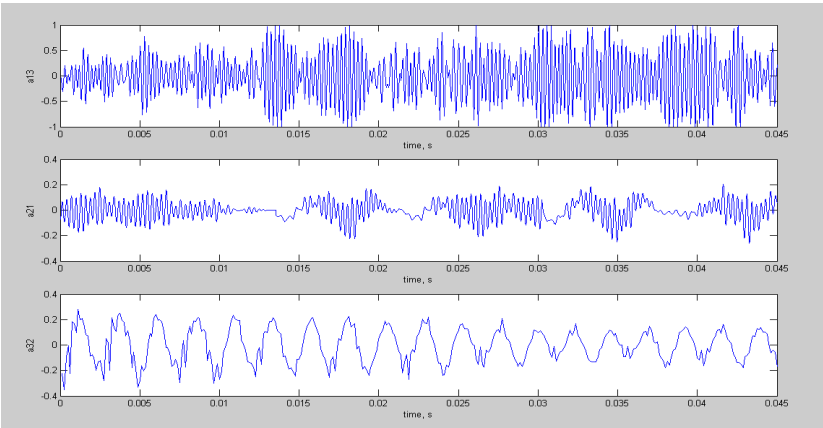



Рис. 1. Ділянки сигналів, що відповідають звуку „і” зі швидкостями передачі та від джерел звуку, що відповідають табл. 1

Божко В.І. (ВІТІ НТУУ „КПІ”)

# МЕТОДОЛОГІЯ АРХІТЕКТУРНОЇ РЕАЛІЗАЦІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КРИТИЧНОГО ЗАСТОСУВАННЯ В СИСТЕМАХ ЩО ІНТЕНСИВНО ЙОГО ВИКОРИСТОВУЮТЬ

Архітектура програмного забезпечення (ПЗ) систем що інтенсивно використовують програмне забезпечення (Software Intensive Systems, SIS) та працюють в областях критичного застосування (КЗ) повинна задовольняти суворим вимогам з функціональної безпеки (ФБ) цільової метасистеми. До числа SIS, наприклад, відносяться різнорідні автоматизовані системи керування, вбудовані бортові транспортні системи, телекомунікаційні й корпоративні системи, у тому числі й на базі web-сервісів.

Архітектура ПЗ сучасних SIS є компонентною і розподіленою, її розробка як правило носить концептуальний характер (часто з використанням UML)[1]. Пропонується ряд мов опису (Architecture Description Languages, ADL) і методів проектування архітектури ПЗ (DoDAF, TOGAF, FEAF, ATAM, CBAM, QAW, ARID, ADD). Детальний аналіз ADL, таких як ACME, Aesop, C2 SADL, Rapide і причин їхнього важкого впровадження в практику реалізації в ПЗ SIS КЗ представлений в [2]. Відмічається, що ФБ архітектури ПЗ включає як безпеку центрального ядра системи, так і інших взаємозалежних компонентів, що уможливлює поширення збою в критичному компоненті архітектури по ланцюзі компонентів, однак, це явище не повинне призводити до порушення вимог з функціональної безпеки до SIS КЗ в цілому.

При аналізі методів підвищення безпеки ПЗ SIS варто враховувати розходження в підходах для апаратного й програмного забезпечення. Необхідний рівень ФБ ПЗ не можна забезпечити аналогічно дублюванню найбільш критичних по безпеці архітектурних апаратних компонентів, оскільки дублювання програмних компонентів приведе також і до дублювання помилок. В роботі [3] систематизовані методи, що використовують мультиверсійність і формальний підхід. Результати досліджень демонструють, що використання мультиверсійності й формальних методів на самих ранніх етапах розробки істотно зменшує ймовірність помилок у програмних компонентах, однак їхнє застосування зв’язане зі значними матеріальними витратами.

Актуальним науковим завданням є розробка елементів методології підтримки архітектурних рішень програмного забезпечення SIS що забезпечить прийнятний рівень витрат на забезпечення необхідного рівня функціональної безпеки SIS КЗ.

Для вирішення поставленого завдання пропонується ітераційна процедура декомпозиції проекту програмної підсистеми на архітектурні елементи з урахуванням ризиків реалізації механізмів міжпроцесної взаємодії, що дозволяє виділити критичні компоненти архітектури, які є кандидатами на розробку формальними методами й (або) з реалізацією мультиверсійності. Оцінку прийнятих архітектурних рішень пропонується проводити із застосуванням методології системотехніки за комплексним критерієм цілісності обраного варіанта архітектури ПЗ.

ЛІТЕРАТУРА

1. *Bass B., Clements P., Kazman R.* Software Architecture in Practice, 2nd Edition. – Boston:Addison-Wesley, 2003, – 560 с.

2. *Wood E.* The Past, Present and Future of Software Architecture. – Режим доступа: http://www.eoinwoods.info/index.php?page=articles.

3. *Скляр В.В.* Оценка качества и экспертиза программного обеспечения. Лекционный материал / Под ред. Харченко В.С. – Харков: Национальный аэрокосмический университет им. Жуковского Н.Е. „ХАИ”, 2008. – 204 с.

к.т.н. Борисов І. В.(ВІТІ НТУУ „КПІ”)
Макарчук О. М. (ВІТІ НТУУ „КПІ”)

# ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ В КАНАЛАХ З НАВМИСНИМИ ЗАВАДАМИ

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; уніфікація й стандартизація засобів і комплексів зв’язку; освоєння нових діапазонів частот.

Для вирішення проблеми сумісності засобів радіозв’язку різних стандартів і діапазонів у теперішній час для тактичної ланки управління Збройних Сил провідних країн світу розробляється технологія програмованих радіостанцій (*software defined radio*, *SDR*). Програмована радіостанція використовує стандартні апаратні засоби для виконання функцій обробки цифрових сигналів за допомогою програмного забезпечення.

У процесі функціонування засобів радіозв’язку військового призначення на них впливають різні фактори, що порушують їх нормальну роботу. Системи радіозв’язку є першочерговим об’єктом радіоелектронної боротьби. Постійне вдосконалення засобів радіорозвідки та радіозавад, впровадження автоматизованих комплексів радіоелектронного подавлення призвело за останні роки до істотного підвищення можливостей по радіоподавленню засобів радіозв’язку. Враховуючи це, стає досить складним завдання забезпечення стійкого радіозв’язку в умовах радіоелектронного подавлення. Успішне її вирішення неможливо без застосування спеціальних технічних і організаційних заходів по забезпеченню завадозахищеності систем радіозв’язку.

Аналіз існуючих методів забезпечення завадозахищеності засобів радіозв’язку показав, що перспективним напрямком вирішення цього завдання є застосування адаптивних сигнально-кодових конструкцій на основі турбо-кодів. Це завдання не є вирішеним при низьких відношеннях сигнал-завада в каналі зв’язку.

Під адаптивними сигнально-кодових конструкцій розуміється динамічна зміна схем модуляції та кодування при передачі наступних блоків інформації з метою адаптації частотної ефективності засобів радіозв’язку до стану каналу. Рішення про вибір адекватних сигнально-кодових конструкцій приймається на приймальному боці відповідно до оцінки стану каналу з передачею інформації за допомогою зворотного зв’язку на сторону передавача.

Розрахунки та результати імітаційного моделювання показують, що використання адаптивних сигнально-кодових конструкцій з *M*-позиційними сигналами та турбокодами в каналах з навмисними завадами дозволяє отримати енергетичний виграш в завадозахищеності до 6 дБ у порівнянні з відомими методами.

ЛІТЕРАТУРА

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

2. *Волков Л. Н., Немировский М. С., Шинаков Ю. С.*Системы цифровой радиосвязи: базовые методы и характеристики. Учебное пособие. – М: Эко-Трендз, 2005. – 392 с.

3. *Системы* подвижной радиосвязи: [пер. с польск. Рудинского И. Д.; под ред. Ледовского А. И.]. – М: Горячая линия –Телеком, 2006. – 536 с.

4. *Банкет В. Л., Ищенко Н. А.* Пространственно-временное кодирование – эффективный метод помехоустойчивой передачи цифровой информации в системах мобильной связи. Эль-Дакдуки А. С. – Зв’язок, 2004. – № 8. – С. 40 – 43.

Бугера М.Г. (ВІТІ НТУУ „КПІ”)
Сілко О.В. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ЗАБЕЗПЕЧЕННЯ АВТЕНТИЧНОСТІ НАВЧАЛЬНОЇ ЗВІТНОСТІ В ОБ’ЄКТНО-ОРІЄНТОВАНОМУ НАВЧАЛЬНОМУ СЕРЕДОВИЩІ

Для забезпечення автентичності результатів виконання тестового контролю в об’єктно-орієнтованому середовищі пропонується застосувати методику, яка полягає у створенні спеціальної відмітки в файлі звітності, яку неможливо імітувати власноруч. Такий підхід має виключити можливість видачі чужих результатів тестування за свої та модифікацію їх на сервері навчального закладу. Методика передбачає виконання наступних етапів:

1. Вибір та структуризація вихідної інформації для створення спеціальної відмітки у файлі звітності з проходження тестового контролю.
2. Застосування алгоритму двоключового шифрування до файла звітності тестового контролю.
3. Перевірка автентичності звітності з тестового контролю на сервері навчального закладу.

*Перший етап* методики передбачає:

– вибір правил генерації і розповсюдження з серверу навчального закладу ідентифікаторів студентів $e_i$ та $d_i$, які утворюють пару, і виступають відповідно відкритим та закритим ключами системи шифрування;

– вибір правил генерації і розповсюдження з серверу навчального закладу ідентифікаторів наборів завдань тестового контролю $w_j$ та $v_j$, які виступають відповідно відкритими ключами для системи шифрування;

– вибір правил генерації результатів тестового контролю та формування файла звітності.

Перед початком тестування студент отримує від сервера навчального закладу відкритий ключ $e$ та розпочинає проходження тестового контролю. Після завершення проходження тестового завдання, система за внутрішніми механізмами виставляє оцінку у вигляді масиву байт *M*, який разом з ідентифікатором тесту *w* передається до підсистеми захисту.

Сутність *другого етапу* методики вимагає застосування підсистеми захисту, яка здійснює:

– шифрування масиву *M* двоключовим алгоритмом: на першій ітерації алгоритму ключем виступає ідентифікатор тестового завдання $w$, на другій – ідентифікатор студента $e$ за яким обчислюється закритий ключ шифрування $d$:

$$M \rightarrow E_w, m_i \; m = m' \quad ,$$
$$M' \rightarrow E_d, m_i \; m' = m'' \; , \qquad (1)$$

де $E$ – функція шифрування.

– відправку зашифрованого файла звітності з результатами тестового контролю на сервер навчального закладу.

*Третій етап* методики передбачає:

– перевірку автентичності на сервері навчального закладу.

На сервері навчального закладу зберігаються відкриті ключі $e_i$ та $v_j$, які дозволяють провести встановлення автентичності отриманого файла звітності тестового контролю під час його отримання, збереження у базі даних та генерації звітних відомостей.

Для апробації програмної реалізації 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”, створити інтерфейс для отримання результатів *M* від модуля тестового контролю та передачі їх на сервер.

Бурба О.І. (в/ч А1906)
Жилінський І.В. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ФОРМУВАННЯ ОБРИСУ АВТОМАТИЗОВАНИХ СИСТЕМ НА СТАДІЇ РОЗРОБКИ КОНЦЕПЦІЇ

Створення автоматизованих систем (АС) представляє собою сукупність впорядкованих в часі взаємопов’язаних, об’єднаних в стадії та етапи робіт, виконання яких є необхідним і достатнім для її створення у відповідності з заданими вимогами. Ці стадії та етапи в сукупності складають життєвий цикл АС. В життєвому циклі будь-якої АС найбільш важливою передпроектною стадією є розробка концепції, результати якої є інформаційною основою для розробки технічного завдання (ТЗ) на створення системи. Конкретним втіленням концептуальних ідей щодо створення АС є її обрис, який є основою для формування вимог до створюваної системи. Під обрисом АС слід розуміти множину вузлів та автоматизованих робочих місць, множину функціональних підсистем і функцій АС, засоби їхньої реалізації. Тому від обгрунтованості цих результатів у вирішальній мірі залежить якість та обгрунтованість положень ТЗ як головного документу на створення АС.

Практика створення АС показує високу ціну помилкових проектних рішень на цій стадії проектування через їхню низьку наукову обгрунтованість. В ході проведення робіт на подальших стадіях створення АС виникає необхідність зміни положень ТЗ, збільшення об’ємів фінансування та строків виконання робіт.

Характерними особливостями стадії розробки концепції є неповнота інформації, наявність кількох варіантів створення системи і необхідність вибору одного з них, неможливість експериментальної перевірки пропонуємих рішень і точного прогнозування їх наслідків.

У роботах, які присвячені проектуванню АС, досить детально дослідженні питання на стадії технічного проектування, коли розробник володіє достатньо повною інформацією про створювану систему. В цей же час питання, які вирішуються на етапах концептуально проектування, висвітлені в загальному, що не дає можливості застосовувати їх у якості методичного апарату і переводить процес прийняття рішень у площину застосування досвіду та інтуїції розробника, що може негативно відобразитися на науковій обгрунтованості положень ТЗ. Тому актуальним науково-практичним завданням є розробка методичного апарату формування обрису АС.

В доповіді розглянута методика формування обрису АС на стадії розробки концепції, що дозволить підвищити наукову обгрунтованість відповідних проектних рішень та врахувати особливості ранніх стадій проектування.

В теперішній час для формування обрису АС широко застосовується агрегативно-декомпозиційний підхід, який покладено в основу цієї методики. Він полягає у послідовній декомпозиції цілей системи, її завдань та функцій з подальшим агрегуванням елементів для генерації варіантів побудови системи в цілому на відповідному рівні деталізації.

Застосування цього підходу полягає у послідовному вирішенні таких завдань: визначення кількості рівнів та вузлів АС; розподіл функцій АС по її рівням; вибір технічних засобів для вузлів системи. Цей підхід можна використовувати на стадії розробки концепції АС тільки в якості загального методичного базису, оскільки на цій стадії проектування розробник не володіє достатньо повними специфікаціями системи, а роботи, які є розвитком агрегативно-декомпозиційного підходу, можна використовувати на етапах ескізного та технічного проектування.

Вхідними даними методики є організаційно-штатна структура та множина завдань системи, а вихідними – кількість вузлів АС, кількість АРМ посадових осіб, її підсистеми і функції, а також засоби реалізації цих функцій.

к.т.н. Бурячок В.Л. (в/ч А1906)
Кафтан В.О. (в/ч А1906)
Костюк Т.Я. (в/ч А1906)

# КЛАСИФІКАЦІЯ ОБ'ЄКТІВ ЗА МЕТОДОМ КЛАСТЕРІЗАЦІЇ КІЛЬКІСНИХ ДАНИХ

При підготовці проведення порівняльного аналізу деякої вибірки з $R$ складних об'єктів (засобів розвідки) ключовим моментом є реалізація процедури, яка дозволить за визначеними критеріями здійснити її раціональний розподіл на сукупність декількох непересічних множин. Одним із можливих шляхів рішення даної задачі є застосування математичних методів кластерного аналізу. Отриманий результат в даному випадку може суттєво залежати від наступних факторів: відсутності однозначно найкращого критерію якості кластеризації; невизначеності щодо попередньої кількості кластерів відносно деякого суб'єктивного критерію; залежності результату кластеризації від метрики (або міри близькості об'єктів), вибір якої також суб'єктивний і визначається експертом.

Алгоритм реалізації методики, що вирішує дану задачу полягає в такому:

по-перше, формується матриця, елементами якої можуть бути показники:

– альтернатив-критеріїв, якщо використовується якісна шкала;

вихідної вибірки даних для $r_i$ об'єктів та $p_k$ ознак по кожному з них, якщо використовується кількісна шкала (де $N$ – кількість об'єктів, $i=\overline{1,N}$, $j=\overline{(i+1),N}$; $Q$ – кількість всіх критеріїв (ознак), $k=\overline{1,Q}$);

по-друге, отримана матриця за деяким відомим правилом приводиться до нормального виду;

по-третє, формується матриця близькості, елементи якої будуть визначатися як міжточкові відстані між парами альтернатив $r_i$ та $r_j$ :;

по-четверте, за матрицею близькості для пари альтернатив $r_i$ та $r_j$ :

– множина з $R$ об'єктів поділяється на підвибірки (диполі) близько розташованих об'єктів $A \bigcap B$;

– проводиться довизначення (регуляризація) сформованих кластеризацій $A$ і $B$ шляхом додаткової перевірки та поділу множини об'єктів на підмножини $C \bigcap D$;

– обчислюються між точкові відстані для підвибірок $A \bigcap B$ і $C \bigcap D$. Це триватиме до тих пір, поки всі об'єкти не увійдуть до множин $A \bigcap B$ та $C \bigcap D$;

по-п'яте, здійснюється перебір гіпотез про число кластерів $H_{AB}$ для підвибірок $A \bigcap B$ і $H_{CD}$ для підвибірок $C \bigcap D$ та обчислюються індекси, що відповідають масивам узгодженості ($F_{ij}^{yzg}$) і неузгодженості ($F_{ij}^{neyzg}$). Більше значення $f_{ij}^{yzg}$ ($f_{ij}^{yzg} \in [0,1]$) означає, що за критерієм узгодженості альтернатива $r_i$ переважає альтернативу $r_j$. Більше значення $f_{ij}^{neyzg}$ ($f_{ij}^{neyzg} \in [0,1]$) означає, що за критерієм неузгодженості навпаки альтернатива $r_j$ переважає альтернативу $r_i$;

по-шосте, проводиться перебір кластеризацій за сумарним критерієм несуперечності $H_{\Sigma}$, та визначаються пороги домінування шляхом порівняння індексів узгодженості – $f_{ij}^{yzg}$ і неузгодженості – $f_{ij}^{neyzg}$ з порогом кластеризації – $\rho_{пор}$. Оптимальній кластеризації відповідатиме випадок, коли $H_{\Sigma} \to 0$.

Реалізація запропонованого алгоритму дозволить:

– за сумарним критерієм несуперечності або індексами домінування прийняти рішення щодо раціонального розподілу множини з $R$ об'єктів (засобів розвідки) на групи, що у певному смислі схожі один на одного;

– вибрати найкраще, за визначеними критеріями, технічне рішення з усіх можливих.

Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Гребеніченко А.Р. (ВІТІ НТУУ „КПІ”)

# АЛГОРИТМ ВИБОРУ РАЦІОНАЛЬНОГО СЦЕНАРІЮ МОДЕРНІЗАЦІЇ МЕРЕЖІ ДОСТУПУ

Алгоритм вибору раціонального сценарію модернізації мережі доступу дозволяє шляхом перебору технологій, варіантів сценаріїв модернізації мережі доступу, розрахунку техніко-економічних характеристик здійснити вибір раціонального сценарію модернізації на основі прагматичного підходу.

Мета розробки та вибору сценарію модернізації мережі доступу полягає в забезпеченні ефективності прийняття управлінських рішень Оператором зв’язку по проведенню заходів пов’язаних з підтриманню конкурентоспроможності телекомунікаційної компанії та отримання прибутків.

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

Постановка задачі:

Задано:

– перелік технологій для забезпечення абонентського доступу;

– характеристики експлуатованої мережі доступу та її структура;

– сума інвестицій виділених для проведення модернізації;

– перелік телекомунікаційного обладнання.

Необхідно:

– розробити та вибрати раціональний сценарій модернізації мережі доступу;

– розрахувати основні техніко-економічні характеристики модернізованої мережі.

Обмеження:

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

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

Основні етапи реалізації методики:

1. Аналіз характеристик експлуатованої мережі доступу.
2. Формування цілей модернізації мережі доступу.
3. Вибір технологій використовуваних в мережі доступу.
4. Розробка $i$-го сценарію модернізації на підставі вибраних технологій.
5. Розрахунок техніко-експлуатаційних характеристик $i$-го сценарію модернізації мережі доступу.
6. Вибір телекомунікаційного обладнання та визначення переліку робіт з модернізації мережі доступу.
7. Розрахунок економічних характеристик і-го сценарію модернізації мережі доступу.
8. Розрахунок часу на проведення модернізації мережі доступу.
9. Запис результатів розрахунків характеристик $i$-го сценарію модернізації мережі доступу в базу даних.
10. Визначення закінчення розробки всіх можливих сценаріїв модернізації мережі доступу настає тоді коли шляхом перебору можливостей створений $i$-тий сценарій із множини реальних сценарії $\{I\}$.
11. Вибір раціонального сценарію модернізації мережі доступу за визначеними критеріями оптимальності.

12. Процес вибору раціонального сценарію закінчується коли ухвалюється найбільш раціональний сценарій на основі рішення багатокритеріальної оптимізаційної задачі та експертних оцінок.

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

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

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

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

Алгоритм вибору раціонального сценарію модернізації мережі доступу надає можливість здійснити більш ефективний та прагматичний вибір сценарію модернізації, але вона не вирішує всіх питань та потребує подальшого розвитку. Виходячи з цього розробка методик планерування сучасних мереж доступу і відповідних інструментальних засобів можна рахувати за важливе завдання для Операторів зв’язку.

ЛІТЕРАТУРА

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

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

3. *Рогинский В.Н., Харкевич А.Д., Шнепс М.А.* и др. Теория сетей связи: Учебник для вузов связи / Под ред. В.Н. Рогинского. – М.: Радио и Связь, 1981. – 428 с.

4. *Росляков А.В.* Сети доступа. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2008. – 96 с.

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

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

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

8. *Соколов Н.А.* Эволюция местных телефонных сетей. – Пермь: ТОО „Типография Книга”, 1994. – 144 с.

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

Вакуленко О.В. (ВІТІ НТУУ „КПІ”)
Липовий О.І. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ СИСТЕМ УПРАВЛІННЯ СУЧАСНИМИ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

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

Розвиток сучасних мереж та послуг телекомунікацій в умовах появи на ринку багатьох операторів телекомунікацій визначається низкою чинників, а саме:

для розвитку і реконструкції телекомунікаційних мереж, де поряд із новітніми цифровими системами передачі співіснує застаріле аналогове обладнання, використовують сучасні новітні технології;

у галузі працюють оператори телекомунікацій з різними формами власності;

побудова і реконструкція мереж телекомунікацій або окремих їх фрагментів здійснюється із застосуванням обладнання та технічних засобів одного призначення різних виробників і постачальників;

номенклатура й обсяг телекомунікаційних послуг значно розширюються, зростають вимоги до якості та швидкості надання послуг споживачам, до оптимального та ефективного використання ресурсів телекомунікаційних мереж, до їх надійності;

більше уваги приділяють створенню систем управління телекомунікаційними мережами із застосуванням сучасних апаратних і програмних засобів.

Одним із напрямків забезпечення підвищення надійності є ефективне управління ресурсами мереж. Створювані СУ сучасними телекомунікаційними мережами мають бути автоматизованими і враховувати перспективні технології і концепції, а також відповідати стандартам і рекомендаціям міжнародних організацій.

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

багаторівневості, ієрархічної побудови;

централізації управління з можливістю децентралізації функцій управління;

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

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

використання єдиної системи стандартів з технічного, інформаційного і програмного забезпечення на базі рекомендацій ITU, стандартів ETSI, ISO, державних та галузевих стандартів. Функціональна структура СУ телекомунікаційними мережами щодо попередження і дій у надзвичайних ситуаціях має охоплювати повний перелік проблем, що стосуються надзвичайних ситуацій, включаючи етапи їх прогнозування, попередження і підготовки до функціонування в умовах надзвичайних ситуацій, а також ліквідації їх наслідків.

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

режим повсякденної діяльності (стаціонарне функціонування);

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

надзвичайний режим (дії у надзвичайній ситуації);

післянадзвичайний режим (ліквідація довгострокових наслідків надзвичайних ситуацій).

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

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

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

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

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

лінії зв'язку, виділені канали зв'язку;

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

доступ до мереж передачі даних і телематичних служб;

канали радіозв'язку, використовувані в зоні надзвичайних ситуацій;

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

Управління телекомунікаційними мережами в умовах надзвичайних ситуацій здійснюється через НЦУ. НЦУ виконує функції загального управління телекомунікаційними мережами України та забезпечує їх ефективне функціонування для задоволення потреб споживачів.

ЛІТЕРАТУРА

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

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

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

4. *Стеклов В.К., Беркман Л.Н.* Телекомунікаційні мережі. – К.: Техніка, 2001. – 650 с.

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

к.в.н. Вертегел С.Г. (в/ч А1906)
Тупкало В.Є. (в/ч А1906)

# ВИЗНАЧЕННЯ РІВНЯ АВТОМАТИЗАЦІЇ ЗАВДАНЬ І ФУНКЦІЙ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

Автоматизація управління є актуальним і складним завданням. Цей процес вимагає визначення як існуючого, так і необхідного рівня автоматизації з метою урахування його під час розробки технічних завдань на створення автоматизованих систем управління. Пропонується аналітична методика визначення рівня автоматизації. В її основу покладено розбиття процессу управління на групи завдань, що виконуються органами управління у повсякденній та бойовій діяльності. В кожній групі завдань виділяються окремі функції, які підлягають автоматизації. Наприклад, для першої групи завдань такими функціями є: отримання розвідувальних даних; облік і реєстрація даних; первинна обробка і сортування; пошук даних за обраними критеріями; видача за запитами. Після цього визначається коефіцієнт рівня автоматизації і-ої групи завдань ($\boldsymbol{k_{ri}}$), як відношення кількості автоматизованих функцій з урахуванням ступеня їх автоматизації до кількості автоматизованих функцій у цій групі. Якщо всі функції у групі виконуються автоматизовано, то коефіцієнт рівня автоматизації дорівнює 1. В подальшому розраховується дійсний коефіцієнт рівня автоматизації і-ої групи завдань ($\boldsymbol{k_{di}}$) з урахуванням функцій, які неавтоматизовані, та коефіцієнт рівня автоматизації і-ої групи завдань (*K)* щодо усього процесу управління. У такий спосіб здійснюється розрахунки по кожній групі завдань.

Для розрахунку та оцінювання рівня автоматизації завдань, що вирішуються в органах військового управління, використовуються такі аналітичні залежності:

$$k_{ri} = \frac{\sum_{j=1}^{m} \mu_j}{100m}; \quad (1)$$

$$\boldsymbol{k_{di}} = \frac{\boldsymbol{k_{ri} v_{ai}}}{100}; \quad (2)$$

$$\boldsymbol{K} = \frac{\sum_{i=1}^{n} \boldsymbol{k_{di} v_i}}{100}, \quad (3)$$

де $n$ – кількість груп завдань; $i$ – номер окремої групи завдань відповідно до порядку; $m$ – кількість окремих дій в алгоритмі; $j$ – номер окремої дії відповідно до порядку; $\mu_o$– ступінь автоматизації j-ї дії ($\mu_o$= 0, 1), що досягається за рахунок засобів автоматизації, якими оснащено орган управління; $K$ – коефіцієнт рівня автоматизації процесу управління; $\boldsymbol{k_{ri}}$– розрахунковий коефіцієнт рівня автоматизації і-й групи завдань; $\boldsymbol{k_{di}}$– дійсний коефіцієнт рівня автоматизації і-й групи завдань; $\boldsymbol{v_i}$– обсяг завдань (%) і-ї групи зі всього переліку завдань; $\boldsymbol{v_{ai}}$– обсяг автоматизованих завдань (%) і-ї групи зі всього переліку завдань і-ї групи; $\mu_o, v_i, \boldsymbol{v_{ai}}$– визначаються методом експертного оцінювання (методом Дельфи); $\boldsymbol{k_{ri}}$– характеризує ступінь автоматизації завдань з і-ї групи, яка реалізована на засобах автоматизації; $k_{di}$– розраховується з урахуванням завдань і-ї групи, які не автоматизовані.

Після отримання для кожного пункту управління дійсних коефіцієнтів рівня автоматизації ($\boldsymbol{k_{di}}$ – за формулою 2) за всіма групами завдань, розраховується коефіцієнт рівня автоматизації процесу управління (К – за формулою 3). Якщо рівень автоматизації дорівнює 1, це означає що весь обсяг завдань, який покладено на орган військового

управління, автоматизовано на 100%, з урахуванням, що кожне завдання окремо має коефіцієнт рівня автоматизації – 1. Отримані значення коефіцієнтів дозволяють кількісно оцінювати ступінь автоматизації груп завдань, які вирішує орган управління.

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

# УЗАГАЛЬНЕНА ХАРАКТЕРИСТИКА ПРОТОКОЛІВ ВИПАДКОВОГО МНОЖИННОГО ДОСТУПУ З КОНТРОЛЕМ НЕСУЧОЇ

Протоколи з **випадковим розділянням ресурсу** відрізняються можливістю конфліктів або колізій. Одним з найпростіших в реалізації є протокол **неконтрольованого доступу**, де передача здійснюється в умовах повної відсутності взаємної координації між абонентами. Кожний абонент, що підготував до передачі пакет, в довільний момент часу починає передачу. Очевидно, що вірогідність конфлікту при цьому найбільша.

Але при низькому навантаженні на мережу такі протоколи використовуються. Для зменшення вірогідності конфлікту застосовують протоколи, що базуються на попередній перевірці стану радіоканалу. В простішому випадку перед передачею контролюють наявність сигналу несучої, що свідчить про зайнятість каналу.

Першим з опублікованих протоколів неконтрольованого випадкового доступу є **протокол ALOHA**. Цей протокол дозволяє передачу абонентам в довільний за їх вибором момент часу. Передавши пакет абонент на протязі певного часу очікує підтвердження від адресата. Якщо підтвердження не отримано, то приймається рішення про пошкодження пакету в конфліктній ситуації та призначається повторна передача, причому для виключення вірогідності повторного конфлікту початок передачі визначається через випадковий проміжок часу. Перевага такого протоколу - простота реалізації.

Протоколи випадкового доступу з **перевіркою стану каналу** перед початком передачі досить широко використовуються, особливо в комп’ютерних мережах. Кожний з цих протоколів може бути реалізований як в вільному, так і в тактовному (синхронному) варіанті.

Сутність **гнучкого** протоколу множинного доступу з контролем несучої (МДКН) складається в тому, що перед початком передачі абонент перевіряє наявність несучої в радіоканалі. Якщо сигнал не виявлено, то передається пакет. В супротивному випадку передача відкладається на деякий час, що визначається затримкою, яку вибирають випадковим чином з визначеного інтервалу. Перед повторною передачею заходи повторюються. Відсутність сигналу несучої перед початком передачі не дає гарантії безконфліктної передачі із-за кінцевого часу розповсюдження радіосигналу між абонентами. В гнучкому протоколі застосовується система позитивного квиткування. Після передачі пакету в період деякого часу абонент очікує підтвердження від адресату. Якщо підтвердження не отримано, то приймається рішення про руйнування пакету та призначається його повторна передача.

Можлива модифікація гнучкого протоколу – очікування звільнення каналу та після цього призначення передачі через випадковий проміжок часу, вибраний з деякого інтервалу. Такий метод носить назву **інтервальний.**

В **жорсткому (наполегливий)** протоколі МДКН при необхідності почати передачу та відсутності сигналу несучої в каналі абонент, як і в гнучкому протоколі, передає пакет. Якщо встановлена зайнятість каналу, то абонент безперервно перевіряє наявність несучої та при її зникненні починає передачу.

Компромісним варіантом цих двох протоколів є ***P* – жорсткий (*P* – наполегливий)** протокол, він відноситься до типу синхронних та діє наступним чином. Якщо пакет готовий до передачі та канал знаходиться у вільному стані, то пакет передається з вірогідністю $P$, а з вірогідністю $(1 - P)$ передача затримується на один такт. Якщо і в черговому такті виявлено вільний стан каналу, то процес повторюється. В супротивному випадку призначають повторну спробу передачі у відповідності з випадковим розподілом затримки. Якщо абонент при спробі передачі виявляє канал зайнятим, то він чекає його звільнення, перевіряючи на

початку кожного такту сигнал несучої та коли канал звільняється діє за описаним алгоритмом.

Гнучкий та жорсткий протоколи МДКН є базовими на основі яких розроблено багато інших. Найбільш відомий – протокол множинного доступу з **контролем несучої та виявленням конфліктів** в процесі передачі (МДКН/ВК). Виявити конфлікт можливо декількома способами: порівнюючи символи, що передаються та приймаються при прослуховуванні та виміром енергії сигналів в каналі спеціальним детектором конфліктів. Протокол досить ефективний, так як зменшується час знаходження каналу в стані передавання конфліктуючих пакетів. Канал звільняється в момент виникнення конфлікту на противагу базовим протоколам, де про конфлікт відомо після передачі.

Наступні протоколи, де мінімізовано час, коли канал використовується для передачі пошкоджених із–за конфлікту пакетів – прогнозуючі протоколи. Їх відносять до протоколів, де стан зайнятості каналу визначається не по наявності сигналу несучої, а по спеціальній ознаці зайнятості, управління яким здійснюється децентралізовано відповідними процедурами. Відомо два таких протоколи: протокол множинного доступу з контролем зайнятості радіоканалу та визначенням черговості передачі між конфліктуючими абонентами (**МДКН – Р, або рандомізуючий** від англійського random – навмання, всліпу) та **прогнозуючий протокол**. Вказані два протоколи можуть бути або з жорстким, або з гнучким управлінням.

Дії абонентів при виявлені зайнятого стану каналу по гнучкому та жорсткому протоколу **МДКН – Р** аналогічні діям абонентів при гнучкому та жорсткому протоколах МДКН відповідно. Відмінність в організації процедури визначення початку передачі при вільному стані каналу.

Абоненти, що вимагають в довільний момент часу канал для передачі (активні абоненти) та визначивши стан каналу як вільний, інформують решту абонентів мережі про початок циклу передачі та випадковим чином визначають черговість своєї передачі в цьому циклі. Для цього активні абоненти включають на короткий термін передавач без подачі на нього маніпуляційного коду. В каналі виникає сигнал несучої заданої тривалості. До початку чергового часового вікна решта абонентів мережі, що находяться в режимі прийому, зафіксують цей сигнал та встановлять ознаку початку циклу та ознаку зайнятості каналу.

При **прогнозуючому протоколі** кожний абонент постійно перевіряє сигнал несучої в каналі та при його отриманні встановлює ознаку зайнятості каналу. Після зникнення несучої ознака зайнятості скидається з затримкою на один такт, чим забезпечується резервування часу на початок передачі пакету при сприятливому прогнозі. Виділимо два варіанти дії абонентів (в залежності від значення системного параметра $P$) при надходженні запиту на передачу, коли встановлено ознаку зайнятості каналу: якщо $P = 0$, то абоненти відкладають передачу та повторюють її через інтервал часу випадкової тривалості з середнім значенням $X$, якщо $P = 1$, то абоненти очікують момент звільнення каналу, перевіряючи його стан в кожному черговому такті. Протокол, до складу якого входять дії по 1-му варіанту, називають **гнучким прогнозуючим**, по 2-му варіанту – **жорстким прогнозуючим**. На основі базових прогнозуючих протоколів запропоновано нові протоколи – **стабілізований та слідкуючий**.

Також в обмеженнях вказується, що в розглянутих протоколах застосовується відповідна система масового обслуговування з Пуасонівським потоком на вході , в якій не успішно обслужені заявки ставляться в чергу повторних заявок. Але не було висунуто припущення, що можуть траплятись втрати заявок вхідного потоку в джерелах повторних викликів (ДПВ) внаслідок, наприклад, зменшення їх актуальності та недоцільності повторення. Тому всі вищезазначені протоколи можуть бути **з втратами заявок в ДПВ**, або всі заявки ставляться в чергу повторних заявок – **без втрат заявок в ДПВ**.

Подальшим напрямом розвитку зазначених протоколів є передбачення про можливість обслуговування як одиночних так і пар конфліктуючих заявок які співпадають по тривалості що має актуальність для синхронних систем радіозв’язку.

Войтко Ю.М., (ІТС НТТУ „КПІ”)
к.т.н. Карпенко Б.О. (ВІКНУ)
к.т.н. Якорнов Є.А. (ІТС НТТУ „КПІ”)

# ВИЗНАЧЕННЯ РІЗНИЦІ РІЗНИЦЬ ФАЗ В МІКРОХВИЛЬОВИХ ФАЗОВИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Останнім часом при просторово-часовій обробці сигналів мікрохвильового діапазону в системах спеціального призначення починають використовувати їх фазові співвідношення більш високого порядку, наприклад, різницю різниць (подвійну різниць) фаз $\Delta\Delta = \Delta_{12} - \Delta_{32}$ між трьома приймальними антенами [1, 2]. Тому виникає задача безпосереднього визначення введеного параметра.

У роботи [2] показано, що визначити $\Delta\Delta\varphi$ можна трьома шляхами: 1) застосуванням двох стандартних фазометрів або в мікрохвильовому діапазоні двох фазометрів інтерференційного типу [3]; 2) схемною реалізацією на основі НВЧ мостів; 3) створенням алгоритмів обробки, що дозволяють по сигналах на виходах антен безпосередньо обчислювати вказаний параметр.

Схемна реалізація другого шляху припускає підключення до виходів антен двох синфазно-протифазних мостів, різницеві виходи яких сполучені з входами третього моста. Тоді на виходах останнього утворюються відповідно сумарні і різницеві коливання, а в пристрої обробки визначення подвійної різниці фаз проводиться за допомогою відомих співвідношень.

Більш перспективним, на наш погляд, є третій варіант побудови вимірників $\Delta\Delta\varphi$ шляхом програмної реалізації пристрою обробки завдяки розробці аналогово-цифрових перетворювачів (АЦП) мікрохвильового діапазону або перенесенню оброблюваних сигналів в діапазони стійкої роботи АЦП з одночасним їх підсиленням.

В докладі також представлений ще ряд структурних схем різних вимірників $\Delta\Delta\varphi$ і деякі підходи щодо усунення неоднозначності фазових відліків у фазометрах інтерференційного типу і урахування неідентичності напруг на виходах квадратичних детекторів.

ЛІТЕРАТУРА

1. *Абросимов В. Н., Алексеева В. И., Гребенко Ю. А.* и др. Использование системы NAVSTAR для определения угловой ориентации объектов. Зарубежная радиоэлектроника. 1989, № 7.

2. *Карпенко Б.О., Якорнов Є.А., Авдєєнко Г. Л.* Визначення подвійної різниці фаз у фазових мікрохвилевих системах вимірювання координат. Збірник наукових праць Військового інституту Київського національного університету імені. Тараса Шевченка. – К.: ВІКНУ, 2007. Вип. № 6.

3. *Войтко Ю. Н., Якорнов Е.А.* Определение фазовых сдвигов в широкополосных четырехдетекторных фазоизмерительных схемах. Известия ВУЗов – Радиоэлектроника, К.: 1995, № 5.

Восколович О.І. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ ПАРАМЕТРІВ ПРИ ПРОЕКТУВАННІ РАДІОМОДЕМІВ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З БАГАТОЧАСТОТНИМИ СИГНАЛАМИ

Технологія ортогонального частотного мультиплексування – *OFDM* (*Orthogonal Frequency Division Multiplex*) широко застосовується в мережах безпроводового доступу стандартів *IEEE* 802.11 та *IEEE* 802.16, системах цифрового радіомовлення *T-DAB* і *DRM*, цифрового телебачення *DVB-T*, а також у *xDSL*-модемах.

До основних переваг технології OFDM слід віднести стійкість до завмирань сигналу за умов багатопроменевості та частотно-селективних завмирань, а також високу спектральну ефективність. Багаточастотна структура групового сигналу зменшує чутливість системи передачі до імпульсних завад і дозволяє ефективно боротися із зосередженими за спектром завадами. За рахунок цього перспективним є застосування технології *OFDM* в системах радіозв’язку спеціального призначення.

Тому метою доповіді є аналіз параметрів модемів спеціального призначення з *OFDM*, які необхідно враховувати на етапі проектування.

До основних параметрів, значення яких необхідно визначити перед формуванням *OFDM*-сигналу відносяться: кількість піднесучих, частотний інтервал між ними, тривалість символу, тривалість захисного інтервалу (циклічного префікса), розмірність дискретного перетворення Фур’є (ДПФ), необхідна потужність.

Вихідними даними для вибору параметрів *OFDM*-символу є: смуга частот $\Delta F$, що відводиться для радіолінії; швидкість передачі інформації $v_{\text{і}}$, яка повинна забезпечуватись в каналі (кількість інформаційних біт за секунду); види модуляції та кодування; параметри каналу зв’язку (час кореляції завмирань $\tau_{\text{к}}$, розширення затримки $\Delta\tau$ сигналу в багатопроменевому каналі).

Відстань між піднесучими вибирається в залежності від наступних параметрів: доплерівське розсіювання спектра; максимальний час затримок променів (перевідбитих копій сигналу); максимально можлива тривалість символу (час когерентності параметрів каналу).

Циклічний префікс (захисний інтервал) вводиться в структуру сигналу для усунення шкідливого впливу міжсимвольної інтерференції. Розмір префікса $T_{\text{зі}}$ вибирається виходячи зі значень двох параметрів: максимально можливий зсув у часі між перевідбитими копіями сигналу $\Delta\tau_{\max}$; необхідне співвідношення між тривалістю символу без префікса та самого префікса (у випадку коли префікс використовується для знаходження тактової синхронізації).

Максимально можливу кількість піднесучих можна знайти, якщо поділити загальну смугу частот, відведену для передачі, на відстань між піднесучими: $N = F/\Delta f$. З іншого боку, кількість інформаційних піднесучих $N_{\text{інф}}$, необхідну для забезпечення заданої швидкості, можна визначити як відношення сумарної швидкості передачі радіолінії $R$ до швидкості передачі на одній піднесучій $R_n$.

Ган С.О. (ІТС НТУУ „КПІ”)

# ТЕНДЕЦІЇ БЕЗПЕКИ ІНФОРМАЦІЇ В СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Будь-яка організація, успішна тільки в тому випадку, якщо їх виробничі системи функціонують без збоїв. Умови використання обладнання або ПЗ, саботаж або втрата даних можуть завдати великої шкоди. Застосування Ethernet замість польових шин вперше передбачає використання технологій безпеки.

При виборі відповідної стратегії забезпечення безпеки виникає дві труднощі. По-перше, необхідно враховувати особливості фізичних умов на місцях і топологію існуючих і мереж, що розгортаються, а по-друге – потреба в адекватній концепції управління всією системою. Такі системи польових шин, як Interbus або Profibus, завдяки своїм нестандартним протоколам, операційних систем і додатків, а також ізольованості мереж, досить добре захищені від зовнішніх атак.

Однак тенденція переходу до відкритих платформ автоматизації на основі промислового Ethernet (Industrial Ethernet) обумовлює потребу в підвищенні рівня безпеки. Об’єднання систем в мережу, наявність з’єднань між різними зонами, а також поява інтерфейсів для віддаленого обслуговування створюють умови, за яких виникають загрози, звичні для офісних мереж: віруси, троянські програми, атаки з метою викликати відмову в обслуговуванні (Denial of Service, DoS), а також зловмисне скачування секретних документів.

Для запобігання збоїв у мережі та можливого порушення процесу спеціалізованої діяльності була запропонована трьохетапна концепція, реалізація якої дозволить забезпечити всеосяжний захист при одночасному дотриманні вимог технології автоматизації.

Етап 1: механічні заходи забезпечення безпеки. Найпростіший спосіб захисту від неправомірного доступу до виробничої мережі – використання механічних пристроїв блокування.

Етап 2: безпека без втрати продуктивності. Керовані комутатори, такі, наприклад, як Factory Line від Phoenix Contact, пропонують цілий ряд функцій забезпечення безпеки, сумісних з промисловим Ethernet. Вони дозволяють регулювати доступ, блокують небажані потоки даних, ускладнюють прослуховування даних.

Крім того, ці функції сприяють істотному підвищенню надійності експлуатації та доступності систем, забезпечуючи організацію віртуальних локальних мереж (Virtual Local Area Network, VLAN), контроль доступу на основі адрес MAC, а також обмеження доступу за допомогою технології Port Security.

Етап 3: придатні для промислової середовища пристрої забезпечення безпеки з функціями брандмауера і маршрутизатора. Децентралізоване застосування пристроїв з функціями брандмауера і маршрутизатора забезпечує індивідуальну захист розподілених систем автоматизації.

ЛІТЕРАТУРА

1. *Інго Хільгенкамп,* Торстен Рессель „Захист промислових мереж” www.osp.ru/lan/2008/12.

2. *Wu HEQUAN* „TELECOMMUNICATIONS: CHALLENGES & TRANSFORMATION” ЖУРНАЛ „Telecom Engine” www.telecommagazine.com.

Гахов С.О. (НАОУ)

# МЕТОДИКА ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Функціонування інформаційних систем спеціального призначення, як звісно, полягає у забезпеченні процесів прийняття рішення відповідними посадовими особами органів управління, доведення відповідної інформації, яка є відображенням даного прийнятого рішення до об'єкту управління та отримання інформації про його стан. Важливість даного питання висуває вимоги щодо забезпечення захищеності інформації та системи у цілому від несанкціонованого доступу (далі НСД), а також оцінювання їх рівня.

Аналіз літературних джерел показує, що у відповідності до вимог кількісної оцінки характеристик захищених інформаційних систем (далі ІС) у якості керованої змінної найчастіше вводиться узагальнений показник – рівень захищеності, необхідне значення якого залежить від максимального рівня критичності оброблюваної в даний період часу інформації.

Дослідження показують, що властивості захищеності процесів функціонування розподілених ІС залежать від їх якості, якості процесів їх функціонування та якості процесів функціонування системи управління захищеними обробкою та обміном інформації, що вимагає застосування комплексного підходу до забезпечення прояву даних властивостей та розроблення відповідної методики їх оцінювання. Тому, будемо розглядати захищеність як складну комплексну, системну та функціональну властивість процесів функціонування системи.

При розгляді захищеної інформаційної системи спеціального призначення як цілеспрямованої системи необхідно розглядати кожну окрему мету існування даної системи та відповідну їй функціональну систему. Декомпозиція функціональної системи на компоненти (у залежності від ступеня деталізації) є відображенням розкладання складної функції, що реалізовується, на елементарні. При цьому дослідження властивостей захищеності необхідно здійснювати для кожної утворюваної функціональної системи.

Основу задачі аналізу, яка пов'язана з дослідженням якості захищеної системи (компоненту) і якості процесів її функціонування, складає оцінювання відповідності показників захищеності інформації і системи цілому від НСД вимогам, що висуваються. Результати (вимоги) розв'язання задачі аналізу є вихідними для розв'язання задачі синтезу.

Адекватні математичні моделі захищеної ІС, її компонентів та процесів функціонування складають основу методики розрахунку показників захищеності системи та процесів її функціонування. Аналіз та інтерпретація даних моделей дозволяє встановити та виразити залежності показників захищеності від параметрів системи, зовнішнього середовища, структури та алгоритмів взаємодії як між компонентами системи у процесі їх функціонування, так і між процесами функціонування системи управління захищеними обробкою та обміном інформацією.

Основною метою оцінювання ефективності захисту інформації в ІС від НСД є встановлення факту наявності та прояву властивостей захищеності у ході функціонування системи, що дозволяє зробити висновок про загальний рівень захищеності інформації і системи в цілому від НСД та про відповідність потрібному рівню гарантій безпеки.

Процес оцінювання захищеної системи умовно можна поділити на основних два етапи: вимір характеристик системи, тобто визначення або обчислення її показників (кількісних або якісних) та оцінювання системи (її якості) за прийнятим критерієм (висновки) [1].

Основними властивостями захищеності, які повинні бути забезпечені в процесі функціонування розподіленої інформаційної системи, вважаються: конфіденційність інформації, конфіденційність інформації при обміні, цілісність інформації, цілісність

інформації при обміні, доступність інформації, а також основні властивості захищеної системи: цілісність, доступність та спостереженість системи [3]. У якості узагальнених показників даних властивостей процесів функціонування захищених систем застосовуються математичні вирази типу коефіцієнту корисної дії [2], які є найбільш показовими з точки зору наявності протиріччя у системі, вироблення відповідних вимог та визначення напрямку подальших дій. Застосовуючи означення, які запропоновані в [3], здійснюється формалізація даних властивостей та розглядається їх взаємозв'язок з точки зору функціонально-системного підходу.

Враховуючи те, що захищеність системи (як відповідна якість системи) та інформації (як відповідна якість процесу функціонування системи) є системними (комплексними) властивостями, вони оцінюються непрямим методом: показники захищеності системи та інформації складають відповідні вектори, які розглядаються як формальні моделі якості захищеної системи і якості властивостей захищеності інформації від НСД.

Аналіз математичних виразів властивостей захищеності дозволив зробити важливий висновок: додавання компонентів, які реалізують функції захисту, у систему призводить до підвищення її рівня системності. Усунення вразливостей системи та процесів її функціонування (як мета) призведе до підвищення рівня системності і детермінованості як ІС-компонентів, так і розподіленої системи у цілому. І, навпаки, підвищення рівня системності і детермінованості ІС призведе до підвищення рівня захищеності системи і інформації від НСД. Дані положення визначають умови та шляхи забезпечення безпеки інформації від НСД в ІС, а саме:

створення ІС з найвищим рівнем системності і детермінованості;

інтегрування компонентів захисту до ІС, які забезпечують (підвищують) найвищий рівень її системності і детермінованості.

Основними факторами, що впливають на результат функціонування системи та рівень захищеності інформації від НСД, є:

якість системи, що полягає в наявності компонентів, які реалізують відповідні функції захисту (один із показників якості системи – повнота реалізацій функцій захисту), та зв'язків між усіма компонентами системи. Основними показниками якості системи можна вважати рівень системності і рівень детермінованості;

якість забезпечення умов функціонування ІС (управління системою), що визначається властивостями функціонування компонентів протоколів інформаційної взаємодії. Основним показником забезпечення умов функціонування ІС (якості управління) можна вважати результативність процесу її функціонування.

Таким чином, запропонована методика оцінювання ефективності захисту інформації від НСД в інформаційних системах спеціального призначення, яка базується на моделях якості захищеної системи і якості процесів її функціонування, дозволяє врахувати системні протиріччя, які розширюються існуючими можливостями НСД, об'єктивно оцінити рівень захищеності системи та інформації від НСД та визначити шляхи впливу на систему та процеси її функціонування (виробити вимоги до реалізації відповідного управління) з метою забезпечення необхідного (максимального) рівня захищеності інформації та системи у цілому від НСД.

ЛІТЕРАТУРА

1. *Петухов Г. Б., Якунин В. И.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. – М. : АСТ, 2006. – 504 с. – ISBN 5-17-034652-2.

2. *Теслер Г. С.* Новая кибернетика. – К. : Логос, 2004. – 404 с. – Библиогр.: с. 396-397. – ISBN 966-581-488-5.

3. *Термінологія в галузі* захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. – К. : ДСТСЗІ СБ України, 1999. – 26 с.

Генов М.С. (в/ч А1906)

# КОМБІНОВАНІ МЕТОДИ ЗАХИСТУ ПОЛІГРАФІЧНОЇ ПРОДУКЦІЇ

Дизайнерські методи захисту за допомогою особливих прийомів верстки й програм для обробки зображення практично вичерпали потенціал. Контрольні й штрихові коди, сховані зображення, сполучені малюнки, спеціальні „дефекти”, антисканерні сітки й навіть гильоширні елементи й мікротекст вже освоєні зловмисниками. Графічні елементи легко копіюються за допомогою сучасної сканируючої і друкованої техніки.

Деякі методи захисту поліграфічної продукції:

Спеціальні види растрування. Лінійчаті, концентричні й будь-які інші „неправильні” види растрів хоча й трохи погіршують сприйняття картинки, але ставлять значний бар’єр для фальшивок. Принаймні, їх не можна буде повторити в офсеті, не маючи в друкарні унікальних алгоритмів растрування. Ефективні й нетрадиційні види кольороподілу: дуплекс, триплекс, 5 -, 6 - або 7 - барвиста печатка.

Англійська Trustcopy оголосила про спеціальні оптичні водяні знаки - шарі, що доповнює видимий захист продукції. Це може бути складне зображення (портрет) або просто серія цифр. На одній ділянці етикетки комбінується до 20 - ти шарів водяних знаків Trustcopy. Для їхнього відтворення підходять практично всі матеріали й способи - офсет, глибокий і високий друк, флексографія, струминні й лазерні принтери. Щоб побачити знаки, потрібна лінза-ключ. Її одержують всі учасники ланцюга поставок (виробник, вистриб’ютори й роздрібні компанії), щоб перевіряти продукцію протягом усього шляху до споживача. Фальсифікатор про наявність водяних знаків не здогадується й не зможе підробити їх або скопіювати.

Більше високим рівнем захисту в діапазоні класичних захисних фарб відрізняються фарби й лаки, що комбінують різні захисні ефекти: наприклад, фарби термохромні й оптикозмінні (OVI), люмінесцуючі різними кольорами під Уф-променями короткохвильового й довгохвильового діапазону, а також Ік-випромінюванням. Завдяки тому, що всі ефекти зібрані в одній фарбі, з’являється додаткова можливість для звуження кола осіб, що знають про той або інший захисний ефект.

ГК „Дубль В” представила унікальну технологію „Цандерс Ефалін форм” від Zanders: на паперове полотно вибірково наноситься спеціальний шар, що впливає на проникнення фарби в структуру паперу. Завдяки цьому пігментація частини волокон міняється. Шар може мати додаткові ефекти (перламутровий, різнобарвний і захисний).

Даний перелік методів захисту поліграфічної продукції не повний, але при розгляді перерахованих вище технологій, можна зробити висновок, що можливості захисту в даній області можна підвищити за допомогою комбінування або зміни вже існуючих методів. При цьому дуже важливо знайти вдалий компроміс між вартістю засобів захисту і її ефективністю

ЛІТЕРАТУРА

1. *Журнал FlexoTech* http://www.paperandprint.com/flexo-tech/index.htm.

2. *Журнал Graphic* Arts Monthly (Поліграфія щомісяця) http://www.gammag.com.

3. *http:*//www.privacypolice.org.

4. *Fogra F*orschungsgesellschaft Druck e.V. (Fogra Graphic Technology Research Association; Fogra — дослідницька асоціація в області поліграфічних технологій) http://www.fogra.org.

д.т.н. Герасимов Б.М. (ВІТІ НТУУ „КПІ”)
Шугалій Є.П. (УВМА)

# РОЗПОДІЛ ІНФОРМАЦІЙНОГО РЕСУРСУ МІЖ РОБОЧИМИ МІСЦЯМИ ОПЕРАТИВНОГО ПЕРСОНАЛУ ОРГАНІВ УПРАВЛІННЯ ВІЙСЬКАМИ

Ефективне функціонування системи управління Збройних Сил України в сучасних умовах може бути досягнуто тільки при широкому втіленні інформаційних технологій у діяльність органів військового управління. ПУ (КП, ЗКП, ТПУ) обладнані автоматизованими робочими місцями і автоматизованими інформаційними місцями, де посадові особи органів управління різних ланок і належностей працюють у єдиному інформаційному просторі. Збільшення кількості задач та обсягу інформації, обробка яких забезпечується використанням автоматизованих робочих місць, значно ускладнює завдання раціонального розподілу інформаційного ресурсу між робочими місцями оперативного персоналу в інформаційно-телекомунікаційній системі органів управління.

Одним з можливих підходів до вирішення даного завдання є застосування методу динамічного програмування [1, 2], який дозволяє знайти оптимальне рішення в задачах розподілу однорідного дискретного ресурсу по об’єктах, що доповнюють. У випадку однорідності дискретного ресурсу ефективність розподілу визначається тільки кількістю одиниць виділеного ресурсу на кожен об’єкт.

Для інформаційно-телекомунікаційної системи органів управління інформаційний ресурс, який підлягає розподілу між автоматизованими робочими місцями, визначається кінцевою множиною елементів, кожен з яких описується значенням із множини атрибутів. Неоднорідність інформаційного ресурсу значно ускладнює рішення задачі раціонального розподілу. Тому, при вирішенні задачі варто враховувати, що ефективність розподілу буде визначатися не тільки кількістю елементів (одиниць), що виділяються на автоматизовані робочі місця, але і значеннями їх атрибутів, які змінюються від елемента до елемента. Задача відноситься до класу задач цілочисельного програмування з бульовими змінними. Якщо множина можливих варіантів рішень на розподіл інформаційного ресурсу невелика, то оптимальне рішення може бути отримане методом прямого перебору всіх можливих варіантів, але збільшення числа можливих варіантів призводить до значного зростання обчислювальних витрат, що робить неможливим використання цього методу.

У доповіді розглядається сутність застосування моделі раціонального розподілу неоднорідного інформаційного ресурсу за автоматизованими робочими місцями [3], яка полягає в оптимізації розподілення інформаційних модулів за робочими вузлами інформаційно-телекомунікаційної системи органів управління з урахуванням необхідних (зі сторони користувача) та існуючих (зі сторони кінцевих систем) просторово-часових та об’ємно-інформаційних ресурсів. Відмінність даної моделі від існуючих полягає в представленні багатокрокового процесу вибору рішень в просторі параметрів та етапів управління, що описуються підмножинами одиниць неоднорідних ресурсів, з подальшим застосуванням методу динамічного програмування, що дозволяє оптимізувати функціональну структуру інформаційно-телекомунікаційної системи органів управління.

## ЛІТЕРАТУРА

1. *Беллман Ричард.* Динамическое программирование и современная теория управления / Беллман Ричард. – М.: Наука, 1969. – 27 с.

2. *Осинский Л.М.* Методы оптимизации с приложениями к военному делу / Осинский Л.М. – К.: КВИРТУ ПВО, 1971. – 259 с.

3. *Ніколаєнко О.Є.* Модель оптимального розподілу неоднорідного дискретного ресурсу в локальній обчислювальній мережі на основі методу динамічного програмування / Ніколаєнко О.Є., Шугалій Є.П., Шугалій О.О. // Збірник наукових праць НАОУ. – 2008 р. – № 76. – С. 45 – 52.

д.т.н. Герасимов Б.М. (ВІТІ НТУУ „КПІ”)
Шугалій Є.П. (УВМА)

# МЕТОДИКА СИНТЕЗУ СТРУКТУРИ ОРГАНІВ УПРАВЛІННЯ ВІЙСЬКАМИ ПО КРИТЕРІЮ ОПЕРАТИВНОСТІ

Організаційно-технічну основу управління військами складає система управління, яка включає органи управління, пункти управління та засоби управління. Органи управління призначені для виконання функцій з управління військами в різноманітних ланках. В усіх випадках вони займають центральне та визначне місце в системі управління. У зв’язку зі збільшенням розмаху та динамічності бойових дій різко зросли обсяг та зміст завдань управління при скороченні наявних термінів їх виконання. Вирішення задачі підвищення оперативності управління передбачає застосовування математичних методів аналізу та моделювання, які враховують об’єм робіт, що підлягає виконанню в різних умовах обстановки, перевірені норми часу на виконання кожної роботи та внаслідок багаторазових розрахунків за різноманітними варіантами дозволяє визначити склад та структуру органів управління [1].

У доповіді розглядається вдосконалена методика синтезу раціональної ієрархічної структури органів управління військами сутність якої полягає в урахуванні критерію оперативності при визначенні числа рівнів структури органів управління і числа елементів на кожному рівні ланки управління. Методика базується на застосуванні математичного апарату теорії масового обслуговування [2]. Вихідні дані та обмеження: $S$ – множина допустимих структур реалізації ієрархічної структури системи управління, яка характеризується кількістю рівнів ієрархії $Q = \overline{1,k}$ та кількістю підсистем (пунктів управління) на кожному рівні $m_k$; кожній системі відповідного рівня ієрархії підпорядковано однакове число підсистем наступного рівня (система однорідна); потоки задач, що вирішуються найпростіші; час рішення задач розподілено за експоненціальним законом; черги задач для кожної підсистеми необмежені. Раціональний варіант ієрархічної структури системи управління військами повинен відповідати визначеній системі критеріїв. В якості основного критерію оцінки структури пропонується обрати – час на вирішення задач управління $T$, а в якості обмеження – вартість системи $C$.

Потрібно: знайти такий варіант ієрархічної структури системи управління військами $S_0$, при якому забезпечується мінімізація часу на вирішення задач управління: $S_0 = \arg\min_{S_0 \in S} T(S)$, при обмеженні: $C(S) \le C_{доп}$, де $C_{доп}$ – гранично допустима вартість структури системи управління.

В цьому випадку рішення задачі зводиться до вибору раціональної кількості рівнів ієрархії та кількості підсистем на кожному рівні $m_k$ [3].

Перевагами даної методики є можливість отримання верхніх оцінок критеріальних функцій для різних варіантів ієрархічної структури органів управління військами, проведення попереднього відбору найбільш перспективних варіантів. Розроблено програмне забезпечення, яке реалізує повний перебір можливих варіантів структури для методики синтезу раціональної ієрархічної структури. Наведений приклад вибору раціональної ієрархічної структури органів управління військами для конкретних вихідних даних, які описують особливості функціонування органів управління.

ЛІТЕРАТУРА

1. Довідник з протиповітряної борони / [А.Я. Торопчин, І.О. Романенко, Ю.Г. Даник и др.]. – К.: МО України. – Х.: ХВУ, 2003. – 368 с.

2. Вентцель Е.С. Теория верятностей / Вентцель Е.С. – М.: Наука, 1964. – 576 с.

3. Подиновский В.В. Оптимальные решения многокритериальных задач / Подиновский В.В., Ногин В.Д. – М.: Наука, 1982. – 260с.

Гєлєсєв В.О. (ІТС НТТУ „КПІ”)
к.т.н. Карпенко Б.О (ВІКНУ)
к.т.н. Якорнов Є.А. (ІТС НТУУ „КПІ”)

# ВИКОРИСТАННЯ ВАГОВОЇ МІЖКАДРОВОЇ ОБРОБКИ В СИСТЕМАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ДЛЯ СЕГМЕНТАЦІЇ РУХОМИХ ОБ’ЄКТІВ ЗОБРАЖЕННЯ

Використання руху, одного з основних ознак розпізнавання об’єктів, яким користуються в живому світі, широко застосовується при обробці зображень. В прикладних задачах обробки зображень рух виникає при відносному переміщенні сенсорної системи і спостережуваної цілі, що відбувається в різних областях життєдіяльності, у тому рази в системах спеціального призначення.

В даний час сегментація об’єктів здійснюється, в основному, за допомогою просторових і частотних методів.

Основою просторових методів сегментації є виділення різницевого зображення при пороговій обробці. Альтернативою припущення про те, що ненульові елементи різницевого зображення відносяться до об’єктів, що рухаються, слід вважати шум. Хоча помилкові шумові складові, котрі присутні в різницевому зображенні, є серйозною перешкодою їх вдається зменшити за допомогою порогового аналізу зв’язності.

Проте при такій фільтрації можуть бути втрачені дрібні об’єкти або об’єкти , що рухаються повільно.

Одним із способів розв’язання цієї проблеми є використання декількох кадрів зображення, які дозволяють ігнорувати в різних різницевих зображеннях випадкові зміни, що обумовлені шумами .

Накопичені різницеві зображення (НРЗ) формуються шляхом порівняння опорного зображення з кожним подальшим кадром послідовності. Найчастіше розглядають три види накопичених різницевих зображень: абсолютні, позитивні і негативні.

На практиці не завжди вдається отримати опорне зображення, що складається тільки з нерухомих елементів, і тоді його доводиться будувати на підставі обробки набору позитивних і негативних НРЗ. Така складна побудова опорного зображення потребує не тільки багато часу, але і великої продуктивності обчислювальних засобів.

Пропонується новий підхід виділення об’єктів зображень, що рухаються, з використанням відносних n-кратних різницевих зображень (ВРЗ). Відносні n-кратні різницеві зображення формуються на основі послідовного різницевого зображення за допомогою ВРЗ (n-1) кратності. В даний час використовуються різницеві зображення, що являють собою ВРЗ першої кратності.

Пропонований у доклади підхід дозволяє використовувати як опорне зображення перший необхідний кадр, який автоматично є опорним у всіх ВРЗ довільної кратності. Цей метод значно спрощує і підвищує ефективність виділення об’єктів, що рухаються.

Крім того, він дозволяє застосовувати апарат кронекерівського (тензорного, зовнішнього) добутку і різко скоротити необхідний об’єм математичних обчислень.

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

# ПРОЦЕДУРА РОЗПОДІЛУ ПАМ’ЯТІ АВТОМАТИЗОВАНИХ КОМПЛЕКСІВ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Пам’ять – функціональна частина комплексу, призначена для приймання, зберігання та видачі інформації. Пам’ять будується за ієрархічним принципом. В основу побудови ієрархії, як правило, покладаються два основні параметри пам’яті: швидкодія $t_o$ та ємність С.

У доповіді розглядається процедура розподілу запам’ятовуючих пристроїв за рівнями ієрархії, враховуючи вартісні обмеження та часові і частотні характеристики алгоритму реалізації функціональної задачі.

Вся інформація, яка циркулює в автоматизованих комплексах спеціального призначення, умовно поділяється на постійну та змінну. Під масиви даних постійної інформації пропонується виділяти розділи пам’яті на жорсткому диску з дублюванням її в залежності від об’єму на дисках CD або ж DVD. З метою забезпечення зберігання змінної інформації та конфіденційних даних пропонується використовувати флеш-пам’ять та ключові НГМД. Застосовуючи процедури розподілу пам’яті, були отримані рівні ієрархії та відповідні їм види пам’яті з основними параметрами.

На вершині ієрархії розташовуються такі види пам’яті як:

надоперативна ($t_o$=2–10 нс та С=1–4 кБ);

стекова ($t_o$=20–50 нс та С=64 кБ);

кеш L1 ($t_o$=2–10 нс та С=16 кБ);

кеш L2 ($t_o$=20–50 нс та С=256 кБ–1 МБ);

кеш L3 ($t_o$=20–50 нс та С=1–8 МБ);

управляюча пам’ять ($t_o$=2–10 нс та С=16–64 кБ);

буферна ($t_o$=20–50 нс та С=2, 8, 16, 32 МБ).

Другий рівень ієрархії включає:

оперативну пам’ять динамічну: DRAM ($t_o$=2,5–20 нс та С=256–2048 МБ);

статичну: SRAM ($t_o$=2,5–20 нс та С=256 кБ-1МБ);

постійну пам’ять PROM ($t_o$=50–200 нс та С=16–1024 кБ); EEPROM ($t_o$=50–200 нс та С=16–1024 кБ); UV PROM ($t_o$=50–200 нс та С=16–1024 кБ); Flash ($t_o$=20–60 нс та С=256 МБ–16ГБ).

На наступному рівні ієрархії розташовується зовнішня пам’ять:

НЖМД ($t_P$=5–10 мс, $t_o$=20–60 нс та С=80 ГБ–4 ТБ),

НГМД ($t_P$=100–500 мс, $t_o$=200–300 мкс та С=1,44–2,88 МБ),

CD ($t_P$=50–100 мс, $t_o$=40–120 нс та С=210–900 МБ),

DVD ($t_P$=5–10 мс, $t_o$=20–60 нс та С=1 ГБ–50 ГБ).

В основі схеми ієрархії лежить архівна пам’ять на магнітній стрічці ($t_P$=60–120 с, $t_o$=100–200 нс та С=20 МБ–20 ТБ). Для зовнішньої та архівної пам’яті під $t_P$ розуміється час пошуку області пам’яті для запису або зчитування інформації. Наводяться алгоритми режимів запису і зчитування даних для мікросхем внутрішньої пам’яті. Під внутрішньою розуміється електронна (напівпровідникова) пам’ять, яка встановлюється на системній платі або на платах розширення і виконується у вигляді модулів.

ЛІТЕРАТУРА

1. *Гук М.* Аппаратные средства IBM PC. Энциклопедия. / Гук М. – Спб.: Питер, 2001. – 928 с.

2. *ДСТУ 2*869-94 Системи оброблення інформації. Обладнання периферійне. Терміни та визначення.

к.т.н. Горбенко В.І. (ВІТІ НТТУ „КПІ”)
к.т.н. Павлюк С.В. (в/ч А1906)
Ратанін Є.Г. (в/ч А1906)
Сілко О.В. (ВІТІ НТТУ „КПІ”)

# ПРОЦЕДУРА ВИЗНАЧЕННЯ ПАРАМЕТРІВ МАТРИЦІ ПЕРЕМЕЖІННЯ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Канали зв’язку телекомунікаційних систем характеризуються наявністю шумів, завад, викривлень та інтерференцій різної природи й інтенсивності. Це призводить до того, що ефективність роботи апаратури прийому-передачі даних зменшується, що проявляється в пропусках початку прийому даних і в збільшенні часу на запити для повторної передачі.

Такий пропуск викликає неможливість правильного налаштування апаратури прийому-передачі даних, однією із основних підсистем якої є підсистема декодування. Підсистема декодування залежно від виду передачі забезпечує реалізацію алгоритмів обробки бітового потоку, використовуючи параметри матриці перемежіння, пропуск яких не дозволяє здійснювати подальший прийом даних. Зокрема, пропуск параметрів матриці перемежіння не дозволяє здійснювати подальший прийом даних.

Для вирішення задачі прийому даних пропонуються процедура та алгоритми обробки інформації, які дозволяють визначити параметри матриці перемежіння. В основу процедури визначення параметрів матриці перемежіння покладено принципи принципи застосування декодування згорткових кодів.

Для розпізнавання параметрів матриці перемежіння використовується декодування згорткових кодів за алгоритмом Вітербі (декодер максимальної правдоподібності). Для кожного можливого варіанта параметрів матриці перемежіння застосовується декодер Вітербі з фіксованою шириною вікна декодування. Математичне співвідношення для обчислення метрики ребра на $i$-му кроці процедури визначення параметрів матриці перемежіння має вид

$$BM_i = d_H(\mathrm{r}[i], \mathrm{v}[i]),$$

де $BM_i$ – метрика ребра на і-му кроці процедури;

$d_H$ – відстань Хеммінга;

$\mathrm{r}[i]$ – вхідне кодове слово підсистеми декодування;

$\mathrm{v}[i]$ – кодове слово, яке прогнозується на виході підсистеми декодування.

Критерієм прийняття рішення про правильно визначений варіант є мінімальна міра розбіжності шляху для вхідного кодового слова підсистеми декодування.

Таким чином, запропонована процедура визначення параметрів матриці перемежіння дозволяє підвищити ефективність роботи апаратури прийому-передачі даних телекомунікаційних систем в нестійких каналах зв’язку.

ЛІТЕРАТУРА

1. *Блейхут Р.* Теория и практика кодов контролирующих ошибки. / Блейхут Р. – М.: Мир, 1986. – 576 с.

2. *Морелос-Сарагоса Р.*Исскуство помехоустойчивого кодирования. Методы, алгоритмы, применение. / Р. Морелос-Сарагоса. – М.: Техносфера, 2005. – 320 с.

3. *Вернер М.* Основы кодирования. – М.: Техносфера, 2004. – 288 с.

4. *Бурдаев О.В., Иванов М.А.* Ассемблер в задачах защиты информации. – М.: КУДИЦ-ОБРАЗ, 2002. – 320 с.

к.т.н. Горьков В.К (НАОУ)

# ОРГАНІЗАЦІЯ РОЗРОБКИ ТЕХНІЧНОГО ПРОЕКТУ ІНФОРМАЦІЙНИХ СИСТЕМ

Інформаційна система – це сукупність програмно-технічних елементів та організаційних структур об'єднаних для надання інформаційних послуг з використанням інформаційних технологій. В загальному випадку поняття інформаційної системи зводиться до сукупності функціонально зв'язаних підсистем збору, систематизації, збереження, обробки та цілеспрямованого використання інформації.

Будь-яка інформаційна система – це сукупність двох складових: структурно-організаційної та структурно-функціональної.

Перша надає уявлення про структурну побудову системи та сукупність найбільш важливих зв'язків між ними.

Друга розкриває сутність функціональної взаємодії складових в процесах, які визначають механізми досягнення цільового призначення системи. При цьому треба мати на увазі, що певна частина програмних засобів забезпечує нормальне функціонування технічних засобів (готовність системи до виконання завдань), а інша – виконання на них задач прикладного характеру як загального так і спеціального призначення.

Підставою для розробки технічного проекту системи є технічне завдання, затверджене замовником.

Технічний проект системи – це технічна документація, затверджена у встановленому порядку, що містить загальносистемні проектні рішення, алгоритм рішення задач, а також оцінку економічної ефективності автоматизованої системи керування і перелік заходів щодо підготовки об'єкта до впровадження.

Технічний проект розробляється з метою визначення основних проектних рішень по створенню системи. На цьому етапі здійснюється комплекс науково-дослідних і експериментальних робіт для вибору найкращих варіантів рішень, проводяться експериментальна перевірка основних проектних рішень і розрахунок економічної ефективності системи.

Економіко-організаційна частина технічного проекту містить пояснювальну записку щодо основ для розробки системи, перелік організацій розробників, коротку характеристику об'єкту з вказівкою основних техніко-економічних показників його функціонування і зв'язків з іншими об'єктами, короткі свідчення про основні проектні рішення по функціональній і частинах системи, що забезпечують.

У розділі про організаційну і функціональну структуру системи надаються обґрунтування виділених підсистем, їхній перелік і призначення; перелік задач, що, розв'язуються у кожній підсистемі, з короткою характеристикою їхнього змісту; схема інформаційних зв'язків між підсистемами і між задачами в рамках кожної підсистеми.

Для кожної задачі, включеної в комплекс першочергових, виконуються її постановка й алгоритм рішення. У цей розділ технічного проекту включаються:

– організаційно-економічна сутність задачі (найменування, ціль рішення, короткий зміст, метод, періодичність і час рішення задачі, способи збору і передачі даних, зв'язок задачі з іншими задачами, характер використання результатів рішення, у яких вони використовуються);

– економіко-математична модель задачі (структурна і розгорнута форма представлення);

– вхідна оперативна інформація (характеристика показників, їх значимість і діапазон зміни, форми представлення);

– нормативно-довідкова інформація (НДІ) (зміст і форми представлення);

– інформація, яка має бути збережена для зв'язку з іншими задачами;

– інформація, що накопичується для наступних рішень даної задачі;

– інформація з внесення змін (система внесення змін і перелік інформації, що піддається змінам);

– алгоритм рішення задачі (послідовність етапів розрахунку, схема, розрахункові формули);

– контрольний приклад (набір заповнених даними форм вхідних документів, умовні документи з що накопичують і зберігають інформацію, форми вихідних документів, заповнені за результатами рішення задач прогнозування відповідно до розрахунків при використанні комплексів моделювання).

Інформаційна частина технічного проекту поєднує джерела надходження інформації і способи її передачі для рішення першочергового комплексу функціональних задач; сукупність показників, використовуваних у системі; склад документів, терміни і періодичність їхнього надходження; основні проектні рішення по організації фонду нормативно-довідкової інформації; склад нормативно-довідкової інформації, включаючи перелік реквізитів, їхнє визначення, значимість, діапазон зміни і перелік документів нормативно-довідкової інформації; перелік масивів нормативно-довідкової інформації, їхній обсяг, порядок і частота коректування інформації; пропозиції по уніфікації документації, контрольний приклад по внесенню змін у нормативно-довідкову інформацію; структурна форма нормативно-довідкової інформації з описом зв’язку між її елементами; вимоги до технології створення і ведення фонду; методи збереження, пошуку, внесення змін і контролю; визначення обсягів і потоків інформації.

Математична частина технічного проекту містить обґрунтування структури математичного забезпечення, а також обґрунтування вибору системи програмування, у тому числі перелік стандартних програм.

Математичне забезпечення на рівні прикладних програм має забезпечити рішення задач прогнозування, які виконуються на всіх етапах рішення задач управління.

Цей комплекс задач та моделей може складатись, як за спеціалізацією задач, що виконуються, так і комплексні моделі, завдяки яким можуть прогнозуватись задачі загального порядку.

Перелік задач, що виконуються в межах рішення задач управління встановлюється при організації проектуванні і визначенні змісту та порядку виконання основних задач управління.

Технічна частина технічного проекту припускає опис і обґрунтування схеми технічного процесу обробки даних; обґрунтування вимог до розробки нестандартного устаткування; обґрунтування і вибір структури комплексу і технічних засобів і його функціональних груп; комплекс заходів щодо забезпечення надійності функціонування технічних засобів.

Таким чином нами розглянута організація загальної послідовності відпрацювання розробки технічного проекту інформаційних систем в цілому та його складових частин.

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

# ГІБРИДНЕ КОДУВАННЯ ТА ВИНЕСЕНЕ КОМПАНДУВАННЯ

1. Цифрові системи передачі з імпульсно-кодовою модуляцією (ЦСП з ІКМ) прийняті у міжнародному масштабі за основний тип цифрової каналоутворювальної апаратури, реалізація якої здійснюється за двома стандартами – американському та європейському. В Україні прийнятий європейський стандарт. Використання цієї апаратури на різних лініях зв’язку розширюється. Передбачається, що лінії зв’язку повинні бути достатньо якісними (ймовірність помилкового прийому одиничного елемента не повинна перевищувати $P \leq 10^{-4}$). У противному випадку апаратура переходить у аварійний режим функціонування із втратою зв’язку по каналах ТЧ. Тому є проблематичним використання ЦСП з ІКМ без необхідної модернізації у польових системах зв’язку різних спеціалізованих структур при виникненні ситуацій з погіршенням якісних показників ліній зв’язку.

2. При розробці систем з ІКМ перших поколінь і наступній їх стандартизації вважалося, що основним навантаженням каналів ТЧ будуть мовні сигнали, що відповідало тодішній і відповідає загалом сьогоднішній практиці. Але розвиток телекомунікацій привів до збільшення ваги в навантаженні немовних сигналів (факс, передача даних, Internet, IP-телефонія, телевимірювання, ін.) і цей процес має сталу тенденцію до розширення. Тому технічні рішення, прийняті при побудові систем з ІКМ, з орієнтуванням на мовні сигнали, для інших сигналів далекі від оптимальних.

3. Як відомо[1], щільність ймовірностей миттєвих значень мовних сигналів зростає при наближенні до нуля і зменшується при наближенні до встановленого значення динамічного діапазону зміни сигналу. Це враховувалось при розробці принципу компандування і кодування симетричним кодом миттєвих відліків сигналу в базовій апаратурі ІКМ-30 європейського стандарту (ІКМ-24 американського стандарту). При передачі гармонічних посилок з випадковою початковою фазою, рівномірно розподіленою в межах 0–2π, щільність ймовірностей найменша при переході синусоїди через нуль і максимальна при переході через амплітудне значення. Така протилежність знижує відношення сигнал/шум на виході каналу для синусоїдального сигналу.

4. При погіршенні якісних показників лінії зв’язку (ймовірність помилок в цифрову лінійному сигналі $P \geq 10^{-4}$) визначальними у відношенні сигнал/шум на виході каналу ТЧ є шуми декодування кодових комбінацій з помилками. Величина цих шумів залежить від типу коду, яким кодуються миттєві відліки сигналу для передачі по лінії зв’язку, рівня цього сигналу на вході каналу та щільності ймовірностей миттєвих значень сигналу.

Набір цих факторів формує своє мінімальне значення шумів декодування (рис).

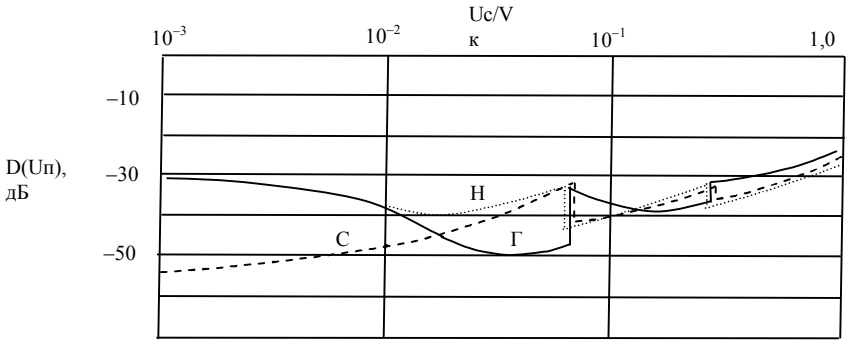



Рис. Залежність дисперсії шумів декодування D(Uп) від миттєвих значень сигналу Uc, нормованих до величини динамічного діапазону Vк;
С, Н, Г – коди: симетричний, натуральний, Грея

Як видно, при низьких рівнях сигналу, що надходить на вхід каналу ТЧ системи з ІКМ, суттєве зниження дисперсії шумів декодування дає симетричний код, при середніх рівнях сигналу перевагу має код Грея, а при високих рівнях сигналу всі коди приблизно однакові.

5. У системах з ІКМ широке використання знаходять для кодування миттєвих відліків сигналу коди: симетричний (європейський стандарт), натуральний (американський стандарт), Грея (спеціалізована обробка сигналів). У кожного із них своя область мінімізації шумів декодування в залежності від рівня вхідного сигналу та його ймовірнісних характеристик. Це стало мотивацією пошуку певного гібридного алгоритму кодування із врахуванням найбільш прийнятних характеристик кожного коду. Варіант такого кодування досліджувався і показав на основі моделювання певне покращення відношення сигнал/шум декодування на виході каналу. Слід зазначити, що можливість оптимального адаптивного кодування відліків сигналу розглядалася в [2], але використання воно не знайшло із-за складності реалізації; тому дані із [2] слід вважати граничними для оцінки степені наближення до них інших методів кодування, технічна реалізація яких може бути прийнятною.

6. Компандування (нелінійна компресія сигналу) дає змогу підвищити відношення сигнал/шум квантування, підсилюючи в більшій мірі слабі значення (відліки) сигналу і менше підсилюючи більші за значенням відліки. Пряму операцію підсилення на передавальній стороні здійснює компресор, а зворотну на приймальній стороні – експандер. В реальних системах до сигналу завжди добавляється певний шум апаратурного походження та шум з кабельної лінії і процеси перетворення здійснюються над сумішшю сигналу та шуму. Якщо абонент достатньо віддалений від апаратури, то основним буде шум, який накладається на сигнал в абонентській лінії. Разом із сигналом він надходить на компресор і аналого-цифровий перетворювач (АЦП). Збільшити відношення сигнал/шум перед АЦП, а, отже, і на виході каналу, можна, якщо компандер винести з апаратури в кінцевий абонентський апарат. Сигнал отримує в апараті відповідне підсилення при незмінності потужності шумів в абонентській лінії і відношення сигнал/шум перед АЦП зростає. Для технічної реалізації телефонний апарат необхідно доопрацювати, розмістивши в ньому компандер. Відповідні зміни повинні бути реалізовані і в апаратурі.

7. Статистика помилок в лініях зв’язку показує [3], що найбільш ймовірними із них є однократні, двократні та трикратні. На них припадає приблизно 90% усіх сполук помилок. Тому питання захисту від помилок відноситься насамперед до цієї серії помилок. Ймовірнісні характеристики помилок можуть бути розраховані на основі конкретної математичної моделі, прийнятної для заданої лінії зв’язку. Щодо мовних сигналів, то із-за їх високої інформаційної надмірності дія помилок не приводить до таких наслідків, як при передачі даних. Сучасні модеми, які використовуються в АПД, мають свою систему захисту від помилок, але при цьому в каналах низької якості різко падає швидкість обміну. Саме на такі канали слід орієнтуватись у польовій системі зв’язку, враховуючи можливість РЕП. Тому доцільність використання додаткового захисту від помилок в каналах з ІКМ має суттєве підґрунтя. Реалізація захисту може здійснюватись використанням завадостійкого кодування із виправленням помилок, повторенням інформаційних кодових комбінацій стандартних кодів, спеціальною обробкою найбільш вагомих розрядів кодових комбінацій.

У літературі питання захисту від помилок розглядалося стосовно кодових комбінацій кожного окремого каналу. Можливість захисту всієї цифрової послідовності (240 біт) чи її кожної половини, а також можливість та ефективність повторення інформаційних комбінацій простого коду, використання спеціальної обробки його найбільш вагомих розрядів потребує подальших досліджень.

ЛІТЕРАТУРА

1. *Джон К.* Беллами. Цифровая телефония: Пер. с англ. – М.: Эко-Трендз, 2004. – 640с.

2. *А.И.Величкин*. Теория дискретной передачи непрерывных сообщений. – М.: Сов. радио, 1970. – 296с.

3. Статистика ошибок при передаче цифровой информации: Пер. с англ. – М.: Мир, 1966. – 304с.

Гулак Ю.С.(ЦНДІ ОВТ ЗСУ)
Долгаленко О.В. (ЦНДІ ОВТ ЗСУ)

# УДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ОБ'ЄКТІВ ТА ПІДРОЗДІЛІВ ЗБРОЙНИХ СИЛ ВІД ПОРУШНИКІВ

Як свідчить досвід останніх локальних війн та збройних конфліктів нашого часу, підготовка і проведення операцій (бойових дій) в сучасних умовах не здійснюється без широкого застосування засобів інформаційного впливу. У документі Держдепартаменту США „Операції сил XXI століття" від 1994 року констатується: „Початку всіх операцій в умовах мирного часу (і під час війни) повинно передувати проведення інформаційної війни". Досвід використання протиборчими сторонами новітніх інформаційних технологій та засобів впливу на свідомість людей свідчить про те, що інформаційні операції, стають, як правило, складовою частиною загального плану (сценарію) ведення операцій і бойових дій. Інформаційно-психологічні операції США, Великобританії, ФРН, Франції, інших іноземних державах давно стали одним з дієвих засобів досягнення національних цілей як у мирний, так і у воєнний час. Технологічно розвинуті країни світу постійно вдосконалюють науково-технічні можливості підготовки і проведення інформаційно-психологічних операцій. Супутникові системи розповсюдження інформації, теле- та радіомовні комплекси повітряного базування „Commando Solo", галогенні ефекти, радіоприймачі з фіксованими частотами, технології використання мережі Інтернет та електронної пошти в останнє десятиліття поповнили арсенал психологічної війни. Інформаційно-психологічні операції збройних сил США (Гренада, Панама, Перська затока, Югославія, Ірак) показали, що в загрозливий період вони забезпечують дезорієнтацію та зниження морально-психологічної стійкості військовослужбовців і цивільного населення до опору. Це дозволяє ще до початку бойових дій паралізувати волю до боротьби, досягнути певної раптовості нападу та за рахунок цього посилити ефективність дій своїх військ. Сьогодні війни з традиційною зброєю стають окремими елементами в загальній інформаційній війні, яка давно вийшла на рівень цивілізацій. Поняття „психологічна війна", „інформаційно-психологічна операція", „психологічна боротьба", „інформаційно-психологічне протиборство" і ін. використовуються сьогодні дуже часто і, як правило, характеризують такі методи боротьби, які безпосередньо не пов'язані зі збройною боротьбою. У вітчизняній науковій літературі ще не вироблено єдиної термінологічної бази, класифікації інформаційних і психологічних операцій. Сьогодні ще відсутня науково-методологічна база досліджень в цій галузі, несистематизовані погляди науковців щодо інформаційно-психологічного забезпечення застосування військ (сил) в сучасних локальних війнах і збройних конфліктах. Існує і багато інших проблем, особливо тих, що пов'язані з розвитком сучасних технічних засобів, технологічних програм, створенням і використанням новітніх технологій. Розглядається проблема удосконалення способів та засобів визначення місцезнаходження порушників території, що охороняється, за рахунок використання тепловізорів. Теоретичні основи теплової локації для цих потреб реалізовані в пристрої, який містить вузькоспрямовану антену, підсилювач високої частоти, детектор, фільтр низької частоти та індикатор, що забезпечує відображення місцезнаходження джерела теплового випромінювання. Цей пристрій дозволяє визначати наявність джерела теплового випромінювання, а також розраховує напрям на об'єкт випромінювання, так званий „пеленг". Недоліком відомих пристроїв виявлення порушників території, що охороняється, є його недостатні функціональні можливості, оскільки він здатний визначити лише пеленг та не спроможний визначити координати місцезнаходження порушника, оскільки для цього треба обробити принаймні два пеленги з двох різних місць. Щоб уникнути хибних тривог, кордон території, що охороняється, додатково обладнується третім каналом сканування, що розміщується між основними каналами, а територія додатково обладнується пристроєм перевірки. Результат визначення координат перетинання пеленгів передається на пристрій перевірки.

Гулак Ю.С.(НАОУ)

# ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ПІДГОТОВЦІ І В ХОДІ ВЕДЕННЯ ОБОРОННОЇ ОПЕРАЦІЇ ЗБРОЙНИМИ СИЛАМИ УКРАЇНИ

Зі вступом людства в еру електроніки до традиційних методів розвідки додалися технічні засоби електронної розвідки.

Дані технічні засоби розвідки (ТЗР) в змозі охоплювати великі відстані і простори, межі яких визначаються особливостями розповсюдження електромагнітних хвиль. Саме вони у наш час є основним засобом, який використовується для обміну інформацією за допомогою технічних засобів передачі інформації, яким притаманні різного роду випромінювання.

Технічна розвідка ведеться скрито. Часто неможливо встановити не тільки масштаби, але і сам фронт розвідувального проникнення, що має місце.

Для досягнення високої ефективності операцій (бойових дій) і повної реалізації бойових можливостей своїх військ, ТЗР відіграють головну роль, що можуть дозволити собі збройні сили економічно розвинених держав.

Виходячи з положень воєнної доктрини України, у разі розв’язування війни, завдання наших Збройних Сил полягатиме в тому, щоб відбити напад агресора, зірвати вторгнення його озброєних сил і забезпечити їх ураження. У досягненні цілей відбиття агресії противника особливе місце належить оборонній операції, в той же час надто складними і відповідальними етапами такої операції будуть її підготовка.

Тому виконання першочергових завдань щодо захисту інформації, забезпечення її конфіденційності та протидія ТЗР особливо при підготовці оборонної операції в сучасних умовах стає все більш складною проблемою, що зумовлено низкою обставин, основними з яких є: підвищення ролі автоматизації процесу управління військами та ускладнення шифрувальних технологій.

При підвищенні ролі та можливостей ТЗР в операціях, на що вказує аналіз війн та збройних конфліктів останнього десятиліття, великого значення набувають заходи із забезпечення скритності функціонування системи управління військами, що включають в себе створення комплексного захисту інформації та протидії ТЗР в інтересах застосування військ Збройних сил України.

Умови підготовки і ведення оборонної операції, організації і здійснення заходів скритності управління військами безсумнівно зроблять визначальний вплив на бойове застосування всіх родів військ і спеціальних військ, порядок роботи командира з організації операції (бою).

Однак, розроблені теоретичні положення і науково-обґрунтовані практичні рекомендації щодо скритності управління військами від розвідки противника при підготовці і в ході ведення оборонної операції на теперішній час, на жаль, не повною мірою адаптовані до змін, які відбулися в основних закономірностях і тенденціях розвитку збройної боротьби, існуючі методики оцінки скритності управління військами не завжди можуть бути застосовані та не дозволяють оцінити особливості підготовки оборонної операції, не враховують зміни організаційно-штатної структури об’єднань, з’єднань Збройних Сил України, форм та методів ведення збройних операцій у сучасних умовах.

Таким чином, з урахуванням вищевикладеного, виникає гостра необхідність у вдосконаленні методики оцінки скритності управління військами, розробці теоретичних положень з створення комплексної системи забезпечення скритності управління військами і практичних рекомендацій з її застосування при підготовці і в ході оборонної операції, що, враховуючи пріоритетну роль скритності в загальному об’ємі заходів, які проводяться, при підготовці і в ході оборонної операції, набуває великого оборонного значення. Без розв’язання цієї задачі говорити про підвищення ефективності ведення оборонної операції в цілому не можливо.

Гурський Т.Г. (ВІТІ НТУУ „КПІ”)
Марченко А.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Толюпа С.В. (ДУІКТ)

# ПЕРСПЕКТИВНІ НАПРЯМКИ РОЗВИТКУ ШИРОКОСМУГОВИХ СИСТЕМ РАДІОЗВ’ЯЗКУ

Розвиток безпровідного зв’язку супроводжується безперервною зміною технологій, в основі яких лежать стандарти стільникового зв’язку *GSM* і *CDMA*, а також стандарти систем передачі даних *IEEE* 802. Історично технології безпровідного зв’язку розвивалися двома незалежними напрямами – системи телефонного зв’язку (стільниковий зв’язок) і системи передачі даних (*Wi-Fi*, *WiMAX*). Але останнім часом спостерігається явна тенденція до злиття цих функцій. Більш того, об’єм пакетних даних в мережах стільникового зв’язку третього покоління (3*G*) вже перевищує об’єм голосового трафіку, що пов’язано з впровадженням технологій *HSPA* (*High Speed Packet Access*). У зв’язку з цим, саме поняття мереж наступного, четвертого, покоління (4*G*) нерозривно пов’язано із 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 3*G*”. Причому кожна з них займає свою нішу на ринку безпровідного зв’язку. Проте вимоги кінцевих користувачів до послуг, що надаються, постійно підвищуються. Мобільні мережі повинні використовуватися не тільки для стільникового зв’язку, але і для передачі відео, мобільного телебачення, музики і роботи з Інтернетом з високими швидкостями і якістю передачі. Саме з цією метою в рамках проекту співпраці в створенні мереж третього покоління 3*GPP* (3*G Partnership Project*) була почата розробка технології *Long-Term Evolution* (*LTE*).

*LTE* базується на трьох основних технологіях: мультиплексування за допомогою ортогональних несучих *OFDM* (*Orthogonal Frequency Division Multiplexing*), багатоантенні системи *MIMO* (*Multiple Input Multiple Output*) і еволюційна системна архітектура мережі *SAE* (*System Architecture Evolution*).

У порівнянні з раніше розробленими системами 3*G*, радіоінтерфейс *LTE* забезпечить поліпшені технічні характеристики. Зокрема, в *LTE* ширина смуги пропускання може варіюватися від 1,4 до 20 МГц, що дозволить задовольнити потреби різних операторів зв’язку, що володіють різними смугами пропускання. Також очікується, що *LTE* поліпшить ефективність використання радіочастотного спектра, тобто зросте об’єм даних, що передаються в заданому діапазоні частот. *LTE* дозволить досягти значних агрегатних швидкостей передачі даних – до 50 Мбіт/с для висхідного з’єднання (від абонента до базової станції) і до 100 Мбіт/с для низхідного з’єднання (від базової станції до абонента) (у смузі 20 МГц). При цьому повинна забезпечуватися підтримка з’єднань для рухомих абонентів (швидкість до 350 км/год). Зона покриття однієї базової станції – до 30 км в штатному режимі, але можлива у зонах радіусом понад 100 км.

Нова архітектура мережі *SAE* повинна забезпечити широке комерційне використання будь-яких послуг на основі *IP* і забезпечення безперервного обслуговування абонента при його переміщенні між мережами безпровідного доступу, які не обов’язково можуть відповідати стандартам *3GPP* (*GSM*, *UMTS*, *WCDMA* і т.д.).

В мережі з архітектурою *SAE* можуть застосовуватися вузли тільки двох типів – базові станції та шлюзи доступу. Зменшення кількості типів мережевих вузлів дозволить операторам зменшити витрати як на розгортання мереж, так і на їх подальшу експлуатацію.

Таким чином, в даний час широкосмугові системи радіозв’язку продовжують бурхливо розвиватися. Розробка та впровадження технології *LTE* є ще одним підтвердженням цьому та важливим етапом в процесі переходу до мереж четвертого покоління 4*G*.

Дідик В.О. (ВІТІ НТУУ „КПІ”)
Натальченко О.О. (ВІТІ НТУУ „КПІ”)
Шевченко Л.Ю. (ВІТІ НТУУ „КПІ”)

## ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ АСУ

Складові безпеки АСУ:

1) безпека комп’ютера;

2) безпека мережі;

3) безпека АСУ.

Під мережною безпекою розуміють усі питання пов’язані з взаємодією всіх пристроїв мережі. Це захист даних у момент їх передачі лініями зв’язку. І захист даних від несанкціонованого віддаленого доступу в мережі.

Цілісність – гарантія зберігання даними правильних значень, що забезпечуються забороною для неавторизованих користувачів яким-небудь чином змінювати, модифікувати, руйнувати чи створювати дані.

Класифікація погроз безпеці. Погрозою називається будь-яка дія спрямована на порушення безпеки АСУ. Реалізована погроза називається атакою.

Ризик – ймовірнісна оцінка величини можливого збитку, що може понести власник інформаційного ресурсу в результаті атаки.

Ненавмисні погрози викликаються помилками в проектуванні АСУ, помилками в програмному забезпечені., помилками в діях персоналу.

Навмисні погрози створюються шляхом дезорганізації роботи АСУ, виведення системи з ладу, проникнення в систему і несанкціонований доступ до даних. Типи погроз.

– незаконне проникнення в один із комп’ютерів під видом легального користувача;

– нелегальні дії легального користувача;

– „підслуховування” трафіка.

Політика інформаційної безпеки дає відповіді на наступні питання.

1. Яку інформацію захищати?
2. Який збиток при втраті чи розкритті тих або інших даних?
3. Хто чи що є можливим джерелом погрози, якого роду атаки на безпеку АСУ можуть бути початі?
4. Які засоби використовувати для захисту кожного виду інформації?

Антивірусна боротьба. Вірус представляє собою програму, яка самовідтворюється та здатна упроваджувати свої копії у файли, системні області, комп’ютерні мережі, а також приводити до порушення нормального функціонування комп’ютерів.

Антивірусами називаються програми, призначені для захисту даних від руйнування, виявлення і видалення комп’ютерних вірусів. Різновиди антивірусних програм:

– фільтри або сторожі;

– детектори;

– доктора чи фаги;

– ревізори;

– імунізатори чи вакцини.

ЛІТЕРАТУРА

1. *Олифер В.Г., Олифер Н.А.* Сетевые операционные системы. – СПб.: Питер, 2001. –538 с.

2. *Мамиконов А.Г.* Проектирование АСУ. – М.: Высшая школа, 1987. – 303 с.

3. *Липаев В.В.* Тестирование программ. – М.: Радио и связь, 1988. – 296 с.

4. *Шохин Б.П.* Комплексы средств отображения информации в АСУ. – К.: КВИРТУ, 1993. – 209 с.

Драглюк О.В. (ВІТІ НТУУ „КПІ”)
Лімaнська О.Л. (ВІТІ НТУУ „КПІ”)

# ДЕЦЕНТРАЛІЗОВАНІ ОДНОРАНГОВІ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ

На сьогоднішній день все більшого розвитку набувають стільникові мережі передачі даних. Якщо розглядати комп’ютерні мережі, то тут є вже досить велика кількість мереж типу p2p (Peer To Peer). eMule, uTorrent – це найбільш розповсюджені та відомі мережі такого типу. Дані мережі використовують свої власні протоколи передачі даних, комп’ютери в них виступають односчасно як клієнтами так і серверами. Всі вони знаходяться на одному рівні, а така мережа називається одноранговою. Такі мережі в основному використовуються як файлообмінні, а компьютери – як місця зберігання даних та передачі їх іншим клієнтам, для забезпечення їх роботи необхідне спеціалізоване програмне забезпечення.

Розвиток знайшли також розподілені децентралізовані мережі, які можуть самоорганізовуватись та управляти необмеженим числом вузлів з мінімальними витратами процесорного ресурсу і пам’яті. Завдяки цьому в майбутньому можлива побудова всесвітньої розподіленої, анонімної і не контрольованої мережі, окремо від Інтернету, без підтримки будь-яких служб, провайдерів і тому подібного. Така мережа складається з комп’ютерів, фізично сполучених один з одним, тому немає необхідності надбудови над вже існуючою мережею. Інакше кажучи, використання таких мереж може замінити третій рівень моделі *OSI* своїми власними протоколами. Прикладом таких мереж є мережа *NETSUKUKU*, що використовує свій власний протокол динамічної маршрутизації *Npv7_HT*.

Протокол *Npv7* – побудований на основі теорії фракталів, а сама мережа розглядається як фрактал. Для розрахунку всіх необхідних шляхів зв’язку вузла з рештою всіх вузлів протокол використовує особливий метод, званий *Quantum Shortest Path Netsukuku* (*QSPN*). Фрактал – це математична структура з дробовою розмірністю, яка володіє властивістю рекурсивності: кожна її частина є зменшеною копією цілого. Тому можливе велике стискування структури, яка може безмежно розширюватися. А це означає, що потрібно всього лише декілька кілобайт для зберігання всієї карти маршрутів мережі. Саму структуру маршрутної карти можна розглядати як висококластеризований граф вузлів.

З іншого боку, *QSPN* є метаалгоритм в тому сенсі, що не слідує ніяким математичним правилам, а використовує випадковість і хаос, які не вимагають складних обчислень. *QSPN* виконується в реальних мережах, вузли посилають *QSPN* пакети для створення мережі. З цієї причини не завжди вірне твердження, що певний пакет буде відісланий раніше якого-небудь іншого.

Протокол *Npv7* може використовуватися в будь-якій ситуації, коли необхідно з’єднати кінцеві пристрої між собою а також може бути впроваджений в будь-які комунікаційні системи, які зараз використовуються.

ЛІТЕРАТУРА

1. *Кормен Т.*, *Лейзерсон Ч.*, *Ривест Р.* Алгоритмы: построение и анализ, М.: МЦНМО, 1999.

2. *Прохода А.Н.* Обеспечение интернет-безопасности. Практикум: учеб. пособие для вузов/ *А.Н. Прохода.* – М.: Горячая линия-Телеком, 2007. – 180 с.

3. *Галицкий А.В.*, *Рябко С.Д.*, *Шаньгин В.Ф.* Защита информации в сети – анализ технологий и синтез решений / *А.В. Галицкий*, *С.Д. Рябко*, *В.Ф. Шаньгин*. – М. : ДМК Пресс, 2004. – 616 с.

Драчук О.В. (ВІТІ НТУУ „КПІ”)

# ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ВНЕСЕННЯ ПОМИЛОК ДЛЯ ПОШУКУ ДЕФЕКТІВ БЕЗПЕКИ В ПРОГРАМНИХ ПРОДУКТАХ

Технологія внесення помилок (*fault injection*) вже більше півстоліття використовується для перевірки відмовостійкості апаратних пристроїв. По мірі переходу від аналогових технологій до цифрових об’єм використовуваного програмного забезпечення росте по експоненті. Виникає резонне питання: які існують засоби перевірки надійності програм?

Протягом останніх десятиліть було розроблено ряд технологій внесення помилок для виявлення серйозних проблем в комерційних програмних продуктах. Більшість із цих програмних систем були створені на засоби комерційних фірм і, відповідно, відсутні у арсеналі програмного забезпечення структурних підрозділів Збройних Сил України. Програмні системи внесення помилок – такі, як *DEPEND*, *DOCTOR*, *Xception*, *FERRARI*, *FINE*, *FIST*, *ORCHESTRA*, *MENDOSUS* і *ProFI* – продемонстрували, що технологія внесення помилок дозволяє успішно виявляти різні недоліки комерційних програм. При розробці більшості із перерахованих технологій дотримувалася одна мета – представити для розробників засоби для перевірки відмовостійкості програмних продуктів.

Лише деякі із цих рішень в комерційному і приватному секторах розроблялись для пошуку дефектів безпеки в програмних продуктах. Однак в сучасному світі безпека з кожним днем відіграє все більш важливу роль, тому і потреби в технологіях, що забезпечуватимуть її підвищення в програмних продуктах, постійно ростуть.

Зазвичай спеціалісти по забезпечуванню якості, які працюють у відділах безпеки структурних підрозділів Збройних Сил України, використовують методи ручного аналізу (в першу чергу – це реконструкція і аналіз вихідних текстів) для виявлення потенційних проблем безпеки в програмних продуктах. При всій корисності цих навиків для кваліфікованого спеціаліста, вміння використовувати автоматизовані технології відіграє важливу роль. Використовуючи знання, отримані на стадії реконструкції, аналітик може швидко налаштувати свій програмний додаток для автоматичного тестування, та підвищити таким чином ефективність своєї роботи.

Одним із найбільш вдалих аспектів перевірки відмовостійкості полягає в тому, що якщо скласти список всіх програмних помилок, допущених програмістами світу за скільки-небудь тривалий термін часу, а потім побудувати тест для кожної помилки в тестовому додатку, то, зрештою, вдалось би забезпечити безпеку цього додатку.

Написання програм на основі технологій внесення помилок стимулює вивчення класів атак та сприяє кращому їх розумінню. З кожним новим класом атаки (вивченим або виявленим самостійно) зустрічаються нові прийоми і методи, які сприяють вивченню інших. А автоматизація цього процесу дозволяє виявити дійсні помилки в захисті та підвищити безпеку інформаційних систем структурних підрозділів Збройних Сил України.

ЛІТЕРАТУРА

1. *Козиол Дж., Личфилд Д., Эйтэл Д., Энли К.,* и др. Искусство взлома и защиты системы. – Спб.: Питер, 2006. – С. 210 – 223.

2. *Норткат С., Новак Дж.* Обнаружение нарушений безопасности в сетях, 3-е издание.: Пер. с англ. – М.: Издательский дом „Вильямс”, 2003. – С. 121 – 155.

3. *Андроник А.М., Богдано В.В., Домуховский Н.А., Коллеров А.С., Синадский Н.И., Хорьков Д.А., Щербков Н.Ю.* Защита информации в компьютерных сетях. Практический курс: учебное пособие. Екатеринбург: УГТУ-УПИ, 2008. – С. 48 – 123.

к.військ.н. Дружинін С.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Климович О.К. (ВІТІ НТУУ „КПІ”)
Захараш О.М. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ СТРАТЕГІЙ МАРШРУТИЗАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Одним з найбільш важливих завдань в телекомунікаційній мережі військового призначення являється використання необхідної стратегії маршрутизації для мережної архітектури. Ретельний аналіз функціонування мережі та потенційних можливостей її росту допоможе виявити проблеми та оптимальні шляхи їх вирішення. Значну роль відіграє проблема вибору стратегії маршрутизації повідомлень для забезпечення нормованої якості обслуговування в телекомунікаційній мережі військового призначення.

Мета даного напрямку дослідження полягає у розгляді та визначені можливості використання ряду аналітичних моделей для різних типів стратегій маршрутизації. Відповідно до цього проведений аналіз процедур маршрутизації відповідно до статичних і динамічних стратегій. Враховуючи переваги й недоліки процедур маршрутизації у практичних ситуаціях сформульовані стратегії, які можуть мати деякі з бажаних переваг обох процедур.

Запропоновано використовувати квазістатичну процедуру маршрутизації, у якій зміни напрямків зв’язку будуть тільки в даних інтервалах часу й (або) щораз, коли відбуваються надзвичайні ситуації в телекомунікаційній мережі військового призначення. При зростанні трафіку та затримок у необхідній секції мережі процедура маршрутизації зі статичної стратегії змінюється на динамічну і навпаки.

ЛІТЕРАТУРА

1. *Дружинин С.В., Климович О.К.* Анализ протоколов маршрутизации в информационно-телекоммуникационной сети автоматизированной системы управления специального назначения // Сборник научных трудов Харьковского университета Воздушных Сил им. И. Кожедуба „Системы обработки информации”. – 2006. – №5(11). – С. 85 – 88.

2. *Нюнькина Ю.П., Скатков А.В.* Игровая маршрутизация трафика в сети передачи данных, классический и квантовый подходы // Радіоелектронні і комп’ютерні системи. – 2006. – №7(19). – С. 185 – 190.

3. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.

4. *Хабракен Д.* Как работать с маршрутизаторами Cisco. – М.: ДМК Пресс, 2005. – 320 с.

5. *Стасєв Ю.В., Рубан І.В., Дуденко С.В., Сумцов Д.В., Тимочко О.І.* Комп’ютерні мережі. Технології, протоколи та моделювання: Навчальний посібник. – Х.: ХУПС, 2005. – 359 с.

6. *Амато В.* Основы организации сетей Cisco. – М.: Издательский дом „Вильямс”, 2004. – 512 с.

7. *Королев А.В., Кучук Г.А., Пашнев А.А.* Управление сетевыми ресурсами. – Х.: ХВУ, 2004. – 272 с.

8. *Кривошеєв Є.А., Климович О.К., Скуйбіда В.Ю.* Модель гібридної маршрутизації в мережах з комутацією пакетів // Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2004. – №4. – С. 95 – 101.

к.військ.н Дружинін С.В. (ВІТІ НТУУ „КПІ”)
Рвачова Н.В. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ВИЗНАЧЕННЯ ДОСТУПНОЇ ДЛЯ ТРАФІКУ ДАНИХ ПРОПУСКНОЇ СПРОМОЖНОСТІ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

Узагальнена модель телекомунікаційної мережі містить велику кількість як проміжних, так і кінцевих вузлів, кожен з яких обслуговується згідно із вимогами та можливостями мережі в конкретний момент часу. Інтенсивність зміни завантаженості мережі (пропускної спроможності) залежить від багатьох факторів, таких як: кількість одночасно організованих з’єднань; вимог до якості обслуговування кожного потоку; розміру буферної пам’яті маршрутизаторів; швидкості та алгоритму обробки черг; типу інформації, що передається [1]. Для повноцінного завантаження телекомунікаційного каналу мережному додатку слід знати пропускну спроможність, яка доступна для передачі даного потоку [2]. Знаючи доступну пропускну спроможність можна керувати передачею трафіку та формувати такі його характеристики, які відповідатимуть реальному стану мережі та виключать її перевантаження.

Пропонується методика визначення доступної для трафіку даних пропускної спроможності телекомунікаційної мережі, суть якої полягає у визначенні стану завантаженості мережі для конкретного потоку даних у будь-який момент часу. Відомо, що загальна пропускна спроможність мережі – це пропускна спроможність її найвужчого місця. Ресурси каналу постійно перерозподіляються між користувачами у відповідності із дисциплінами обслуговування. Тобто, вільна частина пропускної спроможності мережі змінюється у часі. Визначення пропускної спроможності відбувається для потоку заявок, який формується згідно із стандартними протоколами телекомунікаційних мереж. Тому інтервал часу між генерацією сусідніх заявок задається випадковою величиною, розподіленою за експоненціальним законом. Якщо інтенсивність цього потоку менше або дорівнює частині пропускної спроможності, що не використовується, то приймається рішення про обслуговування потоку, інакше – формується відмова. Для визначення частини зайнятих ресурсів мережі, додаються інтенсивності усіх потоків, що в даний момент часу займають канал. Різниця між значенням загальної пропускної спроможності каналу та сумарним значенням інтенсивності передачі даних є доступною кількістю ресурсів каналу. Доступна пропускна спроможність для потоку даних буде відповідати мінімальному значенню пропускної спроможності кожного з каналів мережі.

На основі запропонованої методики створено імітаційну модель процесу передачі інформації телекомунікаційною мережею. Імітаційна модель побудована з використанням блоків з бібліотеки Simulink у програмному середовищі MatLab [3]. Визначено кількісні значення доступної пропускної спроможності для трафіку даних при наявності конкуруючого потоку, інтенсивність якого змінюється у часі. Отримано дані щодо черг, які утворюються у буферних пристроях проміжних вузлів та кількості втрачених сегментів. Ряд експериментів, проведених з використанням імітаційної моделі, довів адекватність та ефективність використання методики під час моделювання телекомунікаційних мереж. Запропоновану методику визначення доступної для трафіку даних пропускної спроможності доцільно використовувати для розробки методів управління інтенсивністю відправки даних у телекомунікаційних мережах.

ЛІТЕРАТУРА

1. Таненбаум Э. Компьютерные сети.: Пер. с англ. – Спб.: Питер, 2002. – 848 с.

2. Кучерявый Е.А. Управление трафиком и качество обслуживания в сети Интернет. – СПб.: Наука и техника, 2004. – 336 с.

3. Дьяконов В.П. MATLAB 6/6.1/6.5 + Simulink 4/5. Основы применения. Полное руководство пользователя / Дьяконов В.П. – М.: СОЛОН-Пресс. – 2002. – 768 с.

к.військ.н. Дружинін С.В. (ВІТІ НТУУ „КПІ”)
Янсонс Я.В. (ВІТІ НТУУ „КПІ”)
Шинкарьов М.М. (ВІТІ НТУУ „КПІ”)

# ІМІТАЦІЙНА МОДЕЛЬ ДЛЯ ВИЗНАЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В МЕРЕЖАХ IP ТЕЛЕФОНІЇ

Якість передачі інформації – один із основних показників для користувачів. Якість передачі характеризувалася ступенем задоволення абонента. Розвиток будь-якої технології передачі призводить до необхідність дослідження якісного рівня передачі. Не достатньо вже лише передати данні, їх треба передати якісно.

На сучасному етапі розвитку телекомунікаційних мереж гостро постає питання не лише дослідження, а й забезпечення інтегральної якості обслуговування [1]. Телекомунікаційні мережі набули максимального поширення, як за територією так і за галуззю в якій використовуються [2]. Через факт зрощування послуг (аудіо, відео, данні) та мереж надання цих послуг (проводові, безпроводові), виникають певні труднощі для забезпечення показника якості обслуговування класичними методами. Викає багато спірних питань, щодо керування процесом забезпечення якості обслуговування. Подібне керування може бути, як централізоване [3], так і розподілене [4]. До головних недоліків відносять низьку пропускну здатність центру керування, низьку живучість мережі, складність керування та інші. Розвиток розподілених центрів керування спрямований на вирішення задач покращення процесу керування та відповідно на забезпечення належної якості обслуговування. Більшість розглядаємих систем підтримують стандарт взаємодії відкритих систем (OSI). Але якщо в межах виконання своїх функцій за призначенням недоліки майже відсутні, то при виконанні складної оптимізаційної задачі керування забезпеченням якості обслуговування, взаємодія протоколів та інтерфейсів є недостатньою. Як варіант вирішення цього недоліку може бути застосування крос-рівневої взаємодії [5]. Головною перевагою крос-рівневої архітектури є можливість взаємодії між різними (несусідніми) рівнями стеку протоколів.

В даній роботі пропонуються імітаційна модель для визначення якості обслуговування апаратури в мережах IP телефонії. Перевагами даної моделі є можливість емулювання процесів характерних для певного середовища. Модель дозволяє дослідити вплив багатьох негативних факторів на якість передачі мовних сигналів. Такими негативними факторами є: обмеження пакетів для передачі, різного роду затримки, джиттер, ймовірність втрати пакетів, ймовірність спотворення пакетів, ширина смуги пропускання, варіанти роз’єднання.

Можливість дослідження якості передачі є одним із етапів на шляху до вирішення задачі забезпечення необхідної якості обслуговування. В якості моделі каналу передачі інформаційних сигналів використовується емулятор каналу, замість будь-якої математичної моделі каналу. Перевагою такого підходу є високий коефіцієнт кореляції результатів отриманих за допомогою реальних каналів і каналів створених емуляторами.

Таким чином, зростає потреба у високоякісних послугах. Організації, що відповідають за розробку та впровадження вимірювальної та регулювальної апаратури в найближчому майбутньому зіткнуться з проблемою забезпечення якості обслуговування різноманітних послуг, що надаються одночасно по різного роду каналах та у системах з різною архітектурою. Імітаційні моделі подібного плану здатні забезпечити вирішення цих питань.

ЛІТЕРАТУРА

1. *Farrel A.* Network quality of service: know it all. – Morgan Kaufmann, 2008. – 351 p.

2. *Zhu H., Chlamtac I.* QoS for Multimedia Services in Wireless Networks // Resource management in wireless networking. – Springer, 2005. – P. 1 – 34.

3. *Дымарский Я.С.* Управление сетями связи. – М.: ИТЦ „МК”, 2003. – 384 с.

4. Wang F. Y. Networked control systems: theory and applications - Springer, 2008. – 352 p.

5. Ibnkahla M. Adaptation and cross layer design in wireless networks – CRC Press, 2009. – 526 p.

Єсаулов М.Ю. (ВІТІ НТУУ „КПІ”)

# АЛГОРИТМ ОБ’ЄКТИВНОЇ КЛАСТЕРИЗАЦІЇ ЗАГРОЗ БЕЗПЕКИ

Поняття небезпеки пронизує поле інформаційної безпеки. Ми використовуємо такі терміни, як „небезпека управління”, „оцінка небезпеки”, „модель загроз” і „аналіз ризиків” щодня й ці теми самі собою виявляють предмет незліченних документів і статей.

Аналіз ризиків є складовою частиною діяльності з інформаційної безпеки. Загальне поняття життєвого циклу інформаційної безпеки включає ідентифікацію ризиків, як ключовий компонент. Аналіз ризиків за суттю використовується для ідентифікації й оцінки загрози.

У роботі [1] автори дають більш складне визначення аналізу ризиків і визначають це, як „асистематичний процес дослідження загроз, що стоять перед ІТ-активами, уразливості цих активів і свідчення вірогідності того, що ці загрози будуть усвідомлені”. Таким чином, аналіз ризиків був традиційним шляхом ідентифікації загроз відносно ІТ-активів та кількісного визначення вірогідності появи загрози й уразливості ІТ-системи, що викликала цю загрозу. Аналіз ризиків, таким чином, вважають за достатній механізм забезпечення безпеки ІТ-активів, які є, головним, чином фізичними, та оцінки загроз і вразливості ІТ-системи, які можуть бути оцінені за допомогою якісних або кількісних методів. Відповідно до аналізу ризиків, оцінені загрози мають бути належним чином керовані. Управління ризиками включає визначення першочергових загроз, які повинні бути зменшені до прийнятного рівня із застосовуванням відповідних заходів і засобів безпеки. Тому постає задача кластеризації визначених загроз безпеки ІТ-активів за рівнями небезпеки.

Розглядається задача об’єктивного (тобто та, що не потребує особистої участі дослідника) поділу $n$-мірного простору ознак $x_1, x_2, x_3, x_4,..., x_n$ загроз безпеки на області (кластери), що відповідають компактним групам зображень. Кожне зображення задане рядком (точкою) вибірки спостережень. Об’єктивна кластеризація зображень (точок) заснована на переборі множини кластеризацій-претендентів за критеріями несуперечності з метою вибору оптимальної, самої несуперечливої кластеризації. Необхідність модифікації алгоритму пов’язана з бажанням усунути суб’єктивний характер поділу вибірки даних на дві частини й застосувати при виборі кластеризації спосіб виміру відстаней, використовуваний в „методі найближчого сусіда” (метод без розрахунків среднеквадратичних відстаней).

Розглянемо алгоритм об’єктивної кластеризації загроз безпеки.

1. Вихідні дані діляться на чотири підвиборки $A \cap B$ и $C \cap D$ і узгодження кластеризации, обраних на підвиборках $A \cap B$, із кластеризациями на $C \cap D$ використовується для відсівання „неправильних” несуперечливих кластеризации (операція регуляризації вибору кластеризації). Уводиться поняття диполів – пар близько розташованих друг від друга точок. Одна вершина диполя надходить в одну підвиборку, а інша – в іншу. Таким способом досягається найбільша взаємна близькість точок утворюючих підвиборки.

2. Перебір кластеризації виконується за спрощеним алгоритмом, що не вимагає розрахунків среднеквадратических відстаней між точками.

Перебір за диференційними критеріями (що мають властивості зовнішніх критеріїв) як критерія балансу дискретизації, так і критерія несуперечності дозволяє замінити людину-експерта з його суб’єктивними поглядами про кількість і склад точок кластерів (класів).

ЛІТЕРАТУРА

1. *Mariana Gerber,* Rossouw von Solms. Management of risk in the information age. Computers & Security №24, 2005. – P. 16 – 30.

2. *Ивахненко А.Г., Ивахненко Н.А.* Непараметрические прогнозирующие модели МГУА. Автоматика №2, 1989. – С. 3 – 12.

3. *Ивахненко А.Г., Ивахненко Н.А.* Модифицированный алгоритм объективной кластеризации данных. Автоматика №2, 1986. – С.11 – 19.

Загребельний О.Ю. (ВІТІ НТУУ „КПІ”)
Біленький А.В. (ВІТІ НТУУ „КПІ”)

# НЕЧІТКА СИСТЕМА УПРАВЛІННЯ ДОСТУПОМ В МОБІЛЬНИХ РАДІОМЕРЕЖАХ

Перспективні мережі зв’язку 4G передбачають використання мобільних радіомереж (МР) або MANET (Mobile Ad-hoc Networks). Під МР розуміється мережа радіозв’язку з динамічною, що самоорганізуються, архітектурою побудови, яка допускає відсутність базових станцій і фіксованих маршрутів передачі інформації [1]. Всі вузли мережі мобільні. Під вузлом мережі розуміється пристрій, побудований на основі ЕОМ, що реалізує функції маршрутизатора, та радіоінтерфейсу. Вузли обмінюються інформацією безпосередньо між собою або застосовують ретрансляцію пакетів. Одним із завдань при проектуванні системи управління МР є побудова ефективної підсистеми управління доступом [2]. Проте, ефективність застосування того або іншого методу доступу (МД) до радіоресурсу залежить від характеристик конкретної МР (число вузлів, пропускна спроможність радіоканалів тощо) і умов її функціонування (динаміки зміни топології, навантаження, виду трафіку тощо). Тому ідеального, „на всі випадки”, МД не існує. Таким чином, необхідно, щоб кожен вузол мережі самостійно оцінював поточну ситуацію і здійснював управління доступом (методами доступу) з урахуванням керуючих рішень на інших рівнях моделі OSI (Open System Interconnection) [3].

Існує декілька шляхів, щоб зробити МД для МР адаптивними, включаючи різні механізми встановлення зв’язку, запобігання зіткненням, контролю інтенсивності трафіку, комбінування МД та інші [4]. Враховуючи, що розробка методів управління доступом для МР є складним процесом, а керування доступом вимагає адаптивного рішення в реальному масштабі часу, пропонується нечітка система управління доступом в МР.

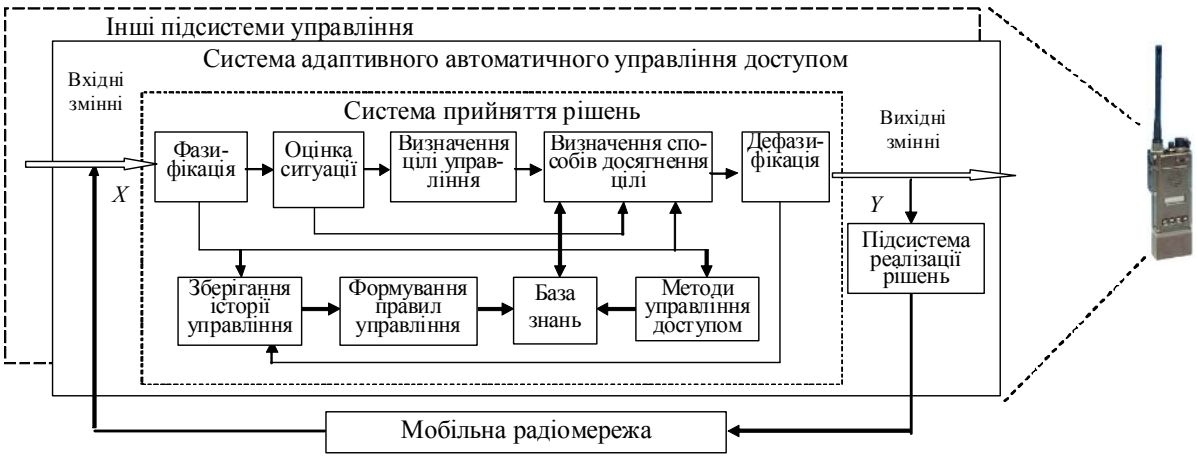



Рис. 1. Схема нечіткої системи управління доступом

## ЛІТЕРАТУРА

1. *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.

2. *Миночкин А.И., Романюк В.А.* Методы множественного доступа в мобильных радиосетях // Зв’язок. – 2004. – № 2.

3. *Малярчук М.В., Миночкин А.И., Романюк В.А.* Методология управления мобильными радиосетями // Труды 5-й НПК СИЭТ’04. – 2004. – С. 29.

4. *Farago A., Myers A.D., Syrotiuk V.R., Zaruba G.V.* Meta-MAC protocols: automatic combination of MAC protocols to optimize performance for unknown conditions // IEEE JSAC, vol. 18, № 9, sept. 2000.

5. *Креденцер Б.П., Ленков С.В., Миночкин А.И., Зубарев В.В.* Интеллектуализация управления мобильными радиосетями // Труды 5-й НПК СИЭТ’04. – 2004. – С. 28.

к.т.н. Залогін С.М. (ВІТІ НТУУ „КПІ”)
Іванков Ю.М.(ВІТІ НТУУ „КПІ”)
Малишкін В.В.(ВІТІ НТУУ „КПІ”)
Тамаровський В.В.(ВІТІ НТУУ „КПІ”)

# ОЦІНКА ЕФЕКТИВНОСТІ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ МАСОВОГО ОБСЛУГОВУВАННЯ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

У доповіді розглянутий аналіз роботи обчислювальної системи (ОС) массового обслуговування спеціального призначення, яку можна розглядати як сукупність програм і технічних засобів, розгорнутих на пункті управління або в пункті розподілу (комутації) каналів (повідомлень) для обміну інформацією в процесі управління військами (силами). Вона складається зі зв’язаних між собою робочих станцій (РС), які спільно використовують апаратні й програмні ресурси. Вона призначена для обслуговування якогось потоку заявок (повідомлень або „вимог”), що надходять у якісь випадкові моменти часу. Такими заявками можуть бути заявки, які виконують завдання функціональних підсистем:

– формування, доведення і контролю виконання завдань та розпоряджень;
– діловодства та електронного документообігу;
– інформаційно-розрахункової підсистеми;
– електронної пошти;
– відеоконференцзв’язку;
– інформаційно-довідкової підсистеми на базі Web-сервісів.

Обслуговування заявки триває якийсь випадковий час, після чого робоча станція звільняється й готова до прийому наступної заявки. Стан ОС міняється стрибком у моменти появи якихось подій (приходу нової заявки, закінчення обслуговування, або моменту, коли заявка залишає чергу). Випадковий характер потоку заявок і часу обслуговування приводить до того, що в якісь періоди часу на вході ОС може утворюватися (скапливаться) зайво велика кількість заявок; в інші ж періоди ОС буде працювати з недовантаженням або взагалі простоювати.

Таким чином, виникає завдання (проблема) про знаходження характеристик, що визначають ефективність роботи ОС і дозволяють оптимизувати її роботу незалежно від способу обробки інформації в ній. Такими характеристиками ОС є: відносна й абсолютна пропускні здатності, імовірність відмови заявок, середнє число зайнятих у роботі робочих станцій.

Для вирішення цієї проблеми в доповіді функціонування ОС описується через всі можливі її стани і інтенсивності переходу з одного в інше запропонованою математичною імовірнісною моделю у вигляді графа станів. Передбачається, що всі потоки подій, що переводять систему по гілкам графа, – найпростіші. Користуючись запропонованим графом, були складені й вирішені алгебраїчні рівняння для фінальних імовірностей станів ЛОМ. Отримані аналітичні вираження використалися для визначення таких характеристик ефективності ОС, як її відносна й абсолютна пропускні здатності, фактична продуктивність (при заданій кількості повідомлень, що обслуговують одною РС), імовірність відмови повідомлень, середнє число зайнятих у роботі РС.

При проектуванні польової мережі для заданих значеннях коефіцієнта навантаження обчислювальної системи спеціального призначення і імовірності відмови повідомлень було вирішено завдання визначення найменшого числа працюючих робочих станцій, здатних задовольнити задані вимоги.

Таким чином, проведений аналіз роботи обчислювальної системи масового обслуговування на основі запропонованої математичної імовірнісної моделі у вигляді графа станів ОС продемонстрував ефективність методу для одержання практичних результатів.

д.т.н. Замаруєва І.В. (ВІКНУ ім. Т.Шевченка)
Бабіч О.М.(в/ч А1906)

# МЕТОДИКА ВИЯВЛЕННЯ ОЗНАК МАНІПУЛЮВАННЯ СВІДОМІСТЮ В ІНФОРМАЦІЙНИХ ТЕКСТОВИХ ПОВІДОМЛЕННЯХ ЗМІ

Українському суспільству характерна зацікавленість політичними процесами. Виявлення в інформаційному просторі України інформації з ознаками маніпулювання свідомістю на користь певних політичних інтересів (моніторинг) є одним із пріоритетних завдань забезпечення інформаційної безпеки учасників політичних процесів. З цією метою проведено наукове дослідження з розробки методики виявлення ознак маніпулювання свідомістю в інформаційних текстових повідомленнях ЗМІ. Пропонується оцінювання ЗМІ на наявність маніпулювання свідомістю на основі визначення наступних складових: дані про джерело; дані про повідомлення. Кожна з цих складових розраховується на підставі даних про властиві їй параметри.

Дані про інформаційне джерело включають такі параметри: обсяг та охоплення мовлення, частоту виходу в ефір, мови віщання, тематику, відомства/комерційні структури, зацікавлені у його функціонуванні. Дані про повідомлення формуються на підставі оцінювання наступних його параметрів: актуальність змісту; семантична забарвленість та її спрямованість щодо певних учасників ситуації, про яку йдеться у повідомленні; наявність у повідомленні загальних ознак маніпулювання свідомістю; наявність факторів, що сприяють підвищенню ефективності впливу інформаційного повідомлення на цільову аудиторію, зокрема спеціальних мовних прийомів. На підставі визначених критеріїв апріорі оцінюється кожна складова ЗМІ з наданням вагових коефіцієнтів, і виділяються пріоритетні групи джерел, які потребують пильної уваги в ході моніторингу.

Внесок кожного вагового коефіцієнту в оцінку ступеню важливості параметру повідомлення розраховується за формулою:

$$q_n = \frac{x_n}{\sum_{i=1}^{K} x_i}; \qquad (1),$$

де $q_n$ – внесок вагового коефіцієнту $x_n$ в розпізнання ступеню важливості параметру; $x_n$ - ваговий коефіцієнт важливості параметру оцінювання;

$\sum_{i=1}^{K} x_i$ – сума всіх вагових коефіцієнтів важливості параметру оцінювання.

Для оцінки ступеня важливості складової використовуємо формулу:

$$G_j = \sum_{j=1}^{l} q_i; \qquad (2)$$

де $G_j$ – показник ступеню важливості складової ЗМІ;

$q_i$ – внесок вагового коефіцієнту в розпізнавання ступеню важливості складової ЗМІ;

$l$ – кількість показників, що характеризують параметр $G_j$.

На підставі оцінки параметрів кожної складової виявляються ознаки маніпулювання свідомістю в інформаційних текстових повідомленнях ЗМІ та приймається рішення про пріоритетність інформаційно-аналітичного опрацювання масиву джерел ЗМІ.

ЛІТЕРАТУРА

1. *Закон України* „Про основи національної безпеки України”, інфодиск „Законодательство Украины”.

2. *О.В. Литвиненко.* Спеціальні інформаційні операції та пропагандистські кампанії. http://psyfactor.org/infops/htm.

к.т.н. Заруднєв Д.І. (в/ч А1906)
Стейскал А.Б. (в/ч А1906)

# МАТЕМАТИЧНА МОДЕЛЬ ДИСКРЕТНИХ ПОВІДОМЛЕНЬ ЦИФРОВИХ СИСТЕМ РАДІОЗВ'ЯЗКУ

Як відомо, під інформаційною системою розуміють систему, яка функціонує на основі використання інформації про події, ситуації та процеси, які відбуваються в межах системи, що розглядається [1]. Системи управління та зв'язку є типовими інформаційними системами [1]. Прикладами цифрових систем зв'язку є системи передачі даних, радіорелейного та супутникового радіозв'язку. Стрімкий розвиток світових засобів передачі інформації обумовив найбільш велику різноманітність даних, що циркулюють саме в бездротових цифрових системах зв'язку.

Як показали теоретичні дослідження та досвід практичної роботи [2], цифрові бездротові системи зв'язку, як складові глобальної телекомунікаційної мережі, можуть бути носіями і джерелами інформації різного характеру та представляють безпосередній інтерес для різних спеціальних служб та відомств. В наслідок цього основною задачею даних структур є забезпечення ефективного інформаційного доступу до конфіденційних даних, що передаються каналами цифрових систем зв'язку. Аналіз відкритих джерел показав, що на сьогодні методологія, яка забезпечує ефективність інформаційного доступу до дискретних повідомлень (ДП) на самому початковому етапі їх аналізу – коли ДП представляє собою двійкову послідовність, яка отримана після демодуляції сигналу [3], та коли її ще неможливо віднести до будь-якого класу, потребує удосконалення та узагальнення.

Одним з початкових етапів, що застосовуються при дослідженні ДП, є проведення етапу моделювання. Як відомо, модель передує проведенню наступних більш прикладних етапів – розробок методів, методик, алгоритмів. Від правильності проведення процесу моделювання та вибору відповідної моделі напряму залежить подальше більш детальне і практичне дослідження дискретних повідомлень. На підставі вищевикладеного можна зробити висновок, що розробка математичної моделі дискретних повідомлень, що циркулюють в цифрових системах зв'язку, є актуальною задачею. Розглянемо дискретне джерело інформації, на виході якого з'являється послідовність букв або інших символів, які беруться з відповідного алфавіту $X = \{x_1, x_2, \ldots, x_n\}$. У разі синтезу математичної моделі дискретного джерела зазвичай вважають, що кожний з символів алфавіту в повідомленнях з'являється з апріорно відомою ймовірністю $p_k = P\{X = x_k\}, k = 1, \ldots, n$, $\sum_{k=1}^{n} p_k = 1$, де символ $P\{\cdot\}$ визначає ймовірність виконання умови, що стоїть в його дужках. В даному випадку $p_k$ – ймовірність появи символу $x_k$ з $X$. Для більшості ДП, які застосовуються практично, дані ймовірності відомі та достатньо встановлені експериментальним шляхом. Кожному символу алфавіту, що використовується, у взаємно однозначну відповідність ставиться послідовність бітів. Тобто текстові символи чи інші символи кодуються з використанням двійкового алфавіту (нумеруються у двійковій системі числення). Множину вказаних подій з відомим розподілом ймовірності його елементів називають ансамблем ті записують по різному [4]:

$$X = \begin{pmatrix} x_1, x_2, \ldots, x_n \\ p_1, p_2, \ldots, p_n \end{pmatrix} = \begin{pmatrix} \mathbf{x}^T \\ \mathbf{p}^T \end{pmatrix}; \quad \{X, \mathbf{p}\}.$$

По суті вектор $\mathbf{x}$ представляє собою сукупність незалежних випадкових величин, сумісна щільність розподілу яких дорівнює $P(\mathbf{x}) = \prod_{k=1}^{n} p_k$.

Якщо кожному символу $x_k$ азбуки $X$ поставлено у відповідність двійкове число, то його елементи дорівнюють *0* або *1* та створюють вектор $\chi_{k,q_k}$, другий символ якого вказує на розмірність вектора. В загальному випадку розмірність $q_k$ береться зростаючою зі

зменшенням ймовірності $p_k$ (це економно – коди, які передаються частіше, є більш короткими). Тому, більш простою математичною моделлю дискретного повідомлення $X$ є модель, яка представлена у вигляді таблиці (1) та назви рядків якої вказані в наведеній таблиці праворуч [4]:

$$X \to \begin{pmatrix} x_1, & x_2, & \cdots & x_k \\ \boldsymbol{\chi}_{1,q_1} & \boldsymbol{\chi}_{2,q_2} & \cdots & \boldsymbol{\chi}_{k,q_{n1}} \\ p_1 & p_2 & \cdots & p_k \\ m_1 & m_2 & \cdots & m_k \end{pmatrix}; \quad \begin{bmatrix} \lhd \text{ элементи алфавіта } X = \{x_{\mathrm{k}}\} \\ \lhd \text{ вектори двійкових кодів } x_k \\ \lhd \text{ ймовірність використання } x_k \\ \lhd\, m_k - \text{кількість елементів } x_{\mathrm{k}} \text{ в } X \end{bmatrix},$$

(1)

Побудована таким чином математична модель характеризується багатьма показниками. Наведемо деякі з них. Для конкретного повідомлення $X$ с заданим алфавітом випадковим є вектор $m = (m_1, m_2 \cdots m_n)^T$. В багатьох випадках в якості першого наближення розподілу цього вектору об'єму $N$ ( $N = m_1 + m_2 + \cdots + m_n$ ) приймається поліноміальний дискретний розподіл, який має наступний вигляд [5]:

$$P(m) = \frac{N}{m_1! m_2! \cdots m_n!} p_1^{m_1} p_2^{m_2} \cdots p_k^{m_n},$$

де $m_n$ – цілі числа; $p_k > 0, \quad k = 1, 2, \ldots, n; \quad p_1 + p_2 + \ldots + p_k = 1$.

Вирази для математичного очікування довільного елементу наведеного розподілу, а також його другого та третього центральних моментів елементів дорівнюють [5]:

$$\mu_{1k} = E(m_k) = n\, p_k; \eta_k = \sigma_k^2 = E(m_k - \mu_{1k})^2 = n\, p_k (1 - p_k), \eta_{kt} = -n(p_k p_i);$$

$$\eta_{kkk} = E(m_k - \mu_{1k})^3 = n p_k (1 - p_k)(1 - 2p_k), \eta_{kki} = -n p_k\, p_i (1 - 2p_k),$$

$$\eta_{kij} = 2n p_k p_i p_j, \quad k \neq i \neq j = 1, 2, \ldots, n.$$

При достатньо великій кількості елементів алфавіту, зазвичай ймовірності $p_k$ малі, тому при моментному описі $m$ можливо обмежитися використанням математичного очікування цього вектору і його кореляційною матрицею:

$$\boldsymbol{\mu} = n(p_{1,}, p_2, \ldots, p_n)^T = n\mathbf{p}^T, \quad M = n^2 \mathbf{p}\mathbf{p}^T.$$

Представлена у вигляді таблиці (1) модель є базовою та може виступати у якості прототипу для аналізу різних конкретних типів дискретних повідомлень. В кожному з конкретних випадків рядки базової моделі можуть уточнюватися і доповнюватися в залежності від досліджуємого ДП. Запропонована математична модель узагальнює процес аналізу дискретних повідомлень і дозволяє розділити їх аналіз на етапи, послідовно наближаючись до інформаційного наповнення, яке міститься у ДП. Математична модель орієнтована на повідомлення, наявних саме в високошвидкісних бездротових цифрових системах зв'язку. Це обумовлено складною структурою двійкових послідовностей, які притаманні даним системам. Тому ефективність інформаційного доступу до даних повідомлень неможлива без своєчасного аналізу кожного з етапів даної моделі.

ЛІТЕРАТУРА

*1.Левин Б., Шварц В.* Вероятностные модели и методы в системах связи и управления. – М.: Радио и связь, 1985. – 312 с., ил – (Статистическая теория связи . Вып. 24).

*2. Столлингс В.* Беспроводные линии связи и сети.: Пер. с англ. – М.: „Дом Вильямс", 2003. – 640 с.

*3.Гаранин М.В., Журавлев В.И., Кунегин С.В.* Системы и сети передачи информации: Учеб. пособие для вузов. – М.: Радио и связь, 2001. 336 с.

*4.Чернецкий В. И.* Математическое моделирование стохастических систем. –Петрозаводский гос. универс., 1994. – 488 с.

5.*Переверзев Е. С. и др.* Случайные сигналы в задачах оценки состояния технических систем. – К.: Наук думка, 1992. – 252 с.

Захараш О.М. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ МЕТОДІВ МОДЕЛЮВАННЯ ІМОВІРНІСНО-ЧАСОВИХ ХАРАКТЕРИСТИК МУЛЬТИСЕРВІСНИХ МЕРЕЖ ЗВ’ЯЗКУ

Сучасні темпи розвитку інформаційних і телекомунікаційних технологій призводять до того, що існуючі програмні засоби аналізу, моделювання і оптимізації телекомунікаційних мереж, які побудовані на моделях Ерланга для однорідного трафіку в двоточкових каналах, перестають відповідати сучасним вимогам.

У системах зв’язку відбувається перехід від моносервісних систем голосового зв’язку, що діють на принципах комутації каналів, до мультисервісних систем з комутацією пакетів для інтегральної передачі голосу, даних, відео і ін. з диференціацією і управлінням якістю послуг (QOS – Quality-of-Services). На сьогоднішній день послуги, які широко використовуються користувачами: на основі технології мобільного зв’язку з пакетною комутацією GPRS/EDGE – доступ в Інтернет, WAP – доступ, e-mail, доступ в корпоративні мережі, телематика. У зв’язку з цим виникає необхідність в засобах моделювання імовірнісно-часових характеристик (ІЧХ) систем зв’язку для оцінки якості послуг, заснованих на теорії багатовимірних розподілених черг з пріоритетним обслуговуванням для інтегрального трафіку в багатоточкових радіоканалах множинного доступу.

Найбільш поширеними методами розрахунку ІЧХ телекомунікаційних систем є імітаційне моделювання, а також аналітичні методи, які носять зазвичай імовірнісний характер і будуються на основі понять апарата теорії телетрафіка вірогідності і марківських процесів.

При аналітичному моделюванні процеси або об’єкти, які досліджуються, замінюються математичними моделями. Оскільки події, що відбуваються в телекомунікаційних мережах множинного доступу, носять випадковий характер, то для їх вивчення найбільш відповідними є імовірнісні математичні моделі теорії масового обслуговування. Об'єктами дослідження в теорії масового обслуговування є системи масового обслуговування і мережі масового обслуговування.

Сучасні зарубіжні програмні засоби, такі як COMNET III (CACI Products), BONes Designer (Alta Group of Cadence Design Systems) OPNET Modeler (MIL3), NETSYS (Cisco), Netmaker XA (Make Systems) та ін. направлені, в основному, на побудову імітаційних моделей. Їх основний недолік – відсутність інформації про те, які припущення і спрощення закладені в моделі, тому помилки моделювання виявляються тільки на останніх стадіях проектування мережі.

Існуючі методи моделювання подібних систем мають ряд недоліків, до яких слід віднести: надання вхідних потоків заявок як простих, без урахування їх неоднорідності, вхідних втрат і розподілених в просторі черг; до уваги не беруться помилки в каналі, повторні потоки навантаження по переспросах, реальні системні параметри протоколів і дисципліни пріоритетного обслуговування.

Таким чином, завдання моделювання імовірнісно-часових характеристик телекомунікаційних мереж на сучасному етапі розвитку інформаційних технологій є актуальним, як і завдання поліпшення імовірнісно-часових характеристик шляхом адаптивного розподілу мережевих ресурсів.

## ЛІТЕРАТУРА

1. *Степанова И.В., Кондратов А.Г.* Методика выбора ресурса радиоканалов трафика в сетях мобильной связи // Труды Московского технического университета связи и информатики. – М.: „ИД Медиа Паблишер”, 2007. – С. 55 – 59.

2. *Markhasin A., Karpenok D.* Analytical Comparing of the QoS-Oriented MAC Protocols for Future Global All-IP-ATM Wireless Communications Environment // 8-я Международная конференция „Связь-2004”, Иссык-Куль, 22 августа – 29 августа 2004. – Том 2. – С. 197– 207.

Звір В.Б.(НАОУ)

# ШЛЯХИ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Збільшення пропускної здатності нових поколінь техніки зв'язку, тобто значний обсяг втрат інформації у випадку їхнього простою, викликали необхідність підвищення вимог до якості їхнього функціонування, розроблення й впровадження сучасних алгоритмів відновлення об'єктів технічної експлуатації. Якість функціонування елементів телекомунікаційної мережі (ТКМ) залежить від ефективності реалізації процесів задоволення потреб різноманітних комплексів зв'язку, від забезпечення умов функціонування техніко-технологічних структур, які реалізують функції ТКМ.

Оскільки у ході застосування ТКМ за призначенням, стан, як окремих комплексів зв'язку, так і системи в цілому може змінюватися, то ефективність функціонування мережі буде істотно залежати від достатності й своєчасності реалізації заходів технічної експлуатації. При цьому в стані непрацездатності можуть виявитися елементи ТКМ різних рівнів її побудови. Вибір конкретних способів компенсації цих змін залежить від виду інформаційних потоків та їхнього пріоритету.

Для часткового або повного усунення наслідків таких відмов необхідно передбачити виконання ряду заходів, спрямованих на відновлення елементів мережі. При цьому необхідне значення середнього часу відновлення порушених з'єднань, призначених для передачі повідомлень, залежить від категорій інформаційних потоків, що обслуговуються.

Від вибору способу реорганізації ТКМ істотно залежить швидкість реагування служб системи управління та системи забезпечення на зміну обсягів інформаційних повідомлень і станів ТКМ, а також їхня ефективність ( в тому числі і економічна).

З аналізу структурної ієрархії процесу технічної експлуатації слідує, що функції, які виконуються при її реалізації, зростають за складністю виконуваних завдань із ростом рівня їхнього впровадження. Чим вище рівень ієрархії системи прийняття рішення, тим вище ступінь узагальнення причин погіршення якості функціонування ТКМ. І навпаки, чим нижче рівень прийняття рішення, тим з більш унікальними подіями стикається особовий склад та органи управління при виконанні заходів технічної експлуатації.

Виходячи з цього можна виділити такі рівні відновлення інформаційних напрямків зв'язку: – рівень оперативного відновлення, призначений для відновлення з'єднань, які обслуговують інформаційні потоки найвищого пріоритету;

– рівень оперативно-технічного відновлення, що забезпечує відновлення частини елементів ТКМ з метою організації з'єднань для передачі всього обсягу повідомлення;

– технічний рівень відновлення, призначений для ремонту й відновлення технічного ресурсу обладнання, споруд з метою забезпечення своєчасної передачі в повному обсязі інформаційних потоків з необхідною якістю в усіх створених напрямках зв'язку.

Процес забезпечення експлуатаційної надійності ТКМ є складним комплексом взаємопов'язаних заходів, який вимагає великих фінансових і матеріальних витрат. Причому вони можуть, залежно від стану ТКМ, виконуватися на різних рівнях. Виконання заходів на кожному з них, вимагає різних витратних механізмів. Основною перешкодою при розгляді проблеми технічної експлуатації мережі є відсутність єдиного підходу до оцінки відмовостійкості мережі, який повною мірою описує процес функціонування ТКМ в різних умовах експлуатації. Основними труднощами на шляху пошуку такого підходу є складність одержання статистичних результатів необхідної точності, які були б придатні для аналізу і синтезу складних систем.

Для ТКМ спеціального призначення необхідно мати відповідний методологічний інструмент обґрунтування вибору засобів забезпечення заданої відмовостійкості й експлуатаційної надійності у ході еволюційного розвитку мережі з урахуванням зміни потреб в інформаційному обміні споживачів різних категорій.

Звягінцев О.Г (ІТС НТУУ „КПІ”)
к.т.н. Ладик О.І. (ІТС НТУУ „КПІ”)

# МОДЕЛЮВАННЯ СИСТЕМИ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ WCDMA

WCDMA (англ. *Wideband Code Division Multiple Access* – широкосмуговий CDMA) – технологія радіоінтерфейсу, яка обрана більшістю операторів стільникового зв’язку для забезпечення широкосмугового радіодоступу з метою підтримки послуг систем 3G [1].

Технологія оптимізована для надання високошвидкісних мультимедійних послуг, таких як відео, доступ до Інтернету та відеоконференції; забезпечує швидкості доступу до 2 Мбіт/с на коротких відстанях та 384 Кбіт/с на великих з повною мобільністю. Такі величини швидкості передачі даних потребують широку смугу частот,тому ширина смуги WCDMA становить 5 МГц.

Застосовані принципи функціонування окремих вузлів системи, побудованої на базі технології WCDMA, є досить складними в різних аспектах.

Моделювання – один з методів, який використовується при проектуванні і дослідженні як принципів роботи системи в цілому, а також її окремих вузлів.

Основна загальна мета моделювання полягає у спостереженні за системою, яка схильна до впливу зовнішніх або внутрішніх факторів при досягненні системою певного стану, який може бути як задано, так і невідомо, через відсутність інформації або за будь яких інших обставин.

Моделювання дозволяє визначити, чи може система функціонувати за таких умов чи ні, під час зміни стану. Залежно від реальної моделі мета розширюється та конкретизується [2].

При моделюванні окремих підрозділів системи WCDMA потрібні:

– розробка різних вузлів системи з можливістю імітації їх роботи;

– розробка блоків для задання параметрів моделювання;

– надання можливості перегляду осцилограм в різних точках моделі.

Повинні бути розглянуті наступні принципи побудови системи WCDMA, які характеризують як всю систему взагалі та і її відмінність від інших систем сімейства CDMA:

– принципи передачі в прямому та зворотному каналах; з урахуванням кодування чи без нього;

– принципи обслуговування абонентів за рівнями пріоритету та відповідно формування швидкостей передачі даних;

– окремі блоки базових станцій та розрахунок кількості абонентів, яких може обслужити одна базова станція за певних умов;

– формування кодованого потоку даних в каналах;

– узгодження швидкостей пакетної передачі даних та інше.

Кінцевим результатом дослідження є побудова багатоцільової моделі системи з можливістю її розвитку.

ЛІТЕРАТУРА

1. *Невдяев Л.М.* Мобильная связь 3-го поколения – М.: МЦНТИ, 2000. – 208с.

2. *Формализация и* компьютерное моделирование: Учебное пособие. – Омск: Омск. гос. ун-т, 2000. – 160 с.

Іваненко О.О. (ВІТІ НТУУ,,КПІ”)

# ШЛЯХИ УДОСКОНАЛЕННЯ ВОЛОКОННО-ОПТИЧНОЇ СИСТЕМИ ПЕРЕДАЧІ

У даний час, з метою підвищення ефективності функціонування систем зв’язку, планується широке впровадження волоконно-оптичних ліній зв’язку (ВОЛЗ). Це дозволить розв’язати існуючі проблеми по безперервності і своєчасності управління вже в найближчий час і відкриває подальші перспективи з покращення оперативно-технічних характеристик системи зв’язку в цілому.

Сучасні технології високошвидкісної передачі ґрунтуються у першу чергу на використанні оптоволоконних середовищ, які в теперішній час забезпечують максимально можливу пропускну спроможність. Саме тому технологія оптоволоконних середовищ передачі продовжує швидко розвиватись в усьому світі, в тому числі і в нашій країні. В майбутньому оптоволоконні середовища передачі повністю замінять електричні кабелі.

З всієї сукупності параметрів оптоволоконних систем зв’язку найважливішими є їх оптичні характеристики. Основною характеристикою, що контролюється на стадії будівництва є затухання оптичного волокна (ОВ). Воно вимірюється на вході оптичного кабелю (ОК), при монтажі кабельних муфт і зварюванні волокон кабелю, проведення приймально-здавальних випробувань ВОЛЗ.

У доповіді зроблено аналіз переваг волоконно-оптичного зв’язку, як найбільш перспективного на сучасному етапі розвитку телекомунікаційних технологій. Проведено порівняння застосування волоконно-оптичного лінійного тракту (ВОЛТ) з звичайними електричними кабелями, використання яких особливо важливо на мережах зв’язку спеціального призначення.

Розглянуті питання розробки вимірювального комплексу для контролю параметрів ВОЛТ, та необхідність його застосування.

Використання комплексів для автоматизованого контролю ВОЛТ дозволяє проводити:

1. Швидку локалізацію та ідентифікацію несправності ВОЛТ:

обрив оптичного кабелю із-за будівельних робіт, пожеж, автодорожніх та залізничних аварій, стихійних лих, або саботажу;

несправності, які викликані виходом з ладу компонентів волоконно-оптичної системи передачі (ВОСП), неякісними зварними з’єднаннями, збільшенням витрат через попадання у кабель вологи та пошкодженням комунікації в лінії.

2. Виявлення тенденції зміни параметрів лінії зв’язку, що дозволяє прогнозувати несправності ВОЛТ.

3. Проведення випробувань ВОЛТ одним кваліфікованим спеціалістом, що підвищує ефективність обслуговування великої довжини тракту при найменшій кількості персоналу.

4. Значне зменшення кількості обладнання, необхідного для обслуговування ділянок лінії, що зменшує проблеми, які пов’язані з використанням цього обладнання.

5. Спрощення проектування, будівництва та здачі в експлуатацію нових ліній передачі, завдяки стандартизованій документації, яка використовується разом з накопиченим досвідом експлуатації таких ліній передачі.

Таким чином проведений аналіз ВОСП показав перспективність даного напрямку досліджень. Розробка і застосування комплексів автоматичного контролю ВОЛТ дозволить підвищити ефективність роботи з ВОСП, як на етапі проектування, так і в процесі їх експлуатації та технічного обслуговування..

ЛІТЕРАТУРА

1. *Иванов А.Б.* Волоконная оптика: компоненты, системы передачи, измерения. − М.: „ Компания САЙРУС СИСТЕМС”, 1999.

2. *ДСТУ 3345-96*. Системи передавання волоконно-оптичні. Загальні технічні вимоги. К.: Держстандарт України, 1996.

к.т.н. Ільінов М.Д. (ВІТІ НТУУ „КПІ”)
Шафранський О.П. (ВІТІ НТУУ „КПІ”)
Шацький І.О. (ВІТІ НТУУ „КПІ”)

# РЕЗУЛЬТАТИ ЕКСПЕРИМЕНТАЛЬНОГО ДОСЛІДЖЕННЯ ЕЛЕКТРИЧНИХ ХАРАКТЕРИСТИК НИЗЬКОПРОФІЛЬНИХ АНТЕН НА ЦИЛІНДРИЧНІЙ ПОВЕРХНІ

Інтенсивний розвиток радіосистем зв’язку з рухомими об’єктами передбачає не тільки вдосконалення принципів її організації, впровадження нових завадостійких методів обробки сигналів, використання новітніх технологій в будівництві апаратури, але й пошук нових принципів у компонуванні найважливішого елемента кожної радіосистеми – антено-фідерного пристрою (АФП). Електричні характеристики АФП, особливо на низхідній ділянці радіолінії, визначають не тільки енергетичний потенціал, але і принцип організації системи зв’язку та її надійність в цілому. Тому питання щодо модернізації АФП старого зразка, котрі в наш час знаходяться в експлуатації, а також розробка нових зразків антенної техніки базових та абонентських станцій, є актуальними і мають практичне значення.

В останній час з’явилося ряд публікацій [1, 2, 3] з новими підходами щодо побудови АФП базових станцій, які направлені не тільки на покращення їх електричних характеристик, але і на суттєву масо-габаритних показників та покращення надійності антени в цілому. Новизна технічного рішення полягає в переході від випромінюючих елементів (ВЕ) антенної решітки електричного типу до ВЕ магнітного типу. В якості випромінювачів магнітного типу пропонується застосувати низькопрофільні антени (НПА). Випромінювач у вигляді НПА являє собою дві металеві пластини, одна з яких виконує функцію екрану, інша менших розмірів – випромінювач. В проміжку між пластинами, відстань між яками $h \leq \lambda$, де $\lambda$ – довжина хвилі, розміщується вузол збудження електричного чи магнітного типу. Такі антени в наш час широко використовуються як самостійні випромінювачі, наприклад: в абонентських комплектах навігаційної системи GPS, чи елементах антенних решіток [4]. НПА відносяться до антен дифракційного (магнітного) типу, оскільки випромінювання здійснюється з щілин, утворених екраном і верхньою пластиною.

Технічне рішення, запропоноване в роботах [1, 2, 3], передбачає виконання НПА циліндричної форми і носить виключно теоретичний характер. З метою підтвердження теоретичних результатів, приведених в роботі [3], був виготовлений робочий макет НПА на циліндричній поверхні з простою (квадратною) конфігурацією верхньої пластини. Дослідження проводилися в лабораторних умовах в діапазоні дециметрових хвиль для випадку вертикальної і горизонтальної поляризації випромінюючого поля. Під час досліджень було проведено вимірювання характеристики направленості методом обертанням антени, як для різних зразків НПА на циліндрі, так і для різних поперечних розмірів циліндричного екрана. Вимірювання здійснювались на циліндричному екрані з поперечним перерізом $ka = 1$ та $ka = 2$, де $ka$ – електричний радіус циліндричної поверхні. Перш за все була досліджена конструкція НПА на плоскому екрані з метою пошуку оптимальної точки для підключення живлення фідера. В подальшому даний робочий макет був перенесений на циліндричний екран, із відповідною корекцією верхньої пластини квадратної форми. Всі дослідження електричних характеристик НПА на циліндрі проходили з використанням стандартної вимірювальної апаратури.

Результати досліджень показані на рис. 1. На рис. 1а суцільною лінією зображена експериментально виміряна нормована діаграма направленості НПА з вертикальною поляризацією для значень $ka = 1$ та $ka = 2$, що відповідає значенню $2a/\lambda = 1/\pi$ та $2a/\lambda = 2/\pi$, де $a$ – радіус циліндра. Аналогічні дані, для НПА з горизонтальною поляризацією, зображені на рис. 1б. Пунктирна лінія, на кожному з графіків рис. 1, показує

теоретично розраховані діаграми направленості для кожного випадку розміщення НПА на циліндрі.

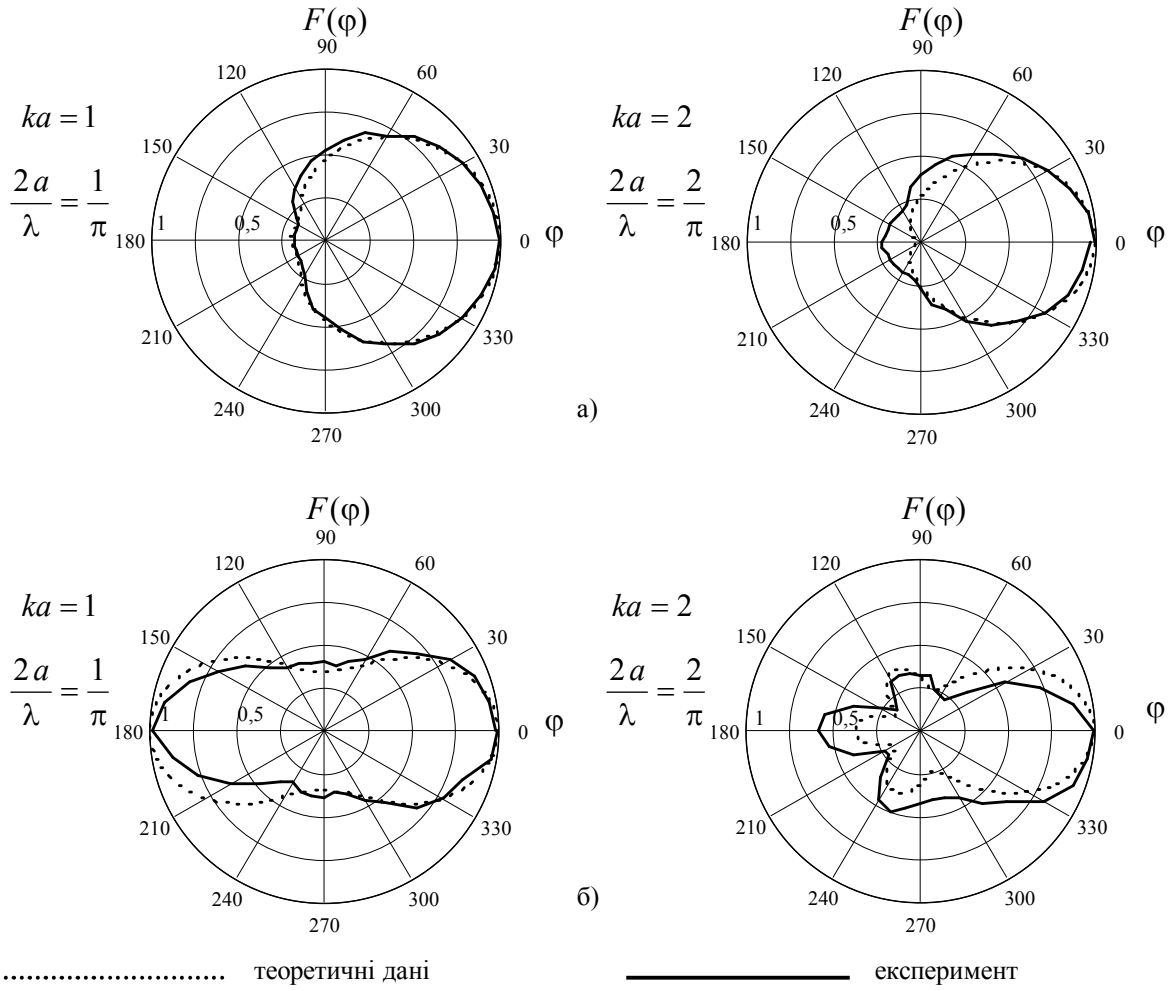



Рис. 1

Отримані результати дозволяють зробити наступні висновки: по-перше експериментальні зовнішні характеристики НПА на циліндричній поверхні практично повторюють результати теоретичних досліджень в роботі [3]; по-друге НПА на циліндричній поверхні з горизонтально-поляризованим випромінюванням, в залежності від значення $ka$ дозволяє формувати як квази ненаправлене ($ka = 1$) так і секторіальне ($ka = 2$) випромінювання в азимутальній площині. НПА з вертикальною поляризацією – лише секторіальне. Крім того, зменшення поперечних розмірів циліндричної поверхні дасть змогу покращити характеристику направленості в азимутальній площині.

ЛІТЕРАТУРА

1. *Luk Kuai-man, Lee Kai-Fong, Dashele J.S.* Analysis of the cylindrical-rectangular parch antenna. // IEEE Transactions on antennas and propagation, 1989. – AP-37 – № 2. – P. 143 – 147.

2. *Gabriel'yan D.D.*, *Zvezdina M.Yu.* The influence of impedance surface of cylinder on the dipole pattern. // Proceedings of 3-rd International Conference Antenna Theory and Techniques, 1999. – P. 113 – 116.

3. *Ильинов М.Д., Шацкий И.А., Цимура Ю.В.* Горизонтально поляризованные УКВ антенны с ненаправленным излучением в горизонтальной плоскости. // Збірник наукових праць ВІТІ НТУУ „КПІ”, 2009. № 2.

4. *Ильинов М.Д.* Микрополосковые антенные устройства. – М: ж. „Зарубежная радиоэлектроника”, 1981. № 10.

к.т.н. Ільінов М.Д. (ВІТІ НТУУ „КПІ”)
Шацький І. О. (ВІТІ НТУУ „КПІ”)
Шафранський О.П. (ВІТІ НТУУ „КПІ”)

# АНТЕНА БАЗОВОЇ СТАНЦІЇ СИСТЕМИ МОБІЛЬНОГО РАДІОЗВ’ЯЗКУ

На теперішній час широкого застосування набув відносно новий тип антен – низькопрофільні, 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 [1]. 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 $\lambda$ – довжина хвилі, одна з яких виконує функцію екрана, друга, певних розмірів, є випромінюючим елементом. В просторі між пластинами розміщується вузол збудження електромагнітних хвиль. На практиці найбільш широкого застосування набули НПА з простою формою верхньої пластини (випромінюючого елемента): прямокутною, квадратною та круговою. За рахунок введення діелектричного матеріалу в простір між пластинами, розмір випромінювача можна зменшити в $1/\sqrt{\varepsilon_r}$ раз, де $\varepsilon_r$ – відносна діелектрична проникність високочастотного діелектрика. Даний тип антен належить до класу щілинних випромінювачів, в даному випадку випромінювання здійснюється із торців щілин, утворених випромінювачем та екраном. Одним із нових напрямків розвитку техніки НПА є використання в їхній конструкції циліндричних екранів, що еквівалентно розміщенню низькопрофільного випромінювача над циліндричною поверхнею [2]. Застосування НПА з циліндричним екраном дозволить створити антени як з ненаправленою так і секторною характеристикою направленості (ХН) в азимутальній площині, що дасть змогу використати їх в якості антен базових станцій для систем мобільного зв’язку, а також в якості передаючих антен телевізійного мовлення.

В наш час основним типом передаючих антен базових станцій різних систем мобільного радіозв’язку, а також телерадіомовлення метрового та дециметрового діапазону довжин хвиль, є синфазні антенні решітки, побудовані на випромінюючих елементах електричного типу (симетричні вібратори різної конструкції). Вагомим недоліком таких антен є висока металоємність, низькі масо-габаритні показники, а відповідно і значні витрати на їх виготовлення. Дані недоліки можна усунути якщо компонувати антенні решітки на випромінюючих елементах у вигляді НПА з циліндричним екраном, тобто перейти від випромінюючих елементів електричного типу до випромінюючих елементів магнітного типу. Даний перехід дозволить не лише зменшити масу і габарити антенної решітки, а і значно покращити електричні характеристики антени та надійність її роботи в цілому.

Аналіз зовнішніх характеристик НПА можна здійснити на основі апертурної моделі [3], згідно з якою НПА, що має прямокутну форму випромінюючого елемента, розташованого над циліндром, можна розглядати як систему двох щілин прорізаних на циліндричній поверхні. Таким чином розв’язок задачі, про поле випромінювання НПА на циліндричній поверхні, зводиться до розв’язку дифракційної задачі про поле випромінювання щілини кінцевих розмірів на циліндрі, поздовжньої чи поперечної орієнтації відносно його осі.

Для горизонтальної поляризації апертурна модель НПА на циліндрі представляє собою систему із двох діаметрально протилежних поздовжніх щілин, прорізаних в металевому циліндричному екрані, за умови, що діаметр циліндра рівний $2a = \lambda/\pi$ або $ka = 1$, де $a$ – радіус циліндра. ХН даної кільцевої синфазної антенної решітки в азимутальній площині, згідно [4], має вигляд:

$$f(\varphi) = \left| \frac{2}{H_0^{2\prime}(ka)} + 2\sum_{i=1}^{\infty} j^n \frac{\cos(n\varphi) + \cos[n(\pi - \varphi)]}{H_n^{2\prime}(ka)} \right|. \quad (1)$$

Для поля випромінювання з вертикальною поляризацією апертурна модель НПА на циліндрі має вид двох поперечних щілин, рознесених вздовж осі циліндра на відстань $d = \frac{\lambda}{2\sqrt{\varepsilon_г}}$. Вираз для ХН в азимутальній площині має вигляд:

$$f(\varphi) = \left| \frac{1}{H_0^{2}(ka)} + 2\sum_{i=1}^{\infty} j^n \frac{\cos(n\varphi)}{H_n^{2}(ka)} \frac{\sin\frac{n\psi}{2}}{\frac{n\psi}{2}} \right|. \quad (2)$$

Вираз (2), на відміну від робіт [5, 6] по дифракції магнітних випромінювачів на циліндрі, отримано з урахуванням рівномірного розподілу ліній електричного поля $E_\tau$ на щілині кінцевих розмірів. Результати теоретичних розрахунків показані на рис. 1. На рис. 1а представлена діаграма направленості (ДН) випромінювача на циліндрі з горизонтальною поляризацією для двох випадків: $\varepsilon_г = 1$ і $\varepsilon_г = 4$ при $ka = 1$. На рис. 1б. показана ДН у випадку вертикальної поляризації для двох пари значень: $ka = 1$, $\psi = \pi$ і $ka = 2$, $\psi = \pi/2$ при $\varepsilon_г = 1$.

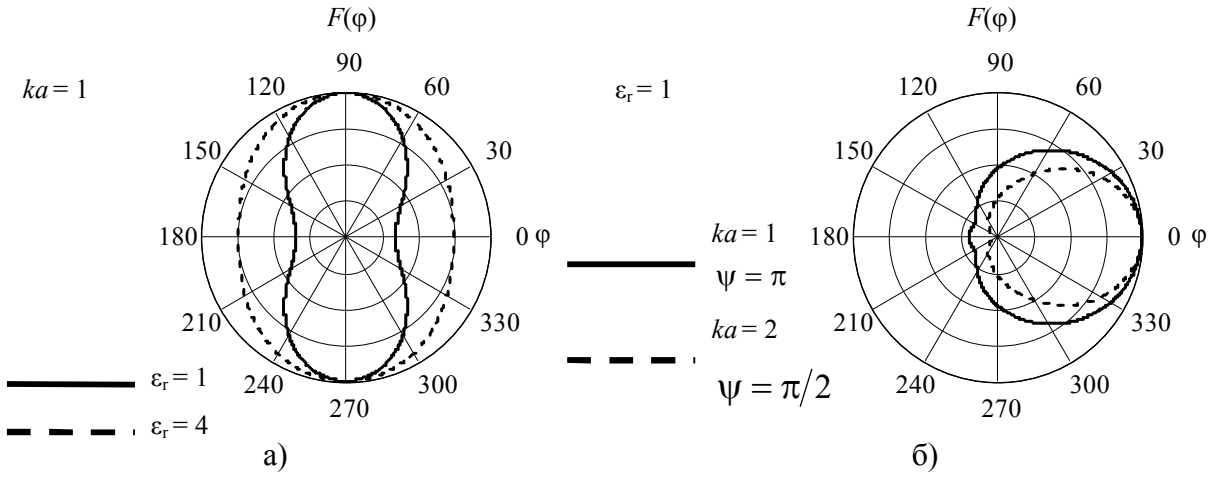



Рис. 1

Отже, згідно отриманих даних, можна стверджувати, що для антен з горизонтальною поляризацією поля, НПА на циліндрі дозволяє формувати як ненаправлене так і секторіальне випромінювання в азимутальній площині. Для антен з вертикальною поляризацією поля, НПА дає змогу сформувати секторіальне випромінювання в азимутальній площині, для отримання ненаправленого випромінювання необхідно перейти до кільцевих антенних решіток із НПА.

ЛІТЕРАТУРА


1. *Ерохин Г.А., Чернышев О.В.* Антенно-фидерные устройства и распространение радиоволн. – М.: Горячая линия–Телеком, 2007. – 491 с.
2. *Luk Kuai-man, Lee Kai-Fong, Dashele J.S.* Analysis of the cylindrical-rectangular parch antenna. // IEEE Transactions on antennas and propagation, 1989. – AP-37 – № 2. – P. 143 – 147.
3. *Цибизов К.Н., Ильинов М.Д.* Микрополосковые антенны. – К: Общество „Знание”, 1980. – 28 с.
4. *Резников Г.Б.* Антенны летательных аппаратов. – М.: Советское радио, 1967. – 415 с.
5. *Gabriel'yan D.D.,* Zvezdina M.Yu. The influence of impedance surface of a circular cylinder on the dipole pattern. // Proceedings of 3-rd International Conference Antenna Theory and Techniques, 1999. – P. 113 – 116.

Ільницький С.В. (НАОУ)
Сілко О.В. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ЩОДО СИНТЕЗУ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ, ПРОБЛЕМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

Розвиток інформаційних технологій військового призначення за останні роки зробив актуальною проблему модернізації системи військової освіти. Закордонний і вітчизняний досвід розвитку освіти вказує на те, що майбутнє освіти невід’ємно пов’язане з подальшим використанням дистанційного навчання.

**Дистанційне навчання (ДН)** є формою одержання освіти, поряд з очною і заочною, при якій в освітньому процесі використовуються кращі традиційні й інноваційні методи, засоби і форми навчання, основані на комп’ютерних і телекомунікаційних технологіях [1].

Таким чином, актуальним напрямом трансформації системи військової освіти, на сьогоднішній день, є створення системи дистанційного навчання (СДН) Збройних Сил України. Вона має стати підсистемою системи військової освіти, яка являє собою сукупність взаємодіючих між собою з метою організації та здійснення дистанційного навчального процесу в єдиному інформаційно-освітньому середовищі: адміністративного персоналу; підрозділів дистанційного навчання; слухачів, які навчаються з використанням технологій дистанційного навчання; науково-педагогічних працівників.

Однак, незважаючи на сформовану стратегічну політику розвитку дистанційної освіти у межах освітньої системи України взагалі, існує ряд проблем, що ускладнюють створення СДН військових фахівців. Отже, набуває актуальності завдання розроблення методичних підходів щодо проектування СДН військових фахівців для Збройних Сил України.

Оскільки закордонний досвід створення СДН військових фахівців не може бути автоматично застосованим в інтересах Збройних Сил України, при проектуванні та побудові такої системи доцільно спиратися на досвід проектування автоматизованих систем управління, що базуються на комп’ютерних мережах [2].

Будь-яка система дистанційного навчання представляє собою складну систему. Теорія проектування таких систем базується на дослідженні процесів функціонування окремих її підсистем та елементів. З погляду методології проектування СДН, зазвичай, виділяють такі складові частини процесу проектування: загальносистемне проектування СДН, проектування програмного забезпечення та проектування апаратних засобів.

Загальною методологією, яку можна застосувати до процесу створення СДН, є системний аналіз, який дозволяє вирішити складні проблеми аналізу складових частин СДН, їх взаємний вплив, а також всебічної оцінки навколишнього середовища.

На ранніх стадіях проектування СДН найбільша увага відводиться обґрунтуванню доцільності розроблення, техніко-економічній оцінці, вибору раціональних структур, теоретичній оцінці основних характеристик СДН (ефективності, надійність, життєздатності, безпеки, пропускної спроможності каналів зв’язку тощо).

Процес проектування СДН являє собою складний ітеративний (покроковий) процес, який складається з ряду послідовних етапів. Кожний з них складається з ряду послідовних та функціонально взаємопов’язаних елементів системного аналізу.

Розглянемо сутність основних ітераційних процесів та послідовних етапів при проектуванні СДН.

***На етапі 1*** проводиться оцінка доцільності розроблення та попередній вибір структури СДН. Така оцінка проводиться на основі відповідних критеріїв (інтегральних, диференціальних). Один з елементів системного аналізу полягає у визначенні можливих варіантів структурних схем СДН.

***На етапі 2*** проводиться попередній вибір технічних рішень та оцінка варіантів реалізації СДН. Конкретні технічні рішення оцінюються за допомогою різноманітних часткових моделей, призначених для оцінки різних варіантів технічних рішень за обраними частковими критеріями.

***На етапі 3*** проводиться кінцевий вибір структури СДН. Цей вибір базується на результатах досліджень попередньо етапу. Метод експертних оцінок може бути використаним для визначення остаточного рішення щодо вибору структури СДН, з урахуванням попередньо отриманих результатів.

***На етапі 4*** проводиться вибір алгоритмічних рішень побудови підсистем та СДН у цілому. Такий вибір засновується на результатах:

математичного моделювання процесів, які проходять в СДН;

оцінці впливу якості інформаційного забезпечення на показники ефективності СДН;

оцінці впливу структури мережі, телекомунікаційних засобів та процесів, які виникають у мережі.

***На етапі 5*** проводиться остаточний вибір технічних рішень щодо розроблення апаратури. Важливим елементом системного аналізу на даному етапі є вибір структури та типів апаратних засобів для побудови СДН. Принципово важливим елементом системного аналізу на даному етапі є визначення методів організації взаємодії людини з апаратними засобами СДН.

***На етапі 6*** проводиться вибір головних рішень щодо розроблення програмного забезпечення СДН. Характерною вимогою для СДН є необхідність оброблення великих обсягів різнорідної інформації за одиницю часу. Ефективність роботи СДН визначається побудовою та функціонуванням керуючих програм реального часу та мережених операційних систем, які забезпечують надійне та безпечне функціонування СДН у будь-яких умовах, у тому числі в умовах її повного завантаження.

***На етапі 7***, що зветься етапом створення СДН на базі обраних рішень, визначаються режими роботи СДН. Оптимальне використання обчислювальних ресурсів у ході функціонування СДН зводиться до реалізації таких алгоритмів і програм, які дозволяють забезпечити працездатність СДН при відхиленні параметрів від заданих в технічному завданні.

***На етапі 8*** проводиться налаштування, дослідна експлуатація та впровадження СДН.

Усі ці ітераційні процеси після чергового етапу можуть повертатись до попереднього, і це пов’язано з необхідністю прийняття найбільш правильних рішень. Повторення етапу (етапів) впливає на підвищення якості проектних рішень.

Теоретична основа проектування СДН – це сукупність математичних методів та моделей. Еволюція методів аналізу та синтезу включає послідовний перехід від детермінованих методів до імовірнісних, а вже від них – до методів теорії нечітких множин.

З вищерозглянутого можна зробити наступний висновок про те, що завдання проектування СДН військових фахівців є надзвичайно складним та потребує координованих зусиль великої кількості фахівців у різних аспектах інформаційних технологій, педагогіки та психології. Обов’язковою складовою успішного розв’язання цього завдання має стати створення умов до залучення найкращого як вітчизняного, так й закордонного досвіду накопиченого, у військовій та цивільній освіті.

ЛІТЕРАТУРА

1. *Гороховський О. І.* Методичні аспекти створення навчальної літератури для дистанційного навчання: методичний посібник. – В.: ВНТУ, 2004. – 121 с.

2. *Азаренко Е. В., Герасимов Б. М., Шохин Б. П.* Проектирование автоматизированных систем управления на компьютерных сетях. – Севастополь: Гос. Океанариум, 2007. – 272 с.

Каравацький В.О.(в/ч А 1906)

# ТЕНДЕНЦІЇ РОЗВИТКУ ЕЛЕМЕНТНОЇ БАЗИ ЗАСОБІВ ТЕЛЕКОМУНІКАЦІЙ, ТЕОРІЇ ЕЛЕКТРОЗВ'ЯЗКУ ТА АНТЕННО-ФІДЕРНИХ ПРИСТРОЇВ

Сучасний рівень розвитку збройної боротьби потребує постійного вдосконалення телекомунікаційних систем військового призначення.

При цьому невід'ємною складовою таких комплексних систем є засоби зв'язку та апаратура управління, до яких висуваються безпрецедентно високі вимоги щодо надійності, завадозахищеності, енергоспоживання тощо. Поки що промисловість України не спроможна забезпечити весь спектр потреб для створення засобів телекомунікації, які б відповідали сучасним вимогам.

По-перше, раціональним є створення систем телекомунікацій за уніфікованим блочним принципом, який реалізовує можливості нарощування, гнучкої зміни конструкції, зміни схемотехнічних рішень та способів вирішення завдань.

Виключення складають тільки індивідуальні засоби зв'язку спеціального призначення. Одним з таких рішень є підвищення надійності апаратури за рахунок збільшення показника напрацювання на відмову та зменшення кількості елементів принципових схем за рахунок використання стандартних схемних рішень, а саме: процесорів, контролерів та мікросхем. Навіть при однаковому напрацюванні виріб з меншою кількістю елементів має більш високий показник надійності.

Ще одне з перспективних питань розвитку – це створення нового принципу аналогово-цифрового контролю стану апаратури, перехід від кількісного контролю до якісного. Наприклад, стрілковий індикатор варто замінити на три або навіть на два різнокольорових світлодіоди, що дає змогу оперативно контролювати якісний стан приладу та у разі виходу з ладу оперативно локалізовувати несправність на рівні блоків, субблоків, плат в залежності від ступеня деталізації вмонтованої системи контролю.

Третя тенденція розвитку – це використання новітніх технологій, елементної бази та схематичних рішень при створенні та експлуатації блоків живлення апаратури зв'язку. Наприклад, в існуючій апаратурі дуже рідко використовується або взагалі не використовується принцип імпульсного перетворення вторинної напруги блоків живлення. Взагалі, створення імпульсних блоків живлення високої надійності (за виключенням новітньої техніки, яка щойно розробляється) для існуючої техніки не проводиться, хоча відомо що більше 50% відмов техніки стається з вини блоків живлення.

Слід створювати блоки живлення для існуючої апаратури з метою подовження терміну експлуатації, тим самим створюючи базу для подальшої модернізації, отримання практичних результатів роботи апаратури та поступового переходу на нову елементну базу.

Наведені у доповіді результати у сукупності розв'язують актуальну науково - практичну задачу, що полягає у визначенні тенденцій розвитку елементної бази засобів телекомунікацій.

Карловський І.В. (ВІТІ НТУУ „КПІ”)
Штаненко С.С. (ВІТІ НТУУ „КПІ”)

# ШЛЯХИ ВДОСКОНАЛЕННЯ ДІАГНОСТИКИ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

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.

Насичення ЗСУ складною сучасною технікою зв’язку та автоматизації разом з підвищенням вимог до ефективності процесів управління призводить до ускладнення і різкого підвищення ролі експлуатації і ремонту радіоелектронної апаратури (РЕА). У цілому ряді випадків чинник недостатньо високої кваліфікації обслуговуючого персоналу засобів зв’язку та автоматизації є причиною суттєвого зниження ефективності практичного використання цих засобів. У першу чергу це стосується процедур непланового ремонту техніки після експлуатаційних відмов і пошкоджень.

Аналіз різних складових часу відновлення РЕА свідчить, що найбільші труднощі у обслуговуючого і ремонтного персоналу, як правило, на етапі виявлення причин виникнення відмов. У той же час, у прикладній науковій дисципліні технічної діагностики достатньо детально розроблена проблема алгоритмізації виявлення дефектів в непрацездатній РЕА. Однак низка причин, що пов’язана зі складністю використання рекомендацій технічної діагностики недостатньо кваліфікованим обслуговуючим персоналом, на сьогодні стримує впровадження цих рекомендацій в практику експлуатації і ремонту РЕА у військових умовах. У результаті реальні витрати часу на відновлення техніки після відмов і пошкоджень часто значно перевищують допустимі за умовами її практичного застосування значення .

Широке впровадження засобів обчислювальної техніки, при виконанні деяких умов, здатне суттєво змінити цю несприятливу ситуацію до кращого. Йдеться мова про розробку і практичне впровадження спеціальних програмних засобів підтримки діагностичної діяльності обслуговуючого і ремонтного персоналу, які базуються на технології і методах штучного інтелекту, а саме діагностичних експертних систем (ЕС).

Діагностичні ЕС співвідносять спостережувані порушення поведінки системи з причинами, що зумовили їх, спираючись на один з двох наступних методів. Перший має на увазі використання деякої таблиці асоціативних зв’язків між типами поведінки систем і діагнозами. У другому методі спільне використання знань про те, як влаштована система, і знань про слабкі місця конструкції дозволяє будувати припущення про несправності, сумісні із спостережуваними даними.

Обчислювальна потужність діагностичних ЕС визначається, в першу чергу, нарощуваною базою знань (БЗ), в якій зберігаються еталонні дані, що описують дану область, і правила, що описують доцільні перетворення даної області. Сучасні діагностичні ЕС дозволяють оперувати нечіткими визначеннями, дозволяючи ефективніше використовувати і зберігати одержані знання, полегшуючи процес їх придбання, а система в цілому стає гнучкішою.

Таким чином, застосування діагностичних ЕС значно підвищить ефективність діагностування РЕА, оскільки дозволить оперативно аналізувати різноманітну інформацію по особливостях ситуації, що склалася, виробляти необхідні рекомендації про можливість усунення тієї або іншої несправності, враховувати нелінійності і невизначений характер протікаючих в них процесів і приймати оптимальні рішення по експлуатації і ремонту даної апаратури.

к.т.н. Карпенко Б.О. (ВІКНУ)
Ліпчевська І.Л. (ІТС НТУУ „КПІ”)
Мазуренко О.В. (ІТС НТУУ „КПІ”)
к.т.н. Якорнов Є.А. (ІТС НТУУ „КПІ”)

# ИСКРЕТНІ АНТЕННІ СИСТЕМИ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З КОНТРОЛЬОВАНИМ РОЗДІЛЕННЯМ РАДІОСИГНАЛІВ ЗА ВІДСТАННЮ

Невпинний розвиток техніки та практична технологічна завершеність існуючих методів забезпечення перешкодозахищеності та прихованості радіосигналу змушує шукати новы підходи підтримки ефективності радіоапаратури спеціального призначення. Таким підходом є усунення функціонального недоліку дискретних антенних систем (АС), що полягає у розширенні їх можливостей щодо розділення сигналів у просторі не тільки за кутовими координатами, а й за відстанню.

Формування тривимірно селективних діаграм направленості можливе лише в ближній і проміжній зоні, тобто дане явище притаманно полям дифракції наближення Френеля. Основним функціональним принципом даних систем є процес формування поля дифракції Фраунгофера, тобто поля дальньої зони, в області дифракції Френеля, що в теорії дифракції ще називається фокусуванням. Його особливості розглянемо далі.

Даний принцип може бути реалізований на АС, структура якої може мати прямолінійну форму чи форму замкненої ламаної (багатокутника). Формування характеристик направленості (ХН) даних АС має наступні особливості у порівнянні з тими, що працюють з дальньою зоною: амплітуда збудження *n*-ого елемента АС залежить від затухання на шляху розповсюдження від станції корреспондента до цього елемента; сигнал до кожного *n*-ого елемента АС приходить під різним азимутом; кожен елемент АС має ХН, яка також може залежати від відстані. Характер ХН за відстанню такий же як і за азимутом, згідно [1], тобто, рівень та кількість головних, бокових пелюсток та мінімумів пропорційні рівню та кількості головних побічних фокальних областей та мінімумів.

Основний функціональний принцип – фокусування, на якому базуються дані АС характеризується формуванням фокальної області з найкращими умовами прийому в точці розміщення станції кореспондента зі створенням умов максимального придушення перешкоди. Формування фокальних областей обмежене за відстанню від фазового центра (ФЦ) даної АС половиною гіперфокусної відстані та природним затуханням при розповсюдженні, що ставить певні вимоги до конструкції АС для формування її ХН, яка відповідатиме умовам функціонування. Зі збільшенням відстані від ФЦ чітко виражена фокальна область перетворюється в зону функціонування даної АС з рівномірним розподілом потужності за відстанню до точки наведення фокусу, за якою рівень ХН різко спадає.

Специфіка структури та обробки сигналу даної АС вносить деякі особливості в формування показника перешкодозахищеності у порівнянні з класичним виразом: [1], в даних АС декілька приймальних антен і присутня додаткова система обробки сигналу, що дозволяє збільшити підсилення прийому; дані АС мають тривимірну направленість, тому перешкода придушується значно сильніше, а ефективність придушення перешкоди залежить від її розміщення відносно ХН всієї АС і ХН кожного її окремого елемента.

Якість функціонування таких систем залежить від досягнення якнайкращої її ХН, що можливо забезпечити методами, котрі притаманні нинішнім АС.

ЛІТЕРАТУРА

1. *Кремер И. Я., Кремер А. И., Петров В. М.* Пространственно - временная обработка сигналов. – М.: Радио и связь, 1984. – 223 с.

к.т.н. Катін П.Ю. (ВІТІ НТУУ „КПІ”)
к.т.н. Кузавков В.В. (ВІТІ НТУУ „КПІ”)
Гунько Д.Ю. (ВІТІ НТУУ „КПІ”)

# ТЕСТУВАННЯ ПРОГРАМ ОБРОБКИ ЗОБРАЖЕНЬ З ЧИСЕЛЬНОЮ ОЦІНКОЮ ЕФЕКТИВНОСТІ ДЛЯ СИСТЕМ ВІДЕОСПОСТЕРЕЖЕННЯ

Для спеціальних систем відеоспостереження, що постійно вдосконалюються, створюється нове програмне забезпечення спеціального призначення (ПЗСП). Актуальність даного напрямку визначається великим обсягом відеоінформації, що отримують під час роботи систем безпеки (відеоспостереження). Зазвичай в установі цілодобово працюють від 4 до 8 відеокамер, запис здійснюється безперервно. Отже обсяг отриманої для обробки відеоінформації, може досягати сотень гігабайт. Таким чином до ПЗСП, що застосовуються в системах безпеки, визначаються особливі вимоги щодо режимів функціонування та якості.

Якість програмного забезпечення, відповідно до першої частині стандарту ISO 9126-1 (ГОСТ Р ИСО / МЭК 9126-93) , визначається в 6-ти структурних наборах характеристик: функціональність, надійність, практичність, ефективність, можливість супроводження.

Розглянемо більш детально таку характеристику як ефективність. Відповідно до ISO 9126-1, ефективність це набір атрибутів, що відносяться до співвідношень між рівнем якості функціонування програмного забезпечення і обсягом ресурсів, що використовуються, при визначених умовах. Ефективність має дві основних субхарактеристики: за часом та за обсягом використаних апаратних ресурсів обчислювальної системи.

Відповідно до ISO 9126-1 ефективність за часом це здатність програмного забезпечення виконувати задані функції в інтервалі часу, що відповідають заданим вимогам. Зважаючи на великий обсяг відеоінформації, що обробляється за допомогою ПЗСП, ефективність за часом є важливим елементом якості програмного забезпечення. Огляд джерел показав відсутність методик чисельної оцінки ПЗСП. В цих тезах наведена нова методика чисельної оцінки ефективності ПЗСП.

*Основне призначення методики* – отримання чисельної оцінки ефективності ПЗСП або окремих елементів за часом. Вона може бути застосована на етапах розробки і кінцевого тестування ПЗСП.

*Вихідними даними* для статистичної оцінки є тривалість роботи блоку програми (програми в цілому) при обробці вибірки графічних файлів. Файли, які містять різну графічну інформацію зібрані у вибірки, відповідно до типу і розміру. Тривалість обробки кожного файла у вибірці фіксується і формуються вибірки тривалості часу обробки (ВТЧ).

*Під час реалізації методики припущено* (з подальшою перевіркою), що емпіричний розподіл у ВТЧ відповідає нормальному закону розподілу випадкової величини.

Час обробки графічних файлів визначався з використанням функції Time().FormatString („nn:ss:gg”) мови C++.

Передбачалося, що помилки вимірювання часу за допомогою тестових елементів значно менш дисперсії у ВТЧ. У випадку наявності в програмі чисельних відмов або „витоку” пам’яті варіант реалізації відкидався, ВТЧ не визначалася.

*Працездатність методики підтверджується результатами, що отримані* під час тестування прототипів програми обробки зображення. В табл.1 (рядок 1) показані результати використання методики під час застосування загальновідомого алгоритму усереднення із застосуванням функції GetPixel і SetPixel (мови C++). Для порівняння в табл.1 (рядок 2) показані результати використання методики із застосуванням того ж самого алгоритму, з використанням властивості ScanLine (мови C++).

*Таблиця 1*

| **Варіанти реалізації** | **Розмірність файлів, (розмірність вибірки, елементи)** | **Оцінка математичного очікування тривалості реалізації програми, с** | **Оцінка середньоквадратичного відхилення тривалості реалізації програми, с** | **Довірчий інтервал** |
|---|---|---|---|---|
| ПЗСП з використанням GetPixel, SetPixel | 1024×640 (100) | 3,286 | 0,036033 | ±0,108099 |
| ПЗСП з використанням ScanLine | 1024×640(100) | 1,2312 | 0,02054 | ±0,107022 |

Чисельне значення у вибірках не нормоване. З табл. 1 видно, що оцінка математичного очікування в першому рядку значно більша ніж у другому, при однакових файлах у вибірці і її об'ємі. Отже час обробки графічних файлів ПЗСП з використанням GetPixel, SetPixel приблизно в 3 рази більше ніж час обробки графічних файлів ПЗСП з використанням ScanLine. Гістограма ВТЧ показана на рис.1.

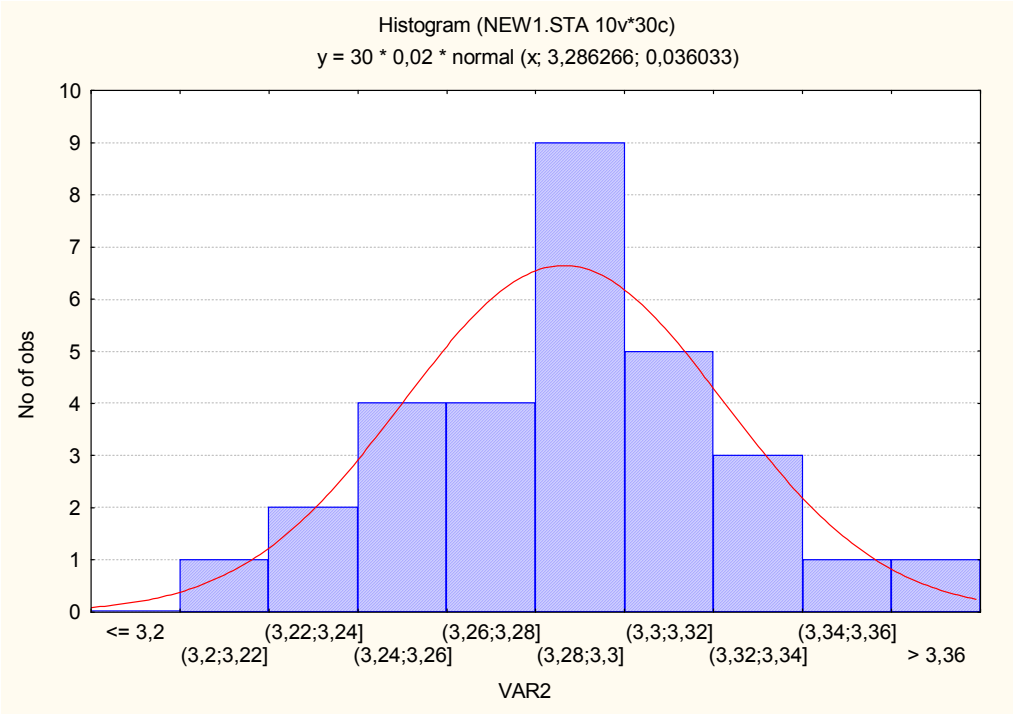



Рис. 1. Графічне зображення гістограми вибірки ВТЧ

Таким чином, програмне забезпечення з використанням властивості ScanLine дає можливість обробляти графічний файл з найменшою затратою часу ніж програмне забезпечення з використанням методів GetPixel/SetPixel. Отримані результати підтверджують відомий факт, а методика придатна для тестування з чисельною оцінкою ефективності інших програм обробки зображень.

Коваленко А.О. (ВІТІ НТУУ „КПІ”)

# УДОСКОНАЛЕНИЙ СТЕГАНОГРАФІЧНИЙ МЕТОД ЦЕНТРУВАННЯ ЗНАЧЕНЬ КОЛІРНИХ КОМПОНЕНТ

При робастному до стиснення з втратами приховуванні інформаційних повідомлень у кольорових сильнонасичених зображеннях доцільно застосовувати метод з центруванням значень колірних компонент. Одним з недоліків цього методу є те, що під час зміни значення пікселя колірної компоненти враховується тільки номер інтервалу приховування, і не враховується близькість необхідного під діапазону сусіднього інтервалу. Таким чином, в деяких випадках значення колірної компоненти змінюється на величину, що дорівнює приблизно 3/4 ширини інтервалу, у той час, як такий самий ефект міг бути досягнути зі зміною у 1/4.

На рис. 1 показано приклад впровадження біту „0” в вихідне значення пікселя 47 для вихідного та удосконаленого методу центрування значень колірних компонент (при використанні інтервалу впровадження 16).

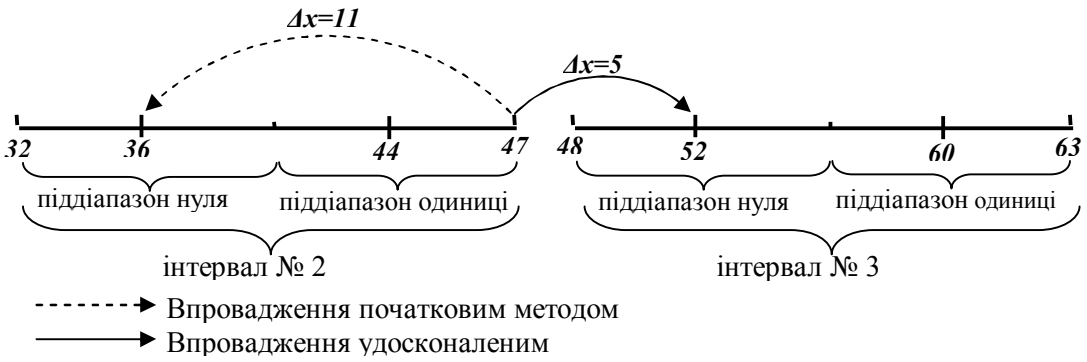



Рис. 1 Приклад впровадження біту „0” вихідним і удосконаленим методом (для інтервалу впровадження, що дорівнює 16)

Як видно з даного прикладу, при застосуванні початкового методу значення колірної компоненти змінюється на 11 рівнів градації яскравості, у той час як впровадження новим методом дозволяє приховати біт, змінивши значення лише на 5 рівнів.

Складністю формулювання аналітичного виразу для даного алгоритму приховування є те, перший та останній інтервали мають лише по одному сусідньому інтервалу праворуч та ліворуч відповідно (в іншому випадку відбудеться вихід за діапазон значень колірних компонент [0; 255]). Для врахування даного факту можливе застосування в алгоритмі перевірки умови значення колірної компоненти на близькість до границі, але більш доцільним для цього виявилося застосування апарату цілочисельної математики (а саме – ділення без остачі), тому в кінцеву формулу було введено „поправочні” коефіцієнти, які враховують близькість значення колірної компоненти до границь діапазону [0; 255].

Необхідно також відзначити, що алгоритм декодування для даного удосконалення методу не змінюється. Це зумовлено тим, що значення колірних компонент центруються так само у піддіапазони, але з урахуванням того, під діапазон якого інтервалу найближчий.

Зрозуміло, що стійкість методу до стиснення з втратами при такому впровадженні не змінюється, тому що, як зазначалося раніше, стійкість методу залежить лише від ширини інтервалу, коефіцієнту стиснення та частоти колірного перепаду вихідного контейнера.

Таким чином, удосконалений метод впровадження дозволяє (у порівнянні з початковим) зменшити похибку, що вноситься у вихідний контейнер, а саме зменшити середньоквадратичне відхилення утвореного стего на 10 %–15 %, а співвідношення сигнал/шум та пікове співвідношення сигнал/шум підвищити відповідно на 9 %–12 % та 7 %–9 %.

Ковбаса Ю.В. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ СТАНДАРТІВ ТЕХНОЛОГІЇ CDMA

Розділення каналів – це дуже важливий принцип, що дозволяє ефективніше використовувати смугу частот. CDMA називають широкосмуговою системою і сигнали йдуть в ефірі шумоподібними. Широкосмугова, тому що займає широку смугу частот. Шумоподібні сигнали тому, що коли в ефірі на одній частоті, в один і той же час працюють декілька абонентів, сигнали накладаються один на одний. Завадостійка тому, що при виникненні в широкій смузі частот (1,23 МГц) сигналу-перешкоди, вузького діапазону (<150кГц), сигнал прийметься майже неспотворений.

На відміну від розділення каналів за частотою або часом, кодове розділення дозволяє досягнути максимальної ефективності і є найбільш перспективною технологією на сьогоднішній день CDMA (Code Division Multiple Access) – система множинного доступу з кодовим розділенням – стала багатообіцяючою системою, що з’явилась на світовому ринку. Саме цю технологію пов’язують з мережами третього покоління. При доступі з кодовим розділенням абоненти розділяються методом спеціального шифрування. Технологія CDMA не підрозділяє абонентів на фіксованих і мобільних і не обмежує їх в доступі до послуг мережі при переміщенні. За характеристиками якості передачі, мови, параметри CDMA можна порівняти з якістю провідних каналів, при цьому випромінювана потужність, як і рівень шумів, зменшується. Існує декілька варіантів технології CDMA, до 3G найбільш близьким є широкосмуговий множинний доступ – WCDMA, що забезпечує більш високу передачу даних, а також EV-DV.

Мобільний зв’язок третього покоління будується на основі пакетної передачі даних. Для реалізації систем третього покоління розроблені рекомендації за глобальним уніфікованим стандартом мобільного зв’язку:

– забезпечення якості передачі мови, що порівнюється з якістю передачі провідних мереж зв’язку;
– забезпечення безпеки, у порівнянні з безпекою у провідних мережах;
– забезпечення національного та міжнародного роумінгу;
– ефективне використання спектра частоти;
– пакетна і канальна комутація;
– підтримка багаторівневих сотових структур;
– взаємодія з системами супутникового зв’язку;
– поетапне збільшення швидкості передачі даних до 2 Мбіт/с.

Першим етапом розвитку технології CDMA став стандарт CDMAOne (IS-95A/B). Стандарт CDMA2000 1X є наступним етапом у розвитку технології CDMA після CDMAOne. Мережі CDMA2000 1X пропонують значне покращення якості звуку і збільшення ємності звукових каналів при високій швидкості та мультимедійності передачі даних.

CDMA2000 (IMT-MC) розділений на дві фази – 1X і 3X. Перша фаза IS-95C, а друга 1X-EV (evolution), яка розділена на – CDMA2000 1X EV-DO (data only – тільки дані) і CDMA2000 1X EV-DV (data & voice – дані та голос).

Мережі CDMA2000 1X функціонують в тій же смузі частот, що і мережі CDMAOne, але вони володіють у 2 рази більшою пропускною спроможністю голосових каналів і швидкістю передачі даних 144 Кбіт/с. Реалізована фаза CDMA2000 1X не є повноцінною 3G, так як не відповідає потребам швидкості передачі даних до обов’язкових двох мегабіт.

Стандарт CDMA2000 1X EV є подальшим удосконаленням стандарту 1X. З його допомогою досягається найефективніше використання частотного спектра, збільшується пропускна здатність передачі даних, досягається найбільша швидкість передачі інформації від 2 до 5 Мбіт/с в тій же смузі частот 1.25 МГц. Потреби операторів стандарту 1X EV поділяють на два етапи. На першому етапі для більш ефективного способу передачі

інформації потрібне досягнення швидкості передачі даних більш 2.4 Мбіт/с (CDMA2000 1X EV-DO). При реалізації другого етапу досягаються швидкості передачі звуку і даних в реальному масштабі часу (CDMA2000 1X EV-DV). Стандарт 1X EV-DV повністю відповідає всім потребам 3G.

Мережі третього покоління 3G працюють на частотах дециметрового діапазону близько 2 ГГц, передаючи дані зі швидкістю 2 Мбіт/с. Вони дозволяють організовувати відеотелефонний зв'язок, дивитись на мобільному телефоні фільми и телепрограми і т. д.

Ціль всієї індустрії телекомунікацій – створить єдине всесвітнє середовище мобільного зв'язку, що підтримує широкосмугові системи та забезпечує глобальну мобільність, в результаті, виникло деяке сімейство стандартів, що забезпечує послуги третього покоління.

В системах IMT-MC основні параметри мережі – зона обслуговування, пропускна здатність (ємність) підсистеми радіодоступу і якість обслуговування – взаємопов'язані, і тому є можливість покращити одні параметри за рахунок інших. Тому у системах IMT-MC немає жорстких обмежень по ємності (soft capacity), і при збільшенні навантаження на деякі сектори їх пропускання здатність може бути збільшена за рахунок зменшення зони покриття і/або деякого збільшення ймовірності помилкових фреймів (frame error rate, per), яке не приводить до значного зменшення якості мови і параметрів передачі даних. Переваги систем cdma2000 при голосовому зв'язку вокодери, що застосовуються в системі cdma2000 (EVRC), забезпечують не тільки більш ефективну передачу мови, ніж у системі GSM (8 кбіт/с замість 13 кбіт/с), використовують адаптивну швидкість передачі в залежності від ступені активності мови, але і забезпечують зниження рівня навколишнього шуму за рахунок адаптивного регулювання порогів переходу до різних швидкостей передачі в залежності від рівня шуму.

Таким чином, збільшення швидкості передач відбувається тільки при зростанні активності мови, а не при зростанні рівня навколишнього шуму.

А отже, очевидно, що розвиток технології cdma2000 1x в майбутньому відкриває все більші перспективи перед операторами, що її використовують, за рахунок збільшення швидкості передачі даних і покращення інших характеристик системи.

ЛІТЕРАТУРА

1. *Пестряков В.Б., Афанасьев В.П., Гурвиц В.Л.* и др.; под ред. Пестрякова В.Б. Шумоподобные сигналы в системах передачи информации. – М.: Сов. радио, 1973. – 424 с.

2. *T. Stefansson.* CODIT – a Possible Candidate for UMTS. Proceedings. The Sixth Nordic Seminar on Digital Mobile Radio Communications. DMR VI 1994, 90 – 96.

3. *Диксон Р.К.* Широкополосные системы. Пер. с англ./Под ред. В.И. Журавлева. – М: Связь, 1979. – 304 с.

4. *Варакин Л.Е.* Системы связи с шумоподобными сигналами. – М.: Радио и связь 1985, 1985. – 384С.

5. *Смирнов Н.И.* Проектирование микроэлектронных устройств обработки шумоподобных сигналов. Часть 1. Корреляционные свойства ШПС. Учебное пособие. М.гМЭИС. 1988. –40 с.

6. *Тузов Г.И., Сивов В.А., Прытков В.И.* и др.; под ред. Тузова Г.И. Помехозащищенность радиосистем со сложными сигналами. – М.: Радио и связь, 1985. – 256 с.

7. *Петрович Н.Т. Размахнин М.К.* Системы связи с шумоподобными сигналами. – М.: Сов. радио, 1969. – 232 с.

8. *Алексеев А.И., Шереметьев А.Г., Тузов Г.И., Глазов Б.И.* Теория и применение псевдослучайных сигналов. – М.: Наука, 1969 – 365 с.

к.т.н. Кокотов О.В. (НТУУ „КПІ”)
Шевченко А.С. (ВІТІ НТУУ „КПІ”)

# МОДЕЛЬ ЗАГРОЗ ІНФОРМАЦІЇ В СИСТЕМАХ БЕЗПРОВОДОВОГО ЗВ’ЯЗКУ В УМОВАХ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

В сучасній стратегії розвинутих держав велику увагу приділяють концепції ведення інформаційних операцій (війн). Під поняттям інформаційної війни розуміють комплексний вплив на систему державного та військового управління протиборчої сторони, який вже в мирний час призвів би до прийняття сприятливих для нас рішень, а в ході війни повністю паралізував структуру управління противника. Одночасно з наступальним впливом інформаційне протиборство передбачає забезпечення надійного захисту національної інфраструктури країни. Наступальні інформаційні операції на військовому рівні представляють собою комплексне проведення за єдиним замислом і планом такі заходи: радіоелектронне подавлення; фізичне знищення (вивід з ладу); оперативне маскування; програмно-математичний вплив на інформаційно-управляючі системи.

Системи безпроводового зв’язку (СБЗ) є найбільш вразливою складовою в телекомунікаційній мережі. Для забезпечення захищеності інформації, що передається СБЗ, необхідно оцінити і мінімізувати ризики, які виникають в результаті реалізації атак противником (порушником). Але перед усім необхідно оцінити загрози захищеності СБЗ.

Синтезована модель загроз СБЗ представлена на рис. 1. При побудові приведеної моделі загроз СБЗ враховувались лише нижні два рівні моделі взаємодії відкритих систем. Це обумовлюється тим, що захисту інформації на вищих рівнях приділяється достатньо уваги, і переважно вони технічно не реалізовані в більшості СБЗ, особливо спеціального призначення. Структурно в складі СБЗ окремо виділені такі складові, як система управління (СУ) та система захисту (СЗ). Вказані загрози носять як штучний так і природній характер.

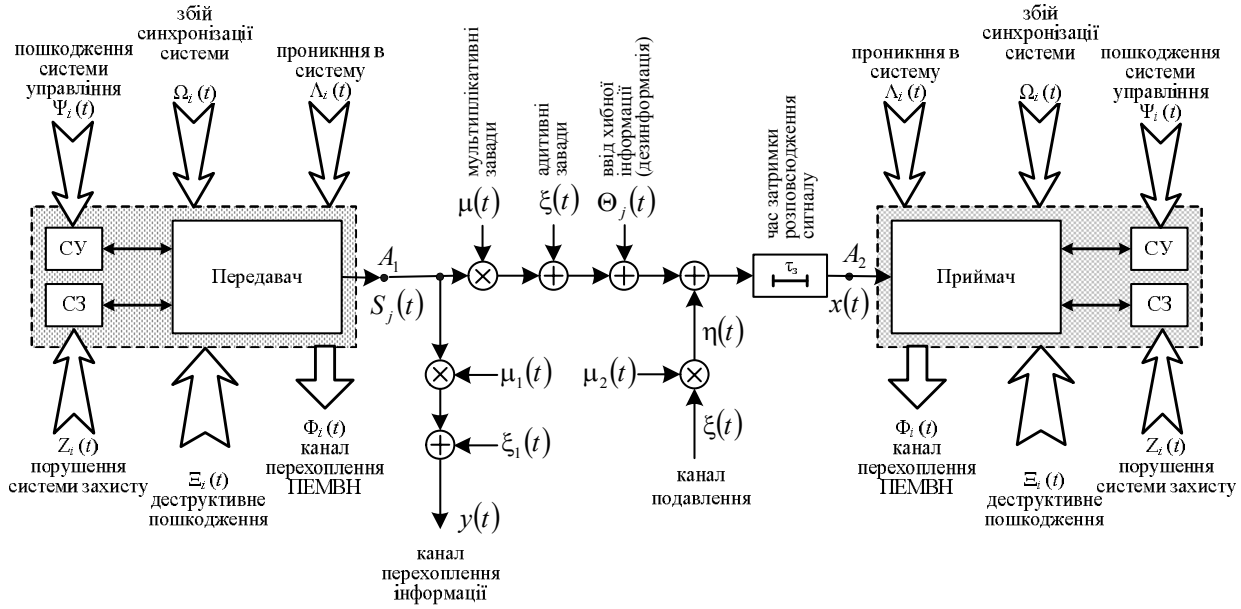



Рис. 1. Модель загроз системам безпроводового зв’язку

Загрози інформації, приведені в моделі загроз, діляться по критеріях безпеки на загрози конфіденційності, цілісності та доступності інформації. Крім того, ці загрози можна класифікувати по об’єктах впливу: загрози каналу зв’язку, загрози СУ, загрози СЗ та загрози безпосередньо СБЗ.

Приведена загальна модель загроз для СБЗ дозволить виділити та оцінити порушників, які створюють ці загрози, оцінити ризики, розрахувати захищеність СБЗ та застосувати необхідні механізми захисту СБЗ.

к.т.н. Колос Ю. О. (ЖВІ НАУ)
к.т.н. Манько О. В. (ЖВІ НАУ)
Орищук І. О. (ЖВІ НАУ)

# ХАРАКТЕРИСТИКИ ТА ПАРАМЕТРИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЯК ЗАСОБУ ЗДІЙСНЕННЯ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Економічні розрахунки та прийняті міжнародним товариством договори і мораторії на застосування засобів вогневого ураження створили передумови активному використанню інформаційного простору для вирішення різноманітних конфліктів, реалізації національних інтересів за визначеним напрямком. Доповнення просторово-часового континууму ще одним виміром – інформаційним – для ведення бойових дій не є новим в історії військового мистецтва. Але розвиток технологій зі здійснення цілеспрямованого впливу як на інформаційні системи держави, так і на морально-психологічний стан усіх верств населення зумовлює необхідність більш ретельного опрацювання питання щодо розробки та створення системи протидії такому впливу. На сьогоднішній день це питання є актуальним не тільки для нашої держави, але й для інших країн, які здійснюють перехід до інформаційного суспільства.

Функціонування сучасних інформаційних інфраструктур суспільства невід'ємно забезпечуються як наземними телекомунікаційними лініями, так і супутниковими системами телекомунікацій, які поряд із відомими перевагами, зокрема забезпеченням глобального зв'язку, характеризуються швидким розгортанням широкосмугових каналів зв'язку і наданням високошвидкісних послуг численним користувачам. Бурхливий розвиток світових і національних інформаційних інфраструктур завдяки впровадженню супутникових телекомунікаційних систем, нових технологічних рішень, високошвидкісних методів передачі даних значно збільшує можливості користувачів з доступу до інформаційних ресурсів. Це підвищує вірогідність здійснення цілеспрямованого інформаційно-психологічного впливу (ІПсВ) через телекомунікаційні мережі.

У доповіді наводяться результати аналізу використання телекомунікаційних мереж для здійснення заходів інформаційно-психологічного впливу у ході вирішення військових конфліктів.

Запропоновано характеристики та параметри для якісної та кількісної оцінки інформаційно-психологічного впливу, який здійснюється через телекомунікаційні мережі. Серед таких параметрів і характеристик слід виділити:

технічні, які викликають зацікавленість з огляду на можливість доступу до них та їх подавлення (частота, види модуляції, кодування сигналу та ін.);

просторово-часові – час та тривалість передачі інформації, зона дії, місця розташування передавачів;

інформаційно-психологічні – спрямованість, інформаційний привід, прийоми та способи маніпуляції свідомістю та ін.

Розглядаються частотно-просторово-часові діаграми роботи телекомунікаційних систем та порядок їх використання при плануванні та здійсненні заходів протидії зовнішньому деструктивному інформаційно-психологічному впливу.

У доповіді приділяється увага веденню моніторингу інформації, яка циркулює в телекомунікаційних мережах, з метою виявлення деструктивного інформаційно-психологічного впливу. Запропоновано систему параметрів, за якими ведеться моніторинг, та способи їх оцінки й попередньої обробки.

ЛІТЕРАТУРА

1. *Прибутько П. С., Лук'янець І.Б.* Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. – К., 2007. – 252 с.

к.т.н. Колос Ю.О. (ЖВІ НАУ)
к.т.н. Міхєєв Ю.І. (ЖВІ НАУ)

# ТЕХНОЛОГІЇ ВИКОРИСТАННЯ ЗАСОБІВ ІНФОРМАЦІЙНОЇ БОРОТЬБИ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Активне використання можливостей інформаційних мереж у всіх сферах життєдіяльності, в тому числі у військовій, призвело до того, що вони стали одним з найважливіших середовищ інформаційної боротьби. Застосування сучасних інформаційних технологій, спеціальних програмних продуктів у інформаційних мережах дозволяють знецінювати традиції, змінювати культурні і духовні цінності громадян, впливати на морально-психологічний стан користувачів, у тому числі, і на особовий склад збройних сил держави [1, 2]. Тому інформаційна безпека, засоби ведення інформаційної боротьби, методи та засоби протидії інформаційним ударам в інформаційних мережах у даний час знаходяться у центрі загальної уваги.

В доповіді пропонується в якості основних форм загроз у інформаційних мережах вважати програмні, інформаційні та комбіновані акції. Програмні акції застосовуються шляхом впровадження спеціальних програм або зміною програмного забезпечення об'єкту (комп'ютерні віруси, логічні бомби, різного роду помилки, що свідомо вводяться в програмне забезпечення об'єкту, DOS-атаки серверів та робочих станцій).

Розглядається зміст програмних акцій в комп'ютерній мережі, який включає: визначення цілі акції; здійснення фізичного доступу до інформаційної мережі; подолання процедури ідентифікації (аутентифікації) в мережі; визначення топології мережі (сканування) та знаходження об'єкту впливу (атаки); розширення чи обмеження права доступу до інформаційних ресурсів мережі; впровадження у мережу деструктивних спеціальних програмних продуктів чи модифікація наявного програмного забезпечення.

Об'єктом впливу інформаційних акцій в першу чергу є свідомість, підсвідомість користувача та взагалі його психіка. Особливість проведення інформаційних акцій полягає у прихованій для об'єкту впливу реалізації методів інформаційно-психологічного впливу за допомогою інформаційних мереж. Узагальнюються та систематизуються інформаційні акцій в інформаційних мережах в результаті яких може здійснюватись: підміна суспільних цінностей, створення комп'ютерної залежності користувачів, психологічний тиск через інформаційні повідомлення, порушення законів логіки, зміна переконань, як з одного питання так і системи переконань у цілому. Засобами реалізації інформаційних акцій можуть виступати: відео та аудіо інформація, електронні повідомлення, комп'ютерні ігри.

У доповіді наведені приклади застосування інформаційних технологій із зазначенням їх особливостей, які дозволяють підвищити ефективність захисту як інформаційних мереж, так і виявлення інформаційно-психологічного впливу.

ЛІТЕРАТУРА

1. *Манойло А. В., Фролов Д. Б.* Информационно-психологические операции как организационная форма реализации концепции информационно-психологической войны, СПб.: Проблемы информационной безопасности. Компьютерные системы. 2003, N 2, С. 7–14.

2. *Почепцов Г. Г.* Информационные войны. М.: „Рефл-Бук", К.: „Ваклер" – 2000. – 576с.

Кондратюк А.Г. (ВІТІ НТУУ „КПІ”)

# ШЛЯХИ ПІДВИЩЕННЯ ФУНКЦІОНАЛЬНОЇ ЖИВУЧОСТІ НАПРЯМКІВ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Телекомунікаційна мережа (ТКМ) спеціального призначення функціонує для забезпечення доставки повідомлень в необхідному для управління підрозділами обсязі із заданою якістю. Для того, щоб забезпечити своєчасну доставку повідомлень у заданому обсязі, ТКМ повинна володіти відповідною перепускною спроможністю. У процесі функціонування на телекомунікаційну мережу спеціального призначення (її елементи) діють різні фактори, які порушують її нормальну роботу. Особливо такі дії проявляються в умовах надзвичайних ситуацій та бойових дій. Вони приводять до порушень роботи ліній зв’язку, фізичному виходу з ладу елементів ТКМ, іншими негативними наслідками, які приводять ТКМ у стан, при якому вона не може забезпечувати процес доставки повідомлень (або немає можливості забезпечувати цей процес на заданому рівні), відповідно перепускна спроможність зменшується до нуля. Для забезпечення функціональної живучості ТКМ була розроблена низка механізмів. Кожний з нижче перерахованих механізмів працює на відповідному рівні моделі взаємодії відкритих систем (OSI). Для захисту інформації від помилок і їхнього виправлення на канальному рівні використовується надлишкове кодування. Вибір надлишкового коду визначає вірогідність передачі інформації, складність реалізації процедур кодування і декодування і впливає як на продуктивність тракту передачі даних так і на функціональну живучість ТКМ в цілому.Для забезпечення передавання різних типів потоків на визначеному рівні розроблені системи мережевого керування, які оперують поняттям якості обслуговування (Quality of Service (QoS)). Якість обслуговування відображає здатність ТКМ надавати окремим інформаційним потокам більшу смугу перепускання, ніж іншим, та складається з таких частин: засоби забезпечення QoS в окремих мережевих пристроях (процедури опрацювання черг, керування потоком, диспетчеризації); методи та механізми координації діяльності пристроїв у мережі для забезпечення наскрізних параметрів якості передавання потоку; засоби та платформи керування для аналізу та керування наскрізними параметрами потоків для адміністратора мережі. Для гарантованого передавання повідомлення за призначенням на транспортному рівні використовують механізм протоколу TCP, котрий для перевірки цілісності пакетів застосовує контрольні суми, а для відстежування процесу передавання – механізм вікон. Аналіз вищезазначених механізмів дозволяє зробити висновок про необхідність комплексного підходу до забезпечення функціональної живучості ТКМ, який поєднає в собі різнопланові властивості механізмів забезпечення визначеної перепускної спроможності, що працюють на різних рівнях (OSI). Це можливо шляхом модифікації алгоритму прийому-передачі повідомлень напрямком ТКМ. В алгоритмі прийому-передачі для отримання повідомлення адресат повинен прийняти всі пакети з яких складається повідомлення без викривлень. Викривлення або не отримання хоча б одного пакету все повідомлення прийнятим не буде, а викривлений пакет буде перезапитаний. Кількість перезапитів може доходити до безкінечності якщо на ТКМ здійснюється вплив агресивного зовнішнього середовища, а саме будь яких завад. В результаті цього, відправлене повідомлення не буде отриманим, що є неприпустимим. Рішення цієї проблеми є спроба зменшення кількості транзакцій при передачі текстової інформації з використанням методик зменшення кількості транзакцій текстового повідомлення шляхом відновлення інформації, що була викривлена під час передачі та методики прогнозування груп символів в пакеті повідомлення. Завдяки існуванню кореляційних зв’язків між текстовими символами в повідомленні можливо з заданою вірогідністю відновити викривлену інформацію та зробити висновок про ступінь приналежності відновленого пакету повідомлення пакету відправленому через телекомунікаційну мережу.

Кононова І.В. (ВІТІ НТУУ „КПІ”)
Петров А.В. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ МОЖЛИВОСТЕЙ IP-ТЕЛЕФОНІЇ З ПОГЛЯДУ БЕЗПЕКИ ФУНКЦІОНУВАННЯ МЕРЕЖІ

IP-телефонія – це технологія, яка зв’язує світ телефонії і світ Інтернет. До недавнього часу мережі з комутацією каналів (телефонні мережі) і мережі з комутацією пакетів (IP-мережі) існували практично незалежно один від одного і використовувалися для різних цілей.

Для систем IP-телефонії, побудованих на базі Рекомендації ITU-T H.323, питання безпеки розглядаються в Рекомендації H.235. Ця рекомендація описує ряд технічних вимог, включаючи питання безпеки: аутентифікація користувачів і шифрування даних. Якщо для IP-телефонії стандарту H.323 використовуються мережі з пакетною комутацією, що не забезпечують гарантованої якості обслуговування QOS, то з тих же самих технічних причин не забезпечується і безпечне обслуговування.

Для забезпечення гарантованого зв’язку в реальному масштабі часу по небезпечних мережах необхідно розглядати дві головні області забезпечення безпеки – аутентифікація і секретність. Або, якщо дивитися ширше, це проблема доступу до мережевих ресурсів і проблема доступності інформації безпосередньо в каналах мультисервісної мережі. Причому проблема доступу до ресурсів мережі не обмежується тільки аутентифікацією користувача, в результаті якої він фактично лише отримує певні послуги; мова йде також про доступ до адміністрування мережі і мережевого устаткування, до баз даних (що дуже актуально для компаній, які надають послуги Інтернету).

В каналах мережі IP-телефонії, небезпеку представляє загроза підслуховування. Відповідно до Рекомендації H.235 в системі повинні бути реалізовані чотири основні функції безпеки: аутентифікація; цілісність даних; секретність; перевірка відсутності боргів.

Аутентифікація користувача забезпечується управлінням доступу в кінцевій точці мережі і виконується сторожем, адміністратором зони H.323. Аутентифікація ґрунтується на використанні загальних ключів з цифровим сертифікатом. Для авторизації сертифікатів вони включають, наприклад, ідентифікатори провайдера послуг.

Цілісність даних і секретність забезпечується криптографічним захистом. Перевірка відсутності боргів гарантується тим, що кінцева точка може відмовити в обслуговуванні виклику. Для забезпечення безпеки згідно рекомендації H.235 можуть використовуватися існуючі стандарти: IP-безпека (IP Security – IPSec) і безпека транспортного рівня (Transport Layer Security – TLS).

Для забезпечення безпечного зв’язку в системі на базі Рекомендації H.323 використовуються механізми захисту інформації каналу управління викликом Q.931, інформації каналу управління для мультимедіа комунікацій H.245, інформації каналів передачі мультимедіа. Канал управління викликом (H.225.0) і канал сигналізації (H.245) повинні працювати в захищеному або незахищених режимах, що починається з першої станції.

Спростити процес впровадження технології IP-телефонії покликаний проект TIPHON (Telecommunication and Internet Protocol Harmonization over Networks), реалізація якого дозволить успішно вирішити задачі встановлення, модифікації і завершення телефонних з’єднань, включаючи процеси міжмережевої взаємодії, управління безпекою виклику, запиту якості обслуговування, шифрування, аутентифікації та інші.

У проект включені наступні механізми захисту для забезпечення безпеки телефонного зв’язку з кінцевих пристроїв, засновані на додатку J рекомендації ITU-T H.323: Механізм захисту, заснований на цифрових сертифікатах (CBSP); Механізм захисту, заснований на паролях (PBSP); Механізм захисту, заснований на шифруванні інформації.

Компанії 3Com, Cisco і ряд інших повідомили про підтримку стандарту IP-телефонії – Open Settlement Protocol (OSP), який призначений для вирішення взаємодії мереж різних провайдерів. Це простий протокол, що дозволяє різним компаніям – власникам засобів зв'язку, здійснювати комунікації в межах всієї країни. Наприклад, він дозволяє встановлювати автора дзвінка, санкціонувати обслуговування виклику і вказувати розрахункову інформацію, яка буде включена в записи, що містять подібні дані про цю транзакцію.

Робоча група інституту ETSI схвалила цей протокол, а виробники найближчим часом мають намір провести його тестування. Новий протокол був розроблений в рамках проекту TIPHON.

Питання безпеки в протоколах SIP і MGCP. Даний протокол, використовується абонентськими пунктами для встановлення з'єднання, не володіє серйозним захистом і орієнтований на застосування рішень третіх фірм (наприклад, PGP). Як механізм аутентифікації RFC 2543 пропонує декілька варіантів і, зокрема, базову аутентифікацію (як в HTTP) і аутентифікацію на базі PGP. Намагаючись усунути слабку захищеність даного протоколу, Майкл Томас з компанії Cisco Systems розробив проект стандарту IETF, названий „SIP security framework", який описує зовнішні і внутрішні погрози для протоколу SIP і способи захисту від них. Зокрема, до таких способів можна віднести захист на транспортному рівні за допомогою TLS або IPSec. Компанія Cisco в своїй архітектурі безпеки корпоративних мереж SAFE, дуже велика увага приділяє практичним питанням захисту IP-телефонії.

Стандарт MGCP, визначений в RFC 2705, який не застосовується на крайових пристроях (шлюзи MGCP можуть працювати як з компонентами, підтримуючими H.323, так і з компонентами, підтримуючими SIP), використовує для захисту голосових даних протокол ESP специфікації IPSec. Може також використовуватися і протокол AH (але тільки не в мережах IPv6), який забезпечує аутентифікацію і цілісність даних (connectionless integrity) та захист від повторень, передаваємих між шлюзами. В той же час, протокол AH не забезпечує конфіденційності даних, яка досягається застосуванням ESP (разом з іншими трьома захисними функціями).

ЛІТЕРАТУРА

1. *Амато В.* Основы организации сетей Cisco. Том 1. М.: Издательский дом „Вильяме", 2002.

2. *Амато В.* Основы организации сетей Cisco. Том 2. М.: Издательский дом „Вильяме", 2002.

3. *Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л.* IP-телефония. М.: Радио и связь, 2001.

5. *Лукацкий А.В.* Атаки на VPN. „Компьютер-Пресс", № 3. 2002.

6. *Лукацкий А.В.* IP-опасность для бизнеса. „Мир связи. Connect", № 8. 2002.

7. *Лукацкий А.В.* Системы обнаружения атак. „Сетевой", № 4. 2002.

8. *Олифер В.Г., Олифер НА*. Компьютерные сети. СПб.: Питер, 2002.

9. *Росляков А.В., Самсонов М.Ю., Шибаева И.В.* IP-телефония. М.: Эко-Трендз, 2003.

10. *Смит Ричард Э.* Аутентификация: от паролей до открытых ключей. М.: Издательский дом „Вильяме", 2002.

11. *Столлинз Вильям.* Криптография и защита сетей. Принципы и практика. 2-е издание. М.: издательский дом „Вильяме", 2002.

12. *Уэнстром Майкл.* Организация защиты сетей Cisco. М.: Издательский дом „Вильяме", 2003.

13. Материалы сайта НПО Информ-защита http://www.infosec.ru.

14. Материалы сайта НИИ Телекоммуникационных систем http://www.niits.ru.

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

# БЕЗДРОТОВІ ТЕХНОЛОГІЇ ДОСТУПУ ДО ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

Умови експлуатації більшості абонентських кабелів не дозволили зберегти в заданих нормах ті характеристики, які є істотними з точки зору передачі сигналів, що вимагають ширшої смуги пропускання в порівнянні з тією, що забезпечується каналом тональної частоти. Крім того, пристрої кросування кабельних жил вносять спотворення до сигналів, що передаються, які особливо помітні за межами смуги пропускання каналу тональної частоти.

Актуальність проблем, пов’язаних з модернізацією мереж доступу, що експлуатуються, пояснюється двома основними чинниками. По-перше, ті технічні характеристики, які властиві більшості абоненських лініям, не можуть забезпечити сучасні вимоги до надійності зв’язку і до якості передачі телефонної й іншої (зокрема, – дискретної) інформації. По-друге, мережі доступу, що існують нині, стають „вузьким горлом” для процесу введення того нового вигляду інфокомунікаційних послуг, які орієнтовані на істотне розширення пропускної спроможності абонентських ліній і/або на вищі показники якості передачі інформації.

Одним із шляхів вирішення цих проблем і є бездротові технології доступу. Успіхи в області електроніки дозволяють створювати радіотехнічне устаткування з такими характеристиками якості і надійності, які раніше забезпечувалися тільки засобами проводового зв’язку.

Одним із широкосмугових мереж бездротового доступу представлено технологією *Wi-Fi (Wireless Fidelity)*. Ця абревіатура використовується для сукупності *WLAN (Wireless Lokal Area Netvork)*, переважно які відповідають стандартам *IEEE* 802.11a і *IEEE* 802.11*b*.

Такі мережі створюються в зонах обслуговування потенційних клієнтів (*hot spot*) – аеропорти, готелі, бізнес-центри і подібні до них місця. У цих зонах вмонтовуються базові станції, обслуговуючі територію, визначену ліцензією на послуги широкосмугового доступу в *Internet.* Мережа працює за принципом локальної мережі, що і пояснює її другу назву – *WLAN*. Для мереж *Wi-Fi* виділено два основні діапазони: 2,4 ГГц і 5 ГГц.

У цих діапазонах можуть бути організовані мережі бездротового доступу із швидкістю обміну даними до 54 Мбіт/с (стандарт *IEEE* 802.11*g*), але поки за верхній кордон вважається величина 11 Мбіт/с, що визначене стандартом *IEEE* 802.11*b*. Вихід абонентів в *Internet* забезпечується через цифрові комутаційні пристрої, які встановлюються біля кожної базової станції.

**Висновки.** У більшості розвинених країн мережі доступу модернізуються за рахунок встановлення різного радіотехнічного устаткування. Це пояснюється багатьма причинами: економія витрат на прокладання кабелів (особливо в складних геологічних умовах), скорочення об’єму робіт по технічному обслуговуванню лінійних споруд, прискорення введення устаткування в комерційну експлуатацію.

Очевидні експлуатаційні переваги мереж бездротового доступу підкріплюються зниженням цін на відповідне устаткування. Ці аргументи свідчать про те, що при модернізації всієї системи зв’язку особливу увагу слід приділити оптимальному використанню засобів бездротового доступу.

к.військ.н. Костина О.М.(ЦНДІ ОВТ ЗСУ)

# НАПРЯМИ РОЗВИТКУ ЗАСОБІВ ЗВ'ЯЗКУ І АВТОМАТИЗАЦІЇ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Провідним напрямом розвитку системи зв'язку і автоматизації управління військами є побудова цифрової інтегральної мережі зв'язку (ЦІМЗ) Збройних Сил України, яка дозволить створити єдине інформаційне поле в інтересах усіх видів і родів військ усіх ланок управління.

Основу ЦІМЗ складає транспортна мережа, яка надає ресурс для розгортання єдиної автоматичної телефонної мережі Збройних Сил України та мережі АСУ „Дніпро" для всіх видів Збройних Сил України і родів військ усіх ланок управління.

Наступним пріоритетом розвитку системи зв'язку і автоматизації Збройних Сил України є переобладнання мобільного компонента.

Особлива увага в даному питанні приділяється тому, щоб польові комплекси засобів зв'язку і автоматизації всіх ланок управління різних видів Збройних Сил України були сумісні між собою та ЦІМЗ і створили єдине транспортне середовище для передавання повідомлень в інтересах всіх військ (сил).

Заміна існуючих засобів зв'язку і автоматизації (переозброєння військ) здійснюється такими шляхами:

використання засобів як вітчизняного, так і іноземного виробництва цивільного і військового призначення. Цей шлях характерний для стаціонарного компонента;

закупівля засобів іноземного виробництва військового призначення. Цей шлях доцільний у випадку, коли виробництво відповідних зразків промисловістю України неможливе або економічно недоцільне;

модернізація існуючих комплексів та засобів зв'язку і автоматизації, розробка та випуск перспективних засобів промисловістю України. Модернізація доцільна у відношенні засобів, які мають достатній запас ресурсу, за своїми закладеними технічними рішеннями можуть бути модернізовані для роботи в цифрових системах, та з врахуванням економічної доцільності модернізації.

Для здійснення визначених напрямів розвитку системи зв'язку і автоматизації проводиться ряд науково-дослідних (НДР) і дослідно-конструкторських (ДКР) робіт, метою яких є розробка оперативно-тактичних (тактико-технічних) вимог, системотехнічних питань побудови системи зв'язку і автоматизації, визначення перспективних напрямів її розвитку, модернізація існуючих та розробка перспективних зразків комплексів та засобів зв'язку і автоматизації.

Так, в липні 2007 року на базі ВАТ „Олімп" (м. Світловодськ) проведено державні випробування та прийнято на озброєння модернізовану станцію тропосферного зв'язку Р-417МУ. На даний час підприємство проводить розробку базової цифрової радіорелейної станції та модернізацію станції тропосферного зв'язку Р- 423-1, що дасть можливість інтегрувати їх у ЦІМЗ.

ТОВ „Телекарт-Прилад" (м. Одеса) протягом останніх чотирьох років проводить розробку цифрових засобів зв'язку та автоматизації військового призначення, сумісних зі стандартами провідних країн світу, деякі з яких вже пройшли державні випробування й прийняті на озброєння (радіорелейна станція Р-450; польовий телефонний апарат ТА-01; цифровий телефонний апарат ЦТА-04; цифрова автоматична комутаційна система К-201; УКХ радіостанції Р-030У, Р-005У, Р-002У; маршрутизатор А-201; модеми кабельні М-101 та Ethernet; обладнання комутації та мультиплексування трактів К-1301 та ін.), а розробка ряду з них ще продовжується (комплексна апаратна зв'язку; командно-штабна машина; машина електронно-обчислювальна бортова; КХ радіостанція; термінал тактичний; VoIP шлюз військового призначення).

к.т.н. Коцюба В.П.(ЦНДІ ОВТ ЗСУ)
Ніколаєнко Д.М. (ЦНДІ ОВТ ЗСУ)

# РОЗВИТОК УПРАВЛІННЯ ЧАСТИН І ПІДРОЗДІЛІВ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ СИСТЕМ В СУЧАСНИХ УМОВАХ

В теорії воєнного мистецтва і практиці підготовки військ (сил) питання управління просідають одне з найважливіших місць, оскільки воєнна наука завжди розглядала ефективне управління військами (силами), як одну з важливих умов перемоги, підкреслюючи його особливу роль у досягненні успіху в операції.

На сьогоднішні це важливо ще й тому, що управління, як ніколи раніше, стає одним з основних чинників збройної боротьби, який визначає не тільки її хід та результат, але й саму можливість ведення бойових дій військами та силами. Необхідно також зауважити, що ефективне управління військами та силами в мирний та воєнний час – це один з потужних важелів інтенсифікації розвитку усіх сторін військової справи. Можна мати найновішу зброю, бойову техніку і добре навчений особовий склад, але коли вони заздалегідь не будуть переведені в потрібну ступінь бойової готовності, своєчасно введенні в дію та націлені на завдання поразки агресору, то існуючі потенційні можливості військ (сил) можуть бути не реалізовані, і, як наслідок, не виконані бойові завдання. В сучасному воєнному мистецтві є як позитивні, так і негативні приклади наведеної тези. Так, чотири близькі за змістом операції: „Буря в пустелі”, „Лис пустелі”, „Союзницька сила” та „Свобода Іраку” – явили собою спробу досягнення політичних цілей країнами (групою країн) воєнним шляхом.

Аналіз цих операцій дозволяє помітити одну важливу тенденцію концептуального характеру – трансформування сучасної воєнної стратегії від орієнтації на масштабні загальновійськові операції до переважаючого застосування повітряно-ракетних ударів високоточною зброєю із застосуванням глобальної системи управління, елементи якої можуть бути одночасно розгорнуті на декількох континентах з широким використанням повітряного та космічного простору. Аналіз проведених операцій збройних сил передових у воєнному відношенні країн світу кінця 20 початку 21 сторіччя дозволив виявити такі тенденції, що безпосередньо стосуються теорії і практики управління військами:

по-перше, це поступовий переходу від управління силами і зброєю як двох відносно самостійних складових до управління збройною боротьбою, яке передбачає взаємне інтегрування всіх складових і необхідність одночасного впливу органів управління на процес збройної боротьби в реальному часі;

по-друге, це значні зрушення в бік інформатизації та автоматизації управління військами та зброєю із широким використанням космічного простору. Причому для збройних сил провідних країн світу питання автоматизації управління військами та зброєю – вже практично вирішена проблема, зараз проводиться подальше удосконалення та розвиток автоматизованих систем управління. Для цих країн більше значення мають питання, які стосуються всебічної інформатизації роботи органів управління усіх ланок;

по-третє, це зростання вогневого та інформаційного впливу на системи державного та військового управління противника.

Переконливим прикладом цього є повітряно-космічна морська ударна операція збройних сил США та Великої Британії у Югославії, коли за рахунок вогневого, радіоелектронного та інформаційного впливу альянс здійснив блокування більшої частини державної та військової системи управління Югославії. Інший приклад такого масштабу можна навести з досвіду збройного конфлікту в Перській затоці.

Аналіз досвіду війн та збройних конфліктів, особливо бойових дій у зоні Перської затоки та на Балканах свідчить, що планування і здійснення оперативно-тактичних заходів щодо захисту підрозділів зв’язку та інформаційних систем від ударів високоточної зброї, а також скритого управління ними істотно знижує ефективність цих ударів, а також ускладнює дії розвідувально-диверсійних груп.

Коченовський Д.О (ВІТІ НТУУ„КПІ”)

# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ GRID ТЕХНОЛОГІЙ В СУЧАСНИХ ТЕЛЕКОМУНІКАЦІЯХ

У концепції розвитку наукової сфери України зазначається, що реалізація стратегічного курсу України на інтеграцію у Європейське співтовариство, побудова процвітаючої держави неможлива без розвитку сучасних інформаційних технологій.

Серед пріоритетних напрямків інформатизації та розвитку сучасних інформаційних технологій є створення Національної Grid-інфраструктури для наукових досліджень.

Grid-технології і всесвітня Grid-мережа поступово замінюють уже звичайний Internet з його Web-послугами як засіб сумісного використання обчислювальних потужностей та сховищ даних, перетворення їх на своєрідний гігантський віртуальний комп’ютер, доступний у режимі віддаленого доступу з будь-якої точки, незалежно від місця розташування користувача.

Grid є технологією забезпечення гнучкого, безпечного і скоординованого загального доступу до ресурсів.

Grid – це розподілене середовище, функціонування якого забезпечується спеціальним програмним забезпеченням – у вигляді сервісів. Сервіс мають мережевий інтерфейс, завдяки чому стає можливим віддалене обслуговування клієнтів. На відміну від моделі „клієнт-сервер” у Grid той або інший набір сервісів установлено на кожному ресурсі, хоча використовують традиційне серверне обслуговування.

Для кооперативної діяльності сукупність сервісів має задовольняти дві структурні умови.

– кожен тип сервісу повинен мати стандартний протокол доступу, відповідно до якого реалізується прикладний інтерфейс (*API – Appliation Programming Interface*) клієнтів, У межах стандартних протоколів допустимі різні способи реалізації сервісного обслуговування;

– сукупність сервісів на різних ресурсах має бути узгодженою. Це допускає відому уніфікацію наборів сервісів на основі тотожності їх семантики, а також наявність загальних правил, регламентів і організаційних угод, на які спирається конфігурація сервісів.

Національна Grid-інфраструктура створюється для обслуговування різноманітних організацій з різноманітними характеристиками і вимогами до ресурсів. Для об’єднання різнорідних ресурсів єдина обчислювальна інфраструктура повинна мати єдину архітектуру. Можливість упорядковування різноманітного обладнання і ресурсів забезпечується попереднім визначенням базових функцій Grid-інфраструктури.

Grid-технології активно застосовують у світі як державні організації управління, оборони, сфери комунальних послуг, так і приватні компанії, наприклад, фінансові та енергетичні. Останнім часом Grid-технології застосовують у ядерній фізиці, у сфері захисту навколишнього середовища, прогнозування погоди і моделювання кліматичних змін, числовому моделюванні в машино- та авіабудуванні, біологічному моделюванні, фармацевтиці тощо.

Для забезпечення цього використовувати істотно відмінні механізми доступу, наприклад паралельне передавання даних широкосмуговою мережею від віддаленого паралельного комп’ютера до локального паралельного комп’ютера.

Кочетков О.В. (ВІТІ НТУУ„КПІ”)

# ПІДВИЩЕННЯ ЗАВАДО - СТІЙКОСТІ ПАКЕТІВ ПОВІДОМЛЕНЬ У ЦИФРОВИХ ЛІНІЯХ ЗВ’ЯЗКУ РУХОМИХ ОБ’ЄКТІВ

Лінії зв’язку пересувних об’єктів, насичених випромінюючими радіоелектронними засобами, працюють у складної завадової обстановці. Крім завад, викликаних впливом відображення від підступаючої поверхні за рахунок богатопроміневого розповсюдження радіохвиль при сильно вирадженної різновисотності антен радіоліній, також характерні вплив короткочасних завад, по рівню значно перевищуваємий приймаємий сигнал .

Захист від імпульсних завад за допомогою бланкирування прийому у момент впливу завад крім того веде до втрати частки інформації, а також викликає порушення роботи системи синхронізації, що в свою чергу викликає знижування ефективності використовуваних засобів боротьби з завадами богатопрміневості і в кінцевому рахунку веде до затримання пакетів повідомлень.

Для підвищення завадо – стійкості цифрових ліній зв’язку рухомих об’єктів та скорочення часу доставки пакетів пропонується метод компенсації завад богатопрміневості та імпульсних завад, застосовуваний до сигналу складної структури, ураховуючи обмеження на затримку та забезпечуючий безперервне звучання відновлюваної мови на приймальної стороні. За допомогою цього методу можливо значно підвищити завадо - стійкість відправлених абонентами повідомлень.

ЛІТЕРАТУРА

1. *Слюсар В. И.* Идеология построения мультистандартных базових станций перспективных систем связи// Радиоэлектроника. (Изв. высш. учеб. завед.). – 2001. – № 4. –С. 3 – 12.

2. *Слюсар В.И.* Быстродействующие АЦП: достижения и перспективы // Радиоэлектроника (Изв. высш. учебн. завед.). – 2000. – №3. – С. 42 – 46.

3. *Conticello C.* Spread Spectrum Communications: an Overview // Alta Frequenza, 1987. – V. LVI. – № 6. – P. C. 255 – 264c.

4. *Тузов Г.И., Козлов М. Р.* Помехозащищенность систем связи, использующих сигналы с псевдослучайной перестройкой рабочей частоты // Зарубежная радиоэлектроника, 1989. – № 3. – С. 19 – 32.

5. *Putman C A., Rappaport S S., Schilling D.L.* A Comparison of Schemes for Coaisc Acquisition of Frequency-Hopped Spread-Spectrum Signals // IEEE Trans, 1983. – V. COM-31. – № 2. – P. 183 – 189c.

6. *Levilt B.K., Cheng U., Polydoros A., Simon M.K.* Optimum Detection of Slow Frequency-Hopped Signals // IEEE Trans, 1994. – V. 42. – № 2/3/4. – P. 1990-2000.

7. *Кравченко В.Ф., Рвачев В.А., Рвачев В.Л.* Математические методы обработки сигналов на основе атомарных функций// Радиотехника и электроника. – Т.40. – № 9. –1995. – С. 1385–1406.

8. *Бабич В. Д., Кувшинов О. В., Лівенцев С. П., Лежнюк О. П.* Модульовані сигнали : Навчальний посібник. – К.: КВІУЗ, 2001. – 185с.

к.т.н. Круковський І.А.(ЖВІ НАУ)
к.т.н. Перегуда О.М. (ЖВІ НАУ)

# МЕТОДИКА ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Якість (корисність) програмного забезпечення (ПЗ) досить складна та ємна категорія. Традиційно під корисністю ПЗ розуміють ступінь виконання конкретним засобом свого функціонального призначення. У найпростішому випадку оцінкою цього може бути висновок щодо відповідності ПЗ вимогам до функціонального призначення, наприклад, „відповідає вимогам" або „не відповідає вимогам". Проте, коли кілька ПЗ в цілому відповідають таким вимогам, виникає потреба порівняти їх між собою, щоб обрати кращий. Ще більше ускладнюється задача, коли необхідно оцінити корисність ПЗ для певної корпоративної групи користувачів. У такому випадку необхідно ввести певну систему показників якості ПЯ (корисності) ПЗ.

Показник якості може бути числовим або якісним (лінгвістичним) значенням, яке характеризує оцінку корисності певних функцій (характеристик) ПЗ. Показники якості можуть бути частковими та комплексними (узагальненими). Часткові показники дозволяють оцінити ПЗ за якоюсь однією характеристикою (наприклад, швидкодія, обсяг необхідної оперативної пам'яті, можливість роботи з певним форматом даних, ін.). Часткових ПЯ для одного ПЗ може бути велика кількість і характеристики ПЗ які відповідають цим показникам можуть бути нерівнозначні за своєю важливістю. Узагальнені ПЯ є результатом агрегатування кількох часткових показників.

Оцінювання ПЗ лише за частковим показниками можливе лише у випадку відносно невеликої кількості цих показників (згідно „правила Міллера" – від 1 до 9). При використанні узагальненого ПЯ цієї вади немає, але, коли значення узагальнених показників близькі, виникає потреба оцінити ПЗ за частковими показниками, що у деяких випадках неможливо. Крім цього, процес визначення корисності ПЗ конкретними групами користувачів у багатьох випадках виходить за можливості його повного формального опису, що також потребує ґрунтовного порівняльного аналізу ПЗ за обраними частковими показниками. За результатами дослідження розроблено методику оцінювання якості ПЗ, яка дозволяє здійснювати оцінювання за системою часткових та узагальнених ПЯ, у тому числі з використанням єдиного комплексного показника.

Методика заснована на використанні системного підходу та експертної інформації. В основу методики покладено модернізований метод аналізу ієрархій Сааті. Особливістю методики є те, що вона дозволяє оцінити ПЗ одночасно за великою кількістю різнорідних часткових показників якості, які об'єднані в ієрархічну структуру.

Методика складається з двох етапів.

На першому етапі будується модель оцінювання якості ПЗ у вигляді кількарівневої деревовидної ієрархічної структури часткових ПЯ. Кількість рівнів показників, які об'єднуються в ієрархічну структуру визначається за кілька етапів шляхом опитування експертів. На цьому ж етапі шляхом попарного порівняння визначається важливість часткових показників на кожному ієрархічному рівні.

На другому етапі, з використанням отриманої на першому етапі моделі оцінювання проводиться безпосереднє оцінювання якості ПЗ шляхом експертного оцінювання з використанням п'ятибальної число-лінгвістичної шкали для всіх часткових ПЯ. Після цього обчислюються значення узагальнених ПЯ, у тому числі значення єдиного головного узагальненого ПЯ ПЗ. Крім цього, проводиться грунтовний порівняльний аналіз ПЗ за обраними показниками з використанням OLAP моделювання.

Перевагами методики є врахування великої кількості різних ПЯ при оцінюванні ПЗ, врахування важливості обраних показників, а також можливість розгляду та порівняльного аналізу різних засобів за окремими частковими чи частково узагальненими показниками.

к.т.н. Круковський І.А.(ЖВІ НАУ)

# РОЗШИРЕНІ ВИМОГИ ДО РЕАЛІЗАЦІЇ OLAP У ПРИКЛАДНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Надбудовані над сховищами, вітринами, кіосками даних (Data Warehouse, Data Mart) засоби швидкого аналізу багатовимірної інформації (On-line Analytical Processing, OLAP) є важливими елементами систем підтримки прийняття рішень (Decision Support System, DSS), які часто називають інформаційно-аналітичними системами і відносять до систем управління знаннями (Knowledge Management System, KMS), що є основою засобів бізнес-розвідки (Business Intelligence, BI). DSS з OLAP часто використовують для реєстрації, класифікації, пошуку, багатовимірного аналізу даних, який також доповнюють інтелектуальним аналізом даних (Data Mining, DM), ін.

Для визначення OLAP у 1993 р. Е. Кодд і партнери опублікували 12 правил, що у 1995 р. доповнені і відомі як „12+6 правил Кодда”.

У 1995 р. Н. Пендс і Р. Кріт році піддали критиці тест Кодда і розробили на його основі узагальнений тест „FASMI” (Fast Analysis of Shared Multidimensional Information, FASMI).

З того часу тести незмінні і є стандартами „де факто” для OLAP. Аналіз публікацій, створення і використання DSS з OLAP показує, що їх реалізація згідно вказаних тестів значно підвищує ефективність програмних засобів підтримки інформаційно-аналітичної роботи. Проте, у вимогах тестів є недоліки, що тиражуються у прикладних системах, тому тести необхідно удосконалити.

Недоліком тестів є розробка вимог до аналізу „даних” та „інформації” без урахування базових властивостей „знань” у KMS, насамперед, властивості їх „ситуативної активності”. У результаті, розробники та користувачі DSS з OLAP не приділяють увагу реалізації багатокритерійних продукційних правил ситуативної самоактивації даних на основі модусу поненс логіки та інтеграції їх з функціями багатовимірного аналізу, хоча це просто реалізувати як окрему функцію або логічне продовження базових функцій DM у сучасних системах із вбудованою мовою рівня 4GL. Вказана властивість знань є глобальною і не може бути проігнорована. Виходячи з цього, до 5 -ти ключових слів тесту FASMI можливо добавити ще одне – „Active”, як позначення вимоги забезпечення інтегрованої функції ситуативної самоактивності даних.

Другим суттєвим недоліком існуючих тестів є вимога обов’язкової наявності розділеного доступу користувачів до елементів бази даних в OLAP-системі. Проте, у реальних умовах експлуатації DSS групою користувачів, склад якої з часом змінюється, наявність розділеного доступу до бази даних приводить з різних причин до створення умов для порушень безпеки інформації, у тому числі катастрофічних для BI корпоративного рівня. Для усунення недоліку доцільно використовувати комбінації резервування й реплікації OLAP-системи, відкриття реплік у режимі „тільки для читання”, ін. Для позначення цієї особливості їх функціонування можливо замінити позначення 3-го ключового слова у тесті FASMI з „S” на „S*”.

Ще один суттєвий недолік тестів може проявлятися при розробці рознесених інформаційних систем, у яких знання створюються у підсистемах, проте можуть об’єднуватися не тільки шляхом ієрархічної інтеграції, але й шляхом ситуативної синергетичної інтерації. Необхідність забезпечення синергії (Sinergia, S) знань є глобальної вимогою і також не може бути проігнорована. Хоча цю вимогу можливо вважати базовою для Data Warehouse, проте у багатьох випадках його функції доцільно відразу покласти на OLAP, тому доцільно віднести дану вимогу і до відповідних прикладних систем.

Отже, під час розробки DSS із вказаними вище особливостями доцільно удосконалити тестові вимоги до прикладної реалізації OLAP, а удосконалений тест можливо позначити як FAS*MASI.

Крупська М.В. ( ІТС НТУУ „КПІ”)
к.т.н. Ладик О.І.( ІТС НТУУ „КПІ”)

# УДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ ШИРОКОСМУГОВОГО ДОСТУПУ CDMA

Система WCDMA Ericsson представляє новий метод розгортання технології CDMA, що включає мінісоти і адаптивні антени. Використовуючи когерентну демодуляцію як в зворотному, так і в прямому каналах, система WCDMA може обслуговувати у вісім разів більше абонентів на еквівалентну смугу, ніж існуючі вузькосмугові системи. Це буде забезпечувати пропускну спроможність для більш ніж [1]: 1) 100 одночасних розмов на несучу при використанні 8 кбіт/с вокодера; 2) 50 одночасних користувачів Інтернет на несучу, кожен з яких працює, безпосередньо використовуючи швидкість передачі даних 384 кбіт/с.

У разі „естафетної передачі” зі зміною несучої частоти (при переході мобільної станції стільникового від одного рівня до іншого) безперервність зв’язку забезпечується використанням двочастотних приймачів, які підтримують сигналізацію на двох частотах, або переходом на режим з тимчасовим поділом, званий „компресуваним режимом”, коли інформація, що передається MS і BTS в 10 мс-му кадрі CDMA, стискається в два рази за рахунок зміни швидкості PN коду. При цьому потужність переданих сигналів подвоюється. Друга половина цього кадру використовується для вимірювання та сигналізації в сусідньому радіоканалі.

Крім того, система WCDMA Ericsson буде надавати більшу гнучкість у швидкості передачі даних користувача, що є однією з концепції WCDMA, розробленої в проекті CODIT. Змінна швидкість передачі даних – починаючи з 8 кбіт/с і до 384 кбіт/с може визначатися для різних і множинних абонентів на кожній 5 МГц несучої. Більш того, послуги з різним вимогою до якості, такі як мова і пакетні дані, можуть підтримуватися з відмінною пропускною спроможністю і покриттям.

Система WCDMA сполучена останнім мінісотовим протоколом передачі з асинхронним режимом передачі (ATM) – відомим як Адаптований рівень 2 ATM (AAL2). Цей протокол буде використовуватися для передачі даних між базовою станцією та центром комутації рухомого зв’язку через контролери базових станцій. Стандартизований на початку 1997 Форумом ATM, AAL2 дозволяє більшій кількості пакетів даних передаватися більш ефективно і з меншою затримкою. Таким чином, дані передаються лише тоді, коли абонент знаходиться в активному з’єднанні. Цей розвиток протоколу ATM дозволяє майже 300 голосовим з’єднанням передаватися через стандартну T1/E1 лінію, де раніше могли передаватися тільки 30 голосових з’єднань. Такий же виграш можливий при передачі даних. Оскільки AAL2 надає функції, необхідні для „м’якого” handoff між несучими, все це рішуче знижує вартість передачі даних.

Удосконалення Ericsson технології з кодовим поділом включають новий метод handoff між несучими WCDMA. Названа Тим-Частотний Handoff (IFHO) це нова технологія полегшує використання мікросот з малою потужністю. IFHO дозволяє, також, установку мікросот в порядок, званий Ієрархічна Стільниковий Структура (HCS). Це робить можливим, наприклад, використання мікросоти для збільшення пропускної спроможності в офісній будівлі, на даху якого, в той же час, встановлена макросота. Ericsson успішно розгорнув технологію HCS в системах другого покоління з тимчасовим ущільненням, таких як стандарти GSM і IS-136. Використовувані разом, IFHO і HCS дають відмінність у плануванні системи з кодовим поділом і створюють велику потужність мережі WCDMA, ніж існуючі вузькосмугові системи. WCDMA, також, повністю підтримує використання само-юстірующіхся антен (AAA), технології, в якій випромінювання антени направляється на кожного абонента. Це є корисним у місцях, де можливе обмеження радіочастотного спектра для широкосмугового обладнання. Використовуючи технологію AAA, прикріплений до

станції абонент може обслуговуватися з широкосмуговими послугами і як пропускна здатність, так і покриття можуть постійно поліпшуватися. На відміну від вузькосмугових систем, кожне термінальне підключення WCDMA може постачати до шести різних послуг - починаючи з голосу і до комбінації послуг з передачі даних, таких як факс, електронна пошта та відео. Кожна з шести послуг може оптимізуватися як необхідна швидкість передачі даних і специфічний стандарт якості. Для забезпечення оптимальної гнучкості і усунення інтерференції між абонентами, які працюють з різною швидкістю на одній РЧ несучої, система WCDMA використовує, також, спеціальні широкополосні коди, звані ортогональний Фактор зі змінним розширенням (OVSF-коди).

Іншим вдосконаленим властивістю технології WCDMA є найпотужніший метод повного придушення інтерференції, який виключає інтерференцію від інших абонентів, і також, збільшує пропускну здатність. Він виявляє зайвих абонентів і виключає інтерференцію в ряді випадків, які можуть відбуватися в вузькосмугових системах CDMA. Така технологія виключення інтерференції WCDMA дозволяє працювати з мікросотами великої пропускної здатності, коли непередбачена інтерференція скоріше може відбутися в порівнянні з обстановкою в макросоті.

Розробка WCDMA також ліквідувала необхідність у синхронізації між базовими станціями, які в вузькосмуговому обладнанні вимагали використання GPS приймачів на кожній базової станції для встановлення супутникового тріангуляції та забезпечення мікросекундної точності радіопередачі. В якості синхронізації виступають тактові імпульси, що надходять від контролера базових станцій. Кожна базова станція може обслуговувати до шести секторальних антен, за дві несучі на кожен сектор (ширина несе в WCDMA становить 5 МГц). Вихідна потужність передавальної апаратури складає 20 Вт на сектор.

Основні характеристики системи:

робота широкосмугового CDMA з несучої (тактовою) частотою 5 МГц:

гнучкість фізичного рівня, що дозволяє об’єднати всі швидкості передачі даних на одній несучої;

одноразове повторне використання.

Удосконалення включили в себе:

рознесення передачі;

використання адаптивної антени;

підтримка вдосконалення побудови приймачів.

Концепція WDCMA отримала широке визнання; в технічному відношенні найбільше підкупила гнучкість фізичного рівня, що дозволяє забезпечувати різні види сервісу одночасно [2]. Це вагома перевага, особливо при використанні низьких і середніх швидкостей передачі. Як недоліки WCDMA було визнано те, що в не узгодженої системі в режимі TDD при безперервній роботі на прийом і передачу технологія чистої WCDMA не дозволяє поліпшити захист від перешкод при використанні безпровідних телефонів.

ЛІТЕРАТУРА

1. *Тихвинский В.О.* Управление и качество услуг в сетях GPRS/UMTS / В.О. Тихвинский, С.В. Терентьев // М.: Эко-Трендз, 2007. – 400 с.: ил.

2. *Ovesjo, F., Dahlman, E.,* Ojanpera, T., Toskala, A. and Klein, A., „FRAMES Multiple Access Mode 2 – Wideband CDMA”, Proc. IEEE Int. Conf. on Personal Indoor and Mobile Radio Communications, PIMRC'97, Helsinki. Finland, 1 – 4 September 1997. pp. 42 – 46.

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

# МЕТОДИКА УПРАВЛІННЯ РЕЖИМАМИ РОБОТИ ЗАСОБІВ РАДІОЗВ’ЯЗКУ В УМОВАХ НАВМИСНИХ ЗАВАД

Постійне вдосконалення засобів радіорозвідки і радіозавад, впровадження автоматизованих комплексів радіоелектронного подавлення (РЕП) призвело за останні роки до істотного підвищення можливостей супротивника по радіоподавленню систем і засобів радіозв’язку. Враховуючи це, досить складним є завдання забезпечення стійкого радіозв’язку в умовах РЕП. Успішне його вирішення неможливо без застосування спеціальних технічних і організаційних мір захисту від радіорозвідки і радіоподавлення.

Процес передачі сигналів по радіоканалу може бути представлений як конфлікт між системою (засобом) радіозв’язку і джерелом завад (станцією РЕП). Засоби радіозв’язку і станція РЕП мають набір альтернатив – режимів роботи. Вони можуть вплинути на якість процесу передачі інформації, вибравши відповідний режим. Необхідно визначити як здійснювати цей вибір, тобто сформувати стратегію управління режимами роботи засобів радіозв’язку.

Формалізувати опис конфлікту дозволяє теорія ігор. Оскільки інтереси системи радіозв’язку й джерела завад прямо протилежні і немає причин для узгодження їх дій, застосуємо апарат скінчених матричних антагоністичних ігор.

Апарат скінчених антагоністичних ігор може бути використаний у тих випадках, коли система радіозв’язку й джерело завад мають скінчених набір режимів роботи, наприклад, кілька градацій потужності, обмежений набір робочих частот тощо. Можливий вибір і зміна режиму роботи. Система радіозв’язку й станція РЕП оцінюють корисність ситуацій, що складаються в результаті їх дій, хоча б на підставі статистичних даних. Пронумерувавши всі можливі режими роботи учасників конфлікту, їх можна представити у вигляді абстрактних множин. Отримано правило прийняття рішення і відповідні формули для ймовірності правильного приймання, які враховують можливість управління режимами роботи засобів радіозв’язку та зміну режимів роботи джерела завад. Для цього введені ймовірності спостереження реалізацій їх векторів керування. Поточні розподіли обчислюються за допомогою матриць перехідних ймовірностей, які і визначають стратегію зміни режимів роботи. Отримано рішення гри для декількох видів матриці виграшів, що описують ряд реальних ситуацій. Тим самим вирішене завдання формування стратегії управління режимами роботи системи радіозв’язку для розглянутих випадків.

Проведено порівняльний аналіз використання теоретико-ігрового підходу з випадковим вибором режимів. Результати аналізу показують, що найбільш виграшною для системи радіозв’язку є ситуація, коли вона використовує теоретико-ігровий підхід, а джерело завад вибирає режими з однаковими ймовірностями. При цьому виграш у завадозахищеності при використанні розробленої методики становить 12–16 %.

ЛІТЕРАТУРА

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

*2.Портной С. Л., Ортюков С. И., Флорковский Д. А., Гриднев О. А.*Сигнально-кодовые конструкции для высокоскоростных модемов. Радиотехника, 1997. – № 2. – С. 91 – 95.

*3.Борисов В. И. и др.* Помехозащищенность систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000. – 384 с.

*4.Скляр Б.* Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. – М.: Вильямс, 2003. – 1104 с.

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

# ОСНОВИ ІНФОРМАЦІЙНОЇ ВІЙНИ

В сучасному житті з’явився термін „інформаційна ера” через те, що інформаційні системи стали частиною повсякденної життєдіяльності збройних сил. Інформаційна ера також змінила спосіб ведення бойових дій, забезпечивши командирів безпрецедентною кількістю і якістю інформації.

Тепер командир може спостерігати за ходом ведення бойових дій, аналізувати події і доводити інформацію в реальному часі. Однак варто розрізняти війну інформаційної ери і інформаційну війну. Війна інформаційної ери використовує інформаційну технологію як засіб для успішного проведення бойових операцій. А інформаційна війна розглядає інформацію як окремий об’єкт або потенційна зброя і як вигідну мету. Технології інформаційної ери уможливили теоретичну можливість – пряме маніпулювання інформаційним простором супротивника.

Інформація з’являється на основі подій навколишнього світу. Події повинні бути сприйняті якимсь чином і проінтерпретовані, щоб стати інформацією. Тому інформація результат двох речей – сприйнятих подій і команд, необхідних для інтерпретації даних і пов’язані з ними значення.

Це визначення абсолютно не пов’язане з технологією. Про те, що ми можемо робити з інформацією і як швидко ми можемо це робити, залежить від технології. Тому додамо поняття інформаційної функції – це будь-яка діяльність, пов’язана з отриманням, передачею, зберіганням і трансформацією інформації.

Одне з визначень військових інформаційних функцій – це будь-які інформаційні функції, що забезпечують або поліпшують рішення військами своїх бойових завдань.

Можна сказати, що держава прагне придбати інформацію, щоб забезпечити виконання своїх цілей, скористатися цей інформацією і захистити її. Ці використання і захист можуть здійснюватися в економічній, політичній і військовій сферах. Знання про інформацію, якою володіє супротивник, є засобом, що дозволяє підсилити нашу міць і понизити міць ворога або протистояти їй, а також захистити наші цінності, включаючи нашу інформацію. Інформаційна зброя впливає на інформацію, якою володіє ворог і його інформаційні функції. При цьому наші інформаційні функції захищаються, що дозволяє зменшити вплив ворога або можливості вести боротьбу. Тому інформаційна війна – це будь-яка дія по використанню, руйнуванню, перекручуванню ворожої інформації і її функцій; для захисту нашої інформації проти подібних дій; і використанню наших власних військових інформаційних функцій. Це визначення є основою для наступних тверджень.

Інформаційна війна – це будь-яка атака проти інформаційної функції, незалежно від застосовуваних засобів. Бомбардування АТС – операція інформаційної війни. Те ж саме можна сказати і про вивід з ладу програмного забезпечення комп’ютера АТС.

Інформаційна війна – це будь-яка дія по захисту наших власних інформаційних функцій, незалежно від засобів, які застосовуються. Зміцнення і оборона будинку АТС проти бомбардувань – теж частина інформаційної війни. Те ж саме можна сказати і про антивірусну програму, яка захищає програмне забезпечення АТС.

Інформаційна війна – тільки засіб, а не кінцева мета, аналогічно тому як бомбардування – засіб, а не ціль.

Інформаційна війна може бути використана також як засіб для проведення стратегічної атаки або протидії.

Військові завжди намагалися впливати на інформацію, що потрібна ворогові для ефективного керування. Звичайно це робилося за допомогою маневрів і відволікаючих дій. Ці стратегії впливали на інформацію, отримувану ворогом, побічно шляхом сприйняття, вони атакували інформацію ворога побічно. Сучасні засоби виконання інформаційних

функцій зробили інформацію уразливою до прямого доступу і маніпуляції з нею. Сучасні технології дозволяють супротивникам змінити або створити інформацію без попереднього одержання фактів і їхньої інтерпретації.

Характеристики сучасних інформаційних систем, що приводять до появи подібної уразливості: концентроване зберігання інформації, швидкість доступу, розповсюджена передача інформації та великі можливості інформаційних систем виконувати свої функції автономно. Механізми захисту можуть зменшити цю уразливість, але не до нуля.

Складові частини інформаційної війни:

1) психологічні операції – використання інформації для впливу на аргументацію особового складу супротивника;

2) електронна війна – не дозволяє ворогові отримати точну інформацію;

3) дезінформація – надає ворогові помилкову інформацію про наші сили і наміри;

4) фізичне руйнування – частина інформаційної війни, якщо має на меті вплив на елементи інформаційних систем;

5) міри безпеки – прагнення уникнути того, щоб ворог довідався про наші можливості і наміри;

6) прямі інформаційні атаки – пряме спотворення інформації без видимої зміни сутності, у якій вона перебуває.

Так само як і звичайна, інформаційна війна має види бойових дій (інформаційна атака, інформаційна оборона) та цілі.

Існує два способи вплинути на інформаційні функції ворога (атакувати інформаційні функції ворога) – прямо або побічно. Нехай, нашою метою є змусити ворога думати про наявність авіаполку там, де його нема, і діяти на підставі цієї інформації таким чином, щоб це було вигідно нам.

Непряма інформаційна атака: використовуючи інженерні засоби, ми можемо побудувати макети літаків і обманні аеродромні споруди, та імітувати діяльність цієї системи. Ми покладаємося на те, що супротивник буде спостерігати обманний аеродром і вважати його діючим. Тільки тоді ця інформація стане такою, яку повинен мати супротивник на нашу думку.

Пряма інформаційна атака: якщо ми створюємо інформацію про обманний авіаполк у сховищі інформації супротивника, і результат буде такий же. Але засоби, що задіяні для отримання цього результату, будуть дуже відрізнятися. Іншим прикладом прямої інформаційної атаки може бути зміна інформації у базі даних супротивника про наявні комунікації в ході бойових дій (внесення помилкової інформації про те, що мости зруйновані) для ізоляції окремих ворожих частин. Цього ж можна домогтися провівши бомбардування цих споруд. В обох випадках особи, що приймають рішення на основі наявної в них інформації, приймуть те саме рішення – проводити перекидання військ через інші комунікації.

Оборонною стороною інформаційної війни є міри безпеки, що мають своєю метою захистити інформацію – не дозволити супротивникові провести успішну інформаційну атаку на наші інформаційні функції. Сучасні міри захисту, такі як операційна безпека і комунікаційна безпека – типові засоби по запобіганню та виявленню непрямих дій ворога, спрямованих на наші військові інформаційні функції. Навпроти, такі міри захисту, як комп'ютерна безпека, містять у собі дії по запобіганню, виявленню прямих інформаційних дій ворога та організації протидії.

Мета інформаційної війни:

– контроль інформаційного простору, для його використання;

– захист наших військових інформаційних функцій від ворожих дій (контрінформація);

– контроль за інформацією для ведення інформаційних атак на ворога;

– підвищення загальної неефективності військ супротивника за допомогою всебічного впливу на військові інформаційні функції.

к.т.н Кулажський В.І. (НАОУ)
Кульчицький О.С. (НАОУ)

# ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ ПЛАНУВАННЯ ТА УПРАВЛІННЯ АДМІНІСТРАТИВНО-ГОСПОДАРСЬКОЮ ДІЯЛЬНІСТЮ

Планування та управління адміністративно-господарською діяльністю, як правило, здійснюється на базі ERP (Enterprise Resource Planning) – систем які суттєво підвищують її якість шляхом своєчасної обробки, зберігання та передачі по телекомунікаційним каналам необхідної для цього інформації. Така інформація може бути як відкритою, так і з обмеженим доступом, порядок обробки та захист якої регламентується законами України та іншими нормативно-правовими актами. Тому одним із актуальних питань при впровадженні таких систем є питання щодо їх інформаційної безпеки.

Основними загрозами інформаційній безпеці для ERP-систем є зовнішні та внутрішні загрози, які спрямовані на порушення доступності, цілісності й конфіденційності її інформаційних ресурсів [1].

Захист ERP-систем від інформаційних загроз здійснюється у відповідності з політикою безпеки, яка представляє собою якісне або якісно-кількісне вираз властивостей захищеності інформації в термінах, що представляють ERP-систему. Політика безпеки є індивідуальною для кожної ERP-системи і залежить від технології обробки інформації, яка реалізується у даній системі, особливостей її обчислювальної системи, фізичного середовища та середовища користувачів, ступеню обмеженого доступу до інформації та її ресурсам. У загальному випадку вона відображає нестаціонарний стан захищеності інформації в ERP-системі тому що:

сама по собі ERP-система може з часом змінюватися, доповнюватися новими компонентами;

можуть змінюватися впливи зовнішнього середовища на ERP-систему;

можуть змінюватися характеристики самої ERP-системи .

На прикладі системи SAP R/3, що розробила німецька компанія SAP AG (System Analyse und Programmentwicklung) покажемо можливі методи та засоби захисту інформації, які можуть бути використані для забезпечення інформаційної безпеки ERP-систем .

Система SAP R/3 має комплексну систему захисту інформації (КСЗІ), яка складається із чотирьох підсистем: захисту електронних документів **SSF** (Secure Store & Forward), захисту мережних з'єднань **SNC** (Secure Network Communication), **аудита** (Audit Information System), **ідентифікації й аутентифікації** [2,3].

**Підсистема SSF** призначена для забезпечення інформаційного захисту електронних документів, що циркулюють у системі. Такий захист реалізується за допомогою двох механізмів – електронного цифрового підпису (digital signature) та електронного цифрового конверта (digital envelope), заснованих на інфраструктурі відкритих ключів PKI (Public Key Infrastructure), які, у свою чергу, базуються на технології асиметричного шифрування.

Механізм електронно-цифрового підпису дозволяє додавати одну або декілька цифрових підписів до будь-якого набору даних, будь-то файл або таблиця. Також SSF може здійснювати шифрування.

Реалізація підсистеми SSF передбачає використання зовнішніх бібліотек, які реалізують криптографічні функції захисту заданої стійкості. Взаємодія між підсистемою й зовнішніми бібліотеками здійснюється на основі інтерфейсу прикладного програмування SSF API. Система SAP R/3 дозволяє скористатися одночасно декількома зовнішніми бібліотеками з різними криптографічними функціями захисту, які створюються під вимоги вітчизняних нормативно-правових актів.

**Підсистема SNC** призначена для організації захищення мережних з'єднань, які встановлюються між компонентами SAP R/3. Вона дозволяє здійснювати аутентифікацію

суб'єктів, що встановлюють з'єднання, а також забезпечувати конфіденційність і цілісність даних, переданих у рамках установленого з'єднання. SNC реалізується у вигляді зовнішніх допоміжних модулів захисту, взаємодія з якими здійснюється за допомогою відкритого інтерфейсу прикладного програмування GSS-APIv2 (Generic Security Services APIv2 – узагальнений прикладний інтерфейс програмування для реалізації мережного сервісу безпеки).

**Підсистема аудита** призначена для збору інформації про події системи й містить два типи реєстраційних журналів – системний та аудита безпеки. Системний журнал містить відомості про функціонування ERP-системи, журнал аудита безпеки – дані, пов'язані з інформаційною безпекою системи.

Підсистема аудита містить також фільтри, які дозволяють фіксувати всі події, пов'язані з діями користувача, а також всі високо приоритетні події, що стосуються дій адміністратора системи.

**Підсистема ідентифікації й аутентификації** призначена для захисту SAP R/3 від НСД шляхом перевірки аутентифікації даних, наданих користувачами системи. Процедури ідентифікації й аутентифікації підсистеми можуть бути реалізовані наступними способами:

– за допомогою реєстраційних імен і паролів, які вводяться користувачами на етапі одержання доступу до системи;

– за допомогою підсистеми SNC, яка була розглянута вище;

– с використанням сертифікатів X.509. При реалізації даного механізму аутентифікації замість реєстраційних імен і паролів користувач надає свій сертифікат. Аутентифікація з використанням сертифікатів X.509 використається при вилученому підключенні користувачів до системи через мережу Інтернет;

– за допомогою механізму SAP „Logon ticke" який дозволяє реалізувати єдину процедуру реєстрації в системі – Single Sign On (SSO).

Всі розглянуті вище підсистеми захисту інформації SAP R/3, можуть забезпечувати тільки рішення вузького кола завдань інформаційної безпеки, які стосуються захищення мережних з'єднань та криптографічного захисту електронних документів.

Функції же по протидіям іншим загрозам інформаційної безпеці, які реалізуються у вигляді мережних атак, НСД до компонентів системи з консолі управління й ін., покладаються на зовнішні спеціалізовані комплекси захисту інформації. Тому при створювані КСЗІ ERP-систем можуть бути використовувані тільки модулі захисту SAP R/3 із криптографічними бібліотеками заснованими на вітчизняних державних стандартах. При цьому функціональні можливості КСЗІ ERP-системи повинні бути доповнені спеціалізованими засобами захисту інформації (наприклад, системами виявлення інформаційних атак, активного моніторингу, електронними замками й ін.).

ЛІТЕРАТУРА

1. *Зырянов Ю.* Информационная безопасность ERP-систем. – Режим доступа: http://www. citcity.ru/16501/. – Заголовок с экрана.

2. *ADM950. Secure* SAP System Management. Participant Handbook. – SAP AG, 2003. – 307 p.

3. *Сердюк В.А.* Уязвимость и информационная безопасность ERP – систем. – Режим доступа: http://www.connect.a133.nthosting.ru/article.asp?id=3167. – Заголовок с экрана.

д.т.н. Куліков С.П. (в/ч А1906)
к.т.н. Комаров В.С. (в/ч А1906)
Олексіюк В.В. (в/ч А1906)
Демченко Р.М. (в/ч А1906)
Комаров Р.О. (в/ч А1906)

# ТЕНДЕНЦІЇ РОЗВИТКУ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ЯК ЕЛЕМЕНТУ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ

Аналіз результатів використання безпілотних літальних апаратів (БПЛА) у військових конфліктах кінця XX – початку XXI століть підтвердив об'єктивну необхідність створення безпілотної авіації та окреслив основні тенденції її розвитку, а саме: створення ефективної захищеної системи управління та передавання даних; підвищення функціональності БПЛА; активне впровадження розробок з мініатюризації безпілотних апаратів та створення БПЛА вертолітного типу.

У бойовій обстановці БПЛА можуть більш ефективно й оперативно, чим пілотовані літаки, вирішувати завдання тактичної та оперативно-тактичної повітряної розвідки і РЕБ, цілевказання і коректування вогню, бойового управління і зв'язку, метеорологічної, радіаційної, хімічної і біологічної розвідки без ризику для особового складу в інтересах командування різних рівнів видів збройних сил. При цьому скорочується час доведення отриманої інформації до відповідної ланки управління.

Одним з принципових питань, яке розглядається при формуванні підходів до створення комплексів безпілотної авіації і знайшло відображення при виборі і обґрунтуванні технологічних рішень, є їх розгляд як інформаційної системи.

Це питання є спільним для всіх існуючих концепцій, які розглядають застосування комплексів безпілотної авіації як функціонування інформаційної мережі, в якій мають місце процеси отримання інформації, її передачі та обробки. При цьому удосконалення бортових засобів збору та обробки інформації і створення необхідних засобів обміну інформацією розглядаються як взаємозалежні процеси.

Особлива увага приділяється питанням повної автоматизації процесів управління звичайними режимами польоту, удосконаленню системи автоматичного розпізнавання цілей як елементу формування вихідних даних, комплексного використання багатоканальних захищених систем зв'язку із застосуванням космічного, наземного та повітряного компонентів.

На цей час у сфері створення БПЛА провідних країн світу спостерігається тенденція по впорядкуванню досліджень і розробок. Відбувається перехід від окремих програм в інтересах видів збройних сил до єдиної системи комплексів із БПЛА, що значно зменшує вартість процесів їх створення та експлуатації.

Перспективна система комплексів із БПЛА базується на принципі модульного компонування, що дозволяє одержати на одній платформі широкий спектр різних конфігурацій апарата, а також відкриває можливість його застосування для рішення різних спеціальних завдань

ЛІТЕРАТУРА

1. UNMANNED VEHICLES HANDBOOK 2008 – http: //www.uvonline.com.
2. UNMANNED AIRCRAFT SYSTEMS ROADMAP 2005-2030 – http: //www.defenseindastrydaily.com/usas-unmanned-aircraft-systems-roadmap-20052030-01094/
3. ARMADA INTERNATIONAL – http: //www.armada.ch.

к.т.н. Куляниця О.Й. (в/ч А1906)
Рябченко А.М. (в/ч А1906)
Міхальов Р.О. (в/ч А1906)

# ОСОБЛИВОСТІ ОПИСУ ШИРОКОСМУГОВИХ РАДІОСИГНАЛІВ

За останні десятиріччя різко підвищився інтерес до широкосмугових у радіотехнічному значенні сигналів. Це обумовлено можливістю зростання інформативності технічних систем та засобів побудованих на їх основі.

Однак виявилось багато проблемних питань пов'язаних з технічною реалізацією потенційних можливостей складних сигналів. Раціональне використання даних сигналів виявляється не простим і в першу чергу це пов'язане з їхньою внутрішньою структурою. Гостро стоїть необхідність коректного опису цих сигналів за допомогою представлення у формі Гільберта, що є помітно більш складним у порівнянні з відомим квадратурним представленням, що використовується стосовно вузькосмугових сигналів.

Метою даної доповіді є складання короткого викладу відомостей по особливостях опису детермінованих широкосмугових сигналів у часовій та частотній області.

Ці відомості потребують подальшого розширення та узагальнення при описі випадкових широкосмугових сигналів, а також широкосмугових систем. На такій основі можливо порівняно строге рішення багатьох прикладних задач, пов'язаних, зокрема, з аналізом та синтезом елементів радіосистем і систем радіозв'язку з широкосмуговими сигналами.

Перспективність і можливість створення таких систем відмічені давно. Однак їхні серійні зразки ще не знайшли належного застосування.

Це обумовлено багатьма труднощами, що виникають при технічній реалізації даних засобів, у тому числі і відсутністю зазначених вище відомостей.

**Класифікація сигналів.** Якщо спектр сигналу $s(t)$ зосереджений на інтервалі частот $(f_{min}, f_{max})$, то для нього можна ввести параметр $\eta = 0{,}5\Delta F / f_{cp}$

$$\eta = \frac{\Delta F}{2f_{cp}} = \frac{(f_{\max} - f_{\min})}{(f_{\max} + f_{\min})}, \quad f_{cp} = \frac{1}{2}(f_{\max} + f_{\min}), \quad 0 \le f_{\min} \le f_{\max} \le \infty,$$

де $f_{cp}$ – середня частота сигналу; $\Delta F = f_{\max} - f_{\min}$ – ширина його спектру.

Сигнали розділяються на вузькосмугові, широкосмугові та понадширокосмугові (ВС, ШС і ПШС) у залежності від виконання одного з наступних нерівностей: $0 \le \eta \le 0{,}05$; $0{,}05 \le \eta \le 0{,}25$; $0{,}25 \le \eta \le 1$.

Далі під ШС, якщо не обумовлюється, розуміються ШС - і ПШС-сигнали, а загальні співвідношення, що приводяться, з рівним успіхом можуть використовуватися при аналізі складних та простих сигналів.

**Часові характеристики та параметри широкосмугових сигналів.** Часовими характеристиками сигналів, які найбільш часто використовуються, є їх огинаюча, фаза та миттєва частота, що вводяться наступним чином.

Сигналу $\breve{v}(t) = s(t) + j\breve{s}(t)$ ставиться у відповідність комплексний сигнал, до нього пред'являється вимога ортогональності і взаємооднозначного зв'язку його дійсної та уявної частин. Це забезпечує рівність інформаційних можливостей сигналів $s(t)$, $\breve{v}(t)$ і дає підставу вводити зазначені характеристики для комплексного сигналу та приймати їх за характеристики вихідного сигналу.

**Заключні зауваження.** Дані викладки не претендують на повноту й акцентують увагу лише на найбільш важливих аспектах тематики.

а. Опис ШС-сигналів є важким у зв'язку зі складністю проведення перетворення Гільберта, що приводить у більшості практично важливих випадків до інтегралів, що розходяться, апроксимація яких у літературі належним образом не описана.

Це переконливо ілюструється тим, що у фундаментальній довідниковій літературі приведено усього лише 118 результатів цього перетворення, у той час як табличні інтеграли Фур'є, Лапласа та Бесселя представлені значно повніше.

б. При апроксимації вираження $s^h(t)$ зручно користуватись його представленням у наступному вигляді : $s^h(t) = \int_0^\infty \frac{1}{u}\left[s(t-u) - s(t+u)\right]$.

в. Якщо сигнал $s(t)$ відмінний від нуля на півосі *(0, ∞)*, то перетворення Гільберта має вигляд:

$$s^h(t) = \frac{2}{\pi}\int_0^\infty \frac{t\,s(l)}{t^2 - l^2}dl, \quad s(t) = -\frac{2}{\pi}\int_0^\infty \frac{l\,s^h(t)}{t^2 - l^2}dl, \quad \int_0^\infty \left|s^h(t)\right|^2 dt = \int_0^\infty \left|s(t)\right|^2 dt < \infty \quad .$$

**Висновки.** Приведені в доповіді початкові відомості по опису детермінованих широкосмугових сигналів показують, що їхньому використанню в радіотехнічних системах різного призначення, корисність якого не викликає сумнівів, повинна передувати цілеспрямована робота в цьому науковому напрямку.

Виникаючі при цьому труднощі можуть бути подолані на основі сучасного аналізу функцій та використання можливостей існуючого математичного забезпечення.

ЛІТЕРАТУРА


1. *Хармут Х.* Теория секвентного анализа: Пер. с англ. – М.: Мир, 1980. – 574 с.
2. *Хармут Х.* Несинусоидальные волны в радиолокации и радиосвязи: Пер. с англ.. – М.: Радио и связь, 1985. – 376 с.
3. *Астанин Л. Ю., Костылёв А. А.* Основы сверхширокополосных радиолокационных измерений. – М.: Радио и связь, 1989. – 192 с.
4. *Gabor D. Theory of* Cjmmunication. Journ. Inst. Electr. Engrs (London), P. III, 93, 429, 1946.
5. *Евсиков Ю. А., Чапурский В. В.* Преобразование случайных величин в радиотехнических устройствах. М.: Высш. Школа, 1977. – 264 с.
6. *Бендат Дж., Пирсол А.* Прикладной анализ случайных данных: Пер. с англ. – М.:Мир, 1989. – 560 с.
7. *Бейтмен г. и Эрдейи А.* Таблицы интегральных преобразований. Том II: Пер. с англ. – М.: Наука, 1970. – 327 с.

к.т.н. Лаврут О.О. (ВІТІ НТУУ „КПІ”)

# ДИНАМІЧНА ЗМІНА РЕЖИМУ ФУНКЦІОНУВАННЯ СИСТЕМИ СУПУТНИКОВОГО ЗВ’ЯЗКУ ЗА ДОПОМОГОЮ ВИКОРИСТАННЯ ТЕНЗОРНОГО АНАЛІЗУ

Апаратура і ємності комерційних систем зв’язку стають невід’ємною частиною сучасних військових систем зв’язку, забезпечуючи низькі витрати, високу пропускну здатність і нові види обслуговування військових абонентів. Створення перспективної національної системи супутникового зв’язку (ССЗ) потребує оптимального сполучення військового та комерційного сегментів.

З одного боку така ССЗ повинна забезпечувати високу пропускну здатність, швидкість передачі інформації, ефективне використання ресурсу бортового ретранслятора, а з іншого - повинна бути завадозахищеною та прихованою. Очевидно, що ці фактори є взаємовиключними. Виникає протиріччя між вимогами, які висуваються до системи в мирний час і тими вимогами, які необхідно забезпечити в умовах впливу сильних навмисних завад. Врахувати ці протиріччя можна шляхом комплексного застосування як організаційних, так і технічних заходів, тобто врахування основних діючих факторів.

Знизити витрати на розробку, виробництво, розгортання і експлуатацію системи супутникового зв’язку можна орієнтуючись на створення системи, яка дозволяла б вирішувати проблему оперативності доставки повідомлень в обстановці, пов’язаній з різноманітними завадами на основі використання динамічної зміни режиму функціонування.

При розгляді системи супутникового зв’язку як динамічного об’єкту, стан мережі в кожний конкретний момент визначається взаємопов’язаними і одночасно діючими один на одного складовими: різними характеристиками компонентів ССЗ, її алгоритмами функціонування і зовнішніми діючими факторами. Даний стан можна представити у вигляді матриці стану системи супутникового зв’язку в конкретний момент її функціонування, де будуть враховані всі вищезгадані фактори. Очевидно, що при зміні стану ССЗ змінюються (або повинні змінюватись) і значення компонентів, які входять в матрицю. Виникає проблема одночасного врахування усіх параметрів при переході з одного стану в інший.

Звісно, що вирішення подібної задачі в загальному виді не знайдено і отримати необхідний результат можливо тільки на множині припустимих (тобто тих, що реалізуються фізично) параметрів компонентів і алгоритмів функціонування системи. Вирішити подібну задачу методом перебору практично неможливо через її велику розмірність.

Єдиний підхід до дослідження системи супутникового зв’язку як складної системи дозволяють одержати тензорні моделі і методи аналізу. Тензорний аналіз, завдяки закладеним у нього можливостям, є логічним засобом опису реальних об’єктів у їх багатоаспектності і суперечливості. Тензорне подання має максимальну цілісність, дозволяючи сконцентрувати основну увагу на самій системі незалежно від можливих координатних систем її розгляду.

Відповідно до властивостей тензора за його відомими проекціями в одній системі координат можна отримати проекції в інших, якщо відомі закони переходу від однієї системи координат до іншої. Зміна системи координат може означати зміну аспекту розгляду досліджуваної системи, а проекції тензора можуть відображати величини показників, що характеризують основні її властивості в прийнятому для розгляду аспекті.

Таким чином, тензорний опис системи супутникового зв’язку дозволяє отримати цілісне уявлення про систему, її характеристики і властивості в тій чи іншій координатній системі розгляду. Даний підхід дає можливість оперативно оцінювати, прогнозувати стан та відповідно динамічно змінювати режим функціонування ССЗ для оптимальної її роботи в конкретній обстановці, що склалася.

к.т.н Ладик О.І. (ІТС НТУУ „КПІ”)
Головченко І.О. (ІТС НТУУ „КПІ”)

# ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ MIMO

Розробки сучасних систем стільникового зв’язку направлені на забезпечення виконання вимог технологій 4G. Для цього розробляють та застосовують нові технічні рішення. До таких рішень відносять технологію MIMO, яку вже застосовують в стандартах 802.11n, мобільному WiMAX, LTE.

Технологія MIMO (Multiple Input Multiple Output) використовує багато антен для передачі і прийому сигналів на передавальній і приймальній сторонах відповідно, що збільшує пікову швидкість передачі трафіку, середню швидкість передачі даних і пропускну здатність стільників у широкополосних безпроводових мережах, перш за все в умовах роботи там, де не забезпечується пряма видимість.

Багатоелементні антенні пристрої забезпечують:

– розширення зони покриття і зглажування „мертвих” зон;

– використання декількох шляхів поширення сигналу, що збільшує швидкість доставки даних адресату;

– збільшення пропускної здатності ліній зв’язку завдяки формуванню різних фізичних каналів;

– просторове рознесення покращує абсолютну чутливість, що не забезпечує просторове мультиплексування.

Можливості технології MIMO ілюструє рис.1.

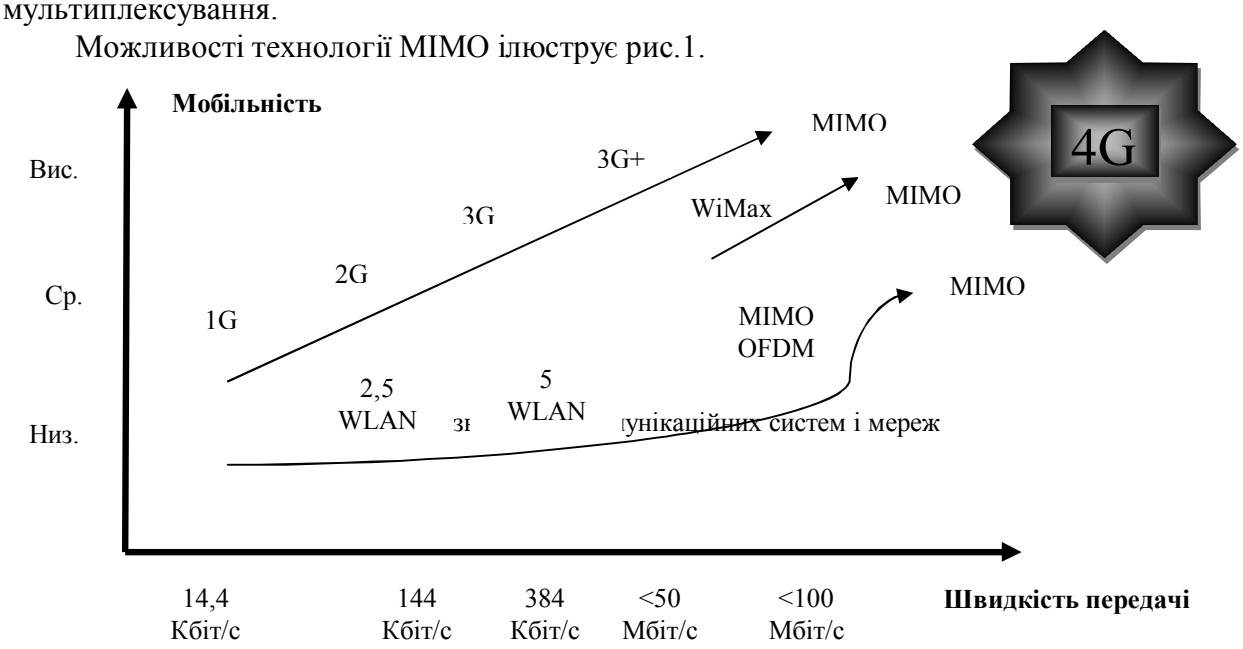



Рис.1. Розвиток телекомунікаційних систем і мереж

Використання техніки MIMO дозволяє в рази збільшити надійність і швидкість передачі даних в радіоканалі з тією ж смугою частот. Це дозволяє задовольнити потреби і очікування користувачів безпроводових мереж.

ЛІТЕРАТУРА

1. *Сперанский В. С., Евдокимов И. Л.* Моделирование сигналов OFDM-MIMO систем беспроводной передачи данных 802.16, Труды Московского технического университета связи и информатики. – М: МТУСИ, 2007.

2. *Бакулин М. Г., Крейнделин В. Б., Шлома А. М.* Новые технологии в системах мобильной радиосвязи. – М: Инсвязьиздат, 2005.

к.т.н. Ладик О.І. (ІТС НТУУ „КПІ”)
Донець А.Ю. (ІТС НТУУ „КПІ”)
Завдовєєва О.С. (ІТС НТУУ „КПІ”)

# ЗАСТОСУВАННЯ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ ПРОЦЕСІВ В СЕРЕДОВИЩІ GPSS

Розробка сучасних нових телекомунікаційних технологій, їх аналіз та дослідження можливі тільки на базі застосування інформаційних систем. До таких систем належить система GPSS, яка є потужним універсальним середовищем для моделювання різних процесів та систем. Вона дозволяє моделювати виробничі та невиробничі процеси: функціонування різних систем масового обслуговування, зокрема і телекомунікаційні системи, проведення воєнних дій, роботу мережі Internet тощо. Система дозволяє управляти процесом моделювання, проводити експерименти, здійснювати оптимізацію, реалізувати візуалізацію процесу функціонування моделі з застосуванням методів мультиплікації.

Імітаційна модель GPSS є формальним описом логіки функціонування досліджуваної системи у часі, що враховує найбільш суттєву взаємодію її елементів та забезпечує можливість проведення статичних елементів.

Під системою масового обслуговування прийнята сукупність послідовно зв’язаних між собою вхідних потоків вимог на обслуговування, накопичувачів, черг, каналів обслуговування і вхідних потоків вимог після обслуговування, де вхідний потік вимог є послідовність вхідних вимог, які потребують в обслуговуванні у системі та підкоряються визначеному закону, а вихідний потік вимог є послідовність вихідних вимог, які були обслужені у системі і підкоряються визначеному закону. Під терміном вимога (транзакт) розуміють об’єкт, який поступає в систему і потребує в певному обслуговуванні в даній системі. Вимога в системі GPSSW – це об’єкт із сукупністю певних ознак, які визначаються унікальним номером. Об’єкт нумерується послідовно, починаючи з номера 1.

Імітаційна модель системи масового обслуговування є моделлю, яка відображає поведінку системи та зміну її стану в часі при заданих потоках вимог, що поступають на входи системи. Параметри вхідних потоків вимог – зовнішні параметри системи масового обслуговування. Вихідними параметрами являються величини, що характеризують властивості системи – якість її функціонування, – наприклад такі, як:

– коефіцієнти використання каналів обслуговування;
– максимальна і середня довжина черги в системі;
– час знаходження вимог у чергах і каналах обслуговування і т.д.

Імітаційне моделювання вважається числовим методом визначення параметрів функціонування найрізноманітніших систем по численним реалізаціям з урахуванням ймовірного характеру протікання процесу. Воно дозволяє досліджувати систему масового обслуговування при різних видів вхідних потоків та різної інтенсивності надходження потреб в систему, а також різноманітних дисциплінах обслуговування потреб.

ЛІТЕРАТУРА

1. *Кудрявцев Е.М.* GPSS World. Основы имитационного моделирования различных систем. – М.:ДМК Пресс, 2004. – 320 с.
2. *Учебное пособие* по GPSS World. /Перевод с английского/. – Казань: Издательство „Мастер Лайн”, 2002. – 272 с.

к.т.н. Ладик О. І. (ІТС НТУУ „КПІ”)
Муравйова О. Г. (ІТС НТУУ „КПІ”)

# СТАНДАРТ IPv6 У МОБІЛЬНИХ МЕРЕЖАХ

За оцінками експертів у найближчі роки продовжиться бурхливий ріст ринку мобільного доступу в Інтернет. В наш час стільникових телефонів та безпровідних технологій мобільність стала дуже важливою потребою як в бізнесі так і в повсякденному житті.

Але на сьогоднішній день ми маємо справу з мікромобільністю, яка забезпечує безперервність зв’язку тільки при переміщенні між зонами дії різних точок доступу в межах однієї мережі. Для того, щоб підтримувати зв’язок з вузлами інших мереж мобільний вузол міг би змінювати свою IP-адресу щораз, як відбувається перехід в іншу мережу, але тоді мобільний вузол не зміг би при такому переході зберегти існуючі з'єднання транспортного й більш високих рівнів.

Механізм „Mobile Ipv6” дозволяє мобільному вузлу переміщатися з однієї мережі доступу в іншу не змінюючи своєї IP адреси, отже забезпечує так звану макромобільність. Мобільний вузол завжди доступний по своїй „домашній” адресі: IP адресі, привласнений мобільному вузлу в межах його „домашньої” мережі. Пакети, направлені по такій адресі, доставляються мобільному вузлу незалежно від того, де в цей момент вузол підключений до Інтернету. Зміна точки підключення не приводить до розриву встановлених раніше з’єднань із іншими (стаціонарними або мобільними) вузлами. Таким чином, переміщення мобільного вузла з „домашньої” мережі в іншу мережу залишається непомітним як для протоколів верхніх рівнів (починаючи із транспортного), так і для прикладних програм. Для цього необхідна деяка інфраструктурна підтримка.

Для такої підтримки в домашній мережі встановлюється ще один маршрутизатор, так званий домашній агент (Home Agent). Його робота полягає в підтримці списку всіх відомих мобільних пристроїв.

Коли ж мобільний вузол перебуває поза домашньої мережі у нього, крім „домашньої” адреси, з’являється один або більше „гостьових” адрес. Пакети, відправлені на „гостьову” адресу, доставляються мобільному вузлу в точку його поточного підключення до чужої мережі. Асоціювання „домашньої” адреси з поточною „гостьовою” адресою називається „прив’язкою” (binding) мобільного вузла.

Опинившись поза мережею, мобільний вузол реєструє на домашньому агенті один зі своїх „гостьових” адрес. Мобільний вузол здійснює реєстрацію прив’язки, направляючи агентові „домашньої” мережі пакет, що містить опцію „Відновлення прив’язки”. Агент „домашньої” мережі у відповідь посилає мобільному вузлу пакет, що містить опцію „Підтвердження прив’язки”.

Надалі агент „домашньої” мережі, використовуючи проксі режим у рамках протоколу „виявлення сусіда”, перехоплює всі Ipv6 пакети, відправлені на „домашню” адресу даного мобільного вузла, перенаправляє їх по тунелю на „гостьову” адресу вузла. Пересилання по тунелю виконується в такий спосіб: кожний перехоплений пакет поміщається агентом в поле корисного навантаження іншого пакета, використовуючи метод Ipv6 інкапсуляції. При цьому Ipv6 заголовок зовнішнього пакета в полі адреси призначення містить „гостьову” адресу мобільного вузла.

Механізм підтримки мобільного підключення повністю інтегрований у стек протоколу IPv6 і, отже, „зрозумілий” абсолютно всім вузлам, що працюють за цим протоколом.

ЛІТЕРАТУРА

1. *Найэл Ричард Мерфи, Дэвид Мэлоун* IPv6. Администрирование сетей. – М.: Кудиц-Пресс, 2006. – 281 с.

2. *Ш. Вегешна* Качество обслуживания в сетях IP - М.: Вильямс, 2003 – 368 с.

Липський О.А. (ВІТІ НТУУ „КПІ”)
Коваленко І.Г. (ВІТІ НТУУ „КПІ”)
Максименко Ю.Л. (ВІТІ НТУУ „КПІ”)
Васильченко В.В. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ ВПЛИВУ НАВМИСНИХ ЗАВАД НА РАДІОРЕЛЕЙНІ ЛІНІЇ ЗВ’ЯЗКУ ПРИ ПЕРЕДАЧІ IP ТРАФІКУ

В сучасних умовах розвитку систем постановки навмисних [1, 2], і їх наближенні до ліній радіозв’язку створюються об’єктивні передумови до застосування оптимального виду навмисних завад за енергетичними, часовими і просторовими характеристиками.

При застосуванні навмисних завад на радіорелейні лінії зв’язку, як показують останні дослідження [3, 4] велика увага приділяється оптимізації структури навмисних завад при спотворенні сигналів радіолінії. При цьому не аналізується структура інформації, протоколи канального і мерережевого рівнів. Це обумовлено тим, що засоби радіоелектронного впливу в основній своїй масі знаходяться на значній відстані від радіоліній зв’язку – це не дозволяє отримати повну інформацію про радіолінію. Проте зміна тактики застосування комплексів постановки навмисних завад [1, 2] дозволяє отримати більш повну інформацію про лінію зв’язку. При перехваті сигналів радіолінії є можливість отримати інформацію про протоколи OSI і визначити тип протоколу від фізичного до прикладного рівня.

На сьогоднішній день сучасні мережі зв’язку будуються на конвергенції загальних мереж зв’язку. Основу для об’єднання таких мереж є Internet protocol (IP). В радіорелейних системах зв’язку – це спричинило до появи протоколу TDM over IP. Даний протокол забезпечує передачу IP трафіку по існуючих потоках E1/ІКМ-30.

Перехват інформації із радіорелейної лінії зв’язку і аналіз протоколів канального рівня дозволяє згенерувати квазіоптимальну навмисну заваду. Дана завада спотворює не всю послідовність сигналів, а лише деяку їх частину. Це приведе до відкидання кадра так, як значення контрольної суми закладене на передавальному боці не співпадає із значенням, розрахованим на приймальній стороні.

Таким чином, спотворення хоча б одного біта в кадрі, може привести до зниження або до повного припинення передачі інформації. При постановці квазіоптимальних навмисних завад також знижується ймовірність виявлення станцій постановки навмисних завад так, як їх вплив відбувається не постійно, а в квазіперіодичні проміжки часу.

Вибіркове спотворення пакетів може здійснюватися в залежності від типу протоколу, що застосовується на транспортному рівні UDP чи TCP. Це викликає блокування голосових пакетів, або даних. На основі аналізу IP адрес можна здійснити блокування інформації окремого користувача мережі, які транспортуються через канал зв’язку.

Вибірковість спотворень, спричинених впливом квазіоптимальних навмисних завад, спричинює великі складностей при з’ясуванні причин, що викликали зниження пропускної спроможності радіорелейного каналу зв’язку. Це змушує здійснювати контроль каналу зв’язку на основі декількох параметрів: кількості спотворених кадрів і щільності розподілу спотворених символів в середині кадра. В якості критерію оцінки доцільно застосовувати критерій Вальда.

## ЛІТЕРАТУРА

[1]. *Кандратьев А.* Перспективные комплекс РР и РЭВ сухопутных войск США „Профет” / А. Кандратьев // Зарубежное военное обозрение . – 2008. – № 7. – С. 37 – 41.

2. *Стрелецкий А.* Мобильный автоматизированный комплекс радиоразведки Сухопутных войск США / А. Стрелецкий // Зарубежное военное обозрение. – 2001. – № 5, 6. – С. 40 – 43.

3. *Современная радиоэлектронная* борьба. Вопросы методологии / под ред. В.Г. Радзиевского. – М.: Радиотехника, 2006. – 424 с.

д.т.н. Лисенко А.І. (ІТС НТУУ „КПІ”)
Валуйський С.В. (ІТС НТУУ „КПІ”)

# ПІДВИЩЕННЯ СТІЙКОСТІ МОБІЛЬНИХ РАДІОМЕРЕЖ ЗВ’ЯЗКУ ЗА РАХУНОК ВИКОРИСТАННЯ СУПУТНИКОВИХ ТА ПСЕВДОСУПУТНИКОВИХ СИСТЕМ

При виконанні розвідувальних-пошукових чи військових операцій завжди виникає потреба в організації стійкої радіомережі зв’язку із мобільними об’єктами. Через зруйновану (або взагалі відсутню) наземну інфраструктуру та нестабільність каналів між мобільними абонентами стійкість мобільної радіомережі погіршується. Отже, виникає проблема підвищення стійкості мобільних радіомереж зв’язку. Для вирішення цієї проблеми останнім часом ведеться пошук і розробка комбінованих (гібридних) рішень на основі існуючих і новітніх розробок у сфері телекомунікацій. Таким комбінованим рішенням для підвищення стійкості мобільних радіомереж може бути використання супутникових та псевдосупутникових систем (на основі безпілотних літальних апаратів (БЛА) [1–4] або наносупутників [5]). Отже, постає актуальна наукова задача – віднайти шляхи комплексування супутникових та псевдосупутникових систем для підвищення стійкості мобільних радіомереж. Для того, щоб визначити шляхи комплексування супутникових (ССЗ) та псевдосупутникових систем зв’язку (ПССЗ), необхідно проаналізувати їх переваги та недоліки. Аналіз літератури свідчить [3,4,6], що основною перевагою супутникових систем зв’язку (ССЗ) є велика зона обслуговування. Для глобального покриття Землі достатньо трьох геостаціонарних супутників. Але ССЗ мають ряд суттєвих недоліків. Через велику відстань супутника від Землі сигнали, випромінювані супутником, мають занадто малу потужність біля поверхні Землі та велику затримку розповсюдження у мережі, що заважає організувати швидкісні інформаційні потоки при компактній наземній апаратурі. В умовах дії потужних завад наземні прилади взагалі можуть вийти із ладу. На відміну від ССЗ псевдосупутникові системи (на основі БЛА: літаків, стратостатів тощо) [] мають кращу енергетику радіолінії (більш високу пропускну здатність); малий час розгортання; значно менші затрати на запуск та модернізацію бортового обладнання. Але як і ССЗ піддаються дії шкідливих завад. Крім того, при великій кількості БЛА у мережі зростає службовий трафік та відповідно зменшується пропускна здатність. Отже комплексне використання ССЗ та ПССЗ може нівелювати їх недоліки та підвищити стійкість функціонування мобільної радіомережі. Позначимо деякі шляхи комплексування: 1. Сумісне використання каналів ССЗ та ПССЗ збільшує структурний ресурс мережі, а отже підвищує її структурну стійкість. За допомогою супутникових каналів можливо резервувати радіолінії „БЛА-Земля”, оскільки БЛА на відміну від супутників більш уразливі при дії шкідливих завад (атак противника). Також використання аероплатформ у міжплатформних лініях зв’язку (МЛЗ) відкриває широкі можливості з побудови просторових мереж на основі платформ різних рівнів: БЛА та супутників. 2. БЛА може виконувати роль активного ретранслятору та значною мірою підвищити енергетику радіолінії „Земля-Супутник”. 3. Розподіл за типом трафіку. Трафік, невеликого обсягу та некритичний до затримок, може передаватися супутниковими каналами (наприклад, службова інформація, що перевантажує ПССЗ). Так, завдяки великій зоні покриття, що охоплює всі БЛА та наземні абоненти, через супутник можливо передавати команди управління з Центру управління на БЛА, а у зворотному каналі отримувати інформацію про місцезнаходження БЛА, абонентів, їх стан та квитанції про виконання ними команд. Трафік, що потребує реального часу (телефонний зв’язок, відеоспостереження тощо), може передаватися високошвидкісними каналами через БЛА. Завдяки вдалому комплексуванню ССЗ та ПССЗ відкриваються нові шляхи до підвищення стійкості і продуктивності функціонування мобільних радіомереж зв’язку. Але при створенні таких складних, багаторівневих, динамічних систем виникає ряд проблем, пов’язаних з вибором та побудовою структури, управлінням та організацією інформаційного обміну у мережі.

д.т.н. Лисенко О.І. (ИТС НТУУ „КПІ”)
Кірчу П.І. (ИТС НТУУ „КПІ”)

# ЗАСТОСУВАННЯ АДАПТИВНОЇ СИСТЕМИ КЕРУВАННЯ БЕЗПІЛОТНИМ ЛІТАЛЬНИМ АПАРАТОМ ПРИ СТВОРЕННІ ЛОКАЛЬНОЇ МЕРЕЖІ ЗВ’ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Сучасні принципи організації зв’язку та технічне оснащення підрозділів зв’язку не дозволяють повністю задовольнити потреби управління військами сучасного бою, що характеризується високою динамікою та розгортається на значних географічних територіях. Тому в цей час розробляється концепція побудови мобільного компонента (МК) мереж зв'язку військового призначення (МЗВП). Передбачається, що архітектура МК МЗВП буде складатися із трьох основних рівнів: 1-й – радіомережі мобільних абонентів (МА) – військовослужбовець, БМП, танк й ін.; 2-й – мережі мобільних базових станцій (МБС), що утворять опорні мережі в різних географічних зонах бойових дій; 3-й – повітряна мережа безпілотних літальних апаратів (БПЛА), що забезпечує зв’язність між даними зонами.

Телекомунікаційні мережі створені між літальними апаратами та між землею і мережею літальних апаратів на даний момент є оплотом побудови системи зв’язку на полі бою. Існуючі системи зв’язку на основі аероплатформ використовують дороге радіообладнання та пілотовані чи безпілотні літальні апарати високої вартості. Тому в нинішній час є не абияк актуальна задача створення легких БПЛА які б мали порівнюючи невелику вартість і могли б використовуватися в якості аероплатформ для створення телекомунікаційної мережі спеціального призначення. Особливістю режимів польоту таких аєроплатформ є попередня невизначеність стосовно можливих збурень каналів телекомунікац, викликана непередбачуваною зміною метеоумов. Це потребує оперативного реагування, тобто оптимізації траєкторного руху ДПЛА в реальному часі. Вузли мобільного компонента МЗВП також повинні швидко адаптуватися до частих змін топології та рівня трафіка, а також ефективно використовувати обмежені мережні ресурси. У таких умовах забезпечити інформаційний обмін із заданою якістю неможливо без ефективної системи управління (СУ) мобільним компонентом, складовою частиною якої є підсистема управління мережі БЛА та система керування окремим взятим літальним апаратом.

Для вирішення даного завдання запропоновано комплексне використання технологій синтезу адаптивного управління за допомогою функцій Ляпунова, яка передбачає застосування еталонної моделі управління, настроєної оптимальним образом, для настройки параметрів регулятора в реальному часі, при зміні динамічних характеристик об’єкту керування. В самоорганізуючихся системах в процесі функціонування відбувається формування алгоритму (його параметрів), дозволяючого оптимізувати систему з точки зору поставленної цілі управління.

На теперішній час одним з найбільш універсальних засобів вирішення задачі синтезу системи управління польотом є метод аналітичного конструювання. Основною відрізняючою особливістю запропонованого алгоритму синтезу системи автоматичного керування аероплатформою є безпошуковість, тобто відсутність пошукових сигналів для ідентифікації параметрів літального апарата.

ЛІТЕРАТУРА

1. *Basu P., Redi J., Shurbanov V.* Coordinated Flocking of UAVs for Improved Connectivity of Mobile Ground Nodes // In Proceedings of IEEE MILCOM’04, 2004.

2. *Ильченко М.Е., Кравчук С.А.* Телекоммуникационные системи на основе висотних аэроплатформ. – Киев.: Наукова думка, 2008. – 579 с.

3. *Timothy X Brown, Brian Argrow, Cory Dixon, Sheetalkumar Doshi, Phillip Nies* Ad hoc UAV-Ground Network (AUGNet) Test Bed // 4th Scandinavian Workshop on Wireless Ad-hoc Networks, May 4-5, Stockholm, 2004.

д.т.н. Лисенко О.І. (ІТС НТУУ „КПІ”)
Мірошниченко А.В. (ІТС НТУУ „КПІ”)

# СИНХРОНІЗАЦІЯ БАЗОВИХ СТАНЦІЙ МЕРЕЖІ МОБІЛЬНОГО ЗВ’ЯЗКУ НОВОГО ПОКОЛІННЯ

Сьогодення ставить перед операторами стільникового зв’язку одну з найскладніших задач за останні п’ятнадцять років. Це – побудова конвергентних мереж, тобто таких, що підтримують широкий спектр послуг(насамперед голосові та відео потоки, високошвидкісний доступ до мережі Інтернет). З огляду на проголошену ITU концепцію ALL-IP, рішення полягає у розгортанні пакетних мереж до рівня базових станцій(БС). Але тоді стає проблемою доведення синхросигналів до цих станцій. Адже несинхронізована система не здатна забезпечувати навіть мінімального рівня якості обслуговування. Існує два щляхи розв’язання цієї задачі.

1. Встановлення обладнання SyncEthernet на шляху від БС до наступного рівня мережі оператора зв’язку. Незаперечними плюсами є захищеність сигналу від впливу навколишнього середовища, сумісність з мережею PTN, можливість переносити синхросигнал високої якості від головного генератора.

З мінусів – залежність від конфігурації кінцевих пристроїв(зловмисник, отримавши доступ до кінцевих пристроїв каналу SyncEthernet матиме змогу порушити процес синхронізації БС), стандартизаційна незавершеність, відсутність можливості синхронізації часу.

2. Долучення до кожної базової станції приймача GPS, з можливістю виділення синхронізації від цієї системи. Серед переваг цього рішення можна назвати насамперед можливість як часової, так і частотної синхронізації, відсутність залежності елементів системи один від одного, практичну неможливість дистанційного втручання у процес синхронізації. Крім того, є можливість надавати послуги синхронізації декільком близько розташованим БС різних операторів, що значно здешевлює вартість такого рішення.

Головний недолік – досить велика залежність від погодних умов. Загальновідомим є нездатність GPS до точних обчислень у плотний сніг чи дощ. Другим недоліком є відносно невелика якість частотної синхронізації, яку неможливо збільшити(на відміну від рішення з SyncEthernet). Крім цих технічних, є також управлінський мінус такої системи. Десятки (а, можливо, і сотні) таких точок синхронізації потребують якоїсь системи моніторингу, вартість якої може перевищити вартість самих GPS-приймачів.

Як доводить досвід, найкращім рішенням є те, що поєднує в собі елементи як першого, так і другого. Наприклад, інформацію по частотній синхронізації можна передавати по каналу SyncEthernet, а по часовій – брати від сигналу GPS. Але вартість такої системи може виявитись занадто великою для впровадження її до широкого вжитку.

Таким чином проблема передачу сихросигналу до БС являє собою дуже цікаву та нетривіальну проблему, що потребує розв’язання у найближчий час.

## ЛІТЕРАТУРА

1. *Antonis Karvelas* Synchronization in packet-based mobile backhaul networks.// Ethernet Academy Articles – 17.09.2009.

2. International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), 1997. ITU-T. G.811 : Timing characteristics of primary reference clocks.

3. IEEE Std. 1588 – 2002 IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. Superseded by 1588-2008.

Литвиненко Є. О. (ВІТІ НТУУ „КПІ”)
Помін А.Г. (ВІТІ НТУУ „КПІ”)

# ЕКОНОМІЧНА ДОЦІЛЬНІСТЬ ПОБУДОВИ КОРПОРАТИВНОГО CDMA

Корпоративний *CDMA* (Code Division Multiple Access) дозволяє підприємствам істотно скоротити свої витрати на зв’язок. Базові станції *CDMA* підключаються до комутатора мобільного зв’язку, а потім до шлюзу взаємодії *CDMA -IP*, що виконує функції *BSC (Base Station Controller)*, оскільки він забезпечує локальну комутацію трафіка від підключених до нього базових станцій.

Таким чином, весь внутрішньокорпоративний мовний трафік з мобільних телефонів на інші телефони для установ – залишається в межах підприємства, не виходячи на зовнішні мережі. Трафік від мобільних телефонів між різними офісами (які використовують рішення Корпоративного *CDMA*) можна передавати по існуючих між ними *IP*-мережах, що особливо вигідно, коли офіси компанії перебувають у різних містах. Весь вихідний трафік на зовнішні мережі маршрутизується через *АТСОЗ (автоматичні телефонні станції окремих закладів)*, тобто розглядаються як виклики з телефону для установ.

Немаловажною перевагою, що з’являється внаслідок локальної комутації трафіка й здійснення внутрішньокорпоративних переговорів без виходу на зовнішні мережі – це підвищення безпеки й конфіденційності зв’язку для підприємства. Потрібно також урахувати, що до корпоративних базових станцій можуть підключитися тільки абоненти, зареєстровані в мережі корпоративного *CDMA*.

Шлюз взаємодії *CDMA-IP* виконує наступні функції: з одного боку, він управляє розподілом радіоресурсів, установленням з’єднання, підтримує різні види кодеків, підтримує шифрування й аутентифікацію користувача, здійснює локальну комутацію трафіка й т.д., тобто виконує функції контролера базових станцій і комутатора мобільного зв’язку. З іншого боку, він підтримує пакетозування *CDMA*-трафіка, керування встановленням з’єднання, компресію/декомпресію при передачі голосу в реальному часі, функції синхронізації й передачі, тобто забезпечує взаємодію з локальною комп’ютерною мережею (ЛАН). Також через шлюз взаємодії *CDMA-IP* забезпечується доступ оператора до корпоративних базових станцій для технічної експлуатації й обслуговування.

Інтегрований шлюз/перехоплювач (*Gateway/Gatekeeper*) – перехоплювач, що підтримує інтерфейс *CSTA* (*Computer Supported Telephony Applications*) з АТСОЗ, що дає можливість адаптувати через (ЛАН) послуги АТСОЗ для використання мобільними телефонами; шлюз, взаємодіючий з перехоплювачем на основі сигналізації Н.323 і підключається до АТСОЗ сполучними лініями *E*1. Шлюз/перехоплювач забезпечує маршрутизацію викликів, ґрунтуючись на корпоративному плані нумерації, здійснює трансляцію адрес, управляє встановленням з’єднання. Через цей вузол проходить весь трафік сигналізації при будь-яких вхідних або вихідних дзвінках з мобільного телефону або на мобільний телефон.

Сервер адміністрування абонентів – цей вузол є ключовим в мережі. Якщо по виконуючих функціях шлюз взаємодії *CDMA-IP* схожий з контролером базових станцій і центром мобільної комутації, то сервер адміністрування абонентів зберігає всі бази даних абонентів з інформацією про їх – номера, займані посади, профілі обслуговування, доступ до додаткових послуг і т. д. На цьому сервері виробляється видалення та реєстрація нових абонентів, зміна профілів користувачів мережі.

Сервер адміністрування абонентів виконує функції керування мобільністю користувачів у межах мережі, тобто він відслідковує, у зоні обслуговування якого шлюзу взаємодії *CDMA-IP* перебуває абонент. Саме він здійснює аутентифікацію користувачів мобільних телефонів *CDMA*, які попадають на територію радіо- покриття корпоративних базових станцій, і дозволяє доступ до них, а отже, і підключення до послуг корпоративного *CDMA* тільки зареєстрованим абонентам (співробітникам підприємства). Сервер адміністрування абонентів

через шлюз сигналізації взаємодіє з регістром оператора мобільного зв'язку для обміну даними про місцезнаходження абонентів, одержанню аутентифікованих параметрів і т. д.

Устаткування *CDMA* має високий ступінь масштабованості, може бути встановлене на підприємствах будь-якого розміру й розширюватися разом з його ростом. Архітектура легко може бути адаптована для підтримки послуг систем 3-го покоління (*UMTS*) *(універсальна система рухливого зв'язку).*

Рішення корпоративного *CDMA* дає вигоди не тільки корпоративним клієнтам, але й операторам мобільного зв'язку.

По-перше, корпоративний *CDMA,* забезпечує вихід на перспективний сектор ринку корпоративних клієнтів, відкриває нове джерело доходів і збільшує конкурентоспроможність оператора за рахунок надання корпоративним клієнтам великої кількості сучасних послуг.

По-друге, корпоративний *CDMA,* забезпечує ріст абонентської бази за рахунок співробітників підприємств. Із впровадженням цього рішення рівень проникнення на території підприємства значно збільшиться.

По-третє, корпоративний *CDMA,* зменшує витрати на надання послуг: знижуються витрати на обслуговування кожного абонента.

Якщо раніше дзвінок кожного співробітника доводилося тарифікувати окремо, то тепер з підприємства береться щомісячна плата на основі кількості підключених співробітників, використаних частот, навантаження на базові станції. І останнє, це крок до переходу мереж, повністю орієнтованих на *IP* (*All- IP*).

Сучасні оператори бездротового зв'язку активно шукають нові шляхи для підвищення прибутковості бізнесу й зміцнення свого фінансового становища. Скорочення вартості експлуатації й управління мережі, а також можливість впровадження нових привабливих мережних послуг і додатків.

Багато операторів переходять від комутації каналів до комутації пакетів, що дозволяє більш ефективно збільшувати обсяги трафіка, підтримувати прибуткові мультимедійні послуги й у той же час скорочувати витрати. Загальна мета складається в переході до мереж *All-IP*, які сполучать кращі якості Інтернету із кращими характеристиками сучасних мереж голосового зв'язку

ЛІТЕРАТУРА

1. *Гордиенко В. Н., Тверецкий М.С.* Многоканальные телекоммуникационные системы. Учебник для вузов – М., Связь, 2006. – ст. 572.

2. *Рихтер С. Г.* Цифровое радиовещание – Горячая Линия-Телеком, 2008. – ст. 640.

3. *Тяпичев Г. А.* Спутники и цифровая радиосвязь. – М.: Радио и связь, 2007. – ст. 536.

4. *Смит С. Р.* Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников –Додэка-XXI, 2008. – ст. 580.

Літвін К.К. (НТУУ „КПІ”)
Літвін К.І. (УТЕЛ)
к.т.н. Шелепенко Ю.В. (ВІТІ НТУУ „КПІ”)

# МОДИФІКАЦІЯ АЛГЕБРАЇЧНОГО ДЕКОДЕРА В АПАРАТУРІ ПЕРЕДАЧІ ДАНИХ

Підвищення достовірності передачі даних в системах зв’язку, як правило, проводиться в два етапи: на першому – використовується корегуючий код в режимі виявлення або часткового виправлення помилок і на другому – повторно передаються кодові комбінації з невиправленими помилками.

Для блокового кодування широке розповсюдження знайшли алгебраїчні методи кодування.

Алгебраїчному декодуванню піддаються коди Боуза-Чоудхури-Хокквінгема, Рида-Соломона та Ріда-Маллера, які є в сучасний час найкращими з точки зору реалізації декодера.

Декодування таких кодів здійснюється за допомогою рішення системи алгебраїчних рівнянь, при цьому процедуру рішення як двійкових, так і недвійкових кодів аналогічні. В апаратурі передачі даних з завадостійким лінійним блоковим кодом знайшли практичне використання три алгоритми декодування: Пітерсона-Гористейна-Цирлера (ПГЦ), Берлекемпа-Мессі (БМ) та Евкліда.

Позитивна властивість алгебраїчного декодера – хороше мікропрограмування.

Декодер, який виправляє помилки, рішає в загальному три задачі: виявляє факт присутності помилки, вираховує їх місцезнаходження та значення.

Проведені дослідження показали, що введення контролю корективності Y(x) (багаточлена локаторів помилок) дозволяє зменшити вірогідність помилкового декодування на 6 дБ, а в деяких випадках – на 20 дБ і більше[1].

Пропонується модифікація рішення ключового рівняння прямого алгоритму Пітерсона, яка ґрунтується на контролі коректності багаточлена локаторів помилок.

Коректність багаточлена перевіряється за допомогою рекурентної генерації компонент синдрому. Введення операції контролю коректності багаточлена локаторів помилок дозволяє знизити на порядок ймовірність помилкового декодування за порогом конструктивної мінімальної кодової відстані.

ЛІТЕРАТУРА

1. *Літвін К.І.* Модифікация алгоритму алгебраїчного декодування Пітерсона-Гористейна-Цирлера. – К. КВІУЗ. Деп..в ДНТБ України №193-Ук 1997. – 11.

Літвін К.І. (УТЕЛ)
Літвін К.К. (НТУУ „КПІ”)
к.т.н Шелепенко Ю.В. (ВІТІ НТУУ „КПІ”)

# БЛОКОВІ СИГНАЛЬНО-КОДОВІ КОНСТРУКЦІЇ КАСКАДНОГО ТИПУ

Основу побудови високошвидкісних пристроїв перетворення сигналів (УПС) по стандартни [канала] тональної частоти (СКТУ) складають багатопозиційні ансамблі сигналів (БАС), які дозволяють для обмеженої фізичної швидкості B=$1/\tau_0$ підвищити швидкість передачі даних (ПД).

Збільшення потужності БАС зменшує евклідовий проміжок між сигналами і призводить до нееквідистантської системи, а ввід допоміжного крата інформації в БАС об’ємно-сферичній упаковці знижує співвідношення сигнал-шум на 2,5…4 дБ і, як наслідок, наявність широкого спектра показників вірності реєстрації елементів маніпуляційного кода Q. Відомо, що вірогідність характеристики БАС можна попередньо розрахувати, а апріорну інформацію використовувати в каналі ПД. В існуючій апаратурі передачі даних (АПД), ця інформація не використовується, що знижує достовірність ПД. Виникає невідповідність між необхідністю в високошвидкісній ПД з використанням ресурсів первинного каналу зв’язку для підвищення достовірності.

У багатьох дослідженнях прикладного характеру робиться припущення, що фігуруючі потоки подій є пуассонівськими (ППП). Це пояснюється не тільки тим, що введення ППП спрощує дослідження і полегшує знаходження рішення, а ще і тим, що ППП (або вельми близький до них за структурою) часто має місце насправді, оскільки в певному значенні він є граничним для різних потоків.

Сумарну інтенсивність потоку помилок в дискретному каналі зв’язку можна зменшити за допомогою багатократного перешкодостійкого кодування, що еквівалентно декореляциії помилок і поліпшенню загальної роботи декодера (у обмін на їх число). Це прояснює фізичну природу енергетичного виграшу в сигнально – кодових конструкціях каскадного типу.

Запропонована методика синтезу блокових сигнально-кодових конструкцій (СКК) на базі каскадних кодів (з оператором внутрішнього кодування, формуючих оптимальні і квазіоптимальні БАС в евклідовій метриці, і зовнішніми завадостійкими лінійними блоковими кодами, які забезпечують дистанційні властивості, що підвищують швидкість ПД для СКТЧ з МСІ, ФД та ін.) [1].

Наведено рішення задачі синтезу СКК для каналів із МСІ і фазовими зрушеннями отримано на базі узагальнених каскадних кодів, де внутрішній код контролює сферичні властивості СКК та МСІ, а зовнішні (згортаючі) коди – дистанційні властивості.

Розроблені структурна схема узагальненого каскадного кодера і декодера для завадостійких сферичних СКК.

ЛІТЕРАТУРА

1. *Літвін К.І.* Модифікация алгоритму алгебраїчного декодування Пітерсона-Гористейна-Цирлера. – К. КВІУЗ. Деп..в ДНТБ Украіни №193-Ук 1997. – 11 с.

Лук'янчук І.В. (ВІТІ НТУУ„КПІ")

# ПІДВИЩЕННЯ БЕЗПЕКИ ПЕРЕДАЧИ ІНФОРМАЦІЇ В СИСТЕМАХ РАДІОЗВ'ЯЗКУ З ВИКОРИСТАННЯМ ШИРОКОСМУГОВИХ СИГНАЛІВ

З розвитком систем радіозв'язку безпека передачі інформації займає одне з основних місць при розробці нових перспективних систем. При порівнянні систем радіо зв'язку з провідними системами зв'язку по перешкодозахищеності, то як правило переваги віддають провідним системам. При розгляданні систем радіозв'язку і провідних систем зв'язку по завадозахищеності, як багаторівневої моделі можливо зробити висновок , що основні зусилля по захисту передачі інформації концентруються на верхніх рівнях цих систем, різниця є лише на початкових рівнях.

При розробці систем радіозв'язку основні зусилля концентрують по захисту передачі інформації, до таких основних загроз, як :

– порушення фізичної цілісності системи;

– перехват передаваємої інформації;

– проникнення в систему.

Для захисту від цих загроз використовують різні методи такі, як методи засновані надпросторової, частотної, поляризаційної селекції сигналів або використовують сигнали структура яких забезпечує високу завадозахищеність.

Аналіз систем по завадозахищеності та скритності для систем радіозв'язку показує, що використання широкосмугових сигналів дозволяє значно підвищити безпеку передачі інформації. Застосування сигналів з широкосмуговим спектром дозволяє отримати виграш у відношенні сигнал/завада. Також при введені до структури широкосмугового сигналу елементу випадковості (псевдо-випадковість), якій знає отримувач, та про якій не має інформації джерело загроз, це примушує останнього синтезувати завадовий сигнал без знання псевдо-випадкового зразка.

Прихованість систем радіозв'язку з широкосмуговими сигналами досягається в першу чергу за рахунок енергетичної прихованості. В даному випадку сигнал передається з дуже низьким рівнем потужності відносно основного шума канала і теплового шума, якій створюється на приймальної антені. В частковості, як що джерелу загроз завчасно невідома структура сигналу при формуванні широкосмугового сигналу методом псевдо-випадкової послідовності, то стає можливим приховати сам факт передачі, маскуючи сигнал шумами або другим найбільш сильним сигналом. Як що структура сигналу жорстко стандартизована, то перевагу необхідно віддати сигналу сформованому методом псевдо-випадкової перебудови частоти, де користувач має можливість задавати послідовність стрибків частоти. Так при використанні в системах радіо зв'язку широкосмугових сигналів можливо досягнути рівня безпеки провідних систем зв'язку.

## ЛІТЕРАТУРА

1. *Помехоустойчивость* и эффективность систем передачи информации / Под ред. А. Г. Зюко. – М.: Радио и связь, 1985. – 272 с.

2. *Борисов В. И.* и др. Помехозащищенность систем радиосвязи с расширением спектра методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000 – 384с.

3. *В.И.Борисов, В.М.Зинчук, и др* Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью./ Под ред. В.И.Борисова. - М.: Радио и связь, 2003. – 640 с..

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

# ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ПРОГРАМНИХ ПРИЙОМІВ ШИФРУВАННЯ ІНФОРМАЦІЇ В ДОДАТКАХ, РОЗРОБЛЕНИХ НА МОВАХ ВИСОКОГО РІВНЯ

Основними критеріями якості програмного забезпечення, на які звертає увагу користувач при обранні клієнта для передачі зашифрованої інформації відкритими каналами зв’язку є: надійність доставки кореспонденції; швидкість відправки і прийому повідомлення; зручний інтерфейс, що полегшує користування; доступність серверів *POP3* та *SMTP*; малий час реакції служби технічної підтримки; сумісність (відсутність) конфліктів із системним, прикладним програмним забезпеченням (ПЗ); відмовостійкість (надійність) – ймовірність відмови захисту, час напрацювання на відмову, імовірність відмови програми захисту (крах), час напрацювання на відмову, частота помилкових спрацьовувань; вартість – вартість / ефективність, вартість / ціна захищаємого ПЗ, вартість / ліквідовані збитки.

Проблема якості програмного забезпечення стає сьогодні все більш гострою, особливо в міру розширення використання новітніх інформаційних технологій і зростання складності ПЗ. Висока якість продуктів дає розробникам не тільки конкурентні переваги і кредит довіри клієнтів, а й полегшує супровід і розвиток програмного забезпечення.

Один з ключових елементів забезпечення якості програмного забезпечення є етап тестування. Тестування – це будь-яка діяльність, спрямована на виявлення помилок у програмному продукті.

Тестування програмного продукту одночасно проводиться за трьома напрямками:

1. Перевірка коду (*review*). Переглядається вихідний код візуально і знаходяться в ньому помилки, а також різні невідповідності коду та вимог до нього. Під вимогою розуміється стандарт, якого дотримуються розробники даного проекту, реакція на ті чи інші дії з боку середовища впливу на ПЗ, поведінку програмного продукту в різних ситуаціях.

2. Тестування високого рівня. Головною метою є з’ясовування, чи задовольняє розробка всім вимогам замовника. Більшість виявлених помилок на цьому етапі пов’язано з помилками взаємодії програмного продукту з користувачем – висновок помилкових повідомлень – неправильна реакція на запит від оператора і т.п.

3. Тестування низького рівня. Тестувальник перевіряє, на скільки логічно повно вихідний код покриває всі можливі варіанти роботи системи, для якої він розробляється.

З зростанням важливості інформаційних технологій для життя суспільства зростає ціна помилок у програмах. У цих умовах на перший план виходять технології та методи тестування програмного забезпечення, які дозволяють своєчасно виявити і виправити ці помилки.

ЛІТЕРАТУРА

1. *Макгрегор Д., Сайкс Д.* „Тестирование объектно-ориентированного программного обеспечения”, Киев, ДиаСофт, 2002.

2. *Агапов А. С., Зенин С. В., Михайловский Н. Э., Мкртумян А. А.* Оценка и аттестация зрелости процессов создания и сопровождения программных средств и информационных систем (*ISO/IEC TR 15504-CMM*), Пер. с англ. Москва, „Книга и бизнес”, 2001.

3. *http://kiev-security.org.ua*.

Люлін Д.О. (НЦЗІ ВІТІ НТУУ „КПІ”)
Іохов О.Ю. (НЦЗІ ВІТІ НТУУ „КПІ”)
Кротов В.Д. (НЦЗІ ВІТІ НТУУ „КПІ”)

# ПЕРЕШКОДОСТІЙКІСТЬ DTMF СИГНАЛІВ ПРИ ПЕРЕДАЧІ КОРОТКИХ ПОВІДОМЛЕНЬ В СИСТЕМАХ ЗВ’ЯЗКУ ЗСУ

На теперішній час сигнали DTMF використовуються в системах передачі сигналу пошукового виклику, в дистанційних системах управління, автовідповідачах, мобільних радіосистемах. У військовій техніці сигнали DTMF поки що не використовуються, що обумовлює інтерес до вивчення можливостей їх використання в сучасних системах зв’язку.

Аналіз застосування DTMF сигналів показав, що їх використання в системах зв’язку надає наступні переваги:

можливість асинхронної передачі кодограм (немає потреби в тактовій синхронізації);

можливість змінювати швидкість передачі та довжини посилки в залежності від інтенсивності перешкод;

простоту реалізації псевдовипадкового перестросовання частоти.

Проведений аналіз принципів формування і обробки DTMF сигналу показав простоту апаратної та програмної реалізації DTMF, але незважаючи на це гарні характеристики з завадостійкості.

DTMF сигнал складається з двох гармонічних складових, що додаються при формуванні, які розподілені на дві групи частот – верхньої та нижньої.

Визначимо середню імовірність правильного прийому в верхній групі частот. Так як імовірності відправки кожної з $f_i$ рівні, отримаємо [1]:

$$P_{ср}^{\ в.гр} = \frac{1}{4}\sum_{i=1}^{4} P_{пр}^{\ в.гр}(f_i / f_i).$$

Аналогічно, для нижньої групи частот:

$$P_{ср}^{\ н.гр} = \frac{1}{4}\sum_{i=1}^{4} P_{пр}^{\ н.гр}(f_i / f_i),$$

де $P(f_i^* / f_i)$ – умовна імовірність того, що при передачі складової $f_i$ буде прийнято рішення о прийомі $f_i$, де $i$ – номер частоти в групі, $i = 1...4$.

$P(f_j^* / f_i)$ – умовна імовірність того, що при передачі складової $f_i$ буде прийнято рішення о прийомі $f_j^*$, $j = 1...4$, $i \neq j$.

Так як здійснюється накопичення часових інтервалів, отримаємо [2]:

$$P(f_i^* / f_i) = \sum_{k=m}^{n} C_n^{\ k} P^k(\tau \in (\alpha_i, \beta_i))(1 - P(\tau \in (\alpha_i, \beta_i)))^{n-k},$$

де $n$ – кількість інтервалів, що накопичуються, $m$ - поріг.

$$P(f_j^* / f_i) = \sum_{k=m}^{n} C_n^{\ k} P^k(\tau \in (\alpha_j, \beta_j))(1 - P(\tau \in (\alpha_j, \beta_j)))^{n-k}$$

Умовна імовірність правильного прийому однієї складової $f_i$ [3,4]:

$$P_{пр}(f_i / f_i) = P(f_i^* / f_i)\prod_{j=1}^{4}\left[1 - P(f_j^* / f_i)\right],\ i \neq j.$$

Імовірність правильного прийому однієї двочастотної посилки, визначається в термін контрольного інтервалу часу (часу накопичення):

$$P_{пр}^{\ \prime} = P_{пр.ср}^{\ в.гр} \cdot P_{пр.ср}^{\ н.гр}.$$

Так як кінцеве рішення про прийом двотональної посилки приймається тільки після перевірки довжини посилки, імовірність правильного прийому можна визначити як:

$$P_{пр} = \left( P_{пр}{}' \right)^{l},$$

де $l = \dfrac{\Delta T}{\Delta t}$, $\Delta T$ – довжина двох тональної посилки, $\Delta t$ – час накопичення часових інтервалів.

Таким чином імовірність похибки дорівнює:

$$P_{ош} = 1 - P_{пр}.$$

На рис. 1 приведені криві залежності імовірності похибки на символ DTMF сигналу (крива 1), на біт (крива 2) від відношення сигнал/шум. Для порівняння приведена (крива 3) залежність залежності імовірності похибки на біт від відношення сигнал/шум для випадку некогерентного прийому сигналів з частотною модуляцією.

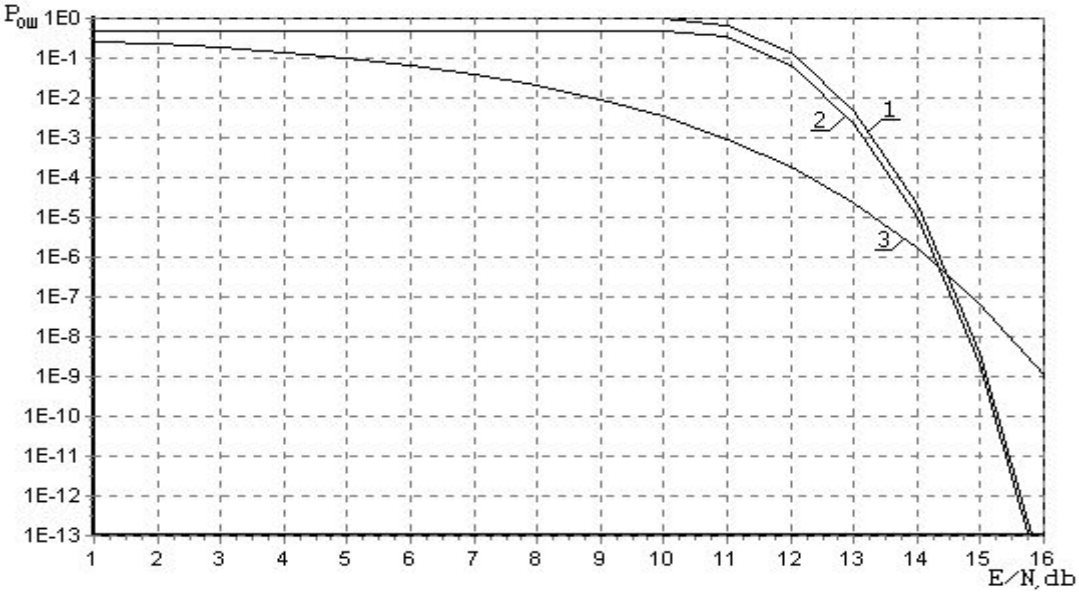



Рис. 1. Залежність імовірності похибки від відношення сигнал/шум

Аналіз кривих показує, що для досягнення ймовірності похибки на біт $10^{-3}$ при використанні DTMF сигналів відношення сигнал/шум повинно бути не менш 13,2 дБ. У разі некогерентного прийому з частотною маніпуляцією для отримання тієї ж імовірності похибки необхідно відношення сигнал/шум 11 дБ. Таким чином DTMF сигнали програє на 2,2 дБ. При імовірності похибки $1 \cdot 10^{-6}$ DTMF сигнали та некогерентний прийом сигналів з частотною модуляцією мають майже однакові значення відношення сигнал/шум 14,4 дБ. Після значення відношення сигнал/шум 14,4 дБ імовірність похибки DTMF сигналу різко знижується у порівнянні з некогерентним прийом сигналів з частотною модуляцією

Таким чином вочевидь перевага DTMF сигналів при значенні відношення сигнал/шум більше 14,4 дБ. DTMF сигнали можуть використовуватись у різних підсистемах систем зв'язку ЗСУ в залежності від завдань, які поставлені перед ними.

ЛИТЕРАТУРА

1. *Вентцель Е.С., Овчаров Л.А.* Теория вероятностей и ее инженерные приложения. – М.: Наука, 1988. – С. 129 –135.

2. *Современная радиолокация* (анализ, расчет и проектирование). Пер. с англ. под ред. Кобзарева Ю.Б. – Издательство „Советское радио", 1969. – С. 129 – 134.

3. *Тихонов В. И.* Выбросы случайных процессов. – М.: Наука, 1970. – С. 319 – 334.

4. *Фомин Я. А.* Теория выбросов случайных процессов. – М.: Связь, 1980.

Малигін М.М. (НАОУ ЦВСД)

# МОДЕЛЬ ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ НА БАЗІ ТЕОРІЇ НЕЧІТКИХ МІР ТА НЕЧІТКО-ІНТЕГРАЛЬНОГО ОБЧИСЛЕННЯ

З розвитком інформаційних технологій з'являються нові та дістають подальшого розвитку існуючи загрози інформації, в наслідок чого питання оцінки рівня захищеності інформації в автоматизованих системах (АС) набуває все більшої актуальності [1]. На сьогоднішній день питання оцінки рівня захищеності інформації вирішується шляхом проведення експертизи АС на відповідність встановленим в державі вимогам щодо захисту інформації. Такий підхід пов'язаний насамперед з тим, що АС характеризуються як складні об'єкти, яким притаманні ряд особливостей а саме:відсутній або є неприйнятно складний формалізований опис АС. Тобто має місце складність побудови однозначної функції, що описує стан або динаміку змін станів АС, реакцію АС на зовнішні впливи; показники, що характеризують АС, носять різнорідний характер; значна частина інформації, яка необхідна для опису АС, як правило, існує у вигляді уявлень та побажань фахівців-експертів. Це найчастіше приводить до нечіткості та неоднозначності формального опису елементів АС. Таким чином особливості АС приводять до значних труднощів при рішенні задачі по оцінки рівня захищеності інформації в АС та здійснюють безпосередній вплив на її результат. Для підвищення точності оцінки рівня захищеності інформації в АС під час проведення її експертизи пропонується застосування відповідної для цього моделі. Структура такої моделі описується у відповідності до концептуальної моделі [2]. Сутність концептуальної моделі полягає в тому, що нехай $a_l$ – тип елемента на *l*-м рівні концептуальної моделі. При цьому $l = \overline{0, N}$, де *N* – кількість рівнів концептуальної моделі. Будемо використовувати $a_l$ для позначення будь якого типу елементу *l*-го рівня як змінну $a_l \in A_l$. Можна записати, що $A_l \bigcap A_{l+1} = \varnothing, \bigcup_l A_l = A$, тобто рівнева структура буде охоплювати усі типи концептуальної моделі. Тоді інтенсивність виразу одного типу через інший можливо ототожнювати у вигляді функції. Якщо інтенсивність вимірюється в решітці $L = [0,1]$ то формально тип $a_l \in A_l$ може бути представлений у вигляді нечіткої міри:

$$\mu_{im_H a_l}(\cdot \mid a_{l+1}) : 2^{im_H a_l \times coim_H a_l} \to [0,1] \quad (1)$$

Таким чином, елемент концептуальної моделі – тип реального об'єкту – описується нечіткою мірою (1). Сукупність всіх нечітких мір для всіх типів концептуальної моделі визначає її представлення:

$$\left\langle a_l \in A_l \subseteq A, \mu_{im_H a_l}(\cdot \mid a_{l+1}), l = \overline{0, N} \right\rangle$$

Узагальнена оцінка захищеності інформації здійснюється шляхом вирішення однокритеріальної задачі для кожного з $a_l$ на основі нечіткого інтегралу (2), значення отриманого для об'єкту с заданим „еталонним"[ 3,4].

$$\oint_A h(x) \mu_{im_H a_l}(\cdot) \quad (2)$$

де $H_\alpha = \{x \mid h(x) \geq \alpha\}$, h(x) – функція, що вимірюється. Використання запропонованої моделі на основі нечітких мір та нечітко-інтегрального обчислення дозволяє максимально ефективно врахувати особливості притаманні АС, уявлення експертів про поняття захищеності інформації в АС, а також вимоги державних нормативно-правових документів.

Малюга А.В. (ВІ КНУ)

# МЕТОДИ ТА ЗАСОБИ КОНТРОЛЮ ЗНАНЬ ТИХ, ХТО НАВЧАЄТЬСЯ У СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ.

Широке застосування сучасних прогресивних телекомунікаційних, інформаційних і комп'ютерних технологій, у першу чергу технологій глобальної мережі Internet, є одним із найперспективніших напрямків розвитку освіти. Гнучкий та оперативний доступ до інформації з будь-якої точки, широкі можливості пошуку потрібних даних, своєчасне їх оновлення та інші переваги сучасних інформаційних технологій стимулюють активне застосування їх у практиці багатьох навчальних закладів, зокрема у вигляді дистанційних елементів навчання. Система дистанційного навчання (СДН) дозволяє організувати навчальний процес таким чином, що, з одного боку, вона дає можливість викладачеві всебічно контролювати процеси навчання студента, складання іспитів і проходження тестів, а з другого боку, дає можливість студенту отримати якісні знання і насамкінець документ, який підтверджує одержання вищої чи додаткової освіти.

Сьогодні гостро стоїть питання про якість знань, отриманих із застосуванням технології дистанційного навчання. СДН повинна мати засоби, що дозволяють перевіряти, чи знаходиться за віддаленим комп'ютером саме той, хто навчається і за якого він себе видає, тобто здійснити ідентифікацію користувача. Вирішити цю проблему можна шляхом застосування додаткового програмного забезпечення для розпізнавання користувачів. Принципи, що лежать в основі відповідних алгоритмів, можна розділити на такі: класифікація психофізичних параметрів і класифікація кола інформаційних інтересів користувача із визначенням динаміки їх зміни [1]. З погляду використання даних методів у СДН викликає найбільший інтерес класифікація психофізичних параметрів користувача, до яких належать клавіатурний почерк та психологічний особистісний профіль. Для настроювання моделей користувачів на першому етапі функціонування системи необхідно передбачити тестування в присутності викладача.

Контроль знань того, кого навчають, є важливою частиною роботи з користувачем. Він забезпечує зворотний зв'язок з тим, хто навчається і призначений в першу чергу для визначення рівня знань того, кого навчають з метою організації адаптивного управління навчанням.

У навчальних системах зазвичай використовуються два основні підходи до організації контролю знань [2]:

1. Оцінка дій того, кого навчають. Цей метод застосовується в експертно-навчальних системах, тобто повчальних системах, заснованих на знаннях. Знання про предметну область і правила оцінки дій того, кого навчають дозволяють системі в ході діалогу з тим, хто навчається визначати рівень його знань без ставлення контрольних питань. За допомогою цього методу можна на високому рівні моделювати взаємодію викладача з тим, хто навчається.

2. Стандартизований контроль знань. Суть полягає в тому, що тому, хто навчається пропонується вибірка спеціальних завдань і по відповідям на них виноситься думка про його знання. Стандартизовані методи контролю знань мають наступні позитивні властивості, що визначають доцільність їх застосування: короткочасність перевірки; стандартність проведення перевірки і аналізу результатів; можливість представлення результатів перевірки в числовій формі; можливість математичної обробки результатів.

Стандартизований контроль знань в автоматизованих системах навчання виконується за допомогою тестів [2]. У загальному випадку, коли перевірку результатів тесту здійснює людина, тест – це набір питань і правильних відповідей до них (еталонів). Якщо ж визначення правильності відповіді покладається на ЕОМ, необхідно включити в тест набір параметрів, керівників алгоритмами перевірки виконання тесту.

Наведемо короткий огляд технологій реалізації тестування, які можуть застосовуватися в системах дистанційного навчання. Порівнюється традиційне створення комп'ютерних тестів вручну і тестування на основі семантичних моделей – на основі семантичної мережі і понятійно-тезисної моделі [3].

Традиційний підхід до створення засобів тестування фактично являє собою комп'ютеризацію ручного створення тестів. Переваги тут полягають власне у використанні інформаційно-комунікаційних технологій замість письмового тестування, що дає додаткові можливості щодо управління формуванням тестів з банку створених завдань, автоматичної перевірки результатів. Однаково і перевагою і недоліком даного підходу є ручне, неавтоматичне створення завдань. Основним недоліком підходу є висока трудомісткість самого процесу по формуванню банку завдань.

Наріжним каменем семантичних мереж є так звані тріади [3]: сутність 1 – відношення – сутність 2. Наприклад є такі сутності „процедура" і „програма". В такому випадку між ними можна встановити відношення типу „є частиною". Тоді отримуємо: сутність „процедура" „є частиною" сутності „програма". Завдання тесту будується шляхом опущення одної з ланок тріади і постановкою запитання про відсутню ланку. Перевагою даного підходу є здатність системи міркувати знаннями з предметної області. Недолік полягає у великих витратах при складанні завершеної цілісної семантичної мережі, яка б коректно відображала дану предметну область, що вивчається.

Понятійно-тезисна модель (ПТМ) передбачає однозначний зв'язок семантичних даних із навчальним матеріалом. Це дає можливості для управління навчальним процесом і процесом контролю знань і їх адаптації. В даному випадку ми маємо інформацію про поняття і їх місце знаходження у навчальному матеріалі. Кількість семантичних одиниць, що стосуються поняття, з легкістю обраховується для кожного навчального фрагменту. Насправді система не міркує знаннями з предметної області, проте щодо окремих висловів чи тверджень, які описують поняття і сприймаються системою „як є", вона володіє інформацією про те, де вони містяться у загальній структурі навчального матеріалу.

Ключовим моментом технології є семантичний розбір навчального тексту. Фактично це заміняє формування баз знань у таких підходах як семантичні мережі, концептуальні графи тощо. Перевагою є природність даного процесу у технології ПТМ. Крім того в даній технології робиться акцент на педагогічному підході, тоді як в традиційних технологіях штучного інтелекту акцентується увага на питаннях характерних для цієї області, що часом є важко прийнятним як для реалізації у рамках педагогічної комп'ютерної системи, так і для працівників-користувачів системи.

У доповіді розглянуті основні підходи до організації контролю знань у системах дистанційного навчання. Наведені основні відомості про проведений аналіз основних існуючих методах та засобах контролю знань тих, хто навчається. Висвітлені основні переваги та недоліки технологій реалізації тестування, які можуть застосовуватися в системах дистанційного навчання.

ЛІТЕРАТУРА

1. *Аванесов В.С.* Научные проблемы тестового контроля знаний / Монография. – М.: Исследовательский центр проблем качества подготовки специалистов, 1994. – 135 с.

2. *Сосюк А.В.* Інтелектуальний автоматизований контроль знань в системах дистанційного навчання // Автоматика. Автоматизация. Электротехнические комплексы и системы. – 2008. – № 2 (22). – С. 94 – 98.

3. *Титенко С.В., Гагарін О.О.* Практична реалізація технології автоматизації тестування на основі понятійно-тезисної моделі // Мат. 10-й Международной конференции Украинской ассоциации дистанционного образования „Образование и виртуальность" – 2006". – Харьков-Ялта: УАДО, 2006. – С. 401 – 412.

Малярчук М.В. (ГУЗІС)
д.т.н. Слюсар В.І.(ЦНДІ ОВТ)

# ПОПЕРЕДНЯ ФІЛЬТРАЦІЯ OFDM СИГНАЛІВ В СИСТЕМІ MIMO ПРИ ДОДАТКОВОМУ СТРОБУВАННІ ВІДЛІКІВ АЦП

Розширення смуги сигналів OFDM до 40 і більше МГц в системах MIMO з цифровим діаграмоутворенням зіштовхується з труднощами формування цифрової діаграми спрямованості антенної решітки в темпі надходження відліків АЦП. Для вирішення цієї проблеми доцільно використовувати додаткове стробування відділків АЦП, що отримало розповсюдження в радіолокаційних системах.

Разом з тим, відомим варіантам виконання цієї операції у разі одноканальної побудови схеми аналого-цифрового перетворення притаманний високий рівень бокових пелюсток амплітудно-частотної характеристики (АЧХ) цифрового фільтра додаткового стробування (ЦФДС) відліків АЦП, що буде знижувати завадозахищеність системи MIMO.

Тому авторами доповіді було запропоновано удосконалені методи додаткового стробування відліків АЦП (заявки на видачу патентів України на корисні моделі №№ u200909210 та u200909211 від 07.09.2009), відмінністю яких є використання попередньої цифрової фільтрації відліків АЦП в режимі „ковзаючого вікна” відповідно до відомих виразів:

$$\mathrm{U}_{\mathrm{t}}^{\mathrm{c}} = U_t - 11\cdot U_{t+2} + 15\cdot U_{t+4} - 5\cdot U_{t+6},\ \mathrm{U}_{\mathrm{t}}^{\mathrm{s}} = 5\cdot U_{t+1} - 15\cdot U_{t+3} + 11\cdot U_{t+5} - U_{t+7}, \quad (1)$$

де t – порядковий номер відліку АЦП, $\mathrm{U}_{\mathrm{t}}^{\mathrm{c}}$, $\mathrm{U}_{\mathrm{t}}^{\mathrm{s}}$ – квадратурні складові напруг.

Метою доповіді є викладення результатів дослідження властивостей математичного моделювання каналу прийому OFDM сигналів, що використовує удосконалений метод додаткового стробування відліків АЦП.

При цьому головна увага приділена з’ясуванню та врахуванню в моделі каналу прийому даних амплітудних і фазових викривлень, що вносяться в сигнал OFDM внаслідок виконання вагового підсумовування відліків АЦП за виразом (1).

За результатами моделювання підтверджено, що поліпшена завадозахищеність удосконаленого методу додаткового стробування відліків АЦП з урахуванням виразу (1) виразно спостерігається лише у випадку довжини стробу 8 та 16 відліків АЦП. Так на рис. 1 наведено модулі АЧХ процедури (1) (лінія 1), відомого алгоритму одноканального ЦФДС (пунктирна лінія) та удосконаленого ЦФДС, що передбачає попередню фільтрацію (1) (суцільна лінія), для довжини стробу 8 віділків АЦП.

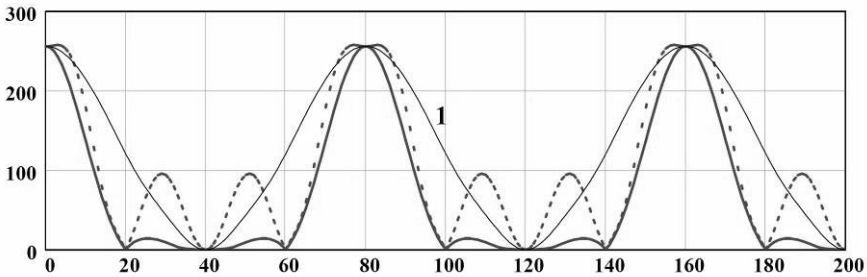



Рис. 1

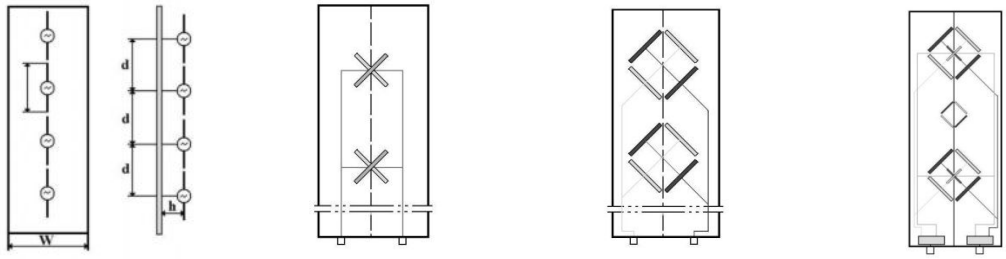
При збільшенні довжини стробу ефективне пригнічення бокових пелюсток АЧХ ЦФДС відбувається лише для частотних регіонів, суттєво віддалених від головних максимумів АЧХ. Ця обставина спонукає до пошуку варіанта процедури (1), що залучала б в обробку більше, ніж 8 відліків АЦП.

Мацаєнко А.М. (ВІТІ НТУУ „КПІ”)
Цімура Ю.В. (ВІТІ НТУУ „КПІ”)
Шацький І.А. (ВІТІ НТУУ „КПІ”)

# СИНФАЗНІ АНТЕННІ РЕШІТКИ НА НИЗЬКОПРОФІЛЬНИХ ВИПРОМІНЮВАЧАХ

Антенний пристрій базових станцій систем мобільного радіозв’язку є найважливішим елементом системи, який визначає її тактико-технічні можливості. Такі антени відносяться до класу високо піднятих, а тому потребують дорогих мачт та живлячих фідерів. Тому питання, пов’язані з розробкою нових технічних рішень з компоновки антенних пристроїв базових станцій, модернізації вже існуючих, які реалізовані в діючих системах мобільного радіозв’язку, актуальні й мають практичну значимість. Специфічною вимогою до антенних пристроїв базових станцій (АП БС), (без впливу на коефіцієнт підсилення) є формування заданої характеристики направленості в азимутальній площині, визначеної принципами побудови систем мобільного радіозв’язку. До найбільш поширених характеристик направленості АП БС відносяться: кругова чи квазікругова; секторна із заданим значенням ширини сектора за рівнем половинної потужності випромінювання; одно- чи двонаправлена, наприклад, для організації радіозв’язку між абонентами, які розташовані вздовж витягнутих об’єктів. Для реалізації цих вимог в теперішній час використовуються такі антени як АШ-h з довжиною провідника h=(0.25..0.625)λ, де λ – довжина хвилі робочого діапазону. Логічним етапом модернізації штирьових випромінювачів, стало створення колінеарних антен, представляючи собою послідовне з’єднання антенних вібраторів через фазозсуваючий вузол. Колінеарні антени знайшли більш широке поширення на практиці порівняно з штирьовими антенами (АШ-h), але їх недоліки такі: мала механічна міцність (за виключенням коаксіальних колінеарних антен); вузький діапазон робочих частот за вихідним опором; складність настройки антени на етапі її розробки. Вказані недоліки колінеарних антен в деякій мірі обмежують їх використання. Найбільш широкими функціональні можливості в плані формування заданих характеристик направленості (ХН) в азимутальній площині можуть забезпечити антенні решітки, які виконані в вигляді симетричного вібратора над циліндричною поверхнею (трубкою) або симетричного вібратора над плоским екраном (панельні антени). При всіх перевагах вібраторних антен для базових станцій систем мобільного зв’язку, особливо метричного діапазону (МХ) та нижньої частини дециметрового (ДМХ), котрі виконані на основі вібратора над циліндричною поверхнею необхідно зауважити й низку їх суттєвих недоліків. По-перше – високі масо-габаритні показники; по-друге – обмеження по формуванню потрібних ХН в азимутальній площині; по-третє – уразливість антенної системи до зовнішнього впливу навколишнього середовища; по-четверте – висока металоємність антени. В підсумку вказані недоліки призводять до високих матеріальних витрат та виготовлення (виробництво), що в свою чергу спонукає до пошуку нових технічних рішень при розробці АП БС для систем зв’язку з рухомими об’єктами. В верхній частині дециметрового діапазону довжини хвиль реалізація антенних решіток з випромінюючим елементом у вигляді вібратора над циліндричною поверхнею ускладнена перш за все при виготовлені конструкції антени, тому доцільно вібраторні антенні решітки створювати на випромінювачах у вигляді симетричного вібратора над плоскою поверхнею. На рис. 1 показано декілька варіантів побудови таких антен, а саме система синфазних вібраторів над плоским екраном шириною W≈(0.5..0.7)λ; два варіанта (рис. 1а, б) вібраторної антенної решітки з кросполяризованим випроміненням; дводіапазонна антенна решітка (рис. 1г). Такі антени широко застосовуються та успішно експлуатуються в теперішній час різними операторами систем стільникового радіозв’язку. Габарити вібраторних антенних решіток ДМХ можливо суттєво скоротити, якщо перейти від випромінюючих елементів електричного типу (симетричних вібраторів) до випромінюючих елементів магнітного типу

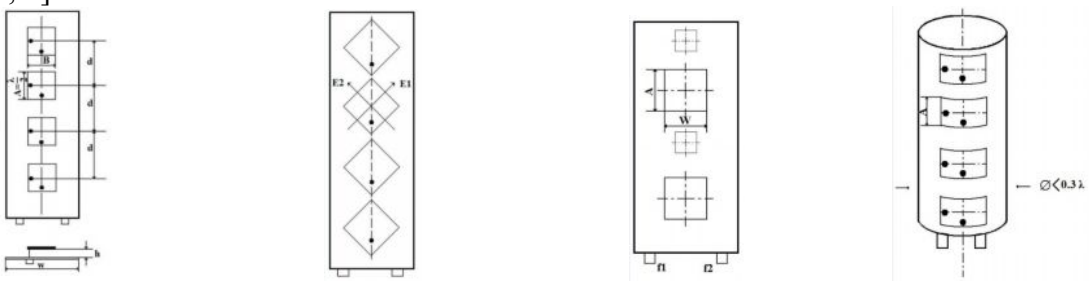
(наприклад, щілинного вібратора), при цьому в якості екрана використовується не тільки плоский екран, а і циліндричний.




а) б) в) г)

Рис. 1

Технічна реалізація нового підходу до компоновки антенних решіток базується на використанні в якості випромінюючих елементів низькопрофільних антен, що відносяться до класу магнітних (щілевих) випромінювачів. Одною із особливостей таких антен є їх компактність та мала вага. Антена представляє собою дві пластини рознесених між собою на відстань h>>λ, де λ – довжина хвиль, одна з яких виконує роль екрана, друга менших розмірів – випромінюючий елемент. В об'єм між пластинами вводиться вузол збудження і діелектрик, що дозволяє скоротити різницю випромінювача в $\frac{1}{\sqrt{\varepsilon}}$ раз, ε – відносна діелектрична проникність заповнюючого матеріалу. Використання низькопрофільних антен в якості випромінюючих елементів в антенній решітці це – зменшення габаритів, покращення електричних характеристик, розширення функціональних можливостей антенної решітки в цілому.На рис. 2 показана синфазна антенна решітка на низькопрофільних випромінювачах, розмір екрана якої рівний $W = \frac{\lambda}{2\sqrt{\varepsilon_r}}$, висота випромінювача h<<λ. На рис. 2 б представлений варіант антенної решітки з кросполяризаційним випроміненням. Рис. 2 в демонструє варіант дводіапазонної антенної решітки. Представлені варіанти антенних решіток дозволяють формувати секторне поле випромінювання в азимутальній площині з сектором приблизно 60° (ширина ДН на рівні половинної потужності). З метою збільшення сектора покриття пропонується антенна решітка на циліндричній поверхні (рис. 2 г). Зменшуючи діаметр (Ø=2 а), фіксуючи розмір верхньої пластини, можливо змінити розмір поперечної випромінюючої щілини, а тим самим змінювати ширину її ДН – від 80° до 160°. Теоретична частина по дослідженню електричних характеристик НПА над циліндричною поверхнею достатньо детально наведена в роботах [1, 2]




а. б. в. г.

Рис.2

У висновку слід відмітити, що використання низько профільних антен в якості випромінюючих елементів антенної решітки, призначених для базових станцій мобільних систем радіозв'язку дозволяє не тільки підвищити масо-габаритні показники, покращити їх електричні характеристики, але й покращити надійність антенно-фідерного пристрою в цілому.

ЛІТЕРАТУРА

1. *Ільінов М.Д., Мацаєнко А.М.* Особливості розрахунку зовнішніх характеристик низькопрофільних випромінювачів над циліндричною поверхнею. – К.: Збірник праць НАОУ, 2007. – № 1 (81). – С. 136 – 146.

д.т.н. Машков О. А. (ВАК України)
к.т.н. Шуренок А. В. (ЖВІНАУ)
Самчишин О. В. (ЖВІНАУ)

# ЗАСТОСУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ СИСТЕМИ РАДІОМОНІТОРИНГУ

Система радіомоніторингу (РМ) – це розподілена інформаційно-керуюча система, яка являє собою розосереджені на деякій території засоби автоматизованої обробки інформації для вирішення завдань накопичення, обробки, збереження й передачі інформації. У сучасних умовах на систему РМ негативно впливають як внутрішні (відмови, збої, помилки корпоративних абонентів), так і зовнішні (активний або пасивний вплив навколишнього середовища) фактори [1]. Тому забезпечення функціональної стійкості системи РМ є актуальним завданням.

Найбільш відомими показниками функціональної стійкості для системи радіомоніторингу є похибка визначення координат об'єктів і джерел радіовипромінення (ОРДРВп) та їх спостереження з необхідною інформативністю [2].

Таким чином, функціональна стійкість системи РМ повинна визначатись через вірогідності знаходження координат ОРДРВп із заданою точністю та їх спостереження з необхідною інформативністю. Одним із шляхів вирішення цього завдання є створення інформаційної системи підтримки прийняття рішення (ІСППР), що забезпечить сумісне використання різнотипних засобів радіомоніторингу, вибір методів пеленгування або їх комплексування, обґрунтування варіанта розподілу сил та засобів системи РМ на пошук і спостереження, що має найбільшу інформативність її цільового застосування.

Реалізація ІСППР для системи РМ базується на відповідних методиках: комплексування застосування засобів кутомірного та різницево-далекомірного методів місцевизначення, з подальшим створенням на її основі математичної моделі визначення координат (з використанням сферичних моделей земної поверхні); розподілу сил та засобів за об'єктами і джерелами радіовипромінення на основі методів динамічного програмування.

Така система підтримки прийняття рішень повинна вирішувати два основні завдання: вибір найкращого рішення з множини можливих та упорядкування можливих рішень за перевагою.

На основі відомих методик синтезу системи підтримки прийняття рішення основними етапами її побудови для системи РМ повинні бути [3]: формування матриці знань про характер ОРДРВп і їх розміщення на базі збору експертної інформації та її обробки; створення баз знань і процедур їхньої обробки (лінгвістичних правил прийняття рішень) у різних станах системи РМ, у тому числі й парируванні наслідків нештатних ситуацій; розробка методики навчання і донавчання системи на основі експертної й оперативної інформації про стан радіоелектронної обстановки.

ЛІТЕРАТУРА

1. *Машков О. А.* Обеспечение функциональной устойчивости сложных иерархических систем / Машков О. А., Машков В. А. // Тези доповідей І Української конференції з автоматичного управління. – Київ. : АН України, 1994 – Ч.І. – С. 205.

2. *Пічугін М. Ф.* Методика забезпечення функціональної стійкості системи радіомоніторингу на основі комплексування пасивних методів місцевизначення / Пічугін М. Ф., Шуренок В. А., Самчишин О. В. // Зб. наук. пр. – Житомир. : ЖВІ НАУ, 2008 – Вип. 1. – С.81– 95.

3. *Герасимов Б.М.* Системы поддержки принятия решений: проектирование, применение, оценка эффективности / Герасимов Б. М., Дивизинюк М. М., Субач И. Ю. – Севастополь.: СНИЯЭиП, 2004 – 320 с.

Мєшков І.Н. (НЦЗІ ВІТІ НТУУ „КПІ”)
Черкасова Ю.О. (НЦЗІ ВІТІ НТУУ „КПІ”)
Висоцька Т.М. (НЦЗІ ВІТІ НТУУ „КПІ”)
Нечушкін М.П. (НЦЗІ ВІТІ НТУУ „КПІ”)

# ТЕНДЕНЦІЇ РОЗВИТКУ МЕРЕЖ РУХОМОГО РАДІОЗВ’ЯЗКУ

Основним видом зв’язку з рухомими об’єктами є радіозв’язок. В останні роки спостерігається бурхливий розвиток мереж радіозв’язку як загального, так і спеціального призначення. Основними тенденціями розвитку мереж радіозв’язку є:

перехід на цифрові методи передавання інформації;

широке застосування елементів обчислювальної техніки для автоматизації процесів ведення і відновлення зв’язку;

збільшення кількості одночасно працюючих мереж шляхом комплексного використання часового, частотного і кодового розділення сигналів;

реалізація пакетних режимів роботи радіомереж;

освоєння нових діапазонів частот;

освоєння завадозахищених режимів роботи засобів радіозв’язку;

впровадження багатопараметричної адаптації та адаптивної компенсації завад;

впровадження ретрансляції для збільшення дальності зв’язку;

вдосконалення елементної бази та уніфікація апаратури.

Для гнучкого і плавного переходу на цифрові методи передавання необхідно провести розробку комплексів уніфікованих засобів радіозв’язку, здатних працювати як у мережах з комутацією каналів, так і у мережах з комутацією пакетів.

У зв’язку з тенденцією постійного ускладнення радіоелектронної обстановки, основна увага в перспективних системах радіозв’язку повинна приділятися підвищенню завадозахищеності.

При цьому алгоритми завадозахисту повинні бути достатньо гнучкими для забезпечення функціонування систем в різних завадових ситуаціях. Як при прийомі, так і при передаванні підвищення завадозахищеності може досягатися різними методами:

підвищенням енергетичного потенціалу радіоліній;

застосуванням завадозахищеного кодування;

використанням принципів адаптації за частотою;

компенсацією завади у приймачі;

підвищенням лінійності вхідних трактів радіоприймальних пристроїв;

використанням сигналів з підвищеною завадостійкістю (ШСС, ППРЧ);

здійсненням просторового і (чи) поляризаційного рознесення сигналів.

Стратегія застосування вищезазначених методів підвищення завадозахищеності повинна припускати управління, в першу чергу, тими параметрами сигналів і систем, які не знижують такі важливі показники як пропускна спроможність, безперервність зв’язку, розвідзахищеність та ін.

## ЛІТЕРАТУРА

1. *Доровских А.В., Сикарев А.А.* Сети связи с подвижными объектами.– К: Техника, 1989.– 158 с.

2. *Головин О.В.* Декаметровая радиосвязь.– М: Радио и связь, 1990.– С. 240.

3. *Громаков Ю.А.* Стандарты и системы подвижной радиосвязи.– Москва, 1996.

к.в.н. Микусь С.А. (НАОУ)
к.пед.н. Романюк І.М. (НАОУ)

# ОСНОВНІ ФАКТОРИ, ЯКІ ВПЛИВАЮТЬ НА ПРОЦЕС ОРГАНІЗАЦІЇ ЗВ'ЯЗКУ ПІД ЧАС ПІДГОТОВКИ МИРОТВОРЧИХ ОПЕРАЦІЙ

В сучасних умовах якість управління бойовими діями є вирішальним фактором успіху. Матеріальною основою управління до цього часу був зв'язок. Але стрімке втілення в процеси управління засобів автоматизації та інформаційних технологій вимагає одночасно зі зв'язком розглядати процеси інформатизації органів управління.

Найбільше розвинуті у воєнному відношенні зарубіжні країни при проведенні багатонаціональних операцій по підтримці миру або при локальних воєнних конфліктах, прагнуть створити таку систему управління, яка дозволила б в масштабі реального часу, здійснювати бойове управління штабами, військами і силами.

Тому у провідних країнах розвитку систем, засобів і військ зв'язку в планах будівництва збройних сил наданий статус найвищого пріоритету. Проведення багатонаціональних операцій по підтримці миру (CRO – crises response operations) вимагає зміни поглядів на організацію процесів забезпечення зв'язку та інформатизації під час управління миротворчими силами.

Це пов'язано з тим, що до цих операцій залучаються різноманітні за функціональним призначенням організаційних систем, які розглядаються як об'єкти управління. В ядро таких сил залучаються країни члени НАТО (EAPC – euro-atlantic partnership council), країни не натовського блоку, так і різноманітні державні і недержавні організації. Участь України у миротворчих операціях розпочалась із затвердженням Верховною Радою України відповідної Постанови.

Метою статті є визначення основних факторів, які впливають на процес організації зв'язку під час підготовки миротворчих операцій.

Головна особливість операцій по підтримці миру (CRO) в швидкості зміні переліку завдань, що вирішують підрозділи і частини миротворчих сил.

Тому на основі аналізу матеріалів проведення сумісних навчань, досвіду операцій по підтримці миру (CRO) розглянемо причини появи особливостей в першу чергу під час першої фази організації зв'язку – плануванні, а саме особливості відпрацювання документів і спільних дій при плануванні і проведенні багатонаціональних миротворчих операцій.

Особливістю цих завдань у тому, що вони вирішуються між країнами, що мають різні принципи і стандарти системи зв'язку та інформатизації, а також відрізняються засобами технічної і програмної реалізації, що залучаються до організації зв'язку в системі управління.

Проблема у тому, що з одного боку є бажання країн-учасниць операції по підтримці миру створити єдину систему зв'язку та інформатизації, а з іншого не спроможність технічної реалізації цього проекту в наслідок не узгодженості стандартів військової техніки зв'язку та автоматизації. Вирішення цього питання за рахунок закупки системи зв'язку в одній з країн НАТО вимагає немалих фінансових витрат.

Фактори, які впливають на організацію зв'язку під час підготовки миротворчих операцій:

1. Мандат, який визначає статус сил. Мандат на проведення миротворчої операції встановлює структуру сил, що застосовуються, а також визначає вихідні дані для процесу планування системи зв'язку та інформатизації, визначає юридичний статус сил; він містить спеціальні та можливі задачі планування системи зв'язку та інформатизації; встановлює порядок та вимоги до зв'язку з Організацією об'єднаних націй (UN), неурядовими організаціями (NGO), іншими урядовими організаціями (OGD), приватними добровольчими організаціями та воюючими сторонами в зоні проведення операції; можливість використання

інфраструктури території проведення операції; час проведення операції, обмеження при її проведенні і тривалість операції.

2. Замисел командира. Замисел командира містить у собі: аналіз ситуації; концепцію операції; результат, що очікується.

3. Загальний аналіз ситуації партнерів та країн членів НАТО з питань зв'язку та інформатизації.

При загальному аналізу ситуації враховуються наступні фактори: процедурні стандарти стосовно обміну офіцерами для зв'язку та взаємодії; технічні стандарти для взаємодії систем зв'язку та інформатизації; процедурні стандарти стосовно питань обміну інформацією; навчальні стандарти для персоналу систем зв'язку та інформатизації; мовні стандарти, що покладаються на національні системи зв'язку та інформатизації при підтримці масштабних операцій; створення кожною нацією політичної, моральної, військової та фінансової позиції вимог мандату; обмеження, що покладаються на національні системи зв'язку та інформатизації при підтримці масштабних операцій.

4. Потенційні можливості сил з питань зв'язку та інформатизації. Інформація щодо потенційних можливостей сил містить у собі таку інформацію: досвід, що був отриманий як результат тестів на взаємодію або подібних розгортань військ; технічні та частотні характеристики системи зв'язку та інформатизації; технічні і процедурні стандарти системи зв'язку та інформатизації; досвід персоналу та його чисельність; можливості щодо ремонту обладнання системи зв'язку та інформатизації.

5. Аналіз та врахування досвіду планування системи зв'язку та інформатизації при проведенні попередніх операції по підтримці миру.

Аналіз та врахування досвіду містить наступні аспекти: критична оцінка досвіду планування системи зв'язку та інформатизації з урахуванням умов реалізації поточної операції по підтримці миру; розповсюдження інформації до всіх країн, беруть участь в операції по підтримці миру; доведення найважливішої інформації до персоналу штабів, який здійснює процес планування системи зв'язку та інформатизації.

6. Розподіл частотного ресурсу. Проводиться аналіз розподілу радіочастотного спектру наступними силами та організаціями на території проведення операції по підтримці миру: власні сили; різноманітні угрупування, нейтральні та комерційні організації; ворожі сили (необхідна ідентифікація робочих частот, необов'язково з метою радіоелектронного придушення); неурядові організації (NGO); інші урядові організації (OGO); приватні добровільні організації (PVO).

7. Аналіз театру проведення операції. При проведенні планування системи зв'язку та інформатизації персонал штабу враховує наступну інформацію щодо території проведення інформації: технічні можливості та вимоги країн, на території яких проводиться операція (з цього приводу проводиться консультація з національними організаціями); наявність контакту з воюючими сторонами з метою встановлення зв'язку з ними з метою покращення взаємодії; необхідність взаємодії з неурядовими організаціями (NGO), іншими урядовими організаціями (OGO); приватними добровільними організаціями (PVO); розподіл радіочастотного спектру різноманітними організаціями на театрі проведення операції по підтримці миру (CRO).

Також враховується наступна інформація стосовно театру проведення операції: стан доріг; ресурси; джерела енергії; географічні фактори; стан навколишнього середовища.

8. Оперативні директиви, інструкції та накази інших органів управління. Головний штаб об'єднаних миротворчих сил як правило має прийняту структуру штабів НАТО, яка містить секції J1–J9.

Тому всі секції повинні забезпечити секцію зв'язку та інформатизації (J6) усіма необхідними документами, директивами та інструкціями від інших служб (розвідка, вогнева підтримка, тилове забезпечення, тощо) для їх цілісного аналізу і подальшого врахування при

плануванні системи зв'язку, а саме подати заявки на потрібну кількість каналів зв'язку і види телекомунікаційних послуг та забезпечення інформаційних технологій.

9. Проведення консультацій, співробітництва та взаємодії між країнами-членами та партнерами. Консультації та співробітництво між країнами учасницями, іншими організаціями, країнами, на території яких проводиться операція, повинні проводиться постійно і на всіх етапах операції.

10. Завдання із зв'язку та інформатизації в операції, що планується. Всі країни – учасниці повинні бути ознайомлені з планами операції. В свою чергу вони повинні ознайомити головній штаб (секцію J6) про свої можливості в організації зв'язку, слабких місцях та можливостях сумісної роботи.

11. Аналіз національних можливостей. Цей фактор має вплив на планування системи зв'язку по таких аспектах: включення до системи зв'язку миротворчих багатонаціональних сил місцеві національні ресурси; більш широка підтримка можливостей системи зв'язку та інформатизації (стільниковий зв'язок та використання каналів зв'язку від національних операторів).

Таким чином, з усього вище сказаного можна зробити висновок, що процес організації системи зв'язку та інформатизації для миротворчих операцій є процес кропіткий і складний. Він суттєво відрізняється від процесу планування в минулому.

Його особливістю є необхідність вирішення багатьох різноманітних питань: від організації управління військами силами в операції до налагодження інфраструктури зв'язку країни, де виконується миротворча операція.

к.в.н. Микусь С.А. (НАОУ)

# МЕТОДИКА ОЦІНКИ РАЙОНІВ РОЗГОРТАННЯ ВУЗЛІВ ЗВ'ЯЗКУ ПУНКТІВ УПРАВЛІННЯ З'ЄДНАННЯ ТА ВІЙСЬКОВИХ ЧАСТИН

Район розгортання КП з’єднання визначається вищим штабом. Райони розгортання запасних командних пунктів (ЗКП), пунктів управління логістики (ПУЛ) з’єднання та КП частин визначаються командиром з’єднання за пропозицією начальника штабу (НШ).

Згідно керівних документів начальник зв’язку (НЗ) після усвідомлення завдання і оцінки обстановки доповідає НШ пропозиції щодо районів розгортання ПУ свого штабу (в тому числі їх запасних районів), підпорядкованих підрозділів і на одну інстанцію вниз. Райони розгортання ПУ повинні відповідати тим завданням, які стоять перед з’єднаннями, частинами та підрозділами (визначаються замислом на операцію).

Оскільки ВЗ є елементом ПУ, НШ повинен надати НЗ райони можливого розгортання ПУ, а НЗ повинен їх оцінити у відношенні зв’язку і надати свої пропозиції щодо місць розгортання ВЗ ПУ. Тому виникло завдання розробки методики оцінки районів розгортання ВЗ ПУ з’єднання та частин.

Для того щоб оцінити райони розгортання ВЗ ПУ з’єднання та частин, необхідно спочатку їх визначити. Визначення районів розгортання ВЗ ПУ з’єднання та частин можливо проводити згідно існуючих методик визначення районів розгортання ВЗ ПУ з’єднання та частин.

Методика оцінки районів розгортання ВЗ ПУ з’єднання та частин включає:

1. Постановку завдання, яка полягає у виконанні таких процедур:

визначенні відстані $L^{a_{\text{рац}}}_{\text{зкп(пул)}}$ між районом розгортання ВЗ ЗКП (ПУЛ) з’єднання, та пунктами виділення каналів (ПВК) мережевих вузлів зв’язку (МВЗ) або зонових вузлів зв’язку (ЗВЗ) Телекомунікаційної мережі загального користування (ТКМ ЗК), до яких буде здійснюватись його прив’язка;

визначенні відстані $L^{d_{\text{рац}}}_{\text{кп}}$ між районом розгортання ВЗ КП з’єднання, та СВЗ ДСОМЗ, до якого буде здійснюватись його прив’язка;

визначенні коефіцієнта врахування прийнятої системи управління $K_{\text{вСУ}}$.

2. Визначення районів розгортання ВЗ ПУ з’єднання здійснюється у відповідності до існуючої методики. ЇЇ результатом є визначення раціонального району розгортання ВЗ ПУ (ЗКП, ПУЛ) з’єднання ($a_{\text{рац}}$) з координатами ($x^{a_{\text{рац}}}$, $y^{a_{\text{рац}}}$) і ПВК ТКМ ЗК ($c^{\text{зкп(пул)}}_{\text{рац}}$) з координатами ($x^{c}_{\text{зкп(пул)}}$, $y^{c}_{\text{зкп(пул)}}$).

3. Визначення районів розгортання ВЗ ПУ частин також здійснюється у відповідності до існуючої методики. ЇЇ результатом є визначення раціонального району розгортання ВЗ ПУ (КП) частини ($d_{\text{рац}}$) з координатами ($x^{d_{\text{рац}}}$, $y^{d_{\text{рац}}}$) і ПВК ТКМ ЗК ($c^{\text{кп}}_{\text{рац}}$) з координатами ($x^{c}_{\text{кп}}$, $y^{c}_{\text{кп}}$).

4. Розрахунок відстані $L^{a_{\text{рац}}}_{\text{зкп(пул)}}$ між ВЗ ЗКП (ПУЛ) з’єднання $a_{\text{рац}}$ і ПВК ТКМ ЗК $c^{\text{зкп(пул)}}_{\text{рац}}$, до якого буде здійснюватись його прив’язка здійснюється відповідно до виразу:

$$L^{a_{\text{рац}}}_{\text{зкп(пул)}} = \sqrt{(x^{a_{\text{рац}}} - x^{c}_{\text{зкп(пул)}})^2 + (y^{a_{\text{рац}}} - y^{c}_{\text{зкп(пул)}})^2},$$

е $(x^{a_{\text{рац}}}, y^{a_{\text{рац}}})$, $(x^{c}_{\text{зкп(пул)}}, y^{c}_{\text{зкп(пул)}})$ - координати вибраного району розгортання ВЗ ЗКП (ПУЛ) $a_{\text{рац}}$ та ПВК ТКМ ЗК, до якого буде здійснюватись його прив'язка.

5. Перевірка умови, чи не перевищує розрахована відстань $L^{a_{\text{рац}}}_{\text{зкп(пул)}}$ між ВЗ ЗКП (ПУЛ) з'єднання і ПВК ТКМ ЗК дальності дії засобів прив'язки $R^{\text{пр}}_{\text{ткм зк}}$. При невиконанні умови $L^{a_{\text{рац}}}_{\text{зкп(пул)}} \le R^{\text{пр}}_{\text{ткм зк}}$ прив'язка до ТКМ ЗК неможлива і коефіцієнт врахування прийнятої системи управління з'єднання $K_{\text{вСУ}} = 0$.

6. Розрахунок відстані $L^{d_{\text{рац}}}_{\text{кп}}$ між ВЗ КП частин $d_{\text{рац}}$ і ПВК ТКМ ЗК $c^{\text{кп}}_{\text{рац}}$, до якого буде здійснюватись його прив'язка здійснюється відповідно до виразу:

$$L^{d_{\text{рац}}}_{\text{кп}} = \sqrt{(x^{d_{\text{рац}}} - x^{c}_{\text{кп}})^2 + (y^{d_{\text{рац}}} - y^{c}_{\text{кп}})^2},$$

е $(x^{d_{\text{рац}}}, y^{d_{\text{рац}}})$, $(x^{c}_{\text{кп}}, y^{c}_{\text{кп}})$ - координати вибраного району розгортання ВЗ КП військових частин $d_{\text{рац}}$ та ПВК ТКМ ЗК, до якого буде здійснюватись його прив'язка.

7. Перевірка умови, чи не перевищує розрахована відстань $L^{d_{\text{рац}}}_{\text{кп}}$ між ВЗ КП військової частини і ПВК ТКМ ЗК дальності дії засобів прив'язки $R^{\text{пр}}_{\text{ткм зк}}$.

8. При виконанні умови $L^{d_{\text{рац}}}_{\text{кп}} \le R^{\text{пр}}_{\text{ткм зк}}$, коефіцієнт врахування прийнятої системи управління об'єднання $K_{\text{вСУ}}$ дорівнює коефіцієнту важливості розрахункової задачі по визначенню районів розгортання ВЗ ПУ з'єднання та військових частин $K_{W_i}$, який визначається методом експертних оцінок ($K_{W_i} = 0{,}12$).

9. При невиконанні умови прив'язка до ТКМ ЗК не можлива і коефіцієнт врахування прийнятої системи управління з'єднання $K_{\text{вСУ}} = 0$.

10. Виводиться значення коефіцієнта врахування прийнятої системи управління об'єднання $K_{\text{вСУ}}$.

Таким чином розроблена методика оцінки районів розгортання ВЗ ПУ з'єднання і військових частин дає результат визначення коефіцієнта врахування прийнятої системи управління з'єднання для визначення коефіцієнта обґрунтування рішення, що виробляється органом управління зв'язком з'єднання під час підготовки операції.

Міцан І.Б. (в/ч А1906)

# МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНЮВАННЯ ЯКОСТІ ПОЛІГРАФІЧНОЇ ПРОДУКЦІЇ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Виготовлення сучасної поліграфічної продукції спеціального призначення (далі – ППСП) захищеної від підроблення є не тільки складним, але й дорогим процесом. Відповідно при виборі прийнятної схеми захисту документу важливим є вирішення задачі достатності системи захисту від підроблення при мінімізації витрат на такий захист. Вирішення такої задачі пов'язане із отриманням об'єктивного оцінювання системи захисту поліграфічної продукції. Об'єктивність та комплексність такої оцінки безпосередньо впливає на ефективність обраної схеми захисту та матеріальні витрати на виготовлення відповідної ППСП. Втім на даний час відсутній методичний апарат оцінки якості зразків ППСП, що розробляються. Розробка методичних підходів щодо оцінки якості захисту зразків поліграфічної продукції спеціального призначення є. актуальною, обґрунтування методу аналізу ієрархій в якості одного із таких можливих підходів наведено в даній доповіді. Як відомо, система захисту документу є багатоступеневою та використовує різноманітні методи, оцінювання відтворення яких потребує не тільки кількісних, але й якісних характеристик. Для вирішення даної задачі можливе використання різних підходів, найбільш відомими з яких є метод узагальненого кількісного (бального) оцінювання, таксономічні методи та метод аналізу ієрархій (МАІ) [1]. В результаті порівняльного аналізу даних методів зроблено висновок про те що для вирішення задачі оцінювання якості відтворених зразків ППСП найбільш доцільним є використання методу аналізу ієрархій. Суть вирішення задачі оцінки системи захисту зразків ППСП за допомогою МАІ, полягає у наступному:

1. Усвідомлюється мета дослідження, тобто оцінювання завдань, що будуть використовуватися з використанням оцінюваних зразків ППСП. Саме виходячи з цих завдань уточнюється ієрархія показників та визначається їх пріоритетність.

2. Проводиться ієрархічна декомпозиція показників системи захисту ППСП.

3. Складаються матриці попарних порівнянь відносної важливості показників другого рівня стосовно загальної мети (першого рівня), показників на третьому рівні – стосовно показників другого рівня, показників четвертого рівня – стосовно показників третього рівня і так далі по дереву ієрархії показників.Попарні порівняння проводяться в термінах домінування одного з елементів над іншим. Для оцінки показників якості, використовується стандартна 9-бальна шкала [2]. В результаті попарних порівнянь отримаємо матриці приорітетів $\|a_{ij}\|$ для кожного елементу вищого рівня, де $a_{ij}$ визначається як відношення чисельних значень важливостей i-го та j-го показників: $a_{ij} = W_i / W_j$ .

4. Після проведення всіх попарних порівнянь, проводиться обчислення узгодженості матриць суджень. Для цього необхідно для кожної матриці обчислити власний вектор $\overline{X}$ , а потім нормалізувати результат, одержуючи тим самим вектор пріоритетів локальних пріоритетів $\overline{P}$ .

$$P_i = X_i \Big/ \sum_i X_i \,, i = \overline{1,n} \,; \sum_i P_i = 1 \,, \quad (1)$$

$$X_i = \sqrt[n]{\prod_{j=1}^{n} a_{ij}} \,, j = \overline{1,n}, \; i = \overline{1,n} \,, \quad (2)$$

Після чого визначається сума суджень (елементів) кожного стовпця матриці парних порівнянь

$$r_j = \sum_i a_{ij}\ ,\ j = \overline{1,n}\ ,\ i = \overline{1,n}\ ;$$

(3)

та розраховується індекс узгодженості (ІУ) за виразом

$$IУ\ = \frac{\lambda_{\max} - n}{n-1},\ n\rangle 1,$$

(4)

де, $\lambda_{\max} = \sum_j r_j P_j,\ j = \overline{1,n}\ \backslash$

Індекс узгодженості подає інформацію про ступінь порушення узгодженості значень пріоритетів визначених у матриці попарних порівнянь. Результатом розподілу індексу узгодженості на число, що відповідає випадковій узгодженості матриці того ж порядку, є відношення узгодженості (ВУ). Середні значення випадкової узгодженості для матриць різного порядку наведені в таблиці 1.

*Таблиця 1*

| Розмір матриці | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Випадкова узгодженість | 0 | 0 | 0,58 | 0,90 | 1,12 | 1,24 | 1,32 | 1,41 | 1,45 | 1,49 |

Зазвичай, величина ВУ не повинна перевищувати 0,1 [3]. При виході відношення узгодженості з цих меж необхідно дослідити правильність постановки задачі та перевірити судження експертів.

5. Етапи 3,4 повторюються для всіх рівнів та груп ієрархії показників.

6. Відповідно до процедури ієрархічного синтезу [2,3] проводиться зважування власних векторів пріоритетів вагами критеріїв. Тобто, для кожної з оцінюваних альтернатив, локальні пріоритети перемножуються на пріоритет відповідного критерію на вищому рівні і підсумовуються за кожним елементом відповідно до критеріїв, на які впливає цей елемент. Таким чином формується складений, або глобальний, пріоритет $\overline{S}$ цього елемента, що потім використовується для зважування локальних пріоритетів, розташованих рівнем нижче і порівнюваних стосовно нього як до критерію. Процес отримання глобального вектору пріоритетів $\overline{S}$ можна описати виразом

$$S_i = \sum_{j=1}^{k} P_{ij} V_j$$

(5)

де $P_{ij}$ – локальні пріоритети, $V_j$ – ваги відповідних критеріїв. Процедура продовжується до самого нижнього рівня.

7. Перевіряється узгодженість усієї ієрархії. Індекс узгодженості кожної матриці нижнього рівня множиться на пріоритет відповідного показника (характеристики) наступного (більш високого) рівня ієрархії, за яким ця матриця складена. Отримані числа підсумовуються. Результат ділиться на вираз такого ж типу, але з випадковими ІУ, які відповідають розмірам кожної виваженої пріоритетами матриці. Отримане значення відносної узгодженості усієї ієрархії вважається прийнятним, якщо воно не перевищує 0,1. Якщо ця вимога не виконується, необхідно поліпшити якість суджень експертів, або переглянути структурування задачі.

8. В результаті виконання описаної послідовності дій буде отримано вектор пріоритетів $\overline{S}$ вищого рівня, який відображатиме відносну порівняльну оцінку запропонованих систем захисту ППСП. Таким чином, запропонований методичний підхід до вирішення задачі оцінки систем захисту ППСП дозволяє розробити методики оцінки системи захисту зразків

поліграфічної продукції спеціального призначення, що потребують захисту від підроблення. Розробка та впровадження таких методик дозволить робити обґрунтовані оцінки систем захисту ППСП, підвищити особисту відповідальність відповідних посадових осіб, уникнути недостатнього рівня захищеності ППСП або необґрунтованих витрат на зайві елементи захисту.

к.т.н. Могилевич Д.І. (ВІТІ НТУУ „КПІ”)
к.т.н. Правило В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)

# СТАН ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ БЕЗДРОТОВИХ ТЕХНОЛОГІЙ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Удосконалення технологій бездротового доступу і розширення сфери їх застосування є одним з найбільш перспективних напрямків розвитку галузі телекомунікацій в Україні та у світі. Сучасні технології бездротового доступу до інформаційних та комунікаційних послуг дозволяють оперативно обмінюватися інформацією в локальних, міських, корпоративних та глобальних мережах (в тому числі в Інтернеті), забезпечуючи при цьому не лише свободу пересування користувачів (номадизм або мобільність), а й вирішення проблеми „останньої милі” у випадку неможливості або недоцільності побудови кабельної системи мереж абонентського доступу.

За радіусом дії й призначенню сучасні бездротові мережі можна розділити на персональні (*Wireless Personal Area Network, WPAN*), локальні *(Wireless Local Area Network, WLAN*), міські (*Wireless Metropolitan Area Network, WMAN*) і глобальні (*Wireless Wide Area Network, WWAN*) [4].

У зв’язку із збільшенням мобільних користувачів, виникає гостра необхідність в оперативному здійсненні комунікацій між ними, в обміні даними, у швидкому отриманні інформації, тому виникає інтенсивний розвиток бездротових технологій. Особливо це актуально у відношенні бездротових мереж, або так званих *WLAN*-мереж. (*Wireless Local Area Network*).

В основі *WLAN*-технологій лежить принцип високочастотного радіозв’язку між вузлами мережі. Інститутом інженерів з електротехніки та електроніки (*Institute of Electrical and Electronics Engineers*) було розроблено групу стандартів 802.11 для бездротових локальних обчислювальних мереж (*WLAN – Wireless Local Area Network*). Ці специфікації визначають засоби радіозв’язку безпроводового клієнта з базовою станцією (або точкою доступу) або між двома і більше бездротовими клієнтами. Найбільше поширення отримали бездротові мережі стандарту *IEEE* 802.11*b*, *IEEE* 802.11*g* та *IEEE* 802.11*a* [1].

Технології *WLAN,* що базуються на сімействі стандартів 802.11, часто позначають терміном *Wi-Fi*. Даний термін був уведений організацією *Wi-Fi Alliance*, для позначення продуктів серії стандарту 802.11*b*, однак сьогодні цей термін застосуються для продуктів, що відповідають будь-якому стандарту із сімейства 802.11. Багато організацій і домашніх користувачів використовують *Wi-Fi* як альтернативу провідним локальним мережам. Крім бездротових домашніх й офісних мереж технологія *Wi-Fi* знайшла широке застосування в сфері організації публічного доступу в Інтернет.

Залежно від конкретного стандарту, мережі *Wi-Fi* працюють на частотах 2,4 або 5 ГГц і забезпечують швидкість передачі даних до 54 Мбіт/с. Зону бездротового доступу на базі декількох хот-спотів називають хот-зоною.

Радикальне збільшення пропускної здатності дає стандарт 802.11*n*, з появою якого пропускна здатність *WLAN* збільшується відразу в кілька разів. Фахівці сходяться в думці, що найближчим часом технологію бездротових мереж 802.11*n* стануть підтримувати не тільки ноутбуки, але й багато побутових електронних приладів і вона буде використатися всіма основними корпоративними й домашніми додатками. Як перспективу розвитку бездротових локальних і персональних мереж фахівці називають пристрої *Cognitive Radios*, які здатні працювати в різних діапазонах по різних протоколах, а також можуть визначати, у якому географічному районі вони перебувають й як там можна працювати, підбудовуючись під місцеві вимоги.

Основою технологій бездротового доступу масштабу міста (*WMAN*) є сімейство стандартів *IEEE* 802.16 [2] (*WiMAX*) и 802.20 (*Mobile Fi*). Найбільш активно розробкою

стандартів *IEEE* серії 802.16 займається *WiMAX Forum* (*Worldwide Interoperability for Microwave Access*) – некомерційна організація, утворена за ініціативою *Intel* і за участю провідних розробників, виробників обладнання та провайдерів послуг. Оскільки дані технології використовуються як стандарти бездротового широкополосного доступу (*Broadband Wireless Access, BWA*), то технологію *WiMAX* також позначають як *BWA* 802.16, а стандарт 802.20 (*Mobile Fi*) – як *BWA-m* (802.20) [5].

*WiMAX* є альтернативою прокладці кабелю або лінії *DSL* при організації останньої милі. Теоретично технологія стандарту 802.16 повинна забезпечувати покриття сигналом площі радіусом до 50 км без прямої видимості. Пропускна здатність *WiMAX* по стандарту становить близько 70 Мбіт/с.

Безумовно, *WiMAX* – нова перспективна ступінь розвитку бездротових технологій, яка гарантує простоту широкосмугового підключення і універсальність використання. *WiMAX* є вигідною альтернативою технологіям *DSL*, достатньо привабливою для провайдерів завдяки можливості відносно простого, оперативного та гнучкого збільшення ємності мереж [3].

Основними проблемами розвитку *WiMAX* в глобальному масштабі є регіональні обмеження робочих діапазонів частот, складна і довготривала процедура сертифікації обладнання *WiMAX*, початкова орієнтація технології лише на мережі фіксованого абонентського доступу. В Україні першим мережі *WiMAX* почало будувати ООО „Українські найновіші технології” (торгова марка „Альтернет”), з березня 2006 року були сертифіковані та здані в комерційну експлуатацію перші базові станції в Києві та Харкові.

Основний напрямок розвитку технології – створення на основі *WiMAX* мереж мобільного доступу національних та глобального масштабів (стандарт *IEEE* 802.20), які в майбутньому створять серйозну конкуренцію „звичайним” стільниковим мережам.

З огляду на вищезазначене можна зазначити – бездротові технології є найбільш перспективним вектором розвитку мереж абонентського доступу. Основними напрямками розвитку цього класу технологій є підвищення швидкостей передавання інформації, рівня безпеки та конфіденційності інформаційного обміну, мобільності користувачів та розширення переліку інформаційно-комунікаційних послуг. Найбільш перспективними технологіями бездротових інформаційно-комунікаційних мереж, розробка яких бурхливо продовжується, запишаються наступні групи технологій:

– серед локальних – стандартів *IEEE* 802.11*g* та 802.11*n*;

– серед міських та глобальних – стандартів *IEEE* 802.16, 802.20.

Стосовно телекомунікаційних мереж військового призначення треба відмітити, що застосування технологій бездротового доступу надасть можливість розвитку мультисервісних мереж, які мають високі швидкісні характеристики. Дані технології можуть бути цілком застосовані як в мобільній так і в стаціонарній компонентах телекомунікаційних мереж військового призначення. При цьому, для абонентів мобільної компоненти ТКМ, найбільш доцільним та перспективним є застосування технологій *WLAN* та *WiFi*. Стосовно стаціонарної компоненти ТКМ, а для її найшвидшої побудови та надійної експлуатації можливе застосування бездротової технології *WiMAX*.

ЛІТЕРАТУРА

1. *IEEE* 802.11: http://grjuper.ieee.org/groups/802/11/index/html.

2. *IEEE* 802.16: http://grjuper.ieee.org/groups/802/16/index/html.

3. *Л. Бараш. WiMAX* как технология универсального широкополосного беспроводного доступа // Компьютерное обозрение, № 44, 2005.

4. *Л. Бараш*. Беспроводные сети – новая шляпа IT-индустрии // Компьютерное обозрение, № 43, 2003. – С. 26 – 29.

5. *А. Прохоров*. Рынок беспроводных сетей в цифрах и фактах. – http://www.compress.ru, 2006.

Назаревич В.В. (ВІТІ НТУУ „КПІ”)

# МАТЕМАТИЧНА МОДЕЛЬ ДЛЯ УПРАВЛІННЯ ТЕРИТОРІАЛЬНО РОЗПОДІЛЕНИМИ ПІДРОЗДІЛАМИ НА ОСНОВІ ГЕОІНФОРМАЦІЙНИХ СИСТЕМ

Досвід минулих війн і аналіз умов підготовки і ведення боїв з погляду на майбутнє переконливо показує, що бойові дії військ і сил можуть бути ефективними лише при наявності чіткої системи управління військами, відповідності можливостей їх боєздатності бойовим і маневреним можливостям підпорядкованих військ і умова, у яких вони діють.

Актуальність теми дослідження визначається потребами широкого круга фахівців в знаннях про математичну основу управління підрозділами, пошуку нового та, в подальшому, єдиного математичного апарата, який дозволить автоматизувати процес управління та полегшити роботу командира.

За оцінками фахівців, застосування ГІС дозволить підвищити ефективність управління військами та зброєю на 40 і більше відсотків. Тому вже сьогодні вони стали не тільки засобом, але і об’єктом протиборства поряд з іншими інформаційними системами. Ціль цього протиборства – забезпечення інформаційної переваги над супротивником.

Метою дослідження є пошук технології побудови системи управління територіально розподіленими підрозділами за допомогою системи зв’язку та геоінформаційних технологій, розробка математичної моделі системи управління територіально розподіленими підрозділами, автоматизація процесу управління на основі запропонованих методів та технологій.

Для досягнення поставленої мети потрібно вирішити такі задачі:

1. На базі існуючого програмного забезпечення розробити нову структуру програмного забезпечення геоінформаційних комплексів реального часу, що дозволяє більш адекватно відображати динамічну обстановку і здійснювати її аналіз у реальному часі, скоротивши при цьому час реакції комплексу порівняно з відомими методами;
2. Розробити математичну модель для управління територіально розподіленими підрозділами;
3. На базі існуючих технологій розробити програмний продукт для управління територіально розподіленими підрозділами.

Під час функціонування системи всі пункти управління та зв’язки між ними будуть створювати зв’язний граф, в якому пункти управління будуть входити в множину вершин, а зв’язки – ребер. Кожному каналу зв’язку буде надаватись відповідна вага, значення якої може обчислюватись окремо для кожної ситуації, в залежності від поставленого завдання. За допомогою алгоритму задачі знаходження мінімального шляху на графі шукається найбільш оптимальний маршрут передачі сигналу (повідомлення) між двома будь-якими станціями системи.

В результаті роботи була запропонована методика побудови системи зв’язку у вигляді графа та розроблений математичний апарат пошуку оптимального шляху між двома об’єктами, який значно автоматизує створення моделей для динамічного відображення стану зв’язку та аналізу існуючих зв’язків в реальному часі, що значно підвищує ефективність управління підрозділами. На основі розглянутих технологій був створений програмний продукт, який включає в себе зазначену методику та математичний апарат.

ЛІТЕРАТУРА

1. *Майкл Н. ДеМерс.* Географические информационные системы. Основы. // Пер. с англ. М: Дата+ , 1999. С. 240.

2. *Казанцев Н.Н., Флейс М.Э., Яровых В.Б.* Использование разнородных пространственных данных в геоинформационных системах // Гис-обозрение, 1994, осень. С. 22 – 24.

Настич Ю.Б. (ВІКНУ)
Бугера М.Г. (ВІТІ НТУУ „КПІ”)

# РОЗРОБКА АЛГОРИТМУ ШИФРУВАННЯ ІНФОРМАЦІЇ „APR” КОМБІНОВАНИМ МЕТОДОМ НА ОСНОВІ ЗАЛИШКОВИХ ЧИСЕЛ

Сучасне суспільство все більшою мірою стає інформаційно-залежним, успіх будь-якого виду діяльності все сильніше залежить від володіння певними відомостями і від відсутності їх у конкурентів. І чим сильніше проявляється вказаний ефект, тим більші потенційні збитки від зловживань в інформаційній сфері, і тим більша потреба в захисті інформації.

Провівши аналіз способів та методів захисту інформації [1 – 3], був зроблений висновок, що серед усього спектра методів захисту особливе місце займають криптографічні методи. На відміну від інших методів, вони спираються лише на властивості самої інформації і не використовують властивості її матеріальних носіїв, особливості вузлів її обробки, передачі і зберігання. Образно кажучи, криптографічні методи будують бар’єр між інформацією, що захищається, і реальним або потенційним зловмисником з самої інформації.

Після детального аналізу існуючих алгоритмів криптографічного захисту інформації, особливу увагу приділивши тим, що стоять на озброєнні провідних країн світу [1, 4 – 5], можливо стверджувати, що завдання надійного захисту інформації, конфіденційності даних від несанкціонованого доступу, яке особливого значення набуває при переміщенні даних і є одним з найстаріших на сьогодні, до кінця не розв’язане і в найближчій перспективі потребує детального дослідження та вдосконалення.

Для вирішення поставленого завдання проводиться дослідження вимог [1], що висуваються до криптографічної системи захисту інформації та на основі поставлених вимог розробляється новий алгоритм шифрування інформації, що має назву: „APR” – (algorithm of partaking with a remain) алгоритм ділення із залишком, в рамках якого:

досліджуються властивості простих чисел і залишки, що утворюються від ділення на них цілих чисел;

знаходиться ряд простих чисел при діленні на які, отримувались би повторювальні залишки з періодом на одиницю меншим від самого простого числа;

розглядається порядок перетворення, на наглядному прикладі, символьних даних з одного з самих розповсюджених кодувань в кодування APR;

описується порядок утворення ключів та підбір вже існуючих алгоритмів для їх пересилання;

розробляються табличні дані по переведенню символьних значень з розповсюджених кодувань в шифрування.

ЛІТЕРАТУРА

1. *Ленков С. В., Перегудов Д.А., Дорошко В.А.* Методы и средства защиты информации. В 2-х томах. – К.: Арий, 2008. – 344 с.

2. *Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н.* Криптографическая защита информации: учебное пособие. – Т.: ТГТУ, 2006. – 140 с.

3. *Дж. Л. Месси.* Введение в современную криптографію. ТИИЭР. – 1988. – т. 75. – № 5. – С. 24 – 42.

4. *У. Диффи.* Первые десять лет криптографии с открытым ключом // ТИИЭР. – 1988. – т. 75. – № 5. – С. 54 – 74.

5. *Лебедев А. Н.* Криптография с открытим ключом и возможности её практического применения. „Защита информации”. – 1992. – Вып. 2. – С. 129 – 147.

к.т.н Наталенко П.П. (ІССЗІ НТУУ „КПІ”)
к.т.н. Шелепенко Ю.В. (ВІТІ НТУУ „КПІ”)

# ПЕРСПЕКТИВИ І НАПРЯМИ РОЗВИТКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Впровадження обчислювальних машин в процеси управління обумовило нові підходи до розвитку телекомунікацій і надаваємих ними сервісних послуг. Очевидним стала інтеграція всіх видів зв’язку засобами мереж передачі даних, що в свою чергу обумовило їх розвиток з точки зору забезпечення вимог по якості різних видів зв`язку.

В доповіді розкрито сучасний стан розвитку телекомунікаційних та ін – формаційних технологій, вказано шляхи поетапного їх впровадження в силових структурах країни. Показана, велика перспектива впровадження технології Internet (стек протоколів TCP/IP) в побудову корпоративних мереж.

Крім того, розкрито стан і напрями подальшого розвитку систем: електронної пошти, електронного документообігу, автоматизованого діловодства. Велика увага приділена розкриттю методологічних основ розробки, збереження і транспортування даних у відповідності до вимог заданої якості.

Особлива увага приділена напрямам забезпечення безпеки в інформаційно-телекомунікаційних системах [1]. Показано, яким чином можна скористатися стандартними програмами і апаратними засобами захисту інформації та напрями розвитку корпоративних засобів захисту у відповідності до корпоративних вимог.

На базі навчального процесу інститутів набрані статистичні дані підготовки спеціалістів та магістрів за напрямом експлуатації апаратних засобів, спеціалізованих та прикладних програм комплексів та засобів автоматизації управління військами та озброєнням.

Достатня увага приділена питанням застосування і створення пошагових довідкових і адміністративних служб. Це вказує на перегляд системи підготовки випускників інституту. Наведені основні вимоги і специфічні особливості підготовки кваліфікаційних спеціалістів по експлуатації автоматизованих систем управління.

Приведені рекомендації по удосконаленню навчального плану підготовки спеціалістів для корпоративних автоматизованих систем управління.

ЛІТЕРАТУРА

1. *Науменко М.І., Стасев Ю.В., Рубан І.В.* „Технології комп’ютерних мереж в АСУ військами” . Харків. МОУ, 2004. – 458 с.

Науменко Ю.Б. (ВІТІ НТУУ „КПІ”)

# РОЗШИРЕНА МОДЕЛЬ ЗАХИСТУ КРИТИЧНИХ СИСТЕМ УПРАВЛІННЯ НА ТРЬОХ РІВНЯХ ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ

Критичні системи управління (КСУ) за визначенням відносяться до класу складних інформаційних систем з управлінням. У КСУ доводиться вирішувати як проблему забезпечення інформаційної безпеки системи, так і завдання забезпечення безпеки інформації на рівнях інформаційної архітектури системи і засобів інформаційних технологій.

Забезпечення інформаційної безпеки в КСУ має значні відмінності від забезпечення інформаційної безпеки в інших класах систем. Ці особливості полягають в жорсткіших вимогах, що пред’являються до безпеки і гарантій захищеності інформації.

Стабільність системи визначається рівнем внутрішніх і зовнішніх дестабілізуючих дій, початковим станом системи і її можливостями по адаптації.

Суттю будь-якої системи управління (підсистеми управління) є обов’язковий набір фізичних і абстрактних інформаційних об’єктів, що мають інформаційно-функціональне значення для реалізації управління.

Матеріальний або абстрактний об’єкт можна представити у вигляді інформаційної моделі об’єкта, що описує на якій-небудь мові його суть, важливу для системи, компонентом якої він є.

Процес управління полягає в зміні семантики моделей об’єктів управління відповідно до семантики функціональних алгоритмів, що використовують для цього семантику алгоритмів обробкою даних. Мають місце ієрархічні стосунки між семантиками. Семантики об’єктів управління і алгоритмів визначені на безлічі мов і безлічі інформаційних об’єктів системи.

Ієрархічні стосунки між інформаційною суттю визначають ієрархічну структуру моделі інформаційної взаємодії складних систем.

Аналіз узагальненої моделі функціональної структури системи з управлінням і моделі інформаційної взаємодії складних систем дозволяє сформулювати фундаментальні принципи інформаційної взаємодії складних кібернетичних систем.

Принципи розділені на ієрархічні категорії, кожна з яких складає рівень взаємодії. Виконання у взаємодіючих системах принципів одного рівня (одній категорії) надає можливості (послуги) для взаємодії на вищестоящому рівні.

Фізичні принципи, що визначають мінімально необхідні вимоги до фізичного рівня організації взаємодіючих інформаційних систем.

Синтаксичний принцип визначає необхідність використання однакових алфавіту, лексики і синтаксису мови для опису семантики даних, передаються і взаємодіючих алгоритмів систем.

Семантичні принципи, що визначають мінімально необхідні вимоги до рівня семантичної (функціональною) організації систем.

Із загальних принципів інформаційної взаємодії складних систем, витікають теоретично можливі загрози безпеці інформації, моделі інформаційної дії на систему і моделі захисту.

Незалежно від технології обробки інформації доступність інформаційних об’єктів (тобто суб’єктів і об’єктів доступу) є результатом взаємодії носіїв інформації на фізичному рівні, мовному опису (уявлення) інформації на синтаксичному рівні і значень на семантичному рівні. Отже, можна побудувати систему захисту інформації, яка реалізує стратегію розмежування доступу, засновану на розширеній моделі захисту з повним перекриттям, і з використанням механізмів захисту на одному або декількох рівнях інформаційної взаємодії складних систем, що дозволить врахувати більшу кількість чинників, що впливають на безпеку інформації, описувати і оцінювати будь-які інформаційні технології і механізми захисту з єдиних позицій і за єдиними критеріями.

к.т.н. Недайбіда Ю.П. (ВІТІ НТУУ „КПІ”)
Ляшенко В.Г. (ВІТІ НТУУ „КПІ”)
Ромащенко В. М. (ВІТІ НТУУ„КПІ”)
Шугалій О.О. (ВІТІ НТУУ „КПІ”)

# МОДЕЛЬ КОНТРОЛЮ ЗАВАНТАЖЕННЯ АСУ В РЕАЛЬНОМУ ЧАСІ ФУНКЦІОНУВАННЯ СИСТЕМ УПРАВЛІННЯ ТАКТИЧНОЇ ЛАНКИ ЗСУ

Найбільш важливими характеристиками, що впливають на вибір технічних рішень при створенні і аналізі АСУ військового призначення [1], є реактивність і пропускна здатність системи управління. Під реактивністю системи розуміється час, який затрачується системою на доведення інформації про стан процесу управління до об’єктів (пунктів) управління, обробку цієї інформації, прийняття рішення і доведення прийнятого рішення до виконуючих органів, а пропускна здатність – сумарний об’єм обчислювальних робіт в одиницю часу, спрямованих на досягнення кінцевої мети системи управління.

Система управління тактичної ланки належить до систем управління жорстко регламентованого режиму реального часу з високою реактивністю на вхідний потік інформації. В таких системах час доведення інформації про стан процесу, що управляється, до пунктів управління становить одиниці секунд, час на обробку зовнішньої інформації, включаючи очікування початку обробки, становить долі секунд, час на прийняття рішень – одиниці секунд, а час доведення прийнятого рішення до виконавчих органів становить десяті долі секунд. В таких системах реальний час є найважливішим параметром, від якого суттєво залежить якість управління і повинен фіксуватися з належною точністю.

В системах такого типу повинні бути організовані служби реального та єдиного часу, які мають регламентувати виконання функціональних задач, в тому числі:

відлік інтервалів часу з необхідною точністю при вирішенні функціональних задач;

відлік астрономічного часу;

організацію періодичних обчислювань;

корегування часової інформації для зміни інтервалів і початку відліку та ін.

Для АСУ тактичної ланки важливо передбачити підсистему організації відновлення і реконфігурації управління при порушеннях ходу обчислювального процесу, несправностях апаратури, відхилення параметрів системи від заданих границь, зміні зовнішнього середовища, виходу з строю елементів системи, трактів передачі даних, зміні характеристик об’єктів управління, зміні загрузки системи, появі перешкод та ін. Ця підсистема на основі даних контролю працездатності пристроїв і підсистем повинна забезпечити переключення на резервне устаткування без перерву обчислювального процесу і управління системи.

Відзначимо, що вирішення зазначених задач процесу управління повинне виконуватись в умовах агресивності зовнішнього середовища, тобто при суттєвій завантаженості АСУ, що приводить до виникнення проблем дотримання граничних значень циклу управління і зниження пропускної здатності системи.

Звично стосовно конкретних АСУ або сукупності АСУ однакового функціонального призначення пропускну здатність стараються вимірювати в категоріях, які відображають реальний фізичний смисл функцій, які виконуються і призначення АСУ. Однак, для зрівняльної оцінки пропускної здатності різних АСУ зазначені категорії частіше за все не є зіставними. В загальному випадку характеристика (одиниця виміру) пропускної здатності АСУ повинна відображати зазначені категорії і в той же час не залежати від призначення і складу конкретної АСУ.

В роботі запропоновано варіант визначення загрузки АСУ в реальному часі на основі представлення моделі процесу управління, як системи масового обслуговування в умовах загальних перевантажень системи.

**Постановка задачі.** Нехай вхідний потік заявок відіграє роль потоку пакетів, що надходять на вхід системи. Будемо вважати, що комутатор водночас вирішує задачу перерозподілу заявок на комутацію пакетів за вихідними маршрутами (рис. 1) (виконує пристрій Пр) і ставить їх в черги ($Ч_i$) за своїми типами ($z_i$).

Задача полягає у обчисленні середнього часу затримки в системі заявок кожного типу в залежності від сумарної загрузки системи.

Нехай відомі математичні очікування $\theta_1, \theta_2, ..., \theta_M$ і другі початкові моменти $\vartheta_1^{(2)}$, $\vartheta_2^{(2)}$, ..., $\vartheta_M^{(2)}$ часу обслуговування заявок типу 1, 2, …, $M$ відповідно. Ці значення характеризують розподіл часу виконання відповідних програм.

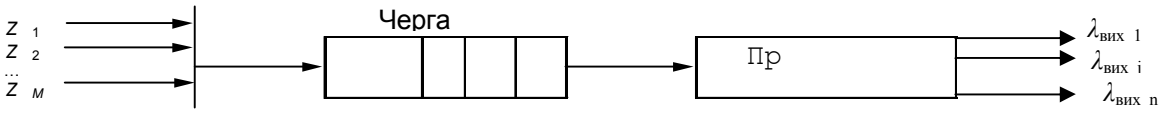



Рис. 1. Організація обслуговування на основі дисципліни *FIFO*

Будемо вважати, що заявки обслуговуються за дисципліною *FIFO*.

Для розглянутої дисципліни середній час чекання заявок у черзі однаковий для всіх типів і становить [2]:

$$\omega_c = \frac{\sum_i^M \rho_i \theta_i (1+\nu_i^2)}{2(1-R_c)},$$

де $R_c$ – середня сумарна завантаженість системи, $\nu_i$ – коефіцієнт варіації часу обслуговування заявки $i$ - го типу.

Із цього співвідношення видно, що середній час очікування пакетів у черзі найменший якщо $\nu_i = 0$, тобто за постійної тривалості обслуговування і збільшується в міру росту дисперсії часу обслуговування. Крім того, середній час перебування пакетів у комутаторі істотно збільшується зі зростанням завантаження пристрою і прагне до нескінченності при $R_c \to 1$.

Обговорені припущення про характер вхідного потоку заявок і їх обслуговування дозволяють одержати граничні значення затримок. Тобто, при невиконанні цих умов, реальні затримки інформації будуть ще більшими.

Неважко показати, що додаткові завантаження системи ($R_d$) створюють додаткові затримки заявок в чергах ($\omega_d$)

$$\omega_d = \frac{(T_\Sigma - T_c)(1-R_c) + T_c R_d}{(1-R_c)[1-(R_c+R_d)]}, \quad \text{і} \quad \frac{\partial \omega_d}{\partial R_d} = \frac{T_\Sigma}{[1-(R_c+R_d)]^2}.$$

Тут $T_c$, $T_\Sigma$ – константи при стаціонарному повному завантаженні системи.

**Висновки.**

1. З співвідношень слідує, що при великій загрузці системи ($R_c \to 1$) додаткова загрузка суттєво збільшує час затримки пакетів в чергах, і навіть невеликі коливання величини $R_d$ можуть привести до порушення циклу управління і зриву усього процесу управління.

2. Вимірюючи час затримки найменш пріоритетних заявок в чергах, можна контролювати рівень загрузки системи управління.

ЛІТЕРАТУРА

1. *Володин С. В., Макаров А. Н., Умрихин Ю. Д., Фараджаев В. А.* Общесистемное проектирование АСУ реального времени. – М.: Изд.- во „Радио и связь”, 1984. – 232 с.

2. *Майоров С.А., Новиков Г.И., Алиев Т.И. и др.* Основы теории вычислительных систем. – М.: Высш. шк., – 1978. – 408 с.

Носовськой Р.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Горбенко В.І. (ВІТІ НТУУ „КПІ”)

# СТРУКТУРА І СКЛАД АВТОМАТИЗОВАНОЇ НАВЧАЛЬНОЇ СИСТЕМИ МОВИ ПРОГРАМУВАННЯ АСЕМБЛЕРУ З ЕЛЕМЕНТАМИ ЗАХИСТУ ІНФОРМАЦІЇ

Аналіз програмного забезпечення автоматизованих систем управління військами Збройних Сил України (ЗСУ) показує, що мова програмування асемблеру використовується для реалізації критичних до часу виконання фрагментів алгоритмів, а також при спряженні спеціалізованих пристроїв автоматизованих систем [1]. При відлагодженні та запуску програм, написаних на мові програмування асемблеру виникають проблеми, які пов’язані з відсутністю інтегрованої оболонки для комплексної розробки, трансляції, компоновки і відлагодження програм, написаних на мові програмування асемблеру. Для вирішення цих проблем, покращення інтерфейсу користувача та підвищення ефективності навчання пропонується розробка автоматизованої навчальної системи мови програмування асемблеру з елементами захисту інформації (АНСАЕЗІ) [2].

Структура АНСАЕЗІ є багатокомпонентною і проектується шляхом декомпозиції за функціональними ознаками складної системи на підсистеми.

В результаті декомпозиції отримані наступні підсистеми:

– підсистема адміністрування;
– підсистема безпеки при авторизації користувачів;
– підсистема навчання [3];
– підсистема перевірки та контролю;
– підсистема звітування;
– підсистема реєстрації.

Сукупність підсистем АНСАЕЗІ вирішує наступні задачі:

– розмежування доступу користувачів до ресурсів АНСАЕЗІ;
– забезпечення тих, кого навчають за допомогою необхідної літератури та учбовими матеріалами (аудіо- та відео- даними) тощо;
– створення середовища для написання та відлагодження програм;
– забезпечення можливості дизасемблювання;
– перевірка знань тих, кого навчають шляхом тестування з елементами захисту;
– аналіз якості навчання за певними тематиками;
– відслідковування тенденцій професійного росту тих, кого навчають;
– отримання звітів за результатами роботи АНСАЕЗІ.

У доповіді розглядаються алгоритми функціонування підсистем при вирішенні перелічених задач, обґрунтовується вибір програмних засобів розробки інтегрованої оболонки, описуються механізм та елементи захисту інформації.

Таким чином, використання запропонованої АСАЕЗІ на етапах навчання та безпеки надає наступні можливості:

по-перше, дизасемблювання – перетворення машинного коду, об’єктного файла або бібліотечних модулів в тексти програм на мові асемблера;

по-друге, використання асемблеру при вирішенні задач захисту інформації [4].

ЛІТЕРАТУРА

1. *Юров В.И.* Справочник по языку Ассемблера IBM PC. – СПб.: Питер, 1998. – 32 с.
2. *Рудаков П.И., Финогенов К.Г.* Язык ассемблера: уроки программирования. – М.: ДИАЛОГ-МИФИ, 2001. – 380 с.
3. *Юров В.И.* Assembler. Учебник для вузов. – СПб.: Питер, 2003. – 163 с.
4. *Бурдаев О.В., Иванов М.А., Тетерин И.И.* Ассемблер в задачах защиты информации. – СПб.: Кудиц-Образ, 2004. – 150 с.

к.т.н. Овсянніков В.В. (ВІТІ НТУУ „КПІ”)
Паламарчук С.А. (ВІТІ НТУУ „КПІ”)
Паламарчук Н.А. (ВІТІ НТУУ „КПІ”)

# ВИМОГИ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ РУХОМИХ ЗАСОБІВ ЗВ’ЯЗКУ

До об’єктів інформаційної діяльності (стаціонарних або тих, що розміщуються в рухомих засобах зв’язку) Збройних Сил України на яких функціонують автоматизовані системи (АС) управління військами як в повсякденних так і в особливих умовах висувається ряд вимог пов’язаних з оперативністю прийняття рішення, прихованістю організації діяльності, достовірністю інформації на основі якої приймаються рішення, мобільності системи управління в цілому. Відповідно до вимог законодавства для забезпечення конфіденційності, доступності, цілісності та спостереженості інформації в кожній з таких АС повинна створюватися комплексна система захисту інформації (КСЗІ).

Створення КСЗІ регламентовано низкою нормативних документів системи технічного захисту інформації (в залежності від виду інформації – мовна, або така, що обробляється в АС). Як правило, КСЗІ складається з організаційних і інженерних заходів, технічних засобів захисту, які спрямовані на захист інформації за двома напрямами: це захист від витоку інформації з обмеженим доступом (ІзОД) технічними каналами – створюється комплекс технічного захисту інформації; захист інформації від несанкціонованого доступу (НСД) – відповідно комплекс засобів захисту (КЗЗ) від НСД. Також визначена обов’язкова послідовність робіт щодо створення КСЗІ в АС.

Відповідно, оброблення ІзОД на ОІД дозволяється лише після завершення робіт зі створення КСЗІ, проведення випробувань та оцінки рівня захищеності інформації на відповідність вимогам нормативних документів системи ТЗІ.

Виконання цих заходів є неможливим для рухомих засобів зв’язку через: відсутність постійної огороджувальної конструкції ОІД; необхідність зміни позицій та ін.

Перелічені питання щодо створення КСЗІ, повинні бути закладені на етапі проектування рухомого засобу зв’язку та відображені в технічному завданні (ТЗ) на його створення з послідуючою їх реалізацією у серійному виробі. Це дозволить значно спростити процедуру вводу та подальшої експлуатації АС.

При визначенні моделі загроз для рухомих засобів зв’язку основний акцент повинен спрямовуватися на захист від витоку інформації від випадкового прослуховування (акустичний канал витоку) та захист інформації від витоку каналами побічних електромагнітних випромінювань та наведень (ПЕМВН).

Зазначене висуває жорсткі вимоги до зразків, що проектуються:

при підключенні проводів та кабелів до кунгу рухомих засобів виникають ПЕМВН, тому контрольована зона біля рухомого засобу зв’язку повинна бути не менше 5 м;

з’єднання повинні здійснюватися за допомогою оптоволоконних ліній, з повною відмовою від використання мідних кабелів, що дасть змогу не порушувати екранування кунгу рухомого засобу зв’язку;

жорстко регламентуються процедури доступності користувача до інформаційних ресурсів системи; автентифікації користувачів системи, підтвердження отримання інформації; достовірність отриманої інформації та ін.

Таким чином, для рухомих засобів зв’язку, що розробляються ці вимоги повинні бути детально описані в ТЗ на створення засобу. Також в ТЗ повинні бути визначені профілі захищеності для кожної підсистеми засобу зв’язку. Для засобів, що вже прийняті на озброєння, але в котрих не реалізовані заходи з захисту інформації необхідно провести аналіз особливостей їх реалізації. За результатами аналізу або відмовитися від їхнього подальшого використання або здійснити доопрацювання (модернізацію) з метою реалізації в них КСЗІ.

Овчаров О.О. (ІСЗЗІ НТУУ„КПІ”)

# МЕТОД ТУРБО КОДУВАННЯ З ПОВТОРЕННЯМ ДЛЯ ПІДВИЩЕННЯ ЗАВАДОЗАХИЩЕНОСТІ БАГАТОКАНАЛЬНОЇ ПРОГРАМОВАНОЇ РАДІОСТАНЦІЇ В УМОВАХ ВПЛИВУ НАВМИСНИХ ЗАВАД

Аналіз сучасного стану військових систем радіозв’язку провідних країн світу показує, що ці системи побудовані за класичною трьохрівневою схемою з використанням реконфігурованих принципів на основі систем стандартів 802.11, 802.16, *HSDPA*, *HSUPA*, 1*xEVDO-Rev B*, систем тактичного радіозв’язку з використанням програмованих радіостанцій *SDR* (*software defined radio*).

Програмовані радіостанції розробляються по програмі *JTRS* (*Joint Tactical Radio System*). В цих мережах на фізичному рівні в якості модуляції сигналу застосовуються спектрально-ефективні, а в якості коригувальних кодів – турбо коди (ТК). Одним з режимів роботи цієї мережі є режим протидії навмисним завадам. При цьому для протидії використовується розширення спектру методом псевдовипадкової перестройки робочої частоти (ППРЧ) та корегувальні коди.

Відомо декілька підходів до підвищення завадозахищеності систем з ТК, які полягають в оптимізації перемежувача в структурі турбо коду, в застосуванні додаткових біт по завершенню кодування блоку даних з метою примусового переведення решітчастої діаграми рекурсивного систематичного згорточного коду ТК у початковий стан, та врахування інформації про стан каналу зв'язку при декодуванні ТК.

Крім того, підвищити завадозахищеність програмованої радіостанції (ПРС) можна шляхом багатократної передачі (3...5 разів) однієї і тієї ж інформації по одному каналу зв’язку або шляхом використання декількох каналів зв’язку (3...5 каналів), що фізично рознесені, якими передається одна і та ж сама інформація.

В системах радіозв’язку з ТК принцип повторення кодованих блоків і наступного їх декодування не був досі розглянутий. Тому в роботі запропоновано метод турбо кодування з повторенням для підвищення завадозахищеності багатоканальної програмованої радіостанції в умовах впливу навмисних завад, який ґрунтується на основі нових аналітичних залежностей для алгоритмів декодування турбо кодів з повторенням.

Результати моделювання характеристик завадозахищеності ПРС з багатоканальною передачею інформації та турбо кодом з повторенням показали, що використання запропонованого методу дозволяє одержати енергетичний виграш в характеристиках завадозахищеності не збільшуючи при цьому надлишковість інформації.

Відмінність розробленого методу від існуючих, що визначає його новизну, полягає в застосуванні в якості корегувального коду з повторенням турбо коду, в введенні допоміжної процедури розрахунку сумарної вихідної логарифмічної функції правдоподібності про передані біти для турбо кодів з повторенням та в урахуванні характеристик завад в алгоритмах декодування турбо кодів з повторенням.

Ефект від впровадження полягає в підвищенні завадозахищеності ПРС з ППРЧ та турбо кодуванням з повторенням. Наприклад, при впливі різних завад на ПРС із ППРЧ, використовуючи ТК з повторенням та двоканальну передачу можна отримати енергетичний виграш в характеристиках завадозахищеності до 14,5 дБ в порівнянні з використанням одноканальної ПРС та ТК без повторення.

Ольшанський В.В. (ВІТІ НТУУ „КПІ”)
Бортнік Л.Л. (ВІТІ НТУУ „КПІ”)

# ЗАДАЧА РОЗРОБКИ ВДОСКОНАЛЕНОГО МЕТОДУ ОЦІНКИ РАДІОКАНАЛУ

Останнім часом в системах радіозв’язку широко застосовується технологія *OFDM*. Задача оцінювання каналу зв’язку в *OFDM*-системах є особливо актуальною, тому що при наявності повної інформації про стан передаточної характеристики каналу можливо застосовувати такі адаптивні алгоритми, як розподіл потужності між піднесучими, вибір раціональних (оптимальних) сигнально-кодових конструкцій, відключення піднесучих із малими відношеннями сигнал-шум тощо та їх комбінації з метою максимізації пропускної спроможності, або мінімізації потужності випромінювання, або підвищення завадостійкості.

Відомі наступні методи оцінювання якості нестаціонарного каналу (прямі та непрямі):

зондування тестовими послідовностями;

використання пілот-тонів;

дослідження каналу через його вплив на характерні особливості робочого сигналу;

методи імовірнісного оцінювання.

Кожен із перелічених методів має свої переваги та недоліки. При розробці удосконаленого методу доцільно поєднати сильні сторони даних і максимально виключити слабкі сторони.

Виходячи з аналізу літератури, присвяченої проблемі оцінювання каналу *OFDM* можна зробити висновок, що для оптимального виконання вимог до оперативності та точності адаптації найбільш ефективним є поєднання методів прямого та непрямого оцінювання.

Очевидно, що чим точніше ми будемо оцінювати канал, тим більшу пропускну спроможність потрібно віддати для цього. Крім цього, за досягнення високої точності потрібно платити ще й складністю реалізації алгоритмів оцінювання. Тому виникає задача вирішення наступного компромісу:

якість оцінки каналу → max;

час оцінки → min;

пропускна спроможність системи → max;

складність реалізації → min.

У відповідності з алгоритмом комбінованого оцінювання якості радіоканалу в реальному часі вимірювання якості каналу за прямим методом відбувається при встановленні зв’язку, або в моменти передачі службової інформації, тобто коли по каналу не передається основна інформація. В ці моменти відбувається швидке та точне оцінювання якості каналу зв’язку за допомогою тестової преамбули.

В іншому випадку здійснюється перехід до обчислення поточної якості каналу за допомогою непрямого методу, що забезпечує неперервність оцінювання. При цьому точність сформованої оцінки значною мірою визначається ступенем усереднення результатів та вимагає достатньо тривалого часу оцінювання.

Якщо непрямий метод не забезпечує з необхідною швидкістю достатньої точності оцінювання, відбувається оцінювання з використанням пілотних піднесучих. Слід зазначити, що рівномірне розташування пілот-тонів в структурі *OFDM*-сигналу не є оптимальним. Тому, у випадку використання пілот-несучих доцільно здійснювати їх розташування у спектрі сигналу в залежності від останньої оціненої реалізації амплітудно-частотної характеристики каналу зв’язку (наприклад, на тих ділянках спектра, де рівень сигналу корельований сильніше, потрібно застосовувати менше пілот-несучих).

Розробка алгоритму комбінованого оцінювання каналу повинна включати наступні етапи: визначення та формулювання показника ефективності; розробка алгоритму, який максимізує (мінімізує) заданий показник – тобто розв’язання оптимізаційної задачі; оцінка ефективності розробленого алгоритму (методу).

Панченко А.Ю. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

# ВИБІР ЗАСОБІВ ВІЗУАЛІЗАЦІЇ МЕРЕЖЕВОГО ОТОЧЕННЯ ОБ’ЄКТА АТАКИ

З розвитком інформаційних технологій, для підвищення ефективності надання державних послуг, передбачається введення концепції електронного уряду, що зумовлює відкритість та доступність інформації для великих соціальних груп суспільства. Очевидним є наявність в інформаційно-телекомунікаційній інфраструктурі держави вузлів, з якими пов’язано функціонування загальнодоступних програм серверного типу, виведення з ладу яких здійснює безпосередній вплив на якість державного управління. Виходячи з цього, можна очікувати спроби порушення роботи інформаційно-телекомунікаційних систем у вигляді мережевих атак [1].

Інформаційна підготовка атаки передбачає виконання наступної послідовності дій:

– відслідковування адрес маршрутизаторів, через які проходить пакет від вузла зловмисника до вузлів об’єкта атаки, та отримання інформації про них;

– збирання та обробка інформації про структуру мережі;

– встановлення структури інформаційно-телекомунікаційної системи;

– логічний висновок щодо найбільш важливих цілей для мережевих атак.

Існують різні методи аналізу мережевого оточення. Але одним з найбільш важливих питань є коректна і зрозуміла візуалізація зібраної інформації для користувача. Інформацію про мережеве оточення мережі зручно подавати у вигляді зв’язаного графа, вершинами якого є вузли мережі, а ребрами – зв’язки між ними. Для вирішення даної проблеми було розроблено ряд спеціальних об’єктно-орієнтованих бібліотек для роботи з графами [2]. В даний момент найбільш відомими об’єктно-орієнтованими бібліотеками для роботи з графами є:

–*LEDA (Library of Efficient Data types and Algorithms)*;

–*GTL (Graph Template Library, University of Passau);*

–*AGraph*.

Бібліотека *LEDA* написана на мові *C++*, представляє різні абстрактні типи даних, спеціальні числові типи даних, графи та допоміжні структури даних для роботи з графами [3]. В *LEDA* реалізовані алгоритми рішення ряду комбінаторних, алгебраїчних, геометричних і теоретико-графових задач, засоби графічного введення і виведення. Бібліотека *GTL* підтримує декілька внутрішніх представлень для графів – у вигляді масивів вершин і ребер, матриці суміжності тощо. Представлення реалізовані у вигляді шаблонних класів; вибір потрібного представлення здійснюється при створенні графа. *GTL* використовує спосіб побудови графів, що заснований багаторазовим наслідуванням і параметричним (шаблонним) класів графів. Бібліотека *AGraph* написана на мові *Object Pascal*. Якщо порівнювати *AGraph* і *LEDA*, то можна відмітити дві суттєві відмінності: перша пов’язана з використанням динамічних масивів для внутрішнього представлення графів у бібліотеці *AGraph*, а друга – *AGraph* для видалення вершин і ребер графа використовує стандартний спосіб знищення об’єктів через метод free, а у *LEDA* знищення відбувається через спеціальні методи об’єктів. Результатом даного аналізу є обґрунтований вибір найбільш зручного і потужного програмного засобу візуалізації структури мережевого оточення об’єкта атаки.

ЛІТЕРАТУРА

1. *Касьянов В.Н., Евстигнеев В.А.* Графы в программировании: обработка, визуализация и применение. – СПб.: БХВ Петербург, 2003. – 504 с.

2. *Оре О.* Графы и их применения. – М.: Мир, 1965 – 260 с.

3. *Нечепуренко М.И., Попков В.К., Майнагашев С.М.* Алгоритмы и программы решения задач на графах и сетях. – Новосибирск: Наука, 1990. –253 с.

Панченко І.В. (НДВ НЦЗІ ВІТІ НТУУ „КПІ”)

# ДОСЛІДЖЕННЯ ФАЗЗІ-СИСТЕМ АВТОМАТИЧНОГО РЕГУЛЮВАННЯ ПОТУЖНОСТІ ПЕРЕДАВАЧА ПРИ „ГЛИБОКИХ” ЗАВМИРАННЯХ СИГНАЛУ В АДАПТИВНОМУ КАНАЛІ РАДІОЗВ'ЯЗКУ

Досліджені процеси у фаззі-системах автоматичного регулювання потужності передавача (АРПП) при дії на системи зовнішніх збудливих дій (завмирань) в середовищі розповсюдження радіохвиль в прямому і зворотному каналах радіозв’язку, які зменшують напругу на виході приймача в прямому каналі радіозв’язку на 98 % від нормального, прийнятого за одиницю.

Дослідження автоматичного регулювання потужності передавача (системи АРПП) з нечіткими регуляторами (фаззі-системи АРПП) і традиційними ПІД-регуляторами проводилися в інтерактивній системі MATLAB при дії на системи зовнішніх збудливих дій (завмирань) в середовищі розповсюдження радіохвиль в прямому і зворотному каналах радіозв’язку, які зменшують напругу на виході приймача в прямому каналі радіозв’язку на 40 % від нормального, прийнятого за одиницю. Регулювання потужності здійснюється за допомогою аттенюаторов, характеристики яких працюють на лінійній ділянці.

Система схильна до зовнішніх збудливих дій (завмирань), які зменшують напругу на виході приймача в прямому каналі радіозв’язку на 98 % від нормального, прийнятого за одиницю.

Імітація завмирань сигналу в середовищі розповсюдження радіохвиль каналу передачі даних (радіоканалу зв’язку) здійснюється наступному образом. Допустимо, що виникають ступінчасті періодичні завмирання сигналу на вході приймача каналу радіозв’язку на 98 % відмінні від нормального. Цю ситуацію можна імітувати генератором періодичних сигналів. При моделюванні період імпульсів вибраний 20 с, а тривалість імпульсів 10 с. Адитивні зовнішні дії (завмирання) у вигляді періодичної послідовності негативних імпульсів подаються на верхній вхід суматора. Періодичні завмирання сигналу на вході приймача каналу радіозв’язку можна імітувати також за допомогою генератора синусоїдальних коливань із зсувом. При моделюванні вибрані коливання з періодом 20 с, амплітудою, рівною 0,49, і зсувом -0,49. Завдання системи автоматичного регулювання потужності передавача АРПП звести помилку розузгодження що виникає під час вступу адитивних зовнішніх обурюючих дій (завмирань) до нуля.

Завмирання сигналу в середовищі розповсюдження радіохвиль каналу радіоуправління також можна імітувати, наприклад, за допомогою генератора синусоїдальних коливань із зсувом. При моделюванні вибрані коливання з періодом 4 с, амплітудою, рівною 0,49, і зсувом -0,49. Адитивні зовнішні дії (завмирання) в каналі радіоуправління у вигляді синусоїдальних коливань подаються на нижні входи суматорів і після відповідної обробки на виході суматора компенсуються.

У системі використовуються моделі аттенюаторів, що враховують реальні властивості аттенюатора: нелінійну статичну регулювальну характеристику і змінну інерційність.

У досліджуваній системі використовується новий тип регулятора, побудований на основі нового методу проектування нечітких регуляторів. Схема регулятора складається з трьох блоків: блоку формувача величин, блоку порівняння величин і розрахунку та блоку нормування вихідної змінної. Причому використовуваний регулятор має блок порівняння, який відрізняється простотою і, головне, може використовуватися з різними формувачами.

На вхід нечіткого регулятора поступають помилка системи. АЦП квантує безперервну помилку системи управління.

У формувачі величин обчислюється перша і друга різниця від помилки. По алгоритму Мамдані визначаються величини в кожен фіксований момент часу і ці величини поступають з виходу формувача на входи блоку порівняння.

Значення відкладаються відповідним чином на вихідні функції приналежності і в блоці порівняння величин і розрахунку проводиться розрахунок ненормованого виходу регулятора. На верхньому суматорі блоку порівняння величин і розрахунку формується чисельник виразу, на нижньому суматорі формується знаменник виразу.

Далі набуте значення в блоці нормування вихідної змінної перераховується у вихідну напругу регулятора. У блоці нормування вихідної змінної перебудовуються граничні значення діапазону.

Радіоланки які були досліджені є істотно нестаціонарними елементами системи і включають ланку чистого запізнювання. Модель радіоланки, яка може бути представлена передавальною функцією, описує загасання і запізнювання радіосигналу в ідеальному (без завад) середовищі розповсюдження і фільтрацію сигналу вихідним фільтром в приймачі. При моделюванні передавальні функції ланок описуються однією і тією ж формулою.

Нечіткий регулятор вимагає окремої настройки для ступінчастих вхідних дій (забезпечення швидкодії системи) і для довільних (еквівалентних синусоїдальних) вхідних дій (забезпечення точності системи, яка визначається мінімальною динамічною помилкою).

Розглянемо модель системи АРПП з нечітким регулятором нового типу в зворотному каналі радіоуправління, в якій аттенюатор в прямому каналі перебудовується безпосередньо сигналом управління. Дана система відрізняється від системи АРПП, розглянутих раніше, відсутністю двигуна і додатковим інтегратором.

Таким чином, боротьба з „глибокими ” завмираннями сигналу в системі АРПП, також як і в системі, при використанні розглянутого нового типу регулятора, який ввімкнено в зворотний канал радіоуправління, є вельми ефективною, що підтверджується високою якістю системи, яка характеризується вельми малими помилками розузгодження в перехідних і сталих динамічних режимах функціонування системи. Система з високою точністю відпрацьовує заданий рівень опорної напруги, якою оператор задає необхідну якість НВЧ-сигнала, що приймається, на виході радіоприймача прямого радіоканалу.

ЛІТЕРАТУРА

1. *Гостєв В.І., Кунах Н.І., Науменко М.І.* Системи автоматичного регулювання потужності передавача в каналах радіозвязку. – К.: „Радіоаматор”, 2007. – 332 с.

2. *Гостев В.И., Панченко И.В., Ткаченко А.Л.* Модели аттенюатора как элемента системы автоматического регулирования мощности передатчика // Вісник Черкаського державного технологічного університету.– 2007, №1 – 2.– С.94 – 98.

3. *Гостев В.И.* Нечеткие регуляторы в системах автоматического управления. – К.: Издательство „Радіоаматор”, 2008. – 972 с.

Пивовар С.О. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ОЦІНКИ ЯКОСТІ ОБСЛУГОВУВАННЯ В IP МЕРЕЖАХ ІЗ ЗАСТОСУВАННЯМ НЕЧІТКОЇ ЛОГІКИ

В даний час використовуються об’єктивні системи оцінки якості, що базуються на об’єктивних показниках якості обслуговування навантаження мережею. Для IP-мереж такими типово є пропускна спроможність, затримка при розповсюдженні пакету, варіація цієї затримки і процент втрачених пакетів. Суттєвою відмінністю об’єктивних показників якості від суб’єктивних являється їх математична сутність, яка дає можливість оперувати з даними оцінками за допомогою відповідних математичних апаратів. Крім того, об’єктивні показники якості можуть бути виміряні достатньо точно. При цьому через наявність різнотипних видів трафіку в *IP*-мережах одні і ті ж виміряні об’єктивні параметри якості по-різному відображатимуться на суб’єктивному сприйнятті якості, а значить, і на суб’єктивній оцінці. Таким чином, існує деякий дуалізм в понятті „якість”. Воно формується з одного боку суб’єктивними оцінками користувачів, з іншого боку – об’єктивними вимірами відділу експлуатації оператора мережі. Слід так само враховувати, що через вказані причини об’єктивні показники якості не можуть бути однозначно відображені на безлічі можливих суб’єктивних оцінок.

Європейський інститут стандартизації в електрозв’язку (*ETSI*) в технічній специфікації *TS* 101 329-2 визначає 3 класи якості обслуговування в системі *IP*-телефонії.

Перший – широкосмуговий. Якість з’єднання цього класу буде краще, ніж в комутованій мережі зв’язку (КМЗ). Для цього використовуються кодеки з більшою смугою пропускання, ніж кодек згідно рекомендації МСЄ-Т G.711.

Другий – вузькосмуговий. Системи цього класу повинні забезпечувати якість мови, сумірну з якістю КМЗ.

Третій клас – максимально можливий. Дані з’єднання придатні для використання, однак, вони не гарантують постійність характеристик якості. Такий клас з’єднань прийнятний, наприклад, в глобальній мережі Internet.

Для кожного класу обслуговування визначені три показники якості: загальна оцінка якості передачі R (*Overall Transmission Quality Rating*), якість мови та затримка з кінця в кінець.

Застосовуючи математичний апарат теорії нечітких множин ми добилися взаємно однозначного відображення об’єктивних і суб’єктивних показників якості обслуговування навантаження в *IP*-мережах. Таким чином, ми можемо на універсальній основі оперувати об’єктивними і суб’єктивними показниками якості нарівні. Крім того, в процесі побудови матриць порівняння ми не мали в своєму розпорядженні точних даних про те, яка якість відповідає тому або іншому показнику, а лише умовно порівнювали їх. Останнє дає можливість працювати при частковій доступності даних, що якісним чином відрізняє апарат нечітких множин від більшості інших.

ЛІТЕРАТУРА

1. *ETSI: „European digital* cellular telecommunications system, Global System for Mobile communications (GSM)” ETR 099 October 1993.

2. *ETSI TC-SMG*. Digital cellular telecommunication system (Phase 2+); CAMEL. GSM Recommendation 03.78; Version 0.9.0, July 1996.

3. *„Развитие технологии* мобильных интеллектуальных сетей GSM” Mobile Communications International/RE Мобильные Коммуникации – Russian Edition № 8-9/2001.

4. *Крылов В.В., Самохвалова С.С.* Теория телетрафика и ее приложения. – СПб.: БХВ – Петербург, 2005. – 288 с.: ил.

Пилипенко А.А. (ВІТІ НТУУ„КПІ”)

# АЛГОРИТМ ПІДВИЩЕННЯ ТОЧНОСТІ НАВЕДЕННЯ В ЦИФРОВИХ АНТЕННИХ РЕШІТКАХ З ВИСОКОЮ РАЗРЕШАЮЧОЮ МОЖЛИВІСТЮ ЗА ДОПОМОГОЮ КОРЕЛЯЦІЙНОЇ МАТРИЦІ

Достоїнством цифрових антенних решіток використовуваємих бортовими ретрансляторами е можливість сформувати достатньо вузьку діаграму направленості променя на наземну станцію. Такій підхід дозволив:

– підвищити перешкодозахищеність каналів зв’язку;

– зменшити вимоги до енергетичного потенціалу ретранслятора;

– підвищити скритність ліній при роботі супутника .

Однак для формування променя, на ретрансляторі необхідно вичислити кутові координати наземних станцій відносно ретранслятора.

Останнє десятиріччя широкого поширення для оцінки в антенних решітках кутових координат набуває метод нелінійного спектрального аналізу заснованого на звернутої кореляційної матриці. Одним із недоліків метода являється те, що наявність власних шумів антенних решіток приводить до зміщення кутових параметрів джерел випромінювання. В той же час кореляційна матриця є вирядженою, та не обертаючою.

Для можливості усунення цього недоліку у методі нелінійного спектрального аналізу заснованого на звернутої кореляційної матриці пропонується замінити кореляційну матрицю на параметр регулярізації оцінювання кутових координат, що дозволить зменшити вплив внутрішніх шумів якій приводить до зміщення кутових параметрів джерел випромінювання. А під час оцінки відносних потужностей сигналів земних станцій дозволить уникнути ефекту придушення слабкого сигналу, шляхом урівняння потужностей. Також перевагою цього методу поряд з високої разрешаючою є згібністю є низки розрахункові витрати.

ЛІТЕРАТУРА

1. *Слюсар В.И.* Торцевые произведения матриц в радиолокационных приложениях // Ред.журн. Радиоэлектроника (Изв. высш. учебн. завед.). – 1998. – №3. – С. 71 – 75.

2. *Лобкова Л.М., Проценко М.Б., Посный О.А*. Взаимные сопротивления излучения круглых рамок в малоэлементных антенных решетках // Радиоэлектроника. – 1999. – Т. 42. – № 2. – С. 27 – 32. (Изв. высш. учеб. заведений).

3. *Бархота В.А. Горшков В.В*., Журавлев В.И. Системы связи с расширением спектра сигналов // Итоги науки и техники. Связь. – М.: ВИНИТИ, 1990. – Т. 5. – С. 186 – 227.

4. *Conticello C.* Spread Spectrum Communications: an Overview // Alta Frequenza, 1987. – V. LVI. – № 6. – P. 255 – 264.

5. *Тузов Г.И., Козлов М. Р.* Помехозащищенность систем связи, использующих сигналы с псевдослучайной перестройкой рабочей частоты // Зарубежная радиоэлектроника. – 1989. – № 3. – С 19 – 32.

6. *Putman C A., Rappaport S S., Schilling D.L.* A Comparison of Schemes for Coaisc Acquisition of Frequency-Hopped Spread-Spectrum Signals // IEEE Trans, 1983. – V. COM-31. – № 2. – P 183 – 189.

к.т.н. Півень С.О.(ЦНДІ ОВТ ЗСУ)
Іванов Б.П. (ЦНДІ ОВТ ЗСУ)

# УДОСКОНАЛЕННЯ ЗВ'ЯЗКУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Зараз в світі йде безперервний процес військово-технічних перетворень у військовій справі. В провідних країнах розробляються концепції воєн шостого покоління, в яких вирішальна роль надається розвідці, автоматизованому управлінню військами, високоточній звичайній зброї, а також зброї на нових фізичних принципах і нетрадиційній зброї.

Як показують результати проведеного аналізу в галузі зв'язку (телекомунікації), автоматизованих систем управління військами та інформатизації органів управління, за останнє п'ятнадцятиріччя наочно простежується збільшення уваги державних органів влади і комерційних структур до постійного оновлення і модернізації засобів і комплексів зв'язку та інформатизації, розробки програмного забезпечення. За досвідом досягнень в галузі зв'язку та інформатизації, що мають подвійне застосування і можуть бути застосовані під час проведення війн шостого покоління у збройних силах суміжних з Україною держав та провідних країн світу, визначені такі тенденції:

1. Удосконалення форм і способів організації зв'язку та інформатизації органів управління здійснюється шляхом цілеспрямованої інтеграції систем зв'язку (телекомунікації) і автоматизації управління на таких рівнях:

на функціональному (послуги) – інтеграція функцій обміну й обробки інформації;

на технологічному – інтеграція видів забезпечення (технічного, програмного, інформаційного і лінгвістичного);

на технічному – застосування новітніх алгоритмів обробки сигналів для ущільнення даних, а саме: алгоритмів хаотичних перетворень, фрактальних відображень та ін.;

на організаційному – інтеграція органів військового управління, частин, підрозділів зв'язку та автоматизації, в тому числі і систем управління зв'язком та автоматизацією.

2. Визначення в системі зв'язку таких основних складових: центрів даних як інтелектуальних систем пам'яті для даних і додатків; телекомунікацій як транспортної мережі, що забезпечує доступ до даних і додатків; клієнтських пристроїв як пристроїв доступу до мережі.

3. Створення єдиного інформаційного простору для військових підрозділів збройних сил шостого покоління, де виконуються роботи за такими напрямами:

забезпечення всіх видів послуг зв'язку шляхом удосконалення існуючих ліній, мереж і вузлів зв'язку різного призначення на основі сучасних (перспективних) засобів зв'язку та автоматизації з метою задоволення зростаючих потреб систем управління військами (силами) в забезпеченні інформаційного обміну та автоматизованої обробки інформації в мирний час та в особливий період на значних відстанях із застосуванням супутникового зв'язку;

забезпечення інформаційної безпеки шляхом проведення єдиної державної технічної політики щодо розробки і виробництва максимально уніфікованих військових засобів зв'язку та автоматизації, які відповідають стандартам блоку НАТО, національним нормативним документам і рекомендаціям Міжнародної спілки електрозв'язку;

орендування для потреб військового зв'язку цифрових каналів і потоків різних швидкостей в комерційних мережах, які знаходяться під контролем країн-членів НАТО;

розробка і впровадження національних технічних засобів захисту інформації, аутентифікації і криптографії, що забезпечують конфіденційність із заданою стійкістю при обміні та обробці інформації засобами імпортного виробництва.

Виконаний порівняльний аналіз тенденцій темпів розвитку військового зв'язку з іншими державами дозволяє зробити висновок, що війська зв'язку та інформаційних систем ЗС України істотно відстають у вирішенні питань підготовки до війн шостого покоління порівняно не тільки з провідними країнами світу, але й із суміжними з Україною державами.

к.т.н. Польщиков К.О. (ВІТІ НТУУ „КПІ”)
Здоренко Ю.М. (ВІТІ НТУУ „КПІ”)
Шкіцькій В.В. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ МЕТОДІВ БОРОТЬБИ З ПЕРЕВАНТАЖЕННЯМИ, ЩО ВИКОРИСТОВУЮТЬСЯ ПРИ ПЕРЕДАВАННІ TCP-ТРАФІКУ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Забезпечення вимог щодо якості обслуговування користувачів при передачі TCP-трафіку в телекомунікаційних мережах є актуальним завданням. Збільшення інтенсивності трафіку в умовах обмеженої пропускної здатності мереж призводить до їх перевантаження. Процес перевантаження супроводжується переповненням поточних черг в маршрутизаторах, відкиданням великої кількості пакетів, і як наслідок – суттєвим погіршенням якості доставки інформації.

В телекомунікаційних мережах найчастіше використовують дві групи методів, спрямованих на вирішення задачі боротьби з мережними перевантаженням при передаванні TCP-трафіку. Перша група методів ґрунтується на адаптивній зміні інтенсивності відправлення пакетів джерелом в залежності від ситуації в мережі. У випадку виникнення перевантаження (ознакою цього є втрата пакету або отримання трьох дублюючих квитанцій) TCP-відправник різко зменшує розмір вікна передавання. При цьому час повернення до попереднього рівня інтенсивності передачі є досить великим. Методи управління вікном (повільний старт, боротьба з перевантаженням, швидке відновлення та швидка повторна передача), що реалізовані в діючих модифікаціях протоколу TCP, мають суттєві недоліки. Основна причина цих недоліків є у тому, що застосування зазначених методів не дозволяє передбачити перевантаження мережі, а лише усуває його наслідки.

Використання методів другої групи спрямоване на попередження переваження у мережі шляхом завчасного відкидання пакетів в маршрутизаторах. Ці методи отримали назву методів активного управління чергами. Найчастіше в телекомунікаційних мережах застосовують метод випадкового завчасного виявлення перевантаження (Random Early Detection, RED). Завчасне відкидання пакетів дозволяє запобігти переповненню поточної черги маршрутизатора, зменшити затримки передавання даних. Крім цього, завчасне відкидання пакетів викликає відповідну реакцію TCP-відправників, що полягає у зменшенні вікна передавання. В результаті створюється комплексна система попередження перевантаження з неявним зворотнім зв’язком. Проте, слід відзначити основний недолік методу RED, що полягає у складності налаштування його параметрів, особливо в умовах динамічної зміни характеристик мережного трафіку.

Отже, методи боротьби з мережними перевантаженнями, що використовуються при передаванні TCP-трафіку, потребують удосконалення з метою забезпечення вимог щодо якості обслуговування користувачів телекомунікаційних мереж.

ЛІТЕРАТУРА

1. *Вишневский В.М.* Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. – 512 с.

2. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958 с.

3. *Вегенша Ш.* Качество обслуживания в сетях IP: Пер. с англ. – М.: Издательский дом „Вильямс”, 2003. – 386 с.

4. *Таненбаум Е.* . Компьютерные сети. 4е изд.: Пер. с англ. – СПб.: Питер, 2003. – 992 с.

5. *Кучерявый Е.А.* Управление трафиком и качество обслуживания в сети Интернет – СПб.: Наука и техника, 2004. – 336 с.

к.т.н. Пономарьов Ю. В. (ЖВІНАУ)
Нетребко Р. В. (ЖВІНАУ)

# МОДЕЛЮВАННЯ ЯК СПОСІБ ПІДВИЩЕННЯ ЯКОСТІ МЕТРОЛОГІЧНОЇ ПІДГОТОВКИ МАЙБУТНІХ ІНЖЕНЕРІВ

У теперішній час проектування, розробка, модернізація, налагодження, обслуговування та експлуатація складних інформаційних систем неможлива без використання різноманітних засобів вимірювальної техніки (ЗВТ), що використовують безліч методів і способів вимірювання.

Це потребує від фахівців впевнених знань цих методів та вмінь практичної роботи із ЗВТ. Під час підготовки майбутніх інженерів постає питання чіткого метрологічного забезпечення навчального процесу.

Проте, як відомо, саме тут виникає безліч труднощів і протиріч у задоволенні зазначеного забезпечення. З одного боку, існує багато ЗВТ так званого „старого” парку, які вже морально і фізично застаріли, не повіряються через відомі вади, постійно виходять з ладу і з кожним роком потребують все більших зусиль для ремонту, що не дає можливості студентам у повному обсязі відпрацювати всі питання і отримати тверді практичні навички. З іншого боку, на даному етапі потрібно більше застосовувати сучасні цифрові ЗВТ, що використовують новітні технології побудови і методи вимірювання.

Проте вони, на жаль, майже практично відсутні у навчальному процесі через вищевказані труднощі метрологічного забезпечення.

Ті ж окремі одиниці зазначених ЗВТ, що існують на кафедрах, не дають можливості всім і у повному обсязі відпрацювати безліч практичних питань, які передбачені навчальним процесом.

Виникає протиріччя між наявною кількістю ЗВТ (метрологічного забезпечення навчального процесу) і необхідною якістю підготовки фахівців. Зрозуміло, що цю проблему одразу й окремою дією не вирішити.

Потрібний комплекс заходів. Одним із таких заходів, на наш погляд, є перехід до моделювання. Адже відомо, що для того, щоб отримати тверді практичні навички в роботі із зазначеними ЗВТ, необхідно багато часу витратити саме на практичну роботу з ними.

Але досвід показує, якщо студенти не з’ясували для себе сутність методів і принципів роботи вимірювальних приладів, з якими вони працюють, то практична робота буде мати низку труднощів.

Незнання та невміння у підготовці приладів до роботи, встановленні початкових положень перемикачів, проведенні балансування та калібрування, правильному під’єднанні їх до електричних кіл, нерішучість та невпевненість дій, виконання безлічі неправильних, поспішних і зайвих перемикань, помилковий вибір режимів роботи і потрібних діапазонів – все це призводить до виникнення додаткових джерел похибок і в решті-решт до отримання результату, що не відповідає метрологічним характеристикам ЗВТ, а в найгіршому випадку – до виникнення неполадок, збоїв та відмов.

Це, у свою чергу, потребує ремонту, налагодження і, як наслідок, до збільшення часу на підготовку фахівців (їх навчання).

Якщо ж студенти знають принципи роботи і сутність методів, які застосовуються під час вимірювання, то в цьому випадку їх дії найбільш спрямовані на швидке і правильне отримання остаточного результату, що значно скорочує час на підготовку фахівців і експлуатацію (ремонт) ЗВТ.

Отримати такі початкові навички можна тоді, коли до початку роботи безпосередньо із ЗВТ попрацювати з моделями зазначених приладів, тобто використати спеціалізовані автоматизовані системи моделювання, наприклад, систему схемотехнічного проектування і моделювання „Electronics Workbench” (EWB). Вона дозволяє за допомогою ПЕОМ швидко і

зручно відпрацювати всі питання щодо використання моделей різноманітних вимірювальних засобів, таких як: різноманітні джерела сигналів (вимірювальні генератори), амперметри, вольтметри, осцилографи тощо.

Досвід показує, що навчившись працювати в зазначеному програмному середовищі із вказаними моделями, студенти потім досить швидко і вміло починають користуватися реальними приладами, не роблячи при цьому безліч помилок і зайвих, невірних дій. Час їх практичної підготовки зменшується.

Тому для якісної підготовки майбутніх інженерів доцільно загальний час, що відводиться на навчання роботи із ЗВТ, поділити пропорційно залежно від ступеня метрологічного забезпечення на дві частини: роботу з моделями ЗВТ у відповідних програмних продуктах і безпосередньо з реальними ЗВТ.

У доповіді наведені приклади використання моделей амперметра, вольтметра, мультиметра, двох типів осцилографів для вимірювання струму і напруги в колах постійного та змінного струму, а також для дослідження форми сигналів і їх параметрів.

Крім того, наведені можливості щодо використання спеціальних режимів аналізу перехідних процесів в електричних колах і дослідження спектрів сигналів.

Аналіз отриманих результатів показує високу адекватність моделей реальним вимірювальним приладам та зручність їх використання у навчанні, оскільки за своїми органами керування, режимами роботи, принципами дії і навіть за власними зовнішніми зображеннями вони наближені до реально існуючих зразків ЗВТ, що максимально сприяє засвоєнню їх роботи під час віртуальних вимірювань.

ЛІТЕРАТУРА

1. *Дорожовець М. В., Мотало В. М., Стадник Б. К. та ін.* Основи метрології та вимірювальної техніки: у 2т. – Львів : Львівська політехніка, 2005. – 826 с.

2. *Козлов М. Г.* Метрология и стандартизация: учебник. – СПб. : Петербургский ин-т печати, 2001. – 372 с.

3. *Карлащук В.И.* Электронная лаборатория на IBM PC. Программа Electronics Workbench и её применение / В. М. Карлащук. – М. : Солон, 1999. – 512 с.

4. *Панфилов Д.И., Иванов В.С., Чупурин И.Н;* под общей ред. Д.И. Панфилова.Электротехника и электроника в экспериментах и упражнениях: практикум на Electronics Workbench: в 2 т. / Д. И. Панфилов, – М. : ДОДЭКА, 1999. – 423 с.

к.т.н. Правило В.В. (ВІТІ НТУУ „КПІ”)
Шарапанюк О.А. (ВІТІ НТУУ „КПІ”)

# МЕТОД ФОРМУВАННЯ СПЕКТРА ШУМОПОДІБНОГО СИГНАЛУ

В наш час, в умовах стрімкого розвитку інформаційного суспільства, широкого розповсюдження зазнають різні системи рухомого зв’язку, які відповідно до вимог сучасного життя повинні мати максимально можливу канальну ємність, надавати як найширший спектр послуг, необхідних користувачеві, забезпечувати конфіденційність передачі інформації, мати низький рівень потужності, що витрачається абонентською станцією і разом з тим забезпечувати відносну простоту та дешевизну реалізації обладнання. Досягнення цих показників в повній мірі залежить від використовуваного методу багатостанційного доступу.

Загально відомо, що все частіше знаходять застосування системи рухомого зв’язку, в яких використовується кодовий розподіл каналів, ефективність якого значною мірою залежить від виду використовуваного шумоподібного сигналу (ШПС) та методу формування спектра частот.

Основною метою доповіді являється синтез доцільних модемів формування спектра шумоподібного сигналу, для систем з багато станційним доступом з кодовим розрізненням сигналів. Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Розглянути різні методи багатостанційного доступу.
2. Дослідити варіанти використання розглянутих методів в різних системах рухомого зв’язку.
3. Виходячи із розглянутих варіантів використання різних методів багатостанційного доступу в системах рухомого зв’язку, здійснити оцінку ефективності кожного методу.
4. Здійснити вибір показників ефективності складних сигналів, що використовуються в системах рухомого зв’язку з кодовим розрізненням сигналів.
5. Здійснити вибір методу формування спектра шумоподібного сигналу для систем з багатостанційним доступом з кодовим розрізненням сигналів.

Об’єктом дослідження являються методи багатостанційного доступу, що використовуються в сучасних системах рухомого зв’язку. Предметом дослідження даного об’єкта є шумоподібні сигнали, а саме особливості формування спектра цих сигналів.

Застосовується системний підхід до об’єкта та предмета дослідження. Методом абстрагування здійснюється вибір основних параметрів систем рухомого зв’язку, та параметрів оцінки шумоподібних сигналів. Методом аналізу цих систем здійснюється оцінка ефективності використання різних методів багатостанційного доступу, що використовуються. Із отриманих результатів робиться висновок щодо подальшого розвитку та поширення стандартів рухомого зв’язку, де використовується кодовий розподіл каналів. Обирається найефективніший метод формування спектра шумоподібного сигналу. Методом синтезу створюються доцільні модеми та здійснюється оцінка ефективності синтезованих пристроїв.

Пропонується здійснити аналітичний та графічний аналіз різних методів формування спектра шумоподібних сигналів. Обрано більш ефективний метод формування спектру вище-зазначеного сигналу, використовуючи який здійснено синтез оптимальних модемів цих сигналів, які відрізняються від існуючих простотою реалізації. При цьому надається можливість формування ШПС з більшими базами, що приводить до загального покращення показників систем рухомого зв’язку, в яких вони будуть використовуватися та здешевлять обладнання цих систем. Синтезовані доцільні модеми можна використовувати в обладнанні, яке застосовується в сучасних відомчих мережах рухомого зв’язку з метою здешевлення, спрощення реалізації, покращення масо-габаритних показників, показників якості, завадостійкості та конфіденційності передачі інформації.

Прищепа Т.О. ІТС НТУУ „КПІ”
д.т.н. Лисенко О.І. ІТС НТУУ „КПІ”

# ВИКОРИСТАННЯ ЄВОЛЮЦІЙНИХ СТРУКТУР ДЛЯ РОЗВ’ЯЗАННЯ ЗАДАЧ СИНТЕЗУ ТА УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ СИСТЕМАМИ

Телекомунікація – одна з самих прибуткових в Україні галузей, яка стрімко розвивається. Тому особливо актуальними є роботи, пов’язані з дослідженням та розвитком телекомунікаційних систем, зокрема мобільних систем зв’язку.

Для телекомунікаційних систем характерними є наступні фактори:

– еволюційний характер їх розвитку;
– функціональна гнучкість системи;
– високі вимоги до міри адаптивності системи;
– вимоги до можливості їх модифікації в режимі реального часу та ін.

Сучасні методи проектування телекомунікаційних систем в основному ґрунтуються на розв’язку окремих задач, прикладами яких можуть бути задачі управління трафіком, задачі оптимізації завантаження каналів передачі даних, задачі забезпечення заданої якості даних та ін.

Як відомо, задачі оптимізації полягають у знаходженні мінімуму (максимуму) заданої функції. Таку функцію називають цільовою. Як правило, цільова функція – складна функція, яка залежить від деяких вхідних параметрів. У задачах оптимізації потрібно знайти значення вхідних параметрів, при яких цільова функція досягає мінімального (максимального) значення. Існує цілий клас методів оптимізації. Умовно їх можна розділити на методи, що використовують поняття похідної і стохастичні методи (наприклад, методи групи Монте-Карло). З їхньою допомогою можна знайти екстремальне значення цільової функції, але не завжди можна бути упевненим, що отримане значення є глобальний екстремум. Знаходження локального екстремуму замість глобального називається передчасною збіжністю. Крім проблеми передчасної збіжності існує інша проблема – час процесу обчислень. Найчастіше більш точні методи оптимізації працюють дуже довго.

Для рішення цих проблем і проводиться пошук нових алгоритмів оптимізації. Запропоновані в 1975 році Джоном Холландом генетичні алгоритми (ГА) відносяться до стохастичних методів.

ГА базуються на теоретичних досягненнях синтетичної теорії еволюції, яка враховує мікробіологічні механізми наслідування ознак у природних і штучних популяціях організмів, а також на накопиченому людством досвіді в селекції тварин і рослин.

Методологічна основа ГА ґрунтується на гіпотезі селекції, яка в загальному вигляді може бути сформульована так: чим більше пристосування особини до умов функціонування, тим більша ймовірність того, що в нащадків відповідних особин ознаки, які визначають пристосування, будуть виражені ще сильніше. Оскільки ГА мають справу з популяціями сталої чисельності, особливу актуальність, на рівні з відбором кандидатів у батьки, набуває відбір особин на елімінування. Стратегія елімінування, повинна відповісти на питання „Від яких особин доцільно відмовитися?”. Це складає не менш важливу компоненту сучасних ГА, ніж стратегія відбору до батьківських груп. Частіше за все особини, які володіють низьким рівнем пристосування, не тільки не приймають участь у генерації нового покоління, а елімінуються з популяції на поточному дискретному кроці еволюції.

Ідея оптимальності, як вірно відмічено [1], прийшла в науку з біології. Багато методів оптимального проектування мають корені в селекційній практиці. Впевнитися в цьому не важко, якщо подивитися на процедуру чисельної оптимізації через призму гіпотези селекції.

При дослідженні технічних об’єктів можна використовувати підхід, при якому починають з формування в просторі області допустимих значень змінних, що характеризують об’єкт, і вибирають у цій області деякі пробні точки. Спочатку за допомогою

математичної моделі технічного об'єкту виконують відображення вибраних точок у простір критеріїв. Потім на основі отриманої інформації у відповідності з вибраною пошуковою стратегією виконують певні перетворення значень вибраних точок у просторі змінних, які завершуються генерацією нових значень пробних точок, які наближають отримані значення до оптимального.

Окреслюючи на загальному рівні цю процедуру можна відмітити явно виражену паралель між закладеною в ній ідеологією пошуку екстремуму і тим, як розв'язуються подібні по змісту задачі в природі, при адаптації організмів до факторів навколишнього середовища.

Опис технічних об'єктів за допомогою векторів змінних проектування передбачає символьне кодування інформації про об'єкт. Категорія „Вектор змінних проектування" відіграє в техніці ту ж саму роль, що і категорія „генотип" у біології. Групуючи ключові параметри об'єкта до вектору змінних, ми надаємо їм статус генетичної інформації. Така аналогія ґрунтується на тому що, з однієї сторони, відповідна інформація використовується для побудови об'єкту, а з іншої сторони, її можна використовувати як вихідні дані при генерації генотипів об'єктів наступного покоління.

У цьому полягає суть генотипів нащадків, які мають координати нових пробних точок, про які йшла мова вище. Подібно до того, як на генетичному рівні в природі відбувається схрещування організмів, у процедурі оптимізації координати нових пробних точок можна отримати в результаті аналогічних перетворень координат попередніх точок. У цьому випадку по суті використовується гіпотеза селекції, оскільки в якості батьківських завжди виступають кращі в генотипному відношенні, а не довільні точки (особини) із популяції потенційних рішень, невдалі ж рішення відкидають на поточному кроці.

ГА запозичають з біології:

– понятійний апарат;

– ідею колективного пошуку екстремуму за допомогою популяції осіб;

– способи представлення генетичної інформації;

– способи передачі генетичної інформації в чередуванні поколінь (генетичні оператори);

– ідею розмноження найбільш пристосованих особин.

Практичне використання ГА, як ефективних процедур структурного синтезу почалося з задач синтезу форми. Доведена Холландом теорема про збіжність стандартного ГА дозволяє розглядати ГА, як метод пошуку глобального екстремуму. Квадратична часова складність ГА прийнятна для комп'ютерної реалізації. Починаючи з середини 80-х років зацікавленість дослідників до даної проблематики різко зросла завдячуючи роботам, представленим на першій і наступних конференціях по ГА.

ЛІТЕРАТУРА

1. *Вороновский Г. К., Махотило К.В., Петрашев С.Н., Сергеев С.А.* Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности. – Х. ОСНОВА, 1997. – 112 с.

2. *Рутковская Д., Пилиньский М., Рутковский Л.* Нейронные сети, генетические алгоритмы и нечеткие системы: Пер. с польск. И.Д. Рудинского – М.: Горячая линия – Телеком, 2006.

3. *Стеклов В.К., Кильчинський Є.В., Колченко О.В.* Архітектура мережі управління телекомунікаціями: Навчальний посібник для студентів вищих навчальних закладів – К.: 2001.

Прохорчук Ю.Ю. (ВІТІ НТУУ „КПІ”)
к.т.н. Макарчук О.М. (ВІТІ НТУУ „КПІ”)

# ПОСЛІДОВНИЙ АНАЛІЗ СТАТИЧНИХ ВИПРОБУВАНЬ

Послідовний аналіз вивчав видатний математик-статистик, Вальд Абрахам, який запропонував метод послідовної перевірки статичних гіпотез. Цей метод виявляється досить ефективним у різних галузях науки і техніки, наприклад, під час вибіркового контролю масової продукції, при статичній обробці результатів фізичних експериментів, у загальній теорії зв’язку (при вирішені задачі виявлення сигналу в шумах). В існуючій теорії перевірки статичних гіпотез кількість спостережень, тобто обсяг вибірки, на яких ґрунтується перевірка, вважається постійним для кожної конкретної задачі. Суттєвою рисою послідовної перевірки гіпотез, на відміну від нині існуючої перевірки, є те, що кількість спостережень, необхідних для прийняття рішення, залежить в даному випадку від результату самих спостережень і отже, є невизначеною заздалегідь, а випадковою величиною.

В послідовній перевірці після кожного спостереження існує 3 рішення:

– прийняти гіпотезу;

– усунути гіпотезу;

– продовжити експеримент та провести додаткове спостереження.

Якщо приймається перше або друге рішення, то перевірка на цьому закінчується. Якщо приймається третє рішення, то виконується нове спостереження. На основі нього знову приймається одне з трьох можливих рішень.

Позначимо $M_m$ множиною всіх можливих вибірок ($X_1 \ldots X_m$). Для кожного цілого m, m-мірний простір розбивається на три неперетинні області $R_m$.

Під час першого спостереження, якщо буде визначена величина $X_1$:

– приймаємо гіпотезу *H*, якщо величина $X_1$, лежить в області $R_1^0$;

– відхиляємо гіпотезу *H*, якщо величина $X_1$, лежить в області $R_1^1$;

– відбувається нове спостереження, якщо величина $X_1$, лежить в області $R_1$.

Під час другого спостереження, якщо буде визначена величина $X_2$:

– приймаємо гіпотезу *H*, якщо величини ($X_1$, $X_2$) лежать в області $R_1^0$;

– відхиляємо гіпотезу *H*, якщо величини ($X_1$, $X_2$) лежать в області $R_1^1$;

– відбувається нове спостереження, якщо величини ($X_1$, $X_2$) лежить в області $R_1$.

Послідовна перевірка закінчується лише тоді, коли гіпотеза приймається або усувається.

На основі цього методу пропонується розробити систему для послідовного аналізу статичних випробувань, яка буде співпрацювати з утилітою *TCPDUMP*. Утиліта *TCPDUMP* створена під операційні системи *Windows* та *Unix*. Дозволяє перехоплювати та аналізувати мережевий трафік, який проходить через комп’ютер, на якому встановлена програма. Метою роботи двох програм є прийняття або усунення гіпотези, в результаті, якої є завчасне виявлення раніше запланованої мережевої атаки на локальну ЕОМ.

ЛІТЕРАТУРА

3. *Вальд Абрахам.* Последовательный анализ. // Москва. – 1960. – С.42 – 45.

4. *Ширяев А.Н.* Статистический последовательный анализ. Оптимальные правила остановки. // Москва. – 2002. – С.20 – 21.

5. *Норткат С.* Обнаружение нарушений безопасности в сетях. // Санкт-Петербург. – 2004. – С. 234.

к.т.н. Проценко М.М. (ЖВІ НАУ)

# МЕТОДИКА ВИБОРУ ВЕЙВЛЕТ-ФУНКЦІЇ ДЛЯ ОБРОБКИ ЦИФРОВИХ СИГНАЛІВ

На даний час набувають поширення алгоритми обробки складних сигналів з використанням вейвлет-перетворення. Перевагами даних алгоритмів є висока швидкодія та достовірність обробки, але питання вибору базисних функцій для різних видів сигналів є не вирішеним. Таким чином, розробка методики вибору вейвлет-фунції для обробки складних сигналів є актуальним науковим завданням.

Суть методики вибору вейвлет-функції для аналізу та обробки різних сигналів полягає у наступному:

на першому етапі обирається сімейство вейвлет-функцій, які є ортогональними та дають можливість реконструкції сигналу;

на другому етапі, обираються функції які мають алгоритми швидкого перетворення;

на третьому етапі здійснюється пряме та обернене вейвлет-перетворення, розраховується середньоквадратична похибка відновлення.

Роботу даної методики перевірено на прикладі лінійно-частотно модульованого (ЛЧМ) та кодо-фазоманіпульованого (КФМ) сигналів з такими параметрами: несуча частота 500 кГц, частота дискретизації 5 МГц, тривалість сигналів $5\times10^{-5}$ с, амплітуда $1\times10^{-3}$ В.

Аналіз похибок відновлення для двох сигналів показав, що найкращі результати дає вейвлет-функція Db1 для діапазону масштабів від 1 до 10.

Слід зауважити, що при зміні діапазону масштабів та параметрів сигналів вейвлет-функція може змінюватися. Отже для аналізу та обробки наявних ЛЧМ та КФМ сигналів при визначених рівнях та властивостях вейвлет-функції найбільш відповідає вейвлет-функція Db1. Це обумовлено тим, що при використані даної базової функції похибка відновлення сигналу мінімальна і складає $6{,}76\times10^{-32}$ В. Крім того обрана вейвлет-функція має просту алгоритмічну реалізацію та описується мінімальною кількістю коефіцієнтів на відміну від інших вейвлетів.

Висновок. Розроблена методика дозволяє обрати найкращу вейвлет-функцію для обробки та аналізу різних сигналів за критерієм мінімуму похибки відновлення сигналів. Для аналізу наявних ЛЧМ та КФМ сигналів (форма подання цифрова) обрана вейвлет-функція Db1 для діапазону масштабів з 1 по 10 при цифровому вейвлет-перетворенні. Розрахунки та моделювання проводились за допомогою універсальної інтегрованої системи комп’ютерної математики MATLAB 6.0.

ЛІТЕРАТУРА

1. *Яковлев А.Н.* Введение в вейвлет-преобразование Учебное пособие. – Новосибирск: изд-во НГТУ, 2003. – 104 с.

2. *Яковлев А.Н.* Основы вейвлет – преобразования сигналов: Учебное пособие. – М.: САЙНС – ПРЕСС, 2003. – 80 с.

3. *Грабар І.Г., Запольский В.Ф., Захаров В.К.,* Кришевский М.Б., Тростенюк Ю.І. Застосування вейвлет-перетворення функції вібросигналу в технічній діагностиці механізмів з ударними навантаженнями // Вісник ЖІТІ. –2002. –№23. – С. 16 – 21.

4. *Дремин И.М., Иванов О.В., Нечитайло В.А.* Вейвлеты и их использование. – УФН №5. – 2001. – С. 465–501.

5. *Астафьева Н.В.* Вейвлет-анализ: основи теории и примеры применения. – УФН №11. –1996. – С. 1145 – 1170.

к.т.н. Радзівілов Г.Д. (ВІТІ НТУУ „КПІ”)
Бевзюк Б.М. (ВІТІ НТУУ „КПІ”)

# МЕТОДИ ОЦІНКИ ФАКТОРІВ, ЩО ВПЛИВАЮТЬ НА ЯКІСТЬ ПЕРЕДАЧІ У ВОСП ЗІ СПЕКТРАЛЬНИМ РОЗПОДІЛОМ КАНАЛІВ

На сьогоднішній день технологія спектрального поділу каналів (СРК), яка також називається „мультиплексування з поділом за довжиною хвилі” (*WDM – wavelength division multiplexing*), є однією із найпоширеніших на транспортній телекомунікаційній (первинній) мережі зв’язку України, оскільки забезпечує практично необмежений потенціал для збільшення інформаційно-пропускної здатності існуючих багатоканальних волоконно-оптичних систем передачі (ВОСП). Однак, поряд з перевагами, варто також враховувати ряд факторів, які істотно впливають на якість передачі у ВОСП із СРК [1], а саме:

– наявність взаємних впливів між каналами внаслідок недосконалості сучасного ущільнюючого устаткування та лазерів, що входять до складу систем передачі;

– наявність нелінійних ефектів в оптичному волокні.

Існуючі методики проектування багатоканальних ВОСП із СРК передбачають розрахунок довжини регенераційної ділянки, втрат і загасання, енергетичного бюджету потужності системи з урахуванням частотного плану та швидкості передачі. При цьому зовсім не враховують лінійні та нелінійні взаємні міжканальні перешкоди у ВОСП із СРК, а також ступінь їхнього впливу на параметри якості передачі.

Тут слід зазначити, що найбільш повну інформативну картину про режим передачі ВОСП із СРК дає спектр групового (мультиплексного) сигналу. Спектральна картина являє собою розподіл потужності канальних сигналів у робочому діапазоні довжин хвиль. Завдяки цьому, за видом спектрального розподілу можна визначити довжини несучих хвиль кожного каналу, потужність та ширину спектра сигналу в кожному каналі і т.д. [1, 2].

Найбільш підходящими для цієї мети вимірювальними приладами є оптичні аналізатори спектра (ОАС), можливості яких дозволяють проводити як тонкий аналіз спектральної структури канальних сигналів, так і спостереження всієї панорами спектра групового сигналу в робочому діапазоні довжин хвиль.

Основні методи оцінки факторів, що впливають на якість передачі у ВОСП зі спектральним розподілом каналів: вимір характеристик 4-канального демультиплексора [3], вимір перехідного загасання на ближньому кінці 4-канального *MUX/DEMUX*-пристрою, оцінки рівня ефекту 4-хвильового змішання за допомогою оптичного аналізатора спектра або за допомогою вимірювача оптичної потужності [4].

**Висновки**. Таким чином, застосовуючи на етапі проектування ВОСП із СРК елементи запропонованої комплексної методики оцінки факторів, що впливають на якість передачі, можна впевнено гарантувати дотримання нормованого значення коефіцієнта помилок при передачі інформації у ВОСП із СРК під час експлуатації.

ЛІТЕРАТУРА

1. *Хиленко В.В., Богданова І.В., Никифоренко К.Б.* Оцінка перехресних завад в *WDM*-системах при проектуванні ВОЛЗ // Радіотехніка. Всеукраїнський міжвідомчий науково-технічний збірник. – 2006. – Вип. 146. – 19 – 24 с.

2. *Богданова І.В.* Оцінка ефекту 4-хвильового змішання при проектуванні ВОЛЗ із використанням *WDM*-систем // Зв’язок. – 2006. – № 7. – 58 – 61 с.

3. *ITU-T Recommendation* G.957 (03/06) Optical interfaces for equipment and systems relating to the synchronous digital hierarchy.

4. *Корнійчук В.І., Макаров Т.В., Панфілов І.П.* Оптичні системи передачі. – К.: Техніка, 1994. – С. 388.

к.т.н. Радзівілов Г.Д. (ВІТІ НТУУ „КПІ”)
Труш О.В. (ВІТІ НТУУ „КПІ”)

# ОЦІНКА ДИНАМІЧНОЇ ТОЧНОСТІ СИСТЕМИ ФОКУСУВАННЯ СТАНЦІЇ ЛАЗЕРНОГО ЗАПИСУ

Разом з науковими і технічними застосуваннями лазери використовуються в інформаційних технологіях для вирішення спеціальних завдань, причому ці застосування широко поширені або знаходяться у стадії досліджень. Найбільш поширеними прикладами таких застосувань є оптична цифрова пам’ять, оптична передача інформації, лазерна станція запису дисків, лазерні друкуючі пристрої, крім того вони застосовуються в обчислювальній техніці як різні пристрої.

В алгоритмічній схемі системи фокусування променя лазера експериментальної станції лазерного запису відмітною особливістю є те, що вона має неявно виражену задаючу дію, і єдиним вимірюваним сигналом є сигнал помилки фокусування, що формується дискримінатором на основі фотодіодів.

Система відстежує нерівності скляного диска-оригіналу з нанесеним шаром фоторезиста при обертанні диска із зміною швидкістю залежно від радіусу запису, при цьому лінійна швидкість запису підтримується рівною 1,2 м; 2,4 м; 4,8 м. залежно від режиму запису. Нерівності є эргодический стаціонарним випадковим процесом із спектральною щільністю вигляду

$$S_x(\omega) = 2D\alpha \frac{(\alpha^2 + \beta^2 + \omega^2)}{(\alpha^2 + \beta^2 - \omega^2) + 4\alpha^2\omega^2}. \qquad (1)$$

Числові параметри $\alpha$, $D$, $\beta$ залежать від партії скла і мають значення не гірше $\alpha = 75$, $D = 4$, $\beta = 250$, що підтверджується експериментальними дослідженнями.

Виходячи з умов забезпечення необхідної якості запису, середньоквадратична помилка системи $\varepsilon$ не повинна перевищувати 0,2 мкм, що відповідає дисперсії, яка визначається наступним виразом:

$$\theta_x^{\,2} = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \left| K_{\theta_x}(j\omega) \right|^2 S_x(\omega) d\omega, \qquad (2)$$

Дисперсія і середньоквадратична помилка системи відповідно мають значення: $\theta_x^{\,2} = 0{,}2436$, $\varepsilon = 0{,}4936$ мкм. Таким чином, середньоквадратична помилка перевищує допустиме значення в 2,45 разу. Звідси витікає необхідність оптимізації системи фокусування.

У зв’язку з тим, що система фокусування є безперервною, а оптимізація здійснюватиметься для дискретної системи, необхідно вибрати період дискретизації $T_д$ з умови адекватності дискретної і безперервної систем в реальному діапазоні частот вхідних сигналів. Виконаємо порівняльний аналіз результатів, які можна отримати при оптимізації системи фокусування на основі відомого методу функцій Ляпунова і з використанням пропонованого методу.

Дисперсія і середньоквадратична помилка при синтезі системи фокусування методом, заснованим на використанні функцій Ляпунова, приймають значення: $\theta_x^{\,2} = 0{,}0692$, $\varepsilon = 0{,}2631$ мкм, що перевищує допустиме значення помилки в 1,3 разу. Дисперсія і середньоквадратична помилка приймають значення: $\theta_x^{\,2} = 0{,}0387$, $\varepsilon = 0{,}1968$ мкм. Набуте значення $\varepsilon$ задовольняє умовам запису.

Таким чином, середньоквадратична помилка системи фокусування при синтезі управління модифікованим методом функцій Ляпунова в порівнянні з результатами, отриманими при використанні класичного методу, зменшилася в 1,34 разу і не перевищує допустиме значення.

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

# ПОРІВНЯЛЬНИЙ АНАЛІЗ КІНЦЕВИХ ЗАСОБІВ ПРОВОДОВОГО ТЕЛЕФОННОГО ЗВ’ЯЗКУ

Незважаючи на широке розповсюдження стільникового радіозв’язку проводовий телефонний зв’язок застосовується у всіх сферах діяльності людства, у тому числі і під час управління військами. Він забезпечує зручність ведення переговорів, відносно велику прихованість порівняно з іншими родами зв’язку (наприклад радіозв’язку), майже не підлягає дії навмисних та системних завад і застосовується у всіх видах бойових дій. Для організації проводового зв’язку використовуються різні засоби: проводові лінії, каналоутворюючі засоби, комутаційні, спеціальні та кінцеві засоби проводового телефонного зв’язку.

Для якісного обслуговування абонентів кінцеві засоби проводового телефонного зв’язку повинні задовольняти цілому ряду вимог: мати змогу працювати у заданих режимах роботи, наприклад, автоматичної телефонної станції з імпульсним та тоновим набором, ручної телефонної станції у режимі місцевої та центральної батареї, забезпечувати дистанційне управління радіостанцією. Для вказаних засобів що використовуються у воєнній організації додатково необхідно забезпечити фізичну міцність, здатність функціонувати в критичних обставинах (заміна штатного елементу живлення елементами цивільного використання або взагалі – можливість працювати без елементів живлення, можливість подачі сигналу „виклику” незалежно від наявності елементів живлення, працювати в однопроводовому режимі). Протягом тривалого часу у воєнній організації держави таким основним телефонним пристроєм був польовий телефонний апарат ТА-57, що загалом задовольняв вищезазначеним вимогам (за винятком роботи в мережі автоматичного телефонного зв’язку з тоновим набором номеру). У 2005 році у Збройних Силах України був прийнятий на озброєння новий польовий телефонний апарат ТА-01 вітчизняного виробництва (ТОВ ”Телекарт-прилад”, м. Одеса). Зазначений польовий телефонний апарат порівняно з попереднім має ряд додаткових функцій, а саме: сучасна елементна база, можливість працювати у мережі автоматичного телефонного зв’язку з тоновим набором номеру, подачі сигналу генератора по лінії для знаходження місця обриву польового кабелю (режим „Тест”), удосконалений кнопочний індукторний виклик, можливість забезпечення електроживлення від зовнішнього джерела. Разом з тим, наявні істотні недоліки, а саме:

відсутнє транспортне положення апарату яке б захищало його від зовнішніх фізичних впливів (наявність сумки для перенесення суттєво не покращує стану справ);

незважаючи на підсилений елемент живлення (1,3 А/год у ТА-57 та 13 А/год у ТА-01) робота забезпечується на значно менший термін (5-6 місяців для ТА-57 та 120 годин для ТА-01) що свідчить про значно більше енергоспоживання телефонного апарату ТА-01;

відсутність можливості подачі сигналу „Виклик” не тільки при відсутності, але і при пониженні робочої напруги елементу живлення;

більша вага порівняно з попереднім зразком (2,8 кг для ТА-57 та 3 кг для ТА-01);

незважаючи на задекларовану у „Посібнику по експлуатації” можливість забезпечення телефонного апарату електроживленням за допомогою трьох елементів 1,5 В з’єднаних послідовно, це досить умовне ствердження – необхідно додаткове сумісне кріплення цих елементів (ніша для елементів живлення значно ширша за сам елемент);

технічна документація, а саме „Посібник по експлуатації” (саме слово „Посібник” зазвичай не використовується у технічній експлуатаційній документації), відпрацьований формально в ньому відсутні принципові схеми, детальний перелік несправностей та порядок їх усунення що не дає змогу якісно освоїти порядок ремонту та експлуатації зазначеного телефонного апарату.

Таким чином, зазначений польовий телефонний апарат тільки умовно можна характеризувати як „кроком вперед”.

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

# МОЖЛИВІСТЬ ЗАСТОСУВАННЯ МЕТОДУ МНОЖИННОГО ДОСТУПУ З КОНТРОЛЕМ НЕСУЧОЇ ТА ВИЗНАЧЕННЯМ КОНФЛІКТУ В КОРПОРАТИВНИХ РАДІОМЕРЕЖАХ

З початку виникнення перших телекомунікаційних мереж з каналами зв’язку, що колективно використовуються, класифікаційна ємність протоколів множинного доступу значно розширилась, з’явилось багато нових протоколів, це вимагає в свою чергу їх класифікацію. Розглянемо класифікацію протоколів.

Поняття множинного доступу в загальному випадку пов’язане з розділенням канального ресурсу між сукупністю незалежно функціонуючих споживачів. Для радіомереж ним є колективно використовуваний всіма абонентами радіоканал.

Для передачі по радіоканалу пакетів повідомлень використовуються різноманітні протоколи. **Протокол** – сукупність однозначно визначених та обов’язкових для виконання всіма абонентами мережі процедур та правил. Протокол фактично є інструментом прийняття рішення про те, в який час та яким чином абонент може користуватись канальним ресурсом. Протоколи розділяють на два великих типа. Перший тип протоколів упорядкує роботу абонентів таким чином, що виключаються випадки, коли два та більше абонентів одночасно приймають рішення про передачу, в наслідок чого руйнуються пакети. Такі протоколи називають протоколами з **детермінованим розділянням каналу**. Безконфліктна передача в таких протоколах здійснюється за рахунок закріплення ресурсу каналу за абонентами. Якщо ресурс каналу закріплюється без врахування динаміки активності абонентів то протокол відносять до протоколів зі **статичним резервуванням**, в протилежному випадку – до протоколів з **динамічним резервуванням**. Статистичне резервування основане на **ортогональному** та **квазіортогональному** розділянні ресурсу. Ресурсами є час, на протязі якого абоненту надається право передачі, або частота, на якій ведеться передача. У відповідність цьому до протоколів з **ортогональним** розділянням ресурсу відносять протоколи з **частотним** та **часовим** розділянням каналів. Прикладом є протокол, що широко застосовується для мобільного зв’язку – GSM. В стандарті GSM використовується багатостанційний доступ з часовим розділянням каналу [8], що дозволяє на одній несучій частоті розташувати 8 мовних каналів одночасно.

В останній час в мережах застосовують протоколи, побудовані на одночасній передачі пакетів в загальній полосі частот – протоколи з **квазіортогональним розділянням**, що використовують різноманітні сигнальні коди (протоколи з **кодовим розділянням**, наприклад, з дискретною зміною частоти), шумоподібні сигнали та узгоджену фільтрацію (протоколи з **шумоподібними системами**).

Прокол з кодовим розділянням (англомовна абревіатура CDMA) впроваджується в останній час дуже активно. Це пояснюється порівняно низькою ціною обслуговування абонентів та підвищеними можливостями по якості та безпеки зв’язку. Багато фахівців в сфері телекомунікацій вважають, що технологія стільникового зв’язку CDMA в найближчий час витіснить як аналогові NMT, AMPS так і цифрові GSM стандарти.

Внаслідок того що протоколи зі статичним резервуванням не забезпечують достатнє функціонування мережі, звились протоколи з **динамічним резервуванням**, що базуються на принципі надання доступу з врахуванням активності абонентів. Протоколи цього типу для свого функціонування вимагають наявність інформації про потребу в ресурсі. Наслідком цього є виникнення додаткових витрат пов’язаних з передачею інформації та управляючих дій. Тобто можлива адаптація під інтенсивність трафіку, але ціна такої адаптації визначається тією частиною пропускної здатності каналу, що витрачається на організацію управління.

Виділяють протоколи з **централізованим** та **децентралізованим управлінням**. Для першого типу необхідний пристрій що виконує функції управління множинним доступом (диспетчер). До нього повинна поступати інформація від абонентів про необхідність передачі. Диспетчер отримує інформацію або шляхом **опитування**, або шляхом **активного резервування**, коли кожний абонент по спеціально виділеному підканалу в режимі **випадкового доступу** або **часового розділяння** передає запит на передачу. При **циклічному опитуванні** диспетчер послідовно опитує всіх абонентів та при наявності у них пакету надає їм право на передачу. Але використання цього протоколу обмежується при значній кількості абонентів. Тому використовують опитування в **випадковому**, або **адаптивному** порядку. В останньому випадку опитуються не всі абоненти, а спочатку видається широкомовний опитувальний сигнал. Якщо отримано відповідь хоча б від одного абонента, то всі абоненти діляться на групи і в кожній з них аналогічним чином визначаються абоненти готові до передачі.

Прикладом такого протоколу є телеметрична система спостереження за товщиною сніжного покриву „SNOTEL" служби меліорації і збереження родючості ґрунту Міністерства сільського господарства США. Система містить понад 500 периферійних станцій метеорного радіозв'язку. Периферійні станції вимірюють різні погодні умови у великій зоні західних штатів США і передають отриману інформацію на ведучу станцію. Для цієї системи була розроблена динамічна структура зі змінною груповою адресацією, у якій кілька периферійних станцій розподіляються в одну і більш груп, і всі станції в одній групі відповідають на одну групову адресу. Кількість одночасно адресуємих периферійних станцій у кожній групі залежить від кількості біт в адресі. Сигнал опитування, що містить більшу кількість адресних біт, є більш спрямованим і відноситься до меншої кількості периферійних станцій. Адреса, що містить меншу кількість біт, більш загальний і дозволяє відповісти на сигнал опитування більшій кількості периферійних станцій.

В протоколах з **активним резервуванням** можливий інший варіант отримання інформації диспетчером. Абоненти при необхідності передачі повідомляють диспетчеру в спеціально відведений час запит. Отримавши за вказаний час всі запити, диспетчер в відповідному порядку надає право передачі кожному з абонентів, що заявили про необхідність передачі. Право передачі може надаватись **без пріоритету**, або **з пріоритетом**, що важливо в силових та корпоративних мережах. За способом передачі запиту виділяють протоколи **з безконфліктною передачею запиту** та з передачею запита на основі **випадкового доступу**.

Протоколи з децентралізованим управлінням розподілу ресурсу каналу будуються або на кільцевій передачі маркера від абонента до абонента (**кільцеве резервування**), що дозволяє передавати пакет, або на передачі маркера зі **змінним пріоритетом**.

У корпоративних радіомережах найбільш широке використання отримав метод називаємий методом множинного доступу з контролем несучої та визначенням конфлікту (англомовна вимова *carrier-sense-multiply-access with collision detection,* **CSMA/CD**).

Цей метод застосовується виключно в мережах з загальним середовищем розповсюдження сигналу. Всі радіостанції такої мережі мають безпосередній доступ до середовища розповсюдження, тому воно може бути використано для передачі даних між будь-якими двома радіостанціями. Одночасно всі радіостанції мережі мають можливість негайно (з урахуванням затримки розповсюдження сигналу по фізичному середовищу) отримати дані, які будь-яка з радіостанції почала передавати в середовище розповсюдження. Простота схеми підключення - це один з чинників, що визначили успіх стандарту Ethernet.

Наступним етапом розвитку радіомереж з **ВМД** (випадковим множинним доступом) є припущення одночасного обслуговування декількох (в частковому випадку – двох) парних заявок. В подальшому виникає необхідність визначення (розрахунку) основних характеристик зазначеного протоколу.

к.т.н. Різуненко А.О. (ВІТІ НТУУ „КПІ”)

# МЕТОД ЗМЕНШЕННЯ ЕНТРОПІЇ ЗНАЧЕНЬ КОЕФІЦІЄНТІВ ТРАНСФОРМАНТ ЗОБРАЖЕНЬ ДЛЯ ПОБУДОВИ ГРАФІЧНОГО КОМПРЕСОРА

На сьогодні ефективність роботи програмних мультимедійних додатків у значній мірі залежить від об’ємів та якості даних, що перетворюються. Наприклад, у завданнях фільтрації графіки та розпізнавання образів якість зображень може нести вирішальну роль у вирішенні проблеми вцілому. Під час роботи графічних процесорів відеоадаптерів обробка, наприклад, ігрової графіки прискорюється за рахунок її компактного подання. Пропускна спроможність каналів передавання цифрової інформації безпосередньо залежить від об’ємів даних, що циркулюють в них. Тому завдання створення сучасних методів цифрової обробки зображень, метою яких є зменшення цифрового описання даних, актуальне і на сьогоднішній день.

Розробка будь-якого формату компресії даних складається із двох етапів: підготовки до стиснення і, власне, самого стиснення – безнадлишкового кодування. Другий етап є вирішеним питанням і включає в себе такі основні групи методів кодування даних як: кодування довжинами серій, словникове кодування, метод Хаффмана, арифметичне кодування [1].

Підвищити ефективність роботи графічних процесорів вдається за рахунок вдосконалення першого етапу – підготовки до безнадлишкового кодування. До головних процедур тут можна включити наступні: зміна кольорової моделі зображення, перетворення корельованих елементів зображення у незалежні коефіцієнти, квантування коефіцієнтів, упорядкування коефіцієнтів, передбачення контексту коефіцієнтів тощо [2]. Метою усіх перерахованих перетворень є зменшення ентропії елементів зображень, тобто створення передумов для витрачання меншої кількості біт для кодування пікселів графічного файлу.

Синтезований метод спрямований на зменшення ентропії значень коефіцієнтів зображень за допомогою їх упорядкування. Процедура оборотна, а, отже, може використовуватися як в графічних архіваторах, так і в компресорах з втратою якості початкових даних. Метод базується на використання підходів, що описані в алгоритмах А.Льюїсом і Г.Ноулесом, Шапіро і Саїдом-Перельманом [3, 4].

Застосування такої процедури у складі графічного формату зменшує ентропію зображень на 5–20 % у залежності від класу останніх, а ступінь компресії відповідно збільшує на 2–10%. Час оброблення даних суттєво не змінюється, оскільки метод нуль-дерева обчислювально нескладний.

ЛІТЕРАТУРА

1. *Прэтт У.* Цифровая обработка изображений: Пер. с англ. – М.: Мир, Кн. 2., 1982. – 480 с.

2. *Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин* Методы сжатия данных: – М.: Диалог-Мифи, 2002. – 384 с.

3. *Shapiro J. M.* Embedded image coding using zerotrees of wavelet coefficients // IEEE Transactions on Signal Processing, 41(12):3445-3462. – 1993.

4. *Said A., Pearlman W.* A new fast and effecient image codec based on set partitioning in hierarchical trees // IEEE Transactions on Circuits and Systems for Video Technology, 6(3):243-250. – 1996.

к.т.н. Роговець М. А. (ЖВІ НАУ)
к.т.н. Шуренок В. А. (ЖВІ НАУ)
к.т.н. Дзюбчук Р. В. (ЖВІ НАУ)

# МЕТОДИКА КОГНІТИВНОГО АНАЛІЗУ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ РОБОТИ

Інформаційно-аналітична робота (ІАР) – це комплекс заходів інформаційних підрозділів щодо забезпечення тривалого накопичення, систематизації, перевірки та тематичної обробки інформації. Зміст цього процесу залежить від структури та особливостей інтегрального об'єкта дослідження (ІОД).

ІОД являє собою слабоструктуровану систему, оскільки аналіз його процесів ускладнюється відсутністю достатньої кількості інформації про їх динаміку (розвиток). Це призводить до ускладнення виконання основного завдання дослідження, що полягає у визначенні логіки розвитку подій на багатофакторному полі [1, 2].

Для вивчення і моделювання процесів, що притаманні ІОД, пропонується застосовувати методи когнітивної структуризації, що дає змогу здійснити узагальнення знань експерта у предметній області та формалізувати процес ІАР.

У результаті проведеного дослідження розроблено методику когнітивного аналізу ІАР, яка включає в себе такі етапи:

1. Математичне формулювання завдання ІАР:

$$y = f(x_1, x_2, ..., x_n),$$

де $x_1, x_2, ..., x_n$ – набір значень факторів, що описують стан ІОД;

$y$ – стан ІОД.

2. Розробка структурно-семантичної моделі ІОД

$$H(t) = f[Y_1(t-1), Y_2(t-1), ..., Y_m(t-1)],$$

де $Y_i(t-1)$ - стан $i$-го елемента ІОД на $t-1$ кроці;

3. Побудова когнітивної моделі ІАР:

$$y_k(t+1) = y_k(t) + \sum_{l \subset M} a_{kl}(y_l(t) - y_l(t-1)), k, l \in M, t = 0,1,...,$$

де $y(\bullet)$ - вектор значень факторів, що описують процес у різні моменти часу;

$M = \{1,2,...,m\}$ - множина вершин;

$a_{kl}$ - елемент суміжних переходів когнітивної карти.

4. Структурний аналіз когнітивної моделі.

Під когнітивною моделлю розуміється когнітивна карта у вигляді зваженого орієнтовного графа $C = (M, G)$, де $M = \{1,2,...,m\}$ - множина вершин, що являє собою сукупність факторів, які описують стан системи; $G \subseteq M \times M$ - множина дуг, що описує причинно-наслідкові зв'язки між факторами та їх взаємний вплив [1, 2].

5. Здійснення предметної інтерпретації результатів когнітивного моделювання.

Розроблена методика когнітивного аналізу ІАР відрізняється від відомих застосуванням теоретико-ігрових моделей та дозволяє у складних ситуаціях, що обумовлюються невизначеністю, виявляти зміни режимів функціонування інтегрованого об'єкта дослідження, здійснювати обґрунтування виявлених змін, прогнозувати подальший розвиток обстановки.

ЛІТЕРАТУРА

1. *Новиков Д. А.* Теория управления организационными системами. – М.: Физматлит, 2007. – 584 с.

2. *Бялецкая Е. М., Квятковская И. Ю.* . О принципах когнитивного моделирования сложных систем. Вестник АГТУ / Астрахань: АГТУ, 2006. – Вип. № 1(30). – С. 116 - 119.

Розум І.Ю. (НАОУ)

# ВІДЕОЗВ'ЯЗОК В ПЕРСПЕКТИВНІЙ СИСТЕМІ ЗВЯЗКУ МЕХАНІЗОВАНОЇ БРИГАДИ

Одним з питань яке в останні роки активно досліджується є управління параметрами відеозображень при веденні відозв'язку. В системі зв'язку бригади процес обміну повідомленнями, та насамперед відеозображеннями, має відносно передачі відеозображень принципові особливості які відрізняють їх від систем загального користування.

По-перше, в СЗБр наданий телекомунікаційний ресурс може змінюватися під впливом зовнішніх факторів, які відповідно обумовлені особливостями функціонування таких систем. Така зміна відбувається як правило в бік зменшення ресурсу який надається.

По-друге, інформація, яка передається засобами відеозв'язку має різну на протязі часу важливість, різні вимоги до якості, абоненти мають різні пріоритети (категорію). Така ситуація потребує створення системи управління якістю відеозображень засобів відеозв'язку відповідно до ресурсів які використовуються цими засобами та пріоритетів користувачів які обмінюються відеозображеннями. Так як ресурс, що надається з телекомунікаційної мережі та вимоги до якості відеозображень від абонентів з часом змінюється така система управління повинна бути адаптована до цих змін. В результаті проведеного аналізу існуючих протоколів ущільнення відеозображень відносно показника якості відеозображень (відношення пікового значення сигналу до шуму PSNR) та діапазону швидкостей в яких протоколи можуть використовуватися визначені переваги протоколу H.264 для використання в спеціальних телекомунікаційних системах. Використання протоколу H.264 порівняно з протоколами H.261 та H.263 дозволяє зберігати більш високу (в середньому на 1,1-2,1 дБ) якість відеозображень в більш широких діапазонах швидкостей передачі відеозображень (від 12 до 1500 кбіт/с для H.264, від 64 до 1024 кбіт/с для H.261 та від 12 до 512 кбіт/с для H.263). Протокол H.264 зберігає більш високі показники якості відеозображень при середніх (від 100) та високих (до 1000) коефіцієнтах ущільнення відеозображень (не менш 19,2 дБ). Функціонування засобів відозв'язку та ВКЗ в системі звязку механізованої бригади має особливості які впливають на якість обміну відеозображеннями та призводять до її погіршення. До таких особливостей відносяться: використання абонентами спільного ресурсу центрів комутації та необхідність розподілу цього ресурсу, наявність абонентів з різними ступенями пріоритетів на якість обслуговування, можливість зміни наявного ресурсу центрів комутації завдяки впливу на систему зв'язку зовнішніх факторів. Визначено, що найбільш придатним для використання в спеціальних телекомунікаційних системах та перед усім в її польової компоненти, відносно умов функціонування цих систем та діапазону використання, є стандарт H.323, що описує організацію конференцій за допомогою мереж, заснованих на пакетній передачі інформації з негарантованою якістю обслуговування абонентів. Проведений аналіз стандарту H.323 та безпосередньо протоколу управління обміном мультимедійною інформацією H.245, відносно можливостей управління якістю відеозображень, виявив недостатню придатність цього протоколу для динамічного управління якістю відеозображення. Визначені протиріччя між існуючими методами управління якістю відеозображеннями та необхідним рівнем цього управління для абонентів які використовують засобами відозв'язку в спеціальних телекомунікаційних системах а саме: необхідність управління якістю відеозображеннями в залежності від наявного ресурсу центрів комутації, урахування пріоритетів абонентів. Необхідність створення спеціальних підходів щодо управління якістю відеозображень засобів відозв'язку які функціонують в спеціальних телекомунікаційних системах. В результаті аналізу вимог абонентів щодо забезпечення потрібної якості передачі відеозображень та умов функціонування спеціальної телекомунікаційної мережі визначена наукова задача щодо забезпечення абонентам якості відеозображень, яка б знаходилась в просторі обмежень на параметри відеозображень, мінімальну якість відеозображення, враховувала умови

функціонування спеціальної телекомунікаційної мережі, пріоритети абонентів та тривалість циклу управління.

к.т.н. Ролік О. І. (ФІОТ НТУУ „КПІ”)
Можаровський П. Ф. (ФІОТ НТУУ „КПІ”)
Покотило О. О. (ФІОТ НТУУ „КПІ”)

# ЗАСТОСУВАННЯ АГЕНТСЬКОГО ПІДХОДУ ДО УПРАВЛІННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЮ СИСТЕМОЮ АСУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Якість функціонування АСУ спеціального призначення безпосередньо залежить від ефективності і надійності роботи інформаційно-телекомунікаційних систем (ІТС), які не тільки забезпечують взаємодію між розподіленими компонентами АСУ чи користувачами, але й надають інформаційні та обчислювальні ресурси, необхідні для продуктивного виконання процесів діяльності. Висока вартість сучасних ІТС, зумовлена численними новітніми інформаційними технологіями (ІТ), інтеграція широкого спектру телекомунікаційного обладнання, необхідність зменшення експлуатаційних витрат і швидкого усунення несправностей, а також ряд інших факторів примушують розробляти та впроваджувати системи централізованого управління ІТС (СУІ) [1]. СУІ надають засоби автоматичного моніторингу, аналізу роботи й управління елементами ІТС (ІТ-елементами), функціональними й технологічними підсистемами АСУ та ін.

Розроблена СУІ із застосуванням агентського підходу [2] як концептуальної основи організації взаємодії серверної частини СУІ з територіально розподіленими об’єктами моніторингу і управління (ОМУ). ОМУ – узагальнене поняття, основна функціональна одиниця СУІ, у якій інкапсульовано властивості і стани ІТ-елементів. Відносно ОМУ визначаються параметри моніторингу та механізми виявлення несправностей і виконання команд управління. Кожен ІТ-елемент усіх рівнів ієрархії містить дерево ОМУ. У якості ОМУ виступають не тільки фізичні та логічні об’єкти але й функції, стани процесів діяльності та ін. Це дозволяє застосовувати універсальні методи роботи СУІ з ОМУ та використовувати єдиний підхід до оцінки їх станів [3].

Порівнюються два основних підходи до моніторингу, що застосовуються в СУІ спеціального призначення, – шляхом здійснення періодичного опитування ОМУ сервером СУІ та через використання активних агентів, що встановлюються на ІТ-елементи. У першому випадку всі задачі з опитування ОМУ та обробки даних моніторингу покладені на сервер СУІ, у другому – задачі моніторингу та оцінки станів виконує агентське ПЗ, яке інформує сервер про стан ОМУ із заданою періодичністю. Для кожного із методів оцінюються: затримка у часі отримання сервером даних про стан ОМУ, задіяність обчислювальних ресурсів обробкою інформації та завантаженість каналів зв’язку (КЗ) передачею
даних моніторингу.

Затримка $T_0$ отримання значення стану ОМУ визначається наступним чином:

$$T_0 = T_П + T_В + T_А + T_К, \tag{1}$$

де $T_П$ – витрати часу на планування опитування, $T_В$ – час, необхідний на вимірювання, $T_А$ – тривалість аналізу для визначення стану ОМУ, $T_К$ – затримка при передачі повідомлень через телекомунікаційну мережу.

Задіяність обчислювальних ресурсів визначається як:

$$P_0 = P_П + P_В + P_А + P_К + P_{ДК}, \tag{2}$$

де $P_П$, $P_В$, $P_А$, $P_К$, $P_{ДК}$ – затрати обчислювальної потужності відповідно на планування, вимірювання, визначення стану ОМУ, компоновку і шифрування повідомлення, що передається, та декодування прийнятого повідомлення в сервері СУІ.

Завантаженість КЗ під час моніторингу ОМУ сервером СУІ не залежить від стану ОМУ та визначається наступним чином:

$$I_0 = \sum_{i=1}^{n} I_{Bi}, \tag{3}$$

$$I_{Bi} = \sum_{j=1}^{m} \left( I_{3j} + I_{Oj} \right), \tag{4}$$

де $I_{Bi}, I_{3j}, I_{Oj}$ – завантаженість КЗ відповідно до вимірювань показників $i$-го ІТ-елементу, запитом показників $j$-го ОМУ та передачею результатів вимірювання, $n$ – кількість агентів, $m$ – кількість ОМУ в ІТ-елементі.

Завантаженість КЗ при застосуванні агентського підходу залежить від стану, в якому перебуває ОМУ, і визначається для окремого ІТ-елемента:

$$I_{Bi} = \sum_{j=1}^{m} \sum_{k=1}^{l} I_{ОМУjk} \cdot P\left( s_j \in \alpha_k \right) + \left( I_З + I_O \right), \tag{5}$$

де $I_{ОМУjk}$ – завантаженість КЗ $j$-м ОМУ, що перебуває у $k$-му класі станів, $P\left(s_j \in \alpha_k\right)$ – ймовірність належності стану $s_j$ ОМУ $k$-му класу станів, $\left(I_З + I_O\right)$ – завантаженість КЗ при перевірці сервером агентського ПЗ у формі запит-відповідь, $l$ – кількість станів ОМУ.

Проведено аналіз величин із (1) – (5) і факторів, що впливають на їх значення та визначаються режимами функціонування СУІ. Приведено результати імітаційного моделювання роботи СУІ для обох підходів та виконано відповідний аналіз. Визначено вимоги до параметрів інформаційної взаємодії між сервером та агентами СУІ. Сформульовано задачу раціонального розподілу обчислювальних навантажень на серверну та агентські частини ПЗ СУІ з урахуванням мінімізації завантаженості телекомунікаційної мережі та затримки при очікуванні результатів оцінки станів ОМУ.

Розроблена структура агента зображена на рисунку. Визначено функції модулів агентського ПЗ, механізми взаємодії між модулями агента та між агентами й сервером СУІ.

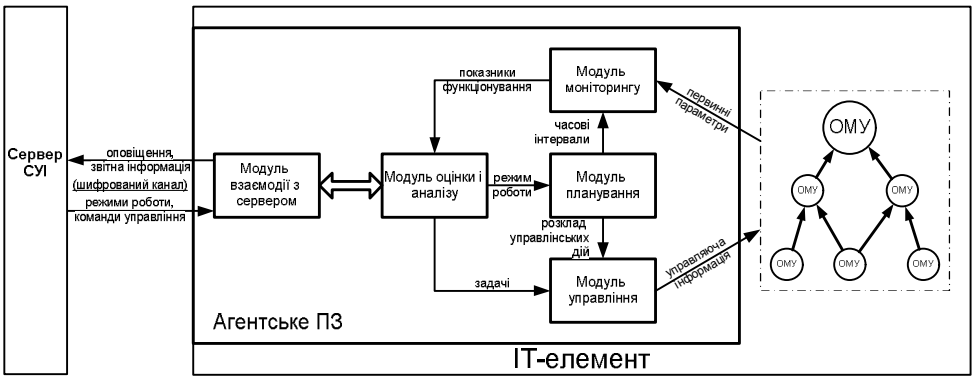



Рис. — Структура агентського ПЗ СУІ

СУІ розроблено в НТУУ „КПІ” із застосуванням технології .NET. Гнучкість агента забезпечують механізми атрибутів та рефлексії типів. Моніторинг використовує функції абстрактної бібліотеки, що дає можливість абстрагування при оцінці та аналізі стану ОМУ.

ЛІТЕРАТУРА

1. *Теленик С.Ф., Ролік О.І., Букасов М.М., Соколовський Р.Л.* Система управління інформаційно-телекомунікаційною системою корпоративної АСУ// Вісник НТУУ „КПІ”. Інформатика, управління та обчислювальна техніка. – К.: – 2006. – № 45.– С. 112 – 126.

2. *Ролик А.И., Соколовский Р.Л.* Распределение мобильных компонентов системы управления информационно-телекоммуникационной системой// Вісник НТУУ „КПІ”. Інформатика, управління та обчислювальна техніка.– К.: – 2007. – № 47. – С. 113 – 124.

3. *Ролик А.И., Глушко Е.В.* Анализ качества функционирования элементов информационно-телекоммуникационных систем// Вісник НТУУ „КПІ”. Інформатика, управління та обчислювальна техніка. – К.: – 2008. – № 48. – с. 113 – 120.

д.т.н. Романов О.І. (ВІТІ НТУУ„КПІ”)
к.т.н. Нестеренко М.М. (ВІТІ НТУУ„КПІ”)

# РОЗВИТОК СИСТЕМ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ НА БАЗІ СТАНДАРТІВ TMN

Впровадження сучасних технологій на мережі, що будуються знову або проходять модернізацію, їх інтеграція з існуючими мережами, високі вимоги до надійності функціонування в умовах різних дестабілізуючих факторів, виникнення локальних та загальномережевих перевантажень, вимагає пильної уваги до питань розробки, впровадження ефективних системи управління, як в нашій країні так і за кордоном. При цьому необхідно забезпечити сполучення мереж, які працюють на базі я від різних виробників, а також враховувати наявність різноманіття стандартних і нестандартних інтерфейсів та безліч інших чинників. Тому, завдання створення систем управління телекомунікаційними мережами – одне з найбільш складних і актуальних на сучасному етапі.

Найважливішою сучасної системи управління являється забезпечення оптимального використання мережі при виконанні вимог до якості обслуговування, рівня сервісу абонентів, надійності функціонування на базі наявної сукупності програмно-технічнихкомплексів та каналів інформаційної мережі.

Створеннясистем управління мережаминенеможливе без орієнтації на стандарти, як для управляючого програмного забезпечення, так мережевого використовується передовими компаніями .

Одним з найбільш розвинутих напрямів стандартизації являється концепція TMN (Telecommunications Management Network). даної концепції є опис інфраструктури структури мережі управління, яка націлена на забезпечення, щодо надання всього комплексу послуг і адміністрування телекомунікаційних мереж. В 1988 році були опубліковані рекомендації М.3010 „Принципи TMN, які поклали початок сімейству специфікацій, що регламентують різні аспекти управління мережами зв’язку.
На сьогоднішній день основним органом, що займається стандартизацією в області TMN, є Міжнародний союз електрозв’язку (ITU-T). При чому, основні документи що мають відношення до TMN, ITU-T згрупував в так звану М-множину.

Крім того, представлений стандарт надає розробникам велику свободу у виборі конкретних конфігурацій. Саме це дозволяє створювати структури TMN, призначені для управління різними мережами зв’язку. Спочатку концепція TMN була застосована до мереж SDH, згодом з’явилися специфікації, орієнтовані на інші телекомунікаційні технології такі, як B - ISDN, ATM, SS7 і так далі.

Стандарти TMN передбачають декілька видів моделей, що дозволяють давати їх опис як на фізичному, так і на логічному рівні.

Для передачі адміністративної інформації між інтерфейсами в рекомендаціях ITU-T і стандартах ISO передбачаються протоколи двох типів – комунікаційні і такі, що відповідають за управління. В якості перших в TMN використовуються стандартні протоколи OSI, а саме протоколи ISDN і системи сигналізації № 7 (SS7). З числа протоколів, що займаються управлінням, вибрані Common Management Information Protocol (CMIP, ITU-T Recommendation X.711) і File Transfer and Management Protocol (FTAM, стандарт ISO 8571). Вказані протоколи організовані в стеки для підтримки конкретних інтерфейсів TMN.

На теперішній час, проводиться активна робота по застосуваннюархітектури TMN для управління різними типами мереж та мережевого обладнання. Дана обставина обумовлює інтеграцію інтерфейсів TMN у всі види нового .

Аналіз сучасних розробок та досягнень, які ведуться в напрямку створення систем управління телекомунікаційних мережами, вказує на той факт що TMNявляєтьсяодним найбільш перспективним в даній галузі.

к.т.н. Рябцев В. В. (НАОУ)
к.т.н. Субач І. Ю. (ВІТІ НТУУ „КПІ”)

# СТРУКТУРА ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ ОСВІТИ ТА ПІДГОТОВКИ

Аналіз сучасного стану розвитку теорії та практики збройної боротьби дозволяє зробити висновок про наявність чіткої тенденції до зростання питомої ваги її інтелектуальної складової [1]. Відповідно зростають вимоги до кваліфікації усіх категорій військових фахівців Збройних Сил України (ЗСУ): від обслуговуючого персоналу озброєння (військової техніки) до посадових осіб органів військового управління. У таких умовах, враховуючи орієнтовану на ресурси модель управління у ЗСУ, людський ресурс, разом із такими традиційними видами як фінансові, матеріально-технічні, інформаційні ресурси, набуває критичної важливості. При цьому основними характеристиками даного типу ресурсу стають не кількісні, а якісні. Найбільш важливою з них в сучасних умовах, без сумніву, є компетентність персоналу. У той же час, практика свідчить про значні проблеми у галузі управління кадрами ЗСУ. Серед них є такі: масові звільнення молодих фахівців, фахівців, які мають досвід участі у миротворчих операціях, міжнародних навчаннях, проходили навчання за кордоном, призначення випускників не за спеціальністю, на посади, які не відповідають рівню їх освіти, а іноді й на посади, що зайняті іншими офіцерами. Основними причинами такої ситуації є: відсутність чіткої, прозорої системи управління кар’єрою військовослужбовців, недостатній рівень взаємодії між системою військової освіти

Виходячи з вищезазначеного, виникає завдання – створення принципово нової системи кадрового менеджменту у ЗСУ, технічною основою якої має стати інтелектуальна система управління якістю освіти та підготовки. Методологічною основою даної системи має стати міждисциплінарна науково-практична концепція „Управління знаннями” (*Knowledge Management*), яка базується на поняттях „компетенції” та „компетентності” [2, 3].

Основними функціональними модулями системи мають стати такі.

1. Інтерфейсний модуль, призначений для забезпечення таких трьох основних режимів роботи інтелектуальної системи.

*Пошуку кандидатів на вакантні посади*. Використовується кадровими органами при вирішенні відповідної задачі.

*Формування кадрової перспективи*. Призначений для формування двох основних документів у відповідності до компетенції кадрових органів:

План кадрових переміщень; План перепідготовки.

*Формування індивідуальної перспективи.* Призначений для визначення кожним військовослужбовцем (працівником ЗСУ) навчальних модулів, курсів, програм підготовки (перепідготовки), необхідних для просування на конкретну посаду.

2. База даних навчальних модулів, яка містить такі дані: назва модуля; освітній рівень; компетенції по модулю у вигляді набору: „знання – вміння – навички”, з необхідною передісторією (модулі, вивчення яких є обов’язковою умовою початку вивчення даного модуля) по кожній компоненті тріади; термін „придатності” одержаних знань /вмінь/ навичок.

3. База даних посад, яка містить: перелік усіх посад у ЗСУ з відповідними паспортами (паспорти мають містити дані про ключові компетенції, необхідний рівень компетентності за ними, відносну вагу кожної з ключових компетенцій).

4. База даних особового складу (у частині, що стосується освіти, підготовки та перепідготовки): коли, які навчальні модулі вивчав, з яким результатом; професійні компетенції (набуті протягом служби) та рівень володіння ними.

5. Модуль встановлення відповідності кандидата посаді. Перевіряє кандидата на посаду та відповідність посаді. Можливі результати роботи модуля:

**ТАК** без перепідготовки (лакуни покриваються за рахунок самостійної підготовки).

**ТАК** з обов'язковою перепідготовкою (формується індивідуальна траєкторія перепідготовки).

**НІ** без зміни базової освіти.

6. Інтелектуальний модуль формування індивідуальної траєкторії навчання. Він має реалізувати такі основні функції.

*Заповнення лакун* („білих плям" у підготовці). Формується доповнення до профілю кандидата (набір компетенцій, які необхідно додати, щоб досягти критерію відповідності).

*Формування потрібної траєкторії.* Потрібним компетенціям ставляться у відповідність навчальні модулі. Формується їх послідовність. Перевіряється наявність таких, що забезпечують модулів у профілі кандидата. В разі потреби, до траєкторії вносяться забезпечуючи модулі в їх логічній послідовності.

*Формування індивідуальної траєкторії.* Потрібна траєкторія співвідноситься з існуючими програмами підготовки. Формується послідовність проходження курсів. В разі повної або часткової неможливості забезпечити індивідуальну траєкторію навчальними ресурсами Міністерства оборони України, генеруються пропозиції щодо використання ресурсів закордонних курсів або курсів цивільних установ.

У результаті роботи модуля формуються Пропозиції до Плану перепідготовки.

7. Інтелектуальний модуль корекції Плану кадрових переміщень. Модуль, фактично, представляє собою базу знань, яка дозволяє по кожній парі: „особа – посада" зробити остаточний висновок:

**ТАК** без перепідготовки.

**ТАК** з перепідготовкою за індивідуальною траєкторію навчання.

**ТАК** з перепідготовкою за індивідуальною траєкторію навчання, але з перенесенням термінів через відсутність можливості пройти усю траєкторію вчасно або з проходженням частини траєкторії після призначення на посаду.

**НІ** через кардинальну невідповідність профілю кандидата профілю посади.

Результатом роботи модуля має стати: скорегований План кадрових переміщень.

8. Інтелектуальний модуль управління кадровим резервом. Основними функціями модулю має бути:

*Визначення найчастіше потрібних навчальних модулів* і формування пропозицій щодо корегування ВВНЗ або створення / корегування планів курсової підготовки;

*Визначення найбільш доцільних напрямів подальшої підготовки* (для особового складу), а в залежності від цього – курсів, проходження яких розширить інваріантність подальшого використання персоналу ЗСУ.

Задача розроблення інтелектуальної системи управління якістю освіти та підготовки вимагає скоординованих зусиль фахівців у різних предметних галузях: управління кадрами, організації освітньої діяльності, управління бойовою (оперативною) підготовкою, сучасних інформаційних технологій, у тому числі – знання орієнтованих. Створення запропонованої системи дозволить вирішувати в комплексі завдання, покладені на новостворену у ЗСУ систему кадрового менеджменту: управління кар'єрою персоналу; його професійної підготовки; соціального забезпечення; адаптації до цивільного життя при звільненні [4].

ЛІТЕРАТУРА

1. *Пермяков О. Ю.* Застосування сучасних інформаційних технологій в збройній боротьбі. Сучасні інформаційні технології у сфері безпеки та оборони. – 2008. – № 2 (2). – С. 69 – 74.

2. *Гапоненко А. Л.* Управление знаниями. – М.: ИПК госслужбы, 2001. – 52 с.

3. *Рябцев В. В.* Управління знаннями в Збройних Силах. Сучасні інформаційні технології у сфері безпеки та оборони. – 2008. – № 2 (2). – С. 47 – 50.

4. *Концепція* кадрової політики у Збройних Силах України. Затверджена наказом Міністра оборони України № 659 від 27 листопада 2007 р.

к.т.н. Савісько П.А. (НАОУ)

# ОПЕРАТИВНО – ТАКТИЧНІ ПРИНЦИПИ ПОБУДОВИ АСУВ

АСУВ Збройних Сил України – сукупність людського інтелекту, інформаційних ресурсів, сучасних інформаційних технологій та засобів інформатизації, об’єднаних у телекомунікаційні і комп'ютерні мережі.

Глобальною метою функціонування АСУВ є ефективне інформаційне і інтелектуальне (аналітичне) забезпечення територіально розділених функціонально взаємозалежних груп посадових осіб ОУ в процесі вироблення ними управлінських рішень.

Поняття „ефективне забезпечення” визначає направленість АСУВ, у – перших, на функціонування відповідно до пропонованих (з боку посадових осіб ОУ) вимог, у – других, на рішення даної проблеми в аспекті максимального використання потенційних можливостей АСУВ.

Слід зазначити, що сформульована глобальна мета функціонування АСУВ є, власне кажучи, і її основним (в аспекті глобального досягнення мети) призначенням.

Принципи побудови АСУВ розглядаються з урахуванням особливостей функціонування ОУ ЗСУ і специфіки інформаційних технологій.

Принцип постійної готовності. Постійна готовність АСУВ до застосування випливає з принципу постійної бойової готовності органів управління військами (силами).

АСУВ є організаційно-технічною системою, за допомогою якої здійснюється інформаційно-аналітичне забезпечення діяльності органів управління військами (силами).

Постійна готовність АСУВ до застосування припускає наявності в її базах даних повної, достовірний і точної інформації (даних), яка адекватно відбиває бойовий стан, бойову і мобілізаційну готовність військ (сил), умов виконання бойових задач.

Постійна готовність АСУВ до застосування досягається:

безперервністю і своєчасністю збору й обробки даних;

організацією надійного збереження даних;

своєчасністю відновлення даних;

забезпеченням цілісності даних;

високим рівнем підготовки фахівців, що обслуговують АСУВ і кінцевих користувачів;

проведенням постійного і безупинного контролю функціонування системи АСУВ.

Принцип відповідності можливостей АСУВ організаційній структурі і бойовим можливостям військ (сил) і засобам, а також составу і структурі системи управління військами, тобто забезпечення єдності управління як по „вертикалі” – ієрархії ОУ військами (силами), так і по „горизонталі” (створення відповідних контурів автоматизованого управління).

Реалізація даного принципу передбачає створення локальних обчислювальних мереж ОУ по всім рівням ієрархії та об’єднання їх засобами телекомунікації в АСУВ ЗСУ (корпоративну обчислювальну мережу).

Цей принцип відображає еволюційний характер розвитку системи управління В свою чергу упровадження автоматизованого управління чинить обернений вплив на організаційну структуру військ, органів і пунктів управління.

Принцип збереження провідної ролі командуючого (командира) в процесах управління військами (силами) і бойовими засобами.

Цей принцип відображає необхідність розробки не автоматичних, а автоматизованих АСУВ. Прийняття рішення, вибір оптимального (раціонального) варіанту рішення на бойові дії із усіх можливих, завжди повинен виконувати командуючий (командир)

Принцип забезпечення зручності роботи посадових осіб органів і ПУ на засобах автоматизації. Цей принцип відображає необхідність створення умов, які забезпечують

максимальну ефективність інтелектуальної діяльності посадових осіб при роботі на засобах автоматизації.

Принцип збереження основних алгоритмів роботи командирів, штабів, органів і ПУ при упровадженні АСУВ.

Цей принцип передбачає забезпечення спадкоємності методів роботи посадових осіб органів і ПУ в різних ланках управління при переході від неавтоматизованого способу управління військами (силами) і засобами до автоматизованого, розумну уніфікацію алгоритмів їх роботи на автоматизованих робочих місцях.

Принцип розумного сполучення централізованого і децентралізованого способу управління, можливості скорого переходу від одного до другого, а також від автоматизованого управління до неавтоматизованого і навпаки.

Принцип забезпечення стійкості, адаптації і самоорганізації АСУВ у відповідності до змін внутрішніх і зовнішніх параметрів її функціонування.

Цей принцип передбачає створення умов застосування основної, дублюючої і резервної систем АСУВ; можливість управління військами (силами) і засобами через інстанцію (а в деяких випадках і через декілька інстанцій); можливість перерозподілу функцій управління між ПУ.

Принцип адаптивності вимагає створення АСУВ, які володіють можливостями до змін своїх параметрів при зміні умов її застосування. в залежності від характеристик зовнішнього середовища. Така зміна обумовлена об'єктивно існуючою частковою невизначеністю бойової обстановки.

Прикладом адаптивності є поєднання в АСУ Повітряних Сил Збройних Сил України централізованого управління з наданням права самостійного ведення бойових дій з’єднанням, частинам і підрозділам родів військ. Адаптивне поводження системи підвищує її живучість і стійкість.

Принцип воєнно-економічної ефективності.

Принцип воєнно-економічної ефективності забезпечить досягнення раціонального співвідношення між витратами на розроблення, створення та впровадження АСУВ Збройних Сил України і цільовими ефектами, що одержуються в результаті її створення.

Принцип вимагає раціоналізувати капіталовкладення в засоби автоматизації, прогнозувати витрати і тривалість розроблення, науково планувати створення і виробництво АСУ в планах військового будівництва.

к.т.н Савісько П.А. (НАОУ)
к.пед.н Романюк І.М. (НАОУ)

# ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОГО ПРОЦЕСУ УПРАВЛІННЯ НА ОСНОВІ НОВИХ (СУЧАСНИХ) ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

У системі управління військами процес вироблення рішень характеризується як інформаційний процес. Від оптимального розподілу функцій між органами управління, їх інформаційного забезпечення, можливості оперативної оцінки обстановки залежить обґрунтованість і ефективність рішень, що приймаються.

Причини, які обумовлюють недостатність інформаційного забезпечення органів управління:

– великий обсяг інформації, що обробляється органами управління;

– велика різноманітність форм представлення інформації;

– великі витрати часу на збір і обробку початкової інформації для підготовки і прийняття рішення, доведення їх до військ, а також представлення доповідей до вищих органів управління.

Основною метою інформатизації органів і пунктів управління ЗСУ є створення і підтримка необхідного рівня інформаційно-аналітичного забезпечення рішення різних функціональних задач в інтересах підвищення бойової готовності військ і управління ними під час підготовки і в ході бойових дій.

Інформатизація органів і пунктів – теорія і практика розробки і широкомасштабного впровадження нормативно-правових документів і сучасних інформаційних технологій, що реалізовують функції і процедури збору, передачі, обробки, зберігання і доведення інформації органам управління в мирний і військовий час.

Таким чином, одним із основних напрямків підвищення ефективності управління військами (силами) є підвищення ефективності інформаційно-аналітичне забезпечення (ІАЗ) процесів управління за рахунок впровадження в систему управління (АСУВ) ЗСУ нових інформаційних технологій (НІТ), орієнтованої на активну участь посадових осіб ОУ в процеси оброблення інформації, що дає змогу максимально приблизити посадових осіб ОУ до інформаційних ресурсів, а також до самого процесу розв’язування інформаційно-управлінських задач.

**Інформаційно-аналітичне забезпечення (ІАЗ) – це сукупність інформаційних продуктів, ресурсів та послуг, що надаються для забезпечення інформаційних потреб керівному складу органів управління та система підтримки прийняття рішень їх управлінської діяльності**. Тобто, поняття ІАЗ безпосередньо зв‘язане з процесом управління, незалежно від того, яким і на якій основі воно здійснюється: за допомогою неавтоматизованої або автоматизованої системи управління військами.

Застосування НІТ забезпечить наступні можливості в організації інформаційного процесу управління в ЗСУ:

1. Комплексну і всебічну інтелектуальну підтримку діяльності посадових осіб ОУ. Дані технології можуть забезпечити: автоматизацію процесів семантичної обробки документальної інформації (смисловий пошук, реферування, анотування, смислову класифікацію, виділення фактографічних даних з тексту документа й ін.). Як показує аналіз, в ОУ значна частина (до 80 %) складає переробка документальної інформації; автоматизацію семантичної обробки графічної аудіо і відеоінформації, включаючи розпізнавання об’єктів, представленими графічними образами або відео зображеннями і аналіз їхніх властивостей; виявлення можливих варіантів взаємодії об’єктів і на основі цього – розпізнавання й аналіз ситуацій; прогнозування за допомогою моделювання процесів розвитку ситуацій, зв’язаних як з бойовими діями, так і з іншими видами діяльності військ; генерацію раціональних варіантів рішень на основі бази знань.

2. Роботу посадових осіб у режимі маніпулювання не стільки даними, скільки знаннями. Посадові особи мають можливість „бачити” за допомогою засобів виводу (екран, принтер) і діяти шляхом вводу (клавіатура, сканер тощо), а не тільки „знати” і „пам’ятати”;

3. Наскрізну інформаційно-інтелектуальну підтримку процесу вироблення рішення на всіх етапах управління на основі інтегрованого БД, яка передбачає єдину уніфіковану форму представлення, зберігання, пошуку, відображення, відновлення та захисту даних;

4. „Електронний документообіг” та перехід до безпаперової технології. Основним принципом безпаперової технології є наявність на машинних носіях усіх необхідних даних для складання документів і можливість їх автоматизованого використання на робочих місцях посадових осіб ОУ. При цьому забезпечується їх друкування або відображення на відеоекранах у різноманітних формах екранного подання. Слід зазначити, що багато посадових осіб ОУ працює не безпосередньо з первинними документами, а з окремими наборами даних, необхідних для виконання конкретних функцій управління. При безпаперовій технології ці дані можуть бути частиною первинного документа, можуть формуватися з різних документів, доповнюватися розрахунками та довідковими показниками, виводитися на екран дисплея у формі електронної таблиці, діаграми тощо. Такий рівень безпаперової технології притаманний локальним мережам ОУ і добре поєднується з технологією розподіленої обробки даних (одноразове введення даних та багаторазове використання їх різними посадовими особами мережі ОУ).

**Основна перевага безпаперової технології полягає не стільки в підвищенні продуктивності праці посадових осіб ОУ та якості документів, скільки у формуванні на машинних носіях даних, що описують предметну область в реальному масштабі часу. Саме це є визначним з позицій можливості інформувати різних посадових осіб ОУ для оперативного управління військами (силами).**

1. Інтерактивний (діалоговий) режим „рішення задач” управління з великими можливостями для посадових осіб впливати на цей процес;

2. Автоматичну інтерпретацію інформації (у тому числі неповної, нечіткої і суперечливої інформації);

3. Автоматичне в реальному часі і просторі перетворення змісту (семантики і прагматики) інформації, тісно і взаємозалежно з інтерактивним режимом „рішення задач” управління;

4. Візуалізацію і девізуалізацію інформації при різних формах і способах її перетворення;

5. Мультимедіа, мовний і відеоінформаційний супровід процесу „рішення задач„ від моменту одержання й аналізу вихідних даних і кінчаючи представленням результатів інтерпретації;

6. Графічне і геоінформаційне інтелектуальне забезпечення процесів управління. Сутність інтелектуалізації геоінформаційних систем (ГІС). До теперішнього часу створено досить великий ряд ГІС. Ці системи відрізняються друг від друга складом і рівнем реалізації функцій по роботі з електронною картою і по формуванню і відображенню графічної інформації на ній.

Однак якщо говорити про інтелектуалізацію обробки графічної обстановки на карті, те першим кроком тут повинний бути перехід від чисто візуального відображення об’єктів до формування й обробки обстановки в цілому, як сукупності семантично взаємозалежних об’єктів з урахуванням їх властивостей і характеристик. Це вимагає створення ГІС – додатків, орієнтованих на військову предметну область, тобто враховуючих не тільки склад і класифікацію умовних знаків, характерних для даної предметної області, але і її семантику (наприклад, формування із сукупності військових об’єктів елементів бойових порядків і наступне маніпулювання ними, облік нормативів взаємного розташування об’єктів, а також обмежень можливостей переміщення об’єктів на місцевості , що задаються, й ін.).

к.т.н. Самойлов І.В. (ВІТІ НТУУ ,,КПІ”)
к.т.н. Кокотов О.В. (НТУУ ,,КПІ”)

# ВИКОРИСТАННЯ ЕКСПЕРТНИХ ПАРНИХ ПОРІВНЯНЬ ДЛЯ ПОБУДОВИ НЕЧІТКИХ ВІДНОШЕНЬ ІНТЕРВАЛЬНОГО ТИПУ В СИСТЕМАХ ДІАГНОСТИКИ

Одним з основних факторів використання експертних систем в технічній діагностиці є можливість збереження та подальшого застосування унікального досвіду експертів-діагностів. Необхідною умовою розв’язання задач діагностики є встановлення залежності „причини-наслідки”. У процесі побудови такої залежності суттєву роль відіграє наявність експертних знань про типові несправності та їх ознаки, які часто надаються в нечіткій формі. Тому моделювання причинно-наслідкових зв’язків здійснюється із застосуванням теорії нечіткої логіки. Модель системи діагностики будується на основі композиційного правила виведення Заде [1] – $B=A\circ R$, в якому носієм діагностичної інформації є матриця $R$ нечітких відношень „причини-наслідки”, що зв’язує вектор мір значимості причин $A$ і вектор мір значимості наслідків $B$.

Будемо вважати відомими: $D = \{d_1, d_2, \ldots, d_n\}$ – множина причин, які підлягають порівнянню з точки зору впливу на виникнення наслідків; $S = \{s_1, s_2, \ldots, s_m\}$ – множина наслідків, які означають зміни кількісних або якісних параметрів стану об’єкта.

Необхідно побудувати нечіткі відношення $R \subset D \times S$, тобто необхідно оцінити міру впливу кожної з причин $d_i$, $i=\overline{1, n}$, на виникнення кожного з наслідків $s_j$, $j=\overline{1, m}$.

Для вирішення цієї задачі згідно [2] пропонується розглядати наслідки як нечіткі множини, що задані на універсальних множинах причин та визначати ступені належності нечітких множин на основі експертної інформації про парні порівняння причин за допомогою 9-ти бальної шкали Сааті. Перевага такого підходу полягає в тому, що він пристосований як для кількісних, так і до якісних параметрів стану об’єкта. Однак використання модифікованого методу парних порівнянь Сааті дозволяє отримувати ступені належності у вигляді числа в діапазоні [0, 1], тобто цій метод дозволяє будувати точні нечіткі відношення, які не спроможні моделювати невизначеність. Тому пропонується метод побудови нечітких відношень інтервального типу в умовах невизначеності. При цьому можуть бути враховані такі джерела невизначеності, як неоднозначність порівняльних оцінок і невизначеність через розбіжність в наслідкових частинах експертних тверджень щодо вибору діапазону оцінок.

Запропонований експертний метод побудови нечітких відношень дозволяє оперувати з інтервальними порівняльними оцінками шкали Сааті і враховувати розбіжності експертів при виборі порівняльної оцінки за рахунок побудови гістограми порівняльних оцінок та їх осереднення.

ЛІТЕРАТУРА

1. *Заде Л.* Понятие лингвистической переменной и её применение к принятию приближенных решений. – М.: Мир, 1976. – 167 с.

2. *Rotshtein A.* Modification of Saaty Method for the Construction of Fuzzy Set Membership Function. FUZZY’97 – Int. Conf. “Fuzzy Logic and Its Applications” in: Zichron, Israel. – 1997. – pp. 125 – 130.

Сівківська А.П.(ІТС НТУУ „КПІ”)
к.т.н. Ладик О.І.( ІТС НТУУ „КПІ”)

# РОЗВИТОК ТЕХНОЛОГІЇ ЧЕТВЕРТОГО ПОКОЛІННЯ СТІЛЬНИКОВОГО ЗВ’ЯЗКУ

Головна відмінність мереж четвертого покоління від попереднього полягає в тому, що технологія 4G повністю заснована на протоколах пакетної передачі даних, у той час як 3G поєднує в собі як передачу голосового трафіку, так і пакетів даних.

4G – четверте покоління мобільного зв’язку, що характеризується високою швидкістю передачі даних і підвищеною якістю голосового зв’язку.

До четвертого покоління відносяться технології, що дозволяють здійснювати передачу да них зі швидкістю, що перевищує 100 мбіт/с. Прикладами технологій 4G є Wi-Fi і WiMax, що мають теоретичну межу швидкості передачі до 1 Гбіт/с. Для порівняння максимальна швидкість передачі через GSM (2G) становить 240 кбіт/с, а в 3G – близько 10 мбіт/с.

Технологія 4G заснований на протоколах пакетної передачі даних. Для пересилання даних використовується протокол IPv6. Для передачі даних використовуються частоти 40 і 60 GHz. Для підвищення завадостійкості планують застосовувати адаптивні антени, які зможуть підлаштовуватися під конкретну базову станцію.

Міжнародна спілка телекомунікацій визначає технологію 4G як технологію безпровідної комунікації, яка дозволяє досягти швидкості передачі даних до 1 Гбіт/с в умовах руху джерела або приймача і до 100 Мбіт/с в умовах обміну даними між двома мобільними терміналами. Пересилання даних в 4G по протоколу помітно полегшує роботу мереж, особливо якщо вони різних типів.

Введення в експлуатацію мереж 4G потребує розв’язанню деяких проблем.

По-перше, на ринку немає абонентських пристроїв. Такі телефони, якщо б існували, споживали б надто багато енергії і не могли б довго працювати на акумуляторах (зараз подібні проблеми є і в 3G-пристроїв).

По-друге, швидкісний доступ в Інтернет і відеосервіси зажадають великих за розміром та більш якісних дисплеїв, ніж ті, які встановлюються в телефони зараз.

Але головна проблема все ж носить принципово інший характер. Справа в тому, що капіталовкладення у розгортання мереж четвертого покоління повинні бути набагато більшими, ніж у 2G і навіть в 3G. Тим часом, інвестори не впевнені в належної економічної віддачі від 4G-проектів. До того ж, деякі виробники пропонують „схрестити” 4G і безпровідні широкосмугові мережі. У різних ситуаціях користувач буде мати можливість вибирати найбільш відповідні способи підключення.

ЛІТЕРАТУРА

1. *Уайлі Дж.* Новітні безпровідні мережі. 4G технології. Уайлі, 2007 – 851с.
2. *Бакланов И.Г.* NGN: принципы построения и организации. М:Эко-Трендз, 2008 – 399с.
3. http://itc.ua/.

Сілко О.В. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ОЦІНКИ ЕФЕКТИВНОСТІ МОДУЛЬНОЇ ПОБУДОВИ КОМПЛЕКСІВ ЗАСОБІВ АВТОМАТИЗАЦІЇ РАДІОТЕХНІЧНИХ ПІДРОЗДІЛІВ ПОВІТРЯНИХ СИЛ ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз сучасної збройної боротьби та вимог, які висуваються до комплексів засобів автоматизації (КЗА) командних пунктів (КП) радіотехнічних підрозділів Повітряних Сил ЗС України [1], доводить необхідність введення до структури АСУ модульного принципу побудови техніки не лише відносно елементів, але й щодо системи озброєння в цілому – це дозволить провести уніфікацію озброєння та досягти найбільшого приросту (відносних одиниць) економічної ефективності. Тому, для покращення наукового обґрунтування планів, пов’язаних з розвитком автоматизованої інформаційної системи радіотехнічних підрозділів Повітряних Сил ЗС України на базі типових обчислювальних модулів (ТОМ), необхідно проводити оцінку застосування різних конструкторсько-технологічних рішень ТОМ при створенні уніфікованих модульних КЗА.

Виходячи з цього, виникає завдання – визначити вплив технічних характеристик ТОМ на пропускну спроможність КЗА, що дасть змогу кількісно оцінити приріст ефективності оснащення КП радіотехнічних підрозділів уніфікованими модульними КЗА.

Для рішення цієї задачі застосовано методику з наступною послідовністю дій:

побудова вихідної множини технічних характеристик ТОМ [2];

вибір технічних характеристик КЗА, який знаходиться на озброєнні КП відповідного рівня ієрархії та обчислення показника ефективності оснащення КП засобами автоматизації через пропускну спроможність;

визначення варіанта оснащення КП комплексом засобів автоматизації на основі типових обчислювальних модулів, який забезпечує найбільший приріст ефективності.

Під час визначення варіанта оснащення КП радіотехнічних підрозділів уніфікованими модульними КЗА вирішується багатокритеріальна задача, яка відноситься до класу багатокритеріальних детермінованих задач вибору рішень великого розміру. Для її рішення пропонується застосувати евристичний алгоритм, який дозволяє знайти квазіоптимальне рішення.

Таким чином, використання запропонованої методики дозволить на етапі вироблення обрису уніфікованого модульного КЗА:

по-перше, порівняти вимоги до пропускної спроможності уніфікованих модульних КЗА різних рівнів ієрархії;

по-друге, оцінити вплив можливих конструкторсько-технологічних рішень при створенні типового обчислювального модуля на тактичний показник КП радіотехнічного підрозділу – „пропускну спроможність” [3].

На основі наведених міркувань розроблена програмна реалізація методик оцінки ефективності модульної побудови КЗА та розглянуто конкретний приклад практичного застосування методики.

ЛІТЕРАТУРА

6. *Нечхаев С.М., Савков П.А., Ляхов М.О.* Можливості комплексів засобів автоматизації „Ореанда” для автоматизації задач управління у Повітряних силах Збройних Сил України. Збірник наукових праць ВІКНУ ім. Тараса Шевченка. – 2007. – № 8. – С. 120 – 123.

7. *Сілко О.В.* Кореляційно-регресійний аналіз залежності техніко-економічних показників обчислювальних модуля від його параметрів. Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2009 р. – № 1. – С. 12 – 15.

8. *Торопчин А.Я, Романенко І.О., Даник Ю.Г, Пащенко Р.Е.* та ін. Довідник з протиповітряної оборони. / – К.: МО України. – Х.: ХВУ, 2003. – 368 с.

к.т.н. Слотвінська Л. І. (ВІТІ НТУУ „КПІ”)

# ЗАХИСТ ПОЛІГРАФІЧНОЇ ПРОДУКЦІЇ ТИСНЕННЯМ

Одним із етапів виготовлення поліграфічної продукції при виконанні якого формуються елементи захисту є брошурувально-палітурний процес (або процес післядрукарської обробки).

Вагомими елементами захисту при виготовленні аналогових бланків документів на цьому етапі є такі, що вносяться у виріб при проведені операції тиснення.

Тиснення може бути безфарбовим і з використанням фольги – спеціального багатошарового поліграфічного матеріалу який є проміжним носієм зображення.

Тиснення безфарбове – це одержання на задруковуваних і незадруковуваних ділянках бланків документів рельєфного, безбарвного зображення.

Тиснення фольгою – це одержання на задруковуваних і незадруковуваних ділянках бланків документів рельєфного кольорового зображення, яке може бути звичайним, блискучим, голографічним в залежності від виду і марки фольги.

Більші можливості щодо захисту відбитків тисненням має голографічна фольга, оскільки відтворити голографічне зображення при спробі фальсифікації важко як з фізичної точки зору, так і з матеріальної. Крім того, голографічна фольга містить голографічне зображення в шарі лаку. При припресуванні фольги на документ лаковий шар переходить на поверхню документа і, при спробі відділити його від основи і перенести на інший носій (документ), руйнується.

Голограми на фользі наносяться на поліграфічну продукцію безпосередньо в ході виробництва. Тиснення фольгою є традиційною поліграфічною технологією і легко виконується при виконанні брошурувально-палітурних процесів.

Метою роботи було проведення аналізу видів поліграфічної голографічної фольги, фірм-виробників та технологій нанесення на бланки документів зображень з допомогою голографічної фольги.

Виготовляють голографічну фольгу спеціалізовані вітчизняні та закордонні підприємства. Це вітчизняні підприємства – спеціалізоване підприємство ГОЛОГРАФІЯ, ООО Київголографія, НВП СПЕКЛ, НТЦ ОПТРОНІКС, НТП Львівські захисні технології, відома в світі фірма Leonard KURZ (Німеччина), концерн „Российские защитые технологи” та деякі інші.

Як правило, голографічна фольга має двомірні та тримірні голографічні зображення, цифрові та комбіновані (одержані методом комбінації різних технологій) голограми. Голографічні зображення можуть додатково мати захисні елементи у вигляді мікротексту, сіток, прихованих рисунків і тексту, нумерації та ін.

Розглянуто марки голографічної фольги, їх властивості, характеристики та способи нанесення.

Проведено аналіз особливостей, переваг і недоліків способу холодного тиснення голографічною фольгою.

Порівняно з процесом гарячого тиснення процес холодного має більш високу швидкість тиснення, не потребує окремого устаткування, для обробки можуть використовуватись матеріали, чутливі до дії температури, а також є можливість растрового друку. Разом з тим, голографічна фольга холодного тиснення дорожче фольги гарячого тиснення із-за необхідності дотримання оптимальної адгезії розділових шарів – при тисненні лаковий шар повинен триматися на основі, а при переведенні зображення на задруковувану поверхню – звільняти його.

На основі аналізу джерел науково-технічної інформації можна констатувати, що процеси захисту з допомогою голографічної фольги розвиваються інтенсивно як у напрямку застосування технології холодного тиснення, так і у напрямку використанням складних типів голограм та додаткових ефектів.

к.т.н. Слюсар І.І. (ВІТІ НТУУ „КПІ”)
д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗСУ)
к.т.н. Зінченко А.О. (НАОУ)

# ШЛЯХИ ПІДВИЩЕННЯ ПОТЕНЦІЙНИХ МОЖЛИВОСТЕЙ СИСТЕМ ЗВ’ЯЗКУ З ЦИФРОВИМ ДІАГРАМОУТВОРЕННЯМ

В умовах існуючої геополітичної обстановки все більше значення приділяється веденню інформаційної боротьби та засобам телекомунікації. Для забезпечення відповідності сучасним тенденціям розвитку систем зв’язку необхідно використовувати новітні технології, які спрямовані на підвищення показників стійкості, мобільності, пропускної спроможності, та інших.

Однією з них є технологія цифрового діаграмоутворення (ЦДУ), що впроваджується у розвинутих країнах світу як для військової сфери так й для загального призначення [1]. Використання зазначеної технології значно розширює функціональні можливості систем зв’язку в цілому [2]. При цьому розрядність і робочий діапазон частот сучасної номенклатури аналого-цифрових і цифро-аналогових перетворювачів забезпечують обробку сигналів на проміжній частоті з набагато більшою потенційною точністю в порівнянні з фазованими антенними решітками. Крім того, що існують технічні рішення дають можливість виконувати процедури багатокоординатної обробки інформації в реальному масштабі часу. Все це свідчить про перспективність технології ЦДУ на основі ЦАР.

Разом з тим, слід зазначити, що більшість зазначених розробок орієнтовано на реалізацію антенних систем з невеликим числом каналів. Це пов’язано з необхідністю узгодження можливостей апаратної частини системи зв’язку та вимог, що висуваються до цифрового сегмента стосовно темпів оцифровки сигналів і обсягам оброблюваної інформації. Як наслідок, досить актуальною є задача обґрунтування рекомендацій щодо підвищення потенційних можливостей систем зв’язку з ЦДУ за рахунок використання нових розробок в області схемотехніки ЦАР і удосконалених методів цифрової обробки сигналів.

В якості основних шляхів щодо підвищення потенційних можливостей систем зв’язку з ЦДУ можливо виділити наступні: орієнтація на схемотехніку гібридних (у тому числі й фокальних) ЦАР; застосування сигналів подвійної поляризації, методів неортогональної частотної дискретної модуляції, а також різних варіантів їхніх комбінацій; реалізація процедур додаткового стробування відліків аналого-цифрових перетворювачів, синтез антенних елементів ЦАР на основі фрактальних структур.

На даний час, технологія ЦДУ залишається предметом активних досліджень. Використання геометрії просторово-заповнюючих кривих підштовхнуло дослідників до застосування в антенних конструкціях аналогічних за властивостями об'єктів звичайної геометрії. В результаті подібних досліджень багатьом фрактальним рішенням вже протиставляються серпантинові та зигзагоподібні АЕ, що перевершують їх за низкою параметрів. Іншим напрямом пошуку є використання для синтезу АЕ ЦАР так званих генетичних алгоритмів оптимізації [3].

ЛИТЕРАТУРА

1. *Слюсар В.И.* Военная связь стран НАТО: проблемы современных технологий // Электроника: Наука, Технология, Бизнес. – 2008. – № 4. – С. 66 – 71.

2. *Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В.* Широкополосные беспроводные сети передачи информации / М.: Техносфера. – 2005. – С. 529 – 542.

3. *Слюсар В.И.* Синтез антенн на основе генетических алгоритмов // Первая миля. Last mile (Приложение к журналу „Электроника: наука, технология, бизнес”). – 2008. – № 6. – С. 16 – 23.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ ЗСУ)
к.т.н. Масесов М.О. (ВІТІ НТУУ „КПІ”)

# ВИМІРЮВАННЯ ХАРАКТЕРИСТИК РАДІОКАНАЛІВ MIMO ТА МУЛЬТИ-MIMO В ПРИЙМАЧАХ СТАНЦІЙ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Згідно сучасних концепцій ведення бойових дій, при побудові польової опорної мережі зв’язку для забезпечення потреб управління військами, суттєва роль відводиться новим базовим зразкам техніки та комплексним апаратним зв’язку. Зразки військової техніки, що прийняті на озброєння останнім часом, не тільки розширюють можливості по забезпеченню зв’язку та передачі інформації, але й корінним чином змінюють загальні принципи побудови системи зв’язку різних ланок управління [1].

Характерною особливістю нових та перспективних засобів зв’язку є використання сучасних технологій. Серед таких слід зазначити відому технологію *MIMO* – множинного входу множинного виходу, сутність застосування якої для побудови перспективних засобів зв’язку військового призначення вже представлена авторами в ряді публікацій [2, 3].

При передачі сигналів з використанням технологій *MIMO* та мульти-*MIMO* (система кількох кореспондентів з використанням каналів *MIMO* між ними) актуальною задачею залишається необхідність точного вимірювання характеристик радіоканалів, які позначаються матрицею $H$ розмірністю $M \times N$ [3]. Її елементи дорівнюють комплексним передавальним характеристикам між $M$ антенами передавача та $N$ антенами приймача. Найбільш відомі дві групи оцінки характеристик радіоканалів. Перша, так звана група „сліпих” методів, спирається на періодичне посилання спеціальних контрольних сигналів, а характеристики каналу визначаються на основі апріорно відомих статистичних характеристик [4]. Суттєвим недоліком першої групи є необхідність значного часу для виміру характеристик з достатньою точністю, що унеможливлює їх застосування в радіоканалах, що швидко змінюються, зокрема тропосферних, радіорелейних, тощо.

Більш розповсюджена друга група методів оцінки характеристик радіоканалу, що передбачає застосування тестувальних сигналів [4]. В них відомі пілот-сигнали посилаються на початку кожного блоку перед передачею інформаційних символів. Якщо ж елементи матриці каналу *MIMO* швидко змінюються у часі та залежать від частоти, то пілот-символи вставляються періодично між інформаційними символами під час передачі блоку. Це так звана модуляція, пов’язана з пілот-символами (*PSAM*).

Важливим параметром, що характеризує ефективність роботи системи *MIMO* або мульти-*MIMO,* є пропускна здатність, яка залежить від значень елементів матриці $H$, кількості просторових радіоканалів, відношення сигнал/шум та часу, що відводиться для передачі пілот-символів. Запропонований підхід придатний до застосування у перспективних тропосферних, супутникових, радіорелейних та станціях абонентського доступу з підтримкою технологій *MIMO* та мульти-*MIMO*. В подальшому будуть досліджені отримані для пропускної здатності аналітичні вирази шляхом математичного моделювання.

ЛІТЕРАТУРА

1. *Слюсар В.І., Тітов І.В., Карєв В.Г.* Концепція перспективної інформаційно-телекомунікаційної системи // Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення : доповіді та тези доповідей IV-ї наук.-техн. конференції, 22 – 23 лист. 2008 р.: доповідь. – К., 2008. – С. 76 – 79.

2 *Слюсар В.И.* Системы MIMO: принципы построения и обработка сигналов // Электроника: наука, технология, бизнес. – 2005. – № 10. – С. 52 – 59.

3. *Слюсар В.І., Масесов М.О.* Метод просторово-часового кодування сигналів тропосферного зв’язку на основі удосконаленої технології мульти-MIMO // Збірник наукових праць ВІТІ НТУУ „КПІ”. – 2009. – Вип. 1. – С. 132 – 136.

4. *Сюваткин В.С., Есипенко В.И., Ковалев И.П.* WiMAX – технология беспроводной связи: теоретические основы, стандарты, применение / СПб.: БХВ-Петербург, 2005. – 368 с.

д.т.н. Слюсар В.І. (ЦНДІ ОВТ)
Троцько О.О. (ВІТІ НТУУ „КПІ”)

# ОЦІНЮВАННЯ ВПЛИВУ ЕФЕКТУ ДОППЛЕРА НА ПРОПУСКНУ СПРОМОЖНІСТЬ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ З БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ

На сьогоднішній день основними телекомунікаційними задачами, вирішуваними за допомогою безпілотних літальних апаратів (БПЛА), є:

– забезпечення єдиної системи передачі даних спеціального призначення (силових міністерств, корпоративних утворень);

– забезпечення єдиного поля цифрового телевізійного та радіомовлення і мобільного зв’язку, доступу до мережі Інтернет;

– спостереження поверхні Землі в оптичному, ІЧ і радіолокаційному діапазонах хвиль, передача відповідних зображень в реальному масштабі часу.

На відміну від наземних засобів зв’язку система передачі даних на базі БПЛА є системою, що складається з мережі безпілотних літальних апаратів-ретрансляторів, яка безпосередньо забезпечує зв’язком стаціонарних і рухомих користувачів.

Під час проектування системи передачі даних на базі БПЛА необхідно провести оцінку її функціонування з урахуванням високих швидкостей літаків-ретрансляторів і впливу ефекту Допплера на розповсюдження радіохвиль. Останній призводить до того, що для відповідності вимогам надійності зв’язку необхідно збільшувати захисний інтервал OFDM-сигналу, а це супроводжується зростанням невикористаної області задіяного частотного діапазону і зниженням пропускної спроможності системи. Крім того, повинен зменшуватись порядок модуляції з переходом від квадратура-амплітудної модуляції (QAM) вищих порядків до QPSK. Отже, якщо не вжити запобіжних заходів, допплерівські зсуви піднесучих можуть викликати погіршення якості демодуляції OFDM-сигналів і часті відмови каналів зв’язку, що не дозволяє гарантувати якісне надання послуг.

Математичний розрахунок впливу ефекту Допплера зводиться до оцінки втрат корисного спектра при збільшенні захисних інтервалів OFDM-сигналів. Втрачений частотний ресурс без компенсації допплерівського зсуву визначається співвідношенням:

$$\Delta F_{Втр} = \Delta F_{З\text{доп}} - \Delta F_З , \qquad (1)$$

де $\Delta F_З = \sum_{i=1}^{n+1} \Delta f_З$ – загальна ширина спектра захисних інтервалів OFDM-сигналу без врахування ефекту Допплера, де $\Delta f_З$ – захисний інтервал OFDM-сигналу; $n$ – кількість підканалів у пакеті OFDM;

$\Delta F_{Зdop} = \sum_{i=1}^{n+1} \Delta f_{Зdop}$ – загальна ширина спектра захисних інтервалів OFDM-сигналу при врахуванні ефекту Допплера, де $\Delta f_{Зdop} = \Delta f_З + 2\Delta f_{dop}$, $\Delta f_{dop}$ – допплерівський частотний зсув, який розраховується за виразом:

$$\Delta f_{dop} = f_0 \frac{\sqrt{1 - \frac{V^2}{c^2}}}{1 + \frac{V}{c} cos\theta},$$

де $f_0$ – носійна частота OFDM-сигналу; $V$ – відносна швидкість руху БПЛА; $c$ – швидкість світла.

Для підвищення пропускної здатності в системах, що розглядаються, пропонується використовувати метод неортогональної частотної дискретної модуляції. В ньому частоти підканалів рознесені за частотою менше, ніж на ширину синтезованого при операції ШПФ частотного фільтра. Це дозволяє досить органічно врахувати допплерівський зсув частоти.

к.т.н. Сова О.Я. (ВІТІ НТУУ „КПІ”)
к.т.н. Жук О.В. (ВІТІ НТУУ „КПІ”)
Жук П.В. (ВІТІ НТУУ „КПІ”)

# ПРОБЛЕМА УПРАВЛІННЯ ПОТОКАМИ ДАНИХ У МОБІЛЬНИХ РАДІОМЕРЕЖАХ З ДИНАМІЧНОЮ ТОПОЛОГІЄЮ

Перспективи реформування і розвитку Збройних Сил України (ЗСУ) тісно пов’язані з впровадженням ефективної системи управління (СУ) військами (силами). У зв’язку з цим, одним з актуальних завдань реформування ЗСУ на період до 2011 року є створення багаторівневої мобільної компоненти (МК) тактичної ланки управління військами, основу якої складатимуть мобільні радіомережі (МР) загального користування, що будуються за технологією MANET (*Mobile Ad-Hoc Networks*). Специфіка завдань, що покладаються на функціонування сучасних телекомунікаційних мереж військового призначення, потребує виконання підвищених вимог до забезпечення доставки великих обсягів інформації з потрібною вірогідністю та оперативністю. Особливої актуальності набувають питання, пов’язані з виконанням зазначених вимог при передачі даних в МР, характерними особливостями яких є: короткочасність існування з’єднань (внаслідок швидкої зміни мережевої топології, мобільності вузлів комутації та впливу деструктивних дій в бойових умовах), різні типи трафіка (відео, мова, дані), неоднорідність її елементів (за енергетичним ресурсом та мобільністю), обмежена пропускна спроможність радіоканалів, значна розмірність (десятки, сотні та тисячі вузлів) і обмежена безпека. Крім того, підвищення вимог до якості передачі різних типів трафіка, робить їх залежними від нижніх рівнів моделі OSI. Більшість типів трафіка чутливі до перевантажень мережі, затримки та втрати пакетів з даними, що передаються в ній, а отже, вимагають застосування методів управління потоками даних, які б забезпечили їх повноцінну роботу в безпровідних мережах з динамічною топологією, до яких відносяться мобільні радіомережі. Існуючі методи управління потоками даних, що використовуються в провідних мережах зв’язку орієнтовані на статичні або квазістатичні умови їх функціонування і не можуть бути використані в МР через високу динаміку топології, характерну цим мережам. З іншого боку, важливість функцій, покладених на систему зв’язку та автоматизації управління військами, їх взаємозв’язок з питаннями національної безпеки держави, обумовлюють необхідність вирішення проблеми управління потоками даних на якісно новому рівні, що визначає її актуальність на сьогоднішній день. Механізм управління потоками даних і ресурсами являє собою множину операційних правил, згідно яких обробляються потоки даних (запитів, повідомлень, пакетів і т.п.). Ці правила повинні визначати маршрути проходження потоків даних, а також стратегії, алгоритми і дисципліни обслуговування у вузлах мережі; прогнозувати, запобігати та виключати перевантаження і блокування шляхом регулювання вхідного трафіка та управління розподілом буферної пам’яті. Управління потоками в мережах з комутацією пакетів має за мету запобігти зниженню ефективності мережі через перевантаження, а також забезпечити відповідність між пропускною спроможністю мережі і вхідним навантаженням. Розрізняють наступні рівні управління потоками даних:

1) міжвузловий рівень – на цьому рівні забезпечується управління потоком даних між двома сусідніми вузлами комутації з метою запобігання переповнення локальних буферів (канальний рівень моделі OSI);

2) рівень доступу до мережі – здійснюється обмеження вхідного потоку за результатами вимірювання внутрішнього навантаження мережі. Управління здійснюється між абонентами і вузлом комутації (мережевий рівень моделі OSI);

3) рівень „вузол комутації – джерело – вузол комутації – адресат”. Запобігає переповненню буферу вузла комутації-адресата (мережевий рівень моделі OSI);

4) рівень „процес-процес”. Запобігання переповненню буферів користувачів на рівні процесів (транспортний рівень моделі OSI). Відомо, що найпоширенішим серед сучасних

засобів, які забезпечують доставку даних у телекомунікаційних мережах з потрібною якістю обслуговування, є протокол TCP (*Transmission Control Protocol*). Він забезпечує виконання вимог щодо забезпечення високої вірогідності доставки інформації шляхом використання квитанцій (підтверджень від адресата) та повторних передач. Однак класичний протокол TCP має низку недоліків, які особливо відчутні при його використанні в мережах з динамічною топологією:

– при втраті сегмента розмір вікна передачі різко зменшується до мінімального значення (це приводить до зниження ефективності протоколу TCP в МР, де ймовірність втрати сегментів є високою);

– втрата сегмента розцінюється протоколом як така, що виникла внаслідок перевантаження мережі (втрати сегментів у мобільній радіомережі часто спричинені розривом каналів зв'язку через високу динаміку топології мережі, що вимагає пошуку та побудови нових маршрутів передачі, замість генерації повторних передач, як передбачено протоколом TCP);

– для визначення максимально можливого вікна передачі передбачено стрімке збільшення інтенсивності відправки сегментів, яке відбувається до втрати пакету (що приводить до сплесків навантаження в мережі, тобто до збільшення ймовірності втрати сегментів). З метою підвищення продуктивності протоколу TCP а також його адаптації до динамічного середовища мобільних радіомереж розроблено багато методів управління потоками даних (TCP *Vegas*, TCP *Reno*, *Random Early Detection* та ін.), які відрізняються один від одного обсягом управляючого впливу, параметром, який використовується в якості метрики контролю потоку та функціонуванням на рівнях моделі OSI. Однак, як показав проведений аналіз, існуючі методи орієнтовані на статичні або квазістатичні умови функціонування мереж зв'язку і не можуть бути застосовані в системі управління МК внаслідок низької оперативності адаптації до зміни топології мережі та необхідності передачі значних об'ємів службової інформації, а також обмежуються кількістю параметрів для управління потоком даних в мережі, що не дозволяє оцінити стан інформаційного напрямку передачі між відправником та адресатом. Крім того, більшість задач, які вирішуються системою управління МК за типом, функціями, етапами, часом і способами реалізації суттєво відрізняються від задач, які вирішуються СУ стаціонарними мережами зв'язку. Таким чином, на сьогоднішній день спостерігається протиріччя між можливостями існуючих методів управління потоками даних та особливостями бойового застосування МР з динамічною топологією, зростаючими можливостями апаратних засобів, а також зростаючими вимогам до якості передачі різних типів трафіка. Відсутність методології, теоретичних положень і математичного забезпечення управління потоками даних в неоднорідних мережах зв'язку з динамічною топологією в значній мірі стримує створення сучасних ефективних систем управління мережами зв'язку тактичної ланки. Тому актуальною є наукова проблема, що полягає в розв'язанні зазначеного вище протиріччя шляхом розробки методології управління потоками даних в неоднорідних мережах зв'язку з динамічною топологією для виконання вимог інформаційного обміну. Розв'язання зазначеної наукової проблеми спрямоване на підвищення ефективності функціонування мобільних компонент перспективних мереж зв'язку військового призначення і пов'язане з синтезом нових методів управління потоками даних для забезпечення заданої якості обслуговування в мережах даного класу. З цією метою проведене обґрунтування та розвиток положень системного підходу до вирішення проблеми управління потоками даних, що дозволило визначити мету функціонування системи управління МК в цілому та місце підсистеми управління потоками даних в ній; проведена класифікація методів управління потоками даних; визначені поняття предметної області, показники і критерії ефективності; визначені вимоги до методів управління потоками даних; проведена декомпозиція рішення даної проблеми на задачі, які передбачають розробку нових методів управління потоками даних за рівнями моделі OSI та рівнями перспективної мобільної компоненти.

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

# ЦИФРОВІ МЕРЕЖІ НОВОГО ПОКОЛІННЯ НА БАЗІ ТЕХНОЛОГІЇ *DWDM* ІЗ ЗАСТОСУВАННЯМ *EDFA*–ПІДСИЛЮВАЧІВ

Основною характеристикою сучасної епохи є стрімкий процес інформатизації. За оцінками експертів, середній об’єм потоку інформації в розрахунку на одного користувача у світі щороку зростає в 11 разів. У достатній мірі відповідає зростаючим об’ємам передаваємих повідомлень оптичне волокно, яке на сьогодні є ідеальним фізичним середовищем для розповсюдження величезних інформаційних потоків на значні відстані.

*DWDM (Dense Wave Division Multiplexing)* – це сучасна технологія передачі і ущільнення в одному оптоволокні декількох оптичних сигналів з різними довжинами хвиль. *DWDM*-обладнання дозволяє по одній парі оптичних волокон передавати на десятках і навіть сотнях довжинах хвиль трафік різних протоколів (*SDH/ATM/IP*) з різними швидкостями. *DWDM* застосовується не тільки для створення нових волоконно-оптичних мереж, а також для модернізації та розширення існуючих мереж з метою істотного підвищення їх пропускної спроможності та доступності.

*EDFA (Erbium Doped Fibre Amplifier)* – підсилювач на оптичному волокні, легованому іонами ербію, застосовується для відновлення сигналу (без його перетворення з оптичного в електричний вид), надає можливість підсилення спектрально-мультиплексованого сигналу, володіє практично точною відповідністю робочого діапазону області мінімальних оптичних втрат світловодів на основі кварцового скла, порівняно низьким рівнем шуму та простотою включення у волоконно-оптичну систему [1]. *DWDM* із застосуванням *EDFA* є найбільш перспективною оптичною технологією передачі даних [2]. Це пов’язано більшою мірою з бурхливим зростанням Інтернет-трафіку, показники зростання якого наближаються до тисяч відсотків. Об’єми мережевого трафіку постійно збільшуються і вимагають більшої пропускної спроможності. На сьогодні встановлено новий світовий рекорд швидкості передачі даних компанією *Alcatel-lucent*, якого було досягнуто зусиллями дослідницького підрозділу *Bell Labs.* Результат – 100 петабіт в секунду на кілометр. Експеримент включав використання 155 лазерів, кожен з яких працював на власній частоті і забезпечував 100 Гбіт/с [3]. Здійснювалась передача об’єму даних, рівного 400 *DVD*, за секунду на відстань більше 7000 км – приблизно як між Парижем і Чикаго.

**Висновки**. Нові мережі, об’єднані в одну глобальну, – на зразок сучасного Інтернету, але з більшою в десятки тисяч разів пропускною спроможністю, – зможуть використовуватися для безперешкодної масової передачі високоякісної мультимедіа-інформації, ефективного обміну даними між світовими суперкомп’ютерами. Україна є невід’ємним сегментом світової телекомунікаційної мережі, тому вітчизняні розробники не мають права опинитись осторонь інформаційних інновацій. Розробка національного плану впровадження більш швидкісних систем передачі шляхом модернізації існуючих ліній, та нових оптоволоконних ліній зв’язку, це завдання, яке потребує науково обґрунтованих рішень, основаних на теоретичних положеннях: систем масового обслуговування, великих систем та прогнозування розвитку ринку телекомунікаційних послуг. Розробка телекомунікаційного обладнання для силових структур та плани по удосконаленню стаціонарної компоненти системи зв’язку Збройних сил України повинні здійснюватися погоджено з зазначеними процесами, щоб уникнути невідповідності технологій мереж доступу модернізованим транспортним мережам.

ЛІТЕРАТУРА

1. *http://ru.wikipedia.org/*.
2. *Каток В. Б.* Волоконно-оптичні системи зв’язку. – К.: Велар, 1999. – 194 с.
3. *http://www.3dnews.ru/.*

к.т.н. Степанов М. М.(НАОУ)
Уварова Т. В.(НАОУ)

# ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ З МОДЕРНІЗАЦІЇ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

У зв'язку із постійним формуванням бюджету Збройних Сил (ЗС) України за остаточним принципом, а також постійним недотриманням коштів, які були заплановані, з'явилась тенденція по скороченню модернізації існуючих та закупівлі новітніх зразків озброєння і воєнної техніки. Такий стан речей веде до скорочення, згортання НДДКР та фізичного і морального старіння систем які знаходяться на озброєнні у ЗС України.

Сучасний розвиток технологій і концепцій ведення бойових дій, а також політичні настанови з трансформації та інтеграція Збройних Сил України до військових формувань європейських держав та держав, що входять до НАТО ставить питання про перехід до інтелектуальних, високотехнологічних зразків озброєння і воєнної техніки.

Тому підтримка ЗС в стані відповідному до сучасних вимог є найактуальнішою задачею на сьогоднішній день, але вирішувати проблему з підтримки ЗС на відповідному рівні потрібно з мінімальними витратами, які необхідно спрямувати на виконання НДДКР для модернізації озброєння.

Простим та ефективним способом з модернізації озброєння є всебічне застосування систем інформаційного забезпечення ведення бойових дій. Одним з видів інформаційного забезпечення дій підрозділів Збройних Сил України, як його основи, повинно стати забезпечення даними про місцевість та місцезнаходження зразка озброєння (топогеодезичне, геодезичне та навігаційне забезпечення). Від якості та своєчасності якого залежить кінцевий результат виконання завдань.

Для мінімального розгортання систем геоінформаційного забезпечення необхідно масове застосування систем визначення координат (GPS), з точністю до 1-го метра, та швидкісних широкосмугових систем передачі даних (обміну даними про координати об'єктів). Це дозволить зробити модернізацію озброєння з мінімальними витратами коштів і при цьому зробити запас для майбутніх зразків озброєння.

Наприклад, при точному та швидкісному визначенні координат точки вогневої позиції окремої гармати, артилерійської батареї і своєчасному їх забезпеченню точними координатами цілей, дає змогу артилерійському підрозділу скритно облаштувати позицію, своєчасно відкрити вогонь на знищення об'єкта, скритно згорнути позицію і перейти до маршу. Основний показник при цьому – скорочення часу на визначення точних (до 1-го м.) координат. Це дозволить:

зменшити час на підготовку до стрільби;

скоротити час стрільби та час на перенос вогню;

зменшити необхідний боєкомплект, для знищення одного об'єкту;

збільшити кількість об'єктів, які може знищити батарея;

Скорочення часу стрільби ускладнює завдання по виявленню противником вогневої позиції і дає змогу своєчасно згорнути позицію та виконати марш.

Як що врахувати стан органів забезпечення боєприпасами то зменшення кількості боєприпасів суттєво вплине на боєздатність підрозділів ЗС України. Тому застосування навігаційних систем дозволить підвищити боєздатність як окремого зразка озброєння так і всієї системи озброєння з мінімальними витратами на модернізацію.

Для вирішення завдань геоінформаційного забезпечення необхідно застосовувати системи визначення координат (GPS), коректуючі станції та системи забезпечення космічними знімками, а також визначити стандарти у форматах геоданих і застосувати єдину (державну) операційну систему (наприклад MyLinux).

Степанюк О. А. (ІТС, НТУУ „КПІ”)

# АНАЛІЗ КОНКУРЕНТНИХ ТЕХНОЛОГІЙ ПОКОЛІННЯ 4G: LTE, MOBILE WIMAX

4G визначається як майбутнє бездротових телекомунікацій зі швидкістю передачі даних до 1 Гбіт/с в умовах руху джерела або приймача і ~100 Мбіт/с в умовах сеансу між двома мобільними терміналами. Побудова мобільних мереж четвертого покоління передбачає відмову від використання комутації каналів (властиву 2G/3G) і повний перехід на комутацію пакетів (all-ip мережі). Сьогодні існує дві технології, що претендують на виконання поставлених завдань: LTE і Mobile WiMax.

Технологія LTE розробляється для створення високошвидкісних систем мобільного зв’язку, оптимізованих для пакетної передачі даних зі швидкістю до 300 Мбіт/с в нисхідному каналі (від базової станції до користувача) і до 75 Мбіт/с у висхідному каналі.

Mobile WiMax – розробка компанії Intel, також відома як IEEE 802.16e(m,j). Позиціонується як універсальна технологія для бездротового широкосмугового доступу. Для підтримки мобільного абонента реалізовано такі специфічні функції, як роумінг та „безшовний” перехід між базовими станціями при пересуванні абонента.

WiMax і LTE мають ряд схожих технологічних рішень. Отже, три прийома, що знайшли успішне застосування як в WiMax, так і в LTE:

MIMO – це специфіка радіоінтерфейсів згаданих технологій. Полягає вона в розділенні потоку інформації на кванти і паралельній трансляції кількома передавачами. Таким чином, збільшується швидкість передачі, а значить і пропускної здатності.

Основна ідея OFDMA – розподіл частотного діапазону на піднесучі частоти, спектри яких не перекриваються і залишаються ортогональними. Саме цей хід дозволяє значно оптимізувати використання дорогого частотного ресурсу.

Технологія інтелектуальної антени (Smart Antenna) дозволяє змінювати діаграму спрямованості кожні 5 мс, що приносить значний виграш у зменшенні потужності передаючих сигналів.

LTE, у розробці якого беруть участь найбільші мобільні оператори, цікавий бізнесу мобільного зв’язку. WiMax же – розробка Intel, і логічно, що цей стандарт орієнтований на надання послуг передачі даних.До того ж, архітектура Mobile WiMax мереж не адаптована до специфічних завдань телефонії. Тому спектр вирішуваних завдань аналізованих технологій перекривається неповсюдно. Варто говорити про можливість паралельного існування розглянутих технологій. Позитивний досвід світової телекомунікаційної спільноти створює сприятливі умови для поступового переходу України на нову ступінь телекомунікаційних послуг. Показовим є те, що вже є приклад реалізації мережі 802.16 в м. Києві. З технологією LTE – складніше. В Україні лише зараз проводиться тендер на видачу частот для розгортання UMTS-мереж (покоління 3G). Хоча LTE технічно і є логічним продовженням стандарту UMTS, важко говорити про оперативний перехід на стандарт з огляду на комерційні інтереси операторів. Хоча для нашого споживацького ринку LTE є досить далеким майбутнім, проте, беззсумнівно, перспективним.

ЛІТЕРАТУРА

1. *Pierre Lescuyer, Thierry Lucidarme.* Evolved packet System (EPS). The LTE and SAE Evolution of 3G UMTS.- 2008. – 353p

2. *Erik Dahlman, Stefan Parkvall, Johan Skoeld, Per Beming*. 3G Evolution, HSPA and LTE for Mobile Broadband, 2nd edition. – 2008. – 651p

3. *K.Fazel, S.Kaiser*. Multi-Carrier and Spread Spectrum Systems. From OFDM and MC-CDMA to LTE and WiMAX. 2nd edition. – 2008. – 380p.

к.т.н. Стрюк О.Ю. (ВІТІ НТУУ „КПІ”)
Дядик Д.Ф. (ВІТІ НТУУ „КПІ”)

# МЕТОД АНАЛІТИЧНОЇ ОЦІНКИ СТУПЕНЯ СТИСКУ ЗОБРАЖЕНЬ

Одним з найбільш об’ємних видів даних є статичні зображення. Для представлення зображень необхідно більшого об’єму пам’яті ніж, наприклад, для представлення текстових даних. Сучасні розробки в області стиску зображень, як правило, є закритими до широкого застосування і комерційними проектами. Це підтверджується рядом передових телекомунікаційних світових компаній, які успішно розробляють і впроваджують в свої системи ефективні методи стиску, без розповсюдження самих алгоритмів стиску. Тому розробка методів стиску, що основані на сучасних підходах теорії кодування інформації є актуальною задачею.

На етапі проектування та розробки алгоритмів стиску зображень розробники стикаються з низкою проблем, пов’язаних з оцінкою створюваних алгоритмів. Оцінка алгоритмів стиску проводиться з певного набору параметрів. Вибір параметрів для порівняння залежить від конкретного призначення даного алгоритму і від класу стискаємих зображень. Деякі алгоритми спрямовані на високу ефективність стиску, інші забезпечують високу швидкість компресії або декомпресії.

Ключовим показником ефективності алгоритму стиску є ступінь стиску. Саме максимально високий ступінь стиску є головним функціональним призначенням існуючих методів стиску. Ефективність стиску прийнято описувати параметром коефіцієнт стиску, який визначають як відношення обсягу вихідних до обсягу стиснутих даних.

Основою розробленого методу аналітичної оцінки ступеня стиску зображень є оцінка інформаційної насиченості даних на виході алгоритмів вейвлет-перетворення, контекстного моделювання PPM та арифметичного кодування. Для коректної оцінки насиченості введено параметр „коефіцієнт використання контексту”, що дозволяє апріорно оцінити кількість символів, що буде оцінено в контексті певного порядку. Вагові коефіцієнти для контекстів кожного з порядків визначається виразом:

$$k_d = \frac{\sum_{j=0}^{255} t(esc \mid c_{d+1j}) - \sum_{j=0}^{255} t(esc \mid c_{dj})}{T(S)},$$

де, $t(esc \mid c_{d+1j})$ – частота появи символу переходу в контексті $c_{d+1j}$;

$d$ – порядок контексту;

$T(S)$ – загальна кількість кодуємих символів вхідного потоку.

Розроблений метод аналітичної оцінки ступеня стиску зображень був апробований шляхом порівняння аналітичних значень ступеня стиску для тестового пакету зображень, з практичними значеннями, отриманими за допомогою створеного програмного комплексу стиску зображень без втрат. Аналіз порівняння показав, що погрішність, при визначенні аналітичного значення ступеня стиску не перевищує 2 % по відношенню до практичного значення. Отримане невисоке значення погрішності, дозволяє зробити висновок про точність використаних в методі припущень та введених параметрів оцінки. Розроблений метод доцільно використовувати на етапі розробки та тестування методів стиску даних, що базуються на алгоритмі контекстного моделювання PPM та арифметичному кодуванні.

ЛІТЕРАТУРА

1. *Maarten J.* Second generation wavelets and applications / Patrick O. // Springer-Verlag London Limited, 2005 – 138 p.

2. *Шульгин В.И.* – Основы теории передачи информации. – Харьков: Нац. аэрокосм. ун-т „ Харьк. авиац. ин-т ” , 2003. – с. 102.

к.т.н. Стрюк О.Ю. (ВІТІ НТУУ „КПІ”)

# МЕТОД ПІДВИЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ АБОНЕНТІВ БАЗОВОЇ СТАНЦІЇ РАДІОМЕРЕЖІ

Швидкий розвиток телекомунікаційних мереж та мультимедійних послуг викликали появу конвергентних інформаційно – комунікаційних мереж. Однією із найбільш важливих вимог, що пред’являються до інформаційно – комунікаційних мереж, є забезпечення для кожного з користувачів мережі заданого рівня якості обслуговування (*QoS, Quality of Service*). Розпочате в останні роки комерційне надання мультимедійних послуг в радіомережах зумовлює підвищення попиту на дослідження і розробки у галузі забезпечення *QoS* для різних технологій безпроводового доступу.

Важливим механізмом забезпечення *QoS* є керування ресурсами мережі, яке полягає в пошуку такої стратегії розподілу ресурсів мережі, яка забезпечує досягнення заданих (або максимально можливих) значень параметрів *QoS* для конкуруючих за доступ до ресурсів мережі інформаційних потоків. Задача пошуку оптимального розподілу ресурсів мережі у загальному випадку зводиться до задачі багатокритеріальної оптимізації для нечітко завданих цілей та альтернатів, вирішення якої має великий ступінь складності. Багатокритеріальність задачі курування ресурсами радіомережі, пороговий характер завдання придатних значень показників *QoS*, викликали пошук підходів, покликаних спростити вирішення цієї задачі.

В якості інтегрального показника при оцінюванні оптимальності розподілу ресурсів мережі 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. 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).

Для кожної з функціонуючих в мережі інформаційних служб можуть бути визначені значення багатовимірного вектору $\{MOS_i\}$, залежні від виділених ресурсів, параметрів мережі, з урахуванням функціональності прикладного програмного забезпечення (кінцевого абонентського обладнання), яке реалізовує дану послугу

$$\{MOS_i\} = F(\{R_i\},\{q\},\{E_i\}), \tag{1}$$

де $MOS_i$ – значення *PQoS* за шкалою *MOS* для інформаційної служби $i$, $i = \overline{1,N}$;

$N$ – кількість інформаційних служб, які функціонують у мережі;

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

$\{q\}$ – показники, які характеризують мережу;

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

Одним із найбільш вагомих ресурсів радіомереж у сегменті „базова станція – мобільні абоненти” є пропускна спроможність радіоканалу між базовою станцією і мобільними абонентами, тому пропонується постановка та метод рішення оптимізаційної задачі спрямованої на максимізацію сумарного значення *PQoS* у сегменті „базова станція – мобільні абоненти” за рахунок керування пропускною спроможністю, кодування аудіовізуальних даних зі зміною швидкістю і з урахуванням рівня завадостійкості каналів між абонентами і базовою станцією.

Оптимізаційна задача вирішується виходячи із припущення про реалізацію у радіомережі наступних алгоритмів і протоколів:

– детермінований доступ до радіоканалу з можливістю виділення кожному інформаційному потоку певного значення пропускної спроможності з дискретністю $\Delta R$;

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

– наявність механізмів класифікації інформаційних потоків, керування чергами, планування передавання;

– можливість транскодування аудіовізуальних даних – зміни в реальному часі швидкості кодування та (або) формату представлення даних.

Для рішення оптимізаційної задачі необхідно – знайти такий розподіл пропускної спроможності базової станції між інформаційними потоками в зоні обслуговування базової станції, при якому виконується

$$\{r_i\}^* = arg \max_{\{r_i\}\in\Omega}\left(\sum_{i=1}^{k} MOS_i(r_i, PLP_i)\right) \quad (2)$$

$$за \quad умови \quad \sum_{i=1}^{k} r_i = R,$$

де $\{r_i\}^*$ – вектор розподілу пропускної спроможності, який забезпечує вирішення задачі (2);

$Q$ – множина можливих значень вектору розподілу пропускної спроможності між $k$ – інформаційними потоками, при дискретності зміни пропускної спроможності $\Delta R$;

$MOS_i$ ($r_i$, $PLP_i$) – значення $PQoS$ по шкалі $MOS$ в залежності від виділеної смуги пропускання і імовірності втрати пакету для кожного з інформаційних потоків;

$r_i$ – значення пропускної спроможності, виділене інформаційному потоку $i$;

$PLP_i$ – середня імовірність втрати пакету для кожного інформаційного потоку;

$R$- максимальне значення пропускної спроможності між базовою станцією і мобільними абонентами.

Вирішення оптимізаційної задачі (2) може бути отримано із використанням динамічного програмування. Вибір даного методу рішення обумовлений:

– можливою в загальному випадку невігнутістю компонентів цільової функції, що не дозволить отримати аналітичне рішення у відповідності до теореми Каруша – Куна – Такера;

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

Можливість використання динамічного програмування для вирішення оптимізаційної задачі (2) обумовлена:

– адитивним характером цільової функції оптимізації;

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

Для вирішення оптимізаційної задачі (2), пропонується алгоритм динамічного програмування, який має низький ступінь складності.

Таким чином, доведена можливість і перспективність використання значення сприйняття якості обслуговування (PQoS) в якості інтегрального показника при визначенні оптимальності розподілу ресурсів радіомереж. Запропонований удосконалений метод керування розподілом пропускної спроможності для максимізації повного значення PQoS у сегменті „базова станція – мобільні абоненти" радіомереж на основі інфраструктури базових станцій. Значення повного PQoS, яких дозволяє досягти запропонований метод, перевищують результати стандартних та відомих перспективних методів керування пропускною спроможністю.

к.т.н. Субач І.Ю. (ВІТІ НТУУ „КПІ”)
Міщенко В.О. (ВІТІ НТУУ „КПІ”)
Симоненко О.А. (ВІТІ НТУУ „КПІ”)
Саєнко О.Г. (ВІТІ НТУУ „КПІ”)

# МОНІТОРИНГ ДАНИХ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ

На сьогодні в галузі інформаційних технологій спостерігається стрімке розширення спектра послуг та інтеграція телекомунікаційних мереж різноманітного призначення. Для забезпечення високої якості обслуговування абонентів під час впровадження сучасних інформаційних технологій потрібна відповідна система управління та моніторингу інформаційної мережі, у складі якої має функціонувати інтелектуальна підсистема підтримки прийняття рішення чергового адміністратора. Зазначена система має надавати адміністратору можливість проведення моніторингу і швидкого реконфігурування мережі, своєчасно знаходити і усувати несправності, забезпечувати розвиток мережі та оперативне підключення абонентів до нових інформаційних послуг.

Аналіз сучасних методів управління телекомунікаційними та інформаційними мережами та основних засад застосування стандартів і концепцій систем управління мережами *(TMN – Telecommunication Management Network, Smart TMN, TINA – Telecommunications Information Networking Architecture, CORBA – Common Objects Request Broker Architecture та ін.)*, а також тенденцій розвитку систем управління телекомунікаційними та інформаційними мережами свідчить про необхідність їхнього подальшого розвитку в цій галузі.

Порівняльний аналіз систем моніторингу інформаційних мереж показує, що якісна система моніторингу та управління інформаційною мережею повинна мати наступні властивості: масштабованість; розподіленість у відповідності до концепції клієнт/сервер; відкритість до нарощування різнорідного обладнання. Якісна масштабованість досягається за рахунок розподіленості системи управління. Розподіленість означає, що система дозволяє включати декілька серверів і клієнтів. Сервери, за допомогою програмних засобів, збирають інформацію про поточний стан мережі від агентів *(SNMP, CMIP, RMON)* та накопичують її в своїх БД.

До числа найбільш популярних програмних засобів моніторингу та управління інформаційними мережами відносяться наступні системи: *Spectrum* компанії *CabletronSystems*; *OpenView* фірми *Hewlett-Packard*; *NetView* корпорації *IBM*; *Solstice* виробництва *SunSoft* – підрозділу *SunMicrosystems*; *Multi Router Traffic Grapher (MRTG)* компанії *Activestate*; *Net Geos.*

Слід зауважити, що всебічну підтримку та управління різнорідного обладнання (різних виробників) на сьогодні не спроможний забезпечити жоден виробник. Під час побудови топології мережі, яка складається з обладнання різних виробників, системи управління та моніторингу роблять помилки, приймають одне обладнання за інше, а під час управління ними підтримують тільки їхні основні функції, інші додаткові функції зазначені системи просто не розуміють, внаслідок чого не можуть ними скористатися.

Проведені авторами дослідження показують, що найбільші переваги серед розглянутих систем управління та моніторингу інформаційними мережами має система *Net Geos*, яка дозволяє найбільш ефективно здійснювати управління параметрами функціонування інформаційної мережі.

ЛІТЕРАТУРА

1. *Хиленко В.В.* Методи підвищення показників якості системи управління телекомунікаційними мережами. – К., 2007. – 236 с.

2. *Субач І.Ю.* Інтелектуальний аналіз збоїв у роботі інформаційних мереж. – Зв’язок. – 2006. – № 1. – С. 34 – 40.

к.т.н. Субач І.Ю. (ВІТІ НТУУ ,,КПІ”)
Міщенко В.О. (ВІТІ НТУУ ,,КПІ”)
Саєнко О.Г. (ВІТІ НТУУ ,,КПІ”)

# МЕТОДОЛОГІЧНІ ОСНОВИ ІНТЕЛЕКТУАЛЬНОГО ЗДОБУТТЯ ЗНАНЬ З СИСТЕМ МОНІТОРИНГУ ІНФОРМАЦІЙНИХ МЕРЕЖ

Інтенсивний розвиток інформаційних мереж в Україні визначає особливу актуальність питання управління та моніторингу мереж з метою забезпечення їх сталої роботи та визначення перспектив подальшого їх розвитку.

Для забезпечення якісного вирішення зазначених задач потрібна відповідна система управління та моніторингу інформаційної мережі, у складі якої має функціонувати інтелектуальна підсистема підтримки прийняття рішень чергового адміністратора.

Така система має надавати адміністратору можливість проведення моніторингу і швидкого реконфігурування мережі, своєчасно відслідковувати позаштатні ситуації в мережі, знаходити і усувати несправності, забезпечувати розвиток мережі та оперативне підключення абонентів до нових інформаційних послуг.

Проведений аналіз предметної області та публікацій дозволив визначити основні принципи, які покладено в основу організації управління і моніторингу інформаційних мереж спеціального призначення (ІМСП):

1. Централізація управління з можливістю децентралізації окремих функцій моніторингу та адміністрування на віддалених інформаційних вузлах.
2. Інтегрований підхід до вирішення завдань адміністрування мережі у межах зони відповідальності особи, що приймає рішення (ОПР).
3. Створення гнучкої архітектури мережі на базі методології відкритих систем, що надає можливість реконфігурації мережі та розширення функцій адміністрування.
4. Забезпечення високого рівня автоматизації процесів управління та функціонування інформаційної мережі.
5. Використання єдиної системи стандартів з технічного, інформаційного, математичного та програмного забезпечення на базі рекомендацій міжнародних, національних та галузевих стандартів.

Зважаючи на вищевикладене, актуальним постає питання впровадження аналітичних інформаційних технологій та нових методів здобуття асоціативних правил на підставі інформації, що перебуває в базах даних (БД) ІМСП у діяльність ОПР під час моніторингу та безпосередньо в процес моніторингу мереж.

Однією з найбільш поширених задач інтелектуального аналізу даних (ІАД) є визначення наборів об’єктів, які часто трапляються.

Під час розв’язування задач ІАД певний інтерес становить знаходження закономірностей у послідовностях подій, які відбуваються в мережі. При їх визначенні можливо з певною мірою впевненості проаналізувати появу подальших подій для прийняття обґрунтованих рішень.

У доповіді пропонується, для здобуття нових знань про функціонування інформаційної мережі застосовувати методи інтелектуального аналізу знань (ІАД) та методику отримання знань з систем моніторингу ІМСП.

Перевага цієї методики полягає не тільки в застосуванні методів виявлення патернів із баз даних (БД) інформаційних систем, а й в урахуванні вагомості тієї чи іншої позаштатної ситуації, що може скластися в інформаційній мережі під час її функціонування в режимі реального часу.

Сушин О.М.(ЦНДІ ОВТ ЗСУ)
Шугалій Є.П. (ЦНДІ ОВТ ЗСУ)

# 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 ЗВІ, 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. Твердохлібов В.В.(ЦНДІ ОВТ ЗСУ)

# НАПРЯМИ РОЗВИТКУ СИСТЕМИ ЗВ'ЯЗКУ СИЛ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

Аналіз воєнних конфліктів останніх років в різних регіонах світу свідчить, що освоїти нові форми і способи знищення противника, досягти інших воєнних та воєнно-політичних цілей вже неможливо без урахування зростаючої ролі і значення сил спеціальних операцій.

Під загальним поняттям спеціальної операції мається на увазі сукупність нестандартних підходів, спеціальних (специфічних) дій та заходів спеціально організованих, підготовлених і забезпечених військ (сил) для досягнення важливих політичних, воєнних і економічних цілей в операціях (бойових діях) об'єднань Збройних Сил України.

Спеціальна операція за типом може бути самостійною або складовою частиною загальновійськової операції. Разом з тим, в будь-якому разі їй притаманна відносна самостійність і автономність. Особливою формою спеціальної операції є інформаційно-психологічна операція, яка являє собою комплекс заходів, в тому числі проведення спеціальних заходів, спрямованих на ведення інтенсивного зовнішнього інформаційно-психологічного впливу на населення, війська противника з метою їх деморалізації та дезорієнтації, підриву морально-бойового духу і примушення до виходу з війни.

До спеціальних операцій відносяться миротворчі і гуманітарні акції, дії з ліквідації наслідків стихійних лих, відновлення цивільної адміністрації і проведення карантинних заходів. Специфіка спеціальної операції полягає у цілях, завданнях, способах та районах її проведення, залученні сил і засобів, що беруть у ній участь, та особливостях управління.

Спеціальні операції відрізняються за масштабами, часом, місцем і умовами проведення.

В умовах сучасної міжнародної обстановки, коли знижується рівень військового протистояння, керівництво збройних сил США звертає особливу увагу на якісний стан військ при деякому скороченні чисельності. Відповідно до положення Об'єднаної концепції будівництва ЗС США до 2010 р. вони повинні прийти до найкращого балансу – досягти найбільших можливостей і різко підвищити взаємодію компонентів, що входять до них, з найменшими витратами. Одним із напрямків у рамках виконання цього завдання є розвиток сил спеціальних операцій.

Як один з найбільш дійових військових інструментів, використовуваних для посилення свого політичного і військового впливу за рубежем, головним чином у країнах „третього світу", американське керівництво розглядає сили спеціальних операцій.

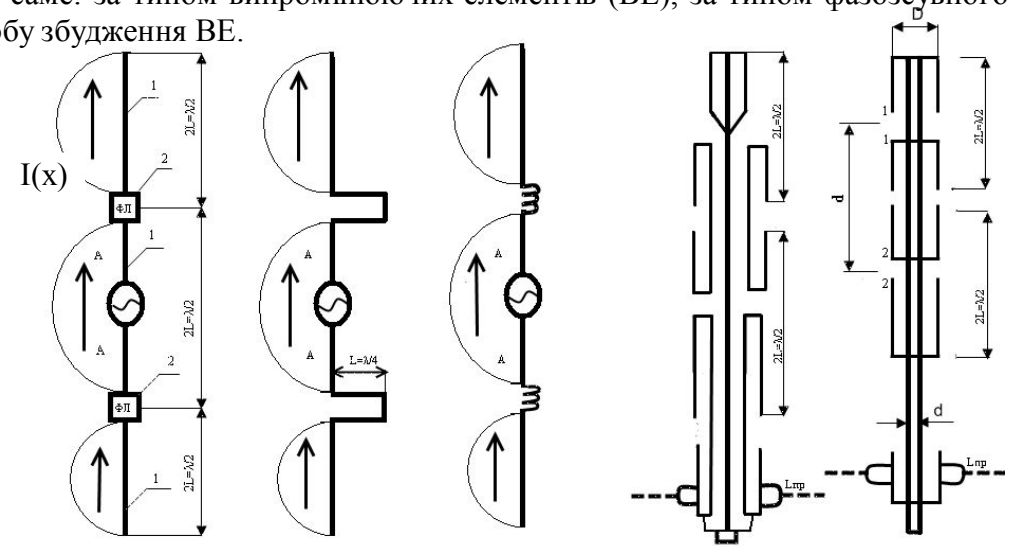
За визначенням представників Міністерства оборони США, сили спеціальних операцій американських збройних сил являють собою спеціально створені, навчені й оснащені формування сухопутних військ, ВПС і ВМС, призначені для вирішення специфічних завдань в інтересах досягнення воєнних, політичних, економічних і психологічних цілей на територіях, що належать іноземним державам або захоплені ними, а також у географічних районах, що становлять для США особливий політичний інтерес.

Одне з питань, що підлягає окремому вивченню – це проблеми впровадження в ЗС України засобів зв'язку іноземного виробництва. Розглядається існуючий на цей час досвід, ставляться завдання на дослідження певних питань та розробляються пропозиції щодо вирішення окремих проблем.

Терезюк О. Э. (ВІТІ НТУУ „КПІ”)
Шацький І. О. (ВІТІ НТУУ „КПІ”)

# КОЛІНЕАРНІ АНТЕНИ

Простота конструкції, висока ефективність, мала масогабаритність, відносно невеликі витрати на виготовлення сприяли великому практичному інтересу до колінеарних антен (КА). Бурхливий розвиток систем радіозв’язку з рухомими об’єктами (сотових, транкінгових, супутникових, систем персонального виклику) у військовій, народногосподарській, комерційній та інших сферах визначило теперішнє місце КА серед численних зразків антенної техніки. Численні конструкції КА можна класифікувати за рядом ознак, а саме: за типом випромінюючих елементів (ВЕ), за типом фазозсувного пристрою, за способу збудження ВЕ.




а) б) в) г) д)

Рис. 1

На рис. 1 показаний вид КА, де цифрами позначено: 1 – ВЕ; 2 – фазозсувний ланцюг (ФЛ), I(x) – розподіл струму в ВЕ, а також деякі різновиди КА таких як КА із чвертьхвильовим ФЛ і ВЕ у вигляді симетричних напівхвильових вібраторів (рис. 1б). На рис. 1в показана КА із ФЛ у вигляді зосередженої індуктивності. На рис. 1г і 1д представлені КА коаксіального виду з різним типом збудження ВЕ, виконаних у вигляді коаксіальних симетричних вібраторів [1].

Основним недоліком розглянутих вище технічних рішень виконання КА є їх вузькосмуговість як по вхідному опорі, так і по зовнішніх характеристиках, за рахунок того, що принцип роботи КА жорстко пов’язаний з довжиною хвилі **λ**.

Більшими функціональними можливостями володіє КА виконана на коаксіальних симетричних вібраторах, збуджуваних паралельно в точках 1 – 1 і 2 – 2 як показано на рис. 1д. Оригінальність конструкції полягає в тому, що верхнє плече ВЕ виконує функцію частотного компенсатора, а нижнє – симетрируючого пристрою. Конструкція цієї антени дозволяє змінювати відстань d між ВЕ, тим самим збільшуючи значення G – коефіцієнта підсилення КА. Дана антена з паралельним живленням має високу механічну міцність, дозволяє здійснювати електричне керування характеристикою направленості та має зменшений „антенний ефект”.

ВЕ КА можна представити у вигляді паралельного з’єднання короткозамкнутої і роз’єднаних чвертьхвильових довгих ліній, що дозволяє записати вираз для вхідного опору $Z_A$ коаксіального симетричного вібратора, при невеликій смузі частот $\Delta f/f_0$ .

Вхідний опір коаксіального вібратора із частотним компенсатором розраховується за наступним виразом:

$$Z_A = \frac{\frac{1}{R_A}}{\left(\frac{1}{R_A}\right)^2 + \left(\frac{\rho_в}{R_A^2} - \frac{1}{\rho_к}\right)^2 \cdot \mathrm{ctg}^2 kl} - j\frac{\left(\frac{\rho_в}{R_A^2} - \frac{1}{\rho_к}\right) \cdot \mathrm{ctg}^2 kl}{\left(\frac{1}{R_A}\right)^2 + \left(\frac{\rho_в}{R_A^2} - \frac{1}{\rho_к}\right)^2 \cdot \mathrm{ctg}^2 kl}. \quad (1)$$

Вираз (1) відповідає випадку невеликого відхилення частоти, при якому умова повної компенсації реактивної складової є виконання співвідношення:

$$\rho_к = \frac{R_A^2}{\rho_в}, \quad (2)$$

де $R_A$ = 73,2 Ом – антенний опір вібратора; $\rho_в = 120\left(ln\frac{\lambda}{2D} - 1\right)$, $\rho_к = 60\,ln\frac{D}{d}$ – хвильові опори вібратора й компенсатора відповідно.

З умови повної компенсації співвідношення (2), не важко отримати вираз який дозволяє знайти співвідношення між поперечними розмірами *D* і *d* коаксіальної лінії, а саме:

$$\frac{D}{d} = L^{\frac{0,74}{ln\frac{\lambda}{2D} - 1}}. \quad (3)$$

Нехай $D/\lambda = 0,1$, тоді $D/d = 3,4$, що відповідає $\rho_к = 73,1$ Ом. На рис. 2 показана частотна залежність складових $R_A$ та $X_A$ вхідного опору, яка наглядно демонструє діапазонні властивості коаксіального симетричного вібратора. В смузі частот, з коефіцієнтом перекриття $K_n$ рівним 1,6, реактивна складова $X_A$ рівна нулю, а $R_A$ – активна складова, близька до значення 75 Ом.

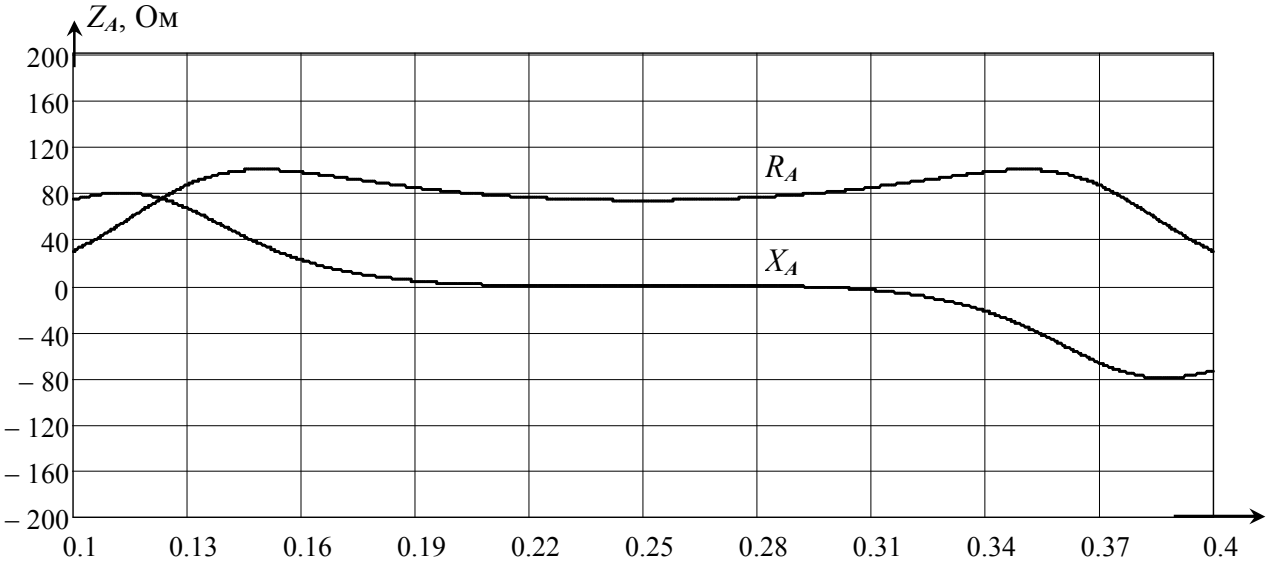



Рис. 2

Таким чином отримані результати наглядно показують, що КА з паралельним збудженням ВЕ, в значній мірі перевершують аналогічні антени з послідовним збудженням.

ЛІТЕРАТУРА


1. *Мишустин Б. А., Слезкин В. Г.,. Редькина Е. А.* Оптимизация характеристик излучения коаксиальных коллинеарных антенн с последовательными делителями питания. 12-я Междунар. конф. КрымИКО-2002. Материалы конференции.– Севастополь: „Вебер”, 2002.– С. 347 – 348.

2. *Вершков М. В.* Судовые антенны. М., Из-во „Сов. радио”, 1972 г., стр 37.

Тимченко О.М. (ЦНДІ ОВТ ЗСУ)

# ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ТА НАПРЯМИ РОЗВИТКУ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ЗБРОЙНИХ СИЛ РОЗВИНЕНИХ КРАЇН СВІТУ

У відповідності до уставів армій США та інших країн НАТО управління військами розглядається як єдиний процес, в ході якого організується й координується діяльність об'єднань, з'єднань, частин та підрозділів. Його організаційно-функціональною основою є система управління, яка створюється на базі комплексної автоматизації.

Значення автоматизації для бойового потенціалу військових формувань безперервно зростає. Це логічно випливає з багаторічних пошукових робіт з розвитку національних систем бойового управління в державах НАТО (ATCCS – АСУ АК США, „Герос" – автоматизація роботи штабів (Німеччина), „Вейвел" – автоматизація управління загальновійськовим підрозділом (Велика Британія)).

Американське командування дійшло до висновку, що тільки АСУ здатні підвищити оперативність управління в 2,5 – 3 і більше в рази, що вважається мінімально необхідним для успішного проведення повітряно-наземної операції.

Процес розробки і впровадження в практику управління військами різних засобів автоматизації зараз вступає в якісно нову фазу свого розвитку – етап комплексної автоматизації управління. На цьому етапі створюються „великі системи", що охоплюють усі ланки військової організації: від первинних військових колективів до вищого командування збройними силами.

У сучасних умовах значно збільшилися площі, з яких необхідно збирати розвіддані. При цьому космічні системи розвідки та раннього попередження забезпечували підвищення ефективності бойових дії ЗС у збройних конфліктах у 1,5 – 2 рази.

Сьогодні проблема стійкості та безперервності управління військами набула особої актуальності. Періодична зміна районів розгортання пунктів управління (ПУ) зменшує імовірність їх виявлення розвідкою противника, сприятиме збільшенню живучості, стійкій та безперервній роботі. Так, за думкою іноземних воєнних фахівців, імовірність виживання ПУ об'єднань при правильній організації зміни районів складає 0,5 – 0,6, а при постійному находженні їх у русі – 0,7 – 0,8.

Разом з тим, переміщення знижує можливість штабів з розв'язання управлінських задач, особливо в умовах, коли противник може виявити та завдати по них вогневі удари перш, ніж вони будуть розгорнуті. Це також обумовлюється труднощами залучення до роботи всього оперативного складу ПУ, зменшенням кількості каналів зв'язку з огляду на неможливість використання в русі основних каналоутворюючих засобів, складністю організації надійної охорони та оборони колон від раптових ударів противника та іншими факторами. А тому завдання збереження живучості ПУ без зниження ефективності їх роботи лишається проблематичним, вимагає пошуку шляхів його виконання.

Складність процесу управління в сучасних умовах вимагає різкого збільшення рівня інтелектуалізації засобів автоматизації. В той же час автоматизація повинна розвиватися на загальновійськовій основі. Саме загальновійськові АСУ повинні об'єднувати окремі видові (родові) АСУ угруповань військ (сил) у єдині системи, які управляються у відповідності до загальних закономірностей. Тому складовими частинами („вертикальними стволами") загальновійськової АСУ повинні стати підсистеми управління розвідки і РЕБ, артилерії, авіації, ППО, флоту, а також технічного, тилового і інших видів забезпеченням.

Таким чином, можна сформулювати основні принципи побудови АСУ угруповань збройних сил розвинених країн:

об‘єднання в єдину глобальну інформаційно-керувальну мережу всіх органів управління, а також сил і засобів розвідки і РЕБ;

організація ефективних вертикальних і горизонтальних зв‘язків у структурі системи;

автоматизована підтримка прийняття рішень та забезпечення планування операцій (бойових дій) на основі комплексних математичних моделей (експертних систем);

оперативне одержання необхідних (санкціонованих) даних будь-яким органом управління;

гнучка структура АСУ та здатність до безперервного розвитку;

модульна побудова глобальної інформаційне-керувальної мережі;

використання єдиних стандартів та форматів документів;

повна сумісність застосованих програмних та апаратних засобів;

гарантований захист інформації від несанкціонованого доступу.

Досвід світових, локальних і регіональних війн переконливо доводить, що автоматизація управління військами в сучасних умовах стає таким же вирішальним чинником успіху, як кількість та якість військ і зброї. Це дозволяє нам сформулювати основні напрями розвитку систем управління ЗС розвинених країн, до яких можна віднести:

1. Створення „великих систем” автоматизації бойового управління, які охоплюють усі ланки військової організації держави: від солдата (первинного військового колективу) до вищого командування збройними силами.

2. Комплексна інтеграція засобів розвідки на базі космічних систем різного призначення, повітряних та морських систем розвідки, передачі розвідувальної інформації, управління військами (силами) і зброєю, вогневого ураження і радіоелектронного подавлення в єдині бойові системи у масштабі угруповань військ на ТВД.

3. Комплексна автоматизації усіх процесів управління військами (силами) і зброєю в реальному масштабі часу від виявлення противника до його знищення, різке збільшення рівня інтелектуалізації засобів автоматизації на загальновійськовій основі.

Все це забезпечить масштабне використання систем керованої зброї.

4. Підвищення мобільності ПУ за рахунок використання вдосконаленої технічної бази, уніфікації зразків техніки рухомих пунктів управління, забезпечення пересування їх повітрям. До речі, в армії США до цього часу залишається базовою машиною для рухомих пунктів управління БТР М-113, на базі якого створено певну кількість штабних та інших машин управління.

5. Підвищення точності визначення координат ПУ та військ за рахунок використання космічної навігаційної системи „NAVSTAR”, GPS, „Spot”, „Landsat” та інших з всіх ланках управління. Система GPS взагалі доведена до окремого військовослужбовця на полі бою (поки ще для окремих категорій військ, зокрема сили спеціального призначення и спецоперацій). В ЗС Росії останнього часу різко збільшилась увага до розробки і застосування малогабаритних навігаційно-зв’язних комплектів типу „Бот” і „Тропа”, а також інформаційно-картографічних систем типу „Планшет”.

6. Збільшення ступеня інформування військ за рахунок створення єдиної інформаційної мережі поля бою. Модернізовані танки М1А2 „Абрамс” та бойові машини піхоти М2А3 „Бредлі” мають на озброєнні елементи нової автоматизованої системи управління тактичною ланкою сухопутних військ („бригада – батальйон”) FBCB, яка забезпечує збирання, обробку та відображення на електронних картах місцевості єдиної інформації про тактичну обстановку в масштабі часу, близькому до реального, а також ідентифікацію цілей та видачу цілевказання засобам вогневого ураження. Крім того, вона координує дії всіх частин і підрозділів від бригади і нижче та доводити необхідні дані до окремої бойової машини.

7. Зменшення часу на проходження оперативної інформації за рахунок впровадження швидкодіючих пристроїв для всіх категорій радіоапаратури.

к.т.н. Ткаленко О.М. (ДУІКТ)

# ПРОТОКОЛ MPLS – НОВА ТЕХНОЛОГІЯ ДЛЯ ВИКОРИСТАННЯ У МЕРЕЖАХ IP

З моменту виникнення і початку використання в комерційних цілях – мережа Internet швидко еволюціонувала з суто дослідницького проекту в комерційну мережу світового масштабу. Мережа Internet є зручним і високоефективним у фінансовому відношенні середовищем для співпраці користувачів, навчання, електронної торгівлі і розваг. Спочатку IP-технології були орієнтовані на передачу даних, для чого було цілком достатньо програмних маршрутизаторів. З появою нових мультимедійних додатків типу IP-телефонії, які вимагали вищих швидкостей передачі і підтримки більшої смуги пропускання, виникла потреба у створенні технологій і пристроїв, що забезпечували б можливість швидкої комутації апаратними засобами. З'явилися нові пристрої комутації, які вирішують проблему вузьких місць комутації в середовищі локальної обчислювальної мережі, а також нові маршрутизатори, що поліпшують ситуацію з маршрутизацією, шляхом перекладання в швидкодіючу апаратну реалізацію процедур перегляду маршрутних таблиць для пересилання пакетів.

Мережа Internet значно була вдосконалена відносно смуги пропускання, кількості вузлів, географічного обсягу та об'єму потоків даних, які передаються. В той же час відбувається еволюція мережі Internet від служби негарантованої доставки у напрямку мережної інфраструктури інтегрованих або диференційованих служб з наданням гарантій якості обслуговування (Quality of Service – QOS), які необхідні управляємим віртуальним приватним мережам (Managed VPNs), передачі голосу в середовищі IP (Voice over IP), відеоконференції і широкосмуговим службам мультимедійних застосувань.

Інфраструктури магістралей провайдерів в даний час використовуються для надання таких послуг, як виділені лінії з тимчасовим ущільненням сигналів, послуг ATM і Frame Relay, голосовим і відеопослугам, а також послуг мережі Internet. Магістралі ATM виключно популярні завдяки їх надійності і універсальності при наданні різних типів послуг. Проте технологія ATM погано інтегрується з IP мережами; крім того, у разі використання IP протоколу в середовищі ATM виникають серйозні проблеми при розширенні мережі.

Останніми роками промисловість шукала способи об'єднання переваг IP технології і режиму асинхронної передачі (Asynchronous Transfer Mode – ATM), наприклад IP маршрутизації з високою продуктивністю і пропускною спроможністю комутації ATM. Це призвело до створення і розвитку технології багатопротокольної комутації з використанням міток (Multiprotocol Label Switching – MPLS), що є поєднанням різних реалізацій IP-коммутації (IP switching), що використовують аналогічний за змістом ATM-обмін мітками (Label Swapping) для прискорення відправки IP-пакетів; при цьому не потрібне внесення змін до існуючих IP-протоколів маршрутизації.

Основними перевагами використання технології MPLS є великі можливості розширення мережі, збільшена швидкість відправки пакетів, інтеграція засобів IP і ATM, перерозподіл потоків даних (Traffic Engineering), використання віртуальних приватних мереж MPLS (Virtual Private Networks – VPN), швидка зміна загальної структури маршрутизації і надійне забезпечення якості обслуговування (Quality of Service).

Використання комутації MPLS в магістралях провайдерів служб Internet стало можливим завдяки тому, що вона прозора для кінцевого користувача. Це призвело до значних змін на структурному рівні. Використання технології MPLS змінило модель одноадресатного пересилання даних, яке основане на адресах одержувачів даних, що в основному залишаються незмінними з моменту появи мережі Internet. Проте, у свою чергу, новий підхід до принципів передачі даних впливає на структуру маршрутизації, вимагаючи вирішення складніших завдань.

Ткачов П.О. (ВІТІ НТУУ „КПІ”)

# МЕТОДИ ТА СПОСОБИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЯКЕ РОЗПОВСЮДЖУЄТЬСЯ НА ОПТИЧНИХ НОСІЯХ ІНФОРМАЦІЇ, ВІД НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ, КОПІЮВАННЯ ТА ТИРАЖУВАННЯ

Порушення авторських прав виробників програмного забезпечення (ПЗ) приводить до багатомільйонних збитків, які вони несуть у результаті нелегального розповсюдження і використання ПЗ. Основними напрямками боротьби з комп’ютерним піратством є законодавчий шлях та шлях використання систем технічного та програмного захисту ПЗ. Основними способами розповсюдження ПЗ є тиражування ПЗ на оптичних носіях типу CD та DVD або використання можливостей системи Internet.

У доповіді проаналізовано стан в області розробки систем програмно-технічного захисту ПЗ, яке розповсюджується на оптичних носіях, від нелегального копіювання та тиражування. Зазначено, що негативні теденції удосконалення технологій злому і копіювання ПЗ обумовлюють високу актуальність розробки та застосування нових методів захисту. У даний час питаннями розробки та комерційного застосування систем захисту займаються такі відомі компанії, як Microsoft (США), Macrovision (США), Sony (Японія) та Protection&Technologies (Росія). Як показано у [1] системи захисту повинні забезпечити як неможливість створення точної копії оригінального CD чи DVD диска, так і зробити дуже скрутною або зовсім унеможливити роботу хакера по злому захищених комп’ютерних програм. З іншого боку, системи захисту повинні бути прозорими для кінцевих користувачів і не створювати додаткових труднощів при використанні захищеного ПЗ.

Крім цього системи захисту повинні бути сумісними з усіма існуючими типами CD та DVD пристроїв для зчитування інформації та легко інтегруватися в існуючі технологічні ланцюжки виробництва дисків у промислових умовах [3].

На відміну від існуючих способів захисту, де використовуються криптографічні методи [5] або методи, пов’язані на аналіз геметрії диску, були запропоновані нові методи та способи захисту оптичних носіїв. Ці методи базуються на тому факті, що на оптичних носіях типу CD та DVD існують специфічні зони, де є можливість запису довільної інформації таким чином, що при копіюванні або тиражуванні в умовах промислового виробництва, ця інформація не буде перенесена на копію [4].

Кінцевим результатом роботи є програмно-технічний комплекс, який має назву „Guardian” (2002 рік) та „IronDisc” (2008 рік) [2,4]. Можливості цього комплексу дозволяють інтегрувати систему захисту в авторське ПЗ та тиражувати захищені диски невеликими партіями на CD-R та DVD+R дисках як за допомогою роботизованого комплексу, так і без нього шляхом застосування типового ПК. Великі тиражи дисків на CD-ROM та DVD-ROM можуть бути зроблені в умовах промислового виробництва, що обумовлюється легкою інтеграцією комплексу в інуючі заводські технології.

ЛІТЕРАТУРА

1. *Ткачев П.А., Синицкий А.Н.* Защита информации на компакт-дисках от нелегального копирования и тиражирования. // Безопасность информации. 2000 – № 4(14).

2. *Ткачев П.А., Синицкий А.Н.* Программа для защиты компакт-дисков от несанкционированного копирования и тиражирования „Guardian”. Свидетельство об официальной регистрации программы для ЭВМ. №2002610215. Российская Федерация. 2002.

3. *American National Standards Institute.* International Committee on Interface Technology Standards T10. Project 1836D. Revision 2a. November 2008.

4. *Pavel Tkachev, Alexander Sinitsky.* Patent application. Storage medium. Attorney Docket No 025864-000300US. October 2008.

5. *Royal Philips Electronics.* Video Content Protection System for the DVD+R/+RW Video Recording Format. System Description. Version 1.3. July 2005.

Токовенко А.В .( ІТС НТУУ „КПІ”)
к.т.н. Ладик О.І.( ІТС НТУУ „КПІ”)

# ПОРІВНЯЛЬНІ ВЛАСТИВОСТІ ТЕХНОЛОГІЇ DECT ТА Wi-Fi

В зв’язку з поширенням технології Wi-Fi для організації безпровідного доступу до мережі Internet у громадянських місцях виникла потреба порівняння її можливості з технологією DECT, яка є технологією мікростільникового зв’язку і також забезпечує абонентський безпроводовий доступ Wireless Local Loop (WLL) до телекомунікаційної мережі.

До переваг обох технологій Wi-Fi та DECT відноситься відсутність використання кабелів, що зменшує вартість їх застосування. Технологія DECT забезпечує роботу в межах свого застосування з пристроями різних виробників, у той же час технологія Wi-Fi має певну сумісність з такими пристроями, що обмежує можливості з’єднання абонентів або зменшує швидкість передачі інформації

Мережі Wi-Fi мають велику швидкість передавання даних, підтримують роумінг, тому клієнтський термінал може переміщуватись між точками доступу. Проте радіус дії станції до точки доступу обмежений.

Технологія DECT дозволяє створення домашніх безпроводових багатотермінальних систем, мікростільникових корпоративних систем, WLL тощо. Вона не потребує частотного планування і дозволяє співіснування різних DECT–систем у загальному частотному діапазоні. Відсутність каналу керування підвищує стійкість до завад.

Випромінення має рівень безпечний до здоров’я. Відстань базових станцій від контролера до 5 км, проте стандарт DECT має низьку швидкість передавання даних відносно стандарту Wi-Fi.

Порівняння властивостей обох технологій наведено у таблиці.

*Таблиця*

| **Властивості техологій** | **DECT** | **Wi-Fi** |
|---|---|---|
| Діапазон частот | 1,9 ГГц | 2,4 ГГц |
| Потужність випромінювання | 10мВт | 100мВт |
| Швидкість передачі даних | до 128 Кбіт/с | від 11 Мбіт/с |
| Хендовер | безшовний | з розривом або затримкою |
| Середній радіус дії БС | 300м | 100м |
| Випадки злому радіо каналу | невідомі | відомі |
| Частотне планування мережі | не потрібно | необхідно |

ЛІТЕРАТУРА

1. *Лукин М.* Стандарты беспроводной связи. Современная электроника, 1/2005.
2. *Григорьев В.А., Лагутенко О.И.*, Распопов Ю.А.. Сети и системы беспроводного доступа. – М.: Экотрендз, 2005.
3. *Дингес С.И.* Мобильная связь: технология DECT. – М.: Солон, 2003.

к.т.н. Толюпа С. В. (НТУУ „КПІ”)
Мінакова М. В. (НТУУ „КПІ”)

# РЕАЛІЗАЦІЯ ІНТЕЛЕКТУАЛЬНИХ ПОСЛУГ НА МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ НОВОГО ПОКОЛІННЯ

Завданнями сучасних телекомунікацій є забезпечення доступу до абонентів, до інформації і забезпечення мобільності. Концепція інтелектуальної мережі (*Intelligent Network, IN*), є способом швидко створювати нові телекомунікаційні послуги відповідно до специфічних для кожної з них вимог, забезпечуючи одночасну і повсюдну доступність цих послуг абонентам будь-якої базової телекомунікаційної мережі.

Досвід функціонування телекомунікаційних операторів в економічно розвинених країнах свідчить про стрімке зростання обсягів виробництва й споживання інтелектуальних послуг, які вже зараз забезпечують компаніям понад третину отриманого прибутку. Незважаючи на високі первісні витрати на створення інтелектуальних платформ, вони не тільки швидко окуповуються за рахунок високого попиту на надані послуги, але й генерують розвиток і модернізацію традиційних телекомунікаційних мереж, підвищуючи цим інвестиційну привабливість телекомунікаційного сектора в цілому [1].

Мультисервісна мережа являє собою універсальне багатоцільове середовище, яке призначене для передачі мови, зображень і даних з використанням технології комутації пакетів. Вона відрізняється надійністю, характерною для телефонних мереж, і забезпечує низьку вартість передачі, розраховуючи на одиницю об’єму інформації. Загалом, основне завдання мультисервісних мереж полягає у тому, щоб забезпечити роботу різнорідних інформаційних, телекомунікаційних систем і додатків у єдиному транспортному середовищі, коли для передачі звичайного трафіка (даних), і трафіка іншої інформації (мови, відео й т. ін.) використовується єдина інфраструктура.

Мультисервісні мережі є самостійним класом мереж, на базі яких може бути здійснене надання широкого набору як традиційних, так і нових послуг. Визначення мультисервісних мереж як самостійного класу означає, що їх регламентація повинна здійснюватися на основі нормативно-технічної бази, що враховує особливості інтеграції різних послуг і системно-технічних рішень в рамках однієї мережі [2].

Базові послуги, що надаються існуючими мережами зв’язку і мультисервісними мережами повинні володіти ідентичними характеристиками. Це означає, що мультисервісні мережі повинні забезпечувати виконання прийнятих норм і вимог для кожного типу послуг, включаючи показники якості, параметри інтерфейсів, адресацію/нумерацію і т. ін.

На початковому етапі розвитку мультисервісна мережа буде інтеграцією мережі з комутацією каналів і з комутацією пакетів. Навряд чи можна припустити, що існуючі мережі комутації каналів (ТМЗК, *ISDN*) просто вимкнуть і забудуть про їх існування. І так само важко сьогодні сказати, яка технологія комутації складе основу мережі майбутнього. Зараз лідерами можна вважати *IP* і АТМ, але при нинішніх темпах розвитку телекомунікацій появу нових і вдалих технологій можна чекати у будь-який момент. З урахуванням того, що в мультисервісних мережах нового покоління передаватиметься і оброблятиметься трафік різних видів (трафік реального часу, трафік даних, відеоінформація), можна виділити три основні напрями робіт:

1) нові телекомунікаційні послуги з універсальним доступом з ТМЗК/*ISDN* і *IP*-мереж, що базуються на основі еволюції концепцій інтелектуальної мережі і конвергенції послуг зв’язку;

2) нові підходи до проблеми якості обслуговування; запропоновано їх немало (*MPLS*, резервування ресурсів *RSVP* і т. ін.), проте робота в цьому напрямі ускладнює відсутність узгодженої структури мультисервісної мережі наступного покоління;

3) і, нарешті, проблема сигналізації і управління в мультисервісній мережі.

В принципі, процес конвергенції розвинутий, і головна проблема на даний момент полягає, мабуть, у відсутності єдиної системи сигналізації, так що напрям (3) можна назвати домінуючим. Єдиної системи сигналізації поки не створено, а ось пристрій, що дозволяє обробляти і перетворювати різні протоколи сигналізації, вже є.

Кожна комунікаційна підсистема мультисервісної мережі може використовувати різну техніку для обробки свого трафіку (голосу, даних або відео), і на кожній стадії цього процесу можуть застосовуватися різні комунікаційні стандарти. На границі мережі ці потоки повинні бути зведені до єдиного формату. Це завдання вимагає значних обчислювальних потужностей. Його виконують відповідні шлюзи.

У випадку переваги на мережі аналогового устаткування, морально й фізично застарілого, можливо модернізувати мережу, використовуючи програмний комутатор у якості розподіленого телефонного концентратора, що дозволить домогтися зниження витрат на будівництво й експлуатацію мережі за рахунок того, що замість двох роздільних мереж (з комутацією каналів і пакетів) буде будуватися одна мережа, функції вузлових (транзитних) АТС буде виконувати програмний комутатор, з'явиться можливість більш економічної організації нових послуг.

При модернізації мережі необхідно планувати модернізацію застарілого набору устаткування, забезпечивши його можливістю надавати базовий перелік послуг, і почати впроваджувати устаткування програмної комутації на транзитному рівні. Поступово нове пакетне транспортне середовище буде розширюватися й заміщати аналогові сегменти так, що в результаті ми перейдемо до цифровізації на всій мережі – від середовища передачі до середовища послуг, з таким інтерфейсом, що дозволить одержувати клієнтові доступ до будь-яких додатків. Навіть настільки поверхневе знайомство з архітектурою мереж наступного покоління дозволяє зробити висновок, що у світі комунікацій відбуваються значні зміни. Народжується нова універсальна технологія передачі різних типів трафіку по єдиній мережевій інфраструктурі. Все це ставить непрості завдання як перед сервіс-провайдерами, так і перед розроблювачами й виробниками устаткування для мультисервісних мереж [3].

Своєчасне розгортання мультисервісних мереж в Україні дає унікальний шанс для прискореного розвитку всієї телекомунікаційної галузі країни, зокрема, в області створення і розвитку конкурентоспроможного вітчизняного виробництва устаткування мереж, що забезпечує високошвидкісний обмін інформацією по всій території країни, а також в області розробки високопродуктивних систем білінгу для здійснення розрахунків за надані абонентам послуги передачі даних.

Зважений підхід України до питань впровадження інтелектуальних послуг на мультисервісних мережах в нашій країні дозволить уникнути ухвалення поспішних рішень, спираючись на досвід побудови таких мереж в інших країнах, і провести ретельний аналіз всіх аспектів цього процесу. Тим самим, Україна отримала унікальний шанс врахувати на практиці як позитивний, так і негативний досвід зарубіжних країн. Професійне вирішення вищезазначених питань – важливий крок до формування конкурентоспроможного телекомунікаційного ринку в Україні.

ЛІТЕРАТУРА

1. *Толюпа С.В.* Принципи побудови мультисервісних мереж на концепції NGN. Вісник Черкаського державного технологічного університету. Спецвипуск. – Черкаси. – 2007. – С. 56 – 59.

2. *Стеклов В. К., Кільчицький Є. В.* Основи управління мережами та послугами телекомунікацій. – К.: Техніка. – 2004. – С. 438.

3. *Беркман Л. Н., Толюпа С. В.* Архітектурна концепція побудови, принцип реалізації, ефективність застосування інтелектуальної телекомунікаційної мережі. Збірник наукових праць ВІТІ НТУУ "КПІ". – № 2. – 2007 р.

Фесьоха В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

# ВИМОГИ ДО МУЛЬТИАГЕНТНОЇ СИСТЕМИ АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКА

Існуючі переваги мультиагентної системи аналізу мережевого трафіка за схемою (менеджер-агент) на відміну від систем з жорсткою структурою підтверджують її доцільне застосування до запобігання та швидкого виявлення мережевих руйнівних інформаційних впливів (мережевих атак). Система представляє собою набір програмних модулів, розподілених по вузлам локальної мережі, що робить її розподіленою і відповідає основній концепції побудови мультиагентних систем [1]. При цьому агенти між собою не взаємодіють.

Роль програмних агентів полягає у збиранні певної інформації про робочі станції та виявленні в локальній мережі ознак мережевих атак з подальшим занесенням відповідних відомостей до бази даних (БД). До програмних агентів висуваються наступні вимоги [2]:

– ідентифікування мережевого інтерфейсу;
– відкриття мережевого інтерфейсу та створення сесії перехоплення пакетів;
– створення фільтру пакетів;
– захоплення і обробка мережевих пакетів;
– закриття сесії перехоплення;
– занесення відомостей до БД;
– кросплатформенність.

Взята за основу для побудови програмних агентів стандартна бібліотека захоплення мережевих пакетів *Libpcap (Packet Capture library)* забезпечить наявність потужного фільтра пакетів для агентів та застосування системи під управлінням різних апаратних платформ, оскільки вона реалізована для багатьох операційних систем [3].

Завданням головного модулю мультиагентної системи – менеджера є централізована обробка даних, яка полягає в:

– зберіганні достатньо великих об’ємів даних про інциденти безпеки;
– інтелектуалізації обробки досить великих масивів даних з метою відкидання хибних інцидентів;
– виведенні інформації про реальний стан локальної мережі та ознак мережевих атак;
– візуалізація реального стану мережі.

Оскільки певний відсоток хибних інцидентів безпеки завжди присутній в результаті моніторингу мережевого трафіка інтелектуалізація централізованої обробки даних дозволить вирішити цю проблему шляхом застосування для обробки інформації менеджером методу нечіткої ідентифікації інцидентів безпеки.

Візуалізація реального стану локальної мережі полягає у відображенні на моніторі структури мережі у вигляді графа, де вершини графа – робочі станції, зв’язки між ними – трафік, з виділенням тої ділянки мережі, де виявлено ознаки мереженої атаки.

Перспективним напрямком удосконалення мультиагентної системи моніторингу мережевого трафіка вважається реагування системи на мережеву атаку не тільки інформативно, а й методом її блокування.

ЛІТЕРАТУРА

1. *Гурєвич Л.В.* Мультиагентні системи / Вільямс, 2003.– 69 с.
2. *Скляров І.С.* Програмування бойового програмного забезпечення під Linux / СПб.: БХВ-Петербург, 2007, 168 – 176 с.
3. *Лукацкий А. В.* Обнаружение атак / СПб: БХВ-Петербург, 2003. – 608 с.

Фігурна О.С. (ІТС НТУУ „КПІ”)

## WiMAX: БЕЗПРОВІДНА МАГІСТРАЛЬ У МАЙБУТНЄ

Нова революційна технологія безпровідного зв’язку під назвою WiMAX останнім часом привертає до себе все більше і більше уваги.

У мережах WiMAX реалізуються найсучасніші технології радіозв’язку, телекомунікацій і комп’ютерних мереж. Стандарт IEEE 802.16 визначає застосування на фізичному (радіо) рівні широкосмугового шумоподібного радіосигналу з кодовою модуляцією OFDM. На канальному рівні використовується сучасна технологія множинного (багатостанційного) доступу TDMA. На транспортному рівні в мережах WiMAX використовується IP протокол передачі даних, який широко використовується у більшості мережах передачі даних, зокрема, в мережі Інтернет.

Існує 2 види WiMAX: мобільний і фіксований. Розробники стандарту шукали оптимальні рішення як для фіксованого, так і для мобільного застосування, але поєднати всі вимоги в рамках одного стандарту не вдалося. Хоча ряд базових вимог збігається, напрямок технологій на різні ринкові ніші привів до створення двох окремих версій стандарту (точніше, їх можна вважати двома різними стандартами). Кожна з специфікацій WiMAX визначає свої робочі діапазони частот, ширину смуги пропускання, потужність випромінювання, методи передачі і доступу, способи кодування і модуляції сигналу, принципи повторного використання радіочастот та інші показники. Саме тому WiMAX-системи, засновані на версіях стандарту IEEE 802.16 e d, практично несумісні.

У порівнянні з технологією WiMAX можна помітити, що системи стільникового зв’язку 3G-покоління багато в чому поступаються можливостями WiMAX стосовно передачі даних. Технологія WiMAX на основі OFDM (OFDMA для підтримки мобільного зв’язку) характеризується ефективнішим використанням спектру, кращою захищеністю передачі в умовах багатопроменевого поширення, вищими швидкостями передачі даних, підтримує симетричну швидкість передачі в обох напрямках і т. п.

За прогнозами ведучих аналітиків телекомунікаційної сфери, до 2013 року користувачів технології WiMAX буде близько 100 млн. При активній експансії технології WiMAX як на розвинутих, так і на ринках, що розвиваються, у технології WiMAX не буде альтернативи в форматі 4G аж до 2013 року.

Переваги розгортання мереж WiMAX очевидні і для операторів, і для користувачів. За рахунок великої території обслуговування базових станцій, компанії зможуть зменшити загальні витрати на закупівлю та монтаж обладнання, а завдяки високій пропускній здатності каналів зв’язку збільшити асортимент послуг, що надаються. Для звичайних користувачів впровадження цієї технології буде означати можливість безпровідного високошвидкісного підключення до Інтернету віддалених приміських місць.

ЛІТЕРАТУРА

1. *Васильев В. Г.* Технология широкополосного беспроводного доступа WiMAX стандарта IEEE 802.16. Киев – „UNIDATA” – 2007. http://www.unidata.com.ua.

2. *T.S. Rappaport*, Wireless Communications, Prentice-Hall, Upper Saddle River, NJ, USA., 1996.

3. *L. Zheng, D. Tse,* Diversity and multiplexing: A fundamental tradeoff in multiple antenna channels," vol. 49, pp. 1073{1096, May 2003.

4. *Yi Gong and Khaled Ben Letaief*, An Efficient SpaceFrequency Coded OFDM System for Broadband Wireless Communications," IEEE Trans. Commun., vol. 51, no. 11, pp. 2019{2029, Nov. 2003.

к.т.н. Фриз П. В.(ЖВІ НАУ)
Рихальський О. Р. (ЖВІ НАУ)

# УДОСКОНАЛЕНА СИСТЕМА ОБСЛУГОВУВАННЯ КОСМІЧНИХ АПАРАТІВ В УМОВАХ ОДНОПУНКТНОЇ ТЕХНОЛОГІЇ УПРАВЛІННЯ

Космічні апарати (КА) як носії бортової цільової апаратури у складі космічних інформаційних систем відіграють основну роль у забезпеченні високої ефективності виконання ними цільових завдань.

У той же час обмежена надійність бортових систем (БС) та недосконала технологія їх обслуговування в орбітальному польоті разом з іншими факторами можуть знижувати ефективність функціонування таких систем.

При цьому під обслуговуванням КА розуміють сукупність операцій контролю технічного стану (ТС) БС та відновлення їх працездатності, а під системою обслуговування (СО) – сукупність відповідних технічних і програмних засобів орбітального та наземного базування, а також спеціально підготовлений обслуговуючий персонал.

У вітчизняних КА спостереження Землі, як правило, передбачаються тільки традиційні підходи до їх обслуговування в орбітальному польоті.

Це означає, що контроль ТС та відновлення працездатності БС КА здійснюється на основі аналізу значної кількості телеметричних параметрів, з яких використовують інформацію лише про минулий або поточний стан КА.

Разом з тим, у масивах телеметричних вимірів опосередковано існує інформація про майбутній стан КА, однак вона на сьогодні в СО практично не використовується. У доповіді запропоновано можливий підхід до удосконалення СО КА на основі прогнозуючого контролю.

Стосовно контролю ТС зазначимо, що в існуючій СО здебільшого застосовують такі види контролю: функціональний (ФК) – контроль правильності функціонування КА тільки в одному із можливих режимів роботи; контроль працездатності (КП) – контроль правильності функціонування КА в усіх передбачених режимах роботи; діагностичний (ДК) – контроль за виявленням місця та причин відмови БС.

Крім того, прогнозуючий контроль – контроль з метою визначення поточного і майбутнього ТС, який у практиці експлуатації КА поки не знайшов застосування, хоча є одним із найбільш інформативних у порівнянні з ФК та КП.

Одним із факторів, що негативно впливають на якість обслуговування КА інформаційних систем, у тому числі й дистанційного зондування Землі, є існуюча однопунктна технологія управління вітчизняними КА, при якій об’єктивно обмежується час на їх контроль та відновлення працездатності.

Наприклад, згідно з типовою добовою циклограмою роботи перспективних КА “Січ-2” телеметричний контроль БС та передача командної інформації на КА передбачена лише на першому, шостому та чотирнадцятому витках і лише, що цілком природно, під час знаходження КА в зоні радіовидимості наземних засобів (протягом 10…15 хв).

У зв’язку з цим сьогодні необхідно приділяти значну увагу теоретичним і прикладним дослідженням на етапах створення та експлуатації КА, спрямованих на підвищення характеристик надійності БС та вдосконалення їх СО. При цьому основними напрямками вдосконалення прийнятої СО КА на етапі їх цільового застосування можуть бути підвищення:

а) коефіцієнта готовності КА за рахунок скорочення часу на їх обслуговування;

б) апостеріорної ймовірності безвідмовної роботи КА на основі ПК.

Основним підходом при вирішенні завдань прогнозування надійності КА є прогнозування за окремим зразком (однією реалізацією – індивідуальне прогнозування). З урахуванням особливостей випадкового процесу (ВП) виміру телеметричних параметрів КА

завдання індивідуального прогнозування стану КА зводиться до задачі визначення апостеріорного закону розподілу часу до першого виходу процесу за межі допустимої області відносно контрольованої реалізації.

Для визначення оператора прогнозування єдиним прийнятним методом є метод статистичного моделювання множини реалізацій умовного ВП та знаходження на цій основі його характеристик.

Відомо декілька підходів до опису ВП: з використанням канонічного розкладу Карунена–Лоева, на основі канонічного зображення В. С. Пугачова, а також часових поліномів з випадковими коефіцієнтами та ін.

У доповіді показано, що для завдань прогнозування надійності КА найбільш доцільним є канонічне зображення В. С. Пугачова. При цьому запропоновано методику опису апріорних та апостеріорних ВП на основі таких зображень, яка дозволяє безпосередньо розв'язати задачу синтезу алгоритмів прогнозуючого контролю.

Для цього додатково реалізовано низку часткових алгоритмів: розрахунку математичного очікування і отримання центрованого ВП; розрахунку координатних функцій і масивів випадкових коефіцієнтів; моделювання випадкових коефіцієнтів; екстраполяції математичного очікування і ВП в цілому.

Випробування синтезованих алгоритмів з використанням телеметричної інформації з вітчизняних КА показало достатньо прийнятну їх ефективність.

ЛІТЕРАТУРА

1. *Чернявский Г. И., Беркетов Г. А., Комаров И. Д.* Индивидуальный прогноз остаточного ресурса сложных технических систем по результатам эксплуатации. Двойные технологии. – 2005. – № 4. – С. 18 – 23.

2. *Давыдов А. Е., Ульянов С. В., Лут М. А.* Предложения по созданию автоматизированной системы прогнозирования надежности и остаточного ресурса КА длительного функционирования. Двойные технологии. – 2003. – № 2. – С. 25 – 31.

3. *Эксплуатация* радиотехнических комплексов / [под ред. А. И. Александрова]. – М. : Сов. радио, 1976. – 208 с.

4. *Лавриненко В. Ю.* Основы эксплуатации радиоэлектронной аппаратуры. – [2-е изд.]. – М. : Высшая школа, 1978. – 320 с.

5. *Космическая система* оптико-электронного наблюдения Земли и связи „Січ-2". Аванпроект // Пояснительная записка. Часть 6. Космический аппарат МС-2 – 8 „Січ-2". ПЗ-6. – НКАУ : ГКБ „Южное", 2002. – № 3481/1. – 192 с.

6. *Фриз П. В., Андреєв О. В., Рихальський О. Р.* Методика оцінки ефективності обслуговування космічних апаратів дистанційного зондування Землі. Вісник ЖДТУ. Технічні науки. – 2008. – № 2 (45). – С. 18 – 23.

к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)
Головко О.О. (ВІТІ НТУУ „КПІ”)

# ВИБІР СПОСОБУ ПРЕДСТАВЛЕННЯ СТРУКТУРИ МЕРЕЖІ В ПАМ’ЯТІ ЕОМ

В сучасних умовах розвиток інформаційно-телекомунікаційної інфраструктури будь-якої країни досягає того рівня, коли будь-який деструктивний вплив на інформаційно-телекомунікаційні мережі значною мірою впливає на країну в цілому. Тому в війнах майбутнього постає важливе питання планування та реалізації спеціальних операцій в інформаційно-телекомунікаційному просторі противника.

Планування операцій вимагає володіння певною інформацією відносно інформаційно-телекомунікаційної інфраструктури противника:

– структура інформаційно-телекомунікаційних мереж;

– відомості про зв’язки інформаційно-телекомунікаційних мереж противника з інформаційно-телекомунікаційними мережами інших країн, противників, союзників та інше;

– відомості про поділ інформаційно-телекомунікаційних мереж противника на під-мережі;

– відомості про довірені мережі противника;

– відомості про програмне на апаратне забезпечення противника.

Виходячи з цього, для отримання відомостей про інформаційно-телекомунікаційну інфраструктуру противника та її математичного опису, доцільно використовувати терміни та поняття теорії графів.

Оскільки отримання відомостей про інформаційно-телекомунікаційні мережі противника є складною обчислювальною задачею, яка вимагає тривалих обчислень, необхідно застосовувати оптимізаційні алгоритми, які б дозволили виконувати планування спеціальних операцій в інформаційно-телекомунікаційному просторі противника за найменший час та отримувати найбільш достовірні дані. Для цього можливо застосовувати різні представлення графу мережі в пам’яті ЕОМ, наприклад: матриця суміжності, масив статичних векторів, масив списків, список векторів, масив *n*-зв’язних списків або список n-зв’язних списків.

Основні вимоги до представлення: можливість зберігати додаткові данні про вершини та ребра графа, також можливість за відносно невелику кількість операцій змінювати зв’язки між вершинами, можливість швидкого визначення вершин, що зв’язані з даною.

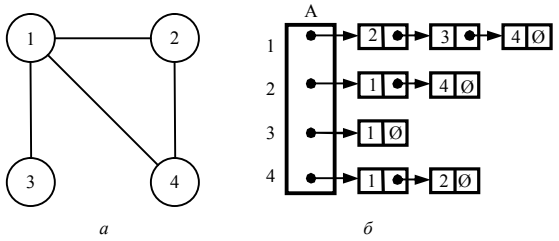



Рис. 1. Способи представлення графа:
*а* – традиційне представлення графа; *б* – масив списків

Як свідчить аналіз джерел за цими напрямками, реалізації цієї задачі відомі різні способи представлення графа в пам’яті ЕОМ. Але оскільки основними операціями, що будуть проводитись з графом будуть визначення вершин, які є суміжні до даної та часта зміна зв’язків між вершинами при постійних вершинах то доцільно представляти граф як масив списків (рис. 1). Використання цього представлення дозволить зберігати в додаткових елементах списку іншу інформацію, наприклад, вагу ребра графа, тощо.

Цема В.Ф. (ІТС НТУУ „КПІ”)
к.т.н. Ладик О.І. (ІТС НТУУ „КПІ”)

# ФУНКЦІЇ ТАРИФІКАЦІЇ ПІДСИСТЕМИ IMS

В телекомунікаційних мережах передавання інформації виникає потреба взаєморозрахунку між користувачем і провайдером послуг. Система розрахунків (тарифікація) є набором процедур, що формують дані про нарахування оплати. Структура підсистеми IMS підтримує два режими тарифікації. При тарифікації в режимі реального часу елементи підсистеми IMS взаємодіють із системою тарифікації в реальному часі. Ця система тарифікації, у свою чергу, взаємодіє в режимі реального часу з абонентськими рахунками, контролюючи або відслідковуючи нарахування плати за використання послуг. При тарифікації в автономному режимі інформація тарифікації збирається після завершення сеансу зв’язку, і система тарифікації не впливає в реальному часі на послугу, що надається.

У системі тарифікації в автономному режимі головну роль відіграє функція збору інформації тарифікації CCF (Charging Collection Function), що приймає розрахункову інформацію від елементів підсистеми IMS (P-CSCFS-CSCF, I-CSCF, BGCF, MGCF, AS, MFRC). Функція CCF обробляє отримані дані, після чого створює й форматує поточний запис даних тарифікації – CDR (Charging Data Record). Поточний запис CDR надходить у систему виставляння рахунків, що формує підсумковий запис CDR з урахуванням інформації, отриманої від інших джерел. Система виставляння рахунків формує фактичний рахунок за послуги.

Тарифікацію в режимі реального часу можуть виконувати такі елементи підсистеми IMS, як S-CSCF, AS і MRFC Коли устаткування користувача UE робить запит у одного із цих елементів на послугу, що вимагає авторизації по параметрах тарифікації, то такий елемент, перш ніж надати абонентові послугу, зв’язується із системою тарифікації в реальному часі OCS (Online Charging System). Система OCS підтримує дві різні моделі тарифікації: пряму тарифікацію події і тарифікацію з резервуванням блоків. При прямій тарифікації система OCS використовує функцію оцінки для знаходження відповідного тарифу для даної події. Після визначення тарифу й вартості з рахунку абонента знімається необхідна сума грошей, і система OCS задовольняє запит відповідного елемента. При використанні такої моделі елемент підсистеми IMS може самостійно надати абонентові відповідну послугу. Сервер додатків AS може надіслати запит і інформувати систему OCS про послугу і про те, скільки разів її потрібно надати. Після цього система OCS, використовуючи функцію оцінки, визначає тариф і підраховує вартість з урахуванням числа наданих послуг. З рахунку абонента знімається певна сума, і система OCS інформує сервер AS про те, що два блоки надання послуги дозволені. У випадку використання моделі тарифікації з резервуванням блоків система OCS, використовуючи функцію оцінки, визначає вартість запитуваної послуги виходячи з інформації про цю послугу, якщо вартість не зазначена в самому запиті. Потім система OCS резервує необхідну грошову суму на рахунку абонента й надає запитуючому елементу відповідну кількість ресурсів. Коли ресурси, надані абонентові, витрачено або послуга успішно завершена, елемент підсистеми IMS інформує систему тарифікації OCS про кількість витрачених ресурсів. Після цього система OCS знімає з рахунку абонента витрачену суму. Така модель тарифікації підходить для тих випадків, коли елемент IMS не може визначити заздалегідь, чи може бути надана дана послуга, або коли необхідна кількість ресурсів невідома до того, як послуга буде використана.

ЛІТЕРАТУРА

1. *H.Kaaranen*, UMTS Networks. Architecture, Mobility and Services – John Wiley & Sons Ltd , 2005. – 406 p.

2. *Poikselka M., Mayer G., Khartabil H.,* The IMS: IP Multimedia Concepts and Services in the Mobile Domain – John Wiley & Sons Ltd , 2004. – 448 p.

Чумак В.К. (ВІТІ НТУУ „КПІ”)
Палій С.С. (ВІТІ НТУУ „КПІ”)

# ВПЛИВ ПЕРЕХРЕСНИХ ЗАВАД В СИСТЕМІ MIMO

В теперішній час для систем радіозв’язку особливо актуальною проблемою є підвищення пропускної спроможності систем. Це обумовлено рядом причин, основними з яких є обмежений частотний ресурс та підвищення вимог до об’єму і швидкості передачі інформації радіозасобами.

Одним з методів підвищення пропускної спроможності є технологія *MIMO* (*Multiple Input Multiple Output* – багато входів – багато виходів). Ідея технології *MIMO* подібна до добре відомого принципу рознесеного прийому, коли в системі зв’язку створюються декілька некорельованих (незалежних) копій сигналу на прийомі. В таких системах, зазвичай, реалізується просторове мультиплексування: потік даних на передачі розбивається на два або більше потоків, кожний з яких передається одночасно з іншими за допомогою різних антен.

У технології *MIMO* поєднані просторово-часові методи приймання з використанням адаптивних антен і методи просторово-часового кодування й просторово-часового розділення сигналів.

Для реалізації просторово-часового розділення сигналів у системах *MIMO* множина виходів (випромінюючих антен) здійснюють передачу декількома шляхами (променями), а приймається ця множина сигналів як множина потоків на кілька приймальних антен (рознесених у просторі). Ключовою властивістю *MIMO* є можливість перетворити ефект багатопроменевого поширення, який значно погіршує якість радіозв'язку, у перевагу для користувача. При застосуванні технології *MIMO* стає можливим збільшення експлуатаційних показників системи радіодоступу без збільшення смуги частот системи.

Але системам з *MIMO* притаманні свої недоліки (при технічній реалізації виникають певні труднощі.

Одною з проблем, які виникають в системах зв’язку з технологією *MIMO*, є наявність перехресних завад. В системах *MIMO* перехресні завади призводять до зменшення пропускної здатності. Вплив перехресних завад на пропускну здатність *MIMO* систем вивчено недостатньо. В зв’язку з цим, дослідження залежності пропускної здатності *MIMO* систем від ступеня подавлення перехресних завад, є актуальним завданням.

В роботі досліджено вплив перехресних завад на пропускну здатність системи *MIMO*. Показано, що вплив перехресних завад на характеристики системи *MIMO* залежить від цілого ряду факторів:

діаграми спрямованості антенних елементів;

відносною відстанню між антенними елементами;

відстанню між передаючими та приймальними антенами.

В результаті проведеного аналізу характеристик системи *MIMO* визначено, що перспективним напрямком вирішення задачі зменшення впливу перехресних завад є розробка методик вибору оптимальних параметрів сигналів та способів обробки сигналів в системі *MIMO* в залежності від конкретного стану радіоканалу.

Чучмій А.В. (ЦНДІ ОВТ ЗСУ)
Гамалій Н.В. (ЦНДІ ОВТ ЗСУ)

# 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 $C^4$ISR. Мережа $C^4$ISR 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 $C^4$ISR 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.

Шевцов С.Ю.(ВІТІ НТУУ „КПІ”)
Фесенко О.Д. (ВІТІ НТУУ „КПІ”)

# ПРОТИРІЧЧЯ МІЖ ЛОГІЧНОЮ СТРУКТУРОЮ І СТРУКТУРОЮ ІНФОРМАЦІЙНИХ ПОТОКІВ В МЕРЕЖАХ SDH

Фізична структуризація мережі корисна у багатьох відношеннях, проте у ряді випадків, що зазвичай відносяться до мереж великого і середнього розміру, неможливо обійтися без логічної структуризації мережі. Найбільш важливою проблемою, що не вирішується шляхом фізичної структуризації, залишається проблема моніторингу і перерозподілу передаваємого трафіку між різними фізичними сегментами мережі SDH.

У великій мережі природним чином виникає неоднорідність інформаційних потоків: мережа складається з безлічі підмереж робочих груп, відділів, філій підприємства і інших адміністративних утворень. Дуже часто найбільш інтенсивний обмін даними спостерігається між комп’ютерами, що належать до однієї підмережі, і лише невелика частина звернень відбувається до ресурсів комп’ютерів, що знаходяться поза локальними робочими групами. (До недавнього часу таке співвідношення трафіків не бралося під сумнів, і був навіть сформульований емпіричний закон „80/20”, відповідно до якого в кожній підмережі 80 % трафіку є внутрішнім і лише 20 % – зовнішнім.)

Зараз характер навантаження мереж багато в чому змінився, широко впроваджується технологія SDH, на багатьох підприємствах є централізовані сховища корпоративних даних, які активно використовуються всіма співробітниками підприємства. Все це не могло не вплинути на розподіл інформаційних потоків. І тепер не рідкі ситуації, коли інтенсивність зовнішніх звернень вище інтенсивності обміну між „сусідніми” машинами. Але незалежно від того, в якій пропорції розподіляються зовнішній і внутрішній трафік, для підвищення ефективності роботи мережі необхідно враховувати неоднорідність інформаційних потоків та моделі її моніторингу.

Мережа SDH з типовою топологією (шина, кільце, зірка), в якій всі фізичні сегменти розглядаються як одне середовище, що розділяється, виявляється неадекватній структурі інформаційних потоків у великій мережі. Наприклад, в мережі із загальною шиною взаємодія будь-якої пари комп’ютерів займає її на весь час обміну, тому при збільшенні числа комп’ютерів в мережі шина стає вузьким місцем. Комп’ютери одного відділу вимушені чекати, коли закінчать обмін пари комп’ютерів іншого відділу, і це при тому, що необхідність в зв’язку між комп’ютерами двох різних відділів виникає набагато рідше і вимагає зовсім невеликої пропускної спроможності.

Не дивлячись на розгалужену фізичну структуру мережі SDH, концентратори поширюють будь-який кадр по всіх її сегментах. Тому кадр, що посилається комп’ютером А комп’ютеру В, хоча і не потрібний комп’ютерам відділів 2 і 3, відповідно до логіки роботи концентраторів поступає на ці сегменти теж. І до тих пір, поки комп’ютер В не отримає адресований йому кадр, жоден з комп’ютерів цієї мережі не зможе передавати дані.

Вирішення проблеми полягає у відмові від ідеї єдиного однорідного середовища, що розділяється. Наприклад, в розглянутому вище прикладі бажано було б зробити так, щоб кадри, які передають комп’ютери відділу 1, виходили б за межі цієї частини мережі в тому і лише в тому випадку, якщо ці кадри направлені якому-небудь комп’ютеру з інших відділів. З іншого боку, в мережу кожного з відділів повинні потрапляти ті і лише ті кадри, які адресовані вузлам цієї мережі.

При такій організації роботи мережі її продуктивність істотно підвищиться, оскільки комп’ютери одного відділу не простоюватимуть в той час, коли обмінюються даними комп’ютери інших відділів.

Шевченко А. С. (ВІТІ НТУУ „КПІ”)
Артюх С. Г. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЇ В СИСТЕМІ ШИРОКОСМУГОВОГО ЗВ’ЯЗКУ СТАНДАРТУ IEEE 802.16

Розвиток стандартів телекомунікаційних систем призводить до виникнення все більше нових загроз інформації, що циркулює в цих системах. Не виключенням став і стандарт широкосмугового зв’язку IEEE 802.16, WiMAX [1, 2].

Міжнародний стандарт ISO/IEC 15408 [3] розроблявся в цілому для інформаційних технологій. Він є на сьогодні основним та найбільш повним стандартом для забезпечення інформаційної безпеки. Але жодний з міжнародних стандартів, тим більше національних, не містять опису дієвих заходів по забезпеченню інформаційної безпеки систем безпроводового зв’язку (СБЗ).

Механізм захисту для систем WiMAX створювався конкретно в рамках розробки стандарту IEEE 802.16. Та при все, система захисту даного стандарту містить „лазійки” для порушників.

Так, розглянувши стандарт IEEE 802.16, були виявлені наступні загрози безпеки інформації:

– можливість подавлення окремих несучих OFDM (каналів OFDMA);

– розширення зони радіоперехоплення інформації за рахунок збільшення зони розповсюдження радіосигналу (внаслідок розповсюдження радіосигналу поза прямою видимістю NLOS);

– загроза збою процесу авторизації абонентських пристроїв в мережі при подавленні (ненавмисних завадах) у момент передачі даних базовою станцією, необхідною для генерації ключа;

– можливість атак фізичного рівня, що ведуть до відмови доступу або лавинний наплив потоку інформації спрямований на виснаження батареї;

– можливість впровадження „хибних” базових станцій (реалізація даної загрози найбільш складна, та потребує значних коштів);

– можливість повторного використання ключа;

– небезпека використання алгоритму шифрування DES, внаслідок його не низької криптостійкості на даний час;

– збільшення об’єктів непрямих атак, за рахунок використання системи для передачі різнорідної інформації (управління відеоспостереженням, банківською системою, IPTV і т.д.)

Аналіз інформаційної безпеки стандарту IEEE 802.16 показав, що існують загрози безпеки характерні для всіх СБЗ. Стандарти безпеки інформації, що розробляються для інформаційних систем, не можуть забезпечити повністю безпеку інформації конкретно в СБЗ. Звідси виникає нагальна необхідність в розробці методів захисту інформації та оцінки захищеності СБЗ.

## ЛІТЕРАТУРА

1. *Шахнович И. В.* Современные технологи беспроводной связи. – Изд. 2-е, испр. и доп. – М.: Техносфера, 2006. – 288 с.

2. *Максименко В.Н., Афанасьев В.В., Волков Н.;* под ред. О.Б. Макаревича. Защита информации в сетях сотовой подвижной связи. – М.: Горячая линия-Телеком, 2007. – 360 с.

3. *ISO/IEC 15408*: 1999 – Information technology – Security techniques – Evaluation criteria for IT security.

Шемендюк О.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

# ОСОБЛИВОСТІ ПРІОРЕТИЗАЦІЇ ПОВІДОМЛЕНЬ В РІЗНИХ УМОВАХ ДІЯЛЬНОСТІ

Робота адміністратора безпеки полягає в обробці, повідомлення, від різних елементів мережі, що надходять на його робоче місце, про порушення безпеки інформаційної системи, які були виявлені за допомогою систем виявлення вторгнень, що використовуються в організації. Аналізуючи ці повідомлення, він своєчасно виявляє інциденти інформаційної безпеки та приймає рішення. Зрозуміло, що адміністратор безпеки не зможе вчасно реагувати на всі повідомлення, що надходять на його робоче місце, та розміщуються в черзі на обслуговування.

Враховуючи різну важливість подій (повідомлень про події) необхідно таким чином встановити послідовність обробки, щоб адміністратор в першу чергу обробляв повідомлення від робочих станцій, які мають найвищий рівень важливості. Аналіз роботи адміністратора безпеки показав, що контроль роботи комп’ютерної мережі, забезпечення безпеки передачі в ній інформації, значною мірою залежить від наступного аналізу черги повідомлень про порушення безпеки інформаційної системи, що з’являється на робочому місці адміністратора безпеки.

Для більш зручної обробки таких повідомлень необхідно проводити певну їх пріоретизацію, для того, щоб повідомлення від найважливіших станцій оброблялись в першу чергу, бо вони мають найвищий рівень важливості. З огляду на це, можна сказати, що при такому сортуванні повідомлення від звичайних робочих станцій будуть аналізуватись адміністратором менш інтенсивно, а можливо і не будуть взагалі. Але повідомлення, наприклад, від сервера баз даних про виявлене порушення безпеки є набагато важливіше і усунення цього порушення принесе набагато більше користі, тому іншими повідомленнями можна знехтувати.

При аналізі повідомлень про інцидент безпеки важливо відмітити такі параметри, важливість оброблюваних повідомлень, час, який витрачає адміністратор безпеки на їх аналіз, а також величину штрафу у випадку перевищення допустимого часу аналізу повідомлення. Провівши аналіз його роботи в різних умовах діяльності, можна виділити два варіанти аналізу повідомлень: без врахування часових обмежень і враховувати час, витрачений на аналіз. В першому випадку виникає максимальна витрата часу але при цьому отримуємо і максимальне значення величини штрафу. В другому випадку необхідно враховувати час, що витрачається на аналіз кожного окремого повідомлення, і при цьому загальна витрата часу не повинна перевищувати допустимого значення. В цьому випадку величина штрафу буде мінімальною.

Таким чином, провівши пріоретизацію черги повідомлень можна значно скоротити потік повідомлень про інциденти безпеки в комп’ютерній мережі та зосередити увагу адміністратора безпеки на найбільш важливих подіях. Подальші дослідження доцільно спрямувати в напрямку пошуку алгоритмів, з допомогою яких можна вирішити дану задачу, а також її програмну реалізацію.

ЛІТЕРАТУРА

1. *Герасимов Б.М., Дивизинюк М.М. , Субач И.Ю.* Системы поддержания принятия решений: проектирование, применение, оценка эффективности. Севастополь: СНИЯЭиП – 2004. – 319 с.

2. *Герасимов Б.М., Тарасов В.А. , Токарев И.В.* Человеко-машинные системы принятия решений с элементами искусственного интелекта. К.: Наукова думка – 1993. – 184 с.

к.т.н. Шестаков В. І. (ЖВІНАУ)
Гудзь С. М. (ЖВІНАУ)

# ФОРМАЛІЗАЦІЯ ЗАДАЧІ РОЗПОДІЛУ СИЛ ТА ЗАСОБІВ МОНІТОРИНГУ МЕРЕЖІ ІНТЕРНЕТ

На сьогоднішній день комп'ютерні мережі (КМ) стали невід'ємною частиною інформаційного простору. Інтернет – це універсальне середовище, що виступає як технічний посередник з передачі інформації, а також є простором хостингу, інформаційним полем, деякою оболонкою, у якій можуть існувати й розвиватися як традиційні, так і раніше не бачені електронні ЗМІ та інші інформаційні проекти [1].

Інтернет розглядається як одне з основних джерел добування розвідувальних відомостей. Вважається, що близько 10–15 % зацікавленої інформації є в Інтернеті вже в готовому вигляді, а інші 85–90 % отримуються у результаті порівняння, аналізу та синтезу розрізнених і розкиданих по різних джерелах фактів, за якими можна скласти, хоча б фрагментарне, уявлення про інформацію, що цікавить [2]. У зв'язку з цим вже давно існує таке поняття, як "комп'ютерна розвідка" (КР). Джерелом розвідувальних відомостей (ДРВ) для КР є сукупність ресурсів, що розміщені у мережі на різноманітних серверах, жорстких дисках окремих комп'ютерів, інформація, що циркулює у мережі, а також мережне обладнання та протоколи передачі даних [3]. У різних джерелах [2–6] міститься велика кількість відомостей, необхідних для проведення КР. Однак відкритим залишається питання ефективного використання наявних сил і засобів у процесі пошуку та спостереження ресурсів КМ, що цікавлять. Актуальним залишається питання забезпечення особи, що приймає рішення, рекомендаціями щодо доцільного та, якщо можливо, оптимального розподілу сил і засобів добування інформації з КМ для своєчасного вирішення завдань з досягнення інформаційної переваги. Метою роботи є постановка та формалізація задачі розподілу сил та засобів добування інформації з КМ для забезпечення своєчасного та якісного виконання завдань спеціальними частинами і підрозділами Збройних Сил України. Виходячи з аналізу типової архітектури КМ, складових етапів добування інформації з таких систем, запропоновано методику визначення раціонального розподілу сил та засобів добування відомостей. При цьому пропонується розділити їх на пости пошуку та спостереження [7].

Пост, що здійснює пошук, – це пост КР, що виконує добування інформації про доменне ім'я, IP-адресу, власника, користувачів, програмне забезпечення ДРВ та передає знайдені відомості до постів спостереження. Пост, що здійснює спостереження, – це пост КР, що виконує доступ до знайдених відомостей, їх перегляд, оцінку та попередній аналіз.

У ході пошуку інформації в КМ кількість постів пошуку буде зменшуватись, а кількість постів спостереження – зростатиме. Планову процедуру, яка буде обґрунтовувати склад і порядок використання сил та засобів КР у цій ситуації, можна назвати розподіленням сил і засобів на спостереження і поточний пошук, тому розв'язання задачі розподілення сил та засобів передбачає комплексну оптимізацію та раціональну розробку двох планів – спостереження і поточного пошуку.

ЛІТЕРАТУРА

1. *Дзюба М. Т., Жарков Я. М., Ольховой І. О., Онищук М. І.*Нарис теорії і практики інформаційно-психологічних операцій: навчальний посібник для курсантів і слухачів. – К., 2005. – С. 14 – 21.

2. *Доронин А. В.* Бизнес-разведка. – К.: Ваклер, 2000. – 564 с.

3. *Меньшаков Ю. К.* Защита объектов и информации от технических средств разведки. – М.: Российский государственный гуманитарный ун-т, 2002. 399с.

4. *Дудихин В. В., Дудихина О.В.* Конкурентная разведка в Интернет. – [2-е изд., испр. и доп.]. – М.: ООО „Издательство АСТ":Издательство „НТ Пресс", 2004. – 229с.

5. *Разведка по* открытым источникам [Електронний ресурс]. – Режим доступу: http://www.onlineci.ru/ oci-in-02.htm.

д.т.н. Шохін Б.П. (в/ч А1906)
Кафтан В.О. (в/ч А1906)
Костюк Т.Я. (в/ч А1906)

# ІНФОРМАЦІЙНО-ПОШУКОВА ПІДСИСТЕМА В СИСТЕМІ РОЗВІДКИ

Сучасний етап розвитку цивілізації характеризується переходом найбільш розвинутої частини людства від індустріального суспільства до інформаційного. Одним з найбільш яскравих явищ цього процесу є виникнення й розвиток глобальної інформаційної комп'ютерної мережі Internet.

Проте розміщення інформації в глобальній комп’ютерній мережі Internet – це тільки частина завдання по обміну даними між користувачами. Основна проблема – це пошук інформації. Цю проблему частково вирішують інформаційно-пошукові системи (ІПС). Проте більшість з існуючих ІПС (Google, Yandex) орієнтовані на пошук в досить широкій предметній області. Для вирішення завдань, які стоять перед воєнною розвідкою необхідно виконувати пошук в більш звуженій та спеціалізованій предметній області.

ІПС відіграють досить значну роль в системах автоматизації інформаційно-аналітичної діяльності та підтримки прийняття рішень, які потребують доступу до неструктурованих даних для подальшого використання в діяльності аналітиків.

На наш погляд перспективна ІПС повинна задовольняти наступним вимогам:

– максимально охоплювати інформаційні ресурси інформаційних мереж (масштаби, формати, мови);

– за рахунок впровадження революційних семантичних методів обробки інформації та методів розпізнавання образів надавати користувачу найбільш точну (адекватну запиту користувача) інформацію;

– оптимально швидко надавати доступ до необхідної інформації користувачу;

– першими в списку результатів пошуку надавати документи, які максимально висвітлюють необхідну користувачу інформаційну картину;

– забезпечувати можливість контролю достовірності інформації;

– виконувати морфологічну обробку слів;

– здійснювати підтримку запитів на заданій мові;

– інтерактивно оновлювати індекс інформаційних ресурсів;

– повнота інформації, як відношення кількості знайдених по запиту документів до загального числа документів в розподіленій інформаційній мережі.

ІПС повинна складатися з наступних модулів:

– обробки запитів користувача та формування списку результатів пошуку;

– пошукової машини;

– збереження запитів;

– сканування розподіленої інформаційної мережі;

– індексування електронної інформації;

– адміністрування.

В перспективній ІПС процес пошуку необхідно реалізовувати із застосуванням принципів розпізнавання образів.

ЛІТЕРАТУРА

1. *Сэлтон Г.* Автоматическая обработка, хранение и поиск информации. – М.: Сов. радио, 1973. – 560 с.

2. *Дубинский А.Г.* Характеристики эффективности информационного поиска в сети Интернет // Научный сервис в сети Интернет: тез. докл. Всерос. науч. конф. – М.: Изд-во МГУ, 2001. – С. 136 – 138.

3. *Файн В.С.* Распознавание образов и машинное понимание естественного языка. – М.: Наука, 1987. – 176 с.

Щербакова Т.П. (ІТС НТУУ „КПІ”)
к.т.н. Ладик О.І. (ІТС НТУУ „КПІ”)

# ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У теперішній час інформація є одним з найважливіших ресурсів людства. Цей факт породжує прагнення володіти цим ресурсом і як наслідок з’являються нові різноманітні засоби несанкціонованого доступу до інформаційних ресурсів(алгоритмічні, програмні, апаратні). Тому існує проблема створення ефективних адекватних засобів інформаційного захисту.

Різноманіття засобів несанкціонованого доступу, їх форм, способів дії та особливостей застосування визначають гранично високу складність задач інформаційного захисту. Вирішення цих задач традиційними технічними та організаційними способами стає малоефективним. Потрібно мати принципово нові ідеї та підходи організації систем інформаційної безпеки. Одним з таких підходів є використання аналогій з організацією життєво важливих актів поведінки і прийняття критичних управлінських рішень в біологічних системах.

Сучасні наукові досягнення в таких областях інформатики як: математичне моделювання стану зовнішнього світу, штучний інтелект, теорія ухвалення рішень, обробка зображень, сигналів і сцен, розпізнавання образів, оптимальне управління, та ін. дозволяють говорити про реальну можливість переходу до нового покоління засобів інформаційного захисту – інтелектуальних систем інформаційної безпеки.

З широкого спектру методів і засобів штучного інтелекту у сфері інформаційного захисту можуть бути ефективно використані і вже використовуються штучні нейронні мережі, М-мережі, експертні системи і системи, засновані на знаннях, еволюційні і генетичні технології, мультиагентні технології та ін.

Зараз зростає і перелік завдань інформаційної безпеки, що вирішуються з використанням інтелектуальних методів і засобів. Серед них задача виявлення вторгнень і атак на автоматизовані інформаційні системи, організація відповідного інформаційного реагування і протидії, проведення періодичного активного контролю наявних засобів захисту, організація автоматизованого аудиту подій безпеки і ін. Для комплексного вирішення цих взаємозв'язаних задач створений і активно розвивається новий інтелектуальний сервіс інформаційної безпеки – активний аудит, який направлений на виявлення підозрілої (зловмисної і/або аномальної) активності з метою оперативного (у масштабі реального часу) прийняття адекватних рішень у відповідь.

Одними з головних засобів інформаційного захисту в сучасних автоматизованих системах обробки інформації є засоби ідентифікації і аутентифікації користувачів, тому вони схильні до найбільшого числа атак. Це привело до появи і активного використання для засобів ідентифікації і аутентифікації різноманітних парольних систем, замково-ключових пристроїв (смарт-карт, магнітних карт, брелків), а також біометричних і криптографічних систем. В біометричних системах ідентифікації та аутентифікації використовуються складні біометричні ознаки особи, що важко піддаються звичайній комп’ютерній обробці, такі як, дактилоскопічні узори, сітка кровоносних судин, райдужна оболонка очей, аналіз особливостей голосу, рукописного і клавіатурного почерків користувачів комп’ютерних

ЛІТЕРАТУРА

1. *Брюхомицкий Ю.А.* Нейросетевые модели для систем информационной безопасности. Учебное пособие. – Таганрог: Изд-во ТРТУ, 2005. – 160 с.

2. *Попов Э.В., Фоминых И.Б., Кисель Е.Б., Шапот М.Д.* Статические и динамические экспертные системы: Учеб. пособие. - М.: Финансы и статистика, 1996. – 320с.

3. *Галушкин А.И.* Теория нейронных систем. Учеб. Пособие для вузов - М.:ИПРЖР 2000 – 416с.

к.т.н. Яблокова С.П. (в/ч А1906)
к.т.н. Куляниця О.Й. (в/ч А1906)
к.т.н. Кальчук І.А. (в/ч А1906)

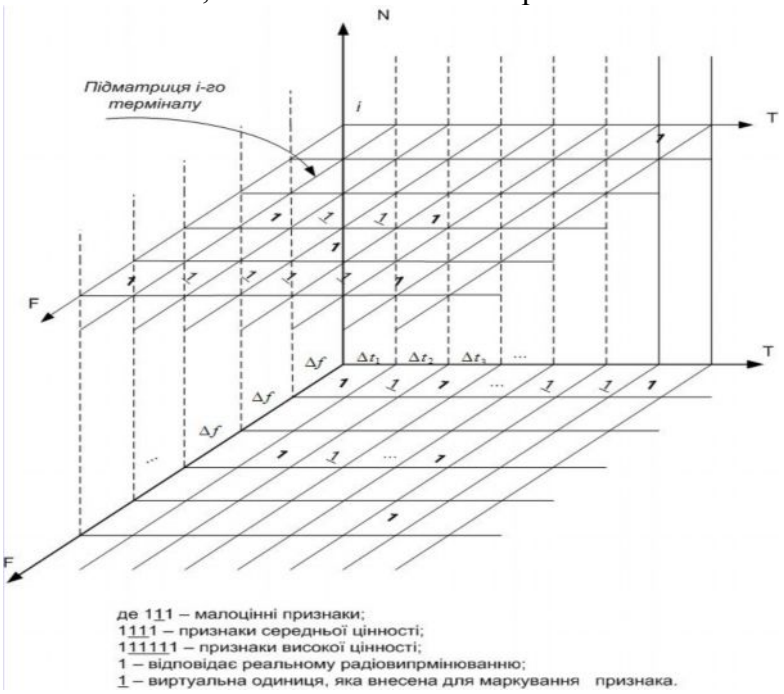
# МАТРИЧНИЙ МЕТОД КЛАСИФІКАЦІЇ РАДІОЗАСОБІВ МЕРЕЖ ЗВ'ЯЗКУ

У роботі розглянутий матричний метод представлення роботи радіомереж різної структури по частоті й тривалості часових інтервалів. Запропоновано методику формування ознак на базі побудованих матриць завантаження, що характеризують процес роботи радіозасобів, яка може бути використана для вирішення завдань класифікації й визначення структури мережі. У цьому випадку конкретний інформаційний зміст повідомлень для технічних засобів зв'язку ніякої ролі не грає.

Як показує практика, у сучасних системах цифрового зв'язку кожному терміналу для передачі інформації в циклі довжиною $T_ц$ виділяється блок стандартних часових інтервалів. Для конкретного користувача послідовність і частота використання часових інтервалів у блоці залежить від пріоритету, що визначає також характер і обсяг переданих даних, тому визначення режиму завантаження циклу дасть можливість одержати структуру мережі, зокрема, виділити управляючий термінал.

Вводиться матричне представлення виділених ресурсів в одному циклі для кожного працюючого в мережі терміналу $i$ ($i=1,...,N$, де $N$ – загальна кількість терміналів у радіомережі). Матричне представлення – це поле двомірних (F – частота, T – час) підматриць, кількість яких визначається числом N. Робота якого-небудь терміналу радіомережі буде адекватно відмічена записом „1" у відповідному матричному елементі підматриці, адреса якого визначається вказівкою частотного рядка й стовпця під номером часового кванта в підматриці, що відповідає номеру термінала. Якщо на будь-якій фіксованій частоті з'являється рівно дві „одиниці", то проміжні матричні елементи будуть заповнюватися віртуальними „1" , що зображено на рисунку. Це буде означати, що між $\Delta t_i^*$ і $\Delta t_i^{**}$ незважаючи на відсутність сигналу здійснювався радіоприйом. Таким чином, чим більше віртуальних одиниць у частотному рядку з урахуванням двох реально зареєстрованих на краях інтервалу [ $\Delta\tau^*;\Delta\tau^{**}$ ], тим вище статус даного термінала в складі мережі.

Обробка вмісту матриць у реальному масштабі часу дозволяє контролювати роботу окремих терміналів і мережі в цілому, що у свою чергу є основою оптимізації використання ресурсу як технічних засобів, так і частотного спектра.



к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
Войцеховський Ю.В. (ВІТІ НТУУ „КПІ”)

# ВОЛОКОННО-ОПТИЧНІ СИСТЕМ ПЕРЕДАЧІ З ДОСЛІДЖЕННЯМ МЕТОДІВ КОМПЕНСАЦІЇ ХРОМАТИЧНОЇ ДИСПЕРСІЇ

Світ телекомунікацій і передачі даних зіштовхується з динамічно зростаючим попитом на частотні ресурси. Ця тенденція в основному пов’язана зі збільшенням числа користувачів Інтернету і також зі зростаючою взаємодією міжнародних операторів та збільшенням обсягів переданої інформації. Смуга пропускання, розрахована на одного користувача, стрімко збільшується. Тому постачальники засобів зв’язку при побудові сучасних інформаційних мереж використовують здебільшого волоконно-оптичні кабельні системи. Це стосується як побудови протяжних телекомунікаційних магістралей, так і локальних обчислювальних мереж. Оптичне волокно (ОВ) у цей час вважається самим досконалим фізичним середовищем для передачі інформації, а також самим перспективним середовищем для передачі більших потоків інформації на значні відстані. Сьогодні волоконна оптика знаходить застосування практично у всіх завданнях, пов’язаних з передачею інформації. Широкополосність оптичних сигналів обумовлена надзвичайно високою несучою частотою, а це означає, що по оптичній лінії зв’язку можна передавати інформацію зі швидкістю близько 1 Терабіт/с.

Широкомасштабне використання волоконно-оптичних ліній зв’язку (ВОЛЗ) почалося приблизно 40 років тому, коли прогрес у технології виготовлення волокна дозволив будувати лінії великої довжини. Зараз обсяги інсталяцій ВОЛЗ значно зросли. У міжрегіональному масштабі варто виділити будівництво волоконно-оптичних мереж синхронної цифрової ієрархії (SDH). Стрімко входять у наше життя волоконно-оптичні інтерфейси в локальних і регіональних мережах Ethernet, FDDI, Fast Ethernet, Gigabit Ethernet, ATM.

Для передачі сигналів в ОВ застосовують два види волокна: одномодове й багатомодове. Свою назву волокна одержали від способу поширення випромінювання в них. Волокно складається із серцевини й оболонки з різними показниками переломлення. В одномодовому волокні діаметр світловідної жили порядку 8–10 мкм, тобто прирівнюєме з довжиною світлової хвилі. При такій геометрії у волокні може поширюватися тільки один промінь (одна мода). У багатомодовому волокні розмір світловодної жили 50–60 мкм, що дозволяє поширення великої кількості променів (багато мод).

Нажаль в процесі передачі сигналів по ОВ є певні фактори, що сильно впливають на якість передачі сигналів у світловодах. Одним з цих факторів є хроматична дисперсія.

У загальному випадку, дисперсія – це розтягування світлового імпульсу, що відбувається під час передачі його в оптичному волокні. Дисперсія сильно обмежує швидкість роботи оптичних систем, помітно знижуючи граничну смугу пропускання. Відмінність часу поширення частотних складових однієї моди приводить до виникнення хроматичної дисперсії.

Хроматична дисперсія може бути компенсована, як за допомогою зменшення смуги випромінюваного спектра лазерного джерела, так і зсувом хроматичної дисперсії кабелю в область більш високих довжин хвиль.

На сьогодні існуючі технології виготовлення компенсаторів дисперсії дозволяють виробляти пристрої для промислового впровадження. Пристрої на основі FBG і DCF компенсації дисперсії в рівній мірі знаходять застосування в мережах, побудованих на SF-волокні. Використання FBG більшою мірою виправдовує себе за компенсації дисперсії в одноканальних системах, тому що FBG може давати великі значення компенсуючої дисперсії (понад 10 000 пс/нм) у вузькій ~ 0,1 нм смузі довжин хвиль. Використання DCF більш

ефективне в багатоканальних WDM-системах через те, що DCF може працювати в широкому діапазоні довжин хвиль.

к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
Корнієнко С.В. (ВІТІ НТУУ „КПІ”)

# АНАЛІЗ МОЖЛИВОСТЕЙ ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

Будь-яка комп’ютерна мережа в найзагальнішому вигляді може бути представлена у вигляді двох взаємодіючих складових: комутаційної системи і сукупності абонентів (включаючи їх устаткування: робочі станції, сервери і ін.). Основним призначенням комутаційної системи є формування транспортного середовища, що забезпечує зв’язок абонентів один з одним. Абоненти мережі потенційно можуть як надавати мережеві послуги, так і споживати їх. Зміна масштабів комп’ютерної мережі наводить до зміни складності її обох складових.

З точки зору розподілу функцій між комп’ютерами в мережі, існує дві основних архітектури мережі: однорангова і клієнт/сервер.

Основною функцією телекомунікаційних систем, що підтримують роботу комп’ютерних мереж, є організація оперативного і надійного обміну даними між абонентами. Головний показник ефективності функціонування телекомунікаційних систем – час доставки повідомлень.

Локальна обчислювальна мережа (ЛОМ) є розподіленою на невеликій території обчислювальною системою, що не вимагає спеціальних пристроїв (за винятком мережевих карт і в складніших конфігураціях – концентраторів) для передачі даних.

Глобальна комп’ютерна мережа (ГКМ) зв’язує інформаційні ресурси комп’ютерів, що знаходяться на будь якій відстані, що передбачає використання різних спеціалізованих пристроїв і каналів зв’язку для високошвидкісної і надійної передачі даних.

Залежно від вигляду ліній зв’язку, що використовуються, канали підрозділяються на дротяні і безпровідні. До безпровідних каналів відносять: супутникові, інфрачервоні, радіорелейні і інші канали зв’язку. У дротяних каналах використовуються телефонні лінії, різного роду кабелі для передачі електричних і оптичних сигналів.

У каналах зв'язку використовується три режими передачі: сімплексний, напівдуплексний і дуплексний.

IP визначає незв’язану пакетну доставку. Ця доставка зв’язує одну або більш пакетно-керовані мережі в глобальну мережу.

Протокол контролю передачі даних (TCP) працює спільно з IP для забезпечення надійної доставки.

Для забезпечення сумісності програм Міжнародної Організації по Стандартизації (ISO) розробила модель мережевої архітектури, що здобула популярність як OSI-модель.

TCP/IP – це установка протоколів, що використовується для зв'язку комп’ютерних мереж і маршрутизації руху інформації між великою кількістю різних комп’ютерів.

Найбільш популярним матеріалом для побудови сучасних комп’ютерних мереж є вита пара. На сьогодні це недорогий і універсальний кабель для створення локальних комунікацій практично будь-якого рівня складності.

Офіційний стандарт 803.u встановив три різні специфікації для фізичного рівня Fast Ethernet.

100BASE-TX – для двопарного кабелю на неекранованій витій парі UTP категорії 5 або екранованій витій парі STP Type1.

100BASE-T4 – для чотирипарного кабелю на неекранованій витій парі UTP категорії 3, 4 або 5.

100BASE-FX – для багатомодового оптоволоконного кабелю, використовуються два волокна.

Fast Ethernet використовує метод передачі даних CSMACD – множинний доступ до середовища з контролем тієї, що несе і виявленням колізій. Fast Ethernet накладає обмеження на відстань між пристроями, що підключаються, – не більше 100 метрів.

Технологія FDDI – це перша технологія локальних мереж, в яких середовищем передачі даних є волоконно-оптичний кабель. Мережа FDDI будується на основі двох волоконнооптичних кілець, які утворюють основну і резервну дороги передачі даних між вузлами мережі. Наявність двох кілець – це основний спосіб підвищення відмовостійкості в

мережі. Як і в Token Ring, в FDDI використовується маркерний метод доступу . відмінність лише в тому, що тут є режим раннього звільнення маркера, який передається після передачі пакета.

Ця технологія відрізняється від Ethernet більше, ніж від Fast Ethernet. А саме: тут використовується інший метод доступу – Demand Priority, який підтримує пріоритетний метод доступу.

За визначенням, сервер – це деякий обслуговуючий пристрій, який в локальній обчислювальній мережі виконує, наприклад, роль центру, що управляє, і концентратора даних. Під сервером, взагалі кажучи, розуміється комбінація апаратних і програмних засобів, яка служить для управління мережевими ресурсами загального доступу.

Від ефективності алгоритмів управління локальними ресурсами комп'ютера багато в чому залежить ефективність всієї мережевої ОС в цілому. Тому, характеризуючи мережеву ОС, були приведені найважливіші особливості реалізації ядра, файлових систем, мережевих сервісів і безпеки.

Для ефективної роботи компанії необхідна централізована програма бухгалтерського обліку, управління фінансами і кадрами, а так само база даних з клієнтами, замовленнями і продажами. Автоматизовані робочі місця співробітників мають бути оснащені програмними пакетами для забезпечення роботи з електронною документацією, можливістю доступу в мережу інтернет, відправки та здобуття електронної пошти.

Сучасний Linux вимагає сучасних апаратних ресурсів, навіть більш ніж Windows, це стосується і оперативної пам'яті, і дискового простору. Залишається лише тішитися тим, що потужності сучасних комп'ютерів постійно збільшуються.

Для забезпечення спільного доступу в інтернет та для забезпечення централізованого управління трафіком необхідно вживання маршрутизатора. За основу може бути узятий як звичайний персональний комп'ютер під управлінням серверної ОС, зі всіма необхідними сервісами і службами (DNS; DHCP; gateway; NAT і так далі) – найчастіше це UNIX-системы. Або готовий пристрій поєднує в собі всі необхідні аппаратно-програмні засоби. У першому випадку є можливість набагато гнучкіше підвести всі функції під конкретні вимоги. Але зростає складність лудіння, необхідно залучення фахівця.

На сьогоднішній день існує безліч фірм, що випускають мережеве устаткування. Найбільш популярними є 3COM, Cisco, Linksys, ATI, D-Link. Різноманітність фірм ускладнює вибір устаткування, оскільки деякі фірми займаються виробництвом вже давно, є брендами і встановлюють високі ціни на свої вироби.

Локальні обчислювальні мережі за останні роки отримали широке розповсюдження в самих різних галузях науки, техніки і виробництва.

Комп'ютерна мережа дозволяє спільно використовувати інформаційні ресурси: каталоги, файли, прикладні програми, ігри, бази даних, текстові файли.

Організація мережі дозволить спростити обслуговування замовників і підвищити його якість. При виписці рахунків всі менеджери користуватимуться єдиною базою даних про користувачів або товари, що є на складі. Для друку рахунків або інших документів можна використовувати один швидкісний принтер.

Особливо широко ЛОМ застосовуються при розробці колективних проектів, наприклад, складних програмних комплексів. На базі ЛОМ можна створювати системи автоматизированного проектування. Це дозволяє реалізовувати нові технології проектування виробів машинобудування, радіоелектроніки і обчислювальної техніки. В умовах розвитку ринкової економіки з'являється можливість створювати конкурентноспроможню продукцію, швидко модернізувати її, забезпечуючи реалізацію економічної стратегії підприємства

ЛОМ дозволяють також реалізовувати нові інформаційні технології в системах організаційно-економічного управління.

к.т.н. Явіся В.С.(ВІТІ НТУУ „КПІ”)
Легкобит В.С. (ВІТІ НТУУ „КПІ”)

# ПЕРСПЕКТИВИ ВПРОВАДЖЕННЯ НОВИХ СТАНДАРТІВ ТЕЛЕКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ

Помітні зміни відбулися в технологіях військових комунікацій за останні роки, зокрема, в області обробки сигналів які, насамперед, пов’язані із впровадженням програмованої архітектури радіозасобів (*Software Defined Radio*). В ідеології побудови тактичних мереж основний акцент зроблений на підтримку мережево-центричних сценаріїв бойових дій. Але головна відмінність нинішнього етапу розвитку тактичних комунікацій, переважно в удосконаленні методів, що використовують у цивільних системах. Результатом цих змін став проект *TACOMS POST – 2000*. Стандарти *TACOMS POST–2000* засновані на підтримці протоколів Інтернету (від *IPv4* до *IPv6*) з використанням наземних, повітряних і космічних ретрансляторів. Серед основних переваг *TACOMS POST – 2000* є можливість передачі відео- та інших мультимедійних даних; підтримку глобальної мобільності за рахунок абсолютної адресації всіх користувачів в адресному просторі *IPv6*; більшу ємність абонентських каналів, їх взаємосумісність; захищеність каналів передачі даних при швидкості трафіку до 1 Гбіт/с.

Архітектура *TACOMS POST- 2000* включає наступні чотири підсистеми:

– Місцева Підсистема Області *Local Area Subsystem (LAS;*
– Підсистема Широкої області *Wide Area Subsystem (WAS);*
– Мобільна Підсистема *Mobile Subsystem (MS);*
– Системи супроводу і підсистема керування *System Management and Control Subsystem (SMCS).*

Всі системи будуються на базі *SDR*-систем і головна перевага технології *SDR* на даному етапі це – можливість домогтися сумісності різнотипних пристроїв. Однак для реалізації всього потенціалу *SDR* необхідно чітко дотримувалися вимог євростандартів щодо конвертації вихідних програмних кодів у формат *Software Communications Architecture (SCA).*

Істотних експлуатаційних переваг досягти неможливо, якщо використовувати *SDR*-технологію лише для того, щоб один пристрій підтримував безліч застарілих стандартів і протоколів. *SDR*-пристрої повинні володіти ще й додатковими можливостями по пропускній здатності, завадозахищеності, крипостійкості й ін. Тому для успіху *SDR*-технології потрібний пошук нових сигнально-кодових конструкцій й алгоритмів їхньої обробки. *SDR* й *SCA*-архітектури дозволяють реалізовувати нові методи обробки сигналів без заміни й переустаткування радіоапаратури, з використанням бібліотек відкритих кодів, що заощаджує час і вартість розробок.

Отже підкреслимо, що в розвитку військового зв’язку суттєво сповільнилися темпи оновлення методів обробки сигналів. З колишнього лідера військові мережі по більшості напрямків потрапили в ар’єргард прогресуючих цивільних технологій. Проте, специфіка військових програм як і раніше стимулює вдосконалення підходів, що зарекомендували себе та надає їм нових якостей.

ЛІТЕРАТУРА

1. *Слюсар І.І., Уткін Ю.В., Дубик А.М., Масесов М.О.* Реалізація перспективних телекомунікаційних технологій та методів цифрової обробки сигналів на вітчизняній елементній базі.// Інформаційні інфраструктура і технології. – Полтава: ПВІЗ, 2007. – № 2. – С. 32 – 36.

2. *Слюсар В.И.* Военная связь стран НАТО: проблемы современных технологий.// Электроника: Наука, Технология, Бизнес. – 2008. – № 4. – С. 66 – 71.

к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
Порох С.В. (ІТС НТУУ „КПІ”)

# ОЦІНКА МОЖЛИВОСТІ ВПРОВАДЖЕННЯ ДОДАТКОВИХ ПОСЛУГ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ПІДПРИЄМСТВА

Новітні технології застосовуються при побудові телекомунікаційних мереж зв’язку масштабів підприємства або навіть оператора зв’язку. Це пов’язано з потребою сполучати декілька філій підприємства, або з’єднувати основні вузли міста. При цьому користувачі вимагають найсучасніших сервісів та послуг, таких як: *IP*-телефонія (*VoIP*), відео за запитом (*VoD*), трансляція телебачення по цифровим каналам зв’язку (*IP-TV*), запис та моніторинг вхідних та вихідних дзвінків (*Mix-Monitor*), надання функцій голосового інтерактивного меню (*IVR*) та інші, для яких потрібні канали з високою пропускною здатністю. Мідні, оптичні та безпровідні мережі, такі як: *FTTB*, *FTTH*, *Ethernet*, *DSL*, *WI-FI*, *WiMAX* можуть надати технічну можливість для впровадження таких сервісів.

Таким чином актуальною є задача реорганізації телекомунікаційної мережі підмприємства з впровадженням додаткових послуг. Телекомунікаційну мережу підприємства можно поділити на мережу передачі данних, телефонну мережу, та мережу цифрового та супутникового телебачення. Впровадження додаткових послуг буде реалізовано безпосередньо в локальній мережі підприємства. За рахунок реорганізації та встановлення додаткового обладнання можна суттєво підвищити швидкість передачі та надійність мережі передачі данних. Майже кожне підприємство для створення локальної мережі (*LAN*) передачі даних використовує звичайні „не інтелектуальні” комутатори 1-го рівня. Якщо замінити їх інтелектуальними маршрутизаторами 3-го рівня (*Level* 3 *Gateway*) та прокласти нові канали „мідної пари” категорії 6-*е*, можна досягти набагато більшої швидкості передачі даних (до 1Гбіт/с), як наслідок в данній мережі зменшиться затримка пакетів при надходженні на локальні сервери. За рахунок інтелектуальної маршрутизації кожному працівнику у відділі можна створити окремі правила на доступ до мережі *Internet* та ресурсів локальної мережі.

Мережа телефонії також зазнає суттєвих змін. При встановленні окремого серверу з програмним забезпеченням *Asterisk* на базі системи *UNIX* та декількох *FXS VoIP* шлюзів, можна перевести телефонну мережу підприємства на *VoIP* мережу з впровадженням додаткових сервісів, серед яких: надання внутрішніх номерів кожному працівнику підприємства; створення інтерактивного голосового меню (*IVR*) на одному або декількох контактних номерах підприємства; запис усіх телефонних дзвінків з можливістю подальшого їх прослуховування; надання функції автоматичного визначення номеру на контактні номери підприємства та багато іншого.

Мережа цифрового та супутникового телебачення, за умови існування такої мережі на підприємстві, не зазнає суттевих змін, але за рахунок надвисокошвидких каналів зв’язку в локальній мережі підприємства можна буде транслювати цифрове телебачення високої чіткості (*HD*), тобто значно збільшити якість трансляцій телебачення по цифровим каналам зв’язку (*IP-TV*) та відео за запитом (*VoD*).

Реорганізована мережа стає уніфікованою, всі сервіси, що будуть впровадженні на підприємстві (Дані, Голос, Текс, Відео) надаються користувачам в межах локальній мережі, яка може бути побудована з використанням технології *Ethernet*.

ЛІТЕРАТУРА

1. *Лагутенко О.И.* Современные модемы. - М.: Эко-Трендз, 2002. – 343 с.

2. *Парфенов Ю.А.* Цифровые сети доступа. Медные кабели и оборудование. – М.: Эко-Трендз, 2005. – 288 с.

3. *Прохоров А.* Рынок беспроводных сетей в цифрах и фактах. – http://www. compress. ru. 2006.

к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
Чередниченко О.Ю. (ВІТІ НТУУ „КПІ”)

# ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ *xDSL* В МЕРЕЖАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ

У сьогоднішньому світі телекомунікацій все більшого значення набуває фактор співіснування стандартних і нових технологій. Саме дана ситуація є основною для мереж наступного покоління. Найбільш економічно ефективним, а також найбільш швидким способом впровадження нових широкосмугових послуг майбутнього виявилося застосування широко розповсюджених мереж доступу на основі мідної пари.

Переважна більшість сучасних цифрових систем передачі (ЦСП) для мідних кабельних ліній побудована на базі технологій, що створювались для цифровізації абонентської ділянки. Ця група технологій об’єднується загальною назвою *xDSL* (*digital subscriber line* − цифрова абонентська лінія). Зараз ЦСП на базі цих технологій використовується не тільки для одночасного підключення окремого абонента до телефонної мережі та мережі передачі даних, але і для організації цифрових телефонних з’єднувальних ліній або магістральних ліній мереж передачі даних.

*xDSL* використовує значно ширшу смугу частот мідної телефонної лінії, чим існуюча телефонна мережа загального користування (ТМЗК). Використовуючи смугу вищих частот, ніж частоти, що використовуються для звичайного телефонного зв’язку (300 Гц − 3400 Гц), *xDSL* дозволяє досягти значно вищої швидкості передачі даних, чим це можливо при використанні обмеженої смуги частот існуючої ТМЗК. Для використання смуги вищих частот, ніж спектр мовного сигналу, устаткування *xDSL* повинно бути встановлене на обох кінцях лінії, а сама фізична лінія повинна забезпечувати можливість передачі сигналу в необхідній смузі частот. Це означає обов’язкове видалення з лінії пристроїв, що обмежують смугу пропускання, таких як пупинівські котушки, а також обмеження числа і протяжності паралельних відведень від абонентської лінії.

Основною перевагою технологій *xDSL* є використання існуючих абонентських ліній місцевої телефонної мережі загального користування для високошвидкісного доступу до послуг мережі. Це дозволяє заощадити витрати на модернізацію мережі абонентського доступу, яка є найдорожчим елементом мережі електрозв’язку. На відміну від інших технологій технологія *DSL* не вимагає попереднього вкладення великих засобів. Деякі інші технології вимагають великих попередніх витрат на створення кабельної інфраструктури і установку станційного устаткування. Часто ці витрати є дуже високими і, на жаль, мають фіксовану суму, незалежно від того, скільки користувачів спочатку підключається до системи. Отже, такі системи дуже критичні до того, який відсоток потенційних користувачів скористається даною послугою.

Технічний прогрес не стоїть на місті, на зміну старим технологіям приходять нові. У сучасних модифікаціях *xDSL* значно збільшена швидкість доступу і максимальна відстань до вузла провайдера. При цьому ціна устаткування зменшилась у декілька разів. Тому на сьогоднішній день *xDSL* по співвідношенню ціна/швидкість/відстань є оптимальним вибором.

ЛІТЕРАТУРА

1. *Парфенов Ю.А*. Цифровые сети доступа. Медные кабели и оборудование. − М.: Эко-Трендз, 2005. – 288 с.

2. *Бакланов И.Г.* Технологии ADSL/ADSL+: теория и практика применения. – М.: Метротек, 2007. – 384 с.

к.т.н. Явіся В.С. (ВІТІ НТУУ „КПІ”)
Шкоденко Ю.П. (ВІТІ НТУУ „КПІ”)

# ВАРІАНТ РОЗВИТКУ МЕРЕЖ МОБІЛЬНОГО ЗВ’ЯЗКУ

Технології стільникового зв’язку розвиваються протягом значного проміжку часу і налічує вже шість поколінь зв’язку (4 базисних покоління + 2 перехідних). Кожне покоління налічує близько десятка технологій і стандартів зв’язку.

В аналогових стандартах застосовувалися частотна модуляція для передачі мови і метод множинного доступу із частотним поділом каналів (FOMA – Frequency Division Multiple Access) зі смугами робочих частот у різних стандартах від 12,5 до 30 Мгц. Це безпосередньо визначало основний недолік аналогових систем – відносно низьку абонентську ємність, що є прямим наслідком недостатньо раціонального використання виділеної смуги частот.

Цей недолік значною мірою був усунутий у стільникових системах другого покоління, орієнтованих на цифрові методи модуляції. Перехід до цифрових стандартів стимулювався широким впровадженням цифрової техніки в системи зв’язку і значною мірою був обумовлений появою надмініатюрних інтегральних схем цифрової обробки сигналів. Разом з тим, перехід до цифрових систем утруднявся широким поширенням багатьох аналогових систем, тобто пряма їхня заміна виявилася неможливою і потрібна була розробка проміжних аналогово-цифрових стандартів. Наприклад, у стандарті D-AMPS була збережена сумісність із системою AMPS, але підвищена ємність каналу керування і помітно розширені функціональні можливості [1].

Одним з найпоширеніших виявився стандарт другого покоління GSM (Global System for Mobile communications – глобальна система мобільного зв’язку в діапазонах 900, 1800 і 1900 МГЦ), у якому застосовується гаусівська частотна модуляція з мінімальним зрушенням частоти для передачі мови і метод множинного доступу з тимчасовим поділом каналів (TDMA – Time Division Multiple Access) [2].

Рух до стандартів третього покоління виявилося досить складним. Сліпа віра в перспективу майбутніх мереж змусила забути провідних світових операторів стільникового зв'язку про розсудливість. У ряді європейських країн за ліцензії було заплачено до декількох десятків мільярдів доларів (у Великобританії – 35 міліьярдів, у Німеччині – 45 мільярдів), у той час як попит на послуги систем третього покоління виявився набагато менше. Більше того, незважаючи на очевидні переваги діючих і перспективних стандартів CDMA, переважне число послуг телекомунікацій, що реалізовані за технологією GSM. Зокрема, виявилося можливим шляхом порівняно нескладної модернізації традиційної мережі GSM забезпечити реалізацію послуг GPRS, EDGE, які в стандартах являються проміжними між другим і третім поколіннями, продекларована як одна з найбільш значимих. Таким чином, можна зробити висновок про те, що технології GSM, як і раніше, будуть домінувати в найближчих років 5. Але сумісність GSM і 3G технологій дозволить плавно, але впевнено впроваджувати технології третього покоління. І можливо за п’ять років частка 3G на ринку телекомунікацій буде значно вищою за GSM. Тобто майбутнє за третім поколінням мобільного зв’язку [3].

ЛІТЕРАТУРА

1. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение . Изд. 2-е, тспр.: Пер. с англ. – М. : Издательский дом „Вильямс”, 2003. – 1104 с.

2. *Карташевский В.Г., Семенов С.Н., Фиростова Т.Н.* Сети подвижной связи. – М.: Эко- Трендз, 2001. – 296 с.

3. *Видання, Ericsson.* Technology in the US PCS Race. „Mobile Communications International”, 1995 вересень/жовтень.

д.філос.н. Ананьїн В.О. (ВІТІ НТУУ „КПІ”)
к.філос.н. Пучков О.О. (ВІТІ НТУУ „КПІ”)

# РОЛЬ ВІЙСЬКОВОЇ ОСВІТИ В ФОРМУВАННІ ОСОБИСТОСТІ ВІЙСЬКОВОГО ПРОФЕСІОНАЛА

На сучасному етапі складання громадянського суспільства, правової української держави, побудови її збройних сил вагомої актуальності набуває визначення концептуальних засад військової освіти. Перехід до інформаційного суспільства, зміна парадигми суспільного розвитку, нові, більш високі вимоги до працівника все це призводить до якісно нової, а саме інноваційної освіти. За таких умов визначення сутності та змісту формування особистості військового професіонала виступає тією науковою проблемою, яка має теоретичне й практичне значення в умовах реформування та розвитку Збройних Сил України.

Проблема формування особистості знайшла певне відображення у наукових дослідженнях В. Андрущенка, В. Абрамова, Е. Афоніна, О. Бойко, М. Варія, О. Гаврілова, Л. Губерського, М. Згуровського, О. Самойлова, О. Турчінова, М. Корольчука, М. Михальченка, Є. Мануйлова, М. Нещадима, В. Пазенка, О. Панфілова, М. Поповича П. Криворучка, М. Ротаня, В. Ягупова, Р. Доор, Ч. Коттона, Н. Коупленда, В. Хаузера та інших вітчизняних та зарубіжних вчених.

У суспільному аспекті формування особистості військового професіонала детерміновано необхідністю забезпечення національної безпеки держави у воєнній сфері, виховання військовослужбовців як громадян і патріотів, забезпечення всебічного, гармонійного та пропорційного розвитку військових професіоналів. Вимогами суспільства до політичних, моральних і професійних якостей військовослужбовців фактично визначається основний зміст формування особистості військового професіонала. У військово-професійному аспекті формування особистості військовослужбовців детерміновано необхідністю забезпечення їх готовності та здатності до виконання завдань за призначенням. Вимоги до формування особистості військового професіонала в освітньому просторі знаходять відображення у наказах, директивах, концепціях, кодексах, інструкціях, положеннях і методичних вказівках органів військового управління, які конкретизують положення законодавчих і нормативно-правових актів з оборонних та військових питань. Способи та форми діяльності суб’єктів соціального формування особистості військового професіонала також обумовлені змістом закономірностей, які визначають функціонування й розвиток суспільства, збройних сил та особистості. З’ясування самого процесу соціального формування особистості військового професіонала саме в освітньому просторі неможливе без осмислення ролі й місця системи військової освіти в широкому соціокультурному середовищі. Оскільки військова освіта є різновидом освіти в цілому, то вона функціонує і розвивається за законами розвитку суспільного та культурного середовища, що її оточує. Українські дослідники В. Андрущенко, Л. Губерський та М. Михальченко підкреслюють, що метою і результатом освітнього процесу має бути освічена людина, як гармонійно складена, культурна, духовна особа, зорієнтована і підготовлена до життя в майбутньому відкритому суспільстві.

Військова освіта є складовою частиною загальної державної освіти. Вона являє собою аналогічно визначений процес становлення і розвитку особистості та передачі їй соціального досвіду. Однак, на відміну від цивільної, військова освіта формує особистість військового фахівця, який повинен і здатен займатися військовою діяльністю. Розглядаючи військову освіту як цілісну систему, військовий педагог М. Нещадим визначає її як сукупність взаємопов’язаних складових, що функціонує в певному соціокультурному середовищі відповідно до притаманних їй закономірностей та принципів із метою ефективної підготовки військових фахівців.

Очевидність взаємозв'язку суспільства та військової освіти визначається, насамперед тим, що мілітарний соціум як носій військової освіти є, водночас, і членом суспільства. Вплив суспільства на військову освіту можна структурувати за такими рівнями. Перший рівень стихійного соціального впливу на майбутніх військовослужбовців формується під дією об'єктивних обставин життєдіяльності суспільства. Другий рівень опосередкованого соціального впливу полягає в здійсненні державою економічних, законодавчих, військових, організаційних заходів для розв'язання певного виду своїх завдань. Ці заходи об'єктивно впливають на зміну можливостей і характеру розвитку, на життєвий шлях тих, хто вирішує присвятити себе військовій справі та освіті. Третій рівень контрольованого соціального впливу є планомірним створенням суспільством і державою правових, організаційних, матеріальних та духовних умов для формування майбутніх офіцерів. Четвертий рівень соціального впливу вимагає враховувати свідому самозміну майбутніх офіцерів, що може мати в цілому як просоціальний, так і асоціальний чи антисоціальний вектор спрямованості.

Основні складові (мережа закладів освіти; нормативно-правова база військової освіти; органи управління військовою освітою) взаємодіють між собою та із зовнішнім середовищем, ґрунтуючись на певних законах, закономірностях та принципах. Їхньому функціонуванню притаманні своєрідні суперечності, що виявляються у процесі досягнення системою військової освіти соціально-державних цілей – як системотворчого елемента – і, водночас, усвідомленого образу передбачуваного результату. Відповідно до Концепції військової освіти в Україні військова освіта інтегрується в державну систему освіти на засадах єдиної законодавчої та нормативно-правової бази. Інтеграція військової і цивільної освіти – не просте, формальне включення низки військових навчальних закладів до складу потужних цивільних університетів та академій, а процес гармонійного об'єднання системи військової освіти і системи вищої цивільної освіти в єдину цілісну загальнодержавну систему освіти.

Актуальність інтеграції військової і цивільної освіти зумовлена об'єктивним характером процесу розвитку світових тенденцій у сфері підготовки військових кадрів. Відтак, висвітлюючи проблеми та перспективи розвитку національної військової освіти доцільно порівнювати наші дії із зарубіжним досвідом у цій сфері. Незаперечним є те, що навіть найкращі моделі систем освіти, створені у світі, не можна механічно переносити на вітчизняні інститути. Крім того, звертаючись лише до світового досвіду, неможливо якісно розв'язувати наші власні проблеми, пов'язані з підготовкою військових кадрів.

Стратегія розвитку військової освіти, що будується на сучасних парадигмальних засадах, має забезпечити створення інноваційної військової освіти з метою досягнення високого рівня професійного, інтелектуального і духовного розвитку та саморозвитку військових професіоналів. Адже стрімкий розвиток військового мистецтва, наукової і технологічної бази, засобів збройної боротьби в західних державах висуває на перший план проблеми особистісної підготовки військових фахівців, які мають бути підготовленими до самостійного оволодіння новими знаннями і технологіями у військово-професійній галузі, здатними до продуктивної діяльності, прийняття та реалізації нестандартних рішень. Водночас, військовий фахівець повинен характеризуватись як гармонійна особистість, спроможна до самовдосконалення, реалізації набутого творчого потенціалу у військово-професійній царині.

Обґрунтовані компоненти парадигми військової освіти сприяють формуванню та розвитку особистості військового професіонала – відповідальної, здатної конструктивно й ефективно виконувати завдання за будь-яких умов і ситуацій військової служби; такої особистості, яка поєднує військовий професіоналізм із громадянською відповідальністю, має відповідний світоглядний кругозір, високу свідомість і моральність. Ці якості у значної мере відповідають сучасній моделі військової освіти, інтегрованої з глобальними трансформаційними процесами в світі, соціумі, освіті, українському суспільстві та його Збройних Силах.

Бецько О.С. (НТУУ „КПІ”)

# ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ІНДИВІДУАЛІЗАЦІЇ НАВЧАННЯ ТА ФОРМУВАННЯ ОСОБИСТОСТІ КУРСАНТІВ ВИЩИХ ВІЙСЬКОВИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Особливості сучасного етапу розвитку освіти в Україні потребують впровадження розвинених форм і методів навчання, що сприяють становленню особистості студента. Особливо актуальними ці завдання є для розвитку збройних сил, зокрема фахівців у галузі телекомунікацій та інформаційних технологій. Саме вони забезпечують обороноздатність та територіальну цілісність держави, відтак, мають відповідати найсучаснішим вимогам, зокрема в сфері інформатизації та використання інформаційних технологій. На новому інформаційному етапі розвитку суспільства особливо гостро постає завдання ефективного використання ІТТ у підготовці висококваліфікованих офіцерських кадрів.

У вищих військових навчальних закладах (ВВНЗ) перевага віддається активним методам навчання, які спрямовані на формування у студентів самостійності, гнучкості, варіативності, критичності мислення. Найпотужнішим джерелом пізнавальної активності курсантів, розвитку їхніх творчих здібностей, інтересів, умінь і навичок та інших інтелектуальних чинників є сьогодні нові інноваційні технології. Актуальним стає питання розробки і впровадження моделей гуманно зорієнтованого навчання і виховання курсантів на основі широкого використання комп’ютерних технологій, зокрема мультимедіа, що дадуть змогу курсанту реалізувати його природній освітній, соціальний і духовний потенціал та забезпечать активізацію всіх сфер діяльності, у першу чергу навчально-пізнавальної. Однією з найсуттєвіших переваг впровадження таких моделей в практику навчання є можливість в повній мірі реалізувати методи індивідуалізації і диференціації. Врахування індивідуальних особливостей курсантів, їх суб’єктивного досвіду дозволяє обрати для кожного оптимальний шлях навчання.

Всебічне застосування в навчально-виховному процесі комп’ютерних технологій навчання має великі перспективи в плані побудови розвинених моделей навчання та розвитку ідей, форм і методів представленої педагогічної технології. Воно сприятиме гуманізації освіти, а також підвищенню ефективності навчання та його інтенсифікації і індивідуалізації в залежності від інтересів, здібностей та власного досвіду курсантів, активізації навчально-пізнавальної діяльності за рахунок введення в навчальну роботу елементів дослідницького характеру, збільшення частки самостійної роботи в навчальній діяльності, що є визначальними для розвитку творчої особистості. Впровадження комп’ютерів у сферу освіти змінює форми, зміст, засоби навчання, наближує його до реалій сучасного життя. Основним завданням викладача у цьому випадку є, як вважає Б.С. Гершунський [1], розвиток особистості того, хто навчається, творчий пошук в організації навчального процесу, добір, розробка і вибір найкращих та найдоцільніших для навчання програмних продуктів.

Прорив через комп’ютеризацію різноманітних видів діяльності, викликаний розвитком Multimedia-технологій, створює інтегроване інформаційне середовище, в якому користувач набуває нових можливостей. При цьому використовуються майже всі сенсорні канали людини. Видатний психолог Б. Ломов [3 – 4] визначає, що комп’ютер є знаряддям людської діяльності, застосування якого якісно змінить можливості пізнання, збільшить накопичення і застосування знань та вважає, що його використання як засобу пізнання людини означає появу нових форм мислення, мнемічної, творчої діяльності, що можна розглядати як фактор історичного поступу психічних процесів людини. Застосування електронної техніки сприяє формуванню таких якостей, як потягу до експериментування, гнучкості, уваги. При цьому

створюються можливості нового нетрадиційного сприймання фактів, встановлення зв'язків між новою та старою інформацією.

Велику увагу дослідники приділяють використанню комп'ютера в процесі вивчення дисциплін мовознавчого циклу. Використання комп'ютера сприяє реалізації найважливішої вимоги комунікативної методики – вдосконалення процесу оволодіння іноземною мовою. Великою перевагою машини є її емоційний вплив на курсантів, що спонукає спрямовувати увагу на формування особистісного ставлення до побаченого.

Швидкість та надійність обробки будь-якої інформації розширення можливостей показу інформації, можливість моделювання за допомогою комп'ютера різних процесів, можливість активізувати змістовну, операційну та мотиваційну сторони навчального процесу, додаткові можливості для індивідуалізації та диференціації навчання, можливість формування за допомогою комп'ютера у курсантів рефлексії своєї діяльності, можливість створення умов для оволодіння курсантами способами організації власної навчальної діяльності, здатність комп'ютера діяти як засіб навчальної комунікації – все це складає потенціал застосування комп'ютера в навчанні іноземних мов [2].

Інформаційно-телекомунікаційні технології у навчанні (ІТТ) розглядаються нами як сукупність принципово нових засобів і методів обробки даних, що є цілісними технологічними системами, які забезпечують збирання, збереження, обробку, передавання і подання інформації, необхідної для педагогічного процесу за допомогою комп'ютерної та телекомунікаційної техніки, локальних та глобальних інформаційних мереж.

Проведений аналіз інновацій у педагогічній теорії та практиці дає підстави вважати, що можливості ІТТ є такими, що дозволяють реалізувати індивідуально-орієнтований підхід до навчання ІМ у ВВНЗ. Для підвищення ефективності навчання в умовах ВВНЗ за допомогою засобів ІТТ необхідно комплексно використовувати основні фактори інтенсифікації навчання: посилення цілеспрямованості, поглиблення мотивації, підвищення інтересу до навчальної діяльності, збільшення інформативної місткості занять, підвищення складності завдань, прискорення темпу навчальних дій, активізація навчально-пізнавальної діяльності курсантів, удосконалення форм організації навчально-виховної діяльності, розвиток умінь та навичок самоосвіти і самовиховання, активізація навчальної діяльності викладача.

Вивчення досвіду використання засобів ІТТ у ВВНЗ в процесі навчання іноземної мови дає змогу визначити можливості вдосконалення методів і організаційних форм навчання за рахунок створення і використання спеціальних програмних засобів – комплексних мультимедійних курсів, які дозволяють реалізувати в навчальному процесі можливості сучасних ІТТ та максимально врахувати специфіку навчального процесу ВВНЗ, пов'язану з особливостями одночасного навчання та військової служби: жорстку регламентацію життєдіяльності курсантів, обмеження використання навчального та особистого часу, підвищені фізичні та психічні навантаження, тощо. Лише за умови комплексного використання сучасних інформаційно-телекомунікаційних технологій можна досягти найбільшого дидактичного ефекту.

ЛІТЕРАТУРА

1. *Гершунский Б.С.* Компьютеризация в сфере образования: Проблемы и перспективы. – М.: Педагогика, 1987. – 264 с.

2. *Далингер В.А.* (Омский педагогический университет) Компьютер и развитие творческого мышления учащихся http://www.nsu.ru/archive/conf/nit/95/ .

3. *Ломов Б.Ф.* Вопросы общей педагогической и инженерной психологии / Б.Ф. Ломов; [Ред-сост. и авт. коммент. В.А. Барабанщиков; Авт. вступ. ст. В.А. Барабанщиков, А.В. Брушлинский, с. 5-24].

4. *Ломов Б.Ф.* Системность в психологии. – М.; Воронеж, 1996. – 383 с.

5. *Сердюков П.І.* Технологія розробки комп'ютерних програм з іноземних мов. – К.: Ленвіт, 1996. – 111с.

Волошина Н.М. (ВІТІ НТУУ „КПІ”)
Терещенко Т.П. (ВІТІ НТУУ „КПІ”)

# СУЧАСНІ АСПЕКТИ ВІЙСЬКОВО-ПАТРІОТИЧНОГО ВИХОВАННЯ МАЙБУТНІХ ФАХІВЦІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Патріотизм є однією з найважливіших соціально-психологічних характеристик людини як особистості. Патріотизм належить до вищих людських почуттів. Необхідність військово-патріотичного виховання у ЗС України зумовлена вимогами, які ставлять перед військовослужбовцями держава і суспільство, Військова присяга і Статути. Високих моральних і патріотичних якостей вимагає від офіцерів Кодекс честі. Особливо велика особиста відповідальність лежить на фахівцях телекомунікаційних систем та мережах спеціального призначення. Від їхніх морально-етичних якостей залежить успіх виконання завдань державного рівня. Дані якості формуються усією системою навчання і виховання у військовому інституті. Метою мого виступу буде охарактеризувати один із елементів даної системи – військово-патріотичне виховання майбутніх офіцерів.

Головною метою військово-патріотичного виховання курсантів є підготовка самовідданих, свідомих захисників Батьківщини, готових за будь-яких умов виступити на захист України, її територіальної цілісності та суверенітету, інтересів українського народу.

Для реалізації мети належить виконати два основних завдання: перше – полягає у формуванні й розвитку громадянина-патріота України, здатного брати активну участь у творчому процесі прогресивного розвитку країни, у зміцненні й удосконалюванні основ суспільства й держави; друге – передбачає здійснення цілеспрямованої підготовки на державному й військово-професійному рівні надійних захисників Батьківщини для успішної реалізації їх функцій, пов’язаних із гарантуванням безпеки і оборони України.

Основними напрямами військово-патріотичного виховання курсантів є:

формування і розвиток загальнолюдських цінностей, національної гідності та свідомості, культури міжнаціональних відносин, необхідних морально-бойових якостей;

вивчення героїчної історії, духовної спадщини, культури, традицій, символів, звичаїв, вірувань та побуту українців;

формування почуття патріотизму, поваги до ЗС України; формування в особового складу свідомого виконання Конституції та законів України, вимог Військової присяги та Статутів ЗС України, наказів командирів і начальників;

вивчення та роз’яснення військовослужбовцям ідейно-теоретичних основ державної незалежності та суверенітету, ролі і місця ЗС, значення військової служби в забезпеченні територіальної цілісності держави; роз’яснення воїнам Військової доктрини України, концептуальних положень розвитку ЗС, розвитку військового будівництва;

вивчення історії формування і будівництва ЗС України, історичних та духовних джерел національної військової організації, пропаганда бойового шляху військового інституту, подвигів і заслуг випускників у воєнний та мирний час; пропаганда життя та діяльності видатних державних, військових та громадських діячів, борців національного руху, заслужених працівників науки, мистецтва та культури;

співробітництво з державними органами влади, громадськими творчими організаціями, ЗМІ з питань військово-патріотичного виховання, військово-фахової орієнтації молоді та підготовки її до служби у Збройних Силах України.

Система засобів військово-патріотичного виховання включає три основних компоненти: соціально-педагогічний, організаційний і матеріально-технічний.

Соціально-педагогічні засоби охоплюють основні теоретичні, методичні й науково-практичні рекомендації, розробки з організації й проведення військово-патріотичного виховання, формування поглядів, переконань, потреб і суспільної думки із проблем забезпечення й зміцнення безпеки держави.

До матеріально-технічних засобів належать: навчальні аудиторії, класи й кабінети; музейні експонати; устаткування, техніка, зброя, макети, навчальні поля, спортивні містечка, тири, тренажери. Неоціненну допомогу можуть надати відповідні ЗМІ, бібліотечки з літературою військово-патріотичної спрямованості, відео- та фонотеки тощо.

Організаційні засоби – це комплекс заходів, що здійснюються з використанням соціально-педагогічних і матеріально-технічних засобів у відповідних формах військово-патріотичної роботи з особовим складом.

Всі три групи засобів патріотичного виховання взаємозалежні, доповнюють один одного, і лише їх комплексне використання в процесі взаємодії суб'єкта й об'єкта цієї діяльності дають максимальний ефект.

Реалізація можливостей військово-патріотичного виховання ґрунтується на інтеграції інтересів суспільства загалом й окремої особистості зокрема, що допускає створення умови для прояву її волі, розвитку громадянськості й підвищення відповідальності за долю Батьківщини в межах існуючого законодавства.

Зміст патріотичного виховання реалізується у відповідних формах виховної роботи. Аналіз військово-педагогічної практики патріотичного виховання дозволяє визначити систему форм цієї діяльності.

Основні форми роботи щодо військово-патріотичного виховання:

лекції, бесіди, диспути, вікторини, тематичні вечори та ранки з питань історії України та її Збройних Сил;

творчі зустрічі особового складу з учасниками війни, ветеранами Збройних Сил та військових частин, працівниками культури, мистецтва, творчої інтелігенції;

тематичні вечори на історико-патріотичну тематику;

літературно-художні та музичні вечори, читацькі конференції, обговорення художньої та публіцистичної літератури з питань військової справи;

місячники військово-патріотичного виховання та оборонно-масової роботи спільно з місцевими державними та громадськими організаціями і рухами;

відвідування музеїв, місць бойової слави, меморіалів та пам'ятників;

військові ритуали ;

участь в історико-патріотичних заходах, які проводяться місцевими органами влади, громадськими організаціями та рухами, музеями, закладами культури;

кінолекторії з військово-патріотичної та історичної тематики;

висвітлення життєдіяльності кращих військових колективів у центральних та місцевих ЗМІ;

вікторини і конкурси з історії України, її збройних формувань;

Головними у цій роботі вважаються заходи підготовки та проведення свят, приурочених до знаменних подій в житті держави і Збройних Сил:

Дня Незалежності України;

Дня Перемоги;

Дня Збройних Сил України;

15 лютого – День вшанування учасників бойових дій на території інших держав;

День створення Військового інституту;

річниці звільнення території України від німецько-фашистських загарбників.

У ЗС України набули широкого поширення нові, нетрадиційні форми військово-патріотичного виховання, які позитивно впливають не лише на особовий склад Збройних Сил, а й на суспільство.

ЛІТЕРАТУРА

1. *Національна програма* патріотичного виховання населення, формування здорового образу життя, розвитку духовності та зміцнення моральних засад суспільства. Постанова Кабінету Міністрів України № 1697 від 1998 року.

Гавриленко К.М. (ВІТІ НТУУ „КПІ”)

# ІНОЗЕМНА МОВА ЯК ЗАСІБ РОЗВИТКУ КОМУНІКАТИВНИХ ЗДІБНОСТЕЙ У КУРСАНТІВ ВИЩОГО ВІЙСЬКОВОГО НАВЧАЛЬНОГО ЗАКЛАДУ

Високий рівень розвиненості комунікативних здібностей працівника забезпечує реальний психологічний контакт з колегами, начальниками і підлеглими. Уміння здолати різноманітні психологічні бар’єри, які виникають в процесі взаємодії, визначають плідність міжособистісних взаємин, за допомогою яких гармонійно поєднуються діловий і особовий рівні спілкування.

Аналіз учбових планів і перелік дисциплін, що вивчаються у військовому вищому учбовому закладі, виявив ряд учбових предметів, при викладанні яких можливий розвиток у курсантів комунікативних здібностей. Одним з таких предметів є іноземна мова. Останнім часом значення цього предмету зросло. Без знання іноземної мови (особливо, англійського) практично неможливо у наш час претендувати на вищий службовий статус (наприклад, військовий спостерігач ООН, військово-дипломатична робота), і тим більше влаштуватися на престижну, високооплачувану роботу на цивільному терені.

Перед практичними заняттями з іноземної мови стоїть завдання розвитку комунікативних здібностей у майбутніх офіцерів. У багатьох роботах, присвячених психології спілкування як основний момент в оптимальному спілкуванні розглядається комунікативна ситуація, в якій людині є що сказати, і вона має потребу висловитися. Створення комунікативної ситуації – це один з методів, який сприяє розвитку комунікативних здібностей у курсанта військового вузу технічного спрямування.

Щоб оцінити значення іноземної мови як навчального предмету в розвитку комунікативних здібностей, потрібно добре усвідомити, що отримує суспільство, країна, якщо її громадяни володіють іноземною мовою, і що дає володіння іноземною мовою людині, а через нього – суспільству. Іноземна мова об’єктивно є суспільною цінністю, і її включення в програму вищої освіти – соціальне замовлення суспільства. Іноземна мова, як і рідна, не існує ізольовано від суспільства і не може жити своїм власним життям. Вона тісно пов’язана зі всіма сферами життєдіяльності суспільства: економікою, політикою, мистецтвом, освітою, військовою сферою і так далі, відображаючи менталітет, культуру країни, яку представляє. Іноземна мова, як і рідна мова, виконує дві важливі функції в життя людини і суспільства: спілкування і пізнання. Проте відмінність полягає в тому, що іноземна мова служить засобом не лише міжособистісного, але і міжнаціонального, міждержавного, міжнародного спілкування.

Таким чином, володіння іноземною мовою стає в даний час однією з умов професійної компетентності, у тому числі і військового фахівця. Відзначаючи важливу роль іноземної мови як учбової дисципліни в процесі підготовки фахівця, слід зупинитися на її основних функціях. Безумовно, одна із загальних функцій іноземної мови як будь-якого іншого учбового предмету полягає в забезпеченні загального розвитку студента, розширенні його світогляду, знань про навколишній світ, про людей, що говорять цією мовою.

Іноземна мова як учбовий предмет вносить помітний вклад і в культуру розумової праці що вчаться за рахунок розвитку таких специфічних учбових умінь, як уміння користуватися двомовними лінгвістичними словниками, граматичними довідниками, пам'ятками для раціонального виконання учбових завдань. Все це учить курсантів працювати самостійно, створює передумови для розвитку потреби в лінгвістичній самоосвіті.

ЛІТЕРАТУРА

1. Nunan, D. 1992. *'Research methods in language learning.'* (p.36). Cambridge: Cambridge University Press.

2. Rivers.W.M.(1992). Communicating Naturally in a second Language, Theory and Practice in Language Teaching (pp24-26). Cambridge University Press.

Гнаткевич Л.О. (НТУУ„КПІ”)

# ПРОБЛЕМИ ФОРМУВАННЯ НАЦІОНАЛЬНОЇ ТЕХНІЧНОЇ ІНТЕЛЕГЕНЦІЇ

Людина із загальним низьким рівнем культури, викривленою системою цінностей та духовною „недорозвиненістю”, навіть якщо має диплом про вищу освіту та великий запас професійних знань, не зможе позитивно впливати на розвиток суспільства. А тому на закладах вищої освіти, які готують професійну еліту (у нашому випадку – технічну, а саме: інженерів телекомунікаційних мереж), лежить відповідальність за формування гармонійної, висококультурної, багатої духовно і морально зрілої особистості.

Загальновизнаним є той факт, що для стійкого розвитку економіки країни необхідно готувати управлінську та науково-технічну еліту. Україна разом з природними багатствами має розвинену систему вищої інженерної освіти.

Безумовно, основна увага у навчальному процесі приділяється вивченню спеціальних технічних дисциплін, ґрунтовні знання з яких будуть міцним фундаментом для формування майбутнього високоякісного інженера. Але не слід забувати, що основна характерна ознака людини, що відрізняє її від інших живих істот, – це здатність індивідуального мислення і формування унікального світогляду.

У наш час людині, яка отримує вищу технічну освіту, замало бути просто гарним інженером, який знається виключно на своїй спеціалізації. Вища освіта повинна бути всебічно розвиваючою. Тому й постає питання про необхідність гуманізації системи вищої технічної освіти, у результаті якої студент з об’єкта навчання перетворюється у суб’єкт творчої, розвиваючої навчально-пізнавальної діяльності.

Освіта є гуманістичною не тоді, коли викладаються переважно гуманітарні курси, а коли у центрі її знаходиться студент як суб’єкт, як особистість, коли у достатньому обсязі відбувається його виховання, яке, як відомо, є процесом систематичного і цілеспрямованого впливу на духовний та фізичний розвиток особистості з метою підготовки її до виробничої, суспільної і культурної діяльності. У широкому розумінні – це передача від покоління до покоління життєвого досвіду, культури, моральних цінностей, створених суспільством. Основним його завданням є формування всебічно розвиненої особистості. Тому виховна роль вузів і полягає, в першу чергу, у формуванні особистості студента, передачі студентській молоді не лише певних знань, професійного досвіду, але й формування професійної культури, створення умов для духовного розвитку, саморозкриття молодої людини в цілому.

Має місце ще одна проблема, що постає перед українськими технічними навчальними закладами, вона пов’язана зі зміною системи економічних відносин у країні. Молоді фахівці, з одного боку, повинні бути здатні швидко адаптуватися до вимог ринкової економіки, а з іншого боку, повинні володіти етикою професіонала, почуттям патріотизму, любов’ю до Батьківщини. У деякій мірі перелічені вище вимоги суперечать одна одній, бо близько 50% студентів, які закінчили такі вузи, працюють не за спеціальністю, і не тільки через нестачу робочих місць, ні, а через низьку заробітну плату, невідповідність претендентів вимогам роботодавців та відсутність зацікавленості здобувачів умовами роботи.

ЛІТЕРАТУРА

1. *Гончаренко С.У.* Український педагогічний словник. – К.: Либідь, 1997. – 376 с.

2. *Корсак К.* Педагогіка XXI століття: проблеми та перспективи // Новий колегіум. – 2001. – № 4. – С. 3 – 7.

3. *Ляшенко Л., Ластовченко І.* Зміни соціокультурного середовища в Україні і значення емоційної зрілості молоді // Рідна школа, 2003. – Січень – С. 31 – 33.

Гнатовська Л.Ю. (ВІТІ НТУУ „КПІ”)

# ТЕЛЕКОММУНІКАЦІЙНІ СИСТЕМИ ТА ФОРМУВАННЯ ОСОБИСТОСТІ ФАХІВЦЯ

Важливе місце в системі випереджальної освіти повинно посідати вивчення останніх досягнень в області інформатики, її засобів і методів, а також перспектив подальшого розвитку і практичного використання. Аналіз досвіду різних країн у викладанні інформатики дозволяє затверджувати, що її потрібно розглядати не тільки як важливий засіб інформаційної підтримки навчального процесу, ефективний педагогічний інструмент, але і як необхідний інструмент освіти. При цьому враховується тенденція перетворення інформатики з технічної дисципліни, яка вивчає методи обробки даних за допомогою обчислювальної техніки, в фундаментальну науку про інформацію і інформаційні процеси в природі і суспільстві. Терміни „інформатизація”, „інформаційні технології”, „інформаційні системи”, „Інтернет” – ці сучасні терміни ледь не найбільш часто зустрічаються у різних контекстах. Інтуїтивно люба освічена людина розуміє зміст цих термінів і може дати для них своє слушне тлумачення. Втім, повсякденний характер застосування цих понять не повинен вводити в оману своєю умовною простотою.

**Телекомунікаційна складова** тісно пов’язана з комп’ютерно-інформаційною і повинна передбачити впровадження сучасних телекомунікаційних систем і технологій з використанням різних середовищ розповсюдження сигналів (радіо, оптоволоконні, радіорелейні, супутникові), методів їх передачі та обробки, неоднорідних інформаційних потоків (аудіо, відео, пересувні зображення, дані, телефонні та інші), зокрема: 1. створення та впровадження телекомунікаційних мікрохвильових та оптичних технологій для здійснення передачі інформаційних потоків різного призначення, у тому числі мультимедійних 2. створення методів комутації неоднорідних інформаційних потоків для надання різних інформаційних послуг (телефонні повідомлення, багатоканальні телевізійні передачі, дані, інтерактивна взаємодія з – Web інформацією та іншими Інтернет-додатками), а також для інтеграції послуг, які надаються локальними, регіональними та глобальними телекомунікаційними мережами; 3. впровадження мобільних телекомунікацій в інформаційні системи і сучасних мобільних термінальних пристроїв, у тому числі для прийому мультимедійних інформаційних потоків; 4. адаптація перспективних світових телекомунікаційних технологій на основі інтеграції процесів цифрової обробки даних та сигналів з використанням для управління обчислювальної техніки з надвисокою продуктивністю.

За висновками експертів в умовах радикального ускладнення життя суспільства, його технічної і соціальної інфраструктури вирішальною стає зміна взаємовідношення людей і інформації, яка є таким же стратегічним ресурсом суспільства, як продукти харчування в „аграрному”, а традиційні матеріальні або енергетичні ресурси в „індустріальному” суспільстві. „Інформаційна революція”, як і попередні „аграрна” і „індустріальна” революції, вирішуючи одні проблеми, породжує нові.

Однією з таких проблем є „інформаційний вибух”, тобто надлишок доступної багатьом сучасним людям інформації, якої з’являється більше, ніж спроможна переварити людська свідомість. Він слугує причиною зниження якості мислення серед людей, в тому числі освічених членів сучасного суспільства. Інформаційне перевантаження – це реальність. Фахівці скаржаться, що вони не встигають стежити за оперативною інформацією, яка відноситься до їх предметної області. При цьому величезні обсяги інформації, особливо зібрані у вигляді статистичних даних, стають полем для помилкової, упередженої або навмисно фальсифікованої їх інтерпретації.

Небезпека того, що нечисленні „експерти”, контролюючі інформаційні потоки, можуть експлуатувати менш освічену частину населення, стає реальністю. Ті, хто не має достатнього доступу до інформаційних систем, будуть знаходитися в досить невигідному становищі вже

до кінця нинішнього століття. Експерти відзначають, що у світі встановилися довгострокові тенденції інформаційно-технологічної зміни людської цивілізації. Головною і визначальною тенденцією другої половини поточного сторіччя є стабільний розвиток процесу проектування і виробництва різноманітних пристроїв на основі мікроелектроніки. Наслідком цього рукотворного феномена є революційне здешевлення інформаційно-зв'язної інфраструктури з наслідками, що важко прогнозуються. Внаслідок технічного прогресу питома вартість робіт з передачі і обробки інформації різко знизиться, що призведе до лавиноподібного збільшення кількості і якості (різноманіття форм) комунікативних процесів у всіх сферах функціонування суспільства.

Істотно зміниться структура зайнятості в нематеріальному виробництві, різко скоротиться трудомісткість посередницьких і інформаційно-пошукових робіт і послуг нематеріального характеру. Зміниться структура інформаційних зв'язків людини: кожний значною мірою індивідуально зможе визначити для себе коло повсякденного і іншого спілкування. На фактуру зв'язків все більше буде впливати схожість життєвих орієнтирів, рівень освіти, культурні переваги, захоплення і інтереси.

Звідси витікає можлива зміна концепції „малого кола" і співвідношення „громадянин-держава". Інформатизація змінює і наукові альтернативи. Якщо XX ст. було століттям аналізу і пройшло під знаком спеціалізації, народження нових професій на стиках наук і сфер діяльності, то XXI ст. обіцяє бути століттям синтезу,узагальнюючих багатодисциплінарних підходів, століттям не „вузьких" професіоналів, а фахівців „з розв'язання проблем". Стрімко зростає новий клас в суспільстві – клас освічених „інтелектуальних службовців" або, як його інакше називають – „клас людей знання".

Цей новий клас в США, Японії, низці інших країн вже сьогодні складає більше за половину зайнятого населення. На думку Міжнародної комісії з освіти для XXI ст. існує реальна небезпека того, що вкореняться два типи суспільства – динамічних і відстаючих, причому це буде залежати від доступу окремих осіб до технологій отримання інформації. Розробка стратегії розвитку і використання інформаційних технологій в сфері освіти є однією з ключових проблем стратегічного планування, як на національному, так і на глобальному рівні. Темпи і напрями змін на нинішньому етапі визначаються не обчислювальною технікою і можливостями телекомунікацій, не програмними засобами, а людьми, їх готовністю до змін, їх запитами і проблемами.

Тому інформатизація освіти в світі загалом, і в Україні, що переживає кризовий період свого розвитку, має величезне значення. Прогнозується, що у XXI ст. конкурентна боротьба буде вже відбуватися не тільки за прибутки або ринки збуту, а за місце географічного регіону в світовій спільноті, за стійкий і безпечний розвиток, за право не розміщувати на своїй території радіоактивні відходи і „брудні виробництва", за право бути, якщо можна так висловитись, суб'єктом історії.

Основними учасниками цієї сутички стануть транснаціональні корпорації, а ареною боротьби – інформаційний простір (кіберпростір – в західній термінології). Співтовариства, які не будуть мати в своєму розпорядженні кадри, ефективно працюючі в цій області, і організації, здатні вести активну політику у вказаній сфері і відстоювати свої інтереси, не мають майбутнього. Ми вступаємо у вік „інформаційної економіки", яка відрізняється своїми законами і „правилами гри".

Єфімова О.М. (ВІТІ НТУУ „КПІ”)

# ПЕДАГОГІЧНІ ПІДХОДИ ТА ВПЛИВ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА НА РОЗВИТОК ОСОБИСТОСТІ У ПРОЦЕСІ НАВЧАННЯ В ВТНЗ

Удосконалення системи вищої освіти України в контексті Болонського процесу вимагає значних змін в організації підготовки фахівців у вищих технічних навчальних закладах (ВТНЗ), підвищення рівня методичного та інформаційного забезпечення самостійної роботи студентів, орієнтації на індивідуалізацію навчання, запровадження новітніх навчальних технологій [1]. Визначення змісту та оптимізація процесу професійної підготовки кваліфікованих фахівців у сфері телекомунікаційних систем та мереж спеціального призначення відповідно до вимог Болонської декларації є також актуальною проблемою вищої школи України. Особливий інтерес до професійного становлення фахівців телекомунікаційних систем та мереж спеціального призначення обумовлюється підвищенням соціальної значущості цієї професії, стрімким зростанням і розширенням сфер її застосування.

Наукові дослідження показують, що студент в процесі професійної підготовки починає виробляти та визначати індивідуальні критерії особистої успішності в роботі; вже у ВТНЗ відбувається формування та визначення „планки” для себе. І в цьому випадку необхідна психолого-педагогічна допомога особистості. Але усвідомлювати цю „планку”, норму, зрозуміти її мінливість, рух – це складний процес, тому що він означає становлення й розвиток нових сторін і граней особистісного „Я” у професії [2, 3].

Багато факторів впливають на перетворення індивідуума в повноцінного, активного громадянина. Серед них політична і законодавча система, соціальні інститути – сім’я і школа, засоби масової інформації. Усе це формує почуття громадянського обов’язку і політичної самовпевненості індивідуума в суспільстві. Кожне самостійне суспільство прагне виховати справжніх громадян, роз’яснюючи, прищеплюючи їм основні політичні цінності. Єдині переконання є основою для будівництва будь-якої держави. Тому державі не байдуже, як формуються політичні переконання її громадян. Громадянське виховання розпочинається в дитинстві, з пояснення основних цінностей суспільства, і триває все життя через знання і дотримання законів. Значну роль у громадянській соціалізації відіграють засоби масової інформації. Вони виконують функції соціальної комунікації, інформування і виховання, формування громадянських цінностей, створюють відповідний соціально-політичний клімат.

В сучасних умовах спостерігається активна розробка і впровадження форм, способів і технологій інформаційно-психологічного впливу на індивідуальну, групову і масову свідомість. До таких джерел, каналів і технологій впливу на свідомість, психологію і поведінку людини можна було б віднести: засоби масової інформації і спеціальні засоби інформаційно-пропагандистської спрямованості; глобальні комп’ютерні мережі і програмні засоби швидкого поширення в мережах інформаційних і пропагандистських матеріалів; засоби і технології, що нелегально модифікують інформаційне середовище, на підставі якої людина приймає рішення; засоби створення віртуальної реальності; чутки, міфи і легенди; засоби підпорогового семантичного впливу; засоби генерування акустичних і електромагнітних полів [4].

Таким чином, зрозуміло, що сучасній людині потрібно багато інформації, обізнаність із багатьма галузями знання, щоб нею не могли маніпулювати і застосовувати у своїх корисливих чи корпоративних інтересах. У більш-менш стабільному демократичному суспільстві запобігти цьому простіше, а в умовах глобальних протиріч, гострої політичної боротьби на етапі становлення інформаційного соціуму це дуже складно, і особливо для формування особистості справжнього фахівця телекомунікаційних систем та мереж спеціального призначення.

Засоби масової інформації виражають і формують громадську думку, яку прийнято розглядати як колективне судження людей, в якому ставлення до подій і явищ виявляється у

формі схвалення, осуду або вимоги. Громадська думка формується в процесі руху інформації в суспільстві, відображає людське буття, суспільну практику людей і виступає як регулятор діяльності. Вона створюється під впливом буденної свідомості (включаючи соціальну психологію), емпіричних знань, навіть забобонів, а також науки, мистецтва, політики і, зрозуміло, всіх джерел масової комунікації.

Актуальна потреба в саморозвитку, намагання до самовдосконалення і самореалізації, самоствердження і самопізнання являють величезну цінність самі по собі. Вони – показник особистісної зрілості і одночасно умова її досягнення. Окрім всього, актуальна потреба в саморозвитку, самоактуалізації, самопізнання і самоствердження – це джерело довголіття людини, джерело патріотичного і національного виховання, це джерело активного довголіття, і не тільки фізичного, але й соціального, особистісного. З виразним намаганням до саморозвитку пов'язані й професійні успіхи, досягнення професійного „акме", а також її професійним довголіттям [5]. Проблема формування особистості студента не зводиться лише до передачі знань про основи тих чи інших наук. Розвиток його як особистості та суб'єкта діяльності – це обов'язково: розвиток інтелекту; розвиток емоційної сфери; розвиток морально-психологічної стійкості, готовності до стресів; розвиток впевненості в собі та сприйняття себе; розвиток позитивного відношення до оточення і сприйняття інших; розвиток самостійності і автономності; розвиток мотивації самоактуалізації самовдосконалення; розвиток самоствердження своєї ментальності, самоусвідомлення себе громадянином-патріотом своєї Батьківщини. Студент – не просто об'єкт соціальних впливів, але й, перш за все, суб'єкт соціального розвитку. Від соціальної зрілості цього суб'єкта, його соціальної відповідальності, терпеливості та саморозвитку залежить формування феномену соціальної зрілості самого суспільства. Визначальним фактором у вирішенні цих проблем може бути викладач вищої школи нашої країни.

Отже, формування особистості фахівців телекомунікаційних систем та мереж спеціального призначення передбачає особистісно-орієнтовану спрямованість. Необхідно ширше подавати майбутньому фахівцеві інформацію про себе й створювати ситуації рефлексивного характеру, де він міг би не тільки проектувати себе, свої відносини, але й здійснювати саморозвиток, самореалізацію, самоактуалізацію. Вирішення цих проблем можливо здійснювати, використовуючи особистісно-орієнтовану технологію навчання, що інтегрує процеси засвоєння й придбання теоретичних знань та практичних умінь. Особистісно-орієнтована технологія навчання припускає єдність загальнокультурного, соціального, духовно-морального, професійно-особистісного розвитку майбутнього фахівця; динамічність змін у змісті, методах і формах професійної підготовки; цілісність і фундаментальність навчання, єдність теорії й практики; орієнтацію на впровадження інноваційних форм навчання, нових інформаційних технологій; створення комфортних психолого-педагогічних умов і творчої обстановки для студентів і викладачів.

ЛІТЕРАТУРА

1. *Сбруєва А.* Болонський процес: пошуки шляхів підвищення конкурентоспроможності європейської вищої освіти / Шлях освіти. – 2002. – № 1. – С. 18 – 21.

2. *Решетова З.А.* Психологические основы профессионального обучения – М.: МГУ, 2000. – С. 12 – 14.

3. *Юдин Э.Г.* Системный поход и принцип деятельности. – М.: Наука, 1998. – С. 381 – 382.

4. *Дзюба М.Т., Жарков Я.М., Ольховой І.О., Онищук М.І* Нарис теорії і практики інформаційно-психологічних операцій. За загал. ред., В.В. Балабіна. – К.: ВІТІ НТУУ „КПІ", 2006. – С. 178.

5. *Коваль А.М.* Соціальна активність та розвиток особистості студентів в умовах соціалізації суспільства.: Суспільство. Держава. Армія. Збірник наукових праць (Суспільні науки) / головний редактор В.О. Ананьїн. – Випуск 14. – К.:ВІТІ НТУУ „КПІ", 2008.

Жицька С.А. (НТУУ „КПІ”)
Жицький К.О. (КНЛУ)

# РОЛЬ ІНОЗЕМНИХ МОВ У ФОРМУВАННІ ОСОБИСТОСТІ ВІЙСЬКОВОГО ФАХІВЦЯ

Проблема організації мовної підготовки та мовного тестування особового складу Збройних Сил України продиктована кардинальними змінами, що мають місце в соціокультурному просторі в цілому і в професійній освіті військових фахівців зокрема. Зростання вимог до володіння іноземними мовами особовим складом Збройних Сил України зумовлене, перш за все, реалізацією курсу держави на європейську та євроатлантичну інтеграцію, активною участю України в міжнародній миротворчій діяльності. Як відзначено у Концепції мовної підготовки особового складу Збройних Сил України (наказ Міністра оборони України № 267 від 01.06.2009), в умовах значної активізації міжнародного військового співробітництва, в тому числі в ході миротворчих операцій ООН, де необхідно підтримувати контакти, будувати конструктивні взаємовідносини з союзниками та дружніми країнами, а також приведення армії у відповідність до вимог та стандартів НАТО гостро поставили питання подальшого розвитку й підвищення ефективності функціонування системи мовної підготовки у Збройних Сил України. Мовна підготовка особового складу Збройних Сил – це комплекс узгоджених між собою, планомірних і послідовних заходів навчального та тренувального характеру, спрямованих на вивчення особовим складом іноземних мов у обсязі, визначеному як необхідний для виконання посадових обов’язків, служби (роботи) та навчання за кордоном.

У зв’язку з цим, проблема мовної підготовки особового складу Збройних Сил України в контексті загальної підготовки до здійснення професійної діяльності набула зараз особливої актуальності. Ми не ставимо під сумнів важливість спеціальних військових дисциплін, але разом з тим вважаємо, що справжнім професіоналам військового мистецтва необхідно обов’язково володіти іноземними мовами так, щоб військові фахівці могли оперувати іноземною мовою у повсякденних ситуаціях на рівні максимально наближеному до рівня носія мови. Більш за все, ми впевнені, що військовослужбовці, котрі вільно володіють іноземними мовами, матимуть більше можливостей не тільки для успішної професійної діяльності, а й для особистого розвитку. Тому ми відносимо проблему мовної підготовки до розряду визначальної у системі професійної підготовки особового складу Збройних Сил України. Виняткова важливість проблеми навчання іноземних мов, у цілому, і у військових навчальних закладах Збройних Сил України зокрема, визнається як закордонними
(Пассов Є.І. [3], Сисоев П.В., Ellis, Savignon S. [4], так і вітчизняними вченими (Ніколаєва С.Ю., Скляренко Н.К. та інші). Розуміючи навчання як процес набуття досвіду – як індивідуального, так і соціокультурного, – були виділені основні типи навчання: „підтримуюче навчання” та „інноваційне навчання”. Аналіз даних типів навчання дозволяє нам окреслити підходи до визначення основних цілей та завдань вивчення іноземних мов у військових закладах Збройних Сил України у контексті Європейського простору вищої освіти. „Підтримуюче навчання”, як відомо, отримало назву „авторитарного” і традиційно притаманне як середній, так і вищій школі. Це навчання – тотально зконструйований процес з чітко запланованими фіксованими результатами, й орієнтує кадетів, військових фахівців на слідування наведеним еталонам, засвоєння даних зразків, тобто пов’язано з ретрансляцією, відтворенням соціального досвіду. „Інноваційне навчання”, чи гуманістичне, особисто-розвиваюче, реалізує в сфері дидактики ідеали розвитку творчого потенціалу людини в процесі навчання, орієнтує кадетів, військових фахівців на самостійне освоєння нового досвіду з неочевидними результатами, розвиток своїх пізнавальних та особистих можливостей, тобто пов’язане з творчим пошуком на основі надбаного досвіду, і тим самим його збагаченням. Враховуючи сучасну тенденцію до розвитку взаємовідносин людини та

суспільства, а також ґрунтуючись на аналізах двох напрямків в освіті, ми прийшли до висновку, що пріоритети зміщуються у бік особистісно-орієнтованого навчання, у рамках котрого тільки і можливе вивчення іноземних мов у військових закладах Збройних Сил України у контексті Європейського простору вищої освіти. Розглядаючи проблему організації мовної підготовки особового складу Збройних Сил України, ми виходимо з положення про те, що будь-які знання мають ціннісне, культурне наповнення, коли вони отримуються (засвоюються) людиною в діяльності. Отже, навчання іноземних мов у військових закладах Збройних Сил України повинно бути орієнтованим, у тому числі, і на розвиток здібностей, оцінки навколишнього світу людини, її особисто з точки зору суб'єкта культури. Як відомо, змістом будь-якої освіти є культура. Як відмічає Є.І. Пассов [3], іншомовна культура – дещо більше, ніж знання та вміння, які забезпечують спілкування з іноземцями. Це, спершу, вміння створити атмосферу особистого спілкування, вміння вести діалог культур, визнання менталітету народу через його культуру, виховання поваги до народу та його культури; здібність усвідомлювати, що в особистому спілкуванні не може бути місця агресивності та нетерплячості до іншого; а також розвиток індивідуальності людини на базі оволодіння іноземною мовою та культурою, прагнення людини до самовдосконалення та зміни. Таким чином, метою сучасної освіти є не просто знання, вміння, навички, а вищезгадані якості особистості. Слід підкреслити важливість формування соціокультурної компетентності, як інтегральної особистої якості, необхідної сьогодні будь-якому фахівцю, але в контексті мовної підготовки особового складу Збройних Сил України ця проблема, на наш погляд, набуває особливого звучання, бо вона „дозволяє людині на основі відрефлексованої наявної системи знань визначати свої ціннісні переваги, виходячи з яких конструювати свою поведінку і відносини з партнерами по взаємодії, надавати конструктивну відповідь на проблемні ситуації в системах відносин „людина – людина", самореалізуватися в конкретних культурно-історичних умовах власної життєдіяльності" [4, с. 26]. Таким чином, можна визначити основні цілі та завдання навчання іноземних мов у військових навчальних закладах Збройних Сил України у контексті Європейського простору вищої освіти. Досягненню високого рівня оволодіння іноземною мовою, тобто максимально наближеного до рівня носія мови, у курсантів і слухачів курсів іноземних мов сприяє вирішення наступних задач:

1. Формування соціокультурної компетентності як професійно вагомої особистісної якості у особового складу Збройних Сил України у плані їх професійної та особистісної готовності до здійснення військової діяльності в контексті європейської та євроатлантичної інтеграції. Невід'ємною складовою соціокультурної компетентності особового складу Збройних Сил України є білінгвальна комунікативна компетентність в усному та письмовому спілкуванні, яку необхідно розвивати з урахуванням соціокультурних від'ємностей сучасного поля культурного світу.

2. Формування у особового складу Збройних Сил України готовності конструктивно вирішувати проблемні ситуації, робити адекватний вибір, жити та взаємодіяти з людьми інших культур, мов, релігій.

3. Розвиток у особового складу Збройних Сил України усвідомлення потреби навчатися протягом усього соціально-значимого життя.

ЛІТЕРАТУРА

1. *Наказ Міністра* оборони України № 267 від 01.06.2009 „Про затвердження Концепції мовної підготовки особового складу Збройних Сил України".

2. *Величко Е.* Подготовка в США военных специалистов со знанием иностранных языков. // Зарубежное военное обозрение. – 1996. – № 4. – С. 7 – 9.

3. *Пассов Е.И.* Коммуникативный метод обучения иноязычному говорению. – М.: Высшая школа 1985. – 208 с.

4. *Savignon S.* Communicative Competence: an Experiment in Foreing Language Teaching. Language and the Teacher: a Series in Applied Linguistics / S. Savignon. – Philadelphia: Center for Curriculum Development, 1972. – 93 p.

к.пед.н. Зарівна О.Т. (ВІТІ НТУУ „КПІ”)
Гангал А.В. (ВІТІ НТУУ „КПІ”)
Хімай Н.І. (ВІТІ НТУУ „КПІ”)

# ПІДГОТОВКА ВІЙСЬКОВОГО ПРОФЕСІОНАЛА В ЗАХІДНІЙ ВІЙСЬКОВІЙ ШКОЛІ

У сучасному світі спостерігається тенденція до професіоналізації армій. Такі армії відрізняються рівнем професіоналізму особистого складу, його чисельністю, обсягом фінансування тощо. Причин появи цей тенденції є декілька. Вони полягають в тому, що в сучасних умовах значно зменшується ймовірність ведення світової війни, а збільшується можливість участі підрозділів армії в локальних воєнних конфліктах та миротворчих операціях. Це потребує достатньо високого рівня підготовки військового фахівця. Проблема підготовки військового професіонала в західних країнах знайшла певне відображення у наукових дослідженнях зарубіжних та вітчизняних вчених: Р. Доора, Р. Річардсона, Ч. Коттона, В. Хаузера Д. Оніщука, Ю. Грошева, Л. Полякова, С. Рожкова, О. Овечкіна, В. Мандрагелі, Л. Іващенка, Ю. Фіногенова, та інших.

В індивідуально-особистісному аспекті формування військового професіонала детерміновано необхідністю реалізації військовослужбовцями своїх духовних і фізичних потенцій, саморозвитку та самореалізації особистості. Таким чином, можна стверджувати, що формування та підготовка військового професіонала обумовлено потребами гуманізації та гуманітаризації військової діяльності, забезпечення національної безпеки держави у воєнній сфері. Способи та форми діяльності суб’єктів соціального формування військового професіонала також обумовлені змістом закономірностей, які визначають особливості функціонування й розвиток суспільства і збройних силі.

Військова освіта історично набуває інтенсивного розвитку з моменту створення в XVII столітті регулярних армій. Обумовлено це тим, що військова справа стала вимагати певного рівня професіоналізму, і, як наслідок, спеціалізація військової діяльності не могла здійснюватися лише на основі досвіду, що набуто в бойових походах і битвах. Потрібні були професіональні знання, вміння, навички, що набуваються в процесі попередньої підготовки в військово-навчальних закладах.

Ретельне дослідження означеної проблеми вимагає обов’язкового виконання двох умов. Перша – з’ясувати сутність та виділити всі сторони цього об’єкта і його зв’язки з навколишнім середовищем. Оскільки військова освіта є різновидом освіти в цілому, то вона функціонує і розвивається за законами розвитку суспільного та культурного середовища, що її оточує. Найбільш загальним нам видається таке тлумачення: Освіта – це суспільно організований та унормований процес постійної передачі попередніми поколіннями наступним соціально значимого досвіду, що характеризується компонентами, які взаємоперетинаються, зокрема, засвоєнням досвіду, вихованням якостей поведінки, фізичним та розумовим розвитком особистості... Провідною діяльністю в освіті є навчальна діяльність. Освіта – специфічна галузь суспільного життя, найважливіша передумова розв’язання основних завдань суспільства і держави, необхідна умова суспільного відтворення та суспільної трудової діяльності, формування кадрів для всіх сфер розвитку суспільства. Основні складові (мережа закладів освіти; нормативно-правова база військової освіти; органи управління військовою освітою) взаємодіють між собою та із зовнішнім середовищем, ґрунтуючись на певних законах, закономірностях та принципах. Інтеграція військової і цивільної освіти – не просте, формальне включення низки військових навчальних закладів до складу потужних цивільних університетів та академій, а процес гармонійного об’єднання системи військової освіти і системи вищої цивільної освіти в єдину цілісну загальнодержавну систему освіти. Порівняльний аналіз цивільної та військової освіти дозволяє не тільки побачити певні відмінності, але й визначити шляхи їх інтеграції. Він демонструє різні рольові зобов’язання студентів і курсантів. Єдиний обов’язок студентів –

навчання. У курсантів обов'язок навчатися поєднується з необхідністю виконувати службові обов'язки, які передбачають, по-перше, високий рівень дисципліни, підпорядкування командирам, чітку регламентацію всього процесу не лише навчання, але й життя, жорсткі норми й правила, що сформульовані у військовій присязі та статутах. По-друге, інтереси служби як особливого виду військової діяльності вимагають від курсантів (кадетів) політичної лояльності режиму та накладають на них низку обмежень прав та свобод. Такий ритм навчання та служби витримують далеко не всі. Так, до Військової академії Сухопутних військ США у Вест-Пойнті щорічно вступають 1500 осіб, а через чотири роки закінчують її лише тисяча офіцерів.

Цивільна освіта схильна до пошуку компромісу між жорсткою централізацією в управлінні освітою й повною автономією її функціонування. Такий стан є характерним для країн з традиційною децентралізацією управління освітою (США, Велика Британія, Німеччина, Франція), за виключенням Японії, де централізація управління виступає національною особливістю навчання і виховання. На відміну від цивільної військова освіта виступає прихильником жорсткої централізації управління за вертикаллю як віддзеркалення усієї військової ієрархічної системи. Світова освітня міграція студентів в межах транснаціональної освіти може бути обмежена лише власними фінансовими можливостями. Для військовослужбовців навчання у цивільних навчальних закладах інших країн цілком виключене, а у військових навчальних закладах можливе лише за службовою необхідністю. У основному придбана військова освіта може бути використана лише в межах своєї країни або в її інтересах. Навчання у військових навчальних закладах інших країн носить блоковий характер (НАТО) і не набуло масовості. Необхідність будь-якого наступного навчання (друга, третя вища освіта) цивільною особою визначається переважно особисто. Військовослужбовці, крім власного бажання, повинні отримати дозвіл командування, який повинен мотивуватися службовою необхідністю.

У військових навчальних закладах США пріоритетна увага приділяється формуванню у кадетів відповідно до концепції „Суцільна особистість" трьох головних якостей, які, на думку військово-політичного керівництва, повинні бути притаманні майбутнім офіцерам: компетентність, відповідальність і відданість своїй справі. Крім того, вважається, що випускник військового навчального закладу повинен бути високоінтелектуальним, всебічно освіченим офіцером. У зв'язку з цим, об'єм військових дисциплін у військових навчальних закладах США знижений і не перевищує 15 % загального об'єму навчального часу, а на гуманітарні дисципліни відводиться більш, ніж 50 % загального часу.

У військових навчальних закладах, незалежно від їх належності до будь-якого виду збройних сил, викладається понад 40 загальноосвітніх навчальних дисциплін, які розподіляються на три категорії: обов'язкові, такі, що вивчаються за вибором, та факультативні. Загальноосвітня програма передбачає засвоєння курсантами дисциплін: філософії, міжнародних відносин, політології, психології, економіки, сучасної історії, військової історії, літератури, географії, математики та інших.

Обґрунтовані компоненти парадигми військової освіти сприяють формуванню та розвитку військового професіонала – здатного конструктивно й ефективно виконувати завдання за будь-яких умов і ситуацій військової служби. Особистості військового фахівця, яка поєднує військовий професіоналізм із громадянською відповідальністю, має відповідний світоглядний кругозір, високу свідомість. Ці якості у значній мірі відповідають моделі західної парадигми інноваційної військової освіти, інтегрованої з глобальними трансформаційними процесами в світі.

ЛІТЕРАТУРА

1. *Астаховой В.И., Сидоренко Н.Л.* Глоссарий современного образования. – Харьков: ОКО, 1998. – 288 с.

2. *Олійник Л.В.* Досвід професійної підготовки військових фахівців в арміях провідних держав світу. / Гуманітарний вісник Збройних Сил України. 2006. №4(5). – С.56 – 62.

Лягіна І.А. (ВІТІ НТУУ „КПІ”)

# КУЛЬТУРНА СВІДОМІСТЬ ЯК ЧИННИК ФОРМУВАННЯ ПОЛІЛІНГВОКУЛЬТУРНОЇ КОМПЕТЕНЦІЇ СТУДЕНТІВ НЕМОВНИХ ВУЗІВ НА ЗАНЯТТЯХ З АНГЛІЙСЬКОЇ МОВИ

Процес міжкультурного спілкування в його сучасному визначенні припускає не тільки обмін інформацією комунікантів (представників різних культур), але й формування у них навичок та вмінь міжкультурного комуніканта. Тобто для ефективності здійснення міжкультурного спілкування необхідно формувати у його учасників полілінгвокультурну компетенцію, набуття якої матиме особливе значення для студента немовного ВНЗ. Він матиме змогу ідентифікувати себе як представника своєї культури, усвідомити власну культурно-мовну ідентичність та самореалізуватися в полікультурному світі. Підтвердження цього положення можна знайти в наукових дослідженнях у галузі лінгвокраїнознавства (Є.М.Верещагін, В.Г.Костомаров, Г.Д.Томахін), теорії міжкультурної комунікації (Е.Б. Беррі, Д.Б. Гудков, В.В.Кабакчі, О.А.Леонтович, С.Г.Тер-Мінасова). лінгвокультурології (В.В.Воробйов, В.І. Карасик, Ю.М. Караулов, В.В. Красних, В.О. Маслова), лінгволюдинознавства (В.Г. Байков) та інші.

Ми визначаємо полілінгвокультурну компетенцію як сукупність знань людини – представника однієї культури – про культуру спільноти, мова якої вивчається, національно-культурні особливості та норми соціальної та мовленнєвої поведінки представника іншої культури, а також здатність використовувати ці знання при інтерпретації інших культурних кодів та організовувати власну комунікативну поведінку засобами мови. Слід зауважити, що формування полілінгвокультурної компетенції сприятиме не однобічному, а гармонійному розвитку особистості, оскільки базується на знаннях не тільки чужих, але й власних культурних стандартів. Необхідність формування цієї компетенції зазначена рекомендаціями Ради Європи, які стосуються оновлення освіти, її наближення до замовлення соціуму (Common European Framework … 2003:168). Це рішення пов’язане із створенням умов для практичного використання студентами іноземної мови як засобу соціальної взаємодії в реальних ситуаціях міжкультурного спілкування, як інструменту пізнання іншої картини світу та набуття лінгвокультурного досвіду і його оцінки.

Формування полілінгвокультурної компетенції відбуватиметься завдяки організації викладачем «сюжетів» міжкультурної взаємодії, її плануванню, розробці та реалізації на заняттях з англійської мови в контексті культурно-орієнтованого підходу (Гальскова 2005:5-13) та свідомо-комунікативного методу (Колкер, Установа, Еналиева 2004:12-23).

Інтерес до кола цих проблем зумовлюється тим, що термін „культурна свідомість” має багато синонімічних визначень, і тим, що увага науковців у галузі методики викладання мов більш привернута до формування компетенцій, ніж до розвитку культурної свідомості індивіда, якого ми, слід за Г.В.Єлізаровою (Елизарова 2005:236) розглядаємо як медіатора культур.

Відповідно до мети і пріоритетів зміст навчання будь-якої мови поділяється на чотири змістовні лінії: комунікативну, лінгвістичну, діяльнісну та культурологічну. Інтегративність останньої характеризується багатовимірною структурою і системою культурологічних тем, засвоєння яких неможливе без культурної свідомості людини. Саме культурна свідомість відіграє важливу роль у формуванні вторинної мовної особистості, що згідно з Загальноєвропейськими Рекомендаціями у вивченні і навчанні іноземних мов є провідним завданням курсу іноземної мови.

Аналіз літератури з проблеми виявив, що культурна свідомість є достатньо абстрактним поняттям. Її практично неможливо спостерігати або вимірювати науковими методами. Вона є важливою характеристикою життєвих позицій особистості міжкультурного діалогу, яка має власні цінності та інтереси і спроможна їх захищати.

За визначенням І.В. Привалової (Привалова 2005:28-34), культурна свідомість людини інтегрує знання медіатора культур про культурні предмети, правила і норми комунікативної поведінки партнера. Автор також звертає увагу на співвідношення культурної свідомості із етнополілінгвокультурною свідомістю, яка виконує інтерпретативну та регулятивну функції. В монографії І.В. Привалової також підкреслено, що етнополілінгвокультурна свідомість не конгруентна мовній картині світу, бо містить не тільки свідомі, структуровані та вербалізовані знання, але й підсвідомі. В процесі ж міжкультурного спілкування є необхідним „включення інформаційно-телеологічного режиму" (термін Ю.А.Сорокіна) роботи свідомості та механізмів інформаційного звірення / порівняння (Привалова 2005:38).

Розглядаючи культурну свідомість як чинник успішного міжкультурного спілкування, можна виділити соціоекономічні та лінгвістичні фактори, які сприяють її формуванню: 1) економічний підйом країн: можливості розвитку торгівлі, туристичного бізнесу, навчання за кордоном та ін.; 2) міграція людей; 3) розвиток науки, інформаційних технологій; 4) розширення діапазону мов, носії яких вступають у контакт; 5) необхідність збереження національної культури в процесі глобалізації світу.

Спираючись на дослідження Н.Ф. Бориско, Г.В. Єлізарової, І.В. Привалової (Бориско 2005; Елизарова 2005; Привалова 2005), ми можемо визначити такі складові культурної свідомості:

1) лінгвокраїнознавчі знання про іншу та власну культури, їх розуміння та усвідомлення, а не прийняття як артефакту. Цю складову ми визначаємо як інформаційну свідомість;

2) знання окремої людини або групи людей – представників іншої культури в межах соціуму – становлять культурно зумовлену поведінкову свідомість;

3) знання мови, засобами якої людина висловлює свою культурну позицію, пояснює свої культурні погляди, спираючись на безпосередній власний або соціальний досвід.

Подальшу перспективу дослідження бачимо у розробці комплексу вправ для формування культурної свідомості в продуктивних видах мовленнєвої діяльності.

ЛІТЕРАТУРА

1. *Бориско Н.Ф.* „Общеевропейские компетенции владения иностранным языком: Изучение, обучение, оценка". Анализ некоторых аспектов // Іноземні мови. – 2005. – № 1. – С. 8 –14.

2. *Гальскова Н.Д., Гез Н.И.* Теория обучения иностранным языкам; Лингводидактика и методика: Учеб. пособие для студ. лингв, ун-тов и фак. ин. яз. высш. пед. учеб. заведений. -М.: Издательский центр „Академия", 2005. – 336 с.

3 *.Елизарова Г.В,* Культура и обучение иностранным языкам. – СПб.: КАРО, 2005. - 352 с.

4 *.Колкер Я.М., Устинова К.С, Еналиева Т.М.* Практическая методика обучения иностранному языку. Учеб. пособие для студ. филол. фак. высш. пед. учеб. заведений. – Москва: Издательский центр „Академия", 2004, – 264 с.

5 *.Привалова И.В.* Интеркультура и вербальный знак (лингвокогнитивные основы межкультурной коммуникации): Монография. – М.: Гнозис, 2005. – 472 с.

6. *Common European* Framework of Reference for Languages: Learning, Teaching, Assessing. – CUP, Council of Europe, 2003. – 260 p.

Назаренко І. М. (ВІТІ НТУУ „КПІ”)

# РОЛЬ ЕСТЕТИЧНОГО ВИХОВАННЯ У ФОРМУВАННІ ОСОБИСТОСТІ МАЙБУТНІХ ОФІЦЕРІВ

Боєздатність Збройних Сил України вирішальною мірою залежить від людського фактору, морально-психологічного стану військовослужбовців. Тому одним із головних завдань будівництва та розвитку Збройних Сил України є опрацювання та використання усталених форм і методів виховання, пошук нових можливостей підвищення його ефективності.

Сучасні підходи передбачають досягнення єдності навчання та виховання особового складу, його морально-психологічної готовності до виконання вимог Конституції України, військової присяги і статутів та більш повна реалізація духовного та професійного потенціалу особового складу військ, підвищення його особистої відповідальності за виконання функціональних і службових обов’язків, наказів командирів і начальників.

Професійна підготовка офіцера потребує створення належних умов та застосування різноманітних педагогічних засобів впливу з метою формування високоосвіченої особистості. Високий рівень освіти та фахової підготовки передбачає, окрім іншого сформованість естетичної культури військовослужбовця.

Естетичне виховання дозволяє розвинути у курсантів естетичне ставлення до своєї життєдіяльності, до об’єктів реальності, до праці, сприяє формуванню особистості військовослужбовця розумного, високоморального, духовно багатого, який знає сенс свого життя, цілеспрямовано та активно працює в напрямі найбільш повної самореалізації.

Естетичне виховання курсантів залишається важливим резервом у поліпшенні організації виховної роботи, підвищенні її ефективності. Важливим компонентом культури спілкування і поведінки є розвиток естетичних смаків. Найбільш яскраво зв’язок морального й естетичного в культурі спілкування виражається в етикеті, основними різновидами якого є: загальногромадянський, дипломатичний, професійний, сімейно-побутовий та ін. Розвиваючись, він охоплює звичаї і моральні якості, що визначають уміння поводитися в різних умовах, обставинах, зовнішню охайність людини, вміння ґречно приймати гостей, триматися за столом, провадити бесіду, грамотно й зрозуміло викладати думки тощо.

Етикет воїна Збройних Сил України реалізується в трьох основних сферах: у відносинах, у професійній діяльності, у повсякденній навчальній та професійно-службовій діяльності та в побутових відносинах.

Естетичне виховання посідає особливе місце у формуванні особистості майбутніх офіцерів. Воно здатне гармонізувати, активізувати, підсилити інші аспекти виховання: військове, фізичне, інтелектуальне, моральне, психологічне тощо, сприяючи загальному і всебічному її розвитку.

ЛІТЕРАТУРА

1. *Гамула І. А.* Педагогічні умови впливу службової діяльності на процес формування відповідальності у курсантів військових інститутів МО України. – // Зб. наук. пр. Випуск 2(21). – К.: ВГІ НАОУ, 2001. – С.3 – 11.

2. *Варваров В.И., Вдовюк В.И., Давыдов В.П.* и др.; Под ред. А.В. Барабанщикова. Психология и педагогика высшей военной школы: Учеб. Пособие. – М.: Военизат, 1989. – 366 с.

3. *Ягупов В.В.* Теорія і методика військового навчання: Монографія. – К: Тандем, 2000. – 380 с.

Несин Ю.М. (НТУУ „КПІ”)

# НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ПРИЙНЯТТЯ РІШЕНЬ

Ті часи, коли всесвітня мережа була інформаційним майданчиком лише для найпотужніших світових організацій, давно минули. Сьогодні до Інтернет-спільноти може долучитися не лише компанія, але й фактично будь-яка фізична особа.

У свою чергу контент, який створюється користувачами сервісів, зробив можливим безліч технологій на зразок блогів, Вікіпедії, подкастингу тощо. Користь від цих технологій для прийняття рішень очевидна, адже це один із найкращих та найефективніших способів полегшити прийняття рішення спеціального призначення. Проте, сучасні системи аналізу лише частково справляються із цим завданням, адже вони здатні ефективно працювати тільки з чітко окресленим масивом інформації і часто не здатні ефективно обмінюватися даними з іншими системами. Іншими словами, програми, які здатні працювати з різними типами даних, рідко можуть взаємодіяти між собою.

Процесно-центричні інформаційні технології здатні суттєво скоротити цикл ретрансляції даних від системи до системи, а значить – адаптувати їх для зручнішого використання і тим самим підвищити швидкість прийняття рішення в цілому.

Окрім того, завжди актуальною залишається розробка нових інформаційних систем. Наприклад, зростання кількості мобільних споживачів змушує замислитися про розробку мобільних корпоративних інформаційних систем. Проте, до сих пір максимум, на що могли розраховувати особи, які приймають рішення, – це мобільна електронна пошта. А тенденції вказують на подальший розвиток мобільних технологій, завдяки яким можна отримати доступ до даних систем із будь-якої точки світу, що, безперечно, також сприятиме підвищенню гнучкості та швидкості прийняття рішення.

Нині інформаційні технології поширюються далеко за межі Інтернет і доходять практично до усіх галузей. Наприклад, 90 % усіх нововведень в автомобілях BMW припадає на програмне забезпечення та комп’ютерну галузь. Машини BMW стали величезною мережею комп’ютерів. Схожі тенденції відбуваються і в інших галузях, навіть у консервативному машинобудуванні. Технології користуються шаленим попитом. Наприклад, у тому ж Китаї лише виробництвом мікрочіпів займаються 400 компаній. І вони розвиваються. Процвітання Китаю та Індії ґрунтується на двох рушійних силах: глобалізація та поширення інформаційних технологій. І саме нові інтелектуальні технології стоять в центрі прийняття рішень спеціального призначення.

Повертаючись до історії інформаційних технологій можна зробити висновок, що для зростання та розвитку технологій одних лише винаходів та інновацій може виявитися замало. Потрібна сприятлива екосистема, яка б підтримала розвиток технологій.

Отже, сполучення та модифікація різноманітних тенденцій у сфері технологій, починаючи від апаратного та програмного забезпечення, інфраструктури, і закінчуючи розробкою систем, призведе, зрештою, до того, що основною конкурентною перевагою стане гнучкість та вміння швидко змінюватися.

ЛІТЕРАТУРА

1. *Алькема В.Г., Сумець О.М.* Логістика. Теорія та практика. Навч. посіб. – К.: „Видавничий дім”, „Професіонал”, 2008. – 272 с.

2. *Козак І.А.* Інформаційні технології віртуальних організацій: Навч.посіб. – К.: КНЕУ, 2005. – 336 с.

3. *Гевко І.Б.* Методи прийняття управлінських рішень. Підручник для ВНЗ. – К.: „Кондор”, 2009 . – 187 с.

к.пед.н. Романюк І.М. (НАОУ)
к.в.н. Микусь С.А. (НАОУ)

# ПРИНЦИПИ КРЕДИТНО-МОДУЛЬНОЇ ТЕХНОЛОГІЇ НАВЧАННЯ

Будь-яка технологія навчання має свої педагогічні особливості, які суттєво відрізняють її від інших навчальних технологій. Окремі з них є провідними, без них навчальна технологія втрачає свою сутність, перестає бути сама собою. В основі навчального процесу лежать вихідні положення (принципи), за якими визначаються організаційні форми, прийоми і методи, навчання. Дидактичні принципи можна поділити на дві групи: загальні і специфічні. Загальні дидактичні принципи стосуються будь-якого навчального пронесу. Частина вихідних положень відносяться до змісту і методів викладання, а саме: принципи доступності, наочності, зв'язку теорії з практикою, професійної спрямованості, науковості. Ряд принципів пов'язані з навчальною діяльністю тих, хто навчається: активності і самостійності систематичності ї послідовності навчання, міцності засвоєння знань, поєднання навчальної діяльності з науковою. Основу специфічних принципів складатимуть ті, які є визначальними у тій, чи іншій технології навчання, вони дають змогу виокремити технологію з-поміж інших, формують її назву. Кредитно-модульна технологія навчання логічно увібрала в себе два дидактичні поняття кредиту і модуля, які суттєво впливають на підхід до організації засвоєння знань з тієї чи іншої дисципліни, а також спонукають підпорядкувати інші навчальні компоненти (форми, прийоми, методи, засоби тощо) своїм вимогам. Специфічними принципами кредитно-модульної технології навчання є: принципи гуманізації і гуманітаризації, демократизації, кредитності, модульності, індивідуалізації, диференціації, інтеграції. **Гуманізація** передбачає беззастережне визнання загальнолюдських цінностей (милосердя, доброта, чесність, правдивість, справедливість, гідність тощо), і формування громадянина-патріота. Гуманізація – це олюднення закладу освіти, створення максимально сприятливих умов для розкриття і розвитку здібностей кожного суб'єкта навчання, формування взаємовідносин на засадах любові до дітей. Принцип гуманізації передбачає таку систему суб'єкт-суб'єктних діалогових взаємовідносин у навчально-виховному закладі, які створюють найсприятливіші умови для розвитку кожним суб'єктом педагогічного процесу своїх духовно-інтелектуальних і творчо-діяльнісних здібностей, неповторних національних, особистісних рис і засвоєння необхідної кількості знань, умінь ї навичок, щоб стати добрим фахівцем. Поняття гуманітарності в освіті видається нам значно ширшим від гуманізації. Зміст слова гуманітарний, включає в себе все, що стосується людини, суспільства. Гуманітаризація в освіті спрямовується не лише на формування гуманістичних взаємин між учасниками навчально-виховного процесу, перетворення тих, хто навчається із об'єкта в суб'єкт навчання, а й передбачає:

– максимальне наближення вивчення кожної навчальної дисципліни до майбутніх потреб тих, хто навчається;

– оптимальне поєднання і узгодження викладання гуманітарних дисциплін і природничо-математичними та професійно орієнтованими;

– посилення ролі гуманітарних наук в усіх навчальних закладах, зокрема й у технічних вищих навчальних закладах;

– формування системи правової культури і правових взаємовідносин у навчальному закладі, які моделюють демократичний устрій держави і включають морально-правову відповідальність учасників навчально-виховного процесу за свої дії відповідно до статуту навчального закладу;

– індивідуалізацію навчання, створення умов для вибору кожним з тих, хто навчається навчальних дисциплін відповідно до структурно-логічних схем та здобуття якісної освіти;

– поєднання загальнолюдських і національних цінностей з світським вихованням;

– формування політичної культури, вміння спілкуватися, відстоювати свої погляди, знаходити компроміси за умов розмаїття політичних сил, не нав'язуючи тим, хто навчається

тих чи інших ідеологічних думок чи позицій. Принцип гуманітаризації спрямовує педагогічні процеси на індивідуальний розвиток і саморозвиток особистості, максимальне наближення вивчення кожної навчальної дисципліни до майбутніх потреб тих, хто навчається, формування системи морально-правових відносин, політичної культури, оптимальне поєднання загальнолюдських і національних цінностей, виховання на засадах християнської моралі, і гуманітарно-зорієнтоване вивчення дисциплін фундаментально і професійної підготовки.

Проблема **демократизації** освітніх процесів логічно випливає з основних засад демократичного суспільства і є його похідною. Важливі суттєві ознаки демократичного навчального закладу:

– забезпечення права вибору випускниками шкіл вищих навчальних закладів лише за покликанням та рівнем підготовки;

– правова нормативність усіх компонентів тих, хто навчається життя і юридична навченість усіх суб'єктів навчально-виховного процесу;

– відкритість і прозорість навчальної установи, свобода слова і запитань;

– громадський компонент в управлінні, повноцінне виконання тих, хто навчається своїх самоврядних функцій, гуманізація суб'єкт-суб'єктних взаємовідносин;

– адаптованість навчальних технологій до реальних потреб тих, хто навчається у здобутті якісної освіти.

Відомо, що кожний з тих, хто навчається – неповторна індивідуальність, зі своїми природними задатками і здібностями, психологічними і фізичними можливостями, зрештою, зі своїм рівнем загальноосвітньої підготовки. Тому одна і та ж сукупність наукових знань матиме різні рівні адаптації, які забезпечуються диференціацією навчального матеріалу, залежно від інтелектуальних можливостей тих, хто навчається. Кожний викладач адаптуючи наукові знання до реальних можливостей тих, хто навчається повинен відчувати критичну межу і не переходити Державний стандарт вищої освіти. Суттєвою ознакою змісту навчання є його доступність, яка забезпечується **диференціацією** когнітивних (знаннєвих) компонентів і тісно взаємопов'язана з індивідуальними особливостями тих, хто навчається. Тобто диференційований зміст навчання, взаємодіючи з суб'єктами навчання, адаптується до них і спонукає зустрічний процес – індивідуалізацію навчання. Власне поняття кредиту й забезпечує реальну індивідуалізацію навчання, оскільки той, хто навчається, з одного боку, має право обирати посильну кількість навчальних дисциплін для наступного засвоєння. Разом з вибором навчальних дисциплін той, хто навчається обирає й найбільш ефективні для себе форми навчання: індивідуальну, індивідуалізовану, індивідуально-групову чи групову. Принцип індивідуалізації передбачає таку технологію організації засвоєння знань, умінь та навичок, яка дає змогу кожному з тих, хто навчається навчатися і розвиватися за індивідуальним планом і програмами, використовуючи оптимальний термін навчання, який відповідає його психолого-фізіологічним можливостям. У зв'язку з **кредитним** вибором навчальних дисциплін спостерігається унікальний процес: ті, хто навчається самостійно і добровільно поділяються, на типологічні групи залежно від рівня своєї підготовленості і реальних можливостей. Звісно, що такий поділ відрізнятиметься від ідеалу і в процесі навчання ті, хто навчається корегуватимуть свої дії: хтось занизив свої можливості, а інший – навпаки. У цих умовах суттєво змінюється роль викладача: він не просто викладає і чекає сесії, а йде на зустріч тим, хто навчається. Вивчивши їхні психологічні особливості, викладач всіма педагогічними методами намагається полегшити і спростити шлях тим, хто навчається до успішного засвоєння змісту навчальної дисципліни. Такими педагогічними засобами є:

– доцільне зменшення навчальних дисциплін у навчальному плані шляхом інтегрування споріднених навчальних дисциплін, які мають спільне ядро знань;

– вмілий, залежно від змісту навчальної дисципліни (трудність і складність, кількість елементів знань тощо), розподіл кредитів між навчальними дисциплінами:

– використання диференційованої (різнорівневої) структури елементів знань навчальної дисципліни, яка адаптується до реальних можливостей тих, хто навчається;

– еклектичне об'єднання навчальних дисциплін у групи (страти) за логічно змістовими лініями з метою зменшення кількості навчальних дисциплін, які вивчатимуться тими, хто навчається одночасно;

– використання високоефективних технологій навчання.

З вищенаведеного випливає, що диференціація виконує важливі функції в кредитно-модульній технології навчання:

– підвищення науковості та доступності навчання, пізнавальної активності тих, хто навчається;

– адаптування змісту навчальних дисциплін до індивідуальних особливостей тих, хто навчається;

– поглиблення, засвоєння дисциплін професійної підготовки, використовуючи максимальну диференціацію їхнього змісту;

– діалектична взаємодія з інтеграцією, посилення розвивальних взаємодій;

– включення тих, хто навчається у науково-дослідну роботу.

Принцип диференціації передбачає горизонтальне і вертикальне структурування навчального матеріалу і адаптування його до реальних психолого-фізіологічних можливостей тих, хто навчається. Принцип кредитності дає змогу тим, хто навчається вільно обирати навчальні дисципліни відповідно до структурно-логічних схем і рекомендацій куратора, спонукає тих, хто навчається брати зобов'язання (і виконувати) щодо вчасного і якісного їхнього засвоєння, а також уніфікує повне навчальне навантаження тих, хто навчається за курсами навчання. Диференційним процесам протидіють інтеграційні.

Під **інтеграцією** у широкому сенсі, слова розуміється приведення змісту освіти до єдиної дидактичної форми для підготовки робітників за групами професій і за професіями широкого профілю, які об'єднуються на основі науково-технічної, соціально-економічної, психоорганізаційної і дидактичної сутностей, що існують у сучасному виробництві і навчанні. Під інтеграцією у вужчому сенсі слова потрібно розуміти приведення загальноосвітніх, загально технічних, спеціальних навчальних предметів, усіх навчально-виробничих робіт в єдиний комплекс (блок). Дидактична інтеграція – це комплекс взаємопов'язаних із диференціацією процесів, які спрямовані на діалектико-методологічне вирішення суперечності між диференціацією й інтеграцією в освіті; включає в себе погоджену інтеграцію змістових компонентів , прийомів, методів і форм навчальної робота, споріднених професій. Дидактична інтеграція у вищій школі виконує такі функції:

– формування цілісних знаннєвих структур у взаємодії загальноосвітніх і професійно-орієнтованих навчальних дисциплін;

– зменшення навчального навантаження на тих, хто навчається у зв'язку з інтеграцією загальнокультурних та суспільних, споріднених професійно-орієнтованих дисциплін, економія навчального часу;

– розвиток абстрактного мислення, узагальнених навичок і вмінь;

– формування основ наукового світогляду, інтегрованих знань з напряму підготовки.

У той же час важко усвідомити, що без добре організованої самостійної роботи тих, хто навчається не можлива індивідуалізація навчання, а тим більше впровадження кредитно-модульної технології навчання. Принцип модульності передбачає організацію засвоєння навчального матеріалу у дискретно-неперервному полі за наперед заданою модульного системою, яка складається з логічно завершених частин навчального матеріалу (модулів), зі структурованим змістом та цілісним навчально-управлінським циклом кожного модуля. Кредитно-модульна технолога навчання, з одного боку, створює реальні можливості для гуманізації і демократизації, індивідуалізації та диференціації, інтеграції і модулювання навчального процесу, а з іншого – ці принципи лежать в її основі, є її специфічними вихідними положеннями, які моделюють нову навчальну технологію.

к.пед.н. Романюк І.М. (НУОУ)

# МОДУЛЬНІ ТЕХНОЛОГІЇ НАВЧАННЯ ЯК НАПРЯМОК У ДОСЯГНЕННІ ВІДПОВІДНОЇ ЯКОСТІ ВИЩОЇ ВІЙСЬКОВОЇ ОСВІТИ

У рамках реформи вищої військової освіти висвітлюються модульні технології щодо підвищення якості вивчення спеціальних дисциплін тими, хто навчається. Розглядається навчальний модуль як завершена структура з цілісним дидактичним змістом.

Освіта є духовним, інтелектуальним, економічним, культурним потенціалом держави. Тому важливо, щоб цей потенціал був могутнім. Одним із шляхів докорінного реформування освіти, у тому числі й військової, є широке запровадження сучасних педагогічних технологій та науково-методичних досягнень. Такими є модульні технології, які забезпечують цілісність і наступність у навчанні при одержанні різних рівнів освіти; підвищення її якості; прозорість і зрозумілість дипломів, варіативність і альтернативність можливостей одержання освіти до індивідуальних потреб та здібностей тих, хто навчається. Модульно-рейтингова система навчання (МРСН), що ще діє в системі освіти, не задовольняє повністю вимог, які постають перед вищими військовими навчальними закладами України в умовах її розбудови. Зміст, форми, методи навчання тих, хто навчається повинні створювати сприятливі умови для одержання такого рівня освіти, який має забезпечувати підготовку випускників – конкурентно спроможних, формувати навички до самостійної роботи, які необхідні для навчання на протязі життя. Аналіз опитувань тих, хто навчається вищих військових навчальних закладів показує, що МРСН зводилась в основному до модульного контролю. Матеріал, що вивчався у семестрі, розбивався на певні модулі і ці модулі оцінювалися певною кількістю балів. Основна увага приділялася контрольним запитанням і завданням з даної теми. Тобто, модуль не розглядався як логічно завершена частина знань з навчальної дисципліни. У нових кредитно-модульних технологіях (КМТ) основна увага приділяється сприйняттю і розумінню того матеріалу, який буде подано у даному модулі. При вивченні матеріалу даного модуля обов'язково враховується мотивація і організація засвоєння знань. Адже цілком раціональним і доцільним є співвідношення: давати тим, хто навчається стільки знань, скільки їм потрібно для успішної майбутньої діяльності. Модульний контроль при цьому є останньою ланкою в навчально-виховному процесі. Для успішного засвоєння модуля матеріал відпрацьовується на лекційних і семінарських заняттях, де тих, хто навчається ознайомлюють з основним змістом модуля, принципами, закономірностями того матеріалу, який вивчається, його головними ідеями, напрямками розвитку науки з цього питання, визначають завдання для самостійної роботи. Для одержання педагогічного ефекту від запровадження модульних технологій навчання необхідно чітко визначити інформаційну функцію, дидактичну роль та призначення усіх запропонованих тим, хто навчається кредитів, а також відпрацювати систему методів, прийомів, вибрати засоби навчання, які будуть допомагати у створенні сприятливих умов для сприйняття і усвідомлення навчальної інформації, формування міцних знань, умінь та навичок їх застосування у службовій діяльності, а також у встановленні рівнозначності між пізнавальними можливостями тих, хто навчається та особливостями організації їх навчальної діяльності. Практична реалізація КМТ у навчально-виховному процесі полягає у системному і поступовому удосконаленні і модернізації традиційних рейтингової, модульної, МРСН. При подачі навчального матеріалу на лекційних заняттях для отримання високого рівня якості знань тих, хто навчається, щоб впливати не тільки на їх „розум", але і на їхні почуття, можна використовувати різноманітні наочні засоби: таблиці, графи, схеми, спеціальні позначення, іншу умовно-графічну наочність. Наприклад, при вивченні модулів „Актуальні аспекти планування бойового застосування підрозділу (частини) зв'язку і АУВ" та „Актуальні аспекти управління підрозділом (частиною) зв'язку і АУВ при підготовці і під час виконання завдань за призначенням" використовувалися схеми організаційно-штатних структур підрозділів, організаційно-технічної побудови елементів системи зв'язку, таблиці оперативно-технічних даних, витяги з різноманітних розпорядчих та керівних документів і т. ін. Усі ці методи

навчання впливають на діяльність тих, хто навчається і приводять до активного засвоєння знань, розвитку пам'яті, уваги. На семінарських заняттях в умовах КМТ крім уже запропонованих схем, таблиць широко застосовуються методичні розробки з тем, які вивчаються, індивідуальні дидактичні завдання на спеціальних картках. Семінарські заняття з конкретної теми – це відносно завершенні ланки навчально-виховного процесу, які є ефективною формою організації навчання для включення тих, хто навчається у посильну діяльність. Тому методичні розробки з тем, що вивчаються у даному модулі, відіграють найважливішу роль у якісному засвоєнні основних питань програмного матеріалу, формування умінь та навичок. При розробці цих методичних вказівок ми розглядали їх як дидактичний елемент структури навчально-виховного процесу, в основі якого лежать принципи активізації самостійної роботи тих, хто навчається. Тому вони мають таку схему.

1. Короткий виклад теоретичного матеріалу. Матеріал, який викладач подає на лекції у логічно систематизованій формі представляє собою складну за змістом навчальну інформацію великого обсягу. У методичних розробках здійснюється виділення окремих структурних елементів понять, що вивчалися на лекційному занятті, коротко і стисло встановлюються логічні взаємозв'язки і відношення між ними.

2. Розв'язання типових завдань. Застосування теоретичного матеріалу, вміння самостійно робити узагальнення, порівняння, систематизацію навчальної інформації, відбувається під час розв'язання стандартних і нестандартних завдань. У запропонованих методичних розробках проводиться розбір типових завдань з теми, що вивчається. При розв'язуванні цих завдань здійснюється засвоєння нових знань, розвиваються творчі здібності та формується слухач як самостійна особистість, що здатна діяти в умовах відсутності безпосереднього та постійного керівництва.

3. Завдання для самостійної роботи (подібні до типових завдань) містять варіанти відповідей. Ці завдання розбиті за рівнями. У першому рівні пропонуються завдання, що потребують тільки основних знань і розуміння конкретних понять з теми. До другого рівня відносяться завдання, які використовуються для формування понять, безпосереднього застосування вивчених варіантів дій. Вони не потребують спеціальної діяльності для пошуку методів прийняття рішення і результат одержуємо через два-три логічних кроки. Такі завдання повинні займати основне місце у навчально-виховному процесі, так як вони спрямовані на стимулювання тих, хто навчається до повторення набутих знань до аналізу навчального матеріалу, до виконання дій для формування умінь та навичок. Завдання третього рівня – це завдання, які застосовуються до глибокого засвоєння тими, хто навчається спеціальних знань, оволодінням деякими методами наукового пізнання. Кожне з цих завдань оцінюється певною кількістю балів. Слухачі виконують їх самостійно, але під керівництвом викладача, яке спрямоване на досягнення певної мети виконання поставлених завдань. Розподіляються конкретні завдання між тими, хто навчається з урахуванням їх індивідуальних пізнавальних можливостей та військового досвіду.

4. Контрольні завдання. Вони підібрані відповідно до розібраних типових завдань, що відпрацьовувалися під керівництвом викладача де ці завдання виконуються вже самостійно, відповідей не містять і обов'язково здаються викладачеві на перевірку. Така схема методичних розробок з кожної теми модуля передбачає виконання таких дидактичних вимог: набуття навичок самостійної роботи, розвиток умінь працювати з довідниковою і методичною літературою, робити узагальнення і висновки, будувати алгоритм прийняття того чи іншого рішення, активізувати свою пізнавальну діяльність. Проведений аналіз сучасного стану КМТ, визначення їх дидактичної сутності, дозволяє зробити висновки, що впровадження їх у навчально-виховний процес вищих військових навчальних закладів є необхідною умовою для досягнення відповідної якості освіти, для розвитку пізнавальних можливостей тих, хто навчається, для реалізації принципу наступності навчання в одержанні різних ступенів освіти, для формування навичок самостійного одержання знань, які необхідні в реаліях сьогодення.

к.пед.н. Уваркіна О.В. (ВІТІ НТУУ „КПІ”)
Степаниця С.Л. (ВІТІ НТУУ „КПІ”)
Коваль А.М. (ВІТІ НТУУ „КПІ”)

# ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ЧИННИК ЗАХИСТУ ОСОБИСТОСТІ В СУЧАСНИХ УМОВАХ

Процеси, що відбуваються в постсоціалістичних країнах висувають багато питань і змушують дослідників переосмислити безліч проблем. Однією з актуальних для сучасних держав, у тому числі й для України, є проблема гарантування інформаційної безпеки людини в сучасних умовах. Розроблені раніше концепції безпеки вимагають постійного удосконалення. Це обумовлено необхідністю нового розуміння світового розвитку залежно від обставин, що безперервно змінюються. Екстраординарного значення набули глобальні проблеми, що загострюються, і вже реально являють загрозу існуванню людства. Науково-технічний прогрес створив умови для прискорення процесів глобалізації громадського життя, становлення взаємообумовленого, взаємозалежного світу. Ці та інші чинники обумовили радикальні зміни суспільно-політичного обличчя світу кінця минулого століття і змусили вчених, політиків звернутись до з’ясування феномена інформаційної безпеки. Науково-теоретичні проблеми інформаційних війн і сучасні методологічні проблеми інформаційної безпеки людини та суспільства у контексті протидії інформаційним війнам стали предметом наукового пошуку В. Андрущенка, О. Білоруса, В. Богуша, М. Дзюби, В. Толубка, В. Пєтухова, Г. Почепцова, В. Ліпкана, О. Литвиненка, Н. Лумана, А. Рося, О. Соболя, В. Трушкова, О. Юдіна, В. Храмова і багатьох інших вчених.

Тотальна інформатизація життя людей призвела до перетворення інформації в чинник, який присутній у кожній із сфер життєдіяльності суспільства. Таке положення дозволяє розглядати інформаційну безпеку, як одну з провідних. Інформаційна безпека є як самостійною складовою національної безпеки, так і складовою частиною кожної з її складових безпеки. Найбільше прийнятним у методичному плані визначенням національної безпеки є таке: це сукупність зв’язків і відношень, які характеризують такий стан особистості, соціальної групи, суспільства, держави, народу, при якому забезпечуються їх тривале, стабільне існування, задоволення і реалізація життєвих потреб, спроможність до ефективного відбиття внутрішніх і зовнішніх загроз, саморозвитку і прогресу. Під кутом цього визначення будемо розглядати зміст поняття інформаційної безпеки.

Плідними є визначення інформаційної безпеки, сформульовані українськими дослідниками В. Толубко та іншими, а саме: як стан інформаційного забезпечення завдань національної безпеки, при якому досягається захищеність і реалізація життєво важливих інтересів, гармонічного розвитку й потреб в інформації особистості, суспільства, держави, незалежно від наявності внутрішніх і зовнішніх загроз.

У змістовному плані під інформаційною безпекою розуміється: по-перше, здатність держави, суспільства, соціальної групи забезпечити з визначеною імовірністю достатні і захищені інформаційні ресурси, надійність функціонування інформаційно-комунікативних систем в інтересах стійкого розвитку суспільства; по-друге, протистояти інформаційним небезпекам і погрозам, негативним інформаційним впливам на суспільну й індивідуальну свідомість, психіку людей, а також на інформаційні структури; по-третє, виробляти особистісні і групові навички і уміння безпечного поводження; по-четверте, підтримувати постійну готовність до адекватних мір в інформаційному протиборстві.

До суб’єктів інформаційної безпеки відносяться: громадяни, громадські або державні організації, які наділені повноваженнями гарантування інформаційної безпеки; державні органи здатні гарантувати інформаційну безпеку. Об’єктами інформаційної безпеки можуть бути окремі особистості, колективи, суспільство, держава, світове співтовариство. Більшість авторів пропонують визначення двох основних видів інформаційної безпеки.

Інформаційна безпека особистості характеризується захищеністю психіки і свідомості від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукування до самогубства, образ і т. ін. Інформаційна безпека суспільства, держави характеризується рівнем їхньої захищеності й, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, суспільної свідомості) стосовно небезпечних (дестабілізуючих, деструктивних, уражаючи інтереси країни) інформаційних впливів, причому як з упровадження, так і до викрадення інформації. Інформаційна безпека держави визначається спроможністю нейтралізувати такі впливи.

Необхідно зазначити, що інформаційні впливи небезпечні (або корисні) не стільки самі по собі, скільки тим, що „оживляють" потужні матеріально-енергетичні процеси, управляють ними. Сутність впливу інформації саме й полягає в її спроможності „оживляти" і контролювати матеріально-енергетичні процеси, параметри яких на багато порядків вище самої інформації. Системний підхід до інформаційної безпеки потребує визначення її суб'єктів, засобів і об'єктів, інформаційних загроз, джерел небезпеки, спрямованості небезпечних інформаційних потоків. Наведемо такі визначення інформаційної загрози: інформаційний вплив (внутрішній або зовнішній), при якому створюється потенційна або актуальна (реальна) небезпека зміни напряму або темпів прогресивного розвитку держави, суспільства, індивідів; небезпека заподіяння шкоди життєво важливим інтересам особистості, суспільства шляхом інформаційного впливу на свідомість, інформаційні ресурси та інфосферу машинно-технічних систем; сукупність чинників, що перешкоджають розвитку й використанню інформаційного середовища в інтересах особистості і суспільства.

Унікальною особливістю інформаційних загроз є те, що вони, з одному боку, являють собою самостійний клас загроз, а з іншого – є реалізаційною основою інших видів загроз на інформаційному рівні, а часто і їх першопричиною.

Джерела інформаційних небезпек можуть бути природними (об'єктивними) і навмисними. Перші виникають у результаті непередбачених помилок і несправностей, випадкових чинників, стихійних лих й ін.

Одна з найбільш поширених причин, які призводять до перекручування інформації в автоматизованих інформаційних системах, і як наслідок, до її втрати, участь спеціаліста в попередньому або підготовчому опрацюванні текстів – реферуванні, анотуванні, індексуванні, класифікації, кодуванні й в інших операціях, які стосуються змісту інформації, що оброблюється. У цьому випадку через суб'єктивізм і розходження в „тезаурусах" цих спеціалістів неможливо домогтися повної ідентичності при опрацюванні семантики близьких документів, у зв'язку з чим перекручування змісту й втрата інформації при пошуку – неминучі. Джерелами навмисних загроз особистості, суспільству, державі, у тому числі й інформаційних, є конфліктні ситуації, викликані суперечностями, обумовленими розбіжністю відповідних інтересів (системи цінностей, цілей) суб'єктів або наявністю в однієї зі сторін стосовно іншої домагань, претензій або інших спонукувань до конфлікту.

Сьогодні існують різні підходи до визначення інформаційної безпеки особистості, суспільства, держави. Таким чином пропонується під інформаційною безпекою розуміти стан захищеності національних інтересів (життєво важливих інтересів особистості, суспільства і держави) в інформаційній сфері від внутрішніх і зовнішніх загроз.

Особливість негативних інформаційно-психологічних впливів на особистість і суспільство у контексті інформаційної безпеки держави полягає в тому, що вони можуть бути виявлені лише в результаті спеціальної експертизи, відповідних наукових досліджень, постійного моніторингу інформаційного простору. Для виявлення небезпеки і потенційних загроз, які мають, як правило, латентний характер, повинні розроблятись і використовуватись спеціальні стандарти безпеки – затверджені у встановленому порядку параметри інформаційно-психологічного впливу, які не викликають негативних наслідків для психіки людини, сформованих у суспільстві стандартів моралі, духовних ідеалів і цінностей.

Шаблій О. С.( НТУУ „КПІ”)

# СУЧАСНІ ПРОБЛЕМИ ФОРМУВАННЯ ОСОБИСТОСТІ ФАХІВЦЯ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА СИСТЕМ ЗВ’ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Смислом і основним показником прогресу людства є розвиток кожної окремої людини на основі її здібностей та особливостей. Процес глобалізації, який супроводжується розвитком сучасних інформаційних технологій, суттєвим чином збільшує сферу комунікації, у якій живе і функціонує людина. Вона отримує нескінченну множину інформаційних впливів з усього світу, вступає у відносини і контакти з громадянами своєї та інших країн. Ці впливи не тільки різноманітні, а й часто суперечливі, протилежні, що суттєвим чином ускладнює визначення самостійної позиції людини.

Тому навчально-виховний процес в освітніх закладах, а також і соціальне середовище суспільства в цілому, мають бути максимально зорієнтовані на формування розвиненої, самодостатньої особистості.

Головною особливістю інформації як частки інфосфери є не її технічні властивості, а особливості соціокультурного функціонування. Інформаційне середовище має розглядатися як один із істотних чинників складного процесу соціальної детермінації поведінки й формування особистості, її самосвідомості, мотиваційно-спонукального процесу; умова різноманітного взаємовпливу і взаєморозуміння людей. Отже, саме тому потрібно зосереджувати увагу не тільки на технічному боці проблеми, а, в першу чергу – на духовному аспекті розвитку людини.

Соціальний та культурний розвиток особистості стимулює її причетність до сфери впливу засобів масової інформації у певних межах. Перебудова диспозиційної структури особистості призводить до якісного стрибка, який на першому етапі виявляється у розширенні діапазону інформаційних (соціокультурних) потреб та підвищенні рівня їх усвідомлення.

Рівень причетності особистості воїна-професіонала до сфери впливу засобів масової інформації підвищується на першому етапі цього розвитку одночасно із засвоєнням індивідом соціального досвіду шляхом належності до соціального середовища, системи соціальних зв’язків, але стабілізується лише на другому етапі, коли у цьому розвиткові починає переважати процес активного виробництва системи соціальних зв’язків особистості за рахунок активної діяльності.

Ефективне формування інформатизації суспільства досягається лише засобами якісної зміни самої особистості, вирішення соціальних програм, інтелектуалізації суспільства, формування інформаційної культури особистості.

Формування особистості військового фахівця в умовах становлення інформаційного соціуму дозволяє виявити типові риси особистості, що мають комплексний характер і всебічно характеризують особистість не тільки із психологічного, а й із соціально-філософського, морального боку, а саме професіоналізм (знання техніки та озброєння, навички їх використання, тактична, морально-психологічна та фізична підготовка тощо); духовність як інтегральна людська якість, сутнісна характеристика внутрішнього світу особистості, яка характеризує ступінь виявлення в особистості ціннісно-трансцендентного начала, онтологічні духовні екзистенціали (добро, красу, любов, істину, творчість, свободу); соціальна відповідальність як вільне виявлення соціальним суб’єктом своїх обов’язків й права обирати за певних умов оптимальний варіант ставлення до дійсності, виходячи із прогресивних інтересів суспільства.

Шалова Н.С. (ВІТІ НТУУ „КПІ”)

# ФОРМУВАННЯ ОСОБИСТОСТІ НАЦІОНАЛЬНОЇ ТЕХНІЧНОЇ ІНТЕЛІГЕНЦІЇ В УМОВАХ СУЧАСНОГО СУСПІЛЬСТВА

Вступ в нову технологічну еру на початку XXI ст. пов’язаний з сучасним станом науково-технічного прогресу, який активно впливає на життя людей і розвиток особистості. Це зумовлює підвищення ролі професійної підготовки фахівців в системі національної освіти і в житті суверенної України. За таких умов виникають нові погляди і методи щодо формування національної технічної інтелігенції.

Особистісна (гуманістична) орієнтація освіти визнана сьогодні вимогою часу. Під кутом зору гуманістичної парадигми як системи вихідних методологічних положень про місце людини в природі і суспільстві доцільно переглянути цілісний навчально-виховний процес для пошуку нових засад його реалізації та прогнозування.

У державній національній програмі „Освіта” як головне завдання професійної освіти визначено, що вона „спрямована на забезпечення професійної самореалізації особистості, формування її кваліфікаційного рівня, створення соціально активного, морально і фізично здорового національного виробничого потенціалу, який посідає важливе місце у технологічному оновленні виробництва, впровадженні у практику досягнень науки і техніки”.

Тому перед педагогічною наукою постає нова проблема – формувати національну технічну інтелігенцію, яка б відповідала вимогам сучасного суспільства. Адже розвиток усіх галузей промисловості і народного господарства, в цілому, в умовах переходу економіки на ринкові відносини потребує нового типу фахівця. Це має бути всебічно освічена, ініціативна особистість, здатна мислити творчо, оволодівати принципово новою технікою і технологією. Такого працівника можна виховати лише у вищих технічних закладах з сучасною матеріально-технічною базою, забезпечених висококваліфікованими інженерно-педагогічними кадрами, укомплектованих контингентом студентів, які психологічно налаштовані на свою майбутню професію, прагнуть оволодіти необхідними професійними якостями.

Врахування традицій вітчизняної вищої школи та аналіз останніх тенденцій суспільного розвитку доводять, що на сьогодні зміст політехнічної освіти мають складати знання:

– наукових принципів найважливіших технологічних процесів провідних галузей народного господарства;

– будови, принципу дії і правил експлуатації найпоширеніших засобів виробництва;

– основ економіки, екології й управління виробництвом, а також практичні вміння управління технічними засобами;

– комунікативно-управлінські та профорієнтаційні навички.

Тільки шляхом поєднання виваженої державної політики з розвитку технічної освіти (узгодження їх „кількості” з „якістю”), впровадження нових навчальних технологій, узгодження вимог промисловості з якістю підготовлених фахівців, за умови врахування передового світового досвіду і поєднання історичних традицій технічної школи України можна відродити національну технічну інтелігенцію

ЛІТЕРАТУРА

1. *Державна національна* програма „Освіта” (Україна XXI століття). – К., 2004. – С. 29.

2. *Інформаційний збірник* Міністерства народної освіти України.–1992. – № 17 – 18. – С. 29.

3. *П’ятницька-Позднякова І.С.* Основи наукових досліджень у вищій школі: Навч. посібник. – К. 2003. – 116 с.

4. *Хруцкий В.И., Корнеев И.С.* Современный маркетинг. – М., 1991.